

# Elementos da Teoria de Aprendizagem de Máquina Supervisionada

Vladimir G. Pestov

# **Elementos da Teoria de Aprendizagem de Máquina Supervisionada**

Vladimir G. Pestov

# **Elementos da Teoria de Aprendizagem de Máquina Supervisionada**

Copyright © 2019 Vladimir G. Pestov.  
Publicado no Brasil / Published in Brazil.

**ISBN** 978-85-244-0428-3

**MSC** (2010) Primary: 68Q3, Secondary: 62H30, 68T05, 68T10

## **Comissão Editorial**

Emanuel Carneiro  
S. Collier Coutinho  
Lorenzo J. Díaz  
Étienne Ghys  
Paulo Sad

**Produção** Books in Bytes

**Capa** Sergio Vaz

## **Realização da Editora do IMPA**

**IMPA**

Estrada Dona Castorina, 110

Jardim Botânico

22460-320 Rio de Janeiro RJ

Telefones: (21) 2529-5005  
2529-5276

[www.impa.br](http://www.impa.br)  
[ddic@impa.br](mailto:ddic@impa.br)

# Sumário

---

<b>1</b>	<b>A geometria de rotulagens</b>	<b>13</b>
1.1	Cubo de Hamming como espaço métrico . . . . .	13
1.2	Teorema isoperimétrico de Harper . . . . .	21
1.3	Cubo de Hamming como espaço probabilístico . . . . .	27
1.4	Concentração de medida . . . . .	36
<b>2</b>	<b>Dimensão de Vapnik–Chervonenkis</b>	<b>46</b>
2.1	Definição e exemplos iniciais . . . . .	46
2.2	Teorema de Pajor e lema de Sauer–Shelah . . . . .	55
2.3	Redes de unidades computacionais . . . . .	57
2.4	Dimensão sensível à escala (fat-shattering dimension) . . . . .	74
<b>3</b>	<b>Aprendizagem PAC</b>	<b>76</b>
3.1	Aprendizagem sob a distribuição puramente atômica . . . . .	77
3.2	Aprendizagem de classes finitas . . . . .	84
3.3	Teorema de Benedek–Itai . . . . .	95
3.4	Taxa de aprendizagem . . . . .	101
<b>4</b>	<b>Classes de Glivenko–Cantelli</b>	<b>106</b>
4.1	Complexidades de Rademacher . . . . .	107
4.2	Minimização da perda empírica . . . . .	125
4.3	Entropia métrica e testemunha de irregularidade . . . . .	129
4.4	Aprendizagem independente de distribuição . . . . .	138
4.5	Tomar cuidado com a mensurabilidade . . . . .	141

<b>5</b>	<b>Consistência universal</b>	<b>149</b>
5.1	Classificador 1-NN de vizinhos mais próximos . . . . .	149
5.2	Erro de Bayes . . . . .	159
5.3	Classificador $k$ -NN . . . . .	164
5.4	Dimensão de Nagata . . . . .	173
<b>6</b>	<b>Redução de dimensionalidade</b>	<b>187</b>
6.1	Maldição de dimensionalidade . . . . .	188
6.2	Lema de Johnson–Lindenstrauss . . . . .	205
6.3	Redução boreliana . . . . .	213
<b>7</b>	<b>Aproximação universal</b>	<b>219</b>
7.1	Problema 13 de Hilbert e teorema da superposição de Kolmogorov . . . . .	220
7.2	Teorema da aproximação universal de Cybenko . . . . .	229
7.3	Minimização de risco estrutural . . . . .	235
<b>8</b>	<b>Compressão amostral</b>	<b>241</b>
8.1	Compressão, descompressão, e aprendizagem . . . . .	241
8.2	Classes extremas . . . . .	248
8.3	Teorema de Moran–Yehudayoff . . . . .	258
<b>A</b>	<b>Variáveis aleatórias: a primeira passagem</b>	<b>271</b>
<b>B</b>	<b>Elementos da teoria de conjuntos</b>	<b>284</b>
B.1	Cardinalidade e ordens . . . . .	284
B.2	Sobre o sistema axiomático ZFC . . . . .	291
B.3	Lema de Zorn . . . . .	295
<b>C</b>	<b>Espaços métricos. Teorema da categoria de Baire</b>	<b>303</b>
C.1	Números reais . . . . .	303
C.2	Métricas, topologias, funções . . . . .	312
C.3	Espaços completos, compactos, e precompactos . . . . .	331
C.4	Teorema da categoria de Baire . . . . .	344
<b>D</b>	<b>Espaços borelianos padrão. Teorema de isomorfismo</b>	<b>350</b>
<b>E</b>	<b>Medidas de probabilidade. Teorema de Carathéodory</b>	<b>356</b>
E.1	Teorema de extensão de medida . . . . .	356
E.2	Parametrização, regularidade, convergência . . . . .	375
<b>F</b>	<b>Teoremas de Hahn–Banach e de Stone–Weierstrass</b>	<b>383</b>
F.1	Espaços normados e espaços de Banach . . . . .	383
F.2	Teorema de Hahn–Banach . . . . .	388
F.3	Teorema de Stone–Weierstrass . . . . .	392

<b>G</b>	<b>Lema de Kronecker</b>	<b>398</b>
<b>H</b>	<b>Integração e desintegração</b>	<b>405</b>
	H.1 Integral de Lebesgue, espaço $L^1(\mu)$ , esperança . . . . .	405
	H.2 Teoremas de Riesz e de Banach–Alaoglu . . . . .	412
	H.3 Convergência de martingales e derivada de Radon–Nikodým . . . . .	421
	H.4 Teorema da desintegração de Rokhlin . . . . .	428
<b>I</b>	<b>Desigualdade de concentração de Paul Lévy</b>	<b>433</b>
	I.1 Fenômeno de concentração . . . . .	433
	I.2 Medida de Haar sobre a esfera euclideana . . . . .	442
	I.3 Concentração de medida na esfera . . . . .	448
<b>J</b>	<b>Teorema Minimax de von Neumann</b>	<b>459</b>
	<b>Bibliografia</b>	<b>463</b>
	<b>Índice Remissivo</b>	<b>472</b>

# Prefácio

---

No Outono do Hemisfério Norte de 2007, o autor decidiu educar-se sobre o assunto de aprendizagem de máquina e ofereceu-se para ministrar um curso de pós-graduação na Universidade de Ottawa, Canadá, baseado inicialmente nas notas [Mendelson 2002] e no livro [Anthony e Bartlett 1999]. O curso foi oferecido novamente em 2012. Com meus alunos de pesquisa nesta área, nós não nos limitamos ao estudo teórico, mas projetamos novos algoritmos e participamos numa série de competições internacionais de mineração de dados, ganhando uma delas em 2013. O nosso modesto seminário de Data Science and Machine Learning cresceu em um verdadeiro grupo de pesquisa na Universidade de Ottawa. Depois de me mudar para o Brasil em 2016, eu ministrei o curso duas vezes na UFSC, Florianópolis, em 2017 e 2018, bem como iniciei um seminário, Grupo de Estudos em Aprendizagem de Máquina (GEAM), na ilha de Santa Catarina. Essas notas de aula, ainda bastante informais, resultam destes cursos e seminários.

As notas são dirigidas principalmente para os matematicamente inclinados. Ao mesmo tempo, elas são quase auto-suficientes, graças a um extenso conjunto de apêndices. É claro que não é realista esperar por um tratamento abrangente de uma área tão vasta; as notas cobrem uma seleção de assuntos altamente subjetiva. No entanto, acredito que elas permitem aprender algumas ideias importantes. Eu evitei propositadamente qualquer tentativa de descrever “aplicações práticas”: nesta área do conhecimento não há necessidade de fazê-lo, dada a curta distância que separa teoria, algoritmos, e implementação.

Esta é uma boa ocasião para reconhecer o quão importante para mim foi a interação nesta área com os meus estudantes de pesquisa ao longo dos anos. Quero mencionar de nome Aleksandar Stojmirović, Christian Despres, Damjan Kalajdzievski, Émilie Idène, Gaël Giordano, Hubert Duan, Igor Artemenko, Ilya Volnyansky, Robert Davies, Sabrina Sixta, Samuel Buteau, Stan Hatko, Sushma Kumari, Varun Singla, Yue Dong.

Sem dúvida, o texto está infestado de erros e lacunas, tanto matemáticos quanto os da expressão portuguesa. Meus agradecimentos vão para os colegas, amigos, e alunos brasileiros que me ajudaram a reduzir o número destes últimos: Aishameriane Schmidt,

Aldrovando Luis Azeredo Araújo, Brittany Beauchamp e Pedro Levit Kaufmann, Maria Inez Cardoso Gonçalves, Natã Machado, e Ricardo Borsoi.

Gostaria de exprimir a minha gratidão pelo apoio do CNPq (bolsa Pesquisador Visitante, Nível 1, Out 2016—Set 2017, processo 310012/2016), da CAPES (bolsa Professor Visitante Estrangeiro Sênior, ao longo do ano 2018, processo 88881.117018/2016-01), e da UFBA, onde sou Professor Visitante Titular desde Março 2019.

*Feci quod potui, faciant meliora potentes.*

Vladimir Pestov  
Rio Vermelho, Salvador, Bahia  
2 de Junho 2019

Instituto de Matemática e Estatística, Universidade Federal da Bahia  
(Professor Visitante)  
Departamento de Matemática, Universidade Federal de Santa Catarina  
(Professor Voluntário)  
Department of Mathematics and Statistics, University of Ottawa  
(Emeritus Professor)



# *Três citações orientadoras*

---



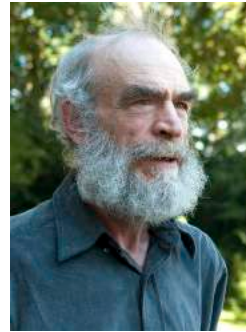
VLADIMIR VAPNIK

“Statistical learning theory does not belong to any specific branch of science: It has its own goals, its own paradigm, and its own techniques.

Statisticians (who have their own paradigm) never considered this theory as part of statistics”.

[Vapnik 2000]

”As the power of computers approaches the theoretical limit and as we turn to more realistic (and thus more complicated) problems, we face ’the curse of dimension’, which stands in the way of successful implementations of numerics in science and engineering. Here one needs a much higher level of mathematical sophistication in computer architecture as well as in computer programming. ...Successes here may provide theoretical means for performing computations with high power growing arrays of data. ...We shall need ... the creation of a new breed of mathematical professionals able to mediate between pure mathematics and applied science. The cross-fertilization of ideas is crucial for the health of the science and mathematics.” [Gromov 1998]



MIKHAÏL GROMOV



SEYMOUR CRAY

”One of my guiding principles is don’t do anything that other people are doing.” <sup>(a)</sup>

---

<sup>a</sup>Computer History Museum, Mountain View, CA, permanent exposition.

# Introdução

---

Vamos começar pela noção básica da *aprendizagem supervisionada*: o *problema de classificação binária*. Para tanto, tomemos uma experiência simples. Geremos  $n = 1000$  pontos aleatórios no quadrado unitário  $[0, 1]^2$ , distribuídos uniformemente e independentemente um do outro. (A *distribuição uniforme* significa que a probabilidade de que um ponto  $x$  pertença a um pequeno quadrado  $[a, a + \epsilon] \times [b, b + \epsilon]$  de lado  $\epsilon > 0$  é proporcional – com efeito, igual – à área do quadrado,  $\epsilon^2$ .) O que conjunto de dados resultante pode parecer, claro, não é uma grade uniforme, mas em vez disso, algo assim (Figura 0.1, esq.).

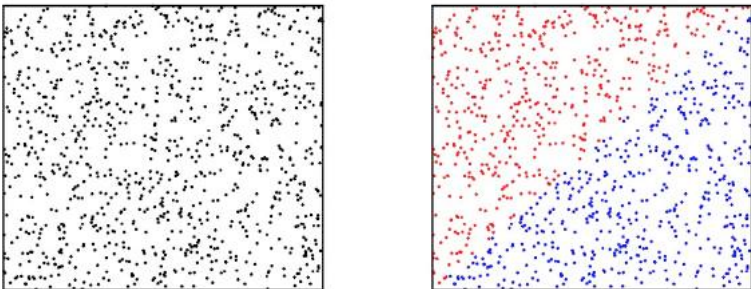


Figura 0.1: Amostra aleatória de 1000 pontos tirados uniformemente do quadrado, não rotulada (esq.) e rotulada (dir.)

Note, em particular, a presença do que aparece como uma estrutura interna de dados significativa: os grandes buracos aqui e ali, agrupamentos de pontos... Estes são, na verdade, desvios aleatórios, não carregando nenhuma informação útil.

O nosso conjunto de dados,

$$X = \{x_1, x_2, \dots, x_{1000}\},$$

é uma *amostra*. O quadrado  $[0, 1]^2$  é o *domínio*.

Agora dividimos os dados em duas classes: a classe  $A$  dos pontos sobre ou acima da diagonal (marcados com vermelho) e a classe  $B$  dos pontos abaixo da diagonal (marcados com azul). Obtemos o que é chamado uma *amostra rotulada* (*labelled sample*). Ver Figura 0.1, (dir.)

Observe um efeito visual interessante: parece que a fronteira entre as duas classes é uma curva ondulada, ao invés de uma linha reta! No entanto, você pode usar uma régua para convencer-se de que não há nenhum erro e os centros de todas as bolinhas vermelhas estão realmente acima da diagonal, enquanto os centros das azuis estão abaixo.

Marcando os elementos de  $A$  com 1 e os elementos de  $B$  com 0, a nossa amostra rotulada pode ser escrita da seguinte maneira:

$$\sigma = (x_1, x_2, \dots, x_{1000}, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_{1000}),$$

onde por valor  $\varepsilon_i$  do rótulo do ponto  $x_i$ , temos  $\varepsilon_i \in \{0, 1\}$ ,  $i = 1, 2, \dots, 1000$ . (Certo, ao invés dos rótulos 0 e 1 se pode usar, por exemplo,  $-1$  e  $+1$ , ou bem  $-$  e  $+$ ...)

Neste exemplo “de brinquedo” a dimensão dos dados é 2, e o conjunto de dados pode ser visualizado, o que ajuda muito para determinar a sua estrutura. Cada ponto é um elemento de  $\mathbb{R}^2$ , representado por duas coordenadas,  $x_i = (x_i^{(1)}, x_i^{(2)})$ . A amostra rotulada  $\sigma$  pode ser tratada como um subconjunto (ordenado) de  $[0, 1] \times [0, 1] \times \{0, 1\}$ , e escrita como uma matriz de dimensão  $1,000 \times 3$ : cada linha  $(x_i^{(1)}, x_i^{(2)}, \varepsilon_i)$  representa um elemento de  $X$ , bem como seu rótulo. Essa representação matricial dos conjuntos de dados é bastante comum. De uma maneira mais abstrata, podemos escrever

$$\sigma \in ([0, 1] \times [0, 1])^n \times \{0, 1\}^n.$$

Chegamos ao seguinte *problema de classificação binária*: a partir da amostra rotulada  $\sigma$ , construir uma função

$$T: [0, 1]^2 \rightarrow \{0, 1\}$$

(chamada *classificador*, *preditor*, ou *função de transferência*), definida sobre todo o domínio, que seja capaz de prever com confiança um rótulo não só para os dados existentes, mas também para novos dados. Pode-se dizer que esse é o problema central da aprendizagem automática estatística *supervisionada*.

Claro que sabemos a resposta para nosso “problema de brinquedo”: ela é dada pelo classificador de verdade

$$T_{true}(x) = \eta(x^{(2)} - x^{(1)}),$$

onde  $\eta$  é a *função de Heaviside*,

$$\eta(x) = \begin{cases} 1, & \text{se } x \geq 0, \\ 0, & \text{se } x < 0. \end{cases}$$

Mas se o problema for mostrado a alguma outra pessoa (ou máquina) que não sabe como as duas classes  $A$  e  $B$  foram formadas, você pode obter outras respostas. Por exemplo, o seu próprio córtex visual, ao analisar a imagem na figura 0.1 (dir.), sugere separar as duas classes com uma linha ondulada! Um tal classificador poderia não ser exato, mas estar perto da verdade para ser aceitável. As chances de *classificação errônea* (o *erro de classificação*) para um novo ponto de dados seriam relativamente pequenos.

Alguém pode sugerir a seguinte solução simplista: atribuir o valor 1 a todos os pontos de dados atuais que estão acima da diagonal, e o valor 0 a todos os outros pontos, atuais e futuros:

$$T(x) = \begin{cases} 1, & \text{se } x \in A, \\ 0, & \text{senão.} \end{cases}$$

Este classificador dá uma resposta correta para todos os pontos atuais  $x_i \in X$ ,  $i = 1, 2, \dots, 1,000$ . No entanto, se nós gerarmos aleatoriamente um novo ponto  $y \in [0, 1]^2$ , com probabilidade  $1/2$  ele ficará acima da diagonal. Ao mesmo tempo, a probabilidade de escolher um ponto em  $X$  é zero. Assim, com probabilidade de  $1/2$ , o classificador  $T$  irá retornar um valor falso para  $y$ . Entre todos os pontos gerados no futuro,

$$x_{1001}, x_{1002}, \dots, x_{1000+n}, \dots,$$

aproximadamente metade deles serão classificados erroneamente. Para  $n$  suficientemente grande, o classificador  $T$  fornecerá uma resposta errada aproximadamente na metade dos casos — certamente um fracasso completo. Jogando a moeda equilibrada podemos conseguir a mesma taxa de sucesso de  $1/2$ , sem usar qualquer classificador, simplesmente atribuindo a um ponto um valor aleatório 0 ou 1.

Como podemos distinguir um bom classificador de um ruim? Ou seja, dado um classificador,  $T$ , existe uma maneira de verificar se  $T$  é suscetível de atribuir a *maioria* dos pontos de dados futuros à classe correta?

À primeira vista, o problema parece completamente intratável: como possivelmente podemos mostrar algo sobre os dados que ainda não existem? Na verdade, é quase incrível que — pelo menos dentro de um modelo teórico — tais predições podem ser feitas com um grau considerável de certeza.

Todavia, vamos deixar este problema para mais tarde. Consideremos um exemplo real: um conjunto de dados da competição CDMC'2013 de mineração de dados para o problema de detecção de intrusos numa rede, coletados por um sistema real IDS (Intrusion Detection System) na Coreia. (Para mais informações, consulte [Song, Takakura e Kwon 2008]. Este conjunto não está disponível publicamente, mas outros conjuntos semelhantes estão, por exemplo<sup>1</sup>.)

<sup>1</sup>DARPA Intrusion Detection Data Sets, MIT Lincoln Lab, <https://www.ll.mit.edu/r-d/datasets>

Cada linha da matriz corresponde a uma sessão, onde as 7 coordenadas são os valores dos parâmetros da sessão. O conjunto de dados contém  $n = 77,959$  elementos, incluindo 71,758 sessões normais (sem intruso), rotuladas +1, e 6,201 sessões ataque (com intruso), rotuladas -1. A Figure 0.2 mostra um extrato das 15 linhas da matriz.

```

.....
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-0.67 2:-0.03 3:0.04 4:1.95 5:-0.05 6:-0.10 7:1.11
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-0.63 2:-0.03 3:0.03 4:1.89 5:-0.05 6:-0.10 7:1.11
+1 1:-0.59 2:-0.03 3:0.03 4:1.83 5:-0.05 6:-0.09 7:1.11
-1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
-1 1:-1.00 2:-0.03 3:-0.09 4:-0.49 5:-0.05 6:-0.15 7:-1.08
+1 1:1.09 2:-0.03 3:-0.02 4:-0.49 5:-0.05 6:-0.15 7:1.11
.....

```

Figura 0.2: Fragmento do conjunto de dados para detecção de intrusos na rede.

O objetivo é de construir um classificador capaz de alertar de um intruso em tempo real com um erro mínimo e uma confiança alta. O que seria o classificador mais natural de se usar, baseado em nossa experiência cotidiana e o senso comum?

Suponha que você queira vender seu carro. Para determinar um preço razoável, você vai buscar algumas informações sobre a venda dos carros do mesmo modelo, idade, milhagem, até a cor. Em outras palavras, você busca um carro o mais semelhante ao seu, e a sua cotação de venda dá uma boa idéia do preço a escolher.

É exatamente como o *classificador de vizinhos mais próximos*, ou o *classificador NN* (Nearest Neighbour Classifier) funciona. Dado um ponto qualquer  $y$  do domínio,  $\Omega$ , buscamos o ponto  $x$  do conjunto de dados atual,  $X$ , mais próximo a  $y$ . O classificador *NN* atribui a  $y$  o mesmo rótulo que o rótulo de  $x$ . Obviamente, a fim de determinar o vizinho mais próximo, precisamos de uma função de semelhança qualquer sobre o domínio:

$$S: \Omega \times \Omega \rightarrow \mathbb{R}.$$

Tipicamente,  $S$  é uma métrica, por exemplo, a métrica euclidiana.

Voltando à venda do carro, provavelmente é mais razoável buscar mais de um carro semelhante ao seu, e determinar o preço baseado sobre uma variedade dos preços destes carros. Obtemos o *classificador de k vizinhos mais próximos*, ou *classificador k-NN*, onde

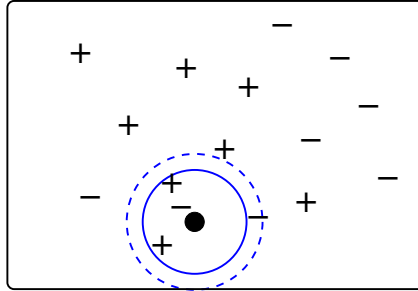


Figura 0.3: O voto majoritário para  $k = 3$ , entre +, +, -, retorna +, a para  $k = 4$ , entre +, +, -, -, é indeciso.

$k$  é um número fixo. Dada a amostra rotulada,

$$\sigma = (x_1, x_2, \dots, x_n, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n) \in \Omega^n \times \{0, 1\}^n,$$

e o ponto da entrada  $y \in \Omega$ , o classificador  $k$ -NN escolhe  $k$  vizinhos mais próximos a  $y$ ,  $x_{i_1}, x_{i_2}, \dots, x_{i_k} \in X$ , e determina o rótulo de  $y$  pelo voto majoritário entre os rótulos  $\varepsilon_{i_1}, \varepsilon_{i_2}, \dots, \varepsilon_{i_k}$ . Se a votação for indecisa (o que é possível se  $k$  for par), o rótulo de  $y$  é escolhido aleatoriamente.

Como podemos garantir que as previsões dadas por um classificador são confiáveis? Na prática, a técnica comumente usada é a *validação cruzada*. O conjunto de dados é dividido aleatoriamente no *conjunto de treinamento* (tipicamente, 75 a 90 por cento dos pontos) e o conjunto de avaliação (o restante 10 a 25 por cento). Somente os dados de treinamento são usados pelo algoritmo, e os dados de avaliação são aplicados para estimar o erro de predição.

Denotemos  $T: \Omega \rightarrow \{0, 1\}$  o classificador,  $X_t$  o conjunto de treinamento, e  $X_a$  o conjunto de avaliação:

$$X = X_t \cup X_a, \quad X_t \cap X_a = \emptyset.$$

O valor seguinte é o estimador estatístico do erro de predição (ou: erro de classificação) de  $T$ :

$$\frac{|\{i : x_i \in X_a, T(x_i) \neq \varepsilon_i\}|}{|X_a|}.$$

O procedimento é iterado muitas vezes, e o valor médio dos erros cada vez estimados serve como uma boa aproximação ao valor do erro verdadeiro de classificação de  $T$ .

Para aplicar classificadores aos conjuntos de dados concretos, é preciso escolher uma linguagem de programação. Teoricamente, qualquer linguagem pode ser utilizada: todas são equivalentes à máquina de Turing! Uma das linguagens utilizada mais comumente em ciência de dados é R, a linguagem de programação estatística, criada no Departamento de Estatística da Universidade de Auckland, Nova Zelândia e baseado em software livre

(no formato do projeto GNU)<sup>2</sup>. A fonte mais abrangente com informações sobre R, *The R Book*, é disponível livremente na web [Crawley 2012].

Sugere-se baixar a linguagem R seguindo as instruções de qualquer uma das fontes mencionadas acima ([Owen 2010] ou [Maindonald 2008]), e experimentar com ela, começando com os exercícios destes livros. Existem muitas implementações disponíveis do classificador  $k$ -NN em R, por exemplo, o classificador IBk do pacote RWeka, ou o do pacote FNN (Fast Nearest Neighbor Search Algorithms and Applications).

**Exercício 0.0.1.** Baixar algum conjunto de dados de Stanford<sup>3</sup>, por exemplo *Phoneme*, e treinar o classificador  $k$ -NN em R.

Aplicando o classificador  $k$ -NN ao nosso conjunto de dados para detecção de intrusos na rede, obtemos um classificador cujo erro de classificação é ao torno de 0.3%.

Certo, é um bom resultado. Todavia, se você participar numa competição, claro que todos os outros participantes vão usar os classificadores padrão. Para melhorar o resultado, é preciso combinar as técnicas conhecidas com as novas abordagens. E antes de melhorar o desempenho do algoritmo, precisamos compreender o que pode ser melhorado, onde há um problema possível?

Mas antes mesmo de examinar esta pergunta, temos uma ainda mais fundamental: por que nós esperamos que o classificador  $k$ -NN funcione, dê resultados confiáveis?

A única maneira de analisar as perguntas deste tipo é no formato de um modelo matemático da aprendizagem supervisionada.

Os dados são modelados pelas *variáveis aleatórias* independentes com valores no nosso domínio,  $\Omega$ . No nosso exemplo “de brinquedo,” o domínio é o quadrado,  $\Omega = [0, 1]^2$ . No segundo exemplo, o domínio é  $\Omega = \mathbb{R}^7$ .

A noção de uma variável aleatória não é apenas o conceito mais fundamental da teoria de probabilidade, mas é, sem dúvida, uma das mais importantes noções em todas as ciências matemáticas. Alguns matemáticos argumentam que, eventualmente, os fundamentos da matemática devem ser alterados de modo que as variáveis aleatórias sejam tratadas juntamente com conjuntos... Nos vamos tratar variáveis aleatórias *ab initio* no apêndice A.

O domínio  $\Omega$  é um espaço métrico separável e completo (como, por exemplo,  $\mathbb{R}^d$ ). Um ponto  $(x, \varepsilon)$  de dados rotulado, onde  $x \in \Omega$ ,  $\varepsilon \in \{0, 1\}$ , é modelado por uma variável aleatória  $(X, Y)$  com valores no produto  $\Omega \times \{0, 1\}$ . Aqui,  $X \in \Omega$  representa um ponto no domínio, e  $Y \in \{0, 1\}$ , o rótulo marcando o ponto. A lei conjunta de  $(X, Y)$  é uma medida de probabilidade,  $\tilde{\mu}$ , sobre  $\Omega \times \{0, 1\}$ . Agora, o ponto  $x \in \Omega$  é dito *instância* da v.a.  $X$ , e o rótulo  $\varepsilon$  é uma instância da v.a.  $Y$ .

É importante ressaltar que, mesmo se sempre supormos que a lei  $\mu$  existe, ela é sempre desconhecida. Também, às vezes o mesmo ponto  $x \in \Omega$  pode aparecer na lista mais de uma vez, obtendo rótulos diferentes.

Uma abordagem alternativa e as vezes mais cômoda é através de uma medida de probabilidade,  $\mu$ , sobre  $\Omega$  (a distribuição de pontos não rotulados), juntada com a *função de*

<sup>2</sup>The R project for statistical computing, <http://www.r-project.org/>

<sup>3</sup><https://web.stanford.edu/hastie/ElemStatLearn//datasets/>



regressão  $\eta: \Omega \rightarrow [0, 1]$ , cuja valor  $\eta(x)$  é a probabilidade de ponto  $x$  ser rotulado 1. As duas abordagens são equivalentes.

Um *classificador* é uma função boreliana (mensurável)

$$T: \Omega \rightarrow \{0, 1\}.$$

Dado um classificador, o seu *erro de classificação* é o valor real, a probabilidade de classificação errada:

$$\begin{aligned} \text{err}_\mu(T) &= P[T(X) \neq Y] \\ &= \mu\{(x, y) \in \Omega \times \{0, 1\}: T(x) \neq y\}. \end{aligned}$$

O *erro de Bayes* é o ínfimo dos erros de classificação de todos os classificadores possíveis sobre  $\Omega$ :

$$\ell^* = \ell^*(\mu) = \inf_T \text{err}_\mu(T).$$

É simples mostrar que, com efeito, o ínfimo é o mínimo, atingido pelo *classificador de Bayes*:

$$T_{\text{bayes}}(x) = \begin{cases} 0, & \text{se } \eta(x) < \frac{1}{2}, \\ 1, & \text{se } \eta(x) \geq \frac{1}{2}, \end{cases}$$

$$\text{err}_\mu(T_{\text{bayes}}) = \ell^*(\mu).$$

O significado do classificador de Bayes é puramente teórico, porque a função de regressão,  $\eta$ , é desconhecida, assim como a lei  $\mu$ .

Uma *regra da aprendizagem* é uma aplicação associando a cada amostra rotulada,  $\sigma$ , um classificador,  $T$ . Dado uma amostra

$$\sigma = (x_1, x_2, \dots, x_n, \varepsilon_1, \varepsilon_2, \dots, \varepsilon_n),$$

a regra produz um classificador,  $T = \mathcal{L}_n(\sigma)$ , que é uma função boreliana de  $\Omega$  dentro  $\{0, 1\}$ .

De maneira mais formal, podemos dizer que uma regra de aprendizagem é uma família  $\mathcal{L} = (\mathcal{L}_n)_{n=1}^\infty$ , onde para cada  $n = 0, 1, 2, \dots$ ,

$$\mathcal{L}_n: \Omega^n \times \{0, 1\}^n \rightarrow \Omega^{\{0,1\}}.$$

Uma maneira conveniente de escrever  $\mathcal{L}_n$  é de avaliar a função  $\mathcal{L}_n(\sigma)$  em ponto  $x \in \Omega$ , obtendo a aplicação

$$\mathcal{L}_n: \Omega^n \times \{0, 1\}^n \times \Omega \rightarrow \{0, 1\}.$$

Estas aplicações de avaliação,

$$\Omega^n \times \{0, 1\}^n \times \Omega \ni (\sigma, x) \mapsto \mathcal{L}_n(\sigma)(x) \in \{0, 1\},$$

devem ser também mensuráveis. Por exemplo, o classificador  $k$ -NN é uma regra de aprendizagem.

A amostra rotulada  $(x_1, x_2, \dots, x_n, \varepsilon_1, \dots, \varepsilon_n)$  é modelada pela sequência

$$(X_1, Y_1), (X_2, Y_2), \dots, (X_n, Y_n)$$

das variáveis independentes com valores em  $\Omega \times \{0, 1\}$ , seguindo a lei fixa porém desconhecida,  $\mu$ . Para cada  $n$ , a regra de aprendizagem só “vê” os  $n$  primeiros pares de variáveis.

O erro de classificação de uma regra de aprendizagem ao nível  $n$  é a esperança do erro sobre todas as amostras rotuladas de tamanho  $n$ :

$$\text{err}_\mu(\mathcal{L}_n) = \mathbb{E}_{\sigma \sim \mu} \text{err}_\mu(\mathcal{L}_n(\sigma)).$$

Existem dois paradigmas principais da teoria de aprendizagem: *consistência universal* e *aprendizagem dentro de uma classe*.

A consistência universal é uma noção mais antiga de duas. A regra de aprendizagem  $\mathcal{L}$  é chamada *consistente* se o erro de classificação converge para o erro de Bayes (o menor possível) em probabilidade quando  $n \rightarrow \infty$ :

$$\forall \varepsilon > 0, \quad P[\text{err}_\mu \mathcal{L}_n > \ell^*(\mu) + \varepsilon] \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Porque não conhecemos a lei subjacente,  $\mu$ , precisamos que a regra de aprendizagem seja consistente para todas as leis possíveis. Isto leva à seguinte definição. A regra  $\mathcal{L}$  é *universalmente consistente* se ela é consistente para cada medida de probabilidade  $\mu$  sobre  $\Omega \times \{0, 1\}$ . O classificador  $k$ -NN foi a primeira regra de aprendizagem cuja consistência universal foi estabelecida.

**Teorema 0.0.2** (Charles Stone [Stone 1977]). *Suponha que  $k = k_n \rightarrow \infty$  e  $k_n/n \rightarrow 0$ . Então o classificador  $k$ -NN em  $\mathbb{R}^d$  (com a distância euclidiana) é universalmente consistente.*

Assim, dentro do modelo atual da aprendizagem estatística, o classificador  $k$ -NN, com alta confiança, dará uma resposta correta a longo prazo, quando o tamanho da amostra é bastante grande.

O teorema de Stone falha nos espaços métricos mais gerais, mesmo no espaço de Hilbert de dimensão infinita. Estudar a consistência universal do classificador  $k$ -NN em vários espaços métricos é um problema interessante, ainda não resolvido completamente. Vamos tratar-nos deste assunto no capítulo 5.

Paradoxalmente, o classificador mais popular e mais eficaz do nosso tempo, a Floresta Aleatória (*Random Forest classifier*, RF), não é universalmente consistente, pelo menos dentro de um modelo simplificado [Biau, Devroye e Lugosi 2008].

Na definição de um algoritmo consistente, o erro de classificação converge para o erro de Bayes em probabilidade. Isso é equivalente ao seguinte. Dado  $\epsilon > 0$  (*erro*) e  $\delta > 0$  (*risco*), existe  $N$  tal que, se  $n \geq N$ , a probabilidade (*confiança*) que o erro de classificação de  $\mathcal{L}_n(\sigma)$  seja inferior a  $\ell^* + \epsilon$  é maior que  $1 - \delta$ . Então, podemos aprender o conceito desconhecido com um qualquer grau de confiança, se temos bastante dados rotulados.

Portanto, não é possível garantir a taxa de convergência uniforme de  $\epsilon$  e  $\delta$  para zero com  $N$ . Com efeito, existem as distribuições  $\mu$  sobre o espaço euclidiano  $\mathbb{R}^m$  cuja convergência do erro e do risco para zero é tão lento quanto se queira.

O segundo paradigma, *aprendizagem dentro uma classe*, se aplica à situação onde o classificador não é universalmente consistente, por exemplo, uma rede neural da geometria fixa, com um número limitado de parâmetros. Aqui, a teoria pode garantir o seguinte: supondo que a amostra pode ser separada pelo classificador bastante bem, com o pequeno *erro de aprendizagem*, o *erro de generalização* estará pequeno também. Em particular, temos os limites uniformes para convergência do erro e do risco para zero.

Relembramos que um classificador binário é uma função mensurável  $f : \Omega \rightarrow \{0, 1\}$ . Frequentemente, não distinguimos entre tal função é o conjunto  $C$  de pontos onde  $f$  toma o valor um:

$$C = \{x \in \Omega : f(x) = 1\}.$$

Neste caso,  $f$  é a função indicadora de  $C$ :

$$f = \chi_C.$$

O conjunto  $C$  neste contexto é chamado um *conceito*. O problema de classificação binária dentro de uma classe é frequentemente analisado sob a hipótese simplificada do que a função de regressão  $\eta$  é determinística, a função indicadora de um conceito. Deste modo, o problema se reduz à aprendizagem de um conceito desconhecido  $C \subseteq \Omega$ . No nosso exemplo “de brinquedo,” o conceito desconhecido é o conjunto  $A$ .

Uma das medidas mais importantes da complexidade de uma classe de conceitos  $\mathcal{C}$  é um parâmetro notável, a *dimensão de Vapnik–Chervonenkis* da classe  $\mathcal{C}$ . Para um subconjunto  $A \subseteq \Omega$ , dizemos que  $\mathcal{C}$  *fragmenta*  $A$ , se cada subconjunto  $B \subseteq A$  pode ser obtido como a interseção de  $A$  com um conjunto  $C \in \mathcal{C}$ :

$$\{A \cap C : C \in \mathcal{C}\} = 2^A.$$

Em outras palavras, cada rotulagem de  $A$  pode ser classificada corretamente com uma função da forma  $\chi_C$ ,  $C \in \mathcal{C}$ .

Por exemplo, o conjunto  $\mathcal{P}$  de todos os semi-planos de  $\mathbb{R}^2$  fragmenta cada subconjunto de três pontos não em posição geral. Ao mesmo tempo, é fácil mostrar que nenhum conjunto com quatro pontos é fragmentado pelos semi-planos.

A dimensão de Vapnik–Chervonenkis (dimensão  $VC$ ) de uma classe  $\mathcal{C}$  de subconjuntos de  $\Omega$  é o supremo de cardinalidades de subconjuntos finitos de  $\Omega$  fragmentados por  $\mathcal{C}$ . Por exemplo, a dimensão  $VC$  da classe de semi-planos em  $\mathbb{R}^2$  é 3.

Agora, um dos resultados principais da teoria de Vapnik–Chervonenkis pode ser formulado assim. Seja  $\mathcal{C}$  uma classe (família de classificadores). As condições seguintes são equivalentes:

- Existem cotas uniformes para o erro de generalização e o risco que dependem apenas de  $n$ , o tamanho da amostra, e não dependem da lei subjacente  $\mu$ .
- A dimensão  $VC$  de  $\mathcal{C}$  é finita.

Algoritmos baseados sobre esta teoria seguem o *Princípio de Minimização do Risco Empírico (ERM)*. A regra  $\mathcal{L}$  está tentando minimizar o erro de aprendizagem, ou bem o *risco empírico*,

$$\frac{1}{n} \#\{i : \varepsilon_i \neq T(x_i)\},$$

onde  $T = \mathcal{L}_n(\sigma)$ . O preço a pagar para controlarmos o erro de classificação é o que tais algoritmos não são universalmente consistentes.

Afinal, há algoritmos que combinam o melhor de dois mundos. Eles são baseados sobre o *Princípio de Minimização do Risco Estrutural*, e são universalmente consistentes ao mesmo tempo que permitem controlar o erro de generalização.

Falemos um pouco sobre a estrutura do texto. No capítulo 1, estudamos o *cubo de Hamming*,  $\{0, 1\}^n$ , um objeto da teoria combinatória, que consiste de todas as sequências binárias de comprimento fixo,  $n$ . Para nos, o cubo tem interesse como o espaço de todas as rotulagens possíveis sobre uma amostra fixa com  $n$  pontos. O cubo de Hamming admite uma métrica e uma medida naturais, e a interação entre as duas estruturas leva a uma geometria e uma versão da análise interessantes. O que é mais importante para nos, é o *fenômeno de concentração de medida*: as funções Lipschitz contínuas sobre o cubo, com constantes de Lipschitz controladas, são altamente concentradas em torno do seu valor mediano (ou: médio), quando  $n$  é bastante grande. Em outras palavras, tais funções têm uma pequena variância.

Pode-se dizer que, intuitivamente, a aprendizagem estatística exige de uma combinação de alta concentração com baixa complexidade. A parte da “alta concentração” está tratada no capítulo 1. Revisitamos a concentração no apêndice I, onde ela vai ser estabelecida para a esfera euclidiana  $S^n$  (a desigualdade clássica de Paul Lévy, que foi o primeiro matemático a isolar o fenômeno explicitamente). A parte da “baixa complexidade” é estudada no capítulo 2, consagrado à dimensão de Vapnik–Chervonenkis. Em particular, estudamos como a dimensão VC se mudar quando as unidades computacionais estão combinadas em uma rede.

Capítulo 3 já trata-se de algumas noções básicas da teoria de aprendizagem automática estatística, inicialmente no contexto de uma lei puramente atômica, quando a distribuição é suportada por uma sequência finita ou enumerável de pontos de massa estritamente positiva. Esta simplificação permite evitar as sutilezas da teoria de medida, e serve como mera ilustração do modelo. Porém, já neste contexto mostramos alguns resultados interessantes, tais como a análise de taxa de convergência do erro de um classificador universalmente consistente para zero, que pode ser tão lenta quanto se queira. Depois de passarmos para medidas gerais, provamos no mesmo capítulo 3 o teorema de Benedek–Itai, afirmando que uma classe de conceitos,  $\mathcal{C}$ , é provavelmente aproximadamente aprendizável sob uma lei fixa,  $\mu$ , se e somente se  $\mathcal{C}$  é precompacto em relação à distância  $L^1(\mu)$ .

A lei dos grandes números diz que, se o tamanho de uma amostra aleatória  $\sigma$  é bastante grande, então, com alta confiança, a medida empírica de um conceito dado,  $C \subseteq \Omega$ , ou seja, a fração de pontos de  $\sigma$  contidos em  $C$ , se aproxima do valor da medida  $\mu(C)$ . Uma classe de conceitos  $\mathcal{C}$  é dito *classe de Glivenko–Cantelli* se, com alta confiança, a mesma conclusão vale para todos os elementos da classe simultaneamente, ou seja, com alta con-

fiança, a medida de cada elemento  $C \in \mathcal{C}$  pode ser aproximada pela medida empírica usando apenas uma amostra aleatória. No capítulo 4 estamos apresentando várias caracterizações de classes de Glivenko–Cantelli sob uma medida fixa, e deduzimos consequências para aprendizagem. Cada classe de Glivenko–Cantelli é *consistentemente aprendizável*, ou seja, cada regra de aprendizagem que busca um elemento da classe induzindo a rotulagem original sempre que possível, aprende  $\mathcal{C}$ . E as classes que são Glivenko–Cantelli uniformemente em relação à medida são exatamente as classes aprendizáveis uniformemente em relação à medida e exatamente as classes de dimensão VC finita.

No capítulo 5 estudamos a noção de consistência universal de uma regra de aprendizagem, e estabelecemos a consistência universal do classificador  $k$ -NN numa grande classe de espaços métricos, os ditos espaços de dimensão de Nagata sigma-finita. Contudo, a descrição completa da classe de espaços métricos onde  $k$ -NN é universalmente consistente resta um problema em aberto.

O assunto do capítulo 6 é o problema seguinte. Em domínios de alta dimensão  $d \gg 1$ , vários algoritmos da ciência de dados muitas vezes levam muito tempo e tornam-se ineficientes. Este fenômeno, conhecido como a maldição de dimensionalidade, é ainda pouco entendido. A redução de dimensionalidade é qualquer função do domínio de dimensão alta para um domínio de dimensão baixa, transferindo o problema de aprendizagem para lá. Nós discutimos alguns aspectos da maldição de dimensionalidade e suas ligações possíveis com o fenômeno de concentração de medida, assim como duas abordagens para reduzir a dimensionalidade: o lema de Johnson–Lindenstrauss (para qual ainda não existe alguma base teórica no cenário da aprendizagem), assim como a redução usando funções injetoras borelianas, que resulta em regras universalmente consistentes.

No capítulo 7, estudamos a capacidade para redes neurais aproximarem uma dada função. Seleccionamos dois resultados importantes. O primeiro, o teorema da superposição de Kolmogorov, diz que, dado  $d \in \mathbb{N}$ , existe uma rede de arquitetura fixa, cujos parâmetros são funções reais de uma variável, que pode gerar todas as funções contínuas em  $d$  variáveis. No entanto, o significado prático desta rede até agora parece ser limitada, pois ela não é facilmente implementável. O segundo resultado, o teorema da aproximação universal de Cybenko, diz que uma rede cujas unidades são funções afins com  $d$  argumentos, e que só tem uma camada escondida, pode aproximar qualquer função  $L^1(\mathbb{R}^d, \mu)$  qualquer que seja  $\mu$ , quando o número de unidades cresce.

Finalmente, no capítulo 8 estudamos a compressão amostral. Assim é chamado um modo de codificar cada elemento  $C$  de uma classe de conceitos,  $\mathcal{C}$ , com uma amostra (rotulada ou não) de tamanho  $\leq d$ , onde  $d$  se chama o *tamanho* do esquema de compressão. O esquema deve satisfazer a restrição seguinte: dada uma amostra finita  $\sigma$ , os conceitos codificados com sub-amostras de  $\sigma$  tendo  $\leq d$  elementos devem produzir todas as mesmas rotulagens sobre  $\sigma$  que os elementos da classe  $\mathcal{C}$ . A maior hipótese em aberto sugere que cada classe de dimensão de Vapnik–Chervonenkis  $\leq d$  admite um esquema de compressão de tamanho  $\leq d$ . Discutimos alguns resultados nesta direção, o mais importante deles sendo o teorema recente de Moran–Yehudayoff afirmando que cada classe de dimensão VC  $\leq d$  admite um esquema de compressão de tamanho exponencial em  $d$ .

Tentámos tornar o texto razoavelmente autónomo com ajuda de apêndices. O apêndice

A contém uma introdução informal à noção de uma variável aleatória, levando o leitor para noções de um espaço boreliano padrão (apêndice D), medida de probabilidade (apêndice E), e esperança / integral (apêndice H). Como pré-requisitos, precisamos elementos da teoria de conjuntos (apêndice B), espaços métricos (apêndice C), e espaços normados (apêndice F), onde introduzimos algumas ferramentas básicas tais como o teorema da categoria de Baire, o teorema de Hahn–Banach, o teorema de Stone–Weierstrass, o teorema de representação de Riesz, etc. Em dois apêndices separados mostramos resultados que não se encaixam na lista acima: o lema de Kronecker (apêndice G) e o teorema Minimax “concreto” de von Neumann (apêndice J). Como já mencionamos, o apêndice I contém a prova da desigualdade de concentração de Paul Lévy.

Alguns comentários sobre a leitura posterior. Meus textos favoritos na área de aprendizagem de máquina teórica são provavelmente [Shalev-Shwartz e Ben-David 2014] e [Vidyasagar 2003]. Acho o livro [Anthony e Bartlett 1999] muito lisível também. A monografia [Devroye, Györfi e Lugosi 1996] oferece uma referência enciclopédica. O livro [Vapnik 2000] é rico em ensinamentos. Também sugiro o livro em preparação interessante [Blum, Hopcroft e Kannan 2016]. A monografia [Dudley 2014] é dedicada à teoria de classes de Glivenko–Cantelli e classes relacionadas. Para alguém que trabalha na análise e teoria de aproximação, a abordagem adotada em [Cucker e Smale 2002; Cucker e D.-X. Zhou 2007] vai ser atraente. O livro [Torgo 2010] pode ajudar a dominar alguns aspectos práticos da ciência de dados.

Estas notas de aula ainda estão em uma forma áspera. Quero convidar o leitor a enviar comentários, criticismos, e correções para <vpst283@uottawa.ca>. Talvez, eventualmente, a segunda edição aparecerá, escrita mais cuidadosamente.

# I

## A geometria de rotulagens

---

O *cubo de Hamming* pode ser visto como o conjunto de todas as rotulagens possíveis de uma dada amostra finita

$$x_1, x_2, \dots, x_n,$$

ou seja, formas de associar a cada ponto de amostra  $x_i$  o rótulo 0 ou 1. O cubo de Hamming, por si só, é um interessante objeto de estudo da geometria discreta.

Neste capítulo, vamos explorar a análise e a geometria do cubo, que nos remeterá às *desigualdades de concentração*.

**Definição 1.0.1.** Seja  $n \in \mathbb{N}$ . O *cubo de Hamming* de dimensão  $n$  is a coleção de todas as seqüências binárias de comprimento  $n$ . É denotado por  $\{0, 1\}^n$  ou  $\Sigma^n$ .

Assim, um elemento  $\sigma \in \Sigma^n$  é da forma

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_n,$$

onde  $\sigma_i \in \Sigma = \{0, 1\}$ , o *alfabeto* de dois símbolos.

Nosso objetivo é equipar  $\Sigma^n$  com algumas estruturas adicionais. A primeira delas será uma distância.

### 1.1 Cubo de Hamming como espaço métrico

### 1.1.1 Distância de Hamming

**Definição 1.1.1.** Seja  $n \in \mathbb{N}$ . A *distância de Hamming* entre duas seqüências de comprimento  $n$ ,  $\sigma, \tau \in \Sigma^n$ , é definida por

$$d(\sigma, \tau) = \#\{i : \sigma_i \neq \tau_i\}.$$

Aqui  $\#$  denota a cardinalidade (o número de elementos) de um conjunto finito. Assim, a distância de Hamming entre duas seqüências de mesmo comprimento é igual ao número de posições nas quais elas diferem entre si. O seguinte é um exercício simples.

**Proposição 1.1.2.** *A distância de Hamming satisfaz as seguintes propriedades.*

1. (*Propriedade de separação*)  $d(\sigma, \tau) = 0 \Leftrightarrow \sigma = \tau$ .
2. (*Simetria*)  $d(\sigma, \tau) = d(\tau, \sigma)$ .
3. (*Desigualdade triangular*)  $d(\sigma, \tau) \leq d(\sigma, \zeta) + d(\zeta, \tau)$ .

Ou seja, a proposição acima garante que a distância de Hamming é uma métrica, e portanto o par  $(\Sigma^n, d)$  é um *espaço métrico* (subs. C.2.1).

Definiremos o *diâmetro* de um espaço métrico  $(X, d)$  como o supremo de distâncias entre todos os pares de pontos de  $X$ :

$$\text{diam}(X) = \sup_{x, y \in X} d(x, y).$$

Temos então que  $\text{diam}(\Sigma^n, d) = n$ , assim o diâmetro do cubo de dimensão  $n$  tende ao infinito quando  $n \rightarrow \infty$ . Para ter um certo controle sobre o tamanho dos cubos no caso assintótico  $n \rightarrow \infty$ , vamos introduzir a seguinte noção.

**Definição 1.1.3.** A *distância de Hamming normalizada* entre duas seqüências de comprimento  $n$  é dada por

$$\bar{d}(\sigma, \tau) = \frac{1}{n}d(\sigma, \tau).$$

Por exemplo,

$$\bar{d}(00110, 10101) = \frac{3}{5}.$$

A vantagem da distância de Hamming normalizada é o fato do diâmetro de  $(\Sigma^n, \bar{d})$  ser igual a um, independentemente do valor de  $n$ . A seguir apresentamos alguns conjuntos associados à distância de Hamming.

**Definição 1.1.4.** Seja  $x$  um ponto num espaço métrico  $(X, d)$  e seja  $\epsilon > 0$ . A *bola aberta* em torno de  $x$  de raio  $\epsilon$  é o conjunto

$$B_\epsilon(x) = \{y \in X \mid d(x, y) < \epsilon\},$$

e a *bola fechada* em torno de  $x$  de raio  $\epsilon$ ,

$$\bar{B}_\epsilon(x) = \{y \in X \mid d(x, y) \leq \epsilon\}.$$



**Exemplo 1.1.5.**  $B_1(0) = \{0\}$ .

**Exemplo 1.1.6.** A bola aberta de raio  $\frac{2}{n}$  em torno de 0 no espaço  $(\Sigma^n, \bar{d})$  consiste de todas as seqüências contendo no máximo um 1.

*Observação 1.1.7.* A estrutura métrica do cubo de Hamming tem sua origem em teoria de códigos corretores de erros, onde as seqüências binárias são vistas como mensagens que serão transmitidas por um canal de comunicações, na presença de ruído, o que significa que alguns bits podem ser corrompidos durante a transmissão. Assumindo que não são muitos os bits corrompidos durante uma transmissão qualquer, digamos não mais do que um dado percentual  $\epsilon < 1$ , existe um eficiente conceito de *código corretor de erros*.

Um *código* é nada mais do que um subconjunto  $A \subseteq \Sigma^n$ . Digamos que  $A$  corrige erros de ordem até  $\epsilon$  se para todos  $a, b \in A$ , as bolas abertas de raio  $\epsilon$  em torno de  $a$  e  $b$  são disjuntas:

$$B_\epsilon(a) \cap B_\epsilon(b) = \emptyset.$$

Esta condição tem o seguinte corolário. Suponha que uma palavra  $\sigma \in A$  foi transmitida e que a palavra  $\sigma'$  foi recebida, com  $\bar{d}(\sigma, \sigma') < \epsilon$  (ou seja, somente uma fração menos do que  $\epsilon$  dos bits foi corrompida). Então,  $\sigma' \in B_\epsilon(\sigma)$  e o fato de que  $a \in A$  e  $\sigma' \in B_\epsilon(a)$  implica  $\sigma = a$ . Assim, para corrigir o erro, é suficiente encontrar em  $A$  o vizinho mais próximo da palavra corrompida,  $\sigma'$ , com relação à distância normalizada de Hamming.

Para uma introdução na teoria de códigos corretores de erros, veja [Hefez e Villela 2017].

## 1.1.2 Homogeneidade

A estrutura métrica do cubo de Hamming é bastante rica. Os resultados que seguem (Proposição 1.1.10 e observação 1.1.12) são válidos para a distância de Hamming e a sua versão normalizada.

**Definição 1.1.8.** Seja  $(X, d)$  um espaço métrico. Uma *isometria* de  $X$  é uma função bijetora  $i: X \rightarrow X$  que preserva as distâncias, isso é, tem a propriedade  $d(x, y) = d(i(x), i(y))$  para cada  $x, y \in X$ .

Por exemplo, toda translação  $x \mapsto x + a$  da reta  $\mathbb{R}$  munida da distância usual é uma isometria. Um outro exemplo da isometria é uma rotação do círculo unitário munido da distância euclideana.

*Observação 1.1.9.* Se o espaço métrico  $X$  é finito, então cada função que preserva as distâncias é automaticamente bijetora.

**Proposição 1.1.10.** O cubo de Hamming  $\Sigma^n$  é metricamente homogêneo, ou seja, para todo  $\sigma, \tau \in \Sigma^n$  existe uma isometria  $i$  de  $\Sigma^n$  tal que  $i(\sigma) = \tau$ .

*Demonstração.* Primeiramente observe que toda aplicação de forma

$$\Sigma^n \ni \sigma \mapsto \sigma + \tau \in \Sigma^n$$

é uma isometria, onde a soma é realizada componente a componente módulo 2:

$$(\sigma + \tau)_i = \sigma_i + \tau_i \pmod{2}.$$

Sejam  $\sigma, \tau \in \Sigma^n$  elementos quaisquer de  $\Sigma^n$ , e seja

$$\zeta = \sigma + \tau.$$

A isometria  $i = \sigma \mapsto \sigma + \zeta$  envia  $\sigma$  para  $\tau$ . □

*Observação 1.1.11.* Na demonstração acima temos que  $i$  permuta  $\sigma$  e  $\tau$ . Porém, nem todo espaço metricamente homogêneo satisfaz esta propriedade (exercício!), a qual é uma forma mais forte de homogeneidade.

*Observação 1.1.12.* As isometrias  $i$  como as apresentadas na demonstração acima são translações em  $\Sigma^n$  quando considerado como um grupo munido da adição (compotente por compotente) módulo 2. Todavia, existem isometrias de outra natureza. A saber, se  $s$  é uma permutação do conjunto  $\{1, 2, \dots, n\}$ , então podemos definir uma isometria de  $\Sigma^n$ , denotada pela mesma letra  $s$ , da seguinte maneira:

$$s(\sigma)_i = \sigma_{s(i)}.$$

Observe que estas isometrias são diferentes das anteriores, pois as permutações mantem o zero (palavra nula) fixo, enquanto a translação, não. A coleção de todas as isometrias  $s$  é isomorfa ao grupo de permutações de posto  $n$ ,  $S_n$ . Pode-se mostrar agora que toda isometria de  $\Sigma^n$  é uma composição de isometrias dos dois tipos apresentados (translações e permutações). Mais exatamente, o grupo de isometrias de  $\Sigma^n$  é o chamado *produto semi-direito*  $S_n \ltimes \Sigma^n$ .

**Definição 1.1.13.** Um espaço métrico  $(X, d)$  é chamado *n-homogêneo*, onde  $n$  é um número natural, se, dados as sub-espacos isométricos  $A$  e  $B$  quaisquer com até  $n$  elementos em cada um e uma isometria  $i: A \rightarrow B$ , existe uma isometria  $j$  de  $X$  que estende  $i$ :  $j|_A = i$ .

Por exemplo, 1-homogeneidade é a homogeneidade métrica usual.

Para uma palavra  $\sigma$ , denote  $\text{supp } \sigma = \{i : \sigma_i = 1\}$ .

**Proposição 1.1.14.** *O cubo de Hamming é 3-homogêneo.*

*Demonstração.* Sejam  $A = \{\sigma_1, \sigma_2, \sigma_3\}$  e  $B = \{\tau_1, \tau_2, \tau_3\}$  duas triplas de palavras quaisquer, tais que  $d(\sigma_i, \sigma_j) = d(\tau_i, \tau_j)$  para todo  $i, j = 1, 2, 3$ .

1. Primeiramente assuma que  $\sigma_1 = 0 = \tau_1$  e  $\sigma_2 = \tau_2$ . Então  $w(\sigma_3) = d(\sigma_3, 0) = w(\tau_3)$ , e como  $d(\sigma_3, \sigma_2) = d(\tau_2, \tau_3)$ , os conjuntos  $\text{supp } \sigma_3 \setminus \text{supp } \sigma_2$  e  $\text{supp } \tau_3 \setminus \text{supp } \tau_2$

(onde  $\sigma_2 = \tau_2$ ) tem o mesmo número de elementos. Logo, existe uma permutação de coordenadas,  $s$ , tal que  $s$  tem  $\text{supp } \sigma_2$  fixo e permuta  $\text{supp } \sigma_3 \setminus \text{supp } \sigma_2$  e  $\text{supp } \tau_3 \setminus \text{supp } \sigma_2$ . Tal  $s$  define uma isometria do cubo, enviando  $\sigma_1 = 0$  e  $\sigma_2$  para se-mesmos e permutando  $\sigma_3$  com  $\tau_3$ .

2. Agora suponhamos que  $\sigma_1 = 0 = \tau_1$ . Neste caso,  $w(\sigma_2) = d(\sigma_2, 0) = w(\tau_2)$ , ou seja,  $\text{supp } \sigma_2$  e  $\text{supp } \tau_2$  tem o mesmo número de elementos, e existe uma permutação de coordenadas, digamos  $t$ , permutando  $\text{supp } \sigma_2$  e  $\text{supp } \tau_2$ . O problema é reduzido para o caso 1, pois  $t(\sigma_1) = 0 = t(\tau_1)$ , entanto  $t(\sigma_2) = t(\tau_2)$ . Podemos escolher  $s$  como no caso 1, e a isometria resultante é da forma

$$t^{-1} \circ s \circ t$$

(verifique!)

3. Finalmente, tratamos o caso geral de duas triplas como acima. Definiremos duas isometrias,  $i_1$  e  $i_2$ , como segue:

$$i_1(\alpha) = \alpha + \sigma_1,$$

$$i_2(\alpha) = \alpha + \tau_1.$$

Então  $i_1(\sigma_1) = 0 = i_2(\tau_1)$ , e as triplas

$$\{i_1(\sigma_1), i_1(\sigma_2), i_1(\sigma_3)\} \text{ e } \{i_2(\tau_1), i_2(\tau_2), i_2(\tau_3)\}$$

satisfazem as hipóteses do caso 2. Escolhemos uma isometria,  $i_3$ , enviando a segunda tripla para a primeira. Logo, a isometria final, enviando  $\{\sigma_1, \sigma_2, \sigma_3\}$  para  $\{\tau_1, \tau_2, \tau_3\}$ , é dada pela composição:

$$i_2^{-1} \circ i_3 \circ i_1.$$

□

*Observação 1.1.15.* É interessante que o cubo de Hamming não é 4-homogêneo, como vemos no exemplo abaixo. A demonstração do lema 1.1.16 e do exemplo 1.1.17 foram feitas por Mike Doherty nas suas soluções de um dever em 2002.

**Lema 1.1.16.** *Se uma isometria do cubo de Hamming deixa 0 fixo, então ela é uma permutação de coordenadas.*

*Demonstração.* Se  $i(0) = 0$ , então  $i$  permuta as palavras com o suporte de um elemento entre elas, e desta maneira, ela determina uma permutação de coordenadas,  $\pi$ . Precisamos verificar que  $i$  age pela permutação sobre todas outras palavras. Toda palavra  $\sigma$  é determinada unicamente pela coleção de distâncias entre ela e as palavras  $00 \dots 0$ ,  $10 \dots 0$ ,  $010 \dots 0$ ,  $\dots$ ,  $000 \dots 01$ . Logo,  $i(\sigma)$  é determinada unicamente pela coleção de distâncias entre  $i(\sigma)$  e as mesmas palavras permutadas pelo  $i$ , logo é igual a  $\pi(\sigma) = \pi(\sigma_1)\pi(\sigma_2) \dots \pi(\sigma_n)$ . □

**Exemplo 1.1.17.** Considere dois quádruplos de palavras (horizontais) em  $\Sigma^4$ :

$$\begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array} \quad e \quad \begin{array}{cccc} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{array}$$

Eles são isométricos (congruentes). Ao mesmo tempo, não existe isometria de  $\Sigma^n$  que envia as palavras correspondentes do primeiro quadro às palavras do segundo. Uma tal isometria,  $i$ , preservaria a palavra zero, então, pelo lema 1.1.16, seria gerada por uma permutação,  $\pi$ , de quatro coordenadas. Examinando as palavras nas 2ª e 3ª linhas, concluímos que a permutação deixa a primeira coordenada fixa:  $\pi(1) = 1$ . Isso não permite à primeira palavra no primeiro quadro ser enviada para a primeira palavra no segundo quadro.

### 1.1.3 Funções

Nosso próximo objetivo é desenvolver uma teoria de funções cujo domínio é  $\Sigma^n$ . Em particular, gostaríamos de saber quais funções são a ser escolhidas como as “agradáveis” de se trabalhar. Os conceitos fundamentais de continuidade e diferenciabilidade, tão importantes em análise, perdem seu significado no caso discreto, pois por exemplo toda função  $f: \Sigma^n \rightarrow \mathbb{R}$  é contínua:

$$\forall \epsilon > 0, \exists \delta > 0, \forall \sigma, \tau \in \Sigma^n, d(\sigma, \tau) < \delta \Rightarrow |f(\sigma) - f(\tau)| < \epsilon,$$

ou seja, dado  $\epsilon > 0$ , basta definir  $\delta = 1$  (para a distância de Hamming normalizada,  $\delta = \frac{1}{n}$ ).<sup>1</sup> A seguir apresentamos uma noção adequada de uma função “agradável” neste contexto.

**Definição 1.1.18.** Uma função real  $f$  sobre um espaço métrico  $(X, d)$  é chamada *Lipschitz contínua* se existe um número real  $L$  tal que para todos  $x, y \in X$

$$|f(x) - f(y)| \leq L \cdot d(x, y).$$

Este  $L$  é chamado uma *constante de Lipschitz* de  $f$ .

O ínfimo de todas as constantes de Lipschitz para uma função Lipschitz contínua  $f$  (que é uma constante de Lipschitz também, exercício), é denotado  $L_f$  ou bem  $\text{Lip}(f)$ . Uma função Lipschitz contínua com  $L = 1$  é chamada uma função *não expansiva*, ou *1-Lipschitz contínua*.

Assim, a constante de Lipschitz  $L$  nos diz que uma função aumenta as distâncias entre os pontos do seu domínio por um fator de  $L$  no máximo.

<sup>1</sup>Com efeito, a topologia de  $\Sigma^n$  é discreta, isso é, cada aplicação de  $\Sigma^n$  para um espaço topológico qualquer é contínua.

*Observação 1.1.19.* De fato, toda função definida no cubo de Hamming, ou em qualquer espaço métrico finito,  $X$ , é Lipschitz contínua: neste caso, temos

$$\text{Lip}(f) = \max_{x,y \in X, x \neq y} \frac{|f(x) - f(y)|}{d(x,y)} < +\infty,$$

pois estamos tomando o máximo em um conjunto finito.

Seria então o caso de se afirmar que o conceito de função Lipschitz contínua não apresenta nenhum significado importante? A resposta é não, pois é justamente o fato de se poder conhecer o valor exato de  $L = \text{Lip}(f)$  que é importante. Informalmente falando,  $L$  mostra quão Lipschitziana uma função Lipschitz contínua é. Os exemplos a seguir vão evidenciar este ponto.

**Exemplo 1.1.20.** Toda função constante é Lipschitz contínua com  $L = 0$ .

**Exemplo 1.1.21.** A função  $\pi_1$  enviando a palavra para o primeiro bit,

$$\pi_1 : \Sigma^n \ni \sigma \mapsto \sigma_1 \in \{0, 1\} \subset \mathbb{R},$$

é Lipschitz contínua com  $L = 1$  em relação à distância de Hamming, e com  $L = n$  em relação à distância de Hamming normalizada. A constante não pode se melhorar: de fato, se  $\sigma = 100 \cdots 0$ , então  $\bar{d}(0, \sigma) = \frac{1}{n}$ , e no mesmo tempo a distância entre as imagens é 1.

**Exemplo 1.1.22.** O número de 1s numa palavra binária  $\sigma$  é o *peso* da palavra, denotado  $w(\sigma)$ :

$$\begin{aligned} w(\sigma) &= \#\{i : \sigma(i) = 1\} \\ &= \sum_{i=1}^n \sigma_i. \end{aligned}$$

De maneira equivalente,

$$w(\sigma) = d(0, \sigma).$$

O peso, visto como a função

$$\Sigma^n \ni \sigma \mapsto w(\sigma) \in \mathbb{R},$$

é Lipschitz contínua com a constante 1 em relação à distância de Hamming.

**Exemplo 1.1.23.** O *peso normalizado* de uma palavra de comprimento  $n$  é definido por

$$\bar{w}(\sigma) = \frac{1}{n} w(\sigma).$$

Por exemplo,

$$\bar{w}(00110110) = \frac{1}{2}.$$

O peso normalizado  $\bar{w}$  é uma função Lipschitz contínua sobre  $(\Sigma^n, \bar{d})$  com  $\text{Lip}(\bar{w}) = 1$ .

**Exemplo 1.1.24.** Visto como uma função

$$w: (\Sigma^n, \bar{d}) \rightarrow \{0, 1\},$$

o peso tem a constante de Lipschitz  $n$ , enquanto o peso normalizado visto como uma função

$$\bar{w}: (\Sigma^n, d) \rightarrow \{0, 1\}$$

tem a constante  $L = \frac{1}{n}$ .

A construção seguinte é uma fonte importante de funções Lipschitz contínuas.

**Definição 1.1.25.** Seja  $A$  um subconjunto não vazio de um espaço métrico  $(X, d)$ . A *função distância de  $A$*  é uma função definida para cada  $x \in X$  por

$$d_A(x) \equiv \text{dist}(x, A) = \inf_{a \in A} d(x, a).$$

Se  $A$  é finito, o ínfimo na definição torna-se o mínimo.

*Observação 1.1.26.* Claro que  $A$  deve ser não vazio: a função  $d_\emptyset$  toma identicamente o valor  $+\infty$ ...

**Lema 1.1.27.** Cada função distância,  $d_A$ , é Lipschitz contínua com  $L = 1$ .

*Demonstração.* Sejam  $x, y \in X$  quaisquer. Dado  $\epsilon > 0$ , existem elementos  $a, b \in A$  tais que  $d(x, a) < d_A(x) + \epsilon$  e  $d(y, b) < d_A(y) + \epsilon$ . Usando a definição de  $d_A$  e a desigualdade triangular, temos

$$\begin{aligned} d_A(x) &\leq d(x, b) \\ &\leq d(x, y) + d(y, b) \\ &< d(x, y) + d_A(y) + \epsilon, \end{aligned}$$

e de maneira semelhante,

$$d_A(y) \leq d(x, y) + d_A(x) + \epsilon.$$

Como as desigualdades são verdadeiras para cada  $\epsilon > 0$ , concluímos que de fato

$$d_A(x) \leq d(x, y) + d_A(y) \text{ e } d_A(y) \leq d(x, y) + d_A(x),$$

como desejado. □

*Observação 1.1.28.* A observação 1.1.19 pode ser invertida: um espaço métrico  $(X, d)$  é finito se e somente se toda função  $f: X \rightarrow \mathbb{R}$  é Lipschitz contínua. Para estabelecer a implicação  $\Leftarrow$ , suponhamos que  $X$  é infinito, ou seja, existe uma aplicação sobrejetora  $\phi: X \rightarrow \mathbb{N}$ . Escolhe um elemento  $x_0 \in X$  e define a função

$$f(x) = \phi(x)d(x, x_0).$$

Como  $\phi(x)$  assume valores positivos arbitrariamente grandes, a função  $f$  não é Lipschitz contínua.

**Definição 1.1.29.** Seja  $f : \Gamma \rightarrow \mathbb{R}$  uma função limitada sobre um conjunto não vazio,  $\Gamma$ . O valor da norma  $\ell^\infty$  de  $f$  é dado por

$$\|f\|_\infty = \sup_{x \in \Gamma} |f(x)|.$$

Se  $\Gamma$  for finito (no caso de nosso interesse,  $\Gamma = \Sigma^n$  será o cubo de Hamming), o supremo é o máximo.

Os fatos seguintes são muito claros.

**Proposição 1.1.30.** *A norma  $\ell^\infty$  tem as seguintes propriedades.*

1.  $\|f\|_\infty = 0 \Leftrightarrow f \equiv 0$ .
2.  $\|\lambda f\|_\infty = |\lambda| \|f\|_\infty$  para todas funções  $f$  e todos  $\lambda \in \mathbb{R}$ .
3.  $\|f + g\|_\infty \leq \|f\|_\infty + \|g\|_\infty$ .
4.  $\|fg\|_\infty \leq \|f\|_\infty \cdot \|g\|_\infty$  (Submultiplicabilidade da norma  $\ell^\infty$ ).
5.  $\|e^f\|_\infty \leq e^{\|f\|_\infty}$ .

(1)-(3) significam que  $\|\cdot\|_\infty$  é uma norma (seção F.1) sobre o espaço vetorial  $\ell^\infty(\Gamma)$  das funções limitadas sobre  $\Gamma$ . □

## 1.2 Teorema isoperimétrico de Harper

Nossa próxima estrutura sobre o cubo de Hamming nasce de uma observação muito simples: dado um subconjunto  $A \subseteq \Sigma^n$ , podemos contar o número dos elementos dele. Este número,  $\#A$ , satisfaz as seguintes propriedades evidentes.

**Proposição 1.2.1.**

1.  $\#\emptyset = 0$ ,  $\#\Sigma^n = 2^n$ .
2. Se  $A \cap B = \emptyset$ , então  $\#(A \cup B) = \#A + \#B$ .

Desse modo, pode-se dizer que a correspondência  $A \mapsto \#A$  é uma medida, chamada a *medida de contagem*. Com efeito, como o conjunto  $\Sigma^n$  é finito, toda família de subconjuntos dois a dois disjuntos é necessariamente finita. Logo, a medida de contagem é mesmo sigma-aditiva:

- (3) *Seja  $A_1, A_2, \dots, A_n, \dots$  uma seqüência qualquer de subconjuntos do cubo dois a dois disjuntos. Então,*

$$\#(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \#(A_i).$$

A soma no lado direito é de fato finita, porque quase todos os termos se anulam.

**Exemplo 1.2.2.** A esfera  $S_r(\sigma)$  de raio  $r \geq 0$ ,

$$S_r(\sigma) = \{\tau \in \Sigma^n : d(\sigma, \tau) = r\},$$

é não-vazia se e somente se  $r \in \{0, 1, \dots, n\}$ . Neste caso, ela satisfaz

$$\#S_r(\sigma) = \binom{n}{r},$$

o coeficiente binomial. De fato, a translação  $x \mapsto x + \sigma \pmod{2}$ , estabelece a correspondência bijetora entre a esfera  $S_r(\sigma)$  e a esfera em torno de zero,  $S_r(0)$ , e a última pode ser identificada com a família de todos os subconjuntos de  $[n] = \{1, 2, 3, \dots, n\}$  contendo exatamente  $r$  elementos.

**Exercício 1.2.3.** Seja  $k \in \mathbb{N}$ . Usar a indução em  $k$  para mostrar que

$$\binom{2k}{k} \leq \frac{4^k}{\sqrt{3k+1}}.$$

Deduzir que, se  $k$  é um número par, então a medida normalizada da esfera de raio  $k/2$  no cubo de Hamming  $\{0, 1\}^k$  satisfaz

$$\mu_{\#}(S_k) \leq \frac{1}{\sqrt{\frac{3}{2}k+1}}.$$

**Exemplo 1.2.4.** A bola fechada,  $\bar{B}_d(\sigma)$ , de raio inteiro  $d \geq 0$ , é a união das esferas:

$$\bar{B}_d(\sigma) = \bigcup_{i=0}^d S_i(\sigma).$$

Como consequência, temos

$$\#\bar{B}_r(\sigma) = \sum_{i=0}^r \binom{n}{i}. \quad (1.1)$$

A estimativa na Eq. (1.1) não é muito conveniente, e por isso vamos obter duas cotas superiores para ela, as quais serão usadas em dois contextos diferentes.

**Lema 1.2.5** (Desigualdade de Euler). *Para todo  $x > 0$  e  $a \in \mathbb{R}$ ,  $a \neq 0$ ,*

$$\left(1 + \frac{a}{x}\right)^x < e^a. \quad (1.2)$$



Este resultado é mostrado nos cursos de Cálculo elementar do primeiro ano, no momento quando a constante de Euler,  $e$ , for definida como o montante no banco que um investidor terá um ano após ser investido R\$ 1 à taxa de juro de 100 % aplicada continuamente – em outras palavras, como o limite

$$e = \lim_{x \rightarrow \infty} \left(1 + \frac{1}{x}\right)^x.$$

O limite existe pois a função sob o sinal do limite é estritamente crescente e limitada acima. A desigualdade de Euler segue-se.

A seguir, apresentamos a primeira estimativa do tamanho da bola no cubo de Hamming.

**Lema 1.2.6.** *Sejam  $1 \leq d \leq n$ . Então*

$$\# \bar{B}_r(\sigma) < \left(\frac{en}{d}\right)^d. \quad (1.3)$$

*Demonstração.* Para todo  $0 \leq i \leq d$ , temos

$$\binom{n}{d}^d \left(\frac{d}{n}\right)^i = \left(\frac{n}{d}\right)^{d-i} \geq 1,$$

e por conseguinte, usando a fórmula binomial e a desigualdade de Euler, concluímos:

$$\begin{aligned} \sum_{i=0}^d \binom{n}{i} &\leq \left(\frac{n}{d}\right)^d \sum_{i=0}^d \binom{n}{i} \left(\frac{d}{n}\right)^i \\ &\leq \left(\frac{n}{d}\right)^d \sum_{i=0}^n \binom{n}{i} \left(\frac{d}{n}\right)^i \\ &= \left(\frac{n}{d}\right)^d \left(1 + \frac{d}{n}\right)^n \\ &< \left(\frac{n}{d}\right)^d e^d \\ &= \left(\frac{en}{d}\right)^d. \end{aligned}$$

□

**Definição 1.2.7.** Dado um subconjunto  $A \subseteq \Sigma^n$  e um número natural  $r$ , denotemos

$$\Gamma_r A = \{\sigma \in \Sigma^n : \exists \alpha \in A, d(\sigma, \alpha) \leq r\}$$

a  $r$ -vizinhança fechada de  $A$  (em relação à distância de Hamming não normalizada).

**Exercício 1.2.8.** Verificar que a  $r$ -vizinhança de uma bola fechada é uma bola fechada:

$$\Gamma_r(B_d(\sigma)) = B_{d+r}(\sigma).$$

O resultado principal desta seção diz que entre todos os subconjuntos do cubo de Hamming, as bolas possuem as menores vizinhanças. Precisamos da definição seguinte.

**Definição 1.2.9.** Um subconjunto  $B$  de  $\Sigma^n$  é chamado uma *bola de Hamming* se existem  $r \in \mathbb{N}$  e  $\sigma \in \Sigma^n$  tais que

$$B_r(\sigma) \subseteq B \subseteq B_{r+1}(\sigma).$$

Em outras palavras, uma bola de Hamming é uma bola fechada mais um pedaço da esfera de raio mais um, ou bem uma região compreendida entre a bola de centro  $\sigma$  e raio  $r$ , e a bola de centro  $\sigma$  e raio  $r + 1$ .

**Teorema 1.2.10** (Desigualdade isoperimétrica de Harper). *Para qualquer  $A \subseteq \Sigma^n$  subconjunto não vazio e  $r \in \mathbb{N}$ , com  $r \leq n$ , existe uma bola de Hamming  $B$  satisfazendo  $\#B = \#A$  e  $\#\Gamma_r B \leq \#\Gamma_r A$ .*

A prova (mais ou menos seguindo [Frankl e Füredi 1981]) ocupa o resto da seção.

**Definição 1.2.11.** A *distância entre dois subconjuntos não-vazios  $A$  e  $B$*  de um espaço métrico  $X$  é a quantidade

$$d(A, B) = \inf\{d(a, b) : a \in A, b \in B\}.$$

(Se pelo menos um de  $A, B$  é compacto, por exemplo finito, então temos o mínimo).

A expressão “distância” é um pouco enganosa, porque a distância entre dois conjuntos não satisfaz necessariamente a desigualdade triangular.

Denotando

$$B = \Sigma^n \setminus \Gamma_r A,$$

temos que  $d(A, B) \geq r + 1$ . Basta mostrar o resultado seguinte.

**Lema 1.2.12.** *Dado dois subconjuntos  $A$  e  $B$  de  $\Sigma^n$  e um número natural  $r$ , com a propriedade  $d(A, B) \geq r$ , existem uma bola de Hamming  $\tilde{A}$  em torno de 0 e uma bola de Hamming  $\tilde{B}$  em torno de 1, tais que  $\#\tilde{A} = \#A$ ,  $\#\tilde{B} = \#B$ , e  $d(\tilde{A}, \tilde{B}) \geq r$ .*

Uma vez que o lema esteja mostrado, teremos  $\Gamma_r \tilde{A} \cap \tilde{B} = \emptyset$ , de onde  $\#\Gamma_r \tilde{A} \leq 2^n - \#\tilde{B}$ , e por conseguinte

$$\#\Gamma_r A = 2^n - \#\tilde{B} \geq 2^n - \#\tilde{B} \geq \#\Gamma_r \tilde{A},$$

como exigido.

Vamos executar uma sequência de transformações simultâneas dos conjuntos  $A$  e  $B$  que não aumentem o tamanho de suas vizinhanças e que os tornam cada vez mais “redondos” de maneira que no final obtemos uma bola de Hamming em torno de 0 e uma bola de Hamming em torno de 1, respetivamente.

**Exercício 1.2.13.** Observe que um subconjunto não vazio  $A \subseteq \Sigma^n$  é uma bola de Hamming em torno de 0, se e somente se, quaisquer que sejam  $\alpha, \beta \in \Sigma^n$ , se  $\alpha \in A$  e  $w(\beta) < w(\alpha)$ , então  $\beta \in A$ . De uma forma rigorosamente equivalente: para cada  $\alpha \in A$  e  $\tau \in \Sigma^n$ , se  $w(\alpha + \tau) < w(\alpha)$ , então  $\alpha + \tau \in A$ .

De mesma maneira, um conjunto  $B \neq \emptyset$  é uma bola de Hamming em torno de 1 se e somente se, qualquer que sejam  $\alpha \in A$  e  $\tau \in \Sigma^n$ , se  $w(\alpha + \tau) > w(\alpha)$ , então  $\alpha + \tau \in A$ .

Dado  $A$  e  $B$  como no lema 1.2.12, escolhamos  $\tau$  do menor peso tal que ou existe  $\alpha \in A$  com  $w(\alpha + \tau) < w(\alpha)$  e  $\alpha + \tau \notin A$ , ou existe  $\beta \in B$  com  $w(\beta + \tau) > w(\beta)$  e  $\beta + \tau \notin B$ . (Se um tal  $\tau$  não existe, então trata-se de duas bolas de Hamming em torno de 0 e 1, e não há nada para mostrar). Definamos a aplicação  $T = T_{A,B,\tau}$  de  $A \cup B$  para  $\Sigma^n$  como segue:

$$\text{se } \alpha \in A, T(\alpha) = \begin{cases} \alpha + \tau, & \text{se } w(\alpha + \tau) < w(\alpha) \text{ e } \alpha + \tau \notin A, \\ \alpha, & \text{de outro modo;} \end{cases}$$

$$\text{se } \beta \in B, T(\beta) = \begin{cases} \beta + \tau, & \text{se } w(\beta + \tau) > w(\beta) \text{ e } \beta + \tau \notin B, \\ \beta, & \text{de outro modo.} \end{cases}$$

É claro que as restrições de  $T$  sobre  $A$  e sobre  $B$  são injetoras. Pode-se mostrar facilmente que se  $a \in A, b \in B$ , e  $T(a) = b$ , então  $T(b) = a$ . De fato, isso não é necessário, pois vamos mostrar em breve que  $d(T(A), T(B)) \geq r$ .

Além disso, se  $\alpha \in A, \beta \in B$ , então  $w(T(\alpha)) \leq w(\alpha)$ ,  $w(T(\beta)) \geq w(\beta)$ , o que significa que o operador  $T$  não aumenta a quantidade

$$\sum_{\alpha \in A} w(\alpha) - \sum_{\beta \in B} w(\beta), \quad (1.4)$$

e de fato, existe pelo menos um elemento  $\gamma \in A \cup B$  que diminui esta quantidade em pelo menos 1. O valor absoluto da expressão (1.4) não excede  $n2^n$ . Isso significa que o procedimento acima (a escolha de  $\tau$  e da aplicação de  $T$ ) só pode ser repetida um número finito de vezes, após o qual chegaremos às duas bolas satisfazendo as conclusões do lema.

A única coisa restante a verificar é a condição

$$d(T(A), T(B)) \geq r.$$

Em outras palavras, quaisquer que sejam  $a \in A, b \in B$ , temos  $d(T(a), T(b)) \geq r$ . Temos três casos distintos.

(1) Ambos os elementos  $T(a), T(b)$  são “antigos”, isso é,  $a \in A \cap T(A), b \in B \cap T(B)$ . Neste caso há nada a mostrar, pois  $d(a, b) \geq r$ .

(2) Ambos os elementos são “novos”:  $a' \in T(A) \setminus A, b' \in T(B) \setminus B$ . Neste caso,  $a' = a + \tau, b' = b + \tau$ , onde  $a \in A, b \in B$ , e temos

$$d(a', b') = d(a + \tau, b + \tau) = d(a, b) \geq r,$$

pois a distância de Hamming é invariante pelas translações.

(3) Um elemento é “novo” e outro, “antigo”. Suponha que  $a' \in T(A) \setminus A$  e  $b \in B \cap T(B)$ . (O caso simétrico  $a \in A \cap T(A)$  e  $b' \in B \setminus T(B)$  é um exercício.)

Se  $b + \tau \in B$ , então podemos concluir:

$$d(a', b) = d(a + \tau, b) = d(a, b + \tau) \geq r,$$

pois  $a \in A$  e  $b + \tau \in B$ . Então, a partir desse momento, suponhamos que  $b + \tau \notin B$ . Como  $T(b) = b$ , concluímos que

$$w(b + \tau) \leq w(b).$$

A adição de  $\tau$  tem efeito de alterar todos os bits em  $\text{supp } \tau$ . A desigualdade acima significa que o número de zeros em  $b\tau$  é menor ou igual ao número de uns em  $b\tau$ , ou seja:

$$w(b\tau) = d(0, b\tau) \geq d(\tau, b\tau). \quad (1.5)$$

Sub-caso (3a):  $\text{supp } b\tau \subseteq \text{supp } a$ , ou seja, para todo  $i$ , se  $\tau_i = 1$  e  $b_i = 1$ , então  $a_i = 1$ . Escrevamos  $b = b_1 + b\tau$ . Agora,  $a'$  e  $b_1$  têm zeros em todas as posições de  $\text{supp } b\tau = \text{supp } \tau \cap \text{supp } b$ , e por isso:

$$\begin{aligned} d(a', b) &= d(a', b_1) + w(b\tau) \\ &\geq d(a', b_1) + d(\tau, b\tau) \\ &= d(a', b_1 + b\tau) + d(b + \tau, b + b\tau) \\ &\geq d(a', b + \tau) \\ &= d(a, b) \geq r. \end{aligned}$$

Sub-caso (3b):  $\text{supp } \tau b \not\subseteq \text{supp } a$ , ou seja, existe  $i$  tal que  $\tau_i = 1$ ,  $b_i = 1$ , e  $a_i = 0$ . Escolhemos um tal índice  $i$ . Como  $w(a + \tau) < w(a)$ , o número de uns em  $a\tau$  é estritamente maior do que o número de zeros. Em outras palavras,  $\#(\text{supp } a \cap \text{supp } \tau) > (1/2)\#\text{supp } \tau$ . Relembremos que o número de uns em  $b\tau$  é maior ou igual ao número de zeros, ou seja,  $\#(\text{supp } b \cap \text{supp } \tau) \geq (1/2)\#\text{supp } \tau$ . Por conseguinte, os subconjuntos  $\text{supp } a \cap \text{supp } \tau$  e  $\text{supp } b \cap \text{supp } \tau$  se encontram, e existe  $j$  tal que  $\tau_j = 1$ ,  $b_j = 1$ , e  $a_j = 1$ . Escolhamos um tal  $j$ . Elimine do suporte de  $\tau$  os índices  $i$  e  $j$ , para obter a palavra  $\tilde{\tau}$  com  $\text{supp } \tilde{\tau} = \text{supp } \tau \setminus \{i, j\}$ . É claro que  $w(a + \tilde{\tau}) = w(a + \tau) < w(a)$ . Como  $\tau$  tem o peso minimal, concluímos que  $a + \tilde{\tau} \in A$ , logo  $d(a + \tilde{\tau}, b) \geq r$ . A palavra  $a' = a + \tau$  só difere de  $a + \tilde{\tau}$  em coordenadas  $i$  e  $j$ . Temos  $(a + \tilde{\tau})_i = a_i = 0$  e  $b_i = 1$ , de onde  $|(a + \tilde{\tau})_i - b_i| = 1$ . Ao mesmo tempo,  $a'_i = 1$ , de onde  $|a'_i - b_i| = 0$ . De mesma maneira,  $|(a + \tilde{\tau})_j - b_j| = 0$  e  $|a'_j - b_j| = 1$ . Concluímos:

$$d(a', b) = d(a + \tilde{\tau}, b) \geq r.$$

*Observação 1.2.14.* Eis o exemplo de espaço métrico finito natural e importante, de fato semelhante ao cubo de Hamming  $\{0, 1\}^n$ , cujo problema isoperimétrico parece ainda estar em aberto.

O grupo simétrico  $S_n$  de posto  $n$  consiste de todas as auto-bijeções do conjunto  $[n] = \{1, 2, \dots, n\}$  com  $n$  elementos (este  $n$  entre colchetes é uma notação da teoria combinatória), munido da lei de composição de aplicações. Definamos a *métrica de Hamming* sobre  $S_n$  como segue:

$$d(\sigma, \tau) = \#\{i \in [n]: \sigma(i) \neq \tau(i)\}.$$

Pode se verificar facilmente que  $d$  é uma métrica *bi-invariante*, ou seja: quaisquer que sejam  $\sigma, \tau, \alpha \in S_n$ ,

$$d(\alpha\sigma, \alpha\tau) = d(\sigma, \tau) = d(\sigma\alpha, \tau\alpha).$$

Quais conjuntos  $B$  possuem o menor tamanho da  $r$ -vizinhança  $\Gamma_r B$  entre todos os conjuntos  $A$  com  $\#A = \#B$ ? Se sabe que as bolas fechadas em  $S_n$  *não têm* esta propriedade.

## 1.3 Cubo de Hamming como espaço probabilístico

### 1.3.1 Medida de contagem normalizada

A cardinalidade do cubo de posto  $n$  é igual a  $2^n$ , e com o intuito de conseguir trabalhar com os cubos de postos diferentes,  $\Sigma^n$  e  $\Sigma^m$ , simultaneamente, vamos realizar a normalização.

**Definição 1.3.1.** Seja  $A \subseteq \Sigma^n$  um subconjunto qualquer. A *medida de contagem normalizada* de  $A$  é dada por

$$\mu_{\#}(A) = \frac{\#A}{2^n}.$$

**Exemplo 1.3.2.** A medida normalizada de um conjunto unitário é

$$\mu_{\#}(\{\sigma\}) = \frac{1}{2^n}.$$

As propriedades da medida de contagem normalizada são seguintes.

**Proposição 1.3.3.**

1.  $\mu_{\#}(\emptyset) = 0$ ,  $\mu_{\#}(\Sigma^n) = 1$ .
2. Se  $A \subseteq B$ , então  $\mu_{\#}(A) \leq \mu_{\#}(B)$ .
3. Se  $A \cap B = \emptyset$ , então  $\mu_{\#}(A \cup B) = \mu_{\#}(A) + \mu_{\#}(B)$ .

Podemos substituir a condição (3) por uma condição formalmente mais forte, a *sigma-aditividade*: dada uma sequência qualquer de subconjuntos dois a dois disjuntos,  $A_1, A_2, \dots$  de  $\Sigma^n$ , temos

$$\mu_{\#}(\cup_i A_i) = \sum_i \mu_{\#}(A_i).$$

É verdadeiro porque temos  $A_i = \emptyset$  a partir de um  $i$  suficientemente grande.

*Observação 1.3.4.* A condição

$$\mu_{\#}(\Sigma^n) = 1$$

significa que  $\mu_{\#}$  é uma *medida de probabilidade*. Do ponto de vista probabilístico,  $\Sigma^n$  é o *espaço de eventos elementares*, ou o *espaço amostral*, que corresponde ao experimento aleatório de jogar uma moeda equilibrada  $n$  vezes. A sequência binária codifica o resultado do experimento, com, por exemplo, 0 correspondente à cara e 1 à coroa. Um *evento* é um subconjunto qualquer de  $A \subseteq \Sigma^n$ . Por exemplo, o subconjunto

$$A = \{\sigma \mid \sigma_1 = 0\}$$

corresponde ao evento “no primeiro lançamento, a moeda tirou a cara”. Neste contexto, a medida de contagem normalizada de um conjunto se interpreta como a *probabilidade* do evento  $A$ :

$$\mu_{\#}(A) = P(A).$$

Para um tratamento um pouco mais sistemático das medidas de probabilidade, veja apêndice E.

**Exercício 1.3.5.** Sejam  $n, r \in \mathbb{N}$ , onde  $r < n/2$ . Mostrar que a medida normalizada de contagem da bola fechada  $\bar{B}_r$  no cubo  $\Sigma^{n+1}$  é estritamente menor do que a medida  $\mu_{\#}$  da bola fechada de mesmo raio no cubo  $\Sigma^n$ .

[ *Sugestão:*  $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$ . ]

A medida de contagem (como qualquer outra medida) pode ser usada para definir uma integral. Vamos integrar funções sobre o cubo de Hamming.

**Definição 1.3.6.** Seja  $f: \Sigma^n \rightarrow \mathbb{R}$  uma função *qualquer*. A *integral* de  $f$  com relação a medida de contagem normalizada é o número

$$\int_{\Sigma^n} f(\sigma) d\mu_{\#}(\sigma) = \frac{\sum_{\sigma \in \Sigma^n} f(\sigma)}{2^n}.$$

Em outras palavras, é o *valor médio* de  $f$ .

Na tradição probabilística, a integral é chamada a *esperança* de  $f$  (ou: da uma variável aleatória cuja realização é  $f$ ), e denotada  $\mathbb{E}(f)$ , ou  $\mathbb{E}_{\mu_{\#}}(f)$ , se for necessário destacar a medida usada.

As seguintes propriedades da esperança são imediatas.

**Proposição 1.3.7.**

1.  $\mathbb{E}(f + g) = \mathbb{E}(f) + \mathbb{E}(g)$ .
2.  $\mathbb{E}(\lambda f) = \lambda \mathbb{E}(f)$ .
3. Se  $f(\sigma) \geq 0$  para todos  $\sigma$ , então  $\mathbb{E}(f) \geq 0$ .

$$4. \mathbb{E}(1) = 1.$$

**Exemplo 1.3.8.** Mostrar que a esperança do peso normalizado,  $\bar{w}$ , é igual à  $\frac{1}{2}$ .

Para mais sobre a integral e esperança, consulte o apêndice H.

**Lema 1.3.9** (Desigualdade de Markov). *Seja  $f$  uma função real sobre um conjunto finito  $X$  tal que  $f$  assume somente valores não-negativos. Então*

$$\mu_{\#}\{x \in X \mid f(x) \geq 1\} \leq \mathbb{E}(f).$$

*Demonstração.* Denotemos

$$A = \{x \in X \mid f(x) \geq 1\}.$$

Agora,

$$\begin{aligned} \mathbb{E}(f) &= \int_X f(x) d\mu_{\#}(x) \\ &= \int_A f(x) d\mu_{\#}(x) + \int_{X \setminus A} f(x) d\mu_{\#}(x) \\ &\geq \mu_{\#}(A). \end{aligned} \tag{1.6}$$

□

Além da esperança, pode-se definir o valor mediano.

**Definição 1.3.10.** Seja  $f$  uma função real sobre um conjunto finito,  $X$ . Um número  $M \in \mathbb{R}$  é chamado um *valor mediano* de  $f$  se ele satisfaz as seguintes condições:

$$\mu_{\#}\{x \in X : f(x) \geq M\} \geq \frac{1}{2} \text{ e } \mu_{\#}\{x \in X : f(x) \leq M\} \geq \frac{1}{2}.$$

**Proposição 1.3.11.** *Cada função sobre um conjunto finito tem um valor mediano com relação à medida de contagem normalizada.*

*Demonstração.* É fácil ordenar  $X$ ,

$$X = \{x_1, x_2, \dots, x_n\},$$

de tal maneira que  $f(x_i) \leq f(x_j)$  quando  $i \leq j$ . Agora  $M = f(x_{\lceil n/2 \rceil})$  é um valor mediano de  $f$ . □

Aqui,  $\lceil x \rceil$  denota o *teto* de um número real,  $x$ :

$$\lceil x \rceil = \min\{n \in \mathbb{Z} : x \leq n\}.$$

**Exemplo 1.3.12.** O valor  $\frac{1}{2}$  é um valor mediano do peso normalizado  $\bar{w}$ .

*Observação 1.3.13.* Intuitivamente, o valor mediano tem a propriedade de que os eventos  $f(x) \leq M$  e  $f(x) \geq M$  ocorrem com a probabilidade  $1/2$  cada um. Portanto, os exemplos fáceis mostram que a igualdade não é sempre possível.

*Observação 1.3.14.* O valor mediano não é, em geral, único. Mais propriamente, os valores medianos de uma função enchem um intervalo fechado. Por exemplo, cada número real estritamente entre 0 e 1 é um valor mediano da função  $\pi_1$  a qual envia uma palavra para seu primeiro bit.

*Observação 1.3.15.* Geralmente, a esperança de uma função não tem de ser um valor mediano. Seja  $x_0 \in X$ , e seja  $f$  a função delta localizada em  $x_0$ :

$$f(x) = \begin{cases} 0, & \text{if } x \neq x_0, \\ 1, & \text{if } x = x_0. \end{cases}$$

Então,  $\mathbb{E}(f) = \frac{1}{n}$ , mais neste caso o único valor mediano é  $M = 0$ .

Como uma das aplicações da pequena teoria a ser desenvolvida, vamos mostrar que se  $f$  é uma função real Lipschitz contínua com  $L = 1$  sobre o cubo de Hamming  $\Sigma^n$ , então a esperança e qualquer valor mediano de  $f$  são muito próximos,  $|\mathbb{E}f - M_f| \leq 1/n$ .

### 1.3.2 Partições e esperança condicional

**Definição 1.3.16.** Seja  $X$  um conjunto. Uma *cobertura* de  $X$  é uma família  $\gamma$  de subconjuntos não vazios de  $X$  cuja união é  $X$ :

$$\cup \gamma = X.$$

Em outras palavras, todo elemento de  $X$  é contido em pelo menos um elemento de  $\gamma$ :

$$\forall x \in X, \exists A \in \gamma, \text{ tal que } x \in A.$$

**Definição 1.3.17.** Uma *partição*,  $\Omega$ , de um conjunto  $X$  é uma cobertura de  $X$ ,

$$\cup \Omega = X,$$

cujos elementos são dois a dois disjuntos:

$$A \cap B = \emptyset \text{ se } A, B \in \Omega, A \neq B.$$



Nesse caso, todo elemento de  $X$  é contido em exatamente um elemento de  $\Omega$ :

$$\forall x \in X, \exists! A \in \Omega, \text{ tal que } x \in A.$$

**Exemplo 1.3.18.** A partição do intervalo unitário  $[0, 1)$  em subintervalos,

$$\Omega = \left\{ \left[ \frac{i}{n}, \frac{i+1}{n} \right) \mid i = 0, 1, \dots, n-1 \right\},$$

é importante na teoria de integração de Riemann.

**Exemplo 1.3.19.** A partição trivial de  $X$ :

$$\Omega = \{X\}.$$

**Exemplo 1.3.20.** A partição mais fina de  $X$ :

$$\Omega_f(X) = \{\{x\} \mid x \in X\}$$

As partições que nos interessam são as do cubo de Hamming.

**Definição 1.3.21.** Sejam  $n \in \mathbb{N}_+$  e  $k \leq n$  números naturais. A aplicação

$$\pi_k^n: \Sigma^n \rightarrow \Sigma^k$$

é definida por

$$\pi_k^n(\sigma_1\sigma_2 \dots \sigma_k\sigma_{k+1} \dots \sigma_n) = \sigma_1\sigma_2 \dots \sigma_k.$$

Dada uma palavra  $\sigma$  de comprimento  $n$ , a aplicação  $\pi_k^n$  acima trunca esta palavra, deixando somente o prefixo dos  $k$  primeiros bits.

**Exemplo 1.3.22.**  $\pi_3^6(001011) = 001$ .

**Definição 1.3.23.** Uma partição padrão  $\Omega_k$  (ou, mais exatamente,  $\Omega_k(\Sigma^n)$ ) do cubo de Hamming  $\Sigma^n$  consiste de subconjuntos

$$A_\tau = \{\sigma \in \Sigma^n \mid \pi_k^n(\sigma) = \tau\},$$

onde  $\tau \in \Sigma^k$ .

Os membros da partição  $\Omega_k$  são definidos pelos primeiros  $k$  bits.

**Exemplo 1.3.24.**  $\Omega_1(\Sigma^n) = \{\{\sigma \mid \sigma_1 = 0\}, \{\sigma \mid \sigma_1 = 1\}\}$ .

**Exemplo 1.3.25.**  $\Omega_0(\Sigma^n)$  é a partição trivial.

**Exemplo 1.3.26.**  $\Omega_n(\Sigma^n)$  é a partição mais fina de  $\Sigma^n$ .

**Definição 1.3.27.** Sejam  $\Omega$  e  $\Psi$  duas partições de um conjunto  $X$ . Dizemos que  $\Omega$  *refina*  $\Psi$  (ou que  $\Omega$  é *mais fina* do que  $\Psi$ , ou ainda que  $\Psi$  é *mais grossa* do que  $\Omega$ ), se todo elemento  $A \in \Omega$  está contido num elemento  $B \in \Psi$ :

$$A \subseteq B.$$

Notação:

$$\Omega < \Psi.$$

Informalmente, é o caso onde todos elementos da partição  $\Omega$  são obtidos quebrando os elementos de  $\Psi$  em pedaços menores.

**Exemplo 1.3.28.** Toda partição refina-se a si mesma:  $\Omega < \Omega$ .

**Exemplo 1.3.29.** Qualquer partição é mais fina que a partição trivial  $\{X\}$ :

$$\Omega < \{X\}.$$

**Exemplo 1.3.30.** A partição mais fina,  $\Omega_f(X)$ , justifica plenamente o seu nome refinando cada outra partição  $\Omega$  de  $X$ :

$$\Omega_f(X) < \Omega.$$

**Definição 1.3.31.** Seja  $\Omega$  uma partição de um conjunto finito  $X$  qualquer, e seja  $f : X \rightarrow \mathbb{R}$  uma função. A *esperança condicional* de  $f$  dada  $\Omega$  é uma função de  $X$  para  $\mathbb{R}$ , denotada  $\mathbb{E}(f \mid \Omega)$ , definida da seguinte maneira. Para cada  $A \in \Omega$ , a função  $\mathbb{E}(f \mid \Omega)$  assume um valor constante sobre  $A$ , igual ao valor médio de  $f$  sobre  $A$ :

$$\mathbb{E}(f \mid \Omega)(a) = \frac{\sum_{x \in A} f(x)}{\#(A)},$$

qualquer que seja  $a \in A$ .

**Exemplo 1.3.32.** A esperança condicional de  $f$  dada a partição trivial de  $X$  é uma função constante assumindo o valor  $\mathbb{E}(f)$ . Podemos escrever:

$$\mathbb{E}(f \mid \{X\}) = \mathbb{E}(f).$$

**Exemplo 1.3.33.** A esperança condicional de uma função  $f$  dada a partição mais fina é a própria função  $f$ :

$$\mathbb{E}(f \mid \Omega_f(X)) = f.$$

As seguintes propriedades da esperança condicional são de simples verificação.

**Proposição 1.3.34.** Sejam  $f$  e  $g$  duas funções reais sobre um conjunto finito  $X$  qualquer, e seja  $\Omega$  uma partição de  $X$ .

1. Se  $f \leq g$ , então  $\mathbb{E}(f \mid \Omega) \leq \mathbb{E}(g \mid \Omega)$ .

2. Se  $g = \mathbb{E}(g \mid \Omega)$  (ou seja, se  $g$  é constante sobre os elementos de  $\Omega$ ), então  $\mathbb{E}(gf \mid \Omega) = g\mathbb{E}(f \mid \Omega)$ .
3. Em particular,  $\mathbb{E}(\lambda f \mid \Omega) = \lambda\mathbb{E}(f \mid \Omega)$ .
4.  $\mathbb{E}(f + g \mid \Omega) = \mathbb{E}(f \mid \Omega) + \mathbb{E}(g \mid \Omega)$ .

□

**Lema 1.3.35.**  $\|\mathbb{E}(f \mid \Omega)\|_\infty \leq \|f\|_\infty$ .

□

**Proposição 1.3.36.** Sejam  $\Psi < \Omega$  duas partições de um conjunto finito  $X$  e seja  $f : X \rightarrow \mathbb{R}$ . Então,

$$\mathbb{E}(f \mid \Omega) = \mathbb{E}(\mathbb{E}(f \mid \Psi) \mid \Omega).$$

Em particular,

$$\mathbb{E}(f) = \mathbb{E}(\mathbb{E}(f \mid \Psi)).$$

*Demonstração.* Dado  $x \in X$ , precisamos mostrar que

$$\mathbb{E}(f \mid \Omega)(x) = \mathbb{E}(\mathbb{E}(f \mid \Psi) \mid \Omega)(x)$$

Seja  $A \in \Psi$  um elemento contendo  $x$ . Denotemos

$$\mathcal{E} = \{B \in \Omega : B \subseteq A\}.$$

Este  $\mathcal{E}$  é uma partição de  $A$ . Temos:

$$\begin{aligned} \mathbb{E}(\mathbb{E}(f \mid \Psi) \mid \Omega)(x) &= |A|^{-1} \sum_{a \in A} \mathbb{E}(f \mid \Psi)(a) \\ &= |A|^{-1} \sum_{B \in \mathcal{E}} \sum_{b \in B} \mathbb{E}(f \mid \Psi)(b) \\ &= |A|^{-1} \sum_{B \in \mathcal{E}} |B| \mathbb{E}(f \mid \Psi)(b) \\ &= |A|^{-1} \sum_{B \in \mathcal{E}} |B| \left( |B|^{-1} \sum_{b \in B} f(b) \right) \\ &= |A|^{-1} \sum_{B \in \mathcal{E}} \sum_{b \in B} f(b) \\ &= |A|^{-1} \sum_{a \in A} f(a) \\ &= \mathbb{E}(f \mid \Omega)(x). \end{aligned}$$

□

### 1.3.3 Martingales

**Definição 1.3.37.** Uma *sequência refinadora de partições* de um conjunto finito  $X$  é uma sequência  $(\Omega_k)_{k=0}^n$  onde  $\Omega_0$  é uma partição trivial,  $\Omega_n$  é a partição mais fina, e cada partição está refinando a partição precedente:

$$\Omega_n < \cdots < \Omega_{k+1} < \Omega_k < \Omega_{k-1} < \cdots < \Omega_0.$$

**Exemplo 1.3.38.** No cubo de Hamming, temos a sequência refinadora canônica de partições:

$$\{\Sigma^n\} = \Omega_0(\Sigma^n) > \Omega_1(\Sigma^n) > \cdots > \Omega_k(\Sigma^n) > \cdots > \Omega^n(\Sigma^n) = \Omega_f(\Sigma^n).$$

**Definição 1.3.39.** Um *martingale* (formado em relação a uma sequência refinadora de partições de um conjunto finito  $X$ ) é uma coleção de funções reais  $(f_0, f_1, \dots, f_n)$  sobre  $X$  tais que para todo  $i = 1, 2, \dots, n$ ,

$$E(f_i \mid \Omega_{i-1}) = f_{i-1}.$$

*Observação 1.3.40.* A palavra *martingale* (masculino; versão mais rara: *martingala*, feminino) chegou no português do francês (*martingale*, feminino), e no francês, em sua vez, do provençal (*martegalo*, masculino), daquela palavra a significação original foi a de uma estratégia de jogo fora de usual, pouco razoável. Veja [Mansuy 2009].

**Lema 1.3.41.** *Seja  $(f_0, f_1, \dots, f_n)$  um martingale sobre  $X$  formado em relação a uma sequência  $(\Omega_k)_{i=1}^n$  refinadora de partições. Para quaisquer que sejam  $i \leq j$ , temos*

$$\mathbb{E}(f_j \mid \Omega_i) = f_i.$$

*Demonstração.* Segue-se pela indução matemática da Proposição 1.3.36. □

O resultado seguinte é imediato, segue por indução.

**Teorema 1.3.42.** *Se  $f$  é uma função sobre  $X$ , então a regra*

$$f_i = \mathbb{E}(f \mid \Omega_i), \quad i = 0, 1, \dots, n$$

*define um martingale sobre  $X$ . De fato, todo martingale é obtido dessa maneira da função  $f = f_n$ .* □

**Exemplo 1.3.43.** Se  $\Omega_i$  são as partições padrão do cubo de Hamming  $\Sigma^n$  (definição 1.3.23), então um cálculo fácil mostra que para cada  $k = 0, 1, \dots, n$

$$E(w \mid \Omega_k)(\sigma) = w_k(\pi_k^n(\sigma)) + \frac{n-k}{2}.$$

Aqui  $w_k$  é o peso de Hamming sobre o cubo  $\Sigma^k$ .

**Definição 1.3.44.** Seja  $(f_0, f_1, \dots, f_n)$  um martingale sobre um conjunto finito  $X$ , formado em relação a uma sequência de partições refinadoras. As *diferenças de martingale* são as funções

$$d_i = f_i - f_{i-1}.$$

*Observação 1.3.45.* Temos a soma telescópica:

$$f = \mathbb{E}(f) + d_1 + d_2 + \dots + d_{n-1} + d_n.$$

**Proposição 1.3.46.**

$$\mathbb{E}(d_i \mid \Omega_{i-1}) = 0.$$

*Demonstração.*  $\mathbb{E}(d_i \mid \Omega_{i-1}) = \mathbb{E}(f_i \mid \Omega_{i-1}) - \mathbb{E}(f_{i-1} \mid \Omega_{i-1}) = f_{i-1} - f_{i-1}$ .  $\square$

**Lema 1.3.47.** Seja  $f: \Sigma^n \rightarrow \mathbb{R}$  uma função Lipschitz contínua de constante  $L = 1$  em relação à distância de Hamming. Seja  $(f_0, f_1, \dots, f_n)$  o martingale correspondente formado em relação à sequência canônica de partições  $\Omega_0, \Omega_1, \dots, \Omega_n$  de  $\Sigma^n$ . Então, para todo  $i = 1, 2, \dots, n$ , as diferenças de martingale,  $d_i = f_i - f_{i-1}$ , satisfazem

$$\|d_i\|_\infty \leq \frac{1}{2}.$$

*Demonstração.* Seja  $0 \leq i \leq n$ . O valor  $f_i(\sigma)$  é o valor médio de  $f$  sobre o conjunto de todas as palavras tendo o prefixo  $\sigma_1\sigma_2 \cdots \sigma_i$ :

$$f_i(\sigma) = 2^{-n+i} \sum_{\delta \in \Sigma^{n-i}} f(\sigma_1\sigma_2 \cdots \sigma_i\delta).$$

Temos então, de mesma forma,

$$\begin{aligned} f_{i-1}(\sigma) &= 2^{-n+i-1} \sum_{\delta \in \Sigma^{n-i+1}} f(\sigma_1\sigma_2 \cdots \sigma_{i-1}\delta) \\ &= 2^{-n+i} \sum_{\delta \in \Sigma^{n-i}} \frac{1}{2} [f(\sigma_1\sigma_2 \cdots \sigma_{i-1}0\delta) + f(\sigma_1\sigma_2 \cdots \sigma_{i-1}1\delta)]. \end{aligned}$$

Por conseguinte,

$$\begin{aligned} |d_i(\sigma)| &= |f_i(\sigma) - f_{i-1}(\sigma)| \\ &= 2^{-n+i} \sum_{\delta \in \Sigma^{n-i}} \left| f(\sigma_1\sigma_2 \cdots \sigma_{i-1}\sigma_i\delta) - \frac{1}{2} [f(\sigma_1\sigma_2 \cdots \sigma_{i-1}0\delta) + f(\sigma_1\sigma_2 \cdots \sigma_{i-1}1\delta)] \right| \\ &= 2^{-n+i} \sum_{\delta \in \Sigma^{n-i}} \left| \frac{1}{2} [f(\sigma_1\sigma_2 \cdots \sigma_{i-1}\sigma_i\delta) - f(\sigma_1\sigma_2 \cdots \sigma_{i-1}\bar{\sigma}_i\delta)] \right| \\ &\leq 2^{-n+i} \times 2^{n-i} \times \frac{1}{2} = \frac{1}{2}. \end{aligned}$$

□

## 1.4 Concentração de medida

### 1.4.1 Desigualdade de Azuma

**Exercício 1.4.1.** O *coseno hiperbólico*,  $\cosh x$ , é definido por

$$\cosh x = \frac{e^x + e^{-x}}{2}.$$

Mostrar que para todo  $x \in \mathbb{R}$ ,

$$\cosh x \leq e^{x^2/2}.$$

*Observação 1.4.2.* Uma função  $f: \mathbb{R} \rightarrow \mathbb{R}$  é dita *convexa* se para todos  $x, y \in \mathbb{R}$  e  $t \in [0, 1]$ ,

$$f(tx + (1-t)y) \leq tf(x) + (1-t)f(y).$$

Em particular, se  $f$  é  $C^2$  e  $f''(x) \geq 0$  para todo  $x$ , então  $f$  é convexa. Por exemplo,  $f(x) = e^x$  é uma função convexa.

O resultado seguinte está entre os principais resultados técnicos do primeiro capítulo. Ele avalia a probabilidade de que o valor de uma função,  $f$ , desvie da sua esperança,  $\mathbb{E}f$ , por mais de um valor dado,  $c > 0$ .

**Teorema 1.4.3** (Desigualdade de Azuma). *Seja  $f: X \rightarrow \mathbb{R}$  uma função sobre um conjunto finito,  $X$ , seja  $(\Omega_0, \Omega_1, \dots, \Omega_{n-1}, \Omega_n)$  uma sequência de partições refinadoras de  $X$ , e seja  $(f_0, f_1, \dots, f_n)$  o martingale correspondente com as diferenças  $(d_1, d_2, \dots, d_n)$ . Então para todo  $c > 0$*

$$\mu_{\#}(\{x \in X \mid f(x) - \mathbb{E}(f) \geq c\}) \leq \exp\left(-\frac{c^2}{2 \sum_{i=1}^n \|d_i\|_{\infty}^2}\right),$$

em particular,

$$\mu_{\#}(\{x \in X \mid |f(x) - \mathbb{E}(f)| \geq c\}) \leq 2 \exp\left(-\frac{c^2}{2 \sum_{i=1}^n \|d_i\|_{\infty}^2}\right).$$

*Demonstração.* Denotemos

$$c_i = \|d_i\|_{\infty} \equiv \max_{x \in X} |d_i(x)|.$$

Fixe o valor  $i = 1, 2, \dots, n$ , e denote

$$t = \frac{1 - \frac{d_i}{c_i}}{2}.$$

Esse  $t$  é uma função sobre  $\Sigma^n$ , tomando seus valores no intervalo  $[0, 1]$ . Temos

$$1 - t = \frac{1 + \frac{d_i}{c_i}}{2},$$

e as diferenças de martingale,  $d_i$ , tornam-se umas combinações convexas de  $\pm c_i$  com coeficientes variáveis:

$$d_i = t(-c_i) + (1 - t)c_i. \quad (1.7)$$

Seja  $\lambda \in \mathbb{R}$  qualquer (o valor exato será escolhido no final da prova). Multiplique a Eq. (1.7) por  $\lambda$ :

$$\lambda d_i = t(-\lambda c_i) + (1 - t)\lambda c_i. \quad (1.8)$$

Usando a convexidade de  $e^x$ , concluímos:

$$\begin{aligned} e^{\lambda d_i} &\leq t e^{-\lambda c_i} + (1 - t)e^{\lambda c_i} \\ &= e^{-\lambda c_i} \frac{1 - \frac{d_i}{c_i}}{2} + e^{\lambda c_i} \frac{1 + \frac{d_i}{c_i}}{2} \\ &= \frac{e^{\lambda c_i} + e^{-\lambda c_i}}{2} + \frac{d_i}{2c_i} (e^{\lambda c_i} - e^{-\lambda c_i}). \end{aligned} \quad (1.9)$$

Estimamos a esperança condicional da função  $e^{\lambda d_i}$  dado  $\Omega_{i-1}$ :

$$\begin{aligned} \mathbb{E} \left( e^{\lambda d_i} \mid \Omega_{i-1} \right) &\leq \mathbb{E} \left( \frac{e^{\lambda c_i} + e^{-\lambda c_i}}{2} \mid \Omega_{i-1} \right) + \mathbb{E} \left( \frac{d_i}{2c_i} (e^{\lambda c_i} - e^{-\lambda c_i}) \mid \Omega_{i-1} \right) \\ &= \frac{e^{\lambda c_i} + e^{-\lambda c_i}}{2} + \frac{1}{2c_i} (e^{\lambda c_i} - e^{-\lambda c_i}) \mathbb{E} (d_i \mid \Omega_{i-1}) \\ (\text{proposição 1.3.46}) &= \frac{e^{\lambda c_i} + e^{-\lambda c_i}}{2} \\ (\text{ex. 1.4.1}) &\leq e^{(\lambda c_i)^2/2}. \end{aligned} \quad (1.10)$$

(Os valores  $c_i$  e funções deles são *constantes*).

Toda diferença de martingale,  $d_j$ ,  $j < i$  é constante sobre os elementos da partição  $\Omega_{i-1}$ . Segue-se que:

$$\begin{aligned} \mathbb{E} \left( e^{\lambda \sum_{j=1}^i d_j} \right) &= \mathbb{E} \left( \mathbb{E} \left( e^{\lambda \sum_{j=1}^i d_j} \mid \Omega_{i-1} \right) \right) \\ (\text{pela proposição 1.3.34(2)}) &= \mathbb{E} \left( \left( e^{\lambda \sum_{j=1}^{i-1} d_j} \right) \mathbb{E} \left( e^{\lambda d_i} \mid \Omega_{i-1} \right) \right) \\ (\text{pela desigualdade (1.10)}) &\leq \mathbb{E} \left( e^{\lambda \sum_{j=1}^{i-1} d_j} \right) e^{\lambda^2 c_i^2/2}. \end{aligned} \quad (1.11)$$

Agora suponha que  $\lambda > 0$ . Levando em conta a observação 1.3.45, concluímos que

$$\begin{aligned}
\mu_{\#}\{\sigma \mid f(\sigma) - \mathbb{E}(f) \geq c\} &= \mu_{\#}\left\{\sigma \mid \sum_{i=1}^n d_i(\sigma) \geq c\right\} \\
&= \mu_{\#}\left\{\sigma \mid \lambda \sum_{i=1}^n d_i(\sigma) - \lambda c \geq 0\right\} \\
&= \mu_{\#}\left\{\sigma \mid e^{\lambda \sum_{i=1}^n d_i(\sigma) - \lambda c} \geq 1\right\} \\
(\text{pela desigualdade de Markov}) &\leq \mathbb{E}\left(e^{\lambda \sum_{i=1}^n d_i - \lambda c}\right) \\
&= \mathbb{E}\left(e^{\lambda d_1} e^{\lambda d_2} \dots e^{\lambda d_{n-1}} e^{\lambda d_n}\right) e^{-\lambda c} \\
(\text{pela desigualdade (1.11)}) &\leq \mathbb{E}\left(e^{\lambda d_1} e^{\lambda d_2} \dots e^{\lambda d_{n-1}}\right) e^{\lambda^2 c_n^2/2} e^{-\lambda c} \\
(\text{usando (1.11)} \text{ recursivamente, } n \text{ vezes}) &\leq \dots \\
&\leq e^{\lambda^2 c_1^2/2} e^{\lambda^2 c_2^2/2} \dots e^{\lambda^2 c_n/2^2} e^{-\lambda c} \\
&= e^{\lambda^2 \sum_{j=1}^n c_j^2/2 - \lambda c}. \tag{1.12}
\end{aligned}$$

Substituímos em (1.12) o valor

$$\lambda = \frac{c}{\sum_{j=1}^n c_j^2}$$

para concluir

$$\mu_{\#}\{\sigma : f(\sigma) - \mathbb{E}(f) \geq c\} \leq e^{-\frac{c^2}{2 \sum_{j=1}^n c_j^2} \|d_j\|_{\infty}^2}. \tag{1.13}$$

A desigualdade gêmea é obtida usando  $-f$  em lugar de  $f$ :

$$\mu_{\#}\{\sigma : \mathbb{E}(f) - f(\sigma) \geq c\} \leq e^{-\frac{c^2}{2 \sum_{j=1}^n c_j^2} \|d_j\|_{\infty}^2}. \tag{1.14}$$

Em conjunto, as duas desigualdades (1.13) e (1.14) implicam

$$\mu_{\#}\{\sigma : |\mathbb{E}(f) - f(\sigma)| \geq c\} \leq 2e^{-\frac{c^2}{2 \sum_{j=1}^n c_j^2} \|d_j\|_{\infty}^2}, \tag{1.15}$$

como desejado. (Aqui usamos a *desigualdade de Boole*, conhecido como o *union bound* em inglês:  $\mu(A \cup B) \leq \mu(A) + \mu(B)$ .)  $\square$

## 1.4.2 Cotas de Chernoff

**Teorema 1.4.4.** *Seja  $f : \Sigma^n \rightarrow \mathbb{R}$  uma função Lipschitz contínua, de constante  $L = 1$  (em relação à distância de Hamming sobre  $\Sigma^n$ ). Então, para todo  $c > 0$  temos*

$$\mu_{\#}\{x : |f(x) - \mathbb{E}(f)| \geq c\} \leq 2e^{-\frac{2c^2}{n}}.$$



*Demonstração.* Lema 1.3.47 junto com a desigualdade de Azuma.  $\square$

### 1.4.3 Lei geométrica dos grandes números

Eis uma versão para a distância de Hamming normalizada.

**Corolário 1.4.5.** *Seja  $f: \Sigma^n \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua em relação à distância de Hamming normalizada. Então para todo  $\epsilon > 0$*

$$\mu_{\#}\{x: |f(x) - \mathbb{E}(f)| \geq \epsilon\} \leq 2e^{-2\epsilon^2 n}.$$

*Demonstração.* A função  $nf$  é 1-Lipschitz contínua em relação com a distância de Hamming não normalizada:

$$\begin{aligned} |nf(\sigma) - nf(\tau)| &= n|f(\sigma) - f(\tau)| \\ &\leq n\bar{d}(\sigma, \tau) \\ &= d(\sigma, \tau). \end{aligned}$$

O teorema 1.4.4 aplicada à função  $nf$  com  $c = n\epsilon$  implica:

$$\mu_{\#}\{x: |nf(x) - \mathbb{E}(nf)| \geq n\epsilon\} \leq 2e^{-\frac{\epsilon^2 n^2}{n}},$$

é como  $\mathbb{E}(nf) = n\mathbb{E}(f)$ , terminámos.  $\square$

Aplicadas ao peso normalizado  $\bar{w}$ , as cotas de Chernoff (corolário 1.4.5) levam a concluir:

$$\forall \epsilon > 0, \quad \mu_{\#}\left\{x \in \Sigma^n: \left|\bar{w} - \frac{1}{2}\right| > \epsilon\right\} \leq 2e^{-2\epsilon^2 n}.$$

Esta desigualdade, conhecida na teoria de probabilidade como a (*fraca*) *Lei dos Grandes Números*, diz que a probabilidade que o número médio de sucessos (caras) obtidos após  $n$  lançamentos de uma moeda equilibrada diferir de  $1/2$  se torna exponencialmente pequena quando  $n \rightarrow \infty$ .

É por isso que a desigualdade mais geral no corolário 1.4.5, válida para todas funções Lipschitz contínuas de constante  $L = 1$ , é as vezes chamada a *lei geométrica dos grandes números*.

### 1.4.4 Volumes das bolas: a segunda estimativa

Como  $\bar{w}(x+1) + \bar{w}(x) = 1$ , temos  $\bar{d}(x, 1) = \bar{d}(x+1, 0) = 1 - \bar{w}(x)$ , e por conseguinte

$$\bar{B}_\epsilon(1) = \{x \in \Sigma^n : \bar{w}(x) - \frac{1}{2} \geq \frac{1}{2} - \epsilon\}.$$

Desta maneira, obtemos a segunda estimativa da medida da bola:

$$\mu_{\#}(\bar{B}_\epsilon) \leq e^{-2(\frac{1}{2}-\epsilon)^2 n}. \quad (1.16)$$

Esta estimativa é melhor do que a dada pelo lema 1.2.6 na região onde  $\epsilon > 0$  é constante, isso é, o raio não normalizado da bola é proporcional à  $n$ :

$$d \sim \epsilon n.$$

A primeira estimativa, a do lema 1.2.6,

$$\mu_{\#}(\bar{B}_\epsilon) \leq 2^{-n} \left( \frac{en}{\lfloor \epsilon n \rfloor} \right)^{\lfloor \epsilon n \rfloor}, \quad (1.17)$$

é melhor na região onde  $d = \lfloor \epsilon n \rfloor$  é constante, ou seja,  $\epsilon = O(n^{-1})$ . Vamos utilizar ambas simultaneamente na análise de aprendizabilidade.

### 1.4.5 Função de concentração

As desigualdades acima – as de Azuma e de Chernoff – são manifestações do *fenômeno de concentração de medida sobre as estruturas de alta dimensão*, que pode ser expresso informalmente da seguinte maneira:

*Tipicamente, sobre uma estrutura  $\Omega$  de alta dimensão, cada função Lipschitz contínua concentra-se em torno de um valor, ou seja, é quase constante em toda parte exceto sobre um conjunto da medida demasiadamente pequena.*

Como o valor típico da função, pode ser escolhido ou a esperança  $\mathbb{E}f$ , ou um valor mediano,  $M_f$ . Neste contexto, o fenômeno pode ser reformulado mais uma vez:

*Tipicamente, numa estrutura  $\Omega$  de alta dimensão, para cada subconjunto  $A \subseteq \Omega$  que contém pelo menos a metade dos pontos, a maior parte dos pontos de  $\Omega$  estão próximos ao  $A$ .*

As noções “dimensão alta” e “pontos próximos” sendo relativas, e a noção será formalizada no contexto assintótico. Um instrumento conveniente para quantificar o fenômeno da concentração de medida é a *função de concentração*. Recordemos que

$$A_\epsilon = \{x \in \Omega : \exists a \in A \rho(x, a) < \epsilon\}$$

é a  $\epsilon$ -vizinhança do sub-conjunto  $A$  de  $\Omega$ .

**Definição 1.4.6.** Seja  $(\Omega, d, \mu)$  um espaço métrico munido de uma medida de probabilidade. A *função de concentração* de  $\Omega$ , denotada por  $\alpha_\Omega(\epsilon)$  ou  $\alpha(\Omega, \epsilon)$  ou simplesmente  $\alpha(\epsilon)$ , é definida pelas condições seguintes:

$$\alpha(\epsilon) = \begin{cases} \frac{1}{2}, & \text{se } \epsilon = 0, \\ 1 - \inf \{ \mu_\#(A_\epsilon) : A \subseteq \Sigma^n, \mu_\#(A) \geq \frac{1}{2} \}, & \text{se } \epsilon > 0. \end{cases}$$

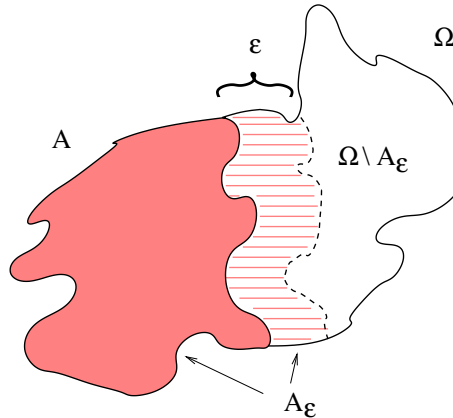


Figura 1.1: A função de concentração  $\alpha(\Omega, \epsilon)$ .

**Exercício 1.4.7.** Mostrar que

$$\alpha(\Omega, \epsilon) \rightarrow 0 \text{ quando } \epsilon \rightarrow \infty.$$

**Definição 1.4.8.** Uma família  $(\Omega_n, \rho_n, \mu_n)$  de espaços métricos com medida de probabilidade é dita uma *família de Lévy* se as funções de concentração tendem a zero pontualmente,

$$\alpha(\Omega_n, \epsilon) \rightarrow 0 \text{ para cada } \epsilon > 0.$$

Ela é uma *família de Lévy normal* se existem  $C_1, C_2 > 0$  tais que

$$\alpha(\Omega_n, \epsilon) \leq C_1 e^{-C_2 \epsilon^2 n}.$$

**Exercício 1.4.9.** Seja  $r \geq 0$  inteiro e  $\epsilon > 0$  qualquer. Então, a  $\epsilon$ -vizinhança aberta de uma bola fechada de raio  $r$  no cubo de Hamming é uma bola aberta de mesmo centro dada por

$$(\bar{B}_r)_\epsilon(\sigma) = B_{r+\epsilon}(\sigma).$$

(Mostra que para  $r, \epsilon > 0$  reais quaisquer isso não é mais verdadeiro).

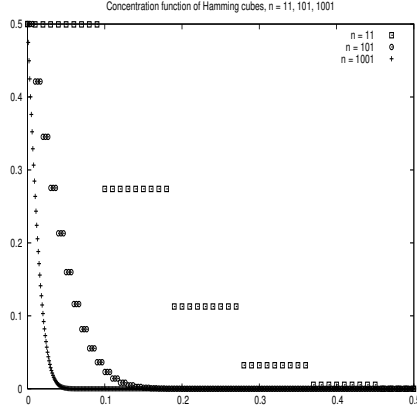


Figura 1.2: As funções de concentração dos cubos de Hamming para  $d = 11, 101, 1001$ .

**Exercício 1.4.10.** O complemento de uma bola aberta no cubo de Hamming é dado por

$$\Sigma^n \setminus B_\delta(\sigma) = \bar{B}_{1-\delta}(\sigma + \bar{1}).$$

**Exercício 1.4.11.** Seja  $n = 2m + 1$  um número ímpar. Mostrar que a bola  $\bar{B}_m(\sigma)$  ( $\bar{B}_{m/n}(\sigma)$ , com relação à distância de Hamming normalizada) tem a medida de contagem normalizada  $1/2$ .

[ *Sugestão:* estudar o seu complemento. ]

**Exercício 1.4.12.** Deduzir que no caso de  $n = 2m + 1$  ímpar, as bolas  $\bar{B}_m(\sigma)$  são as únicas bolas de Hamming com  $2^{n-1}$  elementos.

**Teorema 1.4.13.** *Os cubos de Hamming  $\Sigma^n$  munidos da distância de Hamming e a medida de contagem normalizadas formam uma família de Lévy normal:*

$$\alpha(\Sigma^n, \epsilon) \leq e^{-\epsilon^2 n}.$$

*Demonstração.* Seja  $A$  um subconjunto do cubo que contem pelo menos a metade dos elementos:  $\mu_{\#}(A) \geq 1/2$ , e seja  $\epsilon > 0$  qualquer. Precisamos estimar por cima  $\mu_{\#}(\Sigma^n \setminus A_\epsilon)$ . É claro que pode-se supor sem perda de generalidade que  $\mu_{\#}(A) = 1/2$  (selecionando um subconjunto de  $A$  com exatamente  $2^{n-1}$  elementos: o valor de  $\mu_{\#}(\Sigma^n \setminus A_\epsilon)$  só vai aumentar). Seja  $r \geq 0$  o maior valor inteiro tal que  $r/n < \epsilon$ . Temos  $\bar{B}_r(\sigma) = B_\epsilon(\sigma)$ , qual quer seja  $\sigma$ .

Começamos com  $n$  ímpar,  $n = 2m + 1$ . Segundo o teorema de Harper, assim como os exercícios acima, a bola  $\bar{B}_r(\bar{0})$  tem a propriedade  $\mu_{\#}(\Gamma_R \bar{B}_m(\bar{0})) \leq \mu_{\#}(A_\epsilon)$ , isto é,  $\mu_{\#}(B_{m/n+\epsilon}) \leq \mu_{\#}(A_\epsilon)$ , é por conseguinte,  $\mu_{\#}(\bar{B}_{1-m/n-\epsilon}) \geq \mu_{\#}(\Sigma^n \setminus A_\epsilon)$ . Temos

$$1 - \frac{m}{n} - \epsilon = \frac{1}{2} + \frac{1}{2n} - \epsilon,$$

e segundo a estimativa de tamanho das bolas,

$$\mu_{\#}(\bar{B}_{1-m/n-\epsilon}) \leq e^{-(\epsilon - \frac{1}{2n})^2 n}.$$

Como

$$-2 \left( \epsilon - \frac{1}{2n} \right)^2 n = -2\epsilon^2 n + 2\epsilon - \frac{1}{2n} \leq -\frac{3}{2}\epsilon^2 n$$

(pois  $\frac{1}{2}\epsilon^2 n^2 - 2\epsilon n + 2 \geq 0$ ), deduzimos do corolário 1.4.5:

$$\alpha(\Sigma^n, \epsilon) \leq e^{-\frac{3}{2}\epsilon^2 n}. \quad (1.18)$$

Para  $n$  par,  $n = 2m$ , o argumento é semelhante, mas nesse caso o cubo de Hamming consiste da bola fechada de raio  $m - 1$  ( $(m - 1)/n$ , caso normalizado), mais uma metade de elementos da esfera de raio  $m$ . Em particular, o complemento de conjunto  $A_\epsilon$  tem uma medida menor ou igual da medida da bola de raio  $\frac{1}{2} + \frac{1}{n} - \epsilon$ , cuja medida de contagem normalizada tem estimativa acima

$$e^{-(\epsilon - \frac{1}{n})^2 n}.$$

Como

$$-2 \left( \epsilon - \frac{1}{n} \right)^2 n = -2\epsilon^2 n + 4\epsilon - \frac{2}{n} \leq -\epsilon^2 n$$

(pois  $\epsilon^2 n^2 - 4\epsilon n + 2 \geq 0$  para qualquer que seja  $n$ ), concluímos:

$$\alpha(\Sigma^n, \epsilon) < e^{-\epsilon^2 n}.$$

□

*Observação 1.4.14.* Sem dúvida, as constantes podem ser melhoradas. Em particular, eu não sei a resposta para o seguinte. Dado  $\epsilon > 0$  e  $n$  quaisquer, é verdadeiro que

$$\alpha_{\Sigma^{n+1}}(\epsilon) \leq \alpha_{\Sigma^n}(\epsilon)?$$

Em outras palavras, é verdade que as funções de concentração de cubos de Hamming convergem para zero monotonicamente quando  $n \rightarrow \infty$ ? Aqui, só a transição de um  $n$  ímpar para  $n + 1$  deve ser estudada.

**Exercício 1.4.15.** Seja  $f$  uma função Lipschitz contínua com a constante de Lipschitz  $L \geq 0$  sobre um espaço métrico com medida de probabilidade,  $(\Omega, \rho, \mu)$ . Seja  $M = M_f$  um valor mediano de  $f$ . Provar que

$$\mu\{|f(x) - M| > \epsilon\} \leq 2\alpha\left(\Omega, \frac{\epsilon}{L}\right).$$

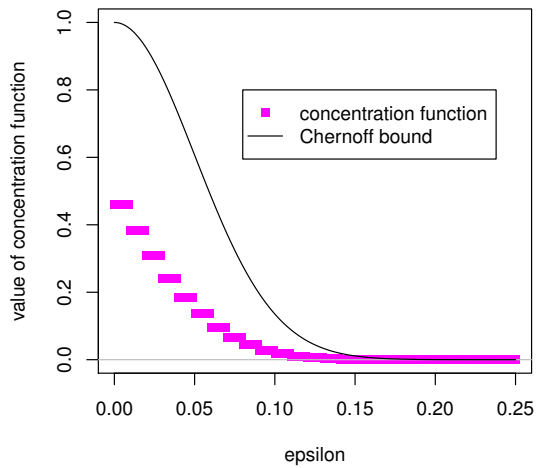


Figura 1.3: Função de concentração do cubo de Hamming  $\Sigma^{100}$  e a cota superior gaussiana de Chernoff

Mais geralmente, se  $f$  é uniformemente contínua de tal modo que

$$\forall x, y \in X, \quad d(x, y) < \delta \Rightarrow |fx - fy| < \epsilon,$$

então

$$\mu\{|f(x) - M| > \epsilon\} \leq 2\alpha(\Omega, \delta).$$

O fenômeno de concentração da medida é o assunto de estudo de uma disciplina matemática relativamente nova: a *análise geométrica assintótica*. Esta introspeção na geometria dos objetos de alta dimensão é da mais alta importância, e tem muitas aplicações e consequências amplas em ciências matemáticas. Veja a monografia [Artstein-Avidan, Giannopoulos e Milman 2015].

A apresentação neste capítulo geralmente seguiu a no livro clássico [Milman e Schechtman 1986], mas com constantes melhoradas como em [Alon e Spencer 1992]. O livro [Ledoux 2001] é uma fonte excelente para a concentração de medida. Veja também o panorâmico de [Schechtman 2003], assim como o livro de [Matoušek 2002].

# 2

## Dimensão de Vapnik–Chervonenkis

---

### 2.1 Definição e exemplos iniciais

Vamos ampliar a nossa perspectiva e estudar as rotulagens sobre os subconjuntos finitos de um domínio,  $\Omega$ , finito ou infinito. Um classificador,  $T: \Omega \rightarrow \{0, 1\}$ , induz sobre uma amostra não rotulada qualquer,  $\sigma = (x_1, \dots, x_n)$ , uma rotulagem  $(\epsilon_1, \dots, \epsilon_n)$  bastante naturalmente:

$$\epsilon_i = T(x_i), \quad i = 1, 2, \dots, n.$$

Um classificador, ou uma função binária, é exatamente a função indicadora de um subconjunto,  $C \subseteq \Omega$ :

$$T = \chi_C, \text{ onde } \chi_C(x) = \begin{cases} 1, & \text{se } x \in C, \\ 0, & \text{se } x \notin C. \end{cases}$$

Em vez de funções binárias, podemos trabalhar com subconjuntos do domínio,  $C \in 2^\Omega$ . Tais subconjuntos  $C \subseteq \Omega$  são chamados de *conceitos*. Dado um conceito  $C$ , um ponto  $x \in \Omega$  é então rotulado 1 se e somente se  $x \in C$ .

Agora suponha que trabalhamos com uma família qualquer  $\mathcal{C} \subseteq 2^\Omega$  de conceitos (uma *classe de conceitos*, *concept class*). Mediante a motivação,  $\mathcal{C}$  é uma família de todos os classificadores produzidos por uma regra de aprendizagem particular, como por exemplo uma rede neural  $\mathcal{N}$  de uma arquitetura fixa, que depende de uma família de parâmetros reais. Os diferentes valores de parâmetros resultam em conceitos diferentes. O algoritmo



de aprendizagem procura um conceito  $C$  dentro da classe  $\mathcal{C}$  que melhor se ajusta a uma dada amostra rotulada,  $\sigma$ , a fim de minimizar o erro empírico (o erro de aprendizagem). Queremos evitar o fenômeno de “overfitting” (sobreajuste), esperando que o *erro de generalização* seja baixo, ou seja, que o conceito escolhido se mostra eficaz para prever novos rótulos. Isso é possível se a complexidade da classe  $\mathcal{C}$  for bastante baixa. Falando de uma maneira informal, a complexidade de  $\mathcal{C}$  dá uma medida de quantas rotulagens diferentes  $\mathcal{C}$  pode produzir em amostras finitas. Uma medida teórica importante da complexidade de uma classe de conceitos é a famosa *dimensão de Vapnik–Chervonenkis*.<sup>1</sup>

**Definição 2.1.1.** Seja  $\mathcal{C}$  uma classe de conceitos no domínio  $\Omega$ . Para um subconjunto  $B \subseteq \Omega$ , denotemos por

$$\mathcal{C}|_B = \{\chi_C|_B : C \in \mathcal{C}\}$$

a família de todas as rotulagens sobre  $B$  induzidas pelos membros da classe  $\mathcal{C}$ . Digamos que um subconjunto finito  $B \subseteq \Omega$  é *fragmentado* (*shattered*) por  $\mathcal{C}$  se cada rotulagem possível de  $B$  é atingida:

$$\mathcal{C}|_B = 2^B = \{0, 1\}^{\#B}.$$

Em outras palavras,  $B$  é fragmentado por  $\mathcal{C}$  se cada função binária sobre  $B$  pode se estender a uma função da forma  $\chi_C$ ,  $C \in \mathcal{C}$ .

Aqui é uma outra maneira de reformular a definição.

**Definição 2.1.2.** Seja  $\mathcal{C}$  uma família de subconjuntos de  $\Omega$ . Um conjunto finito  $A \subseteq \Omega$  é *fragmentado* por  $\mathcal{C}$  se todo subconjunto  $B \subseteq A$  pode ser “retirado” de  $A$  com a ajuda de um elemento apropriado  $C$  de  $\mathcal{C}$ :

$$B = A \cap C.$$

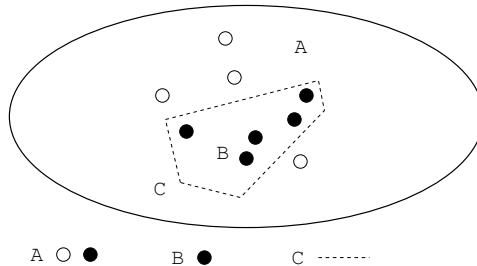


Figura 2.1: Um subconjunto  $A$  fragmentado pela classe  $\mathcal{C}$ .

<sup>1</sup>Pronunciar: Vápnik–Tchervónenkis.

**Definição 2.1.3.** A *dimensão de Vapnik–Chervonenkis* (*dimensão VC*) de uma classe de conceitos  $\mathcal{C}$  é o supremo de cardinalidades de subconjuntos finitos  $A \subseteq \Omega$  fragmentados por  $\mathcal{C}$ . Notação:  $\text{VC-dim}(\mathcal{C})$ .

Em outras palavras, a dimensão VC de  $\mathcal{C}$  é a maior cardinalidade de um conjunto fragmentado por  $\mathcal{C}$ , se existir, e  $+\infty$  se não existir.

*Observação 2.1.4.* Para estabelecer a desigualdade  $\text{VC-dim}(\mathcal{C}) \geq d$ , basta exibir um conjunto  $A \subseteq \Omega$  com  $d$  elementos, fragmentado por  $\mathcal{C}$ . Por outro lado, para estabelecer a desigualdade  $\text{VC-dim}(\mathcal{C}) \leq d$ , é preciso mostrar que nenhum subconjunto com  $d + 1$  elementos é fragmentado. Isso é normalmente a parte mais difícil.

**Exemplo 2.1.5.** Uma classe que consiste de um conceito só,  $\mathcal{C} = \{C\}$ , possui dimensão VC igual a zero. A classe  $\mathcal{C}$  não fragmenta nenhum conjunto unitário,  $\{x\}$ , pois ele sempre induz o mesmo rótulo (1, se  $x \in C$ , e 0, se  $x \notin C$ ), nunca ambos. Por isso,  $\text{VC-dim}(\{C\}) < 1$ . Por outro lado, o conjunto vazio,  $\emptyset$ , é fragmentado por  $\mathcal{C}$ : a restrição da função  $\chi_C$  sobre o conjunto vazio é a função vazia, a única rotulagem possível de  $\emptyset$ . Concluimos:  $\text{VC-dim}(\mathcal{C}) = 0$ .

**Exemplo 2.1.6.** Seja  $\Omega$  um domínio não vazio qualquer, e seja  $\mathcal{C}$  a classe que consiste de dois conjuntos:  $\emptyset$  et  $\Omega$ . Nesse caso, a dimensão VC da classe  $\mathcal{C}$  é 1. Todo conjunto unitário  $\{x\}$ ,  $x \in \Omega$ , é fragmentado:  $\emptyset = \emptyset \cap \{x\}$  e  $\{x\} = \Omega \cap \{x\}$ . Nenhum conjunto com dois pontos diferentes,  $\{x, y\}$ , é fragmentado por  $\mathcal{C}$ , pois um tal conjunto contém 4 subconjuntos diferentes,  $\emptyset$ ,  $\{x\}$ ,  $\{y\}$ , et  $\{x, y\}$ , et só  $\emptyset$  et  $\{x, y\}$  podem ser obtidos como interseções de elementos de  $\mathcal{C}$  com  $\{x, y\}$ .

*Observação 2.1.7.* Mais geralmente, a dimensão VC de uma classe  $\mathcal{C}$  com  $n$  conceitos não excede  $\log_2 n$ . Se um conjunto com  $d$  pontos for fragmentado por  $\mathcal{C}$ , a classe tem que conter pelo menos  $2^d$  elementos dois a dois distintos.

**Exemplo 2.1.8.** Seja  $\Omega = \mathbb{R}$ , e seja  $\mathcal{C}$  a classe de todos os intervalos semi-infinitos crescentes:

$$\mathcal{C} = \{[a, +\infty) : a \in \mathbb{R}\}.$$

Então,

$$\text{VC-dim}(\mathcal{C}) = 1.$$

É claro que todo conjunto unitário,  $\{x\}$ , é fragmentado por  $\mathcal{C}$ : só há dois subconjuntos, o próprio  $\{x\}$  e o conjunto vazio, e ambos são interseções de  $\{x\}$  com um intervalo apropriado. Por outro lado, nenhum conjunto com dois pontos,  $A = \{x, y\}$ ,  $x < y$ , é fragmentado por  $\mathcal{C}$ : qualquer que seja  $a \in \mathbb{R}$ , temos  $\{x, y\} \cap [a, \infty) \neq \{x\}$ .

**Exemplo 2.1.9.** Se agora tomamos todos os intervalos semi-infinitos crescentes bem como decrescentes,

$$\mathcal{C} = \{[a, +\infty) : a \in \mathbb{R}\} \cup \{(-\infty, b] : b \in \mathbb{R}\},$$

o valor da dimensão de Vapnik–Chervonenkis aumenta:

$$\text{VC-dim}(\mathcal{C}) = 2.$$

Todo subconjunto com dois pontos,  $A = \{x, y\}$  é fragmentado por  $\mathcal{C}$ :

$$\begin{aligned} \{x, y\} &= \{x, y\} \cap [x, \infty), & \{x\} &= \{x, y\} \cap (-\infty, x], \\ \{y\} &= \{x, y\} \cap [y, \infty), & \emptyset &= \{x, y\} \cap [y + 1, \infty). \end{aligned}$$

Ao mesmo tempo, nenhum subconjunto com três pontos distintos é fragmentado por  $\mathcal{C}$ . Sejam  $x < y < z$ ,  $A = \{x, y, z\}$ , então o conjunto  $B = \{y\}$  nunca pode ser obtido como a interseção de  $B$  com um intervalo semi-infinito.

**Exemplo 2.1.10.** Agora seja  $\mathcal{C}$  a classe de todos os intervalos fechados finitos,  $[a, b]$ ,  $a, b \in \mathbb{R}$ . Então, mais uma vez,

$$\text{VC-dim}(\mathcal{C}) = 2.$$

Todo conjunto com dois pontos é fragmentado, mais nenhum conjunto com três pontos,  $A = \{x, y, z\}$ , é: o conjunto  $B = \{x, z\}$  de pontos extremos não pode ser obtido como a interseção de  $B$  com um intervalo.

**Exemplo 2.1.11.** Agora seja  $\Omega = \mathbb{R}^2$ , o plano. A classe  $\mathcal{C}$  consiste de todos os semi-planos (abertos, ou fechados, ou bem abertos e fechados, o resultado é o mesmo). Recordemos pois que trata-se dos semi-planos fechados:

$$H \equiv H_{\vec{v}, b} = \{\vec{x} \in \mathbb{R}^2 : \langle \vec{x}, \vec{v} \rangle \geq b\},$$

onde  $\vec{v} \in \mathbb{R}^2$  e  $b \in \mathbb{R}$  são quaisquer:

$$\mathcal{C} = \{H_{\vec{v}, b} : \vec{v} \in \mathbb{R}^2, b \in \mathbb{R}\}.$$

Então,

$$\text{VC-dim}(\mathcal{C}) = 3.$$

Todo conjunto de três pontos não colineares,  $a, b, c$ , é fragmentado pelos semi-planos, o que é mais ou menos evidente geometricamente, veja Figura 2.2.

Ao mesmo tempo, nenhum subconjunto com quatro pontos distintos é fragmentado pelos semi-planos. Sejam  $a, b, c, d$  quaisquer, dois a dois distintos. Existem dois casos a considerar.

Se pelo menos um dos pontos  $a, b, c, d$  for contido dentro do triângulo formado pelos outros três pontos, digamos o ponto  $d$ , então cada semi-plano que contém o conjunto  $\{a, b, c\}$ , sendo um conjunto convexo, tem que conter  $d$  também, veja a Figura 2.3.

Se nenhum dos pontos pertence à envoltória convexa dos três pontos restantes, o quadrilátero  $a, b, c, d$  é convexo. Neste caso, um subconjunto contendo o par de vértices opostos não pode ser a interseção de um semi-plano com  $A = \{a, b, c, d\}$ , veja a Fig. 2.4.

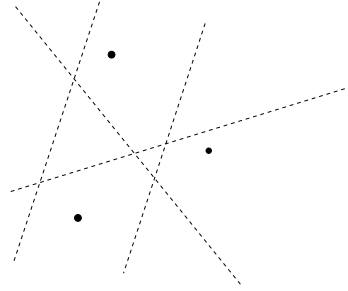


Figura 2.2: Todo conjunto de três pontos em posição geral é fragmentado pelos semi-planos.

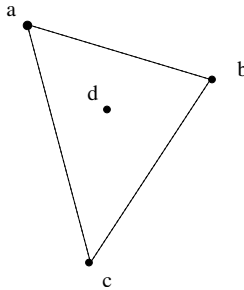


Figura 2.3: Todo semi-plano contendo  $C = \{a, b, c\}$  vai conter  $d$ .

**Exemplo 2.1.12.** Seja  $\mathcal{C}$  a família de todos os retângulos em  $\mathbb{R}^2$  cujos lados são paralelos aos eixos coordenados, ou seja,

$$\mathcal{C} = \{[a, b] \times [c, d] : a, b, c, d \in \mathbb{R}, a < b, c < d\}.$$

Então,

$$\text{VC-dim}(\mathcal{C}) = 4.$$

Para começar, o conjunto

$$A = \{(1, 0), (-1, 0), (0, 1), (0, -1)\}$$

é fragmentado pela classe  $\mathcal{C}$ , o que pode ser verificado diretamente, veja Fig. 2.5.

Ao mesmo tempo, vamos mostrar que nenhum conjunto com cinco pontos diferentes pode ser fragmentado pelos retângulos. Seja  $A$  um tal conjunto. Escolhemos o ponto “mais à esquerda”,  $a$ , ou seja, tal que a primeira coordenada  $a_1 \leq x_1$  para todos  $x =$

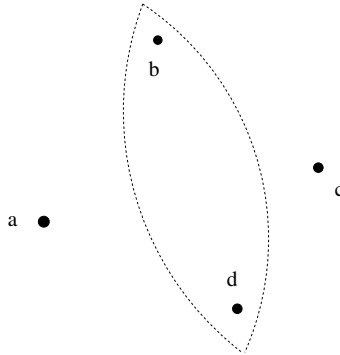


Figura 2.4: Todo semi-plano que contém  $C = \{b, d\}$  vai conter  $a$  ou  $c$ .

$(x_1, x_2) \in A$ . De mesmo modo, escolha o ponto “mais à direita”,  $b$ , o ponto “mais alto”  $d$  (cuja segunda coordenada é maior), assim como o ponto “mais baixo”,  $c$ . Veja Fig. 2.6. (Pode acontecer que não todos os pontos  $a, b, c, d$  sejam dois a dois distintos).

Defina  $B = \{a, b, c, d\}$ . Como  $|A| \geq 5$ , existe pelo menos um ponto  $e$  em  $A \setminus B$  que não foi escolhido. Agora, todo retângulo  $[x, y] \times [z, w]$  que contém  $B$  tem que satisfazer

$$x \leq a_1, \quad b_1 \leq y, \quad z \leq c_2, \quad d_2 \leq w,$$

ou seja,

$$x \leq a_1 \leq e_1 \leq b_1 \leq y,$$

assim como

$$z \leq c_2 \leq e_2 \leq d_2 \leq w.$$

Por conseguinte,  $e \in [x, y] \times [z, w]$  e  $A \cap [x, y] \times [z, w] = A$ . O subconjunto  $B \subsetneq A$  não pode ser obtido de  $A$  como a interseção com um retângulo.

**Exemplo 2.1.13.** Seja  $\mathcal{C}$  a família de todos os paralelepípedos retângulos no espaço  $\mathbb{R}^d$  com os lados paralelos aos eixos coordenados, ou seja, os subconjuntos da forma

$$\Pi = [a_1, b_1] \times [a_2, b_2] \times \dots \times [a_d, b_d].$$

Então,

$$\text{VC-dim}(\mathcal{C}) = 2d.$$

Dado um subconjunto finito  $X$  de  $\mathbb{R}^d$ , denotemos por  $\Pi(X)$  o menor paralelepípedo (fechado) contendo  $X$ , ou seja,

$$\Pi(X) = \bigcap_{i=1}^d \pi_i^{-1}(\text{conv}(\pi_i(X))).$$

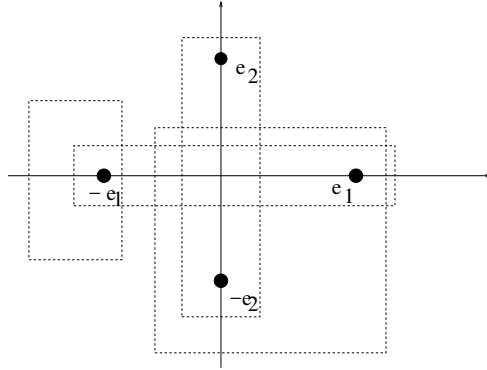


Figura 2.5: O conjunto  $A = \{\pm e_i\}_{i=1}^2$  é fragmentado pelos retângulos.

Aqui  $\pi_i$  é a  $i$ -ésima projeção coordenada de  $\mathbb{R}^d$  para  $\mathbb{R}$ , e a envoltória convexa em  $\mathbb{R}$  é simplesmente o menor intervalo que contém  $\pi_i(X)$ .

A prova da desigualdade  $\leq$  é idêntica à prova no exemplo 2.1.12. Para mostrar a desigualdade  $\geq$ , observemos que o conjunto

$$A = \{\pm e_i\}_{i=1}^d$$

com  $2d$  pontos é fragmentado pelos paralelepípedos. Seja  $B \subseteq A$ . Vamos mostrar que  $\Pi(B) \cap A = B$ , terminando a demonstração. A inclusão  $\supseteq$  é óbvia. Suponha que  $x \in A \setminus B$ . Existe  $i$  tal que  $\pi_i x$  é da forma  $\pm e_i$ . Suponhamos  $b = e_i$  (o argumento no segundo caso  $b = -e_i$  é quase idêntico). O ponto  $e_i$  é o único ponto no conjunto  $A$  cuja  $i$ -ésima coordenada é um. Isso implica

$$p_i(B) \subseteq \{-1, 0\},$$

e pela definição de  $\Pi(A)$ ,

$$b = e_i \notin \Pi(A).$$

O exemplo 2.1.11 estende-se aos espaços vetoriais de dimensão qualquer. Precisamos um resultado técnico seguinte.

**Teorema 2.1.14.** *Seja  $V$  um sub-espço vetorial do espaço  $\mathbb{R}^\Omega$  de todas as funções reais sobre o domínio  $\Omega$ . A dimensão VC da classe de conjuntos*

$$C_f = \{x \in \Omega : f(x) \geq 0\}, \quad f \in V,$$

*é menor ou igual a  $\dim V$ .*

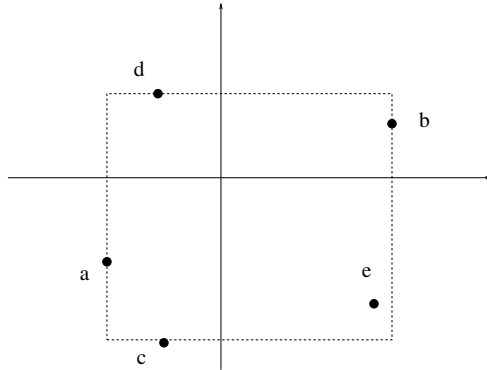


Figura 2.6: Nenhum conjunto  $A = \{a, b, c, d, e\}$  com cinco pontos é fragmentado pelos retângulos.

*Demonstração.* Seja  $\dim V = d$ . Com todo ponto  $x \in \Omega$  pode ser associado um funcional linear  $\hat{x}$  de avaliação no ponto  $x$ , da forma  $f \mapsto f(x)$ , onde  $f \in V$ . Este  $\hat{x}$  pertence ao espaço vetorial dual,  $V^*$ . Seja agora  $A \subseteq \Omega$  um conjunto com  $d + 1$  pontos distintos. Como a dimensão do espaço dual de  $V$  é  $d$ , um dos funcionais lineares de avaliação aos pontos, que denotemos por  $x_{d+1} \in A$ , pode ser expresso como a combinação linear dos pontos restantes,

$$\hat{x}_{d+1} = \sum_{i=1}^d \lambda_i \hat{x}_i, \quad x_i \in A.$$

Definamos

$$B = \{x_i : 0 \leq i \leq d, \lambda_i \geq 0\} \subseteq A.$$

Seja  $f \in V$  tal que  $C_f \cap \{x_1, x_2, \dots, x_d\} = B$ . Neste caso,  $f(x_i) \geq 0 \iff x_i \in B$ , e concluímos

$$f(x_{d+1}) = \hat{x}_{d+1}(f) = \sum_{i=1}^d \lambda_i \hat{x}_i(f) = \sum_{i=1}^d \lambda_i f(x_i) \geq 0,$$

de onde  $x_{d+1} \in C_f$ . O conjunto  $B$  não é da forma  $A \cap C_f$  para  $f \in V$  qualquer.  $\square$

**Exercício 2.1.15.** Investigar a pergunta seguinte: é sempre verdadeiro que a dimensão VC da classe de conceitos  $C_f$ ,  $f \in V$ , é igual a  $\dim V$ , ou pode ser estritamente menor?

**Exemplo 2.1.16.** Seja  $\mathcal{C}$  a coleção de todos os semi-espacos (fechados) no espaço vetorial  $\mathbb{R}^d$ :

$$\mathcal{C} = \left\{ H_{\vec{v}, b} : \vec{v} \in \mathbb{R}^d, b \in \mathbb{R} \right\},$$

onde, como no exemplo 2.1.11,

$$H_{\vec{v},b} = \{\vec{x} \in \mathbb{R}^d : \langle \vec{x}, \vec{v} \rangle \geq b\}.$$

Então,

$$\text{VC-dim}(\mathcal{C}) = d + 1.$$

A desigualdade  $\geq$  é bastante fácil a verificar: por exemplo, os  $d + 1$  pontos

$$0, e_1, e_2, \dots, e_d$$

são fragmentados por  $\mathcal{C}$ , onde  $e_i$  denota o  $i$ -ésimo vetor de base padrão. Seja  $B \subseteq \{0, e_1, e_2, \dots, e_d\}$  qualquer. Defina o vetor  $\vec{v} \in \mathbb{R}^n$  por

$$\vec{v}_i = \begin{cases} -1, & \text{if } e_i \notin B, \\ 1, & \text{if } e_i \in B. \end{cases}$$

Se  $x \neq 0$  e  $x \in B$ , temos  $\langle x, \vec{v} \rangle = 1$ , se  $x \neq 0$  e  $x \notin B$ , temos  $\langle x, \vec{v} \rangle = -1$ , e finalmente  $\langle 0, \vec{v} \rangle = 0$ . Se  $0 \in B$ , definamos  $b = -1/2$ , e se  $0 \notin B$ , definamos  $b = 1/2$ . Em ambos os casos, o semi-espço  $H_{\vec{v},b}$  separa  $B$  do resto do conjunto  $\{0, e_1, e_2, \dots, e_d\}$ .

A cota superior,

$$\text{VC-dim}(\mathcal{C}) \leq d + 1,$$

segue do teorema 2.1.14, notando que a dimensão do espaço  $V$  de todas as funções afins sobre  $\mathbb{R}^d$ , ou seja, as funções da forma

$$\vec{x} \mapsto \langle \vec{x}, \vec{v} \rangle - b,$$

é igual a  $d + 1$ .

**Exemplo 2.1.17.** A dimensão VC da família de todas as bolas abertas euclidianas em  $\mathbb{R}^d$ ,

$$B_r(x), \quad r > 0, \quad x \in \mathbb{R}^d,$$

é igual a  $d + 1$ . (O mesmo vale para as bolas fechadas, ou bem a mistura de ambos tipos).

O resultado segue da observação seguinte: um conjunto  $A \subseteq \mathbb{R}^d$  é fragmentado pelas bolas se e somente se ele é fragmentado pelos semi-espços.

Em primeiro lugar, todo conjunto  $A$  fragmentado pelos semi-espços pode ser fragmentado pelas bolas de um raio bastante grande. De fato, as bolas podem aproximar um semi-plano com alguma precisão. Em particular, não é difícil escolher explicitamente o centro e o raio de uma bola para todo subconjunto de  $X = \{0, e_1, e_2, \dots, e_n\}$ .

Agora, seja  $A$  um conjunto fragmentado pelas bolas. Seja  $B \subseteq A$ . Existem as bolas  $B_1$  e  $B_2$  com  $B_1 \cap A = B$ ,  $B_2 \cap A = A \setminus B$ . Se  $B_1 \cap B_2 = \emptyset$ , então pelo teorema de Hahn-Banach as bolas são separadas por um hiperplano, que separa também  $B$  e  $A \setminus B$ . Caso contrário, a interseção de esferas correspondentes às bolas  $B_1, B_2$  é uma esfera num hiperplano, e como  $B_1 \cap B_2 \cap A = \emptyset$ , os subconjuntos  $B$  e  $A \setminus B$  são separados pelos semi-espços determinados pelo hiperplano.



**Exercício 2.1.18.** Deduzir o *teorema de Helly*: sejam  $x_1, x_2, \dots, x_{d+2}$  pontos em  $\mathbb{R}^d$ . Então o conjunto de índices  $\{1, 2, \dots, d+2\}$  pode ser partilhado em dois subconjuntos disjuntos,  $I$  e  $J$ , de tal maneira que as envoltórias convexas de conjuntos

$$\{x_i : i \in I\} \text{ e } \{x_j : j \in J\}$$

têm um ponto comum.

*Observação 2.1.19.* A situação com a dimensão VC da família de todas as bolas num espaço normado  $E$  de dimensão finita é mais complicada. Para o espaço  $\ell^\infty(d)$ , ela é igual a  $\lfloor (3d+1)/2 \rfloor$ , calculada em [Despres 2014]. O mesmo artigo contém um exemplo de espaço normado de dimensão 3 cuja família de bolas tem dimensão VC infinita.

A nossa apresentação desta seção segue em grande parte (não totalmente) [Anthony e Bartlett 1999].

## 2.2 Teorema de Pajor e lema de Sauer–Shelah

Sejam  $\Omega$  um domínio (conjunto qualquer) e  $\mathcal{C}$  uma classe de conceitos, ou seja, uma família não vazia de partes de  $\Omega$ . Suponhamos que a dimensão VC de  $\mathcal{C}$  é finita,  $\text{VC-dim}(\mathcal{C}) = d$ . Agora suponha que  $\sigma = \{x_1, \dots, x_n\} \subseteq \Omega$  é uma amostra, também finita, mas intuitivamente de uma cardinalidade  $n \gg d$ . A classe  $\mathcal{C}$  induz várias rotulagens sobre  $\sigma$ : se  $C \in \mathcal{C}$ , então

$$\chi_C|_\sigma : x_i \mapsto \chi_C(x_i) \in \{0, 1\}$$

é uma rotulagem. Denotemos

$$\mathcal{C}|_\sigma = \{C \cap \sigma : C \in \mathcal{C}\}.$$

Se  $n > d$ , nem todas as rotulagens sobre  $\sigma$  são desta forma. Qual é o tamanho da classe  $\mathcal{C}|_\sigma$  de todas as rotulagens induzidas pela classe  $\mathcal{C}$  sobre  $\sigma$ ? A resposta é dada pelo importante resultado, mostrado independentemente e aproximadamente ao mesmo tempo por [Sauer 1972], [Shelah 1972], e [Vapnik e Červonenkis 1971], e chamado lema de Sauer ou lema de Sauer–Shelah.

**Teorema 2.2.1** (Lema de Sauer–Shelah). *Seja  $\mathcal{C}$  uma classe de conceitos satisfazendo  $\text{VC-dim}(\mathcal{C}) \leq d$ . Se  $\sigma \subseteq \Omega$ ,  $\#\sigma = n \geq d$ , então*

$$\#\mathcal{C}|_\sigma \leq \#B_d.$$

Em particular,

$$\#\mathcal{C}|_\sigma < \left(\frac{en}{d}\right)^d.$$

Aqui  $B_d$  é uma bola fechada de raio  $d$  no cubo de Hamming de dimensão  $n$  não normalizado.

**Definição 2.2.2.** Dada uma classe de conceitos,  $\mathcal{C}$ , definamos o  $n$ -ésimo coeficiente de fragmentação ( $n$ -th shattering coefficient) de  $\mathcal{C}$  como o maior número de rotulagens induzidas por  $\mathcal{C}$  sobre as amostras com  $\leq n$  pontos:

$$s(n, \mathcal{C}) = \sup\{\#\mathcal{C}|_\sigma : \sigma \subseteq \Omega, \#\sigma \leq n\}.$$

Por exemplo, a dimensão VC de  $\mathcal{C}$  é o supremo de cardinalidades  $n$  tais que

$$s(n, \mathcal{C}) = 2^n.$$

Então, o lema de Sauer–Shelah pode ser reformulado assim:

$$s(n, \mathcal{C}) < \left( \frac{en}{\text{VC-dim}(\mathcal{C})} \right)^{\text{VC-dim}(\mathcal{C})}.$$

A mensagem mais importante deste resultado é que o número de rotulagens induzidas sobre uma amostra de tamanho  $n \rightarrow \infty$  cresce polinomialmente em  $n$ , isto é, relativamente devagar:

$$s(n, \mathcal{C}) = \text{poly}(n) \text{ se } \text{VC-dim}(\mathcal{C}) < \infty.$$

Vamos deduzir o lema de Sauer–Shelah do teorema seguinte.

**Teorema 2.2.3** (Teorema de Pajor [Pajor 1985]). *Seja  $\mathcal{C}$  uma classe de conceitos com  $m$  elementos,  $m \geq 1$ . Então  $\mathcal{C}$  fragmenta pelo menos  $m$  subconjuntos de  $\Omega$  dois a dois diferentes.*

*Demonstração.* Nós já vimos o caso particular de  $m = 1$  no exemplo 2.1.5: uma classe que consiste de único conceito fragmenta pelo menos um conjunto, a saber, o conjunto vazio. Isso é a base da prova.

Suponhamos agora que que a afirmação do teorema é verdadeira para todos  $i$ ,  $1 \leq i \leq m$ , onde  $m \geq 1$ . Seja  $\mathcal{C}$  uma família qualquer de subconjuntos de  $\Omega$  com  $m + 1$  elementos. Segue-se que  $\cup \mathcal{C} \not\supseteq \cap \mathcal{C}$ , e podemos escolher um elemento  $x_0$  que pertence a alguns membros de  $\mathcal{C}$ , mas não a todos deles. Dividamos  $\mathcal{C}$  em duas subclasses:  $\mathcal{C}_0$  consiste de todos  $A \in \mathcal{C}$  que contém  $x_0$ , e  $\mathcal{C}_1$  consiste de todos  $B \in \mathcal{C}$  que não contém  $x_0$ . Ambas são não vazias, e por conseguinte os números

$$k = \#\mathcal{C}_0, \quad l = \#\mathcal{C}_1,$$

satisfazem  $1 \leq k, l \leq m, k + l = m + 1$ . Segundo a hipótese indutiva, existem conjuntos  $A_1, \dots, A_k$  fragmentados por  $\mathcal{C}_0$ , bem como conjuntos  $B_1, \dots, B_l$  fragmentados por  $\mathcal{C}_1$ . Se todos os conjuntos na lista

$$A_1, A_2, \dots, A_k, B_1, B_2, \dots, B_l$$

são dois a dois distintos, então temos uma família de  $m + 1$  conjuntos fragmentados pela classe  $\mathcal{C} = \mathcal{C}_0 \cup \mathcal{C}_1$ . Porém, pode ocorrer que alguns conjuntos nas duas listas  $A_i$  e  $B_j$  são iguais.

Se  $A_i = B_j$ , então este conjunto é fragmentado por  $\mathcal{C}_0$ , assim como por  $\mathcal{C}_1$ . Neste caso, vamos observar que o conjunto  $A_i \cup \{x_0\}$  é fragmentado por  $\mathcal{C}$ . Se  $B \subseteq A_i \cup \{x_0\}$  e  $B \ni x_0$ , então existe um conjunto  $C \in \mathcal{C}_0$  com  $C \cap A = B \setminus \{x_0\}$ , e neste caso,  $C \cap A_i \cup \{x_0\} = B$ . Se  $B \subseteq A_i \cup \{x_0\}$  e  $B \not\ni x_0$ , existe um conjunto  $C \in \mathcal{C}_1$  com  $C \cap A = B$ , o que implica  $C \cap A_i \cup \{x_0\} = B$ . Ao mesmo tempo,  $A_i \cup \{x_0\}$  não pode ser fragmentado por  $\mathcal{C}_0$  (cujos elementos contém  $x_0$ ) nem por  $\mathcal{C}_1$  (cujos elementos não contém  $x_0$ ). Logo,  $A_i \cup \{x_0\}$  é diferente de todos os outros conjuntos na lista.

Concluimos: os conjuntos na primeira lista,  $A_1, \dots, A_k$ , bem como os conjuntos na segunda lista  $B_1, \dots, B_l$  que não se encontram na primeira lista, e os conjuntos  $A_i \cup \{x_0\}$  para todos os conjuntos que se encontram na interseção de duas listas, são todos fragmentados pela classe  $\mathcal{C}$  e são dois a dois diferentes. O número de tais conjuntos é  $m + 1$ .  $\square$

Para deduzir o lema de Sauer–Shelah do teorema de Pajor, seja  $\mathcal{C}$  uma classe de conceitos com a dimensão de Vapnik–Chervonenkis  $\leq d$ . Então, a classe  $\mathcal{C}$ , e por conseguinte a classe  $\mathcal{C}|\sigma$ , não fragmentam nenhum conjunto com mais de  $d$  pontos. Todos os subconjuntos de  $\sigma$  fragmentados pelo  $\mathcal{C}|\sigma$  tem a cardinalidade  $\leq d$ . Segundo o teorema de Pajor, a classe  $\mathcal{C}|\sigma$  fragmenta pelo menos  $s(\mathcal{C}, n)$  subconjuntos dois a dois diferentes de  $\sigma$ . Basta notar que a família de subconjuntos de  $\sigma$  com  $\leq d$  pontos é equipotente à bola  $B_d(0)$ . Concluimos:  $s(\mathcal{C}, n)$  não pode ser maior do que  $\#B_d(0)$ .  $\square$

Revisitemos o lema de Sauer–Shelah no subseção 8.2.4.

## 2.3 Redes de unidades computacionais

### 2.3.1 Unidade de computação

Como nos já mencionamos, a origem de classes de conceitos é algorítmico: cada tal classe,  $\mathcal{C}$ , é uma classe de conceitos (funções binárias) gerados por um algoritmo, para todos os valores de parâmetros possíveis. Um tal algoritmo é conhecido como uma *unidade de computação*. Eis um exemplo simples mas importante.

**Exemplo 2.3.1** (Perceptron). Uma unidade de computação que gera o espaço de todos os semi-espacos do espaço euclidiano  $\mathbb{R}^d$  (como no exemplo 2.1.16) é conhecida na aprendizagem de máquina como *perceptron*. É uma função

$$\eta \left( \sum_{i=1}^d w_i x_i - \theta \right),$$

onde  $w_1, w_2, \dots, w_n, \theta \in \mathbb{R}$  são os valores de parâmetros,  $x_1, \dots, x_d$  são os valores de

entrada (inputs), e  $\eta$  é a função de Heaviside:

$$\eta(x) = \begin{cases} 1, & \text{se } x \geq 0, \\ 0, & \text{se } x < 0. \end{cases}$$

O estado de um perceptron é o vetor de valores de parâmetros,  $\omega = (w_1, w_2, \dots, w_d, \theta) \in \mathbb{R}^{d+1}$ , onde os  $w_i$  são os pesos, e  $\theta$ , o valor limiar. Cada estado determina uma função binária (isto é, um classificador) sobre  $\mathbb{R}^d$ , e um correspondente semi-espaço. Deste modo, o perceptron pode ser visto como uma aplicação

$$\mathbb{R}^{d+1} \times \mathbb{R}^d \rightarrow \{0, 1\},$$

onde  $\mathbb{R}^{d+1}$  é o espaço de estados dele, e  $\mathbb{R}^d$ , o domínio.

Com a base no exemplo acima, vamos isolar a noção formal seguinte, mais geral e mais básico do que a noção de uma regra de aprendizagem (a seguir mais tarde).

**Definição 2.3.2.** Uma *unidade computacional (binária)* é uma aplicação

$$u: \mathcal{W} \times \Omega \rightarrow \{0, 1\},$$

onde  $\mathcal{W}$  é o *espaço de estados* da unidade e  $\Omega$  é o domínio.

Desse modo, dado um estado  $\omega \in \mathcal{W}$  e qualquer ponto  $x \in \Omega$ , a unidade calcula o valor  $u^\omega(x)$ , seja 0, seja 1. Toda aplicação  $u^\omega: x \mapsto u^\omega(x)$  é um classificador sobre  $\Omega$ , e desse modo, a função indicadora de um subconjunto  $C^\omega \subseteq \Omega$  (um conceito).

*Observação 2.3.3.* A unidade de computação  $u$  pode ser assim vista como uma família de conceitos  $C^\omega$ ,  $\omega \in \mathcal{W}$ , indexada com um conjunto de estados. Como o conjunto de estados, pode ser usada a própria classe de conceitos  $\mathcal{C}$ . Assim, não há diferença principal entre uma unidade computacional e uma classe de conceitos.

*Observação 2.3.4.* Eis mais um ponto de vista sobre a noção de unidade de computação. As informações sobre uma tal unidade,  $u$ , podem ser completamente codificadas no subconjunto seguinte do produto cartesiano  $\Omega \times \mathcal{W}$ :

$$\mathcal{C}_u = \{(x, \omega) : x \in \Omega, \omega \in \mathcal{W}, u^\omega(x) = 1\} \equiv \{(x, \omega) : x \in C^\omega\}.$$

Então, pode-se dizer que uma unidade de computação (de ponto de vista puramente conjuntístico) é simplesmente um subconjunto qualquer,

$$\mathcal{C}_u \subseteq \Omega \times \mathcal{W}.$$

As “seções horizontais” do conjunto  $\mathcal{C}_u$  (ao nível  $\omega$ ) são os conceitos  $C^\omega$ .

*Observação 2.3.5.* Vamos eventualmente impor sobre a definição de uma unidade de computação o requerimento adicional que a função  $u: \mathcal{W} \times \Omega \rightarrow \{0, 1\}$  (ou, de modo equivalente, o conjunto  $\mathcal{C}_u$ ) seja *mensurável no sentido de Borel* relativo a uma *estrutura boreliana padrão* sobre  $\mathcal{W}$  e  $\Omega$ . Estas noções estão formalizadas nos apêndices **A** e **D**. Tais restrições não são restritivas, e unicamente servem para eliminar algumas patologias da natureza conjuntística.

**Definição 2.3.6.** Pode acontecer que o domínio de uma unidade de computação,  $\Omega$ , é um produto cartesiano:

$$\Omega = \Omega_1 \times \Omega_2 \times \dots \times \Omega_k.$$

Nesse caso, digamos que  $u$  é uma unidade com  $k$  entradas (inputs):

$$u^\omega(x) = u^\omega(x_1, x_2, \dots, x_d).$$

**Exemplo 2.3.7.** O *perceptron* é uma unidade com  $d$  entradas.

**Definição 2.3.8.** A dimensão de Vapnik–Chervonenkis de uma unidade de computação,  $u$ , é definida como a dimensão VC da classe de conceitos correspondente,

$$\mathcal{C}_u = \{C^\omega : \omega \in \mathcal{W}\},$$

gerada por  $u$ .

**Exemplo 2.3.9.** A dimensão VC de um perceptron com  $d$  entradas é igual à  $d + 1$ .

*Observação 2.3.10.* Na *teoria algorítmica* (ou: *computacional*) de *aprendizagem de máquina* o estudo da natureza e do funcionamento das unidades de computação é particularmente importante, com ênfase sobre a complexidade computacional delas. Não tocamos neste assunto aqui. Veja, por exemplo, [Kearns e Vazirani 1994].

*Observação 2.3.11.* Nessa perspectiva, uma *regra de aprendizagem* é uma unidade computacional cujos estados são todos as amostras rotuladas.

Alarguemos um pouco a nossa coleção de exemplos das unidades computacionais.

**Exemplo 2.3.12** (Regra de histograma). Seja  $\Omega$  um domínio qualquer. Uma unidade computacional para  $\Omega$  chamada *regra de histograma* é determinada pelos valores de dois parâmetros:  $\gamma$ , uma partição finita de  $\Omega$ , e  $\sigma = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n)$ , uma amostra rotulada, onde  $x_i \in \Omega$  e  $\epsilon_i \in \{0, 1\}$ . Desse modo, o espaço de estados do histograma pode ser identificado com o produto cartesiano de família de todas as partições finitas de  $\Omega$  com o conjunto  $\cup_{i=1}^{\infty} \Omega^n \times \{0, 1\}^n$  de todas as amostras rotuladas em  $\Omega$ .

Dado um ponto  $x \in \Omega$  qualquer, assim como uma partição  $\gamma$  e uma amostra rotulada  $\sigma$ , existe um e apenas um elemento  $A \in \gamma$  que contém  $x$  como elemento. Denotemos por  $\sigma \upharpoonright_A$  uma amostra rotulada que consiste de todos os pontos  $x_i$ ,  $i = 1, 2, \dots, n$  em  $A$ , junto com os seus rótulos originais. A regra de histograma assina a  $x$  o rótulo majoritário da amostra  $\sigma \upharpoonright_A$ . No caso de empates (o mesmo número de 0 que de 1 entre os rótulos) a gente pode, por exemplo, sempre escolher 1, de mesmo que no caso onde  $\sigma \upharpoonright_A$  é vazia:

$$u^{\gamma, \sigma}(x) = \eta \left( \sum_{x_i \in A} \left( \epsilon_i - \frac{1}{2} \right) \right).$$

Em particular, a fórmula vai assinar o rótulo 1 a  $x$  no case se  $\sigma$  é disjuncto de  $A$  (pois a soma de uma família vazia de reais é igual a 0).

A origem do termo “histograma” é que o valor da nossa função em todo ponto do domínio é completamente determinado por um “histograma” (ou, melhor, dois histogramas) contando os números de 0s e de 1s em cada elemento da partição  $\gamma$ . O rótulo de  $x$  depende de qual de dois histogramas seja mais alto em  $x$ .

**Exemplo 2.3.13** (Árvore de decisão). Uma árvore de decisão é uma unidade de computação de tipo regra de histograma, cuja partição do domínio  $\Omega = \mathbb{R}^m$  consiste de retângulos, ou seja, produtos cartesianos de intervalos (da forma  $[a, b)$ ,  $(-\infty, a)$ ,  $[b, +\infty)$ , e  $(-\infty, +\infty)$ ).

Os retângulos são tipicamente construídas recursivamente, a partir de uma amostra rotulada,  $\sigma$ . Ao primeiro passo, escolhemos uma coordenada  $i \in [m]$  e um número real  $a_1$ , dividindo o espaço  $\mathbb{R}^m$  em dois retângulos pelo hiper-espaço  $x_i = a$ . A seleção de  $a$  é feita de modo para maximizar uma medida de separação de uma amostra rotulada em duas classes com rótulos mais diferentes possíveis. Cada um de dois retângulos resultantes é dividido em dois sub-retângulos ao longo de uma outra coordenada  $j \in [m]$ , escolhendo os valores  $a_{21}$  e  $a_{22}$ , e o procedimento continua até o momento quando todo retângulo conter menos de  $k$  pontos de  $\sigma$  (o valor  $k$  é predefinido).

### 2.3.2 Agrupando unidades de computação em redes

As unidades de computação podem ser agrupadas em redes, produzindo as unidades cada vez mais complexas.

**Exemplo 2.3.14** (Aprendizagem ensemble (ensemble learning)). Uma estratégia importante para criar novos algoritmos de aprendizagem é de tomar o voto majoritário entre muitas versões de regras de aprendizagem (tipicamente, do mesmo tipo mas com os parâmetros variáveis).

Por exemplo, o algoritmo provavelmente mais popular na prática atual de cientistas de dados, Floresta Aleatória (Random Forest, RF), usa o voto majoritário entre um alto número (por exemplo, 500) de árvores de decisão construídos usando parâmetros escolhidos aleatoriamente (tais como as coordenadas  $i$  de divisão).

Dado um *ensemble* de classificadores,  $u_1, u_2, \dots, u_k$ , e um ponto  $x$ , os valores de predições  $u_1(x), u_2(x), \dots, u_k(x)$ , são alimentados a uma unidade computacional, que conta os votos e sai o valor, 0 ou 1, recebendo mais votos. Uma tal unidade pode ser um perceptron:

$$\eta \left( \sum_i \left( x_i - \frac{1}{2} \right) \right).$$

Graficamente, a rede combinada das unidades de computação pode ser representada assim: Os  $x_i$ ,  $i = 1, 2, \dots, n$ , representam os valores da entrada (inputs), todos alimentados às todas unidades de computação  $u_j$ ,  $j = 1, 2, \dots, k$ . As saídas de unidades  $u_j$  são alimentadas ao perceptron determinando o voto majoritário. A saída do perceptron é a saída da rede. Duas unidades são ligadas por uma aresta se a saída da primeira unidade serve de uma entrada da segunda. As unidades são agrupadas em três camadas: a camada

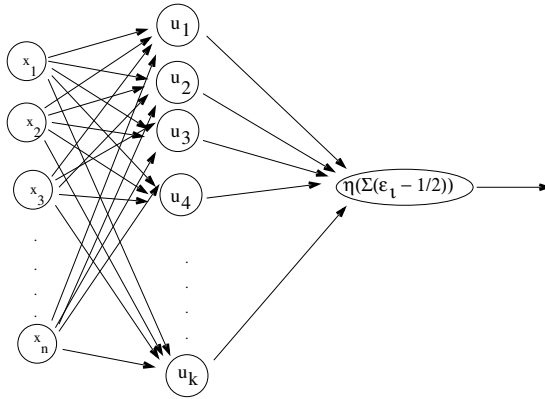


Figura 2.7: Uma rede de aprendizagem ensemble.

0 de valores de entrada, a camada 1 de unidades  $u_j$ , e a camada 2 que só contém a unidade de saída.

Métodos de aprendizagem ensemble são uma ferramenta entre as mais importantes para construir novos algoritmos. Veja por exemplo o livro [Z.-H. Zhou 2012].

Com base no último exemplo, vamos formalizar a noção de uma rede de unidades de computação binárias.

**Definição 2.3.15.** Um grafo dirigido (simples) é um par,  $(V, E)$ , que consiste de um conjunto  $V$  de *vértices*, ou (mais tipicamente nesse contexto) *nós*, e um conjunto  $E \subseteq V^2$  de pares dirigidos  $(x, y)$ , chamados *arestas* ou *arcos*. Suponhamos que  $x \neq y$  (não tem laços). O *grau de entrada* do nó  $x$ ,  $\text{indeg}(x)$ , é o número  $\#\{y \in V : (y, x) \in E\}$ , e o *grau de saída* de  $x$ ,  $\text{outdeg}(x)$ , é definido similarmente.

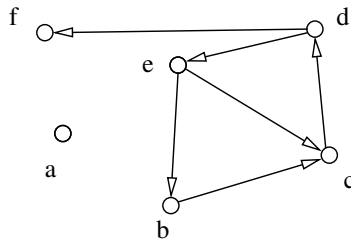


Figura 2.8: Um grafo dirigido com 6 vértices.

Supõe-se que existe pelo menos um nó  $x$  com  $\text{indeg}(x) = 0$ . Tais nós, chamados *nós de entrada*, aceitam os valores de input, tipicamente os valores reais. Por exemplo, se queremos tratar um vetor  $x \in \mathbb{R}^m$ , precisamos  $m$  nós de input, um para cada coordenada  $x_i$ .

A outra hipótese é que existe pelo menos um nó  $x$  com  $\text{outdeg}(x) = 0$ . São os *nós de saída*, produzindo os resultados de computação. Para simplificar as coisas, suponhamos que existe o único nó de saída.

**Definição 2.3.16.** Uma *rede de unidades de computação*,  $\mathcal{N}$ , é um grafo dirigido, que possui pelo menos um nó de entrada e cujos nós que não são os de entrada são unidades de computação binárias, com  $\text{indeg}(u)$  valores de entrada cada uma.

Então, para cada estado  $\omega$  de  $u$ , a função binária  $u^\omega$  aceita  $\text{indeg}(u)$  argumentos. O domínio de  $u^\omega$  é o produto  $\mathbb{R}^p \times \{0, 1\}^q$ , onde  $p + q = \text{indeg}(u)$ . Aqui,  $p$  é o número de  $x$  tais que  $(x, u) \in E$  e  $x$  é um nó de entrada, e  $q$  é o número de  $v$  tais que  $(v, u) \in E$  e  $v$  é uma unidade computacional.

**Definição 2.3.17.** O *espaço de estados* da rede é um subconjunto,  $\mathcal{W}$ , do produto  $\prod_u \mathcal{W}_u$ . Desse modo, um estado  $\omega = (\omega_u)_u$  da rede determina um estado,  $\omega_u$ , de cada unidade computacional,  $u$ .

Na prática, ao invés desse subconjunto, pode-se tratar de uma *parametrização* de  $\mathcal{W}$ . O *treinamento* da rede é um procedimento algorítmico para escolher um estado,  $\omega$ .

**Definição 2.3.18.** No caso se uma rede de unidades computacionais,  $\mathcal{N}$ , não tem ciclos (como um grafo dirigido), ela é dita uma rede *sem realimentação* (*feed-forward*).

A partir desse momento, estudemos somente as redes sem realimentação. Dado um estado,  $\omega$ , de uma tal rede, podem-se definir recursivamente as funções  $f_u^\omega$  em toda unidade de computação, como composições das funções  $u^\omega$ , na ordem determinada pelo grafo. Os argumentos da função  $u^\omega$  são ou os valores das funções  $u^\omega$  onde a unidade  $v$  é ligada com  $u$  ( $(v, u) \in E$ ), ou os valores de entrada atribuídos aos nós de entrada  $x$  ligados a  $u$  ( $(x, u) \in E$ ). A função binária  $f_{u_{out}}^\omega$ , onde  $u_{out}$  é o nó de saída, aceita os valores de input e produz 0 ou 1.

Mais especificamente, enumeremos os nós da rede,  $x_1, x_2, \dots, x_k$  da maneira que se  $(x_i, x_j) \in E$ , então  $i < j$ . Agora, suponha que um valor seja atribuído a cada um dos  $m$  nós de entrada,  $\sigma_1, \dots, \sigma_m$ . Para todo  $i = 1, 2, \dots, k$ , calculamos recursivamente o valor  $f_i^\omega(\sigma) = f_{x_i}^\omega(\sigma)$  como segue:

- $f_i^\omega(\sigma) = \sigma$  se  $x_i$  é um nó de entrada;
- $f_i^\omega(\sigma) = x_i^\omega(f_{i_1}^\omega(\sigma), \dots, f_{i_s}^\omega(\sigma))$ , onde  $x_{i_1}, \dots, x_{i_s}$  são os nós ligados à unidade computacional  $x_i$ .

O que faz o procedimento bem-definido, é o fato de que quando  $j$  for conectado com  $i$ , temos  $j < i$  e logo o valor de  $f_j^\omega(\sigma)$  já foi calculado quando chegar a hora de calcular o valor  $f_i^\omega(\sigma)$ .



Denotemos por  $\mathcal{C}_{\mathcal{N}}$  a família de todas as funções  $f_{u_{out}}^{\omega}$ , onde  $\omega \in \mathcal{W}$ . É a *classe de conceitos gerada* pela rede  $\mathcal{N}$ . Desse modo, a rede  $\mathcal{N}$  torna-se em uma unidade de computação. Em particular, pode-se falar da sua dimensão de Vapnik–Chervonenkis.

Uma classe importante de redes de unidades de computação consiste de *redes neurais artificiais* (*artificial neural networks*, *ANN*).

### 2.3.3 Redes neurais sem realimentação com valor limiar linear

Estas redes (*feed-forward linear threshold networks*) têm uma arquitetura particular, dita *multicamada*. Tal rede é caracterizada pelas propriedades seguintes.

- Cada unidade computacional é um perceptron, e
- os nós do grafo são agrupados em *camadas*, enumeradas com os números naturais,

$$\ell(x_i) = 0, 1, \dots, l,$$

de maneira que

- os nós de entrada pertencem a camada zero, e
- se  $x_i$  é conectado a  $x_j$ , então  $\ell(x_i) < \ell(x_j)$ .

Então, os nós dentro uma camada nunca são conectados, e a última ( $l$ -ésima) camada tem somente um nó, o nó de saída.

**Exemplo 2.3.19** (Perceptron como uma rede neural). O perceptron visto no contexto das redes neurais é o exemplo mais simples e ao mesmo tempo mais antigo historicamente.

Um *perceptron* é uma rede neural artificial com  $d \geq 1$  nós de entrada e um nó de saída, munido de uma função da forma

$$g = \eta \circ z,$$

onde

$$z: \mathbb{R}^d \rightarrow \mathbb{R}$$

é uma função afim,

$$z(x_1, x_2, \dots, x_d) = \sum_{i=1}^d w_i x_i - \theta,$$

chamada de *função modeladora* (*shaping function*), cujos coeficientes  $w_i \in \mathbb{R}$ ,  $i = 1, 2, \dots, d$  são ditos *pesos*, e  $\theta \in \mathbb{R}$  é o *valor limiar*. Enquanto

$$\eta: \mathbb{R} \rightarrow \{0, 1\}$$

e a função de Heaviside:

$$\eta(x) = \begin{cases} 1, & \text{if } x \geq 0, \\ 0, & \text{if } x < 0. \end{cases}$$

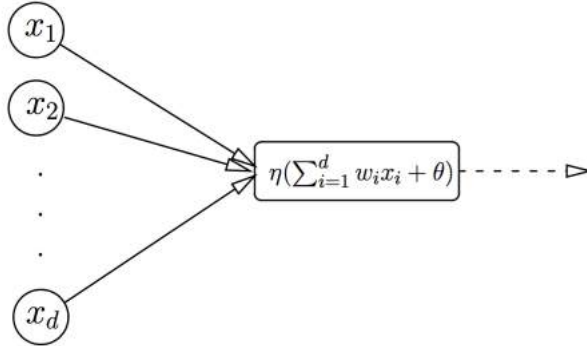


Figura 2.9: Perceptron.

A função  $\eta$  é dita *função de ativação (activation function)*.

A função de ativação dispara um sinal 1 se a intensidade do valor  $\sum_{i=1}^d w_i x_i$  é maior do que o valor limiar  $\theta$ .

### 2.3.4 Dimensão VC de redes das unidades de computação

O restante desta subseção é dedicada à prova do seguinte teorema.

**Teorema 2.3.20.** *Seja  $\mathcal{N}$  uma rede sem realimentação, tendo  $k$  unidades computacionais binárias, incluindo um nó de saída. Seja  $W$  a soma total de dimensões VC de todas as unidades de  $\mathcal{N}$ . Então, para todo  $n$ ,*

$$s(\mathcal{N}, n) \leq \left( \frac{enk}{W} \right)^W, \quad (2.1)$$

e

$$VC\text{-dim}(\mathcal{N}) \leq 2W \log_2 \left( \frac{2k}{\log 2} \right). \quad (2.2)$$

Aqui,  $VC\text{-dim}(\mathcal{N})$  é a dimensão VC da classe de conceitos  $\mathcal{C}_{\mathcal{N}}$  gerada pela rede  $\mathcal{N}$ .

*Observação 2.3.21.* Por exemplo, o teorema se aplica a cada rede neural sem realimentação com valor limiar linear. Neste caso,  $W$  é simplesmente o número total de parâmetros ajustáveis da rede que são os pesos,  $w_{ij}$ , e os valores limiares,  $\theta_i$ , dos perceptrons.

A nossa prova segue, nas suas grandes linhas, [Anthony e Bartlett 1999].

**Lema 2.3.22.** Seja  $f : X \rightarrow Y$  uma aplicação qualquer, e seja  $\mathcal{C}$  uma classe de conceitos sobre  $Y$ ,  $\mathcal{C} \subseteq 2^Y$ . Então a dimensão VC da família de funções binárias do tipo

$$\chi_C \circ f, \quad C \in \mathcal{C},$$

é menor ou igual de  $VC\text{-dim}(\mathcal{C})$ .

*Demonstração.* Exercício. □

**Lema 2.3.23.** Para todos  $\alpha, x > 0$ ,

$$\log x \leq \alpha x - \log \alpha - 1,$$

e a igualdade é atingida se e apenas se  $\alpha x = 1$ .

*Demonstração.* Levar  $\log \alpha$  no lado esquerdo, exponenciar, e usar a expansão de Taylor. □

**Definição 2.3.24.** Um espaço probabilístico finito é um conjunto finito,  $X = \{x_1, x_2, \dots, x_n\}$ , onde cada ponto  $x_i$  tem um peso associado,  $p_i \geq 0$ , tendo a propriedade

$$\sum_{i=1}^n p_i = 1.$$

A medida de probabilidade,  $\mu$ , é definida pelos pesos como segue: se  $A \subseteq X$ ,

$$\mu(A) = \sum_{x_j \in A} p_j.$$

É fácil de verificar que  $\mu$  é uma medida de probabilidade. Por exemplo, a medida de contagem normalizada sobre o cubo de Hamming é uma *medida uniforme* no sentido que os pesos correspondentes são todos iguais:

$$\forall \sigma \in \{0, 1\}^n, \quad p_\sigma = \frac{1}{2^n}.$$

**Definição 2.3.25.** Seja  $X$  um espaço probabilístico finito, com pontos  $x_1, x_2, \dots, x_n$  e probabilidades  $p_i$ . A *entropia* de  $X$  é a quantidade

$$H(X) = \sum_{i=1}^n -p_i \log p_i.$$

**Lema 2.3.26.** *O valor máximo da entropia de um espaço probabilístico finito,  $X$ , como acima é igual  $\log n$ , atingido sobre a distribuição uniforme:*

$$p_i = \frac{1}{n}, \quad i = 1, 2, \dots, n.$$

*Demonstração.* O logaritmo é uma função côncava no seu domínio de definição, ou seja, para quaisquer que sejam  $\lambda_1, \lambda_2 > 0$  e  $p_1, p_2 \in [0, 1]$ ,  $p_1 + p_2 = 1$ , temos

$$\log(p_1 \lambda_1 + p_2 \lambda_2) \geq p_1 \log \lambda_1 + p_2 \log \lambda_2.$$

Pela indução finita, concluímos que, para qualquer que seja a coleção  $\lambda_i > 0$ ,  $i = 1, 2, \dots, n$ ,

$$\log \left( \sum_{i=1}^n p_i \lambda_i \right) \geq \sum_{i=1}^n p_i \log(\lambda_i).$$

No caso  $\lambda_i = 1/p_i$ , deduzimos

$$\log n \geq \sum_{i=1}^n p_i \log \left( \frac{1}{p_i} \right) = H(X),$$

e além disso, se  $p_i = 1/n$ ,  $i = 1, 2, \dots, n$ ,

$$H(X) = \sum_{i=1}^n -p_i \log p_i = \sum_{i=1}^n \frac{\log n}{n} = \log n.$$

□

*Observação 2.3.27.* A noção de entropia foi definida por Claude Shannon no contexto da sua teoria de informação [Shannon 1948]. A entropia é uma medida de incerteza, no sentido seguinte. Suponha que  $x_1, x_2, \dots, x_n$  são as mensagens, e que  $p_1, p_2, \dots, p_n$  são as probabilidades de receber cada uma delas. Quando as probabilidades são todas iguais a  $1/n$ , não temos nenhuma informação sobre qual mensagem é mais provável. Nesse caso, a incerteza é completa, e a entropia atinge o valor máximo,  $\log n$ . Ao contrário, suponha que, por exemplo,  $p_1 = 1$  e  $p_j = 0$ ,  $i \neq j$ , ou seja, a mensagem  $x_1$  vai chegar com probabilidade um. Nesse caso, a certeza é total, e a entropia atinge o seu mínimo, 0. (A expressão  $-0 \cdot \log 0$  surgindo na definição da entropia nesse caso, está tratada como o limite  $\lim_{\epsilon \rightarrow 0} -\epsilon \log \epsilon$ , que existe).

Agora nos temos todas as ferramentas para mostrar o teorema 2.3.20. Escolhemos uma ordem total no conjunto de todas as unidades computacionais,

$$u_1, u_2, \dots, u_k,$$

de maneira que se existe uma conexão de  $u_i$  para  $u_j$ , então  $i < j$ . (É sempre possível de estender uma ordem parcial a uma ordem total). Denotemos por  $\mathcal{W}$  o espaço de estados da rede  $\mathcal{N}$ . Temos

$$\sum_{i=1}^k d_i = W. \quad (2.3)$$

Dado um estado  $\omega$  qualquer, denotemos por  $f_i^\omega$  a função de saída da unidade  $i$ , que é uma composição recursiva de funções  $u_j^\omega$ ,  $j \leq i$ , numa ordem determinada pelas conexões. Em particular,  $f_k^\omega$  é a função binária de saída da nossa rede.

Sejam  $\Omega$  o domínio (por exemplo, pode ser  $\Omega = \mathbb{R}^m$ , onde  $m$  é o número de nós de entrada da rede, mas  $m$  não desempenha papel nessa demonstração), e  $\sigma \subseteq \Omega^n$ , uma amostra fixa. Vamos estimar superiormente o número de funções binárias distintas da forma  $f_k^\omega|_\sigma$ ,  $\omega \in \mathcal{W}$ .

Para todo  $i = 1, 2, \dots, k$ , digamos que dois estados,  $\omega$  e  $\omega'$ , são *indistinguíveis até a unidade  $i$*  se para todos  $j = 1, 2, \dots, i$  e todos valores de entrada  $x \in \sigma$  temos

$$f_j^\omega(x) = f_j^{\omega'}(x).$$

Denotemos essa relação por  $\omega \stackrel{i}{\sim} \omega'$ . Ser indistinguíveis até a unidade  $i$  significa que um observador não pode distinguir o estado  $\omega$  do estado  $\omega'$  somente observando os resultados de cálculo de valores de todas as funções binárias  $f_j^\omega$  aparecendo até e incluindo o nó  $i$  sobre o conjunto  $\sigma$ .

É fácil a ver que  $\stackrel{i}{\sim}$  é uma relação de equivalência sobre o espaço de estados  $\mathcal{W}$  para todo  $i = 1, 2, \dots, k$ , e por conseguinte ela define uma partição finita  $\Upsilon_i$  de  $\mathcal{W}$  em subconjuntos dois a dois disjuntos. Além disso, se  $i < j$ , então a partição  $\Upsilon_j$  refina a partição  $\Upsilon_i$ :

$$\Upsilon_j < \Upsilon_i.$$

Se os valores de duas funções de saída,  $f_k^\omega$  e  $f_k^{\omega'}$ , diferem sobre um  $x \in \sigma$ , então obviamente  $\omega \not\stackrel{k}{\sim} \omega'$ . Por conseguinte, o número máximo de funções duas a duas distintas da forma  $f_k^\omega|_\sigma$ ,  $\omega \in \mathcal{W}$ , é limitado de acima pelo tamanho da partição final,  $\Upsilon_k$ . Vamos estimar  $\#\Upsilon_i$  recursivamente em  $i$ , começando com  $i = 1$ .

Dois estados  $\omega$  e  $\omega'$  quaisquer podem ser distinguidos na unidade  $u_1$  se e apenas se existe  $x \in \sigma$  tal que  $f_1^\omega(x) \neq f_1^{\omega'}(x)$ . De modo equivalente:  $u_1^\omega(x) \neq u_1^{\omega'}(x)$ . Neste caso particular, temos

$$\#\Upsilon_1 = \#\{u_1^\omega \upharpoonright \sigma : \omega \in \mathbb{R}^W\} \leq \left(\frac{en}{d_1}\right)^{d_1},$$

graças ao lema de Sauer-Shelah e a hipótese  $\text{VC-dim}(u_1) = d_1$ .

Agora suponha que o tamanho da partição  $\Upsilon_{i-1}$  já foi estimado. Seja  $A \in \Upsilon_{i-1}$  uma classe de equivalência qualquer dessa partição. Em quantos subconjuntos a relação  $\stackrel{i}{\sim}$  vai

dividir  $A$ ? Se  $\omega, \omega' \in A$ , então para todos  $x \in \sigma$  e todos  $j \leq i-1$  temos  $f_j^\omega(x) = f_j^{\omega'}(x)$ . Em particular, as funções  $u_i^\omega$  e  $u_i^{\omega'}$  tem os mesmos valores de todos os seus argumentos. Em outras palavras, qual quer seja  $\omega \in A$ , a função  $f_i^\omega$  pode ser escrita como  $u_i^\omega \circ g$ , onde a função  $g$  não depende de  $\omega$ . Segundo o lema 2.3.22, a dimensão VC do conjunto de funções  $f_i^\omega, \omega \in A$ , é menor ou igual a  $d_i$ . O lema de Sauer-Shelah implica

$$\#\{f_i^\omega : \omega \in A\} \leq \left(\frac{en}{d_i}\right)^{d_i}.$$

Concluimos: o conjunto  $A$  é dividido pela relação  $\sim^i$  em

$$\leq \left(\frac{en}{d_i}\right)^{d_i}$$

subconjuntos. Cada tal subconjunto corresponde a uma restrição diferente do tipo  $f_i^\omega|_\sigma$ ,  $\omega \in C$ . Por conseguinte,

$$\#\Upsilon_i \leq \left(\frac{en}{d_i}\right)^{d_i} \#\Upsilon_{i-1},$$

então

$$|\mathcal{C}_{\mathcal{N}} \upharpoonright \sigma| \leq |\Upsilon_k| \leq \prod_{i=1}^k \left(\frac{en}{d_i}\right)^{d_i}.$$

Concluimos:

$$\log s(\mathcal{N}, n) \leq \sum_{i=1}^k d_i \log \left(\frac{en}{d_i}\right).$$

A última expressão é remanescente da entropia de um espaço probabilístico finito, e agora vamos manipulá-la. De fato, os valores  $d_i/W$  são as probabilidades, em vista da Eq. (2.3). Denotemos por  $X$  um espaço finito com pesos de pontos iguais a  $d_i/W$ ,  $i = 1, 2, \dots, k$ . Temos:

$$\begin{aligned} \log s(\mathcal{N}, n) &\leq \sum_{i=1}^k d_i \log \left(\frac{en}{d_i}\right) \\ &= W \sum_{i=1}^k \frac{d_i}{W} \left[ \log \frac{W}{d_i} + \log(en) - \log W \right] \\ &= W \cdot H(X) + W \log \frac{en}{W} \\ &\leq W \log k + W \log \frac{en}{W} \\ &= W \log \frac{enk}{W}. \end{aligned}$$

Exponenciando, obtemos a Eq. (2.1).

Temos  $\text{VC-dim}(\mathcal{N}) < n$  se e apenas se

$$s(\mathcal{N}, n) < 2^n,$$

em particular, for o caso quando

$$\left(\frac{enk}{W}\right)^W \leq 2^n,$$

ou seja,

$$n \geq W \log_2 \left(\frac{enk}{W}\right). \quad (2.4)$$

Quando esta desigualdade, (2.4), tem lugar? Aplicamos lema 2.3.23 com

$$x = \frac{enk}{W} \text{ e } \alpha = \frac{\log 2}{2ek}$$

para deduzir

$$\log \left(\frac{enk}{W}\right) \leq \frac{n \log 2}{2W} - \log \left(\frac{\log 2}{2ek}\right) - 1,$$

ou seja,

$$\log \left(\frac{enk}{W}\right) \leq \frac{n \log 2}{2W} + \log \left(\frac{2k}{\log 2}\right),$$

e como  $\log x / \log 2 = \log_2 x$ ,

$$W \log_2 \left(\frac{enk}{W}\right) \leq \frac{n}{2} + W \log_2 \left(\frac{2k}{\log 2}\right).$$

Agora (2.4) é válido quando

$$W \log_2 \left(\frac{2k}{\log 2}\right) \leq \frac{n}{2},$$

ou seja,

$$n \geq 2W \log_2 \left(\frac{2k}{\log 2}\right).$$

de onde obtemos (2.2).

Então, a dimensão VC da rede satisfaz

$$d = O(W \log k),$$

onde  $W$  é a soma de dimensões VC de todas as  $k$  unidades computacionais. Pode-se mostrar que a ordem de grandeza é ótima.

### 2.3.5 A rede sigmóide de Sontag

A função de Heaviside,  $\eta$ , é um exemplo particular de uma função *sigmóide*,  $s: \mathbb{R} \rightarrow [0, 1]$ , isto é, uma função monótona (não necessariamente contínua) com  $\lim_{t \rightarrow -\infty} s(t) = 0$  e  $\lim_{t \rightarrow +\infty} s(t) = 1$ . Por exemplo, a função

$$f(t) = \frac{1}{\pi} \arctan t + \frac{1}{2}$$

é sigmóide, entre muitas outras. Tais funções são frequentemente usadas na teoria de redes neurais como funções de ativação. O exemplo de Sontag [Sontag 1992] mostra uma rede neural simples, com só 4 nós, cujas funções de modelagem são lineares e as funções de ativação são sigmoidais, e que possui um grande poder de fragmentação: não somente a rede tem a dimensão VC infinita, mais ela vai fragmentar “quase todos” subconjuntos finitos de  $\mathbb{R}$ .

#### Lema de Kronecker

Denotemos por  $\mathbb{T}$  o grupo de rotações do círculo, munido da multiplicação usual de números complexos:

$$\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}.$$

Este grupo pode ser também identificado com o grupo aditivo de números reais modulo 1,

$$\mathbb{T} = \mathbb{R}/\mathbb{Z},$$

com a ajuda da aplicação exponencial,  $\mathbb{R} \ni t \mapsto \exp(2\pi it) \in \mathbb{T}$ . O produto  $\mathbb{T}^n$  de  $n$  cópias de  $\mathbb{T}$  é chamado o *toro* de posto  $n$ . Temos a identificação

$$\mathbb{T}^n = \mathbb{R}^n / \mathbb{Z}^n.$$

A reta  $\mathbb{R}$  pode ser vista como um espaço vetorial sobre o corpo  $\mathbb{Q}$  dos números racionais. Como tal,  $\mathbb{R}$  tem dimensão infinita (com efeito, a dimensão de contínuo,  $c$ ). Uma  $n$ -upla dos reais,  $x_1, x_2, \dots, x_n$ , é dita *racionalmente independente* se ela forma uma família linearmente independente em  $\mathbb{R}$  visto como um espaço vetorial sobre  $\mathbb{Q}$ . Ou seja, nenhuma combinação linear não trivial com os coeficientes racionais,  $\sum_{i=1}^n q_i x_i$ , se anula. Ao invés de racionais, bastaria considerar os coeficientes inteiros.

Por uma questão de simplificação cometamos um abuso de linguagem e digamos que uma  $n$ -upla  $x = (x_1, x_2, \dots, x_n) \in \mathbb{T}^n$  dos elementos de  $\mathbb{T}$  é racionalmente independente se qualquer  $n$ -upla de reais,  $x'_1, x'_2, \dots, x'_n$ , enviada sobre a nossa tupla pela função exponencial,  $x_i = \exp(2\pi i x'_i)$ , é racionalmente independente. (Neste caso, pode-se ver que *cada* tupla de reais enviada para a nossa tupla é racionalmente independente).

Finalmente, recordemos que um subconjunto  $A$  de um espaço métrico é *denso* se a aderência de  $A$  em  $X$  é igual a  $X$ .

**Teorema 2.3.28** (Lema de Kronecker). *Seja  $x = (x_1, x_2, \dots, x_n) \in \mathbb{T}^n$ . As condições seguintes são equivalentes:*



1. A órbita de  $x$  no grupo  $\mathbb{T}^n$  (o conjunto de potências  $x^k$ ,  $k \in \mathbb{Z}$ ) é denso em  $\mathbb{T}^n$ .
2. A  $n + 1$ -upla  $x_1, x_2, \dots, x_n, 1$  é racionalmente independente.

Uma prova elementar é apresentada no Apêndice G. Outra prova, talvez mais transparente (embora não trivial), é baseada sobre a teoria de dualidade de grupos abelianos localmente compactos desenvolvida por Pontryagin e van Kampen (veja, por exemplo, Ch. 7 em [Hofmann e Morris 2013]). Um caráter de um tal grupo,  $G$ , é um homomorfismo contínuo  $\chi: G \rightarrow \mathbb{T}$ . Por exemplo, se  $f: \mathbb{R}^n \rightarrow \mathbb{R}$  é um funcional linear tal que o valor de  $f$  sobre cada elemento do reticulado  $\mathbb{Z}^n$  é inteiro, então a fórmula  $\chi(x \bmod \mathbb{Z}) = \exp(2\pi i f(x))$  define um caráter de  $\mathbb{T}^n$ , e pode-se mostrar, usando os resultados básicos da topologia homotópica, que cada caráter de  $\mathbb{T}^n$  é desta forma. O funcional linear  $f$  é necessariamente da forma  $f(x) = \langle x, v \rangle$  para um vetor  $v \in \mathbb{Z}^n$ .

Um dos resultados de base da teoria de Pontryagin e van Kampen diz que se  $H$  é um subgrupo fechado de um grupo abeliano localmente compacto  $G$  e  $x \in G \setminus H$ , então existe um caráter  $\chi$  de  $G$  tal que  $\chi|_H \equiv e$ , e  $\chi(x) \neq e$ . A condição (1) equivale à propriedade de que o menor subgrupo fechado que contém  $x$  é igual a  $\mathbb{T}^n$ , ou seja, de que cada caráter  $\chi$  tal que  $\chi(x) = e$ , é trivial. De maneira equivalente, se  $z \in \mathbb{Z}^n$  e  $\langle z, x \rangle = 0$ , então  $z = 0$ . Mas isso é a condição (2).

### A rede auxiliar

Como um passo intermediário, consideremos uma rede  $\mathcal{N}$  com uma só unidade de computação, cuja função de modelagem é da forma  $f^w(x) = \cos(wx)$ , e a função de ativação é a função de Heaviside usual,  $\eta$ . A rede  $\mathcal{N}$  é binária, com valores de entrada reais e um parâmetro,  $w$ , que toma os valores reais (de fato, inteiros).

**Lema 2.3.29.** *A rede  $\mathcal{N}$  fragmenta cada  $n$ -upla de reais  $(x_1, \dots, x_n)$  tal que*

$$(x_1, \dots, x_n, 1)$$

*são racionalmente independentes.*

*Demonstração.* Denotemos  $y_i = \exp(2\pi i x_i) \in \mathbb{T}$ . Seja  $I \subseteq [n]$ . O lema de Kronecker implica que existe um valor do parâmetro  $w \in \mathbb{Z}$  tal que para todo  $i \in I$  a parte real de  $f^w(y_i)$  é positiva, e para todo  $i \in [n] \setminus I$  a parte real de  $f^w(y_i)$  é estritamente negativa. Concluímos: o valor de saída da nossa rede é igual a 1 para  $x_i$ ,  $i \in I$ , e é igual a 0, para  $x_i$ ,  $i \notin I$ .  $\square$

É claro que essa rede não é sigmóide, mas isto é fácil a contornar.

### Um jeitinho

A idéia de Sontag foi de esconder a função  $\cos x$  dentro uma função sigmóide, adicionando um fator de cosseno,  $a \cos x$ , com o coeficiente  $a$  variável tão pequeno que a adição

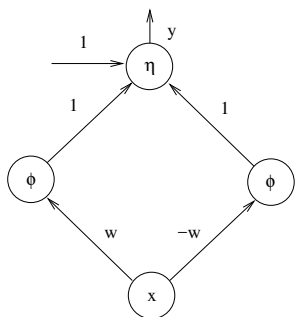
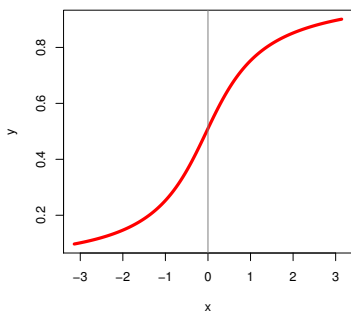


Figura 2.10: Arquitetura da rede de Sontag

Figura 2.11: O sigmóide de ativação  $\phi$  com  $\alpha = 100$

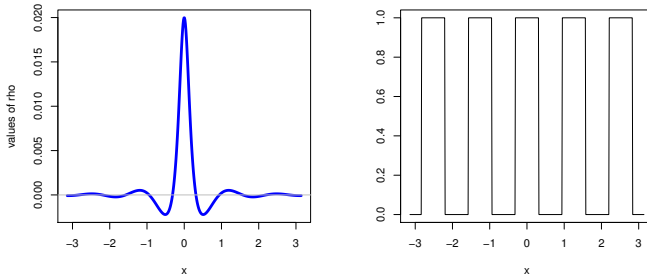


Figura 2.12: A função  $\rho$  com  $\alpha = 100$  e  $w = 5$  (a esq.) e a função binária de saída correspondente (a dir.)

visivelmente tem efeito nenhum sobre a forma de uma função padrão, como  $\frac{1}{\pi} \arctan x + \frac{1}{2}$ . Depois, a gente pode se livrar de arctan facilmente.

A função sigmóide de ativação é da forma

$$\phi(x) = \frac{1}{\pi} \arctan x + \frac{\cos x}{\alpha(1+x^2)} + \frac{1}{2},$$

onde  $\alpha \gg 2\pi$  é fixo, por exemplo,  $\alpha = 100$ . O perceptron da camada de saída tem dois pesos de entrada iguais a um, e o valor limiar, um. A rede gera a função binária

$$y = \eta[\rho(x)],$$

onde

$$\rho(x) = \frac{2 \cos wx}{\alpha(1+w^2x^2)}.$$

Os valores de entrada são reais.

Como o sinal da função  $\rho(x)$  é igual ao sinal de  $\cos wx$ , as duas redes geram a mesma função binária e tem as mesmas propriedades de fragmentação.

Por conseguinte, a rede de Sontag tem dimensão VC infinita. De fato, as suas propriedades de fragmentação são muito mais fortes. Como a dimensão do  $\mathbb{R}$  como um espaço vetorial racional é a igual à cardinalidade de contínuo,  $\dim_{\mathbb{Q}} \mathbb{R} = c$ , existe um conjunto  $X \subseteq \mathbb{R}$  racionalmente independente da mesma cardinalidade que  $\mathbb{R}$ . A rede de Sontag fragmenta todo subconjunto finito de  $X$ .

(Mesmo melhor, pode-se provar que para todo  $n$ , o conjunto de  $n$ -uplas que são racionalmente dependentes tem a medida de Lebesgue nula, então a rede de Sontag fragmenta quase todos conjuntos finitos de reais....)

## 2.4 Dimensão sensível à escala (fat-shattering dimension)

Seja  $\mathcal{F}$  uma *classe de funções*, ou seja, uma família de funções sobre  $\Omega$  tomando valores reais (tipicamente, num intervalo da reta, por exemplo,  $[0, 1]$ ). Qual é a versão correta da dimensão VC para as funções que não são necessariamente binárias? Tem várias, por exemplo, a seguinte.

**Definição 2.4.1.** Seja  $\mathcal{F}$  uma classe de funções reais sobre um conjunto  $\Omega$ . Um subconjunto  $\sigma \subseteq \Omega$  é *pseudofragmentado* (*pseudoshattered*) por  $\mathcal{F}$  se existe uma função  $g: \sigma \rightarrow \mathbb{R}$  tal que, qualquer seja  $I \subseteq \sigma$ , existe uma função  $f_I \in \mathcal{F}$  satisfazendo as condições

$$\begin{aligned} \forall x \in I, \quad f_I(x) &\geq g(x), \\ \forall x \notin I, \quad f_I(x) &< g(x). \end{aligned} \tag{2.5}$$

A *pseudodimensão*, ou *P-dimensão*, de  $\mathcal{F}$ , denotada  $\text{P-dim}(\mathcal{F})$ , é o supremo de cardinalidades de subconjuntos finitos  $\sigma$  de  $\Omega$  pseudofragmentados por  $\mathcal{F}$ .

**Exercício 2.4.2.** Mostrar que a pseudodimensão de  $\mathcal{F}$  é igual a dimensão VC da família de todos os *subgráficos* de funções  $f \in \mathcal{F}$ , ou seja, os conjuntos

$$S_f = \{(x, y) \in \Omega \times \mathbb{R} : f(x) \leq y\}.$$

**Exercício 2.4.3.** Mostrar que se  $\mathcal{F}$  consiste de funções binárias, então  $\text{P-dim}(\mathcal{F}) = \text{VC-dim}(\mathcal{F})$ .

**Exercício 2.4.4.** Seja  $\Omega = \mathbb{R}^d$ , e seja  $\mathcal{F}$  a classe de todas as funções distância de pontos  $x_0 \in \mathbb{R}^n$ ,

$$\mathcal{F} = \{d_{x_0} : x_0 \in \mathbb{R}^d\},$$

onde

$$d_{x_0}(x) = \|x - x_0\|_2.$$

Mostrar que

$$\text{P-dim}(\mathcal{F}) = d + 1.$$

De fato, a noção de *P-dimensão* não é completamente satisfatória. A noção seguinte é mais fina. A *fat-shattering dimension*,  $\text{fat}_\epsilon$ , na verdade não toma um valor único, mas melhor uma coleção de valores às escalas  $\epsilon > 0$  diferentes.

**Definição 2.4.5.** Seja  $\mathcal{F}$  uma classe de funções reais sobre um conjunto  $\Omega$ . Dado um  $\epsilon > 0$ , digamos que o subconjunto  $\sigma \subseteq \Omega$  é  *$\epsilon$ -fragmentado* por  $\mathcal{F}$  se existe uma função

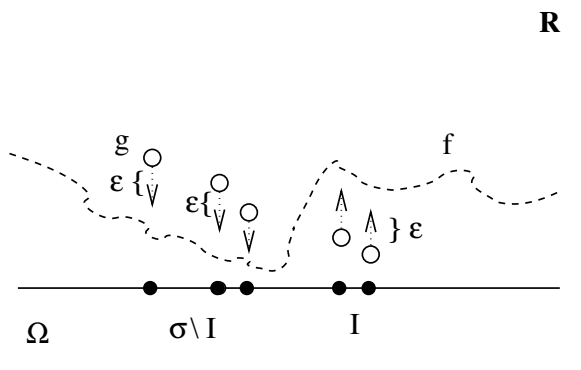


Figura 2.13:  $\epsilon$ -fragmentação.

$g : \sigma \rightarrow \mathbb{R}$  (*testemunha de fragmentação*) tal que, qualquer que seja  $I \subseteq \sigma$ , existe uma função  $f_I \in \mathcal{F}$  satisfazendo as condições

$$\begin{aligned} \forall x \in I, \quad f_I(x) &> g(x) + \epsilon, \\ \forall x \notin I, \quad f_I(x) &< g(x) - \epsilon. \end{aligned} \tag{2.6}$$

A *dimensão  $\epsilon$ -fragmentando* de  $\mathcal{F}$  ( *$\epsilon$ -fat shattering dimension*, em inglês), denotada  $\text{fat}_\epsilon(\mathcal{F})$ , é o supremo de cardinalidades de todos os subconjuntos finitos de  $\Omega$  que são  $\epsilon$ -fragmentados por  $\mathcal{F}$ .

Mais uma vez, não é difícil de verificar que se  $\mathcal{F}$  consiste de funções binárias e  $\epsilon > 0$  é bastante pequeno (por exemplo,  $\epsilon \leq \frac{1}{2}$ ), então  $\text{fat}_\epsilon(\mathcal{F})$  é a dimensão VC de  $\mathcal{F}$ .

**Exercício 2.4.6.** Para todo  $\epsilon > 0$ ,

$$\text{fat}_\epsilon(\mathcal{F}) \leq \text{P-dim}(\mathcal{F}).$$

Se  $0 < \epsilon < \gamma$ , então

$$\text{fat}_\epsilon(\mathcal{F}) \leq \text{fat}_\gamma(\mathcal{F}).$$

**Exercício 2.4.7.**

$$\text{P-dim}(\mathcal{F}) = \sup_{\epsilon > 0} \text{fat}_\epsilon(\mathcal{F}).$$

Não teremos muita chance de trabalhar com essa noção em detalhes. Para mais sobre a dimensão *fat-shattering* pedimos-lhe que consulte [Alon, Ben-David et al. 1997].

# 3

## Aprendizagem PAC

---

Neste capítulo introduziremos algumas noções básicas tais que uma regra de aprendizagem, a aprendizagem PAC (Provavelmente Aproximadamente Correta), e uma classe aprendizável, ilustrando-as no quadro de aprendizagem dentro uma classe sob a distribuição fixa.

O cenário geral da aprendizagem supervisionada é o seguinte. Há um domínio  $\Omega$ , e um conceito desconhecido,  $C \subseteq \Omega$  (ou: um classificador binário desconhecido,  $\chi_C$ ). Este  $C$  é a ser aprendido numa sequência de experiências. Sobre cada amostra finita  $x_1, x_2, \dots, x_n$  de pontos de  $\Omega$ , o conceito  $C$  induz uma rotulagem,  $\epsilon_1 = \chi_C(x_1)$ ,  $\epsilon_2 = \chi_C(x_2)$ ,  $\dots$ ,  $\epsilon_n = \chi_C(x_n)$ . Somos mostrados a amostra rotulada

$$(x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n)$$

e, com base nesta amostra, temos que adivinhar o conceito  $C$ , sugerindo uma *hipótese*,  $H \subseteq \Omega$ .

A bondade da nossa hipótese  $H$  é avaliada através do *erro de generalização*, ou seja, a probabilidade do evento que o rótulo de um ponto qualquer,  $x$ , do domínio seja adivinhado incorretamente:

$$\chi_H(x) \neq \chi_C(x).$$

Isso torna inevitável um contexto probabilístico. Para dar o significado a uma expressão do tipo

$$P[\chi_H(x) \neq \chi_C(x)],$$

o valor aleatório,  $x$ , deve ser modelado por uma *variável aleatória* com valores em  $\Omega$ , de costume denotada por uma letra maiúscula,  $X$ . O significado disso é que não somente  $X_i$  é uma variável (elemento desconhecido) do domínio, mas, além disso, dado um subconjunto  $A$  do domínio, sabe-se a probabilidade do valor de  $X$  pertencer a  $A$ :

$$P[X \in A] = \mu(A),$$

onde  $\mu$  é uma medida de probabilidade sobre o domínio, chamada a *lei* de  $X$ . Assim, uma variável aleatória é uma versão “melhorada” de uma variável usual.

Vamos introduzir este contexto começando com duas situações particularmente transparentes, de fato quase triviais, onde tudo corre bem e pode ser perfeitamente entendido: aprendizagem sob uma medida atômica, e aprendizagem de uma classe de conceitos finita.

## 3.1 Aprendizagem sob a distribuição puramente atômica

### 3.1.1 Aprendizagem num domínio finito

Para começar, suponha que  $\Omega = (\Omega, \mu)$  seja um espaço probabilístico finito:

$$\Omega = \{a_1, a_2, \dots, a_k\},$$

onde a medida de probabilidade  $\mu$  é determinada pelos pesos,  $p_1, p_2, \dots, p_k$ , de todos os pontos, de modo que, qualquer que seja  $A \subseteq \Omega$ ,

$$\mu(A) = \sum_{a_i \in A} p_i.$$

Particularmente,

$$\mu\{a_i\} = p_i.$$

Desse modo, a probabilidade de que a variável aleatória  $X_i$  toma valor  $a_j$ , é dada por

$$P[X_i = a_j] = \mu\{a_j\} = p_j.$$

Segundo o paradigma de aprendizagem, os dados (amostras não-rotuladas) são modelados por uma sequência infinita  $X_1, X_2, \dots, X_n, \dots$  de elementos aleatórios de  $\Omega$ , independentes e identicamente distribuídos, com a lei comum  $\mu$ . Então, dado um conjunto  $A \subseteq \Omega$ , temos para todo  $i$ ,

$$P[X_i \in A] = \mu(A),$$

enquanto a independência significa que, dado pontos quaisquer  $a_{i_1}, a_{i_2}, \dots, a_{i_m}$ , temos

$$\begin{aligned} P[X_1 = a_{i_1}, X_2 = a_{i_2}, \dots, X_m = a_{i_m}] &= P[X_1 = a_{i_1}]P[X_2 = a_{i_2}] \dots P[X_m = a_{i_m}] \\ &= p_{i_1} p_{i_2} \dots p_{i_m}. \end{aligned}$$

De modo equivalente (exercício), mesmo se formalmente mais geral, quaisquer que sejam conjuntos  $A_{i_1}, A_{i_2}, \dots, A_{i_m} \subseteq \Omega$ ,

$$P[X_1 \in A_{i_1}, X_2 \in A_{i_2}, \dots, X_m \in A_{i_m}] = P[X_1 \in A_{i_1}] \cdot P[X_2 \in A_{i_2}] \cdot \dots \cdot P[X_m \in A_{i_m}].$$

(Para uma discussão da noção de uma variável aleatória num contexto mais geral, consulte Apendice A, seguido pelos Apêndices D, E, e H.)

Seja  $C \subseteq \Omega$  um conceito desconhecido. Dada uma amostra aleatória  $(X_1, X_2, \dots, X_n)$  (ou seja, uma coleção finita de variáveis i.i.d. seguindo a lei  $\mu$ ), o conceito  $C$  induz sobre a amostra uma rotulagem, isto é, a sequência de rótulos  $Y_1, Y_2, \dots, Y_n$ :

$$Y_i = \chi_C(X_i), \quad i = 1, 2, \dots, n.$$

Cada rótulo é uma composição de uma variável aleatória,  $X_i$ , com uma função determinística,  $\chi_C$ , e desse modo,  $Y_i$  é uma variável aleatória também. A lei de  $Y_i$  é a imagem direita,  $\chi_{C*}(\mu)$ , da lei  $\mu$  de  $X_i$  sob a aplicação  $\chi_C$ :

$$\begin{aligned} P[Y_i = 1] &= P[X_i \in C] \\ &= \mu(C) \\ &= \chi_{C*}(\mu)(\{1\}), \\ P[Y_i = 0] &= 1 - \mu(C). \end{aligned}$$

**Exercício 3.1.1.** Verificar que as variáveis  $Y_1, Y_2, \dots, Y_n$  são i.i.d.

A observação-chave que permite adivinhar  $C$  é a seguinte: se o tamanho  $n$  de amostra é bastante grande, então, com alta probabilidade, cada ponto de nosso domínio finito vai aparecer pelo menos uma vez entre os pontos da amostra, assim determinando  $C$  completamente.

**fato 3.1.2.** *Seja  $a \in \Omega$ , com  $P[X = a] = \eta$ . Então, a probabilidade que nenhuma de v.a. i.i.d.  $X_1, X_2, \dots, X_n$  toma o valor  $a$  é igual a  $(1 - \eta)^n$ .*

*Demonstração.* Para cada  $i = 1, 2, \dots, n$ ,

$$P[X_i \neq a] = \mu(\Omega \setminus \{a\}) = 1 - \eta,$$

e como as variáveis  $X_i$  são independentes,

$$P[X_1 \neq a, X_2 \neq a, \dots, X_n \neq a] = (1 - \eta)^n.$$

□

**fato 3.1.3.** *Seja*

$$\eta = \min_{i=1}^k p_i.$$

*A probabilidade que existe  $a \in \Omega$  tal que  $X_i \neq a$  para todos  $i$  é limitada acima pelo valor  $k(1 - \eta)^n$ .*



*Demonstração.* O evento “existe  $a \in \Omega$  tal que  $X_i \neq a$  para todos  $i$ ” corresponde, ao nível conjuntístico, ao subconjunto de todas as seqüências  $(x_1, x_2, \dots, x_n) \in \Omega^n$  quem não contém um dos elementos de  $\Omega$ . Isso pode se escrever assim:

$$\bigcup_{j=1}^k \{x \in \Omega^n : \forall i, x_i \neq a_j\}.$$

A probabilidade neste contexto corresponde à medida de produto,  $\mu^{\otimes n}$ , determinada por

$$\mu^{\otimes n} \{x_1, x_2, \dots, x_k\} = \mu\{x_1\} \mu\{x_2\} \dots \mu\{x_k\}.$$

A medida de união de  $k$  conjuntos não excede  $k$  vezes a medida do maior entre eles, como estimado no fato 3.1.2.  $\square$

Agora denotemos

$$\begin{aligned} \text{supp } \mu &= \{a \in \Omega : \mu\{a\} > 0\} \\ &= \{a_j : p_j > 0, j = 1, 2, \dots, k\} \end{aligned}$$

o *suporte* da medida  $\mu$ . O suporte, neste caso, consiste de todos os átomos da medida, ou seja, pontos  $a$  satisfazendo  $\mu\{a\} > 0$ . É claro que a medida do suporte é igual a 1.

**fato 3.1.4.** *Seja  $0 < \delta < 1$  qualquer (o risco). Denotemos*

$$\eta = \min\{p_i : p_i > 0\}$$

o valor do menor átomo. Se

$$n \geq \frac{1}{\eta} \ln \frac{k}{\delta}, \quad (3.1)$$

então, com a probabilidade (a confiança)  $\geq 1 - \delta$ , cada ponto do suporte de  $\mu$  vai aparecer pelo menos uma vez entre os valores tomados pelas variáveis aleatórias i.i.d.  $X_1, X_2, \dots, X_n \sim \mu$ .

*Demonstração.* Segundo fato 3.1.3, bastaria que o valor de  $n$  satisfaça

$$k(1 - \eta)^n \leq \delta.$$

Tomando o logaritmo, obtemos

$$\log k + n \log(1 - \eta) \leq \log \delta,$$

ou seja (como  $\log(1 - \eta) < 0$ ),

$$n \geq \log \frac{\delta}{k} \cdot \frac{1}{\log(1 - \eta)} = \log \frac{k}{\delta} \cdot \frac{1}{-\log(1 - \eta)}.$$

De acordo com lema 2.3.23, substituindo os valores  $\alpha = 1$  e  $x = 1 - \eta$ , temos

$$\log(1 - \eta) \leq -\eta,$$

de onde

$$\frac{1}{-\log(1 - \eta)} \leq \frac{1}{\eta},$$

concluindo o argumento. □

Concluimos: dado um valor  $\delta > 0$  de risco qualquer, desde que  $n$  seja bastante grande (como dado pela Eq. 3.1), com confiança  $\geq 1 - \delta$ , temos o conhecimento completo de rótulos de todos os pontos de  $\Omega$ . A hipótese  $H$  pode consistir de todos os pontos do domínio que aparecem na amostra  $x_1, x_2, \dots, x_n$  e têm o rótulo 1:

$$\begin{aligned} H &= \{a \in \Omega : \exists i, x_i = a \text{ e } \epsilon_i = 1\} \\ &= \{x_i : \epsilon_i = 1, i = 1, 2, \dots, n\}. \end{aligned}$$

Note que nesta fórmula (*regra de aprendizagem*) as variáveis são notadas pelas letras minúsculas, pois elas são elementos do domínio, não importa a lei de distribuição. A regra de distribuição não pode depender de uma lei subjacente (que é sempre desconhecida).

Com a confiança  $\geq 1 - \delta$ , temos

$$H \cap \text{supp } \mu = C \cap \text{supp } \mu.$$

Por conseguinte, a diferença simétrica  $H \Delta C$  é um subconjunto de  $\Omega \setminus \text{supp } \mu$ , que tem medida nula. Nesse caso, o erro de generalização da nossa hipótese é zero:

$$P[\chi_C(X) \neq \chi_H(X)] = \mu(H \Delta C) = 0.$$

A estimativa não depende de  $C$ . Podemos concluir:

**Proposição 3.1.5.** *Seja  $\Omega$  um espaço probabilístico finito, e seja  $\eta > 0$  a medida do menor átomo de  $\Omega$ . Dado um risco  $\delta > 0$ , se*

$$n \geq \frac{1}{\eta} \ln \frac{k}{\delta},$$

*então, com confiança  $\geq 1 - \delta$ , podemos adivinhar qualquer conceito  $C$  exatamente.*

Nesse caso, trata-se da aprendizagem *provavelmente (exatamente) correta*. A palavra “provavelmente” se aplica à alta confiança para adivinharmos o conceito  $C$  corretamente.

Agora passemos a um caso um pouco mais interessante.

### 3.1.2 Aprendizagem num domínio enumerável

Nesta subseção um *domínio*,  $\Omega$ , pode significar um conjunto qualquer. Seja  $\mu$  uma medida de probabilidade discreta, ou puramente atômica, sobre  $\Omega$ . Isso significa que existe uma sequência (finita ou infinita) de pontos dois-a-dois distintos  $a_j \in \Omega$ ,  $j = 1, 2, 3, \dots$  (átomos de medida  $\mu$ ), com  $\mu\{a_j\} = p_j > 0$ , tal que

$$\sum_{j=1}^{\infty} p_j = 1.$$

Dado  $A \subseteq \Omega$ , definamos o valor da medida de  $A$  por

$$\mu(A) = \sum \{p_j : a_j \in A\} = \sum_{j=1}^{\infty} \chi_A(a_j) p_j = \int_{\Omega} \chi_A d\mu.$$

Segue-se, em particular, que

$$\mu(\Omega \setminus \{a_1, a_2, \dots\}) = 0.$$

Nesse caso, o suporte de  $\mu$  é também o conjunto de todos os átomos. Essencialmente, podemos ignorar o resto de  $\Omega$  e assumir que  $\Omega$  seja enumerável, porque a probabilidade para um ponto aleatório a pertencer ao resto é zero:

$$P[X \notin \{a_1, a_2, \dots\}] = 0.$$

Como antes, os dados são modelados por uma sequência infinita  $X_1, X_2, \dots, X_n, \dots$  de elementos aleatórios de  $\Omega$ , independentes e identicamente distribuídos, com a lei comum  $\mu$ . A independência significa a mesma coisa que no caso de  $\Omega$  finito: dado pontos quaisquer  $a_{i_1}, a_{i_2}, \dots, a_{i_k}$ , temos

$$\begin{aligned} P[X_1 = a_{i_1}, X_2 = a_{i_2}, \dots, X_k = a_{i_k}] &= P[X_1 = a_{i_1}]P[X_2 = a_{i_2}] \dots P[X_k = a_{i_k}] \\ &= p_{i_1} p_{i_2} \dots p_{i_k}. \end{aligned}$$

Esta vez, a observação-chave é a seguinte. Seja  $k \in \mathbb{N}_+$  qualquer. Se esperarmos bastante tempo, então, com alta confiança, todos os pontos  $a_1, a_2, \dots, a_k$  aparecerão entre os pontos da amostra  $x_1, x_2, \dots, x_n$ , desde que  $n$  é bastante grande.

Formalizemos esta ideia. Podemos supor sem perda de generalidade que os átomos  $a_j$  sejam ordenados da tal maneira que

$$p_1 = \mu\{a_1\} \geq p_2 = \mu\{a_2\} \geq \dots \geq p_k = \mu\{a_k\} \geq \dots$$

Usando o mesmo argumento que na prova do fato 3.1.4, concluímos que, dado  $k \geq 1$  e  $\delta > 0$ , se  $n$  é maior ou igual ao valor

$$\frac{1}{p_k} \ln \frac{k}{\delta},$$

então, com confiança  $1 - \delta$ , cada ponto  $a_1, \dots, a_k$  ocorre pelo menos uma vez na sequência gerada aleatoriamente,  $X_1, X_2, \dots, X_n$ .

Se  $\epsilon > 0$ , então existe  $k$  tal que a soma das medidas de  $k$  primeiros átomos é pelo menos  $1 - \epsilon$ , ou seja,

$$\sum_{j=k+1}^{\infty} p_j < \epsilon.$$

Denotemos o menor  $k$  com esta propriedade  $k(\epsilon)$ . Concluimos: se

$$n \geq \frac{1}{p_{k(\epsilon)}} \ln \frac{k}{\delta},$$

então

$$\mu^{\otimes n} \{ \sigma = (x_1, x_2, \dots, x_n) \in \Omega^n : \{a_1, a_2, \dots, a_k\} \subseteq \{x_1, x_2, \dots, x_n\} \} \geq 1 - \delta.$$

Agora mais uma vez passemos a aprendizagem *supervisionada*, que se trata das amostras rotuladas. Esta vez, discutamos o problema em mais detalhes. Queremos aprender um conceito desconhecido,  $C \subseteq \Omega$ , escolhido pelo professor (*teacher*). Uma amostra aleatória não rotulada,  $\sigma = (x_1, x_2, \dots, x_n)$ , é gerada pelo gerador de dados aleatórios, e o professor induz a rotulagem  $C \upharpoonright \sigma = (\epsilon_1, \epsilon_2, \dots, \epsilon_n)$  usando o seu conceito segredo,  $C$ :

$$\epsilon_i = \begin{cases} 1, & \text{se } x_i \in C, \\ 0, & \text{se não.} \end{cases}$$

O professor depois mostra a amostra rotulada

$$(\sigma, C \upharpoonright \sigma) = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n)$$

ao aprendiz (*learner*), que fará o melhor que puder para adivinhar o conceito  $C$ . A sua hipótese,  $H = \mathcal{L}(\sigma, C \upharpoonright \sigma)$ , será enviada ao professor, que estima o erro (o erro de generalização), ou seja, a probabilidade que o rótulo de verdade de um ponto aleatório  $X$  não seja igual ao rótulo predito pelo aprendiz:

$$\begin{aligned} \text{erro}_{\mu, C}(H) &= P[Y \neq H] \\ &= P[\chi_C(X) \neq \chi_H(X)] \\ &= \mu(C \Delta H). \end{aligned}$$

Aqui,

$$C \Delta H = (C \setminus H) \cup (H \setminus C)$$

é a diferença simétrica de  $C$  e  $H$ .

A correspondência

$$(\sigma, C \upharpoonright \sigma) \mapsto H = \mathcal{L}(\sigma, C \upharpoonright \sigma),$$

ou seja, o algoritmo usado pelo aprendiz para escolher suas hipóteses, é a *regra de aprendizagem*. A regra *aprende* o conceito  $C$  (sob a distribuição  $\mu$ ) se, quando o tamanho de dados crescer,  $n \rightarrow \infty$ , o erro converge para zero.

Sem se preocupar com a formalização mais exata destas noções, tentemos definir uma regra que aprende o conceito desconhecido,  $C$ , sob a nossa distribuição discreta,  $\mu$ .

Isso é muito simples! Para cada  $\epsilon > 0$  e  $\delta > 0$ , se o tamanho da amostra,  $n$ , for bastante grande, então, com confiança  $\geq 1 - \delta$ , temos entre os pontos de amostra tantos átomos,  $a_1, a_2, \dots, a_{k(\epsilon)}$ , que a soma de suas medidas é  $> 1 - \epsilon$ . Desta maneira, sabemos as rotulagens da maioria de pontos do domínio (a maioria no sentido da lei,  $\mu$ ). Podemos determinar com alta confiança o conjunto

$$C \cap \{a_1, a_2, \dots, a_{k(\epsilon)}\}.$$

A nossa predição pode consistir, por exemplo, de todos os pontos da amostra  $\sigma$  tendo o rótulo 1:

$$H = \mathcal{L}_n(C \upharpoonright \sigma) = \{x_i : \epsilon_i = 1, i = 1, 2, \dots, n\}.$$

Com confiança  $\geq 1 - \delta$ ,

$$\{a_1, a_2, \dots, a_{k(\epsilon)}\} \subseteq \{x_1, \dots, x_n\},$$

o que implica

$$\mu(C \setminus H) < \epsilon$$

e, como  $H \subseteq C$ , concluímos:

$$\text{erro}_{\mu, C}(H) < \epsilon,$$

com a probabilidade  $\geq 1 - \delta$ . A *complexidade amostral* de uma regra de aprendizagem é o mínimo tamanho da amostra necessário para atingir a confiança  $1 - \delta$  e a precisão  $\epsilon > 0$  exigidos. Então, a regra definida acima aprende  $C$  com a complexidade amostral

$$s(\epsilon, \delta) \leq \frac{1}{p_{k(\epsilon)}} \ln \frac{k}{\delta}.$$

A regra aprende  $C$  *provavelmente aproximadamente corretamente*, onde *provavelmente* refere-se a  $\delta$ , e *aproximadamente*, a  $\epsilon$ .

Vamos fazer duas observações. Note-se que a nossa regra possui uma propriedade mais forte: ela pode aprender todos os conceitos  $C \in 2^{\Omega}$  *simultaneamente*, ou seja:

$$\forall \epsilon > 0 \forall \delta > 0 \text{ se } n \geq s(\epsilon, \delta), \text{ então } P \left[ \forall C \in 2^{\Omega} \text{ erro}_{\mu, C}(\mathcal{L}(C \upharpoonright \sigma)) \leq \epsilon \right] > 1 - \delta.$$

Além disso, em vez dessa regra particular, pode-se usar uma regra qualquer que apenas tem a propriedade que a hipótese  $H$  induz sobre a amostra  $\sigma$  a mesma rotulagem que o conceito  $C$ :

$$\mathcal{L}(C \upharpoonright \sigma) \upharpoonright \sigma = C \upharpoonright \sigma.$$

Uma tal regra chama-se *consistente* (com a classe, no nosso caso  $2^{\Omega}$ ). Pode-se dizer que a classe  $2^{\Omega}$  é *consistentemente aprendizável* sob qualquer medida discreta.

## 3.2 Aprendizagem de classes finitas

Vamos passar agora para o caso mais geral, o de uma distribuição fixa  $\mu$  qualquer, não necessariamente discreta, a fim de investigar a pergunta seguinte: é verdade que existe uma regra de aprendizagem,  $\mathcal{L}$ , que aprende a classe de todos os conceitos (borelianos),  $\mathcal{B}_\Omega$ , sob a distribuição  $\mu$ , de mesmo modo que para  $\mu$  puramente atômica? A resposta é negativa, o que nos motiva a procurar por classes que podem ser aprendidas. Os primeiros exemplos são as classes finitas.

Comecemos com algumas formalizações.

### 3.2.1 Aprendizagem sob uma medida fixa: formalizações

Seja  $\Omega$  um domínio, ou seja, um espaço boreliano padrão (veja o Apêndice D). Uma *regra de aprendizagem* sobre  $\Omega$  é uma aplicação que aceita uma amostra rotulada e gera um subconjunto boreliano de  $\Omega$ , normalmente chamado uma *hipótese*,

$$\mathcal{L}: \bigcup_{n=1}^{\infty} \Omega^n \times \{0, 1\}^n \rightarrow \mathcal{B}_\Omega.$$

É mais conveniente tratar  $\mathcal{L}$  como uma família de aplicações,  $\mathcal{L} = (\mathcal{L}_n)_{n=1}^{\infty}$ , uma para cada nível  $n = 1, 2, 3, \dots$ :

$$\mathcal{L}_n: \Omega^n \times \{0, 1\}^n \rightarrow \mathcal{B}_\Omega.$$

A maneira alternativa de representar a regra de aprendizagem é como uma função que aceita uma amostra rotulada  $\sigma = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n) \in \Omega^n \times \{0, 1\}^n$ , bem como um ponto  $x \in \Omega$ , e produz um rótulo, 0 ou 1, para  $x$  baseado sobre as informações dadas por  $\sigma$ :

$$\mathcal{L}_n: \Omega^n \times \{0, 1\}^n \times \Omega \rightarrow \{0, 1\}.$$

Nesta interpretação, para dar sentido às expressões tipo  $P[\mathcal{L}_n = \chi_C]$ , as funções  $\mathcal{L}_n$  devem ser borelianas.

Seja  $C \subseteq \Omega$  um conceito, ou seja, um subconjunto boreliano de  $\Omega$ . Dada uma amostra não rotulada,  $\sigma \in \Omega^n$ , o conceito  $C$  induz uma rotulagem,  $C \upharpoonright \sigma$ . A regra  $\mathcal{L}$  associa com a amostra rotulada  $(\sigma, C \upharpoonright \sigma)$  uma hipótese,  $H = \mathcal{L}_n(\sigma, C \upharpoonright \sigma)$ . Para facilitar, vamos escrever  $H = \mathcal{L}_n(C \upharpoonright \sigma)$ .

Agora suponha que o domínio seja munido de uma distribuição, ou seja, uma medida de probabilidade boreliana qualquer,  $\mu$  (Apêndice E). Para cada hipótese  $H \in \mathcal{B}_\Omega$ , pode-se calcular o *erro de generalização* (com relação ao conceito  $C$  e a medida  $\mu$ ):

$$\text{erro}_{\mu, C}(H) = \mu(H \Delta C) = P[\chi_H(X) \neq \chi_C(X)] = \mathbb{E}(|\chi_H - \chi_C|) = \|\chi_H - \chi_C\|_{L^1(\mu)}.$$

Em particular, chegamos ao *erro de generalização* da regra  $\mathcal{L}$  (ao nível  $n$ ):

$$\text{erro}_{\mu, C} \mathcal{L}_n(C \upharpoonright \sigma).$$

Este erro é em si uma variável aleatória, uma composição da amostra aleatória<sup>1</sup>  $\sigma = (X_1, X_2, \dots, X_n)$  com três aplicações determinísticas: a de rotulagem,

$\Omega^n \ni \sigma \mapsto (\sigma, C \upharpoonright \sigma) = (x_1, x_2, \dots, x_n, \chi_C(x_1), \chi_C(x_2), \dots, \chi_C(x_n)) \in \Omega^n \times \{0, 1\}^n$ ,  
a da regra de aprendizagem,

$$\Omega^n \times \{0, 1\}^n \ni (\sigma, C \upharpoonright \sigma) \mapsto H = \mathcal{L}(\sigma, C \upharpoonright \sigma) \in \mathcal{B}_\Omega,$$

e afinal, a de erro de generalização:

$$\mathcal{B}_\Omega \ni H \mapsto \text{erro}_{\mu, C}(H) \in \mathbb{R}.$$

Pode-se escrever assim:

$$\text{erro}_{\mu, C}(\mathcal{L}((X_1, X_2, \dots, X_n), C \upharpoonright (X_1, X_2, \dots, X_n))).$$

A esperança desta v.a. é o erro médio de generalização da regra  $\mathcal{L}_n$ :

$$\begin{aligned} \text{erro}_{\mu, C}(\mathcal{L}_n) &= \mathbb{E}(\text{erro}_{\mu, C}(\mathcal{L}((X_1, X_2, \dots, X_n), C \upharpoonright (X_1, X_2, \dots, X_n)))) \\ &= \mathbb{E}(\mu(C \Delta \mathcal{L}((X_1, X_2, \dots, X_n, \chi_C(X_1), \chi_C(X_2), \dots, \chi_C(X_n)))))) \\ &= \mathbb{E}(P[\chi_C(X) \neq \mathcal{L}((X_1, X_2, \dots, X_n), \chi_C(X_1), \chi_C(X_2), \dots, \chi_C(X_n))(X))]). \end{aligned}$$

Usualmente, escrevemos a última expressão assim:

$$\mathbb{E}_{\sigma \sim \mu^{\otimes n}}(P_{X \sim \mu}[\chi_C(X) \neq \mathcal{L}(C \upharpoonright \sigma)(X)]),$$

ou, por um ligeiro abuso de notação,

$$\mathbb{E}_{\sigma \sim \mu}(P_{X \sim \mu}[\chi_C(X) \neq \mathcal{L}(C \upharpoonright \sigma)(X)]).$$

Agora podemos formular algumas definições exatas.

**Definição 3.2.1.** A regra  $\mathcal{L}$  aprende o conceito  $C$  sob a distribuição  $\mu$  *provavelmente aproximadamente corretamente* (*probably approximately correctly*, PAC) se

$$\text{erro}_{\mu, C}(\mathcal{L}_n) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Da maneira equivalente: a sequência de v.a. reais  $\text{erro}_{\mu, C}(\mathcal{L}_n(C \upharpoonright \sigma))$ ,  $n = 1, 2, 3, \dots$ , converge para zero em probabilidade:

$$\forall \epsilon > 0, \forall \delta > 0, \exists s = s(\epsilon, \delta), \forall n \geq s, P[\text{erro}_{\mu, C}(\mathcal{L}_n(C \upharpoonright \sigma)) > \epsilon] \leq \delta.$$

[ O que é denotado

$$\text{erro}_{\mu, C}(\mathcal{L}_n(C \upharpoonright \sigma)) \xrightarrow{P} 0 ].$$

<sup>1</sup>Uma advertência: o símbolo  $\sigma$ , nesta área de conhecimento, pode denotar uma amostra aleatória,  $\sigma = (X_1, X_2, \dots, X_n)$ , bem como uma amostra determinística,  $\sigma = (x_1, x_2, \dots, x_n)$ , ou seja, um elemento do conjunto  $\Omega^n$ . De mesmo, para as amostras rotuladas. As vezes, vamos usar  $W$  quando for necessário de distinguir entre as duas.

**Exercício 3.2.2.** Mostrar a equivalência de duas noções acima.

[ *Sugestão:* ela é verdadeira para uma sequência qualquer de v.a. reais que tomam seus valores num intervalo, neste caso, o intervalo  $[0, 1]$ . ]

**Definição 3.2.3.** Seja  $\mathcal{C}$  uma classe de conceitos, ou seja, uma família de conjuntos borelianos  $\mathcal{C} \subseteq \mathcal{B}_\Omega$ . A regra  $\mathcal{L}$  aprende a classe  $\mathcal{C}$  sob a distribuição  $\mu$  *provavelmente aproximadamente corretamente* se

$$\sup_{C \in \mathcal{C}} \text{erro}_{\mu, C}(\mathcal{L}_n) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

De maneira equivalente: dado  $\varepsilon > 0$  (*precisão*) e  $\delta > 0$  (*risco*), existe o valor  $s = s(\varepsilon, \delta)$  (a *complexidade amostral*) tal que, se  $n \geq s(\varepsilon, \delta)$ , então, qualquer que seja  $C \in \mathcal{C}$ ,

$$\mu^{\otimes n} \{ \sigma \in \Omega^n : \text{erro}_{\mu, C} \mathcal{L}_n(C \upharpoonright \sigma) > \varepsilon \} \leq \delta.$$

**Definição 3.2.4.** Diz-se que uma classe de conceitos  $\mathcal{C}$  é *aprendizável* (ou: *PAC aprendizável*) sob a medida  $\mu$  se existe uma regra de aprendizagem,  $\mathcal{L}$ , que aprende a classe  $\mathcal{C}$  sob a distribuição  $\mu$ .

*Observação 3.2.5.* O modelo de aprendizagem provavelmente aproximadamente correta foi sugerido em [Valiant 1984]. A noção é particularmente importante no contexto da aprendizagem independente da medida (seção 4.4).

### 3.2.2 Propriedade geométrica de uma classe $\mathcal{C}$ aprendizável

Vamos examinar a pergunta seguinte, que fica no coração do assunto. Seja  $\mathcal{C}$  é uma classe de conceitos num domínio  $\Omega$  munido de uma lei,  $\mu$ . Suponhamos que existe uma regra  $\mathcal{L}$  que aprende  $\mathcal{C}$  provavelmente aproximadamente corretamente. Vamos notar uma propriedade geométrica de  $\mathcal{C}$  que segue desta suposição.

**Exercício 3.2.6.** Verificar que a função de dois argumentos,  $\mu(C \Delta C')$ , é uma *pseudométrica*, ou seja, satisfaz  $\mu(C \Delta C) = 0$ , é simétrica, e satisfaz a desigualdade triangular. De fato, este valor é igual à distância  $L^1$  entre as funções indicadoras de conjuntos  $C$  e  $C'$ :

$$\lambda(C, C') = \int_0^1 |\chi_C - \chi_{C'}| d\lambda(x) = \|\chi_C - \chi_{C'}\|_1.$$

Sejam  $0 < \varepsilon, \delta < 1$  quaisquer. Seja  $C_1, C_2, \dots, C_k$  um subconjunto finito de  $\mathcal{C}$  de elementos à distância dois a dois  $\geq 2\varepsilon$ . Seja  $n \geq s(\varepsilon, \delta)$ . Para cada  $i = 1, 2, \dots, k$ , denotemos

$$A_i = \{ \sigma \in \Omega^n : \mu(C_i, \mathcal{L}(C_i \upharpoonright \sigma)) > \varepsilon \}.$$



Definamos a função  $f: \Omega^n \rightarrow \mathbb{N}$  por  $f = \sum_{i=1}^k \chi_{A_i}$ . Como  $\mu^{\otimes n}(A_i) \leq \delta$ , temos  $\int_{\Omega} f d\mu^{\otimes n} \leq k\delta$ , logo existe pelo menos uma amostra  $\sigma$  tal que

$$\#\{i: \sigma \in A_i\} \leq k\delta.$$

Para o subconjunto complementar  $I = [k] \setminus J$  com  $> (1 - \delta)k$  índices, temos

$$i \in I \Rightarrow \mu(C_i, \mathcal{L}(C_i \upharpoonright \sigma)) \leq \varepsilon.$$

Graças a nossa escolha de conceitos  $C_i$ , concluímos que, se  $i, j \in I$  e  $i \neq j$ , então

$$\mu(\mathcal{L}(C_i \upharpoonright \sigma) \Delta \mathcal{L}(C_j \upharpoonright \sigma)) > 0,$$

em particular,

$$\mathcal{L}(C_i \upharpoonright \sigma) \neq \mathcal{L}(C_j \upharpoonright \sigma).$$

Mas isso significa que os inputs da regra  $\mathcal{L}$ ,  $C_i \upharpoonright \sigma$  e  $C_j \upharpoonright \sigma$ , são diferentes. Em outras palavras, o cubo de Hamming  $\{0, 1\}^n$  de todas as rotulagens da amostra  $\sigma$  com  $n$  elementos admite uma injeção  $[[k(1 - \delta)]] \rightarrow 2^n$ . Concluímos:  $k(1 - \delta) \leq 2^n$ , ou seja,  $\log_2 k + \log_2(1 - \delta) \leq n$ . Em particular, quando  $\delta \leq 1/2$ ,  $\log_2(1 - \delta) \geq -1$ , e quando  $\delta < 1/k$ , pode-se ver que  $n \geq \log_2 k$ .

Resumamos as observações acima.

**Lema 3.2.7.** *Seja  $\mathcal{C}$  uma classe de conceitos PAC aprendizável sob uma medida  $\mu$ . Então, para cada  $\epsilon > 0$ , as cardinalidades de sub-famílias de  $\mathcal{C}$  de conjuntos  $2\epsilon$ -discretas (isto é, dois a dois à distância  $L^1 > 2\epsilon$ ) são limitadas por acima por  $2^{s(\epsilon, \delta)+1}$ , quando  $\delta \leq 1/2$ .*

Isto significa, em particular, que  $\mathcal{C}$  é *precompacto* (ou: *totalmente limitado*) com relação à distância  $L^1$  (veja a subseção C.3.10). A observação seguinte é imediata.

**fato 3.2.8.** *Suponha que a classe  $\mathcal{C}$  contém uma sequência infinita de conceitos  $C_1, C_2, \dots, C_k, \dots$ , dois a dois a distância  $> \epsilon > 0$  com relação à métrica  $L^1(\mu)$ . Então  $\mathcal{C}$  não é PAC aprendizável sobre  $\mu$ .*

**Exemplo 3.2.9.** Existe uma família de subconjuntos borelianos do intervalo que é infinita e  $1/2$ -discreta. É a família de conjuntos de *Rademacher*, construídos recursivamente assim:

$$\begin{aligned} R_1 &= [0, 1], \\ R_2 &= [0, 1/2], \\ R_3 &= [0, 1/4] \cup [1/2, 3/4], \\ R_4 &= [0, 1/8] \cup [1/4, 3/8] \cup [1/2, 5/8] \cup [3/4, 7/8], \\ &\dots \\ &\dots \\ R_n &= \bigcup_{i=0}^{2^{n-1}-1} [2^{-n+1}i, 2^{-n+1}i + 2^{-n}], \\ &\dots \end{aligned}$$

É fácil a verificar a propriedade desejada: se  $n \neq m$ , então  $\lambda(R_n \Delta R_m) = 1/2$ . Concluímos: a classe de todos os conceitos (borelianos),  $\mathcal{B}_\Omega$ , não é aprendizável sob a medida uniforme no intervalo  $[0, 1]$ .

**Exercício 3.2.10.** Mostre que a mesma conclusão vale para qualquer medida  $\mu$  sobre um espaço boreliano padrão que tem uma parte não atômica.

[ *Sugestão:* use o teorema E.2.1 para reduzir este caso ao caso acima. ]

Agora, duas perguntas merecem a ser investigadas: quando uma dada classe de conceitos,  $\mathcal{C}$ , for PAC aprendizável sob uma medida qualquer  $\mu$ , e quando  $\mathcal{C}$  for consistentemente aprendizável sob  $\mu$ .

Em breve, vamos apresentar uma solução completa do primeiro problema dada pelo teorema de Benedek e Itai. Por enquanto, vamos provar que todas as classes finitas são PAC aprendizáveis.

### 3.2.3 Uma forma mais geral da lei geométrica dos grandes números

No primeiro capítulo mostramos o resultado seguinte (corolário 1.4.5). Seja  $f: \Sigma^n \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua em relação a distância de Hamming normalizada. Então para todo  $\epsilon > 0$

$$\mu_{\#}\{x: |f(x) - \mathbb{E}(f)| \geq \epsilon\} \leq 2e^{-2\epsilon^2 n}.$$

O cubo de Hamming  $\Sigma^n$ , como espaço probabilístico, é o produto de  $n$  cópias do espaço probabilístico simplíssimo:  $\Omega = \{0, 1\}$ , munido da medida de probabilidade

$$\mu\{0\} = \mu\{1\} = 1/2.$$

Este espaço, o espaço de Bernoulli, modeliza o único lançamento de uma moeda equilibrada. No entanto, não há nenhuma razão matemática para que espaço de Bernoulli não possa ser substituído por um espaço probabilístico padrão qualquer,  $(\Omega, \mu)$ . A demonstração permanece a mesma, com algumas modificações óbvias.

Seja  $(\Omega, \mu)$  um espaço boreliano padrão qualquer, munido de uma medida de probabilidade, e seja  $n \in \mathbb{N}$ . Sobre o produto cartesiano  $\Omega^n$ , definamos a métrica (a distância de Hamming normalizada):

$$\bar{d}(x, y) = \frac{1}{n} \#\{i: x_i \neq y_i\}.$$

Uma advertência: esta métrica, em geral, não gera a estrutura boreliana do produto, e de fato ela não é necessariamente mensurável. Contudo, ela se comporta bem.

**Exercício 3.2.11.** Seja  $B$  um subconjunto mensurável de  $\Omega^n$  com relação à estrutura boreliano produto. Mostrar que para todo  $\epsilon > 0$  a  $\epsilon$ -vizinhança de  $B$  formada usando a métrica  $\bar{d}$  é um conjunto mensurável.

**Teorema 3.2.12** (Lei geométrica dos grandes números). *Seja  $f: (\Omega^n, \bar{d}) \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua mensurável com relação à estrutura boreliana do produto sobre  $\Omega^n$ . Então para todo  $\varepsilon > 0$  temos*

$$\mu^{\otimes n} \{x \in \Omega^n : |f(x) - \mathbb{E}f| \geq \varepsilon\} \leq 2e^{-2\varepsilon^2 n}.$$

□

**Exercício 3.2.13.** Refazer a sequência de resultados no primeiro capítulo resultando em corolário 1.4.5 para obter formalmente o resultado mais geral acima.

O teorema admite a forma equivalente seguinte.

**Teorema 3.2.14.** *Sejam  $X_i, i = 1, 2, 3, \dots$ , elementos aleatórios i.i.d. de um espaço boreliano padrão,  $\Omega$ . Seja  $f: (\Omega^n, \bar{d}) \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua e mensurável com relação a estrutura boreliana de produto sobre  $\Omega^n$ . Então para todo  $\varepsilon > 0$  temos*

$$P [|f(X_1, X_2, \dots, X_n) - \mathbb{E}f| \geq \varepsilon] \leq 2e^{-2\varepsilon^2 n}.$$

□

**Exercício 3.2.15.** Estabelecer a equivalência dos teoremas 3.2.12 e 3.2.14.

### 3.2.4 Medida empírica contra a medida subjacente

Seja  $C$  um conceito, isto é, um subconjunto boreliano de  $\Omega$ . Queremos estimar o valor da medida de  $C$ ,  $\mu(C)$ , usando a amostragem. Dado uma amostra com  $n$  pontos,  $x_1, x_2, \dots, x_n$ , pode-se calcular a fração de pontos dela que pertencem a  $C$ :

$$\mu_n(C) = \frac{1}{n} \#\{i : x_i \in C\} = \frac{1}{n} \sum_{i=1}^n \chi_C(x_i). \quad (3.2)$$

A quantidade  $\mu_n$  é a *medida empírica* suportada em  $\sigma = \{x_1, x_2, \dots, x_n\}$ . Vamos denotá-la  $\mu_\sigma$  ou às vezes  $\mu_n$ . A medida empírica é uma medida de probabilidade em  $\Omega$ , um substituto de  $\mu$  disponível a nós.

A pergunta é, qual é a probabilidade de que  $\mu_n(C)$  estima  $\mu(C)$  razoavelmente bem? Ou seja, dado um erro  $\varepsilon > 0$ , qual é o *risco* de um desvio grande,

$$\mu^{\otimes n} \{\sigma \in \Omega^n : |\mu_\sigma(C) - \mu(C)| > \varepsilon\}?$$

A função

$$\Omega^n \ni \sigma \mapsto \mu_\sigma(C) = \frac{1}{n} \sum_{i=1}^n \chi_C(x_i) \in \mathbb{R}$$

possui as propriedades seguintes:

1.  $\sigma \mapsto \mu_\sigma(C)$  é 1-Lipschitz contínua com relação à métrica de Hamming normalizada  $\bar{d}$  sob  $\Omega^n$ . De fato, se  $\bar{d}(\sigma, \tau) = a$ , então  $an$  coordenadas de  $\sigma$  e  $\tau$  são diferentes, e as duas somas diferem por  $an$  no máximo; depois da normalização, concluímos que  $\mu_\sigma(C)$  e  $\mu_\tau(C)$  diferem por  $\leq a$ .
2. A função é Borel mensurável com relação à estrutura boreliana de produto (exercício).
3. A função satisfaz

$$\mathbb{E}_{\sigma \sim \mu}[\mu_\sigma(C)] = \mu(C).$$

De fato,

$$\begin{aligned} \mathbb{E}_{\sigma \sim \mu}[\mu_\sigma(C)] &= \int_{\Omega^n} \frac{1}{n} \sum_{i=1}^n \chi_C(x_i) d\mu^{\otimes n}(x) \\ &= \frac{1}{n} \sum_{i=1}^n \int_{\Omega} \chi_C(x_i) d\mu(x_i) \\ &= \frac{1}{n} \times n\mu(C) \\ &= \mu(C). \end{aligned}$$

A cota de Chernoff (teorema 3.2.12) implica

$$\mu^{\otimes n} \{x \in \Omega^n : |\mu_n(C) - \mu(C)| \geq \varepsilon\} \leq 2e^{-2\varepsilon^2 n}. \quad (3.3)$$

De mesmo, usando notação probabilística, lê-se

$$P [|\mu_n(C) - \mu(C)| \geq \varepsilon] \leq 2e^{-2\varepsilon^2 n}. \quad (3.4)$$

Aqui, a medida empírica  $\mu_n$  em si é uma variável aleatória com valores no espaço de medidas de probabilidade sobre  $\Omega$ , isso é, uma medida aleatória. Segue-se a fórmula escrita mais cuidadosamente:

$$P \left[ \left| \frac{1}{n} \sum_{i=1}^n \chi_C(X_i) - \mu(C) \right| > \varepsilon \right] < 2e^{-2\varepsilon^2 n}.$$

O sinal de probabilidade refere-se à medida produto  $\mu^{\otimes n}$ .

Agora suponha que ao invés de um conceito, temos uma família finita

$$\mathcal{C} = \{C_1, C_2, \dots, C_k\}.$$

Queremos estimar suas medidas simultaneamente, usando a única amostra aleatória disponível,

$$\sigma = \{x_1, x_2, \dots, x_n\}.$$

Isso pode ser feito, embora com uma confiança um pouco pior, usando a cota de união:

$$\begin{aligned} \mu^{\otimes n} \left\{ x \in \Omega^n : \max_{j=1}^k \left| \frac{1}{n} \sum_{i=1}^n \chi_{C_j}(X_i) - \mu(C_j) \right| \geq \varepsilon \right\} \\ \leq k \cdot \max_{j=1}^k \mu^{\otimes n} \left\{ x \in \Omega^n : |\mu_n(C_j) - \mu(C_j)| \leq \varepsilon \right\} \\ \leq 2ke^{-2\varepsilon^2 n}. \end{aligned}$$

**Corolário 3.2.16.** *Dado  $k$  conceitos  $C_1, C_2, \dots, C_k$  e um  $\varepsilon > 0$ , com confiança  $\geq 1 - 2ke^{-2\varepsilon^2 n}$ , a medida empírica de cada um de  $k$  conceitos difere da sua medida por menos de  $\varepsilon > 0$ :*

$$\mu^{\otimes n} \left\{ \exists i = 1, 2, \dots, k \quad |\mu_\sigma(C_i) - \mu(C_i)| \geq \varepsilon \right\} \leq 2ke^{-2\varepsilon^2 n}.$$

Usando a notação probabilística:

$$P \left[ \max_{j=1}^k |\mu_n(C_j) - \mu(C_j)| > \varepsilon \right] \leq 2ke^{-2\varepsilon^2 n}. \quad (3.5)$$

De fato, a mesma prova se aplica no contexto mais geral quando as funções indicadoras são substituídas por funções quaisquer com valores no intervalo  $[0, 1]$ . A papel da medida empírica  $\mu_\sigma$  será exercida pela *esperança empírica* de uma função,

$$\mathbb{E}_{\mu_\sigma}(f) = \frac{1}{n} \sum_{i=1}^n f(x_i).$$

**Teorema 3.2.17.** *Sejam  $f_1, f_2, \dots, f_k$  funções borelianas sobre  $\Omega$  com valores em  $[0, 1]$ . Com a confiança  $\geq 1 - 2ke^{-2\varepsilon^2 n}$ , a esperança empírica  $\mathbb{E}_{\mu_\sigma}$  simultaneamente aproxima a esperança  $\mathbb{E}_\mu$  para todas as funções  $f_i$ ,  $i = 1, 2, \dots, k$  com precisão  $\leq \varepsilon$ :*

$$\mu^{\otimes n} \left\{ \sigma \in \Omega^n : \exists i = 1, 2, \dots, k \quad \left| \mathbb{E}_\mu(f_i) - \mathbb{E}_{\mu_\sigma}(f_i) \right| > \varepsilon \right\} \leq 2ke^{-2\varepsilon^2 n}.$$

**Exercício 3.2.18.** Mostrar o teorema 3.2.17.

Uma classe de funções cujas esperanças podem ser aproximadas simultaneamente pelas esperanças empíricas é dita uma *classe de Glivenko–Cantelli*. Vamos formalizar esta noção em breve.

**Corolário 3.2.19.** *Cada classe finita de conceitos,  $\mathcal{C} = \{C_1, C_2, \dots, C_k\}$ , é PAC aprendizável sob qualquer medida fixa,  $\mu$ , com a complexidade amostral  $s(\varepsilon, \delta) \leq \frac{1}{2\varepsilon^2} \log \frac{2k}{\delta}$ .*

*Demonstração.* Dado um conceito desconhecido,  $C = C_i \in \mathcal{C}$ , e uma amostra  $\sigma$ , assim como a rotulagem  $C \upharpoonright \sigma$  induzida por  $C$ , vamos buscar o elemento  $C_m$  mais próximo a  $C$  no sentido da distância empírica  $L^1(\mu_\sigma)$ :

$$\begin{aligned} m &= \arg \min_{j=1}^k \mu_\sigma(C \Delta C_j) \\ &= \arg \min_{j=1}^k \frac{1}{n} \sum_{i=1}^n |\chi_C(x_i) - \chi_{C_j}(x_i)|. \end{aligned}$$

A hipótese gerada pela nossa regra de aprendizagem será  $H = C_m$ .

Como  $\mu_\sigma(C \Delta C_i) = 0$ , segue-se que  $\mu_\sigma(C \Delta C_m) = 0$  também. Seja  $\epsilon > 0$ . Aplicando corolário 3.2.16 aos conceitos

$$C \Delta C_1, C \Delta C_2, \dots, C \Delta C_k,$$

concluimos que, com confiança  $\geq 1 - 2ke^{-2\epsilon^2 n}$ ,

$$\begin{aligned} \text{erro}_H(C) &= \mu(C \Delta C_m) \\ &\stackrel{\epsilon}{\approx} \mu_\sigma(C \Delta C_m) = 0. \end{aligned}$$

Dado  $\delta > 0$  qualquer, concluimos: se  $n \geq \frac{1}{2\epsilon^2} \log \frac{2k}{\delta}$ , logo, com confiança  $\geq 1 - \delta$ ,  $\text{erro}_H(C) < \epsilon$ .  $\square$

*Observação 3.2.20.* A expressão  $\mu_\sigma(C \Delta H)$  é conhecida como o *erro* (as vezes: *risco*) *empírico*. Por isso, a nossa estratégia de escolha da hipótese se chama *minimização do erro* (ou: de *risco*) *empírico*.

*Observação 3.2.21.* Torna-se explícito que a complexidade amostral da aprendizagem de uma classe finita não depende da medida  $\mu$ . Diz-se que uma tal classe é *uniformemente PAC aprendizável* (tendo em mente: uniformemente sobre todas as medidas de probabilidade).

### 3.2.5 Redução de dimensionalidade no cubo de Hamming

O teorema 3.2.17 pode ser visto como uma técnica de redução de dimensionalidade aleatorizada. Suponha que os dados são realizados como funções borelianas sobre um espaço probabilístico  $(\Omega, \mu)$ , e munidas da distância  $L^1(\mu)$ , dada pela norma

$$\|f\|_{L^1(\mu)} = \int_{\Omega} |f(x)| d\mu(x) = \mathbb{E}_{\mu}(|f|).$$

No caso particular onde  $\Omega$  é finito,  $\Omega = \{x_1, x_2, \dots, x_m\}$ , e a medida  $\mu$  é uma medida uniforme sobre  $[m]$ , cada função  $f: \Omega \rightarrow \mathbb{R}$  é um  $m$ -vetor, e a norma  $L^1(\mu)$  é a norma

$\ell^1(m)$  normalizada (!) sobre o espaço vetorial  $\mathbb{R}^m$  de dimensão  $m$ :

$$\| (f(x_1), f(x_2), \dots, f(x_m)) \|_1 = \frac{1}{m} \sum_{i=1}^m |f(x_i)|.$$

A norma acima é a norma no espaço  $L^1(\mu_m)$ , em relação a medida empírica.

Voltemos no caso de  $\Omega$  geral. Dado uma amostra  $\sigma = (x_1, x_2, \dots, x_m) \in \Omega^m$ , a aplicação

$$f \mapsto (f(x_1), f(x_2), \dots, f(x_m)),$$

pode ser vista como uma projeção do espaço  $L^1(\Omega, \mu)$  sobre o espaço  $\frac{1}{m}\ell^1(m) = L^1(\mu_m)$ .

**Teorema 3.2.22.** *Sejam  $f_1, f_2, \dots, f_n$  funções borelianas quaisquer sobre um espaço probabilístico padrão  $\Omega$  com valores em  $[0, 1]$ . Seja  $\mu$  uma medida de probabilidade boreliana sobre  $\Omega$ . Dado  $\varepsilon > 0$  e  $\delta > 0$ , se*

$$m \geq \frac{1}{\varepsilon^2} \ln \frac{n}{\delta}, \quad (3.6)$$

então com confiança  $\geq 1 - \delta$ , uma projeção aleatória

$$L^1(\Omega, \mu) \ni f \mapsto f \upharpoonright \sigma_m \in L(\mu_m),$$

conserva as distâncias a menos  $\varepsilon$ :

$$\forall i, j = 1, 2, \dots, n, \quad \| f_i - f_j \|_{L^1(\mu)} \stackrel{\varepsilon}{\approx} \| f_i \upharpoonright \sigma_m - f_j \upharpoonright \sigma_m \|_{L(\mu_m)}.$$

Usamos a notação conveniente:

$$a \stackrel{\varepsilon}{\approx} b \iff |a - b| \leq \varepsilon.$$

*Demonstração.* Aplicando o teorema 3.2.17 para  $n(n-1)/2$  funções  $|f_i - f_j|$ ,  $i \neq j$ , temos a conclusão desejada com confiança  $\geq 1 - n(n-1)e^{-2\varepsilon^2 m}$ . A desigualdade

$$n(n-1)e^{-2\varepsilon^2 m} \leq \delta$$

é equivalente a

$$\ln(n(n-1)) - 2\varepsilon^2 m \leq \ln \delta,$$

o que é satisfeito sob a hipótese (3.6).  $\square$

Deste modo, podemos realizar o conjunto de  $n$  dados *provavelmente aproximadamente corretamente* dentro de um espaço vetorial de dimensão  $O(\log n)$ .

**Exercício 3.2.23.** Obter uma modificação do teorema 3.2.22 válida para todas as distâncias  $L^p(\mu)$ ,  $1 \leq p < +\infty$ :

$$\|f\|_{L^p(\mu)} = \left( \int_{\Omega} |f|^p d\mu \right)^{1/p}.$$

Segue-se um caso particular importante.

**Exercício 3.2.24.** Seja  $\Omega = [d] = \{1, 2, 3, \dots, d\}$  um conjunto finito munido da medida de contagem normalizada,  $\mu_{\#}$ . Verificar que o espaço  $L^1(\mu_{\#})$  é o cubo de Hamming  $\Sigma^d$ , e a distância  $L^1(\mu_{\#})$  é a distância de Hamming normalizada.

**Corolário 3.2.25.** Seja  $X \subseteq \Sigma^n$  um conjunto de dados realizado no cubo de Hamming, munido da distância de Hamming normalizada. Denotemos  $n = |X|$ . Sejam  $\varepsilon, \delta > 0$ . Tiremos aleatoriamente de  $[n]$  um subconjunto  $I$  com

$$|I| \geq \frac{1}{\varepsilon^2} \ln \frac{n}{\delta} = O(\log n)$$

elementos. Então, com confiança  $\geq 1 - \delta$ , a projeção

$$x \mapsto x \upharpoonright I$$

de  $X$  sobre um sub-cubo aleatório  $\Sigma^I$  conserva as distâncias entre os elementos de  $X$  a menos  $\varepsilon$ :

$$\forall i, j, \bar{d}^{\Sigma^d}(x, y) \approx_{\varepsilon} \bar{d}^{\Sigma^I}(x \upharpoonright I, y \upharpoonright I).$$

*Observação 3.2.26.* Este gênero de resultados foi usado no artigo [Kushilevitz, Ostrovsky e Rabani 2000] para construir uma esquema de indexação eficaz para busca de vizinhos próximos *aproximadamente correta* no cubo de Hamming. No mesmo tempo, o problema da existência das esquemas da busca *exata* (subseção 6.1.1) não está resolvida. A validade da seguinte conjectura ainda está um problema em aberto.

**Conjetura de maldição de dimensionalidade** [Indyk 2004] *Seja  $X$  um conjunto de dados com  $n$  pontos no cubo de Hamming  $\{0, 1\}^d$ . Suponha que  $d = n^{\omega(1)}$  e  $d = \omega(\log n)$ . Então cada estrutura de dados para a pesquisa exata de semelhança em  $X$ , com o tempo da pesquisa  $d^{O(1)}$ , deve usar o espaço  $n^{\omega(1)}$ .*

As estruturas de dados e os algoritmos são entendidos no sentido do *modelo de sonda de célula* da computação (*cell probe model*) [Bro Miltersen 2000]. Os melhores limites conhecidos [Barkol e Rabani 2002; Patrascu e Thorup 2009] estão longe de resolver o problema. A conjectura foi somente mostrada para algumas estruturas concretas [Pestov 2012, 2013b].



### 3.3 Teorema de Benedek–Itai

Como foi mostrado na seção 3.2.2, uma classe aprendizável sob uma medida fixa não contém famílias infinitas uniformemente discretas. De fato, esta propriedade caracteriza as classes aprendizáveis.

Mediante a motivação, esta propriedade é exatamente o que torna a classe  $2^\Omega$  de todos os subconjuntos de um domínio  $\Omega$  aprendizável sob uma medida discreta qualquer. Dado  $\epsilon > 0$ , existe  $k = k(\epsilon)$  tal que a medida total de átomos  $a_i$ ,  $i > k$ , é menor ou igual a  $\epsilon$ . Por conseguinte, o conjunto finito de  $2^k$  conceitos que são subconjuntos de  $\{a_1, a_2, \dots, a_k\}$  forma uma  $\epsilon$ -rede em  $2^\Omega$ , com relação à distância  $d(C, D) = \mu(C \Delta D)$  medidora do erro de generalização: qualquer que seja  $D \in 2^\Omega$ , existe  $C \subseteq \{a_1, a_2, \dots, a_k\}$ , tal que  $\mu(C \Delta D) < \epsilon$ . (Basta definir  $D = C \cap \{a_1, a_2, \dots, a_k\}$ ). Esta propriedade significa que o conjunto  $2^\Omega$  munido da distância  $d$  é *totalmente limitado*, é no final das contas, essa propriedade é responsável pela aprendizabilidade da classe  $2^\Omega$ .

Para medidas mais gerais, nós já sabemos que as classes finitas são PAC aprendizáveis. Esta observação está ao coração do resultado de Benedek e Itai que dá umas condições necessárias e suficientes da aprendizabilidade sob uma medida fixa. Vamos mostrar o resultado nessa seção.

#### 3.3.1 Números de cobertura e de empacotamento

Relembramos que uma *pseudométrica* sobre um conjunto é uma função de duas variáveis,  $d(x, y)$ , que satisfaz todos os axiomas de uma métrica exceto a primeira: pode ser que  $d(x, y) = 0$  para  $x \neq y$ . Um conjunto munido de uma pseudométrica é chamado um *espaço pseudométrico*. Por exemplo, a rigor, a distância  $L^1(\mu)$  é uma métrica se e somente se a medida  $\mu$  é puramente atômica (exercício).

**Exercício 3.3.1.** Dado um espaço pseudométrico,  $(X, d)$ , mostrar que a relação

$$x \stackrel{d}{\sim} y \iff d(x, y) = 0$$

é uma relação de equivalência, e que o conjunto quociente  $\tilde{X} = X / \stackrel{d}{\sim}$  de classes de equivalência  $[x]$ ,  $x \in X$ , admite uma métrica, definida corretamente pela regra

$$\tilde{d}([x], [y]) = d(x, y).$$

Além disso, mostrar que a métrica  $\tilde{d}$  sobre  $\tilde{X}$  é a maior métrica tal que a aplicação quociente,

$$X \ni x \mapsto [x] \in \tilde{X},$$

é Lipschitz contínua com a constante  $L = 1$ .

O espaço métrico  $(\tilde{X}, \tilde{d})$  é chamado *o espaço métrico associado ao espaço pseudométrico*  $(X, d)$ , ou simplesmente *o quociente métrico* de  $(X, d)$ .

Dado um espaço probabilístico padrão,  $(\Omega, \mu)$ , o símbolo  $L^1(\Omega, \mu)$  tipicamente significa o quociente métrico do espaço de todas as funções borelianas sobre  $\Omega$  munidas da pseudométrica  $L^1(\mu)$  tais que  $L^1(|f|) < \infty$ . (Veja também a subseção H.1.2.) Vamos ser ambíguos, e na maioria de casos no contexto de aprendizagem vamos trabalhar diretamente com o espaço pseudométrico original, sem passar ao espaço métrico quociente, embora usando o mesmo símbolo.

**Definição 3.3.2.** Sejam  $(X, d)$  um espaço pseudométrico e  $Y \subseteq X$  um subconjunto. Então  $Y$  é dito *totalmente limitado* em  $X$ , ou: *precompacto* em  $X$ , se para todo  $\varepsilon > 0$  existe uma cobertura finita de  $Y$  com bolas abertas em  $X$  (definidas de mesmo modo que num espaço métrico):

$$\exists x_1, x_2, \dots, x_k \in X, Y \subseteq \bigcup_{i=1}^k B_\varepsilon(x_i).$$

(Todas as noções necessárias podem ser achadas no apêndice C.)

Esta noção não deve ser confundida com a noção de um subconjunto *relativamente compacto*:  $Y$  é relativamente compacto em  $X$  se e apenas se a aderência de  $Y$  em  $X$  é compacta. Cada subconjunto relativamente compacto é precompacto, mas não o contrário. As noções de um conjunto totalmente limitado e de um conjunto precompacto são rigorosamente sinônimas.

**Exercício 3.3.3.** Mostrar que  $Y$  é totalmente limitado em  $X$  se e somente se  $Y$  é totalmente limitado em si mesmo.

**Definição 3.3.4.** Seja  $\varepsilon > 0$ . Um *número de cobertura* (covering number),  $N_X(\varepsilon, Y)$ , de um subconjunto  $Y$  em um espaço pseudométrico  $X$  é o menor tamanho de uma cobertura de  $Y$  pelas bolas abertas em  $X$ :

$$N_X(\varepsilon, Y) = \min \left\{ k \in \mathbb{N} : \exists x_1, x_2, \dots, x_k \in X, Y \subseteq \bigcup_{i=1}^k B_\varepsilon(x_i) \right\}.$$

É claro que o número  $N_X(\varepsilon, Y)$  é finito para todo  $\varepsilon > 0$  se e somente se  $Y$  é precompacto. No mesmo tempo, os números de cobertura são as características relativas e dependem do espaço ambiente,  $X$ .

**Exercício 3.3.5.** Construir um espaço (pseudo)métrico  $X$  e um subespaço  $Y$  tais que existe  $\varepsilon > 0$  com

$$N_X(\varepsilon, Y) \not\leq N_Y(\varepsilon, Y).$$

A precompactidade de um espaço pseudométrico  $Y$  pode ser também expressa em termos de *números de empacotamento*, que são absolutas (não dependem do espaço ambiente).

**Definição 3.3.6.** Sejam  $X$  um espaço pseudométrico,  $\varepsilon > 0$ . O número de empacotamento (packing number),  $D(\varepsilon, X)$ , é o maior número de pontos à distância  $\geq \varepsilon$  dois a dois:

$$D(\varepsilon, X) = \sup\{n \in \mathbb{N} : \exists x_1, x_2, \dots, x_k \in X, (i \neq j)d(x_i, x_j) \geq \varepsilon\}.$$

**Lema 3.3.7.** Sejam  $X$  um espaço pseudométrico,  $Y \subseteq X$ ,  $\varepsilon > 0$ . Então,

$$N_X(\varepsilon, Y) \leq N_Y(\varepsilon, Y) \leq D(\varepsilon, Y) \leq N_X(\varepsilon/2, Y) \leq N_Y(\varepsilon/2, Y).$$

*Demonstração.* Se temos um  $\varepsilon$ -empacotamento máximo de  $Y$ ,  $x_1, x_2, \dots, x_k$ , então não podemos adicionar mais um ponto  $y$  de modo que as distâncias  $d(y, x_i)$  satisfaçam  $\geq \varepsilon$ . Isso implica que as bolas abertas de raio  $\varepsilon$  em torno de pontos  $x_i$  formam uma cobertura de  $X$ .

Agora, seja  $B_{\varepsilon/2}(x_i)$ ,  $i = 1, 2, \dots, k$  uma cobertura de  $Y$  pelas bolas abertas em  $X$ . Seja  $y_1, \dots, y_m$  um subconjunto finito de  $Y$  de pontos dois a dois à distância  $\geq \varepsilon$ . Cada bola  $B_{\varepsilon/2}(x_i)$  pode conter no máximo um ponto  $y_j$ , o que significa  $m \leq k$ .  $\square$

**Proposição 3.3.8.** O número de empacotamento do cubo de Hamming satisfaz

$$D(\varepsilon, \Sigma^n) \geq e^{2(\frac{1}{2}-\varepsilon)^2 n},$$

quando  $\varepsilon < 1/2$ .

*Demonstração.* Escolhemos um  $\varepsilon$ -empacotamento máximo,  $X$ , de  $\Sigma^n$ . A maximalidade implica que as bolas  $B_\varepsilon(x)$ ,  $x \in X$  cobrem  $\Sigma^n$ , e por conseguinte

$$1 = \mu_\#(\Sigma^n) \leq \sum_{x \in X} \mu_\#(B_\varepsilon(x)) = \#(X) \mu_\#(B_\varepsilon(0)) \leq \#(X) e^{-2(\frac{1}{2}-\varepsilon)^2 n},$$

usando a estimativa do volume da bola da subseção 1.4.4, Eq. (1.16).  $\square$

### 3.3.2 Teorema de Benedek–Itai: aprendizagem sob uma distribuição fixa

**Teorema 3.3.9 (Benedek e Itai [1991]).** Seja  $(\Omega, \mu)$  um espaço probabilístico padrão. Para uma classe de conceitos  $\mathcal{C} \subseteq \mathcal{B}_\Omega$ , as condições seguintes são equivalentes.

- $\mathcal{C}$  é PAC aprendizável.
- $\mathcal{C}$  é precompacto em relação à pseudométrica  $L^1(\mu)$ .

A complexidade amostral de uma classe  $\mathcal{C}$  que satisfaz uma destas condições equivalentes verifica

$$\log_2 D(2\varepsilon, \mathcal{C}) - 1 \leq s(\varepsilon, \delta) \leq \frac{9}{2\varepsilon^2} \ln \frac{2N(\varepsilon/3, \mathcal{C}, L^1(\mu))}{\delta},$$

quando  $\delta \leq 1/2$ .

### A regra de aprendizagem

Suponha primeiramente que  $\mathcal{C}$  seja  $L^1(\mu)$ -precompacto. Dado  $\epsilon > 0$ , escolha uma  $\epsilon/3$ -rede finita, ou seja, conjuntos borelianos

$$H_1, H_2, \dots, H_k$$

tais que, qualquer seja  $C \in \mathcal{C}$ , existe  $i = 1, 2, \dots, k$  com  $\mu(C \Delta H_i) < \epsilon/3$ . Os conjuntos  $H_i$  (hipóteses) não têm que necessariamente pertencer à classe  $\mathcal{C}$ . Elas formam uma *classe de hipóteses*,  $\mathcal{H}$ .

Seja  $C \in \mathcal{C}$  um conceito desconhecido qualquer. Dada uma amostra rotulada,

$$\sigma = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n),$$

temos a medida empírica,  $\mu_\sigma$ ,

$$\mu_\sigma(A) = \frac{1}{n} \#\{i : x_i \in A\}.$$

O que se sabe, é o traço de  $C$  sobre  $\sigma$ :

$$C \cap \text{supp } \sigma = \{x_i : \epsilon_i = 1\}.$$

Dada uma hipótese  $H$  qualquer, pode-se calcular o *erro empírico* de  $H$ :

$$\text{erro}_C(H, \mu_\sigma) = \mu_\sigma(H \Delta C \cap \text{supp } \sigma) = \mu_\sigma(C \Delta H) = \frac{1}{n} \sum_{i=1}^n |\chi_C(x_i) - \chi_H(x_i)|,$$

pois sabemos calcular os valores  $\chi_C(x_i)$  e  $\chi_H(x_i)$  para todos elementos  $x_i \in \sigma$  da amostra. (Os valores  $\chi_C(x_i)$  são determinados pela dada rotulagem da  $\sigma$ , e a hipótese  $H$  é conhecida).

A regra de aprendizagem é a de *minimização de erro empírico* na classe de hipóteses  $\mathcal{H}$ . Em outras palavras, buscamos a hipótese  $H_j$  que minimiza o erro empírico com relação ao conceito  $C$ :

$$j = \arg \min_i \mu_\sigma(C \Delta H_i).$$

Aplicamos o corolário 3.2.16 à classe de conjuntos da forma  $C \Delta H_i$ ,  $i = 1, 2, \dots, k$ , com precisão  $\epsilon/3$ . Concluimos que, com confiança  $\geq 1 - 2ke^{-2(\epsilon/3)^2n}$ , a medida empírica de cada um de  $k$  conceitos  $C \Delta H_i$  difere da sua medida verdadeira por menos de  $\epsilon/3$ :

$$\mu^{\otimes n} \left\{ \exists i = 1, 2, \dots, k \mid |\mu_\sigma(C \Delta H_i) - \mu(C \Delta H_i)| \geq \frac{\epsilon}{3} \right\} \leq 2ke^{-2(\epsilon/3)^2n},$$

ou seja,

$$\mu^{\otimes n} \left\{ \forall i = 1, 2, \dots, k \mid \left| \text{erro}_{\mu, C}(H_i, \mu_\sigma) - \text{erro}_{\mu, C}(H_i, \mu) \right| \leq \frac{\epsilon}{3} \right\} > 1 - 2ke^{-2(\epsilon/3)^2n}.$$

O argumento seguinte se aplica com confiança  $\geq 1 - 2ke^{-2(\varepsilon/3)^2n}$  (isto é: a probabilidade de que o argumento inteiro seja correto) é pelo menos o valor acima.

Sabemos que existe  $i$  tal que  $\text{erro}_{\mu,C}(H_i, \mu) < \varepsilon/3$ . Isso implica que

$$\text{erro}_{\mu,C}(H_i, \mu_\sigma) < \frac{\varepsilon}{3} + \frac{\varepsilon}{3} = \frac{2\varepsilon}{3}.$$

A hipótese  $H = H_j$  escolhida pela nossa regra de minimização do erro empírico pode ser diferente de  $H_i$ , mas ela satisfaz tudo mesmo

$$\text{erro}_{\mu,C}(H_j, \mu_\sigma) \leq \text{erro}_{\mu,C}(H_i, \mu_\sigma) = \frac{2\varepsilon}{3},$$

e por conseguinte

$$\text{erro}_{\mu,C}(H_j, \mu) < \frac{2\varepsilon}{3} + \frac{\varepsilon}{3} = \varepsilon.$$

Então, com confiança  $\geq 1 - 2ke^{-2(\varepsilon/3)^2n}$ , a nossa regra aprende o conceito  $C$  com precisão  $\varepsilon$ .

Resta estimar a complexidade amostral: a desigualdade desejada

$$\delta \leq 2ke^{-2(\varepsilon/3)^2n}$$

transforma-se em

$$\ln \delta \leq \ln(2k) - \frac{2\varepsilon^2}{9}n,$$

ou seja,

$$n \geq \frac{9}{2\varepsilon^2} \ln \frac{2k}{\delta}.$$

### Necessidade de precompactidade da classe

Agora suponhamos que a classe  $\mathcal{C}$  seja aprendizável. Denotemos  $\mathcal{L}$  uma regra de aprendizagem que aprende  $\mathcal{C}$ . Lema 3.2.7 significa que todo  $2\varepsilon$ -empacotamento de  $\mathcal{C}$  é finito, em particular  $\mathcal{C}$  é precompacto, com

$$D(2\varepsilon, \mathcal{C}) \leq 2^{n+1},$$

e a complexidade amostral de aprendizagem de  $\mathcal{C}$  satisfaz

$$s(\varepsilon, \delta) \geq \log_2 D(2\varepsilon, \mathcal{C}) - 1,$$

quando  $\delta \leq 1/2$ .

*Observação 3.3.10.* Note como pouco sensível é a dependência da complexidade amostral sobre  $\delta$ . Diz-se que “confiança é barata” (“confidence is cheap”).

### 3.3.3 Regras consistentes

**Definição 3.3.11.** Uma regra de aprendizagem  $\mathcal{L}$  é dita *consistente com uma classe de conceitos*,  $\mathcal{C}$ , se

- todas as hipóteses produzidas por  $\mathcal{L}$  pertencem a  $\mathcal{C}$ ,

$$\forall n, \forall \sigma \in \Omega^n \times \{0, 1\}^n, \mathcal{L}(\sigma) \in \mathcal{C},$$

- a hipótese induz sobre a amostra a rotulagem original sempre que possível:

$$\forall C \in \mathcal{C}, \forall n, \forall \sigma \in \Omega^n, \mathcal{L}(C \upharpoonright \sigma) \upharpoonright \sigma = C \upharpoonright \sigma.$$

**Definição 3.3.12.** Uma classe de conceitos  $\mathcal{C}$  é *consistentemente aprendizável* se cada regra  $\mathcal{L}$  consistente com  $\mathcal{C}$  PAC aprende  $\mathcal{C}$ .

*Observação 3.3.13.* Se uma classe  $\mathcal{C}$  é consistentemente aprendizável, então ela é aprendizável. Basta notar que cada classe de conceitos,  $\mathcal{C}$ , admite pelo menos uma regra de aprendizagem consistente com ela. Intuitivamente, isso é claro: dada uma amostra rotulada cuja rotulagem é produzida por um elemento de  $\mathcal{C}$ , escolha a hipótese entre todos os conceitos que produz a mesma rotulagem. O que não é totalmente óbvio, é a possibilidade de fazer a escolha de hipóteses de maneira que a aplicação resultante,

$$\mathcal{L}_n: \Omega^n \times \{0, 1\}^n \times \Omega \rightarrow \{0, 1\},$$

seja boreliana. Vamos adiar a discussão para mais tarde (seção 4.5), para não nos perdermos em tecnicidades prematuramente.

*Observação 3.3.14.* Como vimos na seção 3.1, cada classe de conceitos é consistentemente aprendizável sob uma medida discreta.

No mesmo tempo, nem toda classe PAC aprendizável é consistentemente aprendizável. Aqui um exemplo clássico.

**Exemplo 3.3.15.** Seja  $\Omega = [0, 1]$ , o intervalo fechado, munido da medida de Lebesgue,  $\lambda$ , ou seja, a distribuição uniforme. A classe de conceitos,  $\mathcal{C}$ , consiste de todos os subconjuntos finitos e cofinitos do intervalo. (Um subconjunto  $A \subseteq \Omega$  é *cofinito* se  $\Omega \setminus A$  é finito). O espaço métrico associado ao espaço pseudométrico  $\mathcal{C}$ , munido da distância  $\lambda(C \Delta D)$ , consiste de dois pontos: a classe de equivalência do conceito vazio e a do intervalo, a distância 1 um de outro. Em outras palavras, é o espaço métrico  $\{0, 1\}$  com a distância usual. Segundo o teorema de Benedek-Itai, esta classe é PAC aprendizável.

No mesmo tempo, existe uma regra de aprendizagem consistente cujas todas hipóteses são conceitos finitos. Por exemplo, dada uma amostra rotulada

$$\sigma = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n),$$

pode-se definir a hipótese

$$H = \mathcal{L}_n(\sigma) = \{x_i : \epsilon_i = 1, i = 1, 2, \dots, n\}.$$

Esta hipótese,  $H$ , pertence à classe  $\mathcal{C}$  e induz a rotulagem original sobre  $\{x_1, x_2, \dots, x_n\}$ . No mesmo tempo, a regra  $\mathcal{L}$  nunca vai aprender o conceito  $[0, 1]$ : qualquer que seja a hipótese  $H$  gerada pela regra, o erro de aprendizagem é sempre péssimo:

$$\text{erro}_{[0,1]}(H) = \lambda(H\Delta[0, 1]) = \lambda([0, 1] \setminus H) = 1.$$

Concluimos:  $\mathcal{C}$  não é consistentemente aprendizável.

Quando uma classe é consistentemente aprendizável sob uma medida fixa? Mesmo que não haja critério conhecido para esta condição, tem a condição suficiente. Uma classe de Glivenko–Cantelli,  $\mathcal{C}$ , é caracterizado pela condição seguinte: com alta confiança, a medida empírica de todo elemento de  $\mathcal{C}$  aproxima bem a medida de verdade. Verifica-se que as classes de Glivenko–Cantelli são consistentemente aprendizáveis, e a condição de ser Glivenko–Cantelli exprima-se na linguagem de fragmentação. As classes de Glivenko–Cantelli formam o assunto do próximo capítulo.

## 3.4 Taxa de aprendizagem

A taxa de aprendizagem de uma classe  $\mathcal{C}$  sobre uma medida  $\mu$  é o mínimo tamanho de dados,  $n$ , necessário para aprender  $\mathcal{C}$  a uma precisão  $\epsilon$  e com uma confiança desejadas. Em outras palavras, é a taxa de crescimento da função  $s(\epsilon, \delta)$  da complexidade amostral. Como a dependência de  $\delta$  não é muito sensível, usualmente a dependência de  $\epsilon$  é o que é de interesse. Chamamos a *taxa de aprendizagem* a função  $\epsilon \mapsto s(\epsilon, \delta_0)$  com o valor do risco  $\delta_0 > 0$  fixo, imaginando alguma coisa como  $\delta_0 = 0,05$  ou  $\delta_0 = 0,01$ .

Mesmo se cada classe de conceitos é PAC aprendizável sobre cada medida discreta, a taxa de aprendizagem depende da medida e pode ser qualquer, de fato tão lenta quanto desejado.

### 3.4.1 O resultado

**Teorema 3.4.1** (Pestov 2010). *Seja  $\mathcal{C}$  uma classe de conceitos borelianos num domínio boreliano padrão  $\Omega$ , com a propriedade seguinte: existe um conjunto infinito  $A$  tal que todos subconjuntos finitos de  $A$  são fragmentados por  $\mathcal{C}$ . Sejam  $(\epsilon_k)$  e  $(f_k)$  duas seqüências de reais positivos tais que  $f_i \uparrow +\infty$  e  $\epsilon_i \downarrow 0$ , de modo que*

$$\frac{1}{7} > \epsilon_1 > \epsilon_2 > \dots > \epsilon_i > \dots$$

*Seja  $0 < \delta_0 < 1$  qualquer fixo. Então existe uma medida de probabilidade discreta,  $\mu$ , sobre  $\Omega$ , tal que cada regra de aprendizagem consistente com a classe  $\mathcal{C}$  exige uma*

amostra aleatória de tamanho  $n \geq f_k$  para aprender  $\mathcal{C}$  com precisão  $\varepsilon_k$  e confiança constante  $1 - \delta_0$ , qualquer que seja  $i$ :

$$s_{\mathcal{C}}(\varepsilon_k, \delta_0, \mu) \geq f_k.$$

Isso significa que a complexidade amostral de aprendizagem pode crescer exponencialmente, ou como

$$2, 2^2, 2^{2^2}, \dots, 2^{2^{2^2}}, \dots,$$

ou mesmo mais rápido do que isso, por exemplo, como uma função não recursivamente computável. O fato de ser aprendizável com uma taxa de crescimento igual não é particularmente informativo. Usualmente na ciência de computação só as taxas de crescimento polinomiais são consideradas desejadas.

*Observação 3.4.2.* Seja  $\mu$  uma medida uniforme sobre um conjunto finito,  $X$ , com  $n$  elementos, que tem a massa total  $\gamma > 0$ . Isso significa  $\mu\{x\} = \gamma/n$  para todo  $x \in X$ . Então a distância  $L^1(\mu)$  sobre o espaço  $2^X$  de todos os subconjuntos de  $X$  é igual à distância de Hamming normalizada a menos um fator de  $\gamma$ :

$$d(C, D) = \|\chi_C - \chi_D\|_{L^1(\mu)} = \int_X |\chi_C - \chi_D| d\mu = \mu(C \Delta D) = \gamma \bar{d}(\chi_C, \chi_D).$$

*Prova do teorema 3.4.1.* Graças ao teorema 3.3.9 de Benedek-Itai, basta construir a medida discreta  $\mu$  de modo que para cada  $k$  existe uma família de  $\geq 2^{f_k}$  conceitos dois a dois à distância  $\geq 2\varepsilon_k$  um de outro. Substituindo  $f_k$  por  $\max\{f_1, f_2, \dots, f_k\}$  se for necessário, podemos supor que  $(f_k)$  cresce monotonicamente. Denotemos  $\gamma_0 = 1 - 7\varepsilon_1 > 0$  e para todo  $k \geq 1$ ,

$$\gamma_k = 7(\varepsilon_k - \varepsilon_{k+1}).$$

Então,  $\gamma_k > 0$ ,  $k \in \mathbb{N}$ , e  $\sum_{k=0}^{\infty} \gamma_k = 1$ .

Tendo em vista a proposição 3.3.8, escolhemos para cada  $k \geq 1$  um número natural  $m_k$  de modo que

$$e^{2(\frac{1}{2} - \frac{1}{3})^2 m_k} \geq 2^{f_k},$$

ou seja,  $m_k \geq (18 \ln 2) f_k$ . Posemos  $m_0 = 1$ . Agora, para todo  $k \in \mathbb{N}$ , escolhemos uma família de elementos  $\sigma_i^k \in \Sigma^{m_k}$ ,  $i = 1, 2, \dots, f_k$ , com  $\bar{d}(\sigma_i, \sigma_j) \geq 1/3$  se  $i \neq j$ .

Escolhemos um subconjunto infinito enumerável,  $A$ , de  $\Omega$ , cujos subconjuntos finitos são todos fragmentados pela classe  $\mathcal{C}$ . Dividimos  $A$  em subconjuntos  $A_k$ ,  $k \in \mathbb{N}$ , dois a dois disjuntos e finitos,  $\#A_k = m_k$ . Finalmente, definamos  $\mu$  pela condição: se  $a \in A_k$ , então

$$\mu\{a\} = \frac{\gamma_k}{m_k}.$$

É claro que  $\mu(A_k) = \gamma_k$ ,  $k \in \mathbb{N}$ , e  $\mu$  é uma medida de probabilidade discreta sobre  $\Omega$ .



Seja  $k \geq 1$  qualquer. Como  $\sum_{i=k}^{\infty} \gamma_i = 7\varepsilon_k$ , existe  $N > k$  tal que  $\sum_{i=k}^N \gamma_i \geq 6\varepsilon_k$ . Segundo a escolha de  $A$ , existem os conceitos  $C_1, C_2, \dots, C_{f_k} \in \mathcal{C}$  tais que, quaisquer que sejam  $i = k, k+1, \dots, N$  e  $j = 1, 2, \dots, f_k$ , temos

$$C_j \upharpoonright A_i = \sigma_j^i.$$

Se  $j, j' = 1, 2, \dots, f_k, j \neq j'$ , então

$$\begin{aligned} \mu(C_j \Delta C_{j'}) &= \sum_{i=k}^N \mu((C_j \cap A_i) \Delta (C_{j'} \cap A_i)) \\ &= \sum_{i=k}^N \gamma_i \bar{d}(\sigma_j^i, \sigma_{j'}^i) \\ &\geq \sum_{i=k}^N \frac{1}{3} \gamma_i \\ &> \frac{1}{3} \cdot 6\varepsilon_k \\ &= 2\varepsilon_k. \end{aligned}$$

□

### 3.4.2 Consequências para medidas não atômicas

Modifiquemos o resultado acima a fim de construir um exemplo de uma classe de conceitos,  $\mathcal{C}$ , que são subconjuntos de  $\Omega = \mathbb{R}$ , com as propriedades seguintes:

- Qualquer que seja uma medida de probabilidade boreliana sobre  $\Omega$ , a classe não é trivial em relação à distância  $L^1(\mu)$ ;
- $\mathcal{C}$  é PAC aprendizável sob toda medida de probabilidade boreliana sobre  $\Omega$ , e
- a taxa de aprendizagem pode ser tão lenta quanto se queira, incluindo sob medidas difusas.

A classe  $\mathcal{C}$  consiste de todas as uniões de intervalos semi-abertos da forma  $[n, n+1)$ ,  $n \in \mathbb{Z}$ . Dado  $I \subseteq \mathbb{Z}$ , denotemos

$$C_I = \bigcup_{n \in I} [n, n+1).$$

Desse modo, existe uma bijeção natural entre os elementos de  $\mathcal{C}$  e os de  $2^{\mathbb{Z}}$ , dada por

$$\phi(C) = C \cap \mathbb{Z}.$$

Se  $\mu$  é uma medida de probabilidade sobre  $\Omega$ , então  $\phi_*$  é a sua imagem direta, uma medida de probabilidade sobre  $\mathbb{Z}$  dada por

$$\phi_*(\mu)\{k\} = \mu(\{k, k + 1\}).$$

Dada uma regra de aprendizagem,  $\mathcal{L}$ , no domínio  $\mathbb{Z}$ , pode se definir a regra para  $\Omega$ , que denotaremos por  $\mathcal{L}^\phi$ . Ela é dada por

$$\mathcal{L}_n^\phi(\sigma) = \phi^{-1}(\mathcal{L}_n(\phi(\sigma))).$$

**Exercício 3.4.3.** Se a regra  $\mathcal{L}$  PAC aprende a classe  $2^{\mathbb{Z}}$  sob a medida  $\phi_*(\mu)$ , então  $\mathcal{L}^\phi$  aprende  $\mathcal{C}$  sob a medida  $\mu$ , com a mesma complexidade amostral.

Dada uma regra de aprendizagem  $\mathcal{L}$  sobre o domínio  $\Omega$ , pode se definir uma regra para  $\mathbb{Z}$ , usando a imersão canônica,  $i$ , de  $\mathbb{Z}$  dentro  $\mathbb{R}$ :

$$\mathcal{L}^i(\sigma) = \mathcal{L}(\sigma) \cap \mathbb{Z}.$$

**Exercício 3.4.4.** Se a regra  $\mathcal{L}$  PAC aprende a classe  $\mathcal{C}$  sob a medida  $\mu$ , então  $\mathcal{L}^i$  aprende  $2^{\mathbb{Z}}$  sob a medida  $\phi_*(\mu)$ , com a complexidade amostral menor ou igual à complexidade de  $\mathcal{L}$ .

Juntos, os dois exercícios estabelecem a validade da afirmação desejada.

### 3.4.3 Consequências para o classificador 1-NN

O classificador de vizinho mais próximo (1-NN) pode ser definido em todo o domínio munido da uma “medida de semelhança” qualquer (não necessariamente uma métrica). Mais geralmente,  $\Omega$  deve admitir uma família de pré-ordens,  $\prec_x$ , uma para cada ponto  $x \in \Omega$ , tais que  $x$  é o ponto mínimo desta pré-ordem e a condição  $y \prec_x z$  é interpretado como significando que  $y$  é mais perto de  $x$  que  $z$ . As pré-ordens  $\prec_x$  devem satisfazer certas condições de mensurabilidade. No caso de mais de um vizinho mais próximo de  $x$ , vamos desempatar escolhendo o vizinho  $x_i$ , seja aleatoriamente, seja com o índice  $i$  menor. Pelo momento, uma teoria falta nessa generalidade, e apenas existe para espaços métricos.

Vamos tratar o caso que parece até ser trivial, o da métrica zero-um, que so toma dois valores:

$$d(x, y) = \begin{cases} 0, & \text{se } x = y, \\ 1, & \text{se } x \neq y. \end{cases}$$

A estrutura boreliana induzida pela tal métrica contem todos os subconjuntos do domínio, que por conseguinte deve ser enumerável. Concluímos que toda medida de probabilidade sobre  $\Omega$  é discreta. Dado um conjunto finito dos átomos,  $a_1, a_2, \dots, a_k$ , se  $n$  for bastante grande, com alta confiança todos  $a_j$  vão aparecer entre os elementos da amostra aleatória,  $x_1, x_2, \dots, x_n$ . Se  $x_i = a_j$ , o seu vizinho mais próximo é  $a_j$  mesmo, e o rótulo de  $a_j$  vai

ser escolhido para  $x_i$  pela regra 1-NN. Esse argumento estabelece que a regra 1-NN neste contexto PAC aprende a classe  $2^{\Omega}$ . No mesmo tempo, o teorema 3.4.1 implica que a taxa de aprendizagem pode ser tão lenta quanto se queira, para uma medida  $\mu$  apropriada. Esta conclusão vale para caso geral de classificadores  $k$ -NN nos domínios quaisquer.

Mesmo se nessa situação o classificador 1-NN pode aparecer como uma regra de aprendizagem dentro uma classe, na verdade, ele é de uma natureza diferente. Vamos estudá-lo, dentro de um modelo próprio de aprendizagem, no capítulo 5.

# 4

## Classes de Glivenko–Cantelli

---

A noção seguinte está uma das mais importantes na teoria de aprendizagem estatística supervisionada.

**Definição 4.0.1.** Uma classe de conceitos,  $\mathcal{C}$ , sobre um domínio boreliano padrão  $\Omega$  é uma *classe de Glivenko–Cantelli* sob a medida de probabilidade  $\mu$ , ou tem a propriedade de *convergência uniforme de medidas empíricas* (*uniform convergence of empirical means*, *UCEM* property) sob  $\mu$ , se  $\mathcal{C}$  possui a propriedade seguinte. Para quaisquer que sejam  $\epsilon > 0$  e  $\delta > 0$ , existe o valor  $s = s(\epsilon, \delta)$  (a complexidade amostral) tal que, se  $n \geq s(\epsilon, \delta)$ , então, com confiança  $> 1 - \delta$  a medida empírica  $\epsilon$ -aproxima a medida verdadeira para todo conceito  $C \in \mathcal{C}$ :

$$\mu^{\otimes n} \{ \sigma \in \Omega^n : \forall C \in \mathcal{C}, \mu_\sigma(C) \stackrel{\epsilon}{\approx} \mu(C) \} > 1 - \delta. \quad (4.1)$$

De maneira equivalente,

$$\mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| \rightarrow 0 \text{ quando } n \rightarrow \infty. \quad (4.2)$$

Por exemplo, segundo teorema 3.2.17, toda classe finita é uma classe de Glivenko–Cantelli sob qualquer medida. Segue-se facilmente dos resultados da Subseção 3.1.2 que a classe  $2^{\Omega}$  de todos os conceitos é uma classe de Glivenko–Cantelli sob uma medida discreta.

De fato, esta noção está bem definida para classes de *funções*, e a maioria dos resultados tem análogos. Mas nós vamos nos preocupar principalmente com as classes de conceitos. Neste capítulo vamos estudar as propriedades de classes de Glivenko–Cantelli, as suas várias caracterizações, e o seu papel na aprendizagem de máquina.

## 4.1 Complexidades de Rademacher

Vamos brincar com a definição de uma classe G–C, reformulando-a em uma forma equivalente que pode ser interpretada na linguagem da aprendizagem estatística.

### 4.1.1 Simetrização com sinais

Seja  $\mathcal{C}$  uma classe de Glivenko–Cantelli, onde vamos adotar a definição na eq. (4.2). Seja  $\varepsilon > 0$ , e suponha que  $n$  é tão grande que

$$\mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| < \varepsilon.$$

Seja  $\sigma' = (X'_1, X'_2, \dots, X'_n)$  uma amostra independente de  $\sigma = (X_1, X_2, \dots, X_n)$ , o que significa que a lei do par  $(\sigma, \sigma')$  é a medida de produto  $\mu^{\otimes n} \otimes \mu^{\otimes n}$  sobre  $\Omega^n \times \Omega^n$ . Usando a desigualdade triangular junto com as propriedades básicas do supremo e esperança, temos

$$\begin{aligned} \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu_{\sigma'}(C)| &= \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C) + \mu(C) - \mu_{\sigma'}(C)| \\ &\leq \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| + \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_{\sigma'}(C) - \mu(C)| \\ &= \mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| + \mathbb{E}_{\sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_{\sigma'}(C) - \mu(C)| \\ &< 2\varepsilon. \end{aligned}$$

Cada permutação  $\tau$  de coordenadas de  $\Omega^{2n}$ , ou seja, um elemento  $\tau \in S_{2n}$  do grupo simétrico de posto  $2n$ , define um automorfismo boreliano de  $\Omega^{2n}$ ,

$$(x_1, x_2, \dots, x_{2n}) \mapsto (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(2n)}),$$

que conserva a medida de produto  $\mu^{\otimes 2n}$ . Em outras palavras, qualquer que seja um subconjunto boreliano  $B \subseteq \Omega^{2n}$ , temos

$$\mu(\tau(B)) = \mu(B).$$

(Para mostrar este fato, notemos que a medida de conjuntos retangulares é obviamente conservada pelas permutações de coordenadas,

$$\mu(B_1 \times \dots \times B_{2n}) = \prod_i \mu(B_i) = \mu(B_{\tau(1)} \times \dots \times B_{\tau(2n)}),$$

e segundo o teorema de Carathéodory E.1.15 sobre a extensão de medidas, os valores de medida de conjuntos retangulares definem unicamente a medida de produto).

Em particular, a conclusão acima se aplica à transposição,  $\tau_i$ , de  $i$ -ésimas coordenadas de amostras  $\sigma = (x_1, x_2, \dots, x_n)$  e  $\sigma' = (x'_1, x'_2, \dots, x'_n)$ :

$$\tau_i : i \leftrightarrow n + i, \quad 1 \leq i \leq n.$$

Concluimos que a esperança da variável aleatória

$$f(\sigma, \sigma') = \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu_{\sigma'}(C)|$$

é igual à esperança da composição  $f \circ \tau_i$ . Escrevemos  $f$  assim:

$$\begin{aligned} f(\sigma, \sigma') &= \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \chi_C(x_i) - \frac{1}{n} \sum_{i=1}^n \chi_C(x'_i) \right| \\ &= \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n (\chi_C(x_i) - \chi_C(x'_i)) \right|. \end{aligned}$$

O efeito de aplicar a transposição  $\tau_i$  é de substituir o termo  $\chi_C(x_i) - \chi_C(x'_i)$  pelo termo  $\chi_C(x'_i) - \chi_C(x_i)$ , ou seja, multiplicá-lo por  $-1$ . A composição  $\tau$  de um número finito de transposições desse tipo resulta em expressão seguinte:

$$(f \circ \tau)(\sigma, \sigma') = \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i (\chi_C(x_i) - \chi_C(x'_i)) \right|,$$

onde  $\eta = (\eta_1, \eta_2, \dots, \eta_n) \in \{-1, 1\}^n$  é uma sequência de sinais  $\pm 1$ . O conjunto  $\{\pm 1\}^n$  chama-se o *cuco de Rademacher*, um parente próximo do cuco de Hamming.

Resumimos: qualquer que seja  $\eta \in \{\pm 1\}^n$ ,

$$\begin{aligned} \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) - \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x'_i) \right| &= \mathbb{E}_{\sigma, \sigma' \sim \mu} (f \circ \tau)(\sigma, \sigma') \\ &= \mathbb{E}_{\sigma, \sigma' \sim \mu} f(\sigma, \sigma') \\ &= \mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu_{\sigma'}(C)| \\ &< 2\epsilon. \end{aligned} \tag{4.3}$$

### 4.1.2 Cubo de Rademacher

Se pensarmos em  $\{\pm 1\}^n$  como formado pelas funções de  $[n]$  para  $\{1, -1\} \subseteq \mathbb{R}$ , então a distância (normalizada) no cubo de Rademacher seria a distância  $L^1(\mu_{\#})$  relativa à medida de contagem normalizada sobre  $[n]$ :

$$d(\eta, \eta') = \frac{1}{n} \sum_{i=1}^n |\eta_i - \eta'_i| = \frac{2}{n} \#\{i : \eta_i \neq \eta'_i\}.$$

A medida sobre  $\{\pm 1\}^n$  é a medida normalizada de contagem. A aplicação  $i : \eta \mapsto \frac{1}{2}(\eta+1)$  de  $\{-1, +1\}^n$  para  $\{0, 1\}^n$  conserva a medida de contagem normalizada, e multiplica as distâncias pelo fator constante  $1/2$ . Em particular, a imagem de uma esfera (bola) de raio  $r$  é uma esfera (bola) de raio  $r/2$  (os valores da distância normalizada no cubo de Rademacher são os múltiplos de  $2/n$ ). Todas as noções e construções válidas para o cubo de Hamming tem sentido para o cubo de Rademacher, tais que, entre muitas outras, o peso normalizado:

$$\bar{w}(\eta) = \bar{w}_{\{\pm 1\}^n}(\eta) = \frac{1}{n} \sum_{i=1}^n \eta_i.$$

**Lema 4.1.1.** *No cubo de Rademacher,*

$$\mathbb{E}_{\eta} |\bar{w}_{\{\pm 1\}^n}(\eta)| \leq \frac{\sqrt{2\pi}}{\sqrt{n}}.$$

*Demonstração.* Passemos ao cubo de Hamming:

$$\begin{aligned} \mathbb{E}_{\eta} |\bar{w}_{\{\pm 1\}^n}| &= \int_{\{\pm 1\}^n} |\bar{w}_{\{\pm 1\}^n}(\eta)| d\mu_{\#}(\eta) \\ &= 2 \int_{\{0,1\}^n} |w_{\{0,1\}^n}(\sigma) - 1/2| d\mu_{\#}(\sigma) \\ &= 2 \sum_{\sigma \in \{0,1\}^n} |\bar{w}(\sigma) - 1/2| \cdot \frac{1}{2^n}. \end{aligned}$$

Agrupamos os termos da soma, usando o fato que  $\bar{w}(\sigma) = \bar{d}(0, \sigma)$  e por conseguinte o

peso é constante em cada esfera de Hamming,

$$\begin{aligned}
 \sum_{\sigma \in \{0,1\}^n} |\bar{w}(\sigma) - 1/2| \cdot \frac{1}{2^n} &= \sum_{i=0}^n \left| \frac{i}{n} - \frac{1}{2} \right| \mu_{\#} S_{i/n}(\bar{0}) \\
 &= 2 \sum_{i=0}^m \left( \frac{1}{2} - \frac{i}{n} \right) \mu_{\#} S_{i/n}(\bar{0}) \\
 &= \frac{2}{n} \sum_{i=0}^m \left( \frac{n}{2} - i \right) \mu_{\#} S_{i/n}(\bar{0})
 \end{aligned}$$

onde  $m = \lceil n/2 \rceil - 1$ . (Usamos a simetria de termos sob a transposição  $i \leftrightarrow n - i$ ).

Para  $n = 2m$  par,

$$\frac{1}{n} \sum_{i=0}^m \left( \frac{n}{2} - i \right) \mu_{\#} S_{i/n}(\bar{0}) = \frac{1}{n} \sum_{i=0}^{m-1} \mu_{\#} B_{i/n}(\bar{0}),$$

e agora usamos a estimativa do volume da bola da subseção 1.4.4 e depois fazemos a substituição  $j = m - i$ :

$$\begin{aligned}
 \mathbb{E}_{\eta} |\bar{w}_{\{\pm 1\}^n}| &< \frac{4}{n} \sum_{i=0}^{m-1} e^{-2(1/2-i/n)^2 n} \\
 &= \frac{4}{n} \sum_{j=1}^m e^{-2(j/n)^2 n} \\
 &< 4 \int_0^{1/2} e^{-2x^2 n} dx \\
 &\leq \frac{4}{\sqrt{2n}} \int_0^{+\infty} e^{-(\sqrt{2}x\sqrt{n})^2} d(\sqrt{2}x\sqrt{n}) \\
 &= \frac{\sqrt{2\pi}}{\sqrt{n}}.
 \end{aligned}$$



Para  $n = 2m + 1$  ímpar,  $n/2 = m + 1/2$ , e temos

$$\begin{aligned}
 \frac{1}{n} \sum_{i=0}^m \binom{n}{2-i} \mu_{\#} S_{i/n}(\bar{0}) &= \frac{1}{n} \sum_{i=0}^m \left( m - i + \frac{1}{2} \right) \mu_{\#} S_{i/n}(\bar{0}) \\
 &= \frac{1}{n} \sum_{i=0}^{m-1} \mu_{\#} B_{i/n}(\bar{0}) + \frac{1}{2n} \mu_{\#}(B_{m/n}(0)) \\
 &< \frac{1}{n} \sum_{j=1}^m e^{-2(1/2n+j/n)^2 n} + \frac{1}{2n} e^{-2(1/2n)^2 n} \\
 &< \int_0^{\infty} e^{-2x^2 n} dx,
 \end{aligned}$$

etc. □

O argumento acima pode ser generalizado como segue.

**Exercício 4.1.2.** Seja  $X = (X, d, \mu)$  um espaço métrico com medida de probabilidade boreliana, tendo a função de concentração  $\alpha_X$ . Mostrar que, qualquer que seja uma função Lipschitz contínua,  $f$ , com a constante de Lipschitz um, temos

$$|M(f) - \mathbb{E}(f)| \leq \int_0^{\infty} \alpha_X(\epsilon) d\epsilon.$$

(Para uma prova, veja lema 6.2.2). O lema 4.1.1, com constantes um pouco piores, segue-se em aplicando o exercício às funções  $\bar{w}_+ = \max\{\bar{w}, 0\}$  e  $\bar{w}_- = \max\{-\bar{w}, 0\}$  separadamente (cada uma delas tem 0 com valor mediano).

**Exercício 4.1.3.** Deduzir que, se  $X_n = (X_n, d_n, \mu_n)$ ,  $n \in \mathbb{N}_+$  é uma família de Lévy de espaços métricos com medida de probabilidade, e se  $f_n : X_n \rightarrow \mathbb{R}$  são funções Lipschitz contínuas com a constante de Lipschitz um, então

$$|M(f_n) - \mathbb{E}(f_n)| \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

(Para uma solução, consulte a prova do lema 6.2.2.)

**Exercício 4.1.4.** Seja  $\mathcal{X} = (X_n, d_n, \mu_n)_{n=1}^{\infty}$  uma família de Lévy normal. Mostrar que existe uma constante  $C_{\mathcal{X}} > 0$  tal que, para todo  $n$  e toda função Lipschitz contínua com a constante um,  $f_n : X_n \rightarrow \mathbb{R}$ ,

$$|M(f_n) - \mathbb{E}(f_n)| \leq \frac{C_{\mathcal{X}}}{\sqrt{n}}.$$

(Para uma solução, veja a prova do corolário 6.2.3.)

**Exercício 4.1.5.** Mostrar que a constante da família de cubos de Hamming satisfaz  $C_{(\Sigma^n)} < 1$ .

### 4.1.3 Médias de Rademacher

Concentremos a nossa atenção na expressão seguinte da Eq. (4.3):

$$\frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i). \quad (4.4)$$

A escolha de sinais,  $\eta$ , pode ser vista como uma rotulagem de  $\sigma$ , usando os rótulos  $-1$  e  $+1$ . Por causa da simetria de sinais, pode-se mostrar o seguinte.

#### Exercício 4.1.6.

$$\mathbb{E}_\eta \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) = 0.$$

Denotemos

$$\eta_+ = \{i = 1, 2, \dots, n : \eta_i = +1\}, \quad \eta_- = \{i = 1, 2, \dots, n : \eta_i = -1\}.$$

O peso normalizado de  $\eta$ ,

$$\bar{w}(\eta) = \frac{1}{n} \sum_i \eta_i,$$

que toma os valores no intervalo  $[-1, 1]$ , satisfaz as relações seguintes:

$$\bar{w}(\eta) = \frac{1}{n} (\#\eta_+ - \#\eta_-), \quad \#\eta_+ = \frac{n}{2}(1 + \bar{w}(\eta)), \quad \#\eta_- = \frac{n}{2}(1 - \bar{w}(\eta)).$$

Dada uma amostra  $\sigma \in \Omega^n$ , denotemos por  $\sigma_{\eta_+}$ , ou melhor, simplesmente  $\sigma_+$ , uma subamostra de  $\sigma$  do tipo

$$\sigma_+ = (x_{i_1}, x_{i_2}, \dots, x_{i_k}), \quad (i_1, i_2, \dots, i_k) = \eta_+,$$

e da mesma forma para  $\sigma_-$ . Estas  $\sigma_\pm$  são amostras i.i.d. de comprimento  $\#\eta_\pm$  respectivamente, seguindo a distribuição  $\mu$ , e  $\sigma_+$  e  $\sigma_-$  são independentes.

Para interpretar a expressão na eq. (4.4), calculemos o erro de aprendizagem da amostra  $\sigma$  rotulada com sinais com o conceito  $C$ . Ao invés da função binária  $\chi_C$ , temos que usar a função  $2\chi_C - 1$  tomando valores em  $\{\pm 1\}$ :

$$(2\chi_C - 1)(x) = \begin{cases} 1, & \text{se } x \in C, \\ -1, & \text{se } x \notin C. \end{cases}$$

Como

$$\eta_i (2\chi_C(x_i) - 1) = \begin{cases} +1, & \text{se } x_i \in \sigma_+ \text{ e } x_i \in C, \\ & \text{ou } x_i \notin \sigma_+ \text{ e } x_i \notin C, \\ -1, & \text{se } x_i \in \sigma_+ \text{ e } x_i \notin C, \\ & \text{ou } x_i \notin \sigma_+ \text{ e } x_i \in C, \end{cases}$$

temos

$$\begin{aligned} \frac{1}{n} \sum_{i=1}^n \eta_i (2\chi_C(x_i) - 1) &= \frac{\#\{+1\}}{n} - \frac{\#\{-1\}}{n} \\ &= 1 - 2\mu_\sigma(C \Delta\sigma_+) \\ &= 1 - 2\text{erro}_{\mu_\sigma, \sigma_+}(C). \end{aligned}$$

O valor pode ser visto como a *bondade de ajuste (goodness of fit) empírica* de  $\sigma_+$  com  $C$ . O valor máximo de 1 significa o ajuste perfeito.

Daqui, deduzimos

$$\frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) = \frac{1}{2} + \frac{1}{2} \bar{w}(\eta) - \text{erro}_{\mu_\sigma, \sigma_+}(C). \quad (4.5)$$

A interpretação desta expressão é menos transparente. Porém, se  $\eta$  é uma amostra aleatória, então, quando  $n \gg 1$ , com alta confiança,  $\bar{w}(\eta) \approx 0$ , então, os valores da expressão acima vão se aproximar de  $1/2 - \text{erro}_{\mu_\sigma, \sigma_+}(C)$ . Deste modo, vista como uma variável aleatória, a expressão acima é uma medida de bondade de ajuste empírica também.

Revisitamos o exercício 4.1.6, calculando a esperança da nossa soma, dessa vez em  $\sigma$ :

$$\begin{aligned} \mathbb{E}_{\sigma \sim \mu} \left( \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right) &= \mathbb{E}_{\sigma \sim \mu} \left( \frac{\#\sigma_+}{n} \cdot \frac{1}{\#\sigma_+} \sum_{i \in \sigma_+} \chi_C(x_i) - \frac{\#\sigma_-}{n} \cdot \frac{1}{\#\sigma_-} \sum_{i \in \sigma_-} \chi_C(x_i) \right) \\ &= \frac{\#\sigma_+}{n} \mathbb{E}_{\sigma_+ \sim \mu} \mu_{\sigma_+}(C) - \frac{\#\sigma_-}{n} \mathbb{E}_{\sigma_- \sim \mu} \mu_{\sigma_-}(C) \\ &= \frac{1}{2} (1 + \bar{w}(\eta)) \mu(C) - \frac{1}{2} (1 - \bar{w}(\eta)) \mu(C) \\ &= \bar{w}(\eta) \mu(C). \end{aligned}$$

Aqui, usamos a observação que  $\sigma_+$  e  $\sigma_-$  são amostras independentes, distribuídas segundo a medida  $\mu$ , junto com a propriedade  $\mathbb{E}_{\sigma \sim \mu} \mathbb{E}_{\mu_\sigma} f = \mathbb{E}_\mu f$ , estabelecida na subseção 3.2.4.

Deduzimos:

$$\begin{aligned}
2\epsilon &> \mathbb{E}_\eta \mathbb{E}_\sigma \mathbb{E}_{\sigma'} \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) - \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x'_i) \right| \\
&\geq \mathbb{E}_\eta \mathbb{E}_\sigma \sup_{C \in \mathcal{C}} \left| \mathbb{E}_{\sigma'} \left( \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) - \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x'_i) \mid \sigma \right) \right| \\
&= \mathbb{E}_\sigma \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) - \bar{w}(\eta) \mu(C) \right| \\
&\geq \mathbb{E}_\sigma \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right| - \mathbb{E}_\eta |\bar{w}(\eta)| \mu(C) \\
&> \mathbb{E}_\sigma \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right| - \sqrt{\frac{2\pi}{n}}.
\end{aligned}$$

Ou seja,

$$\mathbb{E}_\sigma \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right| < 2\epsilon + \sqrt{\frac{2\pi}{n}}.$$

Quando  $\mathcal{C}$  é uma classe de Glivenko-Cantelli, a expressão

$$\mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right|, \tag{4.6}$$

converge para zero em esperança (de maneira equivalente, em probabilidade). Por conseguinte, o mesmo se aplica à expressão

$$\hat{R}_n(\mathcal{C}) = \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i). \tag{4.7}$$

A expressão acima, (4.7), é chamada a *complexidade de Rademacher empírica* da classe  $\mathcal{C}$ . A complexidade de Rademacher empírica,  $\hat{R}_n(\mathcal{C})$ , é uma *função determinística*, de  $\Omega^n$  para  $[0, 1]$ . Na presença de uma medida  $\mu$  sobre  $\Omega$ , ela torna-se uma variável aleatória. A sua esperança,

$$R_n = \mathbb{E}_{\sigma \sim \mu} \hat{R}_n(\mathcal{C}),$$

chama-se a *complexidade de Rademacher* de  $\mathcal{C}$ .

*Observação 4.1.7.* À luz de eq. (4.5),

$$\hat{R}_n(\mathcal{C})(\sigma) = \frac{1}{2} - \mathbb{E}_\eta \inf_{C \in \mathcal{C}} \text{erro}_{\mu, \sigma, +}(C).$$

Então, o valor de  $\hat{R}_n(\mathcal{C})$  em  $\sigma$  é a esperança da melhor bondade de ajuste com um conceito da classe  $\mathcal{C}$ , da amostra  $\sigma$  rotulada aleatoriamente. Deste modo, o valor de  $R_n(\mathcal{C})$ ,

$$R_n = \frac{1}{2} - \mathbb{E}_{\sigma, \eta} \inf_{C \in \mathcal{C}} \text{erro}_{\mu_\sigma, \sigma^+}(C),$$

é a esperança da melhor bondade de ajuste com  $\mathcal{C}$  de uma  $n$ -amostra rotulada aleatória.

**Exercício 4.1.8.** Mostrar que  $\hat{R}_n(\mathcal{C})(\sigma) \geq 0$  para cada amostra  $\sigma$ .

[ *Sugestão:* se  $\sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) < 0$ , então

$$\sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n (-\eta_i) \chi_C(x_i) \geq \left| \sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right|. ]$$

Para resumir o que nós mostramos até agora: se  $\mathcal{C}$  é uma classe de Glivenko–Cantelli, então

$$R_n(\mathcal{C}) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

#### 4.1.4 O critério

Vamos deduzir a implicação no sentido contrário: se  $R_n(\mathcal{C}) \rightarrow 0$  (ou, da maneira equivalente,  $\hat{R}_n(\mathcal{C}) \rightarrow 0$  em probabilidade), então  $\mathcal{C}$  é uma classe de Glivenko–Cantelli. O argumento é baseado sobre as mesmas idéias de simetrização com sinais, e por isso precisamos usar uma cópia,  $\sigma' = (X'_1, X'_2, \dots, X'_n)$ , independente e identicamente distribuída, da amostra aleatória,  $\sigma$ . Temos:

$$\begin{aligned} \mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) &= \mathbb{E}_\sigma \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n \chi_C(X_i) - \mu(C) \right] \\ &= \mathbb{E}_\sigma \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n (\chi_C(X_i) - \mathbb{E}_{\sigma'} \chi_C(X'_i)) \right] \\ &= \mathbb{E}_\sigma \sup_{C \in \mathcal{C}} \left[ \mathbb{E}_{\sigma'} \left( \frac{1}{n} \sum_{i=1}^n (\chi_C(X_i) - \chi_C(X'_i)) \middle| \sigma \right) \right] \end{aligned}$$

Na última expressão trata-se de uma esperança condicional, que corresponde à integração ao longo das variáveis  $\sigma'$  quando as variáveis  $\sigma$  são fixas. Agora vamos usar o fato que o supremo de integrais de uma família de funções é limitado superiormente pela integral do supremo da família, e depois aplicar o teorema de Fubini:

$$\mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) \leq \mathbb{E}_{(\sigma, \sigma')} \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n (\chi_C(X_i) - \chi_C(X'_i)) \right]$$

Como as transposições  $i \leftrightarrow n + i$  conservam a medida  $\mu^{\otimes 2n}$ , concluímos que para cada  $\eta \in \{\pm 1\}^n$ ,

$$\mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) \leq \mathbb{E}_{(\sigma, \sigma')} \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n \eta_i (\chi_C(X_i) - \chi_C(X'_i)) \right].$$

Por conseguinte,

$$\begin{aligned} \mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) &\leq \mathbb{E}_\eta \mathbb{E}_{(\sigma, \sigma')} \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n \eta_i (\chi_C(X_i) - \chi_C(X'_i)) \right] \\ &\leq \mathbb{E}_{\eta, \sigma, \sigma'} \sup_{C \in \mathcal{C}} \left[ \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(X_i) + \frac{1}{n} \sum_{i=1}^n (-\eta_i) \chi_C(X'_i) \right] \\ &\leq \mathbb{E}_{\eta, \sigma} \sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(X_i) + \mathbb{E}_{\eta, \sigma'} \sup_{C \in \mathcal{C}} \frac{1}{n} \sum_{i=1}^n (-\eta_i) \chi_C(X'_i) \\ &= 2R_n(\mathcal{C}). \end{aligned}$$

Para deduzir a propriedade de Glivenko–Cantelli, vamos aplicar o fenômeno de concentração de medida, que também permite de quantificar o resultado.

**Exercício 4.1.9.** Verificar que a função real

$$\sigma \mapsto \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C))$$

é Lipschitz contínua com relação à distância de Hamming normalizada sobre  $\Omega^n$ , de constante  $L = 1$ .

Por conseguinte, qualquer que seja  $\varepsilon > 0$ ,

$$\begin{aligned} &\mu^{\otimes n} \{ \sigma : \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) - 2R_n(\mathcal{C}) > \varepsilon \} \\ &\leq \mu^{\otimes n} \{ \sigma : \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) - \mathbb{E} \sup_{C \in \mathcal{C}} (\mu_\sigma(C) - \mu(C)) > \varepsilon \} \\ &\leq e^{-2\varepsilon^2 n}. \end{aligned}$$

O argumento idêntico mostra que também

$$\mu^{\otimes n} \{ \sigma : \sup_{C \in \mathcal{C}} (\mu(C) - \mu_\sigma(C)) - 2R_n(\mathcal{C}) > \varepsilon \} \leq e^{-2\varepsilon^2 n}.$$

Deduzimos: com confiança  $\geq 1 - 2e^{-2\varepsilon^2 n}$ , qualquer que seja  $C \in \mathcal{C}$ ,

$$|\mu_\sigma(C) - \mu(C)| \leq 2R_n(\mathcal{C}) + \varepsilon.$$

Nota-se que

$$2e^{-2\epsilon^2 n} \leq \delta$$

quando

$$\epsilon \geq \sqrt{\frac{\ln(2/\delta)}{2n}}.$$

Podemos formular o resultado.

**Teorema 4.1.10.** *Dada uma classe de conceitos  $\mathcal{C}$ , para cada  $n$ , temos com confiança  $1 - \delta$ ,*

$$\sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| \leq 2R_n(\mathcal{C}) + \sqrt{\frac{\ln(2/\delta)}{2n}}.$$

A classe  $\mathcal{C}$  é uma classe de Glivenko–Cantelli se e somente se as complexidades de Rademacher de  $\mathcal{C}$  convergem para zero:

$$R_n(\mathcal{C}) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

*Observação 4.1.11.* Se uma classe  $\mathcal{C}$  ajusta bem as amostras rotuladas aleatórias, então ela sofre de *sobreajustamento* (*overfitting*). Desse modo, teorema 4.1.10 diz que uma classe é a de Glivenko–Cantelli se e somente se ele não sofre de sobreajustamento.

### 4.1.5 Propriedades de complexidades de Rademacher

A noção de complexidades de Rademacher tem sentido para qualquer classe  $\mathcal{F}$  de funções reais sobre o domínio.

**Definição 4.1.12.** Seja  $\mathcal{F}$  uma classe de funções reais. A expressão

$$\hat{R}_n(\mathcal{F})(\sigma) = \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i)$$

chama-se a *complexidade de Rademacher empírica* de classe  $\mathcal{F}$ .

Mais uma vez,  $\hat{R}_n(\mathcal{F})$  é uma função real determinística com valores positivos sobre o domínio, que não depende de uma medida. Na presença de uma medida  $\mu \in P(\Omega)$ , torna-se uma variável aleatória. Estamos principalmente interessados do caso onde  $\mathcal{F} = \{\chi_C : C \in \mathcal{C}\}$  é uma classe de funções binárias. Nesse caso, vamos escrever  $\hat{R}_n(\mathcal{C})$ , etc.

**Definição 4.1.13.** Sejam  $\mathcal{F}$  uma classe de funções borelianas e  $\mu$  uma medida de probabilidade boreliana sobre o domínio. A esperança da complexidade de Rademacher empírica chama-se a *complexidade de Rademacher* da classe  $\mathcal{F}$ :

$$R_n(\mathcal{F}, \mu) = \mathbb{E}_{\sigma \sim \mu} \hat{R}_n(\mathcal{F}),$$

ou: a *média de Rademacher* (*Rademacher average*), no contexto original da análise funcional.

Por exemplo,  $R_n(\mathcal{F}, \mu)$  é bem definida quando a classe  $\mathcal{F}$  consiste de funções com valores num intervalo.

**Proposição 4.1.14.** *Sejam  $\mathcal{F}$  e  $\mathcal{G}$  duas classes de funções com valores num intervalo,  $g$  uma função limitada qualquer, e  $\lambda \in \mathbb{R}$ . Então*

1.  $\hat{R}_n(\mathcal{F} + \mathcal{G}) = \hat{R}_n(\mathcal{F}) + \hat{R}_n(\mathcal{G})$ ,
2.  $\hat{R}_n(\mathcal{F} + g) = \hat{R}_n(\mathcal{F})$ ,
3.  $\hat{R}_n(\lambda\mathcal{F}) = |\lambda|\hat{R}_n(\mathcal{F})$ .

*Demonstração.*

$$\begin{aligned}
 (1) : \hat{R}_n(\mathcal{F} + \mathcal{G}) &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}, g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^n \eta_i (f(x_i) + g(x_i)) \\
 &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i) + \mathbb{E}_\eta \sup_{g \in \mathcal{G}} \frac{1}{n} \sum_{i=1}^n \eta_i g(x_i) \\
 &= \hat{R}_n(\mathcal{F}) + \hat{R}_n(\mathcal{G}).
 \end{aligned}$$

$$\begin{aligned}
 (2) : \hat{R}_n(\mathcal{F} + f) &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \eta_i (f(x_i) + g(x_i)) \\
 &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i) + \mathbb{E}_\eta \frac{1}{n} \sum_{i=1}^n \eta_i g(x_i) \\
 &= \hat{R}_n(\mathcal{F}).
 \end{aligned}$$

$$\begin{aligned}
 (3) : \hat{R}_n(\lambda\mathcal{F}) &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \lambda \eta_i f(x_i) \\
 &= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n |\lambda| \eta_i f(x_i) \\
 &= |\lambda| \hat{R}_n(\mathcal{F}).
 \end{aligned}$$

□



**Corolário 4.1.15.** *Sejam  $\mathcal{F}$  e  $\mathcal{G}$  duas classes de funções tais que  $0 \in \mathcal{F}$ ,  $0 \in \mathcal{G}$ . Então,*

$$\hat{R}_n(\mathcal{F} \cup \mathcal{G}) \leq \hat{R}_n(\mathcal{F}) + \hat{R}_n(\mathcal{G}).$$

*Demonstração.* Como  $0 \in \mathcal{F}$ , concluímos que  $\mathcal{G} \subseteq \mathcal{F} + \mathcal{G}$ , e igualmente para  $\mathcal{F}$ . Agora o resultado segue-se de proposição 4.1.14,(1).  $\square$

Sem a hipótese  $0 \in \mathcal{F}$ ,  $0 \in \mathcal{G}$ , o resultado é falso.

**Exemplo 4.1.16.** Seja  $\mathcal{C} = \{f\}$  uma classe que consiste de uma função só. Como no exercício 4.1.6,

$$R_n(\{f\}) = 0.$$

Agora seja  $\Omega = \{x_1, x_2, \dots, x_n\}$  um domínio finito qualquer com  $n$  pontos, e  $\mathcal{C} = 2^\Omega$ , a classe de todos subconjuntos de  $\Omega$ . Denotemos  $\sigma = (x_1, x_2, \dots, x_n)$ . Se a conclusão do corolário 4.1.15 fosse verdadeira nessa situação, ela implicaria indutivamente que  $\hat{R}_n(2^\Omega)(\sigma) = 0$ . Na realidade,

$$\hat{R}_n(2^\Omega)(\sigma) = \frac{1}{2},$$

atingindo o valor máximo, porque toda rotulagem de  $\sigma$  pode ser ajustada perfeitamente com um conceito  $C \in 2^\Omega$ .

Ao mesmo tempo, vamos ver em breve que o corolário 4.1.15 é “quase” verdadeiro, a menos de um pequeno termo de ajuste.

**Proposição 4.1.17** (Desigualdade de Jensen). *Seja  $\phi$  uma função real côncava, e seja  $X$  uma variável aleatória real. Então,*

$$\mathbb{E}(\phi(X)) \leq \phi(\mathbb{E}(X)).$$

A desigualdade é melhor ilustrada usando uma variável aleatória  $X$  tomando dois valores quaisquer,  $x$  e  $y$ , com as probabilidades  $P[X = x] = t$ ,  $P[X = y] = 1 - t$ . Neste caso,

$$\mathbb{E}(\phi(X)) = t\phi(x) + (1-t)\phi(y) \leq \phi(tx + (1-t)y) = \phi(\mathbb{E}(X)),$$

porque a linha que junta os pontos  $(x, \phi(x))$  e  $(y, \phi(y))$ , no gráfico de  $\phi$ , fica abaixo do gráfico, o que é exatamente a definição de uma função côncava. Este argumento se generaliza por indução sobre todas as combinações convexas finitas, e posteriormente o valor  $\mathbb{E}(\phi(X)) = \int f(x) d\mu(x)$  é aproximado pelos valores de  $\phi$  em combinações convexas finitas.

**Lema 4.1.18** (Lema de Massart). *Sejam  $\mathcal{F}$  uma classe de funções com valores no intervalo  $[-1, 1]$ , e  $\sigma$  uma amostra com  $n$  pontos. Suponha que  $k = \sharp(\mathcal{F} \upharpoonright \sigma) < \infty$ . Então,*

$$\hat{R}_n(\mathcal{F})(\sigma) \leq \sqrt{\frac{2 \log k}{n}}.$$

*Demonstração.* Denotemos a expressão à direita por  $\lambda$ . Identifiquemos  $\mathcal{F} \upharpoonright \sigma$  com o conjunto de todos os vetores  $v \in [-1, 1]^n$  dados por  $v_i = f(x_i)$ . Temos

$$\begin{aligned} \lambda n \hat{R}_n(\mathcal{F})(\sigma) &= \mathbb{E}_\eta \lambda \sup_{f \in \mathcal{F}} \sum_{i=1}^n \eta_i f(x_i) \\ &= \mathbb{E}_\eta \max_{v \in \mathcal{F} \upharpoonright \sigma} \lambda \langle \eta, v \rangle \\ &= \mathbb{E}_\eta \log \max_{v \in \mathcal{F} \upharpoonright \sigma} e^{\lambda \langle \eta, v \rangle} \\ (\text{Jensen}) &\leq \log \mathbb{E}_\eta \max_{v \in \mathcal{F} \upharpoonright \sigma} e^{\lambda \langle \eta, v \rangle} \\ &\leq \log \mathbb{E}_\eta \sum_{v \in \mathcal{F} \upharpoonright \sigma} e^{\lambda \langle \eta, v \rangle} \\ &= \log \sum_{v \in \mathcal{F} \upharpoonright \sigma} \mathbb{E}_\eta \prod_{i=1}^n e^{\lambda \eta_i v_i} \end{aligned}$$

A esperança do produto das variáveis aleatórias independentes é igual ao produto das esperanças (teorema de Fubini). Continuamos:

$$\begin{aligned} \lambda n \hat{R}_n(\mathcal{F})(\sigma) &\leq \log \sum_{v \in \mathcal{F} \upharpoonright \sigma} \prod_{i=1}^n \mathbb{E}_\eta e^{\lambda \eta_i v_i} \\ &= \log \sum_{v \in \mathcal{F} \upharpoonright \sigma} \prod_{i=1}^n \frac{1}{2} (e^{\lambda v_i} + e^{-\lambda v_i}) \\ (\text{exercício 1.4.1}) &\leq \log \sum_{v \in \mathcal{F} \upharpoonright \sigma} \prod_{i=1}^n e^{\lambda^2 v_i^2 / 2} \\ &\leq \log (k e^{n \lambda^2 / 2}) \\ &= \log k + \frac{n}{2} \lambda^2. \end{aligned}$$

Substituindo o valor original de  $\lambda$ , obtemos o resultado. □

**Lema 4.1.19.** *Seja  $\mathcal{F}$  uma classe de funções com valores no intervalo  $[-1, 1]$ . Então,*

$$\hat{R}_n(\mathcal{F} \cup \{0\}) \leq \hat{R}_n(\mathcal{F}) + \sqrt{\frac{2 \log 2}{n}}.$$

*Demonstração.* Seja  $f_0 \in \mathcal{F}$  um elemento qualquer. Nota-se que a classe  $\mathcal{F} - f_0$  contém zero. Usando corolário 4.1.15 e lema de Massart 4.1.18, obtemos:

$$\begin{aligned} \hat{R}_n(\mathcal{F} \cup \{0\}) &= \hat{R}_n((\mathcal{F} \cup \{0\}) - f_0) \\ &= \hat{R}_n((\mathcal{F} - f_0) \cup \{-f_0\}) \\ &\leq \hat{R}_n((\mathcal{F} - f_0) \cup \{0, -f_0\}) \\ &\leq \hat{R}_n(\mathcal{F} - f_0) + \hat{R}_n\{0, -f_0\} \\ &\leq \hat{R}_n(\mathcal{F}) + \sqrt{\frac{2 \log 2}{n}}. \end{aligned}$$

□

**Proposição 4.1.20.** *Sejam  $\mathcal{F}$  e  $\mathcal{G}$  duas classes de funções com valores no intervalo  $[-1, 1]$ . Então,*

$$\hat{R}_n(\mathcal{F} \cup \mathcal{G}) \leq \hat{R}_n(\mathcal{F}) + \hat{R}_n(\mathcal{G}) + 2\sqrt{\frac{2 \log 2}{n}}.$$

*Demonstração.*

$$\begin{aligned} \hat{R}_n(\mathcal{F} \cup \mathcal{G}) &\leq \hat{R}_n((\mathcal{F} \cup \{0\}) \cup (\mathcal{G} \cup \{0\})) \\ &\leq \hat{R}_n(\mathcal{F} \cup \{0\}) + \hat{R}_n(\mathcal{G} \cup \{0\}) \\ &\leq \hat{R}_n(\mathcal{F}) + \hat{R}_n(\mathcal{G}) + 2\sqrt{\frac{2 \log 2}{n}}. \end{aligned}$$

□

**Exercício 4.1.21.** Para uma classe de funções sobre um domínio  $\Omega$ , denotemos por  $\text{conv}(\mathcal{F})$  a *envoltória convexa* de  $\mathcal{F}$ , ou seja, o menor conjunto convexo do espaço linear  $\mathbb{R}^\Omega$  que contém  $\mathcal{F}$ :

$$\text{conv}(\mathcal{F}) = \left\{ \sum_{i=1}^n \lambda_i f_i : n \in \mathbb{N}, \lambda_i \geq 0, \sum \lambda_i = 1, f_i \in \mathcal{F} \right\}.$$

Nota-se que se  $\mathcal{F}$  consiste de funções borelianas com valores num intervalo  $[a, b]$ , então o mesmo vale para  $\text{conv}(\mathcal{F})$ . Mostrar que  $\hat{R}_n(\text{conv}(\mathcal{F})) = \hat{R}_n(\mathcal{F})$ .

**Exercício 4.1.22.** Deduzir que, dada uma classe  $\mathcal{F}$  de funções com valores no intervalo  $[-1, 1]$ , a sua *envoltória convexa simétrica* satisfaz

$$\hat{R}_n(\text{conv}(\mathcal{F} \cup -\mathcal{F})) \leq 2\hat{R}_n(\mathcal{F}) + 2\sqrt{\frac{2 \log 2}{n}}.$$

Já o seguinte resultado não é completamente trivial.

**Lema 4.1.23.** Dada uma classe  $\mathcal{F}$ , denotemos  $|\mathcal{F}| = \{f : f \in \mathcal{F}\}$ . Então,

$$\hat{R}_n(|\mathcal{F}|) \leq \hat{R}_n(\mathcal{F}).$$

*Demonstração.* Omitindo o fator  $1/n$ , temos a desigualdade a mostrar para uma amostra qualquer,  $\sigma = (x_1, x_2, \dots, x_n)$ :

$$\mathbb{E}_\eta \sup_{f \in \mathcal{F}} \sum_{i=1}^n \eta_i |f(x_i)| \leq \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \sum_{i=1}^n \eta_i f(x_i). \quad (4.8)$$

A chave para a prova é dada pelo argumento no caso mais simples de  $n = 1$ . Temos:

$$\begin{aligned} \frac{1}{2} \left[ \sup_{f \in \mathcal{F}} |f(x_1)| + \sup_{f \in \mathcal{F}} (-1)|f(x_1)| \right] &= \frac{1}{2} \sup_{f, g \in \mathcal{F}} (|f(x_1)| - |g(x_1)|) \\ \text{[ porque } |a| - |b| &\leq |a - b| \text{ ]} &\leq \frac{1}{2} \sup_{f, g \in \mathcal{F}} |f(x_1) - g(x_1)| \\ \text{[ é claro que o módulo pode ser suprimido ]} &= \frac{1}{2} \sup_{f, g \in \mathcal{F}} (f(x_1) - g(x_1)) \\ &= \frac{1}{2} \left[ \sup_{f \in \mathcal{F}} f(x_1) + \sup_{f \in \mathcal{F}} (-1)f(x_1) \right]. \end{aligned}$$

No caso de  $n$  qualquer, nós simplesmente aplicamos o mesmo jeito a cada coordenada,

uma após a outra, começando com  $i = 1$ :

$$\begin{aligned}
\mathbb{E}_\eta \sup_{f \in \mathcal{F}} \sum_{i=1}^n \eta_i |f(x_i)| &= \frac{1}{2} \mathbb{E}_{\eta_2, \dots, \eta_n} \left[ \sup_{f \in \mathcal{F}} \left( |f(x_1)| + \sum_{i=2}^n \eta_i |f(x_i)| \right) + \right. \\
&\quad \left. \sup_{f \in \mathcal{F}} \left( -|f(x_1)| + \sum_{i=2}^n \eta_i |f(x_i)| \right) \right] \\
&= \frac{1}{2} \mathbb{E}_{\eta_2, \dots, \eta_n} \sup_{f, g \in \mathcal{F}} \left[ |f(x_1)| - |g(x_1)| + \sum_{i=2}^n \eta_i |f(x_i)| + \sum_{i=2}^n \eta_i |g(x_i)| \right] \\
&\leq \frac{1}{2} \mathbb{E}_{\eta_2, \dots, \eta_n} \sup_{f, g \in \mathcal{F}} \left[ f(x_1) - g(x_1) + \sum_{i=2}^n \eta_i |f(x_i)| + \sum_{i=2}^n \eta_i |g(x_i)| \right] \\
&= \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \left[ \eta_1 f(x_1) + \sum_{i=2}^n \eta_i |f(x_i)| \right] \\
&\leq \dots \\
&\leq \mathbb{E}_\eta \sup_{f \in \mathcal{F}} \sum_{i=1}^n \eta_i f(x_i).
\end{aligned}$$

□

**Exercício 4.1.24.** Generalizar o argumento acima para mostrar a *desigualdade de contração de Ledoux–Talagrand*. Seja  $\phi: \mathbb{R} \rightarrow \mathbb{R}$  uma função Lipschitz contínua de constante  $L \geq 0$ , e  $\mathcal{F}$  uma classe de funções reais no domínio  $\Omega$ . Denotemos

$$\phi \circ \mathcal{F} = \{\phi \circ f : f \in \mathcal{F}\}.$$

Então,

$$\hat{R}_n(\phi \circ \mathcal{F}) \leq L \cdot \hat{R}_n(\mathcal{F}).$$

**Exercício 4.1.25.** Deduzir o seguinte. Seja  $\mathcal{C}$  e  $\mathcal{D}$  duas classes de Glivenko–Cantelli. Então, a classe

$$\mathcal{C} \Delta \mathcal{D} = \{C \Delta D : C \in \mathcal{C}, D \in \mathcal{D}\}$$

é uma classe de Glivenko–Cantelli, que satisfaz

$$R_n(\mathcal{C} \Delta \mathcal{D}) \leq R_n(\mathcal{C}) + R_n(\mathcal{D}) + 2\sqrt{\frac{2 \log 2}{n}}.$$

[ *Sugestão:*  $\chi_{C \Delta D} = |\chi_C - \chi_D| \cdot \cdot$  ]

**Exercício 4.1.26.** Deduzir que se  $\mathcal{C}$  é uma classe de Glivenko–Cantelli e  $D \subseteq \Omega$  um conceito qualquer, então a classe  $\mathcal{C} \Delta D = \{C \Delta D : C \in \mathcal{C}\}$  é a de Glivenko–Cantelli, tendo a mesma complexidade de Rademacher que  $\mathcal{C}$ :

$$\hat{R}_n(\mathcal{C} \Delta D) = \hat{R}_n(\mathcal{C}).$$

*Observação 4.1.27.* A definição da complexidade de Rademacher empírica na eq. (4.7) não é a única usada na literatura. Frequentemente, a complexidade de Rademacher é definida como a esperança da expressão

$$\sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right|.$$

Obviamente,

$$\hat{R}_n(\mathcal{F})(\sigma) \leq \mathbb{E}_\eta \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right|.$$

Ao mesmo tempo, as duas noções diferem já nos casos mais simples.

**Exemplo 4.1.28.** Como vimos no exercício 4.1.16, se  $\mathcal{C} = \{C\}$  é uma classe que consiste de um conceito só, temos

$$R_n(\mathcal{C}) = 0.$$

No entanto,

$$\mathbb{E}_\sigma \mathbb{E}_\eta \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right| = \mathbb{E}_\eta |\bar{w}| \mu(C),$$

um valor positivo de ordem de grandeza  $O(1/\sqrt{n})$ .

Portanto, as duas noções não são tão diferentes.

**Lema 4.1.29.** Se  $\mathcal{F}$  é uma classe que contém a função nula, então

$$\mathbb{E}_\eta \sup_{f \in \mathcal{F}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i) \right| \leq 2\hat{R}_n(\mathcal{F})(\sigma).$$

*Demonstração.* Seja  $\eta$  qualquer. Suponha que  $f \in \mathcal{F}$  é tal que

$$\left| \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i) \right| > 0.$$

Se a expressão sob o valor de módulo é positiva, este valor é atingido por  $\frac{1}{n} \sum_{i=1}^n \eta_i f(x_i)$ . Senão, ele é atingido por  $\frac{1}{n} \sum_{i=1}^n (-\eta_i) f(x_i)$ . Concluímos: existe um subconjunto  $A \subseteq \{\pm 1\}^n$  tal que  $\pm A = \{-1, 1\}^n$  (em particular,  $\mu_{\#}(A) \geq 1/2$ ), e para  $\eta \in A$ , os valores das expressões

$$\sup_{f \in \mathcal{F}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i) \right| \text{ e } \sup_{f \in \mathcal{F}} \frac{1}{n} \sum_{i=1}^n \eta_i f(x_i)$$

são idênticos. Como  $0 \in \mathcal{F}$ , a última expressão não é negativa.  $\square$

**Exercício 4.1.30.** Deduzir que, qualquer que seja uma classe de funções,  $\mathcal{F}$ , com valores em  $[-1, 1]$ ,

$$\mathbb{E}_{\eta} \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \eta_i \chi_C(x_i) \right| \leq 2\hat{R}_n(\mathcal{F}) + \sqrt{\frac{2 \log 2}{n}}.$$

*Observação 4.1.31.* A nossa definição de complexidades de Rademacher (sem valor absoluto) é mais natural por pelo menos duas razões. Ela tem um significado muito claro (observação 4.1.7). Além disso, o lema de Massart torna-se mais elegante.

*Observação 4.1.32.* Recordemos (obs. 4.1.11) que a complexidade de Rademacher,  $R_n(\mathcal{C}, \mu)$ , de uma classe de conceitos  $\mathcal{C}$  interpreta-se como a bondade de ajuste empírica esperada por  $\mathcal{C}$  de uma amostra rotulada aleatória. Segundo o nosso resultado principal (teorema 4.1.10), uma classe  $\mathcal{C}$  é de Glivenko–Cantelli se e somente se sua bondade de ajuste é assintoticamente nula, ou seja, ruim.

Esse resultado mostra que aprendizagem dentro uma classe de Glivenko–Cantelli é impossível? Não, porque na realidade nunca tentamos aprender nos baseando sobre uma rotulagem totalmente aleatória para cada amostra. Dentro do nosso modelo adotado, assumimos que a rotulagem é induzida por um conceito desconhecido, mas sempre o mesmo (ou mudando, mas devagar, como na noção recente do *concept drift*<sup>1</sup>). O fato de máquina de aprendizagem funcionar mal que alimentada com rotulagens aleatórias é um bom indicio, mostra-nos a sua estabilidade, e significa que a máquina não sofre o sobreajusto e vai generalizar bem.

## 4.2 Minimização da perda empírica

### 4.2.1

Vamos deduzir os primeiros corolários do teorema 4.1.10.

**Corolário 4.2.1.** *Seja  $\mathcal{C}$  uma classe de conceitos de Glivenko–Cantelli. Então  $\mathcal{C}$  é consistentemente PAC aprendizável. Se  $\mathcal{L}$  é uma regra de aprendizagem consistente com a*

<sup>1</sup>Que merece uma boa investigação matemática, baseada sobre a teoria de sistemas dinâmicos. O *concept drift* significa a mudança temporal do conceito a ser aprendido, ou seja, uma ação de  $\mathbb{R}_+$  sobre o espaço de conceitos.

classe  $\mathcal{C}$ , então para todo  $n$  e todo  $\delta > 0$ , dado um conceito  $C \in \mathcal{C}$ , temos, com confiança  $1 - \delta$ ,

$$\text{erro}_{\mu, C}(\mathcal{L}_n(C \uparrow \sigma)) \leq 2R_n(\mathcal{C}) + \frac{\sqrt{\ln(2/\delta)}}{\sqrt{2n}}.$$

*Demonstração.* Seja  $C \in \mathcal{C}$  qualquer. A classe  $\mathcal{C} \Delta C$  é Glivenko–Cantelli, com  $\hat{R}_n(\mathcal{C} \Delta C) = \hat{R}_n(\mathcal{C})$  (exercício 4.1.26). Como  $\mathcal{L}$  é consistente, para cada  $\sigma \in \Omega^n$  o erro empírico de aprendizagem é zero, e temos

$$\begin{aligned} \text{erro}_{\mu, C}(\mathcal{L}_n(C \uparrow \sigma)) &= \mu(\mathcal{L}_n(C \uparrow \sigma) \Delta C) \\ &= |\mu(\mathcal{L}_n(C \uparrow \sigma) \Delta C) - \mu_\sigma(\mathcal{L}_n(C \uparrow \sigma) \Delta C)| \\ \text{[ com confiança } 1 - \delta, \text{ por teor. 4.1.10 ]} &\leq 2R_n(\mathcal{C} \Delta C) + \sqrt{\frac{\ln(2/\delta)}{2n}} \\ &= 2R_n(\mathcal{C}) + \frac{\sqrt{\ln(2/\delta)}}{\sqrt{2n}}. \end{aligned}$$

□

*Observação 4.2.2.* No entanto, nem toda classe consistentemente aprendizável é uma classe de Glivenko–Cantelli. O contra-exemplo mais simples é a classe que consiste de todos os subconjuntos finitos do intervalo  $[0, 1]$  munido da medida de Lebesgue.

Seja  $\mathcal{L}$  uma regra consistente com a classe (ou mesmo uma regra qualquer tomando valores em  $\mathcal{C}$ ). Qualquer seja  $C \in \mathcal{C}$ ,

$$\text{erro}_{\mu, C} \mathcal{L}_n(C \uparrow \sigma) = \mu(\mathcal{L}_n(C \uparrow \sigma) \Delta C) = 0,$$

porque  $\mathcal{L}_n(C \uparrow \sigma) \Delta C$  é finito.

Ao mesmo tempo, esta classe não é de Glivenko–Cantelli. Nenhuma amostra  $\sigma$  vai estimar corretamente, por exemplo, a sua própria medida (mais exatamente, a do conceito  $\{x_i : \epsilon_i = 1\}$ ):

$$\sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| = \mu_\sigma(\sigma) - \mu(\sigma) = 1 - 0 = 1.$$

Mesmo assim, a intuição é que as classes consistentemente aprendizáveis não podem ser muito diferentes das classes de Glivenko–Cantelli. Talvez, num sentido, o exemplo acima exprima a única patologia possível. Seria interessante formular um critério necessário e suficiente. Vamos conjecturar um tal critério mais tarde (conjectura 4.3.16).

#### 4.2.2

Com alta confiança, a distância  $L^1$  empírica aproxima bem a distância  $L^1$  entre todos os pares de elementos de uma classe de Glivenko-Cantelli.



**Corolário 4.2.3.** *Seja  $\mathcal{C}$  uma classe de Glivenko-Cantelli. Dado  $\delta > 0$  e  $n$  quaisquer, com confiança  $1 - \delta$  temos*

$$\forall C, D \in \mathcal{C}, \mu(C \Delta D) \stackrel{\varepsilon}{\approx} \mu_{\sigma}(C \Delta D),$$

onde

$$\varepsilon = 2R_n(\mathcal{C}) + 2\sqrt{\frac{2 \log 2}{n}} + \sqrt{\frac{\ln(2/\delta)}{2n}}.$$

*Demonstração.* Usemos o exercício 4.1.25. □

**Exercício 4.2.4.** Formule e mostre o resultado mais geral para classes de funções.

Como toda classe PAC aprendizável, uma classe de Glivenko–Cantelli é precompacta. Isso pode ser estabelecido diretamente, sem passar pela aprendizabilidade.

**Corolário 4.2.5.** *Toda classe de Glivenko–Cantelli é precompacta na pseudométrica  $L^1(\mu)$ .*

*Demonstração.* O argumento é quase mesmo que na prova do teorema 3.3.9 de Benedek–Itai. Seja  $\varepsilon > 0$  qualquer, e  $\delta < 1$ . Suponha que os conceitos  $C_1, C_2, \dots, C_k$  formam um  $2\varepsilon$ -empacotamento na distância  $L^1(\mu)$ . Quando  $n \geq s(\varepsilon, \delta, \mathcal{C} \Delta \mathcal{C})$ , existe pelo menos uma amostra  $\sigma \in \Omega^n$  estimando as distâncias dois a dois entre  $C_i$  com a precisão  $\varepsilon$ . Segue-se que as imagens  $C_i \upharpoonright \sigma$  são dois a dois distintas, e por conseguinte  $k \leq 2^n$ . Concluimos:

$$D(2\varepsilon, \mathcal{C}, L^1(\mu)) \leq 2^{s(\varepsilon, \delta, \mathcal{C} \Delta \mathcal{C})}.$$

□

Já vimos um exemplo de uma classe precompacta que não é consistentemente aprendizável (exemplo 3.3.15). É fácil ver diretamente que esta classe não é de Glivenko–Cantelli, pela mesma razão que na observação 4.2.2.

### 4.2.3

É claro que o significado do corolário 4.2.1 é puramente teórico: não tem razão nenhuma para um conceito desconhecido pertencer à classe  $\mathcal{C}$ . Ainda assim, as noções, resultados, e provas podem ser adaptados simplesmente à situação seguinte mais realista.

**Definição 4.2.6.** Sejam  $\mathcal{C}$  uma classe de conceitos,  $D$  um conceito qualquer (ou seja, um subconjunto boreliano do domínio  $\Omega$ ), e  $\mu$  uma distribuição sobre  $\Omega$ . O erro de aprendizagem do conceito  $D$  pela classe  $\mathcal{C}$  com relação à medida  $\mu$  é a ínfima discrepância entre  $D$  e os ajustes de  $D$  em  $\mathcal{C}$ :

$$\text{erro}_{\mu, D}(\mathcal{C}) = \inf_{C \in \mathcal{C}} \mu(C \Delta D).$$

É uma função determinística sobre a família  $\mathcal{B}(\Omega)$  de todos os subconjuntos borelianos de  $\Omega$ , tomando os valores reais não negativos. Por exemplo, quando  $D \in \mathcal{C}$ , o valor  $\text{erro}_{\mu,D}(\mathcal{C})$  é nulo qualquer que seja a medida  $\mu$ . Ela mede o ínfimo de todos os erros de classificação atingidos quando aprendemos o conceito  $D$  usando a classe  $\mathcal{C}$ , com relação à medida subjacente  $\mu$ .

Visto que, na prática, não há como calcular os valores da função acima, conforma-se com o *erro de aprendizagem empírico*, onde a medida  $\mu$  é substituída com a medida empírica  $\mu_n$  suportada por uma amostra finita  $\sigma$ :

$$\text{erro}_{\mu_\sigma,D}(\mathcal{C}) = \inf_{C \in \mathcal{C}} \mu_\sigma(C \Delta D).$$

Neste caso, o ínfimo é sempre atingido, logo é o mínimo. A função de erro empírico é uma variável aleatória, porque ela depende da amostra aleatória  $\sigma$ .

**Definição 4.2.7.** Seja  $\mathcal{C}$  uma classe de conceitos. Diz-se que uma regra de aprendizagem,  $\mathcal{L}$ , segue o princípio de *minimização de erro empírico* (*empirical risk minimization, ERM*) dentro a classe  $\mathcal{C}$ , se existe uma sequência de constantes

$$(\varepsilon_n), \quad \varepsilon_n \geq 0, \quad \varepsilon_n \rightarrow 0 \text{ quando } n \rightarrow \infty,$$

tal que, para todo  $D \in \mathcal{B}(\Omega)$  e toda  $\sigma \in \Omega^n$ ,

$$\mu_\sigma(\mathcal{L}_n(\sigma, D \upharpoonright \sigma) \Delta D) \leq \text{erro}_{\mu_\sigma,D}(\mathcal{C}) + \varepsilon_n.$$

Desta maneira, a regra acha um ajuste empiricamente quase ótimo para  $D$ , com uma margem de erro permitido  $\varepsilon_n$ .

A prova do seguinte resultado mimetiza a do corolário 4.2.1.

**Teorema 4.2.8.** *Seja  $\mathcal{C}$  uma classe de conceitos, e seja  $\mathcal{L}$  uma regra de aprendizagem seguindo o princípio de minimização da perda empírica dentro  $\mathcal{C}$  com as constantes de erro  $(\varepsilon_n)$ . Quaisquer sejam  $n$  e  $\delta > 0$ , dado um subconjunto boreliano  $D \subseteq \Omega$  qualquer, uma amostra aleatória  $\sigma$  satisfaz, com confiança  $> 1 - \delta$ :*

$$\text{erro}_{\mu,D}(\mathcal{L}_n(D \upharpoonright \sigma)) \leq \text{erro}_{\mu_\sigma,D}(\mathcal{C}) + \varepsilon_n + 2R_n(\mathcal{C}) + \frac{\sqrt{\ln(2/\delta)}}{\sqrt{2n}}.$$

□

Desta maneira, assintoticamente, a regra  $\mathcal{L}$  provavelmente aproximadamente corretamente aprende, dentro a classe  $\mathcal{C}$ , um conceito boreliano,  $D$ , qualquer, atingindo no limite  $n \rightarrow \infty$  o menor erro teoricamente possível.

*Observação 4.2.9.* Eu não sei responder a pergunta seguinte. Seja  $\mathcal{C}$  uma classe consistentemente aprendizável sob a medida  $\mu$ . Seja  $\mathcal{L}$  uma regra satisfazendo o princípio de

minimização do erro empírico como na definição 4.2.7. Segue-se que para cada  $\epsilon, \delta > 0$  existe  $s = s(\epsilon, \delta)$  tal que, se  $n \geq s(\epsilon, \delta)$ , então, dado um subconjunto borealiano  $D \subseteq \Omega$  qualquer, temos

$$\text{erro}_{\mu, D} \mathcal{L}_n(D \uparrow \sigma) \leq \epsilon$$

com confiança  $1 - \delta$ ?

*Observação 4.2.10.* Enquanto as complexidades de Rademacher formam muito tempo uma ferramenta padrão na análise funcional e geometria de espaços de Banach, na teoria de aprendizagem estatística elas surgiram da forma explícita só recentemente [Bartlett e Mendelson 2002; Koltchinskii e Panchenko 2000; Mendelson 2002].

## 4.3 Entropia métrica e testemunha de irregularidade

### 4.3.1

Nessa seção, vamos discutir e mostrar o teorema seguinte, cujas condições (1)-(4) formam o resultado clássico de Vapnik–Chervonenkis [Vapnik e Červonenkis 1971], enquanto a condição (5) foi adicionada por Talagrand mais tarde [Talagrand 1984, 1996].

**Teorema 4.3.1.** *Seja  $\mathcal{C}$  uma classe de conceitos. As condições seguintes são equivalentes.*

1.  $\mathcal{C}$  é uma classe de Glivenko–Cantelli sob a medida  $\mu$ .
2. Para cada  $\epsilon > 0$ ,  $\frac{1}{n} \mathbb{E}_\sigma \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma)) \rightarrow 0$  quando  $n \rightarrow \infty$ .
3. Para cada  $\epsilon > 0$ ,  $\frac{1}{n} \mathbb{E}_\sigma \log \sharp(\mathcal{C} \uparrow \sigma) \rightarrow 0$  quando  $n \rightarrow \infty$ .

As condições seguintes também são duas a duas equivalentes:

( $\neg$  1)  $\mathcal{C}$  não é uma classe de Glivenko–Cantelli sob a medida  $\mu$ .

- (4) Existe  $\alpha > 0$  com a propriedade que, com alta confiança, uma amostra aleatória  $\sigma$  tem uma fração de  $\geq \alpha n$  pontos fragmentados por  $\mathcal{C}$ .
- (5) Existe um subconjunto  $A$  de medida estritamente positiva  $\alpha = \mu(A) > 0$  tal que  $\mu$ -quase toda  $n$ -upla de elementos de  $A$  é fragmentada por  $\mathcal{C}$ , qualquer que seja  $n$ .

O logaritmo aqui é a base 2.

### 4.3.2 Entropia métrica. (2) $\Rightarrow$ (1)

Mesmo se a precompactidade da classe  $\mathcal{C}$  “do ponto de vista” da medida  $\mu$  não é suficiente para ser Glivenko–Cantelli, a precompactidade de  $\mathcal{C}$  estimada “do ponto de vista coletivo” das medidas empíricas torna-se uma condição necessária e suficiente. É claro que para cada amostra  $\sigma$ , o número de cobertura  $N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))$  é limitado por

$2^n$ , e o logaritmo dele, por  $n$ . (Aqui, assumamos, pela conveniência, que o número de cobertura de  $\mathcal{C}$  seja estimado no espaço pseudométrico maior,  $(2^{\Omega}, L^1(\mu_{\sigma}))$ . De modo parecido calculamos o número de cobertura do conjunto  $\mathcal{C} \upharpoonright \sigma$  de todas as rotulagens induzidas por elementos de  $\mathcal{C}$ , no cubo de Hamming correspondente). A condição (2) diz que os logaritmos de números de cobertura divididos por  $n$  convergem para zero em probabilidade. Em outras palavras, a taxa média de crescimento de números de cobertura em relação com a medida empírica é subexponencial em  $n$ .

Com efeito, o limite na condição (2) existe para classes  $\mathcal{C}$  quaisquer.

**Lema 4.3.2** (Lema de Fekete (1923)). *Seja  $(a_n)$  uma seqüência subaditiva, ou seja,  $a_{m+n} \leq a_m + a_n$  para todos  $m, n \in \mathbb{N}_+$ . Então a seqüência  $(a_n/n)$  é convergente, com*

$$\lim_{n \rightarrow \infty} \frac{a_n}{n} = \inf_{n \in \mathbb{N}_+} \frac{a_n}{n}.$$

*Na forma rigorosamente equivalente, seja  $(a_n)$  uma seqüência submultiplicativa de reais positivos, ou seja,  $a_{m+n} \leq a_m a_n$ . Então a seqüência  $(a_n^{1/n})$  é convergente, com*

$$\lim_{n \rightarrow \infty} (a_n^{1/n}) = \inf_{n \in \mathbb{N}_+} (a_n^{1/n}).$$

*Demonstração.* A versão submultiplicativa é um pouco mais simples a manejar, porque só há um caso a ser considerado. Denotemos  $\alpha = \inf_{n \in \mathbb{N}_+} a_n^{1/n} \geq 0$ . Seja  $\varepsilon > 0$  qualquer. Existe  $k$  tal que  $|a_k^{1/k} - \alpha| < \varepsilon/2$ . Seja  $N$  tão grande que para todo  $i = 1, 2, \dots, k$   $(a_i^{1/N} - 1)a_k^{1/k} < \varepsilon/2$ . Agora, seja  $n \geq N$  qualquer. Pode-se escrever  $n = mk + i$ , onde  $0 \leq i < k$ . Temos:

$$\alpha \leq a_n^{1/n} \leq (a_k^m a_i)^{1/n} \leq a_k^{1/k} a_i^{1/N} < a_k^{1/k} + \varepsilon/2 < \alpha + \varepsilon.$$

A forma aditiva se infere exponenciando a seqüência subaditiva, e depois tomando o logaritmo. O caso onde  $\alpha = 0$  corresponde, para uma seqüência aditiva, ao limite  $-\infty$ .  $\square$

**Exercício 4.3.3.** *Seja  $\sigma = (x_1, x_2, \dots, x_m, x_{m+1}, \dots, x_{m+n})$  uma amostra de comprimento  $m + n$ . Denote por  $\sigma_m$  a amostra que consiste dos primeiros  $m$  elementos de  $\sigma$ , e por  $\sigma_n$ , a amostra dos elementos  $x_{m+1}, \dots, x_{m+n}$ . Mostre que*

$$N(\epsilon, \mathcal{C}, L^1(\mu_{\sigma})) \leq N(\epsilon, \mathcal{C}, L^1(\mu_{\sigma_m})) \times N(\epsilon, \mathcal{C}, L^1(\mu_{\sigma_n})).$$

**Exercício 4.3.4.** *Deduz que a seqüência de valores*

$$\mathbb{E}_{\sigma} \log N(\epsilon, \mathcal{C}, L^1(\mu_{\sigma}))$$

é subaditiva.

**Definição 4.3.5.** O valor

$$\begin{aligned}\mathcal{H}(\epsilon, \mathcal{C}, \mu) &= \lim_{n \rightarrow \infty} \frac{1}{n} \mathbb{E}_\sigma \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma)) \\ &= \inf_{n \in \mathbb{N}_+} \frac{1}{n} \mathbb{E}_\sigma \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))\end{aligned}$$

chama-se a *entropia métrica* da classe  $\mathcal{C}$  (em escala  $\epsilon > 0$ , sob a medida  $\mu$ ).

Então, a condição (2) diz que a entropia métrica de  $\mathcal{C}$  sob  $\mu$  é zero em cada escala.

**Exercício 4.3.6.** Mostre que a função

$$\hat{\mathcal{H}}(\epsilon, \mathcal{C}, \mu)(\sigma) = \frac{1}{n} \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))$$

(*entropia métrica empírica*) é Lipschitz contínua com a constante  $L \leq 1$  sobre  $\Omega^n$  com relação à distância de Hamming normalizada. Conclua que o valor da entropia empírica dá uma estimativa provavelmente aproximadamente correta (correndo o risco subgaussiano) para o valor da entropia métrica.

Note que o valor de complexidade de Rademacher empírica em uma amostra  $\sigma$  é completamente determinado pela restrição da classe  $\mathcal{C}$  sobre  $\sigma$ .

*Prova da implicação (2)  $\Rightarrow$  (1).* Fixemos uma amostra  $\sigma$  qualquer e estimemos o valor da complexidade empírica de Rademacher de  $\mathcal{C}$  em  $\sigma$ . Seja  $\epsilon > 0$  qualquer. Escolhemos uma  $\epsilon$ -rede,  $\mathcal{C}' \subseteq \{0, 1\}^n$ , com  $N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))$  elementos, para o espaço métrico  $\mathcal{C} \upharpoonright \sigma$  munido da distância de Hamming normalizada (ou seja, a distância  $L^1(\mu_\sigma)$ ). Segue-se que

$$\mathcal{C} \upharpoonright \sigma \subseteq \mathcal{C}' + B_\epsilon(0),$$

onde a bola aberta é formada no cubo de Hamming. Por conseguinte,

$$\begin{aligned}\hat{R}_n(\mathcal{C})(\sigma) &\leq \hat{R}_n(\mathcal{C}')(\sigma) + \hat{R}_n(B_\epsilon(0))(\sigma) \\ (\text{lema de Massart}) &\leq \sqrt{\frac{2 \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))}{n}} + \epsilon.\end{aligned}$$

A raiz quadrada é uma função côncava, logo a desigualdade de Jensen se aplica:

$$\begin{aligned}R_n(\mathcal{C}) &= \mathbb{E}_\sigma \hat{R}_n(\mathcal{C})(\sigma) \\ &\leq \mathbb{E}_\sigma \sqrt{\frac{2 \log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))}{n}} + \epsilon \\ &\leq \sqrt{2 \mathbb{E}_\sigma \frac{\log N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))}{n}} + \epsilon \\ &< 2\epsilon\end{aligned}$$

quando  $n$  é bastante grande graças à hipótese (2). □

### 4.3.3 Coeficiente de fragmentação médio. (3) $\Rightarrow$ (2)

A expressão em (3),

$$\frac{1}{n} \mathbb{E}_\sigma \log \#(\mathcal{C} \upharpoonright \sigma), \quad (4.9)$$

pode ser vista como uma variante média do coeficiente de fragmentação de  $\mathcal{C}$ :

$$s(n, \mathcal{C}) = \sup_{\sigma \in \Omega^n} \#(\mathcal{C} \upharpoonright \sigma).$$

É claro que

$$\frac{1}{n} \mathbb{E}_\sigma \log \#(\mathcal{C} \upharpoonright \sigma) \leq \frac{1}{n} \log s(n, \mathcal{C}).$$

Observemos que o limite na condição (3) existe pelas mesmas razões que na condição (2).

A condição (3) é formalmente mais forte do que a condição (2), porque a expressão em (3) domina a expressão na condição (2) para todo  $\varepsilon > 0$ . Por isso, (3)  $\Rightarrow$  (2) trivialmente.

### 4.3.4 Montante médio de fragmentação. ( $\neg 4$ ) $\Rightarrow$ (3) e (1) $\Rightarrow$ ( $\neg 4$ )

A quantidade  $\alpha \geq 0$  tal que uma amostra aleatória  $\sigma$  tenha uma parte com  $\sim \alpha n$  pontos fragmentada por  $\mathcal{C}$  foi introduzida por Vapnik e Chervonenkis. A propriedade reflete o princípio geral segundo o qual mais fragmentação significa estar mais longe de uma classe de Glivenko–Cantelli. (As médias de Rademacher são uma outra realização da mesma ideia). Por exemplo, se a classe  $\mathcal{C}$  tiver a dimensão VC finita, então  $\alpha = 0$ , qualquer que seja a medida subjacente  $\mu$ .

Primeiramente, vamos mostrar a existência da constante  $\alpha \geq 0$  para cada classe  $\mathcal{C}$ .

**Exercício 4.3.7.** Mostre que a sequência de reais

$$\mathbb{E}_{\sigma_n} \text{VC-dim}(\mathcal{C} \upharpoonright \sigma) = \mathbb{E}_{\sigma_n} \max\{d : \exists I \subseteq [n], \#I = d, \mathcal{C} \text{ fragmenta } \{x_i : i \in I\}\}$$

é subaditiva. Deduza que a sequência

$$\mathbb{E}_{\sigma_n} \frac{1}{n} \text{VC-dim}(\mathcal{C} \upharpoonright \sigma)$$

converge para um valor  $\alpha = \alpha(\mathcal{C}, \mu) \in [0, 1]$  quando  $n \rightarrow \infty$ .

**Exercício 4.3.8.** Mostre que a função

$$\sigma \mapsto \frac{1}{n} \text{VC-dim}(\mathcal{C} \upharpoonright \sigma)$$

é Lipschitz contínua sobre  $\Omega^n$  munido da distância de Hamming normalizada, com  $L = 1$ . Deduza que para qualquer  $\varepsilon > 0$ , se  $n$  for bastante grande, com alta confiança uma amostra aleatória tem um subconjunto de  $\geq (1 - \varepsilon)\alpha$  pontos fragmentado por  $\mathcal{C}$ .

*Prova da implicação  $(\neg 4) \Rightarrow (3)$ .* Suponha que  $\frac{d_\sigma}{n}$  converge para zero em probabilidade (ou: em esperança), onde  $d_\sigma = \text{VC-dim}(\mathcal{C} \upharpoonright \sigma)$  é a “dimensão VC empírica” da classe  $\mathcal{C}$ , uma variável aleatória. De acordo com o lema de Sauer-Shelah, segue-se que a variável aleatória

$$\begin{aligned} \frac{1}{n} \log \#(\mathcal{C} \upharpoonright \sigma) &\leq \frac{1}{n} \log \left( \frac{en}{d_\sigma} \right)^{d_\sigma} \\ &= \frac{d_\sigma}{n} \left( 1 - \log \frac{d_\sigma}{n} \right) \end{aligned} \quad (4.10)$$

converge para zero em probabilidade também.  $\square$

O caso importante é o onde a classe  $\mathcal{C}$  tem a dimensão VC finita. Neste caso,  $d_\sigma \leq d < \infty$ , e em particular, a entropia métrica converge para zero com uma taxa independente da medida  $\mu$ . É uma observação básica para *distribution-free learning*.

*Prova da implicação  $(1) \Rightarrow (\neg 4)$ .* Mostramos a contrapositiva:  $(4) \Rightarrow (\neg 1)$ . Suponha que, com alta confiança, uma amostra aleatória  $\sigma$  tem uma sub-amostra,  $\sigma_I$ ,  $I \subseteq [n]$ , fragmentada por  $\mathcal{C}$ , com  $|I| \geq \alpha n$  pontos. O valor da complexidade de Rademacher empírica,  $\hat{R}_{[\alpha n]}(\mathcal{C})(\sigma_I)$ , em  $\sigma_I$  atinge o valor máximo,  $1/2$ . É fácil de concluir que  $\hat{R}_n(\mathcal{C})(\sigma) \geq \alpha/2 > 0$ , com alta confiança. Por conseguinte, não ocorre a convergência em probabilidade de  $\hat{R}_n(\mathcal{C})$  para zero, e a classe  $\mathcal{C}$  não é G-C.  $\square$

### 4.3.5 Testemunha de irregularidade. $(5) \Rightarrow (4)$

Assumindo a condição (5), segundo a lei de grandes números, se  $n$  for bastante grande, então, com alta confiança, uma amostra aleatória contém uma fração de  $\sim \alpha n$  pontos que pertencem a  $A$ , logo, são fragmentados. Por conseguinte, (5) implica (4). Portanto, formalmente, a condição (5) é mais forte do que (4). Não somente uma proporção fixa de elementos de cada amostra é fragmentada, mas as amostras fragmentadas são bem situadas em  $\Omega$ . Deste modo, a condição (5) de Talagrand é bastante surpreendente.

**Definição 4.3.9.** Um subconjunto boreliano  $A$  de  $\Omega$  é dito *testemunha de irregularidade* se  $\mu(A) > 0$  e quase toda amostra finita de pontos de  $A$  é fragmentada, ou seja,

$$\forall n \in \mathbb{N}, \mu^{\otimes n} \{ \sigma = (x_1, \dots, x_n) \in A^n, \sigma \text{ não é fragmentada por } \mathcal{C} \} = 0.$$

A fragmentação entende-se como a de uma amostra *ordenada*:

$$\forall I \subseteq [n], \exists C \in \mathcal{C}, \forall i \in [n], i \in I \iff \chi_C(x_i) = 1.$$

Em particular, se  $\sigma$  é fragmentada por  $\mathcal{C}$ , então os elementos de  $\sigma$  são dois a dois distintos.

**Exercício 4.3.10.** Deduzir da nossa definição que uma testemunha de irregularidade nunca contém átomos.

### 4.3.6 (4) $\Rightarrow$ (4<sup>1/2</sup>), uma condição técnica intermediária

Neste momento, temos a equivalência das condições (1), (2), (3), e  $(\neg 4)$ , assim como a implicação (5)  $\Rightarrow$  (4). A última implicação que nos resta, (4)  $\Rightarrow$  (5), vai ser quebrada em duas. Definamos uma condição técnica intermediária.

(4<sup>1/2</sup>) *Seja  $A_n$  o subconjunto de  $\Omega^n$  de todas as amostras fragmentadas por  $\mathcal{C}$ . Então existe uma constante  $\alpha > 0$  tal que*

$$\forall n, \mu^{\otimes n}(A_n) \geq \alpha^n.$$

**Exercício 4.3.11.** Mostre que a sequência  $(\mu^{\otimes n}(A_n))$  é submultiplicativa, e deduza do lema de Fekete 4.3.2 que a sequência

$$(\mu^{\otimes n}(A_n))^{1/n}$$

converge para o seu ínfimo, o valor máximo de  $\alpha$  na propriedade acima. Denotemos

$$r((A_n)_{n=1}^{\infty}) = \lim_{n \rightarrow \infty} (\mu^{\otimes n}(A_n))^{1/n}.$$

As condições seguintes são equivalentes:

- para todos  $n$ ,  $\mu^{\otimes n}(A_n) \geq \alpha^n$ , e
- $r((A_n)_{n=1}^{\infty}) \geq \alpha$ .

*Prova da implicação (4)  $\Rightarrow$  (4<sup>1/2</sup>).* Seja  $n \in \mathbb{N}$  fixo qualquer. Para uma amostra aleatória  $W = (X_1, X_2, \dots, X_n)$ , onde  $X_i$  são elementos aleatórios i.i.d. do domínio  $\Omega$ , seguindo a lei  $\mu$ , vamos estimar por baixo a probabilidade do evento  $W \in A_n$ . A amostra  $W$  pode ser vista como o fragmento inicial de uma amostra aleatória com  $N$  elementos, onde  $N \geq n$ :

$$P[W \in A_n] = \mu^{\otimes N} \{ \sigma = (x_1, x_2, \dots, x_n, \dots, x_N) \in \Omega^N : \\ (x_1, x_2, \dots, x_n) \text{ é fragmentado por } \mathcal{C} \}.$$

Cada permutação  $\tau \in S_N$  de  $N$  coordenadas conserva a medida de produto  $\mu^{\otimes N}$ , e por conseguinte, qualquer que seja  $\tau$ ,

$$P[W \in A_n] = \mu^{\otimes N} \{ \sigma = (x_1, \dots, x_N) \in \Omega^N : (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado} \}.$$

Podemos igualmente, sem mudar o valor, tomar a esperança relativa a medida uniforme sobre o grupo  $S_N$  de permutações:

$$\begin{aligned} P[W \in A_n] &= \mathbb{E}_{\tau} \mu^{\otimes N} \{ \sigma \in \Omega^N : (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado} \} \\ &= \mathbb{E}_{\tau} \mathbb{E}_{\sigma \sim \mu^{\otimes N}} \chi \{ \sigma : (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado} \} \\ &= \mathbb{E}_{\sigma \sim \mu^{\otimes N}} \mathbb{E}_{\tau} \chi \{ \sigma : (x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado} \} \\ &= \mathbb{E}_{\sigma \sim \mu^{\otimes N}} P_{\tau} [(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado} \mid \sigma]. \end{aligned}$$



Usamos o “truque de condicionamento” (“conditioning trick”, veja observação H.4.2): na expressão interior os valores de  $\sigma$  são fixos,  $X_1 = x_2, X_2 = x_2, \dots, X_n = x_n$ , e a probabilidade refere-se ao espaço probabilístico finito  $S_N$  munido da medida uniforme,  $\mu_{\#}$ . Dada a amostra determinística,  $\sigma$ , escolhemos um subconjunto  $D \subseteq [n]$  da cardinalidade  $d = d(\sigma) = \text{VC-dim}(\mathcal{C} \upharpoonright \sigma)$ , fragmentado por  $\mathcal{C}$ . Agora, temos

$$P_{\tau}[(x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)}) \text{ é fragmentado}] \geq P[x_{\tau(1)}, x_{\tau(2)}, \dots, x_{\tau(n)} \in D].$$

Trata-se de um problema da primeira aula de um curso de probabilidade: uma urna contém  $N$  bolas, incluindo exatamente  $d$  vermelhas, e uma pessoa retira  $n$  bolas aleatoriamente. Qual é a probabilidade de que todas as bolas retiradas sejam vermelhas? A probabilidade é dada pela expressão

$$\frac{d}{N} \cdot \frac{d-1}{N-1} \cdot \frac{d-2}{N-2} \cdot \dots \cdot \frac{d-n+1}{N-n+1},$$

de onde

$$\begin{aligned} P[W \in A_n] &\geq \mathbb{E}_{\sigma \sim \mu^{\otimes N}} \frac{d(\sigma)}{N} \cdot \frac{d(\sigma)-1}{N-1} \cdot \frac{d(\sigma)-2}{N-2} \cdot \dots \cdot \frac{d(\sigma)-n+1}{N-n+1} \\ &\rightarrow \alpha^n \text{ quando } N \rightarrow \infty. \end{aligned}$$

□

### 4.3.7 Lema de Fremlin. (4<sup>1/2</sup>) $\Rightarrow$ (5)

**Lema 4.3.12.** *Sejam  $\Omega$  um conjunto e  $(A_n)$  uma sequência de subconjuntos,  $A_n \subseteq \Omega^n$ ,  $n \in \mathbb{N}_+$ . As condições seguintes são equivalentes.*

1. *Existe uma classe  $\mathcal{C}$  tal que para todo  $n$ ,  $A_n$  consiste de todas as amostras de comprimento  $n$  fragmentadas por  $\mathcal{C}$ .*
2. *Para todos  $m, n$ ,  $m \leq n$ , os conjuntos  $A_n$  são invariantes pelas permutações de coordenadas,*

$$\tau(A_n) \subseteq A_n, \quad \tau \in S_n,$$

*assim como pelas projeções:*

$$\pi_m^n(A_n) \subseteq V_m, \quad \text{onde } \pi_m^n(x_1, x_2, \dots, x_m, \dots, x_n) = (x_1, x_2, \dots, x_m).$$

*Demonstração.* A implicação (1)  $\Rightarrow$  (2) é evidente, e para mostrar (2)  $\Rightarrow$  (1), basta criar a classe  $\mathcal{C}$  que consiste de todos os conjuntos finitos  $\{x_1, x_2, \dots, x_n\}$  tendo a propriedade  $(x_1, x_2, \dots, x_n) \in A_n$ ,  $n \in \mathbb{N}$ . □

Vamos chamar provisoriamente (só dentro desta sub-seção) uma sequência  $(A_n)$  de conjuntos borelianos que possui uma das propriedades (1) ou (2) uma sequência *fragmentável*.

**Exercício 4.3.13.** Mostrar que cada medida boreliana sigma-aditiva,  $\mu$ , satisfaz a propriedade: se  $(B_n)$  é uma sequência decrescente de conjuntos borelianos encaixados, então

$$\mu(\cap_n B_n) = \lim \mu(B_n).$$

Uma propriedade análoga também tem lugar para as sequências crescentes.

**Lema 4.3.14.** *Seja  $(A_n)$  uma sequência fragmentável tal que  $\mu^{\otimes n}(A_n) \geq \alpha^n$ , ou seja,  $r(A_n) \geq \alpha$ , onde  $\alpha \in \mathbb{R}_+$ . Então existe uma sequência fragmentável  $(A'_n)$ , tal que  $A'_n \subseteq A_n$ ,  $r(A'_n) \geq \alpha$ , e  $(A'_n)$  é minimal com estas propriedades, ou seja, dado uma sequência fragmentável  $(W_n)$  tal que  $W_n \subseteq A'_n$  e  $r(W_n) \geq \alpha$ , temos para todo  $n$*

$$\mu^{\otimes n}(A'_n \setminus W_n) = 0.$$

*Demonstração.* Vamos definir  $A'_n$  recursivamente. Para  $n = 1$ , definamos

$$s = \sup_{(W_n)_n} \mu(A_1 \setminus W_1),$$

onde o supremo é formado sobre todas as sequências fragmentáveis  $(W_n)_{n=1}^{\infty}$  tendo as propriedades  $W_n \subseteq A_n$  e  $r(W_n) \geq \alpha$ . Se  $s = 0$ , então colocamos  $A'_1 = A_1$ . Se  $s > 0$ , então para cada  $k \in \mathbb{N}_+$  existe uma sequência fragmentável  $(W_n^k)$  tal que  $W_n^k \subseteq A_n$ ,  $\mu^{\otimes n}(W_n^k) \geq \alpha^n$ , e  $\mu(A_1 \setminus W_1^k) > s - 1/k$ . Verifica-se facilmente que a sequência de conjuntos

$$W_n = \bigcap_{k=1}^{\infty} W_n^k$$

é fragmentável, tenha a propriedade  $\mu^{\otimes n}(W_n) \geq \alpha^n$ , e qualquer que seja uma sequência fragmentável  $(Z_n)$  com  $\mu^{\otimes n}(Z_n) \geq \alpha^n$  e  $Z_n \subseteq A_n$ , tenhamos necessariamente  $\mu(W_1 \setminus Z_1) = 0$ . Escolhemos  $A'_1 = W_1$  e continuamos recursivamente.  $\square$

**Teorema 4.3.15** (Lema de Fremlin). *Seja  $\Omega$  um espaço probabilístico padrão, e seja  $(A_n)$  uma sequência fragmentável tal que*

$$\mu^{\otimes n}(A_n) \geq \alpha^n \text{ para todo } n.$$

*Então existe um conjunto boreliano,  $A \subseteq \Omega$ , tal que  $\mu(A) = \alpha$  e para todo  $n$ ,  $\mu^{\otimes n}(A_n \setminus A^n) = 0$ , ou seja, a menos de um conjunto negligenciável,  $A^n$  é contido em  $A_n$ .*

Vamos supor sem perda de generalidade que  $(A_n)$  é uma sequência fragmentável minimal com a propriedade  $r(A_n) \geq \alpha$ . Para cada  $x \in \Omega$  e  $n \in \mathbb{N}_+$ , definamos um conjunto boreliano  $A_{n,x}$ , como a fatia vertical de  $V_{n+1}$  sobre  $x$ :

$$A_{n,x} = \{\sigma \in \Omega^n : x\sigma \in A_{n+1}\},$$

onde  $x\sigma$  é a concatenação de  $x$  com  $\sigma$ . Verifica-se facilmente que a sequência  $(A_{n,x})$  é fragmentável e tem a propriedade  $A_{n,x} \subseteq A_n$ . Logo, o valor de  $r((A_{n,x})_n)$  é bem definido, e não pode ultrapassar  $\alpha$ :

$$r((A_{n,x})_n) = \lim_{n \rightarrow \infty} (\mu^{\otimes n} A_{n,x})^{1/n} \leq \alpha.$$

O nosso conjunto desejado é agora definido como segue:

$$A = \{x \in \Omega : r((A_{n,x})_n) = \alpha\}.$$

Primeiramente, vamos verificar que  $\mu(A) \geq \alpha$ . Para obter uma contradição, suponha que  $\mu(A) = \alpha' < \alpha$ . Usando o exercício 4.3.13, podemos escolher um valor  $\alpha_1$  tal que  $\alpha' < \alpha_1 < \alpha$  e

$$\mu\{x \in \Omega : r((A_{n,x})_n) \geq \alpha_1\} < \alpha_1,$$

ou seja

$$\mu\{x \in \Omega : r((A_{n,x})_n) < \alpha_1\} \geq 1 - \alpha_1.$$

Definamos

$$B_n = \{x \in \Omega : \forall N \geq n, (\mu^{\otimes N} A_{N,x})^{1/N} < \alpha_1\}.$$

Usando exercício 4.3.13, concluímos:  $\lim_{n \rightarrow \infty} \mu(B_n) \geq 1 - \alpha_1$ . Por conseguinte, se  $n$  é bastante grande,

$$\mu(\Omega \setminus B_n) < \frac{1}{2}(\alpha + \alpha_1).$$

Temos

$$\begin{aligned} \mu^{\otimes(n+1)}(A_{n+1}) &= \int_{\Omega} \mu^{\otimes n}(A_{n,x}) d\mu(x) \\ &= \int_{B_n} + \int_{\Omega \setminus B_n} \\ &< \alpha_1^n + \frac{1}{2}(\alpha + \alpha_1) \mu^{\otimes n}(A_n) \\ &= \alpha^n \left( \frac{\alpha_1^n}{\alpha^n} + \frac{1}{2}(\alpha + \alpha_1) \frac{\mu^{\otimes n}(A_n)}{\alpha^n} \right) \\ &\leq \left( \frac{3}{4}\alpha + \frac{1}{4}\alpha_1 \right) \mu^{\otimes n}(A_n) \end{aligned}$$

quando  $n$  é bastante grande, porque  $\alpha_1^n/\alpha^n \rightarrow 0$ , enquanto  $\mu^{\otimes n}(V_n) \geq \alpha^n$ . Concluímos indutivamente: para  $n$  bastante grande e fixo, e  $N > n$  qualquer,

$$\mu^{\otimes(N)}(V_N) \leq \left( \frac{3}{4}\alpha + \frac{1}{4}\alpha_1 \right)^{N-n} \mu^{\otimes n}(A_n),$$

e por conseguinte,

$$r((A_N)_N) = \lim (\mu^{\otimes N}(A_N))^{1/N} \leq \frac{3}{4}\alpha + \frac{1}{4}\alpha_1 < \alpha,$$

uma contradição.

Então,  $\mu(A) \geq \alpha$ . Segundo a definição de  $A$ , para todo  $x \in A$ , a sequência fragmentável  $(A_{n,x})_{n=1}^{\infty}$  satisfaz  $r((A_{n,x})_n) = \alpha$  e  $A_{n,x} \subseteq A_n$ . Como  $(A_n)$  é minimal, temos  $\mu^{\otimes n}(A_n \setminus A_{n,x}) = 0$ . Segue-se, indutivamente em  $k$ , que qualquer que seja  $\zeta \in A^k$ ,  $\mu$ -quase certamente o conjunto

$$V_{n,\zeta} = \{\sigma \in \Omega^n : \zeta\sigma \in V_{n+k}\}$$

satisfaz a propriedade  $\mu^{\otimes n}(A_n \setminus V_{n,\zeta}) = 0$ . Mas isso implica que para todo  $k$ ,  $\mu$ -quase todas amostras  $\zeta \in A^k$  pertencem a  $A_n$ . O lema de Fremlin é mostrado.

A implicação procurada  $(4^{1/2}) \Rightarrow (5)$  segue-se imediatamente no caso onde  $A_n$  consistem de todas as amostras fragmentadas por  $\mathcal{C}$ . Isso termina a prova do teorema 4.3.1.

Agora pode-se formular a conjectura seguinte.

**Conjetura 4.3.16.** *Uma classe de conceitos  $\mathcal{C}$  é consistentemente PAC aprendizável sob uma medida de probabilidade  $\mu$  se e somente se, para cada testemunha de irregularidade  $A$ , o espaço métrico quociente da restrição  $\mathcal{C} \upharpoonright A$  na distância  $L^1(\mu|_A)$  é um conjunto unitário:*

$$\forall C, D \in \mathcal{C}, \mu((C \Delta D) \cap A) = 0.$$

**Exercício 4.3.17.** Mostre que as testemunhas de irregularidade podem ser muitas distintas no mesmo domínio, disjuntas ou parcialmente justapostas. Construir um exemplo de um espaço probabilístico padrão,  $(\Omega, \mu)$ , bem como uma classe de conceitos  $\mathcal{C}$ , tais que  $\Omega$  contém várias testemunhas de irregularidade.

Pode ser que, dado uma classe  $\mathcal{C}$  no domínio  $(\Omega, \mu)$ , existe uma aplicação quociente canônica  $\phi$  de  $\Omega$  para um outro espaço probabilístico,  $(\Upsilon, \nu)$ , munido de uma classe  $\mathcal{D}$ , de modo que  $\nu = \phi_*(\mu)$ ,  $\mathcal{C} = \phi^{-1}(\mathcal{D})$ , e  $\mathcal{C}$  é consistentemente PAC aprendizável se e somente se  $\mathcal{D}$  é Glivenko–Cantelli? Informalmente, uma tal aplicação hipotética,  $\phi$ , colaria cada testemunha de irregularidade em um ponto de  $\Upsilon$ .

## 4.4 Aprendizagem independente de distribuição

A parte mais importante da teoria da aprendizagem dentro de uma classe é a aprendizagem independente da distribuição subjacente (“distribution-free learning”). O conceito significa que a complexidade amostral não depende da medida  $\mu$ , e é uniforme sobre o conjunto  $P(\Omega)$  de todas as medidas de probabilidade borelianas. Esta abordagem justifica-se plenamente, dado que a medida  $\mu$  é geralmente desconhecida. Todas as noções e resultados principais tem versões uniformes, independentes de uma medida. Vamos começar as formulações.

**Definição 4.4.1.** Uma regra de aprendizagem  $\mathcal{L}$  é provavelmente aproximadamente correta (PAC) em relação à classe de conceitos  $\mathcal{C}$  (independentemente de medida), se para todo  $\epsilon > 0$ , todo  $C \in \mathcal{C}$  e toda medida de probabilidade boreliana  $\mu$  sobre  $\Omega$ ,

$$P[\mu(\mathcal{L}(\sigma, C \upharpoonright \sigma) \Delta C) > \epsilon] \rightarrow 0 \text{ uniformemente em } \mu \text{ e } C. \quad (4.11)$$

Em outras palavras,

$$\sup_{\mu \in P(\Omega)} \sup_{C \in \mathcal{C}} \mu^{\otimes n} \{ \sigma \in \Omega^n : \mu(\mathcal{L}(\sigma, C \upharpoonright \sigma) \Delta C) > \epsilon \} \rightarrow 0 \text{ quando } n \rightarrow \infty, \quad (4.12)$$

ou, usando uma notação mais econômica,

$$\sup_{\mu \in P(\Omega)} \mathbb{E}_{\sigma \sim \mu} \sup_{C \in \mathcal{C}} \text{erro}_{\mu, C} \mathcal{L}(C \upharpoonright \sigma) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Da maneira equivalente, existe uma função  $s(\epsilon, \delta)$  (*complexidade amostral* de  $\mathcal{L}$ , independente da medida) tal que para todo  $C \in \mathcal{C}$  e toda  $\mu \in P(\Omega)$ , uma amostra i.i.d.  $\sigma \sim \mu$  de tamanho  $n \geq s(\epsilon, \delta)$  satisfaz  $\mu(C \Delta \mathcal{L}(\sigma, C \upharpoonright \sigma)) < \epsilon$  com confiança  $\geq 1 - \delta$ .

**Definição 4.4.2.** Uma classe  $\mathcal{C}$  é PAC aprendizável se existe uma regra de aprendizagem PAC para  $\mathcal{C}$ , independente de medida.

*Observação 4.4.3.* A classe  $\mathcal{C}$  construída na subseção 3.4.2, que é PAC aprendizável sob toda medida de probabilidade  $\mu$  no domínio, não satisfaz a definição acima, pois cada vez a regra de aprendizagem é diferente, ou seja, ela depende da medida. De fato, a classe não é PAC aprendizável independentemente da medida, pois a taxa de aprendizagem, como foi mostrado, pode ser arbitrariamente lenta.

**Definição 4.4.4.** Uma classe  $\mathcal{C}$  é consistentemente PAC aprendizável se toda regra de aprendizagem consistente com  $\mathcal{C}$  é provavelmente aproximadamente correta, independentemente de medida.

Precisamos também formular uma versão uniforme (independente da medida) de uma classe de Glivenko–Cantelli.

**Definição 4.4.5.** Uma classe de conceitos,  $\mathcal{C}$ , sobre um domínio  $\Omega$  é uma *classe de Glivenko–Cantelli uniforme* se, dado  $\epsilon > 0$  (precisão) e  $\delta > 0$  (risco), existe um valor  $s = s(\epsilon, \delta, \mathcal{C})$  tal que, qualquer que seja  $n \geq s$ , temos para toda medida de probabilidade  $\mu$  sobre  $\Omega$ :

$$\mu^{\otimes n} \left[ \sup_{C \in \mathcal{C}} \left| \frac{1}{n} \sum_{i=1}^n \chi_C(X_i) - \mu(C) \right| > \epsilon \right] \leq \delta, \quad (4.13)$$

onde  $X_1, X_2, \dots, X_n$  são elementos aleatórios de  $\Omega$  i.i.d. distribuídos segundo a lei  $\mu$ .

De maneira equivalente e mais econômica,

$$\sup_{\mu \in P(\Omega)} \mathbb{E}_{\mu} \sup_{C \in \mathcal{C}} |\mu_{\sigma}(C) - \mu(C)| \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

O resultado seguinte é a pedra angular da teoria de aprendizagem dentro de uma classe [Blumer et al. 1989; Vapnik e Červonenkis 1971].

**Teorema 4.4.6.** *As seguintes proposições são equivalentes:*

1.  $\mathcal{C}$  é PAC aprendizável.
2.  $\mathcal{C}$  é consistentemente PAC aprendizável.
3.  $\mathcal{C}$  é uma classe de Glivenko–Cantelli uniforme.
4.  $\sup_{\mu \in \mathcal{P}(\Omega)} R_n(\mathcal{C}, \mu) \rightarrow 0$  quando  $n \rightarrow \infty$ .
5.  $\text{VC-dim}(\mathcal{C}) < \infty$ .

Vamos apresentar uma prova circular, no sentido anti-horário.

(1)  $\Rightarrow$  (5). Seja  $\mathcal{C}$  uma classe PAC aprendizável independentemente da medida, com a complexidade amostral  $s(\epsilon, \delta)$ . Qualquer seja a medida de probabilidade  $\mu$  sobre  $\Omega$ , segundo o teorema 3.3.9 de Benedek–Itai, temos

$$\log_2 D(2\epsilon, \mathcal{C}, L^1(\mu)) - 1 \leq s(\epsilon, \delta),$$

quando  $\delta \leq 1/2$ . Seja  $\sigma$  uma amostra com  $n$  pontos, fragmentada pela classe  $\mathcal{C}$ . Aplicando a desigualdade acima à medida empírica  $\mu = \mu_\sigma$ , ou seja, a medida uniforme suportada sobre  $\sigma$ , e usando a proposição 3.3.8 com  $\epsilon = 1/8$  e  $\delta = 1/2$ , deduzimos

$$\frac{n}{8} \leq \log_2 [s(1/8, 1/2)] + 1,$$

de onde

$$\text{VC-dim}(\mathcal{C}) \leq 8 \log_2 [s(1/8, 1/2)] + 1.$$

(5)  $\Rightarrow$  (4). Veja a subseção 4.3.3, eq. (4.10).

(4)  $\Rightarrow$  (3). Segue-se do teorema 4.1.10.

(3)  $\Rightarrow$  (2). Usamos o corolário 4.2.1. Note que a taxa de aprendizagem é uniforme para todas as regras de aprendizagem consistentes.

(2)  $\Rightarrow$  (1). Segue da observação seguinte.

**Proposição 4.4.7.** *Cada classe  $\mathcal{C}$  admite pelo menos uma regra de aprendizagem consistente.*

*Demonstração.* Uma forma equivalente do Axioma de Escolha (AC) diz que todo conjunto  $X$  admite uma boa ordem, ou seja, uma ordem total,  $<$ , tal que cada subconjunto não vazio de  $X$  tem o elemento mínimo com relação à ordem  $<$ :

$$\forall Y, \emptyset \neq Y \subseteq X \Rightarrow \exists y \in Y \forall z \in Y y < z.$$

Fixemos uma tal ordem sobre  $\mathcal{C}$ . Dada uma amostra  $\sigma$  rotulada por um conceito que pertence a  $\mathcal{C}$ , a família  $\mathcal{C}_\sigma$  de todos os conceitos  $C$  induzindo a mesma rotulagem sobre  $\sigma$  não é vazia, logo possui o elemento minimal, que escolhemos como  $\mathcal{L}(\sigma)$ . A regra  $\mathcal{L}$  é consistente.  $\square$

(Vamos re-examinar este resultado na próxima seção.)

**Exercício 4.4.8.** Nós já caracterizamos as classes  $\mathcal{C}$  que possuem a propriedade de Glivenko–Cantelli (uniforme) sob a classe de todas as medidas, assim como sob a medida fixa. As primeiras são as de dimensão VC finita, as últimas são as classes que não possuem a testemunha de irregularidade de Talagrand. Ambas propriedades estão limitando a quantidade de fragmentação pela classe. Agora estude o problema seguinte: quais condições sobre uma classe  $\mathcal{C}$ , também expressadas na linguagem de fragmentação, são necessárias e suficientes para  $\mathcal{C}$  possuir a propriedade de Glivenko–Cantelli uniforme sob a classe de todas as medidas *não atômicas*?

O problema foi sugerido em [Vidyasagar 2003], problema 12.8. Depois de refletir um pouco, você pode comparar a sua solução com a sugerida em [Pestov 2013c].

## 4.5 Tomar cuidado com a mensurabilidade

Nesta seção, vamos fazer algo de paradoxal: construiremos contra-exemplos aos teoremas principais deste capítulo.

### 4.5.1 Dois contra-exemplos

Lembramos que uma ordem total,  $\preceq$ , é chamada uma *boa ordem* se todo subconjunto não vazio de  $\Omega$  tem mínimo. Uma boa ordem sobre  $X$  é *minimal* se todo segmento aberto inicial,  $\{x \in X : x < y\}$ , tem a cardinalidade estritamente menor do que  $X$ . Para um conjunto  $X$  infinito, a condição equivalente é que todo segmento fechado inicial,

$$I_x = \{y \in X : y \preceq x\},$$

tem a cardinalidade estritamente menor do que a de  $X$ .

Segundo uma forma equivalente do Axioma de Escolha (AC), o *Princípio de Boa Ordem* (*Well-Ordering Principle*), todo conjunto admite uma boa ordem minimal (seção B.3.4).

**Exemplo 4.5.1** (Durst e Dudley [1980], Proposition 2.2). Assumamos a Hipótese do Contínuo (CH). Ou seja, não existem cardinalidades estritamente intermediárias entre a cardinalidade de  $\mathbb{N}$  e a de  $\mathbb{R}$  (seção B.2.3).

Seja  $\Omega$  um espaço boreliano padrão não enumerável, isto é, um espaço boreliano isomorfo ao intervalo  $[0, 1]$ . Escolhemos uma boa ordem minimal,  $\preceq$ , sobre  $\Omega$ . É útil a observar que a ordem  $\preceq$  não tem nada a ver com as ordens usuais bem conhecidas, tais como a ordem usual,  $\leq$ , sobre  $\mathbb{R}$ . Sob a Hipótese do Contínuo, todo segmento fechado inicial,  $I_y$ , tendo uma cardinalidade menor que  $c = 2^{\aleph_0}$ , é enumerável. Formamos uma classe de conceitos  $\mathcal{C}$  que consiste de todos os segmentos iniciais,  $I_y$ ,  $y \in \Omega$ . É claro que a dimensão VC da classe  $\mathcal{C}$  é um.

Agora, seja  $\mu$  uma medida de probabilidade boreliana não atômica sobre  $\Omega$  (por exemplo, a medida de Lebesgue sobre o intervalo  $[0, 1]$ ). Sob CH, todo elemento de  $\mathcal{C}$  é um conjunto enumerável, logo boreliano, de medida zero (um conjunto nulo).

Ao mesmo tempo, para cada amostra finita  $\sigma$ , existe um segmento inicial  $I_y \in \mathcal{C}$  que contém todos os elementos de  $\sigma$ : basta definir  $y = \max_{<} \{x_1, x_2, \dots, x_n\}$ . A medida empírica de  $C$  com relação a  $\sigma$  é um. Concluímos: nenhuma amostra finita pode advinhar a medida de todos os elementos de  $\mathcal{C}$  com uma precisão  $\epsilon < 1$  qualquer e uma confiança não nula. A classe  $\mathcal{C}$  não é uma classe de Glivenko–Cantelli, apesar de ter a dimensão VC um.

*Observação 4.5.2.* Com efeito, no exemplo acima, CH não é necessária, o mesmo argumento é válido sobre uma hipótese bem mais fraca, o Axioma de Martin (MA). Eu não sei se um exemplo com as mesmas propriedades pode ser construído dentro o sistema ZFC, sem hipóteses conjuntísticas adicionais.

O exemplo pode ser modificado, para obter um exemplo de uma classe de conceitos de dimensão VC finita (um) que não é consistentemente PAC aprendizável.

**Exemplo 4.5.3** (Blumer et al. [1989], p. 953). Mais uma vez, sobre CH, adicione à classe de conceitos  $\mathcal{C}$  do exemplo 4.5.1 o conjunto  $\Omega$  como um elemento. Denotemos a nova classe  $\mathcal{C}' = \mathcal{C} \cup \{\Omega\}$ . Sempre temos  $\text{VC-dim}(\mathcal{C}') = 1$ . A toda amostra finita rotulada,  $(\sigma, \tau)$ , associamos a hipótese

$$\mathcal{L}(\sigma, \tau) = I_z, \quad z = \max_{<} \tau. \quad (4.14)$$

É fácil a ver que a regra de aprendizagem  $\mathcal{L}$  é consistente com a classe  $\mathcal{C}'$ .

Ao mesmo tempo,  $\mathcal{L}$  não é provavelmente aproximadamente correta. Para o conceito  $C = \Omega$  a regra  $\mathcal{L}(\sigma, \Omega \upharpoonright \sigma) = \mathcal{L}(\sigma, \sigma)$  vai sempre gerar um conceito enumerável da forma  $I_y$ ,  $y = \max \sigma$ . Por conseguinte, quando a medida  $\mu$  é não atômica,  $\mu(\Omega \Delta I_y) = \mu(\Omega \setminus I_y) = 1$ . O conceito  $C = \Omega$  não pode ser aprendido com a precisão  $\epsilon < 1$  e uma confiança não nula. Ao mesmo tempo, a dimensão VC da classe  $\mathcal{C}'$  é um.

Como é possível que os mesmos resultados possam ser mostrados e refutados ao mesmo tempo? Onde reside o problema? A fim de entender a situação, vamos discutir um paradoxo importante, descoberto na matemática bastante recentemente.

## 4.5.2 Paradoxo de Chris Freiling: uma “refutação” da Hipótese do Contínuo

Vamos discutir um argumento notável contra a validade da Hipótese do Contínuo, sugerido por Chris Freiling [Freiling 1986].

Considere uma experiência mental de *jogar dardo*, que está entre os passatempos favoritos de probabilistas (em terceiro lugar somente depois de lançar a moeda e lançar um dado). Você joga um dardo em um alvo, por exemplo, o quadrado de lado unitário,  $[0, 1]^2$ . O resultado de uma experiência é um ponto,  $x \in [0, 1]^2$ , atingido pelo dardo. Suponha



que a probabilidade de atingir uma região,  $A$ , é proporcional à área (a medida uniforme) dela:

$$P[X \in A] = \text{area}(A) = \lambda^{\otimes 2}(A),$$

onde  $\lambda^{\otimes 2}$  é a medida de Lebesgue. Desse modo, a distribuição de pontos atingidos pelo dardo segue a lei uniforme no quadrado. Em particular, a medida uniforme (de produto) é não atômica: a probabilidade de atingir um ponto particular é zero.

Suponha que a Hipótese do Contínuo seja válida. Como uma consequência, existe uma boa ordem  $<$  sobre o quadrado,  $[0, 1]^2$ , com a propriedade de que, qualquer que seja  $x \in [0, 1]^2$ , o conjunto de pontos que precedem  $x$ ,

$$I_x = \{y \in [0, 1]^2 : y \preceq x\},$$

é enumerável:

$$\forall x \in [0, 1]^2, |I_x| \leq \aleph_0.$$

Lembremos, mais uma vez, que esta ordem não é construtiva, não há algum algoritmo para construí-la. É uma ordem cuja existência segue do Axioma de Escolha (página 294) (o Princípio de Boa Ordem de Zermelo B.3.14).

Suponha agora dois jogadores de dardo, A e B, ou (no espírito da criptografia de chave pública), Alice e Bob, estão jogando dardos, independentemente um do outro. Em outras palavras, há dois independentes variáveis aleatórias,  $X$  e  $Y$ , distribuídas uniformemente no quadrado  $[0, 1]^2$ .

Lembra-se que a independência de variáveis aleatórias  $X$  e  $Y$  significa que para cada par de subconjuntos borelianos do quadrado, digamos  $\Pi_1$  e  $\Pi_2$ , os eventos  $[X \in \Pi_1]$  e  $[Y \in \Pi_2]$  são independentes, ou seja,

$$P[X \in \Pi_1 \wedge Y \in \Pi_2] = P[X \in \Pi_1] \cdot P[Y \in \Pi_2].$$

Por conseguinte, não importa se Alice lança seu dardo primeiro, ou Bob faz: de nenhum jeito isto afetará o resultado da experiência. Por exemplo, pode ser que Alice tem jogado o seu dardo há dez anos, o resultado (um elemento  $x \in [0, 1]^2$ ) foi gravado e mantido em segredo, e agora Bob lança seu dardo, e depois os resultados nos são encaminhados simultaneamente, em envelopes selados, por pessoas diferentes. É possível também que Alice e Bob não saibam da existência um do outro, e mesmo que viverem – e jogarem dardos – em duas extremidades diferentes da terra.

Em qualquer caso, depois de eles jogarem dardos, recebemos dois números:  $a \in [0, 1]^2$  para Alice, e  $b \in [0, 1]^2$  para Bob. Há duas possibilidades:  $a \preceq b$  ou  $b \preceq a$ . Consideraremos ambos os casos.

Suponha primeiro que  $a \preceq b$ . Como os dois eventos eram independentes, podemos assumir sem perda de generalidade que Alice jogou seu dardo primeira. Qual é a probabilidade de que, quando  $a$  for fixado, o resultado do Bob preceder  $a$ ? Como o conjunto de predecessores de  $a$ , que nós denotamos  $S_a$ , à enumerável, a probabilidade do evento é zero:

$$P[Y \in I_a] = 0.$$

É um evento improvável.

Agora suponha que  $b \leq a$ . Dessa vez, podemos assumir igualmente bem que Bob tinha jogado seu dardo primeiro e nós tenhamos o seu resultado,  $b$ . Qual é a probabilidade de que o resultado de Alice seja menor do que o do Bob,  $a \leq b$ ? O conjunto  $I_b$  é também enumerável, logo

$$P[X \in I_b] = 0.$$

Deste modo, concluímos que ambos os resultados,  $a < b$  e  $b < a$ , são improváveis. Por conseguinte, o evento

$$(a < b) \vee (b < a)$$

é improvável. Mas claramente *ou*  $a \leq b$  *ou*  $b < a$  sempre acontece, então a probabilidade do evento acima deve ser um! Chegamos a uma contradição. Ela resulta da Hipótese do Contínuo. Concluímos: a CH é falsa.  $\square$

O argumento de Freiling *refuta* a CH? Não realmente: enganamos um pouquinho. Se você olhar para a “impressão fina” do argumento, torna-se claro que ele não é uma boa prova rigorosa.

Queremos falar da probabilidade do evento que o resultado da primeira experiência precede, com relação à ordem  $<$ , o resultado da segunda experiência:  $a \leq b$ . Ou seja, estamos interessados na probabilidade do evento

$$[X \leq Y].$$

A probabilidade é igual à medida uniforme do conjunto de todos os pares  $(a, b) \in [0, 1]^2 \times [0, 1]^2$  tendo a propriedade  $a \leq b$ :

$$P[X \leq Y] = \lambda^{\otimes 2}\{(a, b) : a \leq b\} \subseteq [0, 1]^2 \times [0, 1]^2.$$

É neste momento particular que o nosso argumento intuitivo perde o rigor matemático: o conjunto acima, ou seja, o gráfico da relação  $\leq$ , não é mensurável, e não pode ser atribuído nenhum valor da medida! A probabilidade do evento  $[X \leq Y]$  é indefinida. O argumento de Freiling não pode ser traduzido em uma prova.

Concretamente, denotemos

$$A = \{(a, b) : a \leq b\}.$$

Para todo  $b \in [0, 1]^2$ , a “fatia horizontal”,  $A_b = \{a \in [0, 1]^2 : (a, b) \in A\}$ , é enumerável, logo tem medida nula. Se  $A$  for mensurável, teríamos

$$\lambda^{\otimes 2}(A) = \int_{[0, 1]^2} \lambda(A_b) d\lambda(b) = 0,$$

e de modo semelhante, a medida do conjunto complementar seria nula também, uma contradição. O que o argumento de Freiling mostra, é só que  $A$  não é mensurável.

No entanto, o significado do argumento acima é muito maior do que um truque divertido. Estamos apenas nos atendo a um tecnicismo puro. E se um dia os matemáticos conseguirem construir uma nova base axiomática que incorporaria tanto os conjuntos quanto as

variáveis aleatórias em um fundamento, o argumento de Freiling se tornaria um *teorema*, mostrando rigorosamente que a Hipótese do Contínuo seja *falsa*.

Freiling ele mesmo propôs incorporar nos fundamentos da matemática um axioma adicional, o chamado *axioma da simetria* (AX).

Deixe-me concluir a sub-seção com uma opinião sobre o argumento de Freiling pertencente à David Mumford [Mumford 2000].

*“Why is not this result as widely known as Gödel’s and Cohen’s, I don’t know. (...) The Continuum Hypothesis is surely similar to the scholastic issue on how many angels can stand on the head of a pin: an issue which disappears if you change your point of view.”*

### 4.5.3 Classes universalmente separáveis

O paradoxo de Freiling nos dá uma chave para entender os exemplos aparentemente contraditórios: a Hipótese do Contínuo não combina bem com mensurabilidade. Examinando as provas de nossos teoremas desta seção, concluimos que o argumento de simetriação não funciona para a classe  $\mathcal{C}$  construída na subseção 4.5.1. Pode-se mostrar (usando o mesmo argumento simples que acima) que para nossa classe, a expressão

$$\mathbb{E}_{\sigma, \sigma' \sim \mu} \sup_{C \in \mathcal{C}} |\mu_{\sigma}(C) - \mu_{\sigma'}(C)|$$

é mal definida, pois a função

$$\sup_{C \in \mathcal{C}} |\mu_{\sigma}(C) - \mu_{\sigma'}(C)|$$

sobre  $\Omega^n \times \Omega^n$  não é mensurável. Isso mostra que algumas hipóteses de mesurabilidade adicionais sobre a classe de conceitos,  $\mathcal{C}$ , são inevitáveis.

Há muitas formas de contornar esta restrição. Escolhemos a mais simples delas, a noção de uma classe universalmente separável.

**Definição 4.5.4.** Uma família de conjuntos borelianos,  $\mathcal{C}$ , de um espaço boreliano padrão,  $\Omega$ , é *universalmente separável* se existe uma sub-família enumerável,  $\mathcal{C}'$ , tal que todo  $C \in \mathcal{C}$  é o limite de uma sequência  $(C_n)$  de elementos de  $\mathcal{C}'$  na topologia de convergência pontual:

$$\forall x \in \Omega, \exists N \forall n \geq N, \chi_{C_n}(x) = \chi_C(x).$$

(Diz-se que  $\mathcal{C}'$  é *universalmente denso* em  $\mathcal{C}$ ).

Vamos deixar como um exercício a verificação que para uma classe universalmente separável todos os conjuntos que aparecem nas provas deste capítulo são mensuráveis. De maneira ilustrativa, só vamos mostrar uma propriedade típica de mensurabilidade de tais classes.

**Proposição 4.5.5.** *Cada classe universalmente separável admite uma regra de aprendizagem consistente que satisfaz a condição de mensurabilidade seguinte. Para todo conjunto boreliano  $B \in \mathcal{B}$ , toda medida de probabilidade  $\mu \in P(\Omega)$ , e todo  $n \in \mathbb{N}_+$ , a função*

$$\Omega^n \ni \sigma \mapsto \mu(\mathcal{L}(\sigma, C \upharpoonright \sigma) \Delta B) \in \mathbb{R} \quad (4.15)$$

é mensurável.

*Demonstração.* Seja  $\mathcal{C}$  uma classe universalmente separável. Seleccionamos uma subclasse enumerável e universalmente densa de  $\mathcal{C}$ ,

$$\mathcal{C}' = \{C_1, C_2, \dots, C_n, \dots\}.$$

Definamos uma regra de aprendizagem,  $\mathcal{L}$ , como segue: dado uma amostra rotulada de tamanho  $n$ ,  $(\sigma, \tau)$ , definamos

$$\mathcal{L}_n(\sigma, \tau) = \begin{cases} \emptyset, & \text{se } \tau \notin \mathcal{C} \upharpoonright \sigma, \\ C_{\min\{k: C_k \upharpoonright \sigma = \tau\}}, & \text{caso contrário.} \end{cases}$$

Informalmente, o algoritmo examina todos os conceitos  $C_1, C_2, \dots$  nesta ordem, e para quando o conceito induzindo a rotulagem desejada for achado.

É fácil a ver que a classe  $\mathcal{C}'$  induz todas as mesmas rotulagens que  $\mathcal{C}$ :

$$\mathcal{C} \upharpoonright \sigma = \mathcal{C}' \upharpoonright \sigma.$$

Logo, a aplicação  $\mathcal{L}$  é bem-definida. É claro que a regra  $\mathcal{L}$  é consistente com a classe  $\mathcal{C}$ . Para verificar que  $\mathcal{L}$  satisfaz a condição de mensurabilidade, definamos para todo  $C \in \mathcal{C}$  e todo  $n$  o conjunto

$$A_C = \{(\sigma, \tau) : \sigma \in \Omega^n, \tau = C \upharpoonright \sigma\} \subseteq \Omega^n \times \{0, 1\}^n.$$

Dado um  $\tau \in \{0, 1\}^n$ , a “fatia vertical” correspondente de  $A_C$ ,

$$A_C \cap (\Omega^n \times \{\tau\}),$$

pode ser escrita como

$$C_1 \times C_2 \times \dots \times C_n \times \{\tau\},$$

onde  $C_i$  é igual a  $C$  se  $\tau_i = 1$  e  $C_i = \Omega \setminus C$  se  $\tau_i = 0$ . Por isso,  $A_C$  é um conjunto boreliano.

Definamos para todos  $k$

$$B_k = \{(\sigma, \tau) : \mathcal{L}_n(\sigma, \tau) = C_k\}$$

e

$$B_0 = \Omega \setminus \bigcup_{k=1}^{\infty} B_k.$$

Temos

$$B_1 = A_{C_1}, \quad B_2 = A_{C_2} \setminus A_{C_1}, \dots,$$

$$B_k = A_{C_k} \setminus \bigcup_{i=1}^{k-1} A_{C_i}, \dots,$$

logo todos os conjuntos  $B_k$  são borelianos, incluindo  $B_0$ . Eles formam uma partição boreliana enumerável de  $\Omega$ , e agora basta mostrar que a nossa função

$$\Omega \ni \sigma \mapsto \mu(\mathcal{L}(\sigma, C \upharpoonright \sigma) \Delta B) \in \mathbb{R},$$

é mensurável quando restrita sobre cada pedaço boreliano,  $B_k$ , desta partição. Mas sobre cada pedaço, a função é constante: sobre  $B_k$ ,  $k \geq 1$  ela toma o valor

$$\mu(C_k \Delta B),$$

enquanto sobre  $B_0$  ela toma o valor  $\mu(B)$ . □

O seguinte pode ser mostrado com algumas modificações cosméticas.

**Proposição 4.5.6.** *Toda classe  $\mathcal{C}$  universalmente separável admite uma regra de aprendizagem  $\mathcal{L}$  mensurável que segue o princípio de minimização de perda empírica.* □

Desse modo, segue-se que todos os resultados de nosso capítulo restam válidos sob a hipótese de que a classe  $\mathcal{C}$  seja universalmente separável.

*Observação 4.5.7.* É interessante que, sob CH (ou MA), pode-se mostrar [Pestov 2011] que a classe  $\mathcal{C}'$  do exemplo 4.5.3 é PAC aprendizável independentemente da medida.

Redefinamos a boa ordem sobre  $\mathcal{C} = \{I_x : x \in \mathbb{R}\} \cup \{\Omega\}$  fazendo  $\Omega$  o elemento minimal (em vez do maximal), e preservando a relação de ordem entre outros elementos. Denotemos a nova ordem  $<_1$ . Definamos a regra de aprendizagem  $\mathcal{L}_1$  de mesmo modo que na eq. (4.14), mas dessa vez o mínimo é entendido no sentido da ordem  $<_1$ :

$$\mathcal{L}_1(\sigma, \tau) = \min_{(<_1)} \left\{ C \in \mathcal{C} : C \upharpoonright \sigma = \bigcap_{\tau \subseteq D} D \right\}. \quad (4.16)$$

Para ver o que faz a diferença, seja  $\mu$  uma medida não atômica sobre  $\Omega$ . Se  $C = \Omega$ , então para toda amostra  $\sigma$  consistentemente rotulada com  $\Omega$  a regra  $\mathcal{L}_1$  vai produzir  $C$ , porque é o conceito mínimo induzindo a rotulagem consistente. Se  $C \neq \Omega$ , então para  $\mu$ -quase todas amostras  $\sigma$  a rotulagem sobre  $\sigma$  produzida por  $C$  é vazia, é o conceito  $\mathcal{L}_1(\sigma, \emptyset)$  gerado pela regra  $\mathcal{L}_1$ , enquanto possivelmente diferente de  $C$ , será um conceito enumerável, significando que  $\mu(C \Delta \mathcal{L}(\sigma, \emptyset)) = 0$ .

Para dar uma prova formal que  $\mathcal{L}_1$  é PAC, note que, quaisquer que sejam  $C \in \mathcal{C}'$  e  $n \in \mathbb{N}$ , a coleção de conceitos dois a dois distintos  $\mathcal{L}_1(\sigma \upharpoonright C)$ ,  $\sigma \in \mathbb{R}^n$  é enumerável

(sob CH), pois elas são todos contidos no segmento inicial da ordem  $<_1$  do conjunto  $\mathcal{C}$  de cardinalidade contínuo. Por conseguinte, a classe de conceitos

$$\mathcal{L}_1^C = \{\mathcal{L}_1(\sigma \cap C) : \sigma \in \mathbb{R}^n, n \in \mathbb{N}\} \subseteq \mathcal{C}' \quad (4.17)$$

é enumerável (assumindo CH). A dimensão VC da classe  $\mathcal{L}_1^C \cup \{C\}$  é  $\leq 1$ , e por ser enumerável, logo universalmente separável, ela é uniforme Glivenko–Cantelli com a complexidade amostral usual  $s(\epsilon, \delta, 1)$ . Por conseguinte, dado  $\epsilon, \delta > 0$ , se  $n$  é bastante grande, temos para cada medida de probabilidade  $\mu$  sobre  $\Omega$  e para cada  $\sigma \in \Omega^n$

$$\mu(C \Delta \mathcal{L}(\sigma, C \cap \sigma)) < \epsilon$$

quando  $n \geq N(\epsilon, \delta, 1)$ .

# 5

## Consistência universal

---

O assunto deste capítulo é o classificador  $k$ -NN de  $k$  vizinhos mais próximos em um espaço métrico separável.

### 5.1 Classificador 1-NN de vizinhos mais próximos

Seja  $\Omega$  um espaço métrico. Dado um ponto  $x \in \Omega$  e uma amostra não rotulada  $\sigma$ , denotemos por  $\text{NN}_\sigma(x)$  o vizinho mais próximo de  $x$  em  $\sigma$ . No caso de empates, ou seja, alguns pontos  $x_i$  que todos atingem o valor da distância  $d(x, \sigma)$ , vamos desempatar, por exemplo, escolhendo  $x_i$  com o menor índice  $i$ , ou escolhendo um dos vizinhos aleatoriamente e uniformemente. Pelo momento a estratégia de desempate não é importante. Quando  $\Omega$  é munido de uma medida de probabilidade boreliana,  $\mu$ , vamos denotar por  $W_n$  uma amostra aleatória com  $n$  elementos i.i.d., seguindo a lei  $\mu$ .

**Teorema 5.1.1** (Lema de Cover–Hart [Cover e Hart 1967]). *Seja  $\mu$  uma medida de probabilidade boreliana sobre um espaço métrico separável  $(\Omega, d)$ . Então, quase certamente,*

$$\text{NN}_{W_n}(X) \rightarrow X \text{ quando } n \rightarrow \infty. \quad (5.1)$$

Vamos esclarecer a proposição, reformulando-la na linguagem conjuntística e da teoria de medida. Um *caminho amostral* é um elemento qualquer,

$$\zeta = (x_1, x_2, \dots, x_n, \dots),$$

do produto cartesiano infinito  $\Omega^\infty = \Omega^{\mathbb{N}^+}$  de  $\mathbb{N}^+$  cópias do domínio,  $\Omega$ . Ou seja,  $\zeta$  é simplesmente uma sequência de elementos do domínio. Todo segmento inicial de um caminho amostral,

$$\zeta_n = (x_1, x_2, \dots, x_n) \in \Omega^n,$$

é uma amostra. Na presença de uma medida de probabilidade  $\mu$  sobre  $\Omega$ , o caminho amostral torna-se uma variável aleatória seguindo a lei  $\mu^\infty = \mu^{\otimes \mathbb{N}^+}$ :

$$W = (X_1, X_2, \dots, X_n, \dots) \in \Omega^\infty.$$

A expressão na eq. (5.1) depende da variável aleatória  $(X, X_1, X_2, \dots, X_n, \dots) = (W, X)$ , combinando o caminho amostral  $W$  com um elemento aleatório  $X$  do domínio, que é independente do caminho. O significado probabilístico da eq. (5.1) é que

$$P[\lim_{n \rightarrow \infty} d(X, \text{NN}_{W_n}(X)) = 0] = 1.$$

(Aqui,  $W_n$  é o segmento inicial de  $W$ .) A reformulação conjuntística:

$$(\mu \otimes \mu^\infty) \left\{ (x, \zeta) \in \Omega \times \Omega^\infty : \lim_{n \rightarrow \infty} d(x, \text{NN}_{\zeta_n}(x)) = 0 \right\} = 1, \quad (5.2)$$

onde

$$d(x, \text{NN}_{\zeta_n}(x)) = d(x, \zeta_n) = \min_{i=1}^n d(x, x_i).$$

**Exercício 5.1.2.** Mostre que o conjunto

$$\left\{ (x, \zeta) \in \Omega \times \Omega^\infty : \lim_{n \rightarrow \infty} d(x, \zeta_n) = 0 \right\}$$

é boreliano.

**Definição 5.1.3.** Seja  $\mu$  uma medida boreliana sobre um espaço métrico  $\Omega$ . Um ponto  $x \in \Omega$  pertence ao *suporte de  $\mu$*  se o valor da medida de toda bola aberta em torno de  $x$  é estritamente positivo:

$$x \in \text{supp } \mu \iff \forall \varepsilon > 0 \mu(B_\varepsilon(x)) > 0.$$

**Exercício 5.1.4.** Mostre que o suporte de uma medida é um conjunto fechado.

**Exercício 5.1.5.** Mostre que o suporte de uma medida boreliana sobre um espaço métrico qualquer é separável.

[ *Sugestão:* observe que dado  $\varepsilon > 0$ , cada família  $\varepsilon$ -discreta de pontos do suporte da medida é necessariamente enumerável... ]



**Exercício 5.1.6.** Seja  $\mu$  uma medida de probabilidade sobre um espaço métrico separável. Mostre que

$$\mu(\text{supp } \mu) = 1. \quad (5.3)$$

*Observação 5.1.7.* Este é o resultado que exige a separabilidade do espaço  $\Omega$ . Mais exatamente, ele vale para qualquer espaço métrico cuja densidade não é um cardinal *mensurável*. Uma das condições equivalentes à definição de cardinal mensurável,  $\tau$ , é a seguinte: um espaço métrico  $\Omega$  de cardinalidade  $\tau$ , munido da métrica zero-um, admite uma medida de probabilidade boreliana não atômica (uma medida de probabilidade definida sobre todos os conjuntos de  $\Omega$ , tendo a propriedade que a medida de cada conjunto unitário é zero). O suporte de uma tal medida é obviamente vazio!

Portanto, em ZFC, não somente a existência de cardinais mensuráveis não pode ser mostrada, mas até mesmo a consistência do sistema “ZFC + existem cardinais mensuráveis”.

**Exercício 5.1.8 (\*).** Seja  $\mu$  uma medida de probabilidade sobre espaço métrico cuja densidade não é um cardinal mensurável. Mostre que vale a conclusão na eq. (5.3).

[ *Sugestão:* todo espaço métrico admite uma base topológica que é a união de uma sequência  $\gamma_n$  de famílias discretas (para todo  $x$  existe  $\varepsilon > 0$  tal que  $B_\varepsilon(x)$  encontra um elemento de  $\gamma_n$  ao máximo). (É uma metade do teorema de metrização de Bing.) Tente mostrar antes de consultar, por exemplo, [Engelking 1989], sect. 5.4. Supondo que a medida de suporte de  $\mu$  é menor que 1, e aplicando o resultado acima ao espaço  $X \setminus \text{supp } \mu$ , mostre que existe uma família discreta (em particular, disjunta) de abertos negligenciáveis cuja união tem a medida estritamente positiva. Deduza que o cardinal  $|\gamma|$  é mensurável. ]

Deste modo, tudo se reduz ao caso separável. Isso significa que a nossa hipótese de  $\Omega$  ser separável não é restritiva.

*Prova do lema de Cover–Hart 5.1.1.* Seja  $x \in \text{supp } \mu$  fixo qualquer, e seja  $\varepsilon > 0$ . Para um elemento aleatório  $X_n \sim \mu$ , a probabilidade do evento  $X_n \notin B_\varepsilon(x)$  é igual a  $1 - \mu(B_\varepsilon(x)) < 1$ . Logo, para um caminho amostral aleatório  $W = (X_1, X_2, \dots, X_n, \dots)$ , qualquer seja  $n$ ,

$$\begin{aligned} P[\forall n X_n \notin B_\varepsilon(x)] &\leq P[X_1 \notin B_\varepsilon(x), \dots, X_n \notin B_\varepsilon(x)] \\ &= (1 - \mu(B_\varepsilon(x)))^n \rightarrow 0 \text{ quando } n \rightarrow \infty. \end{aligned}$$

A sequência de reais  $d(\text{NN}_{\zeta_n}, x)$  é monótona. Logo, com a probabilidade um,  $\text{NN}_{\zeta_n} \in B_\varepsilon(x)$  se  $n \geq N$ , onde  $N$  é bastante grande. Aplicando esta observação para a sequência de valores  $\varepsilon = 1/k$  e usando o fato que a interseção de uma sequência de conjuntos de medida um tem medida um, concluímos que, com probabilidade um,  $\text{NN}_{\zeta_n} \rightarrow x$ . (Aqui, a probabilidade refere-se à medida  $\mu^\infty$  sobre o espaço de caminhos amostrais).

Segundo o teorema de Fubini [H.4.13](#), e usando o exercício [5.1.6](#),

$$\begin{aligned} (\mu \otimes \mu^\infty) \left\{ (x, \varsigma) : \lim_{n \rightarrow \infty} d(x, \varsigma_n) = 0 \right\} &= \int_{\Omega} \mu^\infty \left\{ (x, \varsigma) : \lim_{n \rightarrow \infty} d(x, \varsigma_n) = 0 \right\} d\mu(x) \\ &= \int_{\text{supp } \mu} + \int_{\Omega \setminus \text{supp } \mu} \\ &= 1 + 0 = 1. \end{aligned}$$

□

*Observação 5.1.9.* Seria interessante saber se aprendizagem é possível nos espaços mensuráveis com medida não separáveis (por exemplo, nos espaços probabilísticos de Loeb [[Loeb 1975](#)]), talvez, sob um modelo de aprendizagem diferente.

**Exercício 5.1.10.** Analise onde os axiomas de uma métrica foram usados na demonstração do lema de Cover–Hart. Tente formular e mostrar versões do resultado para “medidas de semelhança”  $d(x, y)$  que não satisfazem todos os axiomas da métrica.

Aqui, uma consequência imediata do lema de Cover–Hart.

**Proposição 5.1.11.** *Seja  $\mu$  uma medida de probabilidade borealiana sobre um espaço métrico separável qualquer,  $\Omega$ . Se  $C$  é um conceito boreliano em  $\Omega$  tal que a fronteira de  $C$ ,*

$$\text{fr}(C) = \bar{C} \setminus \overset{\circ}{C},$$

*é negligenciável,*

$$\mu(\text{fr}(C)) = 0,$$

*então o classificador de vizinhos mais próximos aprende  $C$ , e a convergência de erro para zero é quase certa:*

$$\mu(\mathcal{L}_n^{\text{NN}}(C \upharpoonright \varsigma_n) \Delta C) \xrightarrow{q.c.} 0 \text{ quando } n \rightarrow \infty.$$

*Observação 5.1.12.* A convergência quase certa é uma propriedade mais forte do que a convergência em probabilidade. Ela significa que o erro converge para zero ao longo de quase todo caminho amostral. De fato, temos, para quase todos  $x \in \Omega$  e quase todos os caminhos amostrais  $\varsigma$ ,

$$\mathcal{L}_n^{\text{NN}}(C \upharpoonright \varsigma_n)(x) \rightarrow \chi_C(x). \quad (5.4)$$

Segundo o teorema de Lebesgue sobre convergência dominada (teorema [H.1.17](#)), a convergência quase certa implica a convergência em probabilidade.

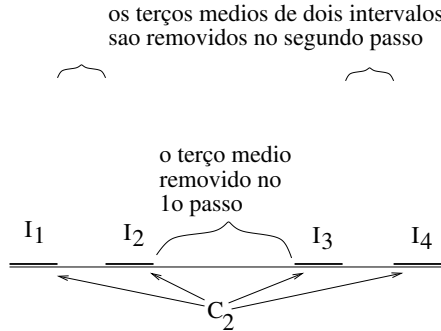


Figura 5.1: A construção do conjunto de Cantor, depois  $n = 2$  passos.

*Demonstração da proposição 5.1.11.* O conjunto aberto  $\overset{\circ}{C}$  é rotulado identicamente com o rótulo 1, e o conjunto aberto  $\Omega \setminus \overset{\circ}{C}$  é rotulado com 0. A união de dois conjuntos tem medida plena (um). Seja  $x$  um elemento qualquer desta união. Suponha que  $x$  pertença ao interior de  $C$ . Segundo o lema de Cover–Hart, para quase todos os caminhos amostrais, existe um  $n$  tal que  $X_n$  toma valor dentro do interior de  $C$ , e desse modo, o vizinho mais próximo de  $x$  vai receber o rótulo 1. Por conseguinte, a regra 1-NN vai associar a  $x$  o rótulo correto, 1, a partir deste  $n$ . Igualmente, para cada elemento  $x$  de  $\Omega \setminus \overset{\circ}{C}$  e quase todos os caminhos amostrais  $\zeta$ , a regra  $\mathcal{L}_n^{\text{NN}}$  vai associar a  $x$  o rótulo correto, 0, a partir de um  $n$ . O teorema de Fubini H.4.13 permite a concluir que o conjunto de pares  $(x, \zeta)$  com a propriedade de que a partir de um  $n$  o rótulo assinado a  $x$  é correto, tem a medida um.  $\square$

O resultado se aplica a cada espaço métrico separável, sem restrição nenhuma. Infelizmente, ele não é muito útil, pois num sentido “a maioria” dos conjuntos borelianos tem uma fronteira de medida não nula.

**Exemplo 5.1.13.** O conjunto de Cantor,  $C$ , é obtido do intervalo fechado  $[0, 1]$  removendo o terço médio,  $(1/3, 2/3)$ , e em seguida, removendo os terços médios  $(1/9, 2/9)$  e  $(7/9, 8/9)$ , de dois intervalos restantes, e cetera. Mais precisamente, a construção é recursiva. Definemos  $C_0 = [0, 1]$ . Para todo  $n \in \mathbb{N}$ , o conjunto  $C_n$  é a união de  $2^n$  intervalos fechados de comprimento  $3^{-n}$  cadaum. Denotemos  $C_{n+1}$  o conjunto obtido de  $C_n$  eliminando os terços médio de todos os intervalos que formam  $C_n$ . Finalmente, definemos

$$C = \bigcap_{n=0}^{\infty} C_n.$$

O comprimento total de  $C_n$  é igual a  $(2/3)^n$ , logo a medida de Lebesgue de  $C$  est nula. No entanto, é um objeto muito interessante.

Os pontos extremos de todos os intervalos abertos removidos pertencem a  $C$ ; eles se chamam os *pontos de primeira espécie*. Eles formam um conjunto enumerável. O restante de elementos de  $C$  chamam-se os *pontos de segunda espécie*. Para ver que eles existem, note que os pontos removidos podem se caracterizar como todos os pontos cuja expansão ternária,

$$x = \sum_{n=1}^{\infty} 3^{-n} d_n, \quad d_n \in \{0, 1, 2\},$$

contém pelo menos um dígito 1. Por conseguinte,  $C$  consiste de todos os pontos  $x \in [0, 1]$  que admitem uma expansão ternária com os dígitos 0 e 2 só. Em particular, os pontos de primeira espécie são os que admitem uma tal expansão ternária finita. Eis um exemplo de ponto de segunda espécie:

$$0.202020202 \dots$$

**Exercício 5.1.14.** Observe que o conjunto de Cantor tem o interior vazio.

**Exercício 5.1.15.** Construa uma versão do conjunto de Cantor do tipo “terço médio” que tem a medida de Lebesgue tão próxima de 1 quanto desejado.

[ *Sugestão:* eliminar em vez de uma terça parte, uma parte menor, e calcular a soma de uma série geométrica... ] Conclua que, dado  $\delta > 0$ , existe um subconjunto aberto,  $U$ , de  $[0, 1]$ , cuja fronteira tem medida de Lebesgue  $> 1 - \delta$ .

**Exercício 5.1.16.** Mostre que no caso geral, quase certamente, todo átomo de  $\mu$  aparece pelo menos uma vez (de fato, um número infinito de vezes) dentro do caminho amostral. Deduza que no caso puramente atômico, o erro de aprendizagem converge para zero quase certamente. De modo mais geral, quase certamente, cada átomo  $x \in \Omega$  satisfaz Eq. (5.4).

Vamos ver dois exemplos de subconjuntos fechados nos espaços métricos separáveis que não podem ser aprendidos pelo classificador de vizinhos mais próximos. Nossa próxima tarefa é entender a geometria de um espaço métrico  $\Omega$  que permite a aprendizagem de conceitos pelo classificador 1-NN.

*Observação 5.1.17.* Na prova da proposição 5.1.11, nós estabelecemos um resultado mais forte do que a mera convergência do erro para zero em probabilidade: mostramos que o erro converge para zero quase certamente. (Veja seção E.2.3). Na parte da aprendizagem automática motivada pela estatística, reforçar os resultados sobre a convergência de erro em probabilidade para convergência quase certa é considerado importante. No entanto, continuaremos com a convergência do erro para zero em probabilidade (ou: esperança).

Eis o resultado central desta subseção.

**Teorema 5.1.18.** *Seja  $C$  um conjunto boreliano qualquer do espaço euclidiano  $\mathbb{R}^d$ . Então, o classificador de vizinho mais próximo aprende  $C$ :*

$$\mathbb{E}_{\sigma \sim \mu^n} \text{erro}_{\mu, C} \mathcal{L}_n^{\text{NN}}(C \upharpoonright \sigma) \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

O resultado é um pouco surpreendente, pois a fronteira de  $C$  pode ser grande, inclusive ser igual ao espaço  $\Omega$  inteiro, e cada vizinhança de um ponto da fronteira vai conter elementos de  $C$  bem como elementos de  $C^c$ . Vamos mostrar que os elementos de  $C$  são mais comuns entre os vizinhos de  $x$  quando  $x \in C$ , e menos comuns quando  $x \notin C$ . Observe que o caso onde  $x$  é um átomo foi já tratado (exercício 5.1.16). A demonstração ocupa o resto da subseção.

Seja  $\varepsilon > 0$  qualquer. Usando o teorema E.2.11, escolhamos dois conjuntos compactos  $K_i$ ,  $i = 1, 2$ , com as propriedades  $K_1 \subseteq C$ ,  $K_2 \subseteq \Omega \setminus C$ ,  $\mu(C \setminus K_1) < \varepsilon/2$ , e  $\mu((\Omega \setminus C) \setminus K_2) < \varepsilon/2$ . Denotemos também  $U = \Omega \setminus (K_1 \cup K_2)$ . Temos:  $C \cap K_2 = \emptyset$  e  $\mu(U) < \varepsilon$ . O nosso conceito  $C$  fica espremido entre dois compactos,  $K_1$  e  $K_2$ .

**Exercício 5.1.19.** Mostrar que a distância,

$$d(K_1, K_2) = \inf\{d(x, y) : x \in K_1, y \in K_2\},$$

entre dois compactos não vazios e disjuntos,  $K_1$  e  $K_2$ , num espaço métrico qualquer é estritamente positiva.

Dado um caminho amostral  $\zeta$  e um número natural positivo  $n$ , definamos a função  $r_{\text{NN}}^{\zeta_n}(x)$  como a distância entre  $x$  e os elementos do segmento inicial  $\zeta_n$ :

$$r_{\text{NN}}^{\zeta_n}(x) = \min_{i=1,2,\dots,n} d(x, x_i).$$

Em outras palavras, é o valor da distância entre  $x$  e o vizinho mais próximo dele em  $\zeta_n$ . Note que a função distância de um conjunto,  $r_n^{\zeta}(x)$  é Lipschitz contínua de constante  $L = 1$ . Note que a função  $r_{\text{NN}}^{\zeta_n}$  depende do caminho amostral, e como tal, pode ser vista como uma função aleatória, ou seja, um elemento aleatório do espaço de funções Lipschitz contínuas.

**Definição 5.1.20.** Uma família  $\mathcal{F}$  de funções entre dois espaços métricos,  $X$  e  $Y$ , é dita *uniformemente equicontínua* se para cada  $\varepsilon > 0$  existe  $\delta > 0$  tal que, quaisquer que sejam  $x, y \in X$ ,

$$d_X(x, y) > \delta \Rightarrow d_Y(f(x), f(y)) < \varepsilon.$$

**Exercício 5.1.21.** Seja  $(f_n)$  uma sequência uniformemente equicontínua de funções (por exemplo, uma sequência de funções 1-Lipschitz contínuas) sobre um conjunto precompacto,  $K$ , que converge para zero simplesmente sobre  $K$  (ou seja, em todo ponto de  $K$ ). Mostrar que  $f_n$  converge para zero uniformemente sobre  $K$ .

**Lema 5.1.22.** *A convergência no lema de Cover–Hart é uniforme sobre todo subconjunto precompacto do suporte da medida. Ou seja, quase certamente, a função  $r_{\text{NN}}^{\zeta_n}$  converge para zero uniformemente sobre todo conjunto precompacto  $K \subseteq \text{supp } \mu$ .*

*Demonstração.* Seja  $A$  um subconjunto enumerável e denso de  $\text{supp } \mu$ . Seja  $\varepsilon > 0$  qualquer. Um argumento padrão mostra que, quase certamente, toda bola  $B_\varepsilon(x)$ ,  $x \in A$ , contém um número infinito de elementos do caminho amostral (exercício; aqui usamos o fato que a medida da bola não é nula). Aplicando esta observação para uma sequência de valores  $\varepsilon = 1/m$ , concluímos: quase certamente, para todos  $\varepsilon > 0$  e  $x \in A$ , a bola  $B_\varepsilon(x)$ ,  $x \in A$ , contém um número infinito de elementos do caminho amostral. Seja  $\zeta$  um caminho amostral qualquer tendo esta propriedade.

Agora seja  $K$  um subconjunto precompacto qualquer do suporte da medida, e  $\varepsilon > 0$ . Cubramos  $K$  com uma família finita de bolas abertas de raio  $\varepsilon$  com centros em  $A$ :

$$K \supseteq \cup_{i=1}^k B_\varepsilon(x_i), \quad x_i \in K.$$

Toda bola  $B_\varepsilon(x_i)$ ,  $i = 1, 2, \dots, k$  contém pelo menos  $k$  elementos de  $\zeta$ . Isso implica, com ajuda da desigualdade triangular, que a partir de um valor de  $n$  bastante grande, temos para todo  $x \in K$

$$r_{k\text{-NN}}^{\zeta_n}(x) < 2\varepsilon.$$

Concluímos que

$$r_{k\text{-NN}}^{\zeta_n} \xrightarrow{K} 0 \text{ quando } n \rightarrow \infty.$$

□

Eis uma consequência imediata.

**fato 5.1.23.** *Quase certamente, se  $n$  é bastante grande, então o vizinho mais próximo de todo elemento de  $K_1$  em  $\zeta_n$  não pertence a  $K_2$ , e reciprocamente.*

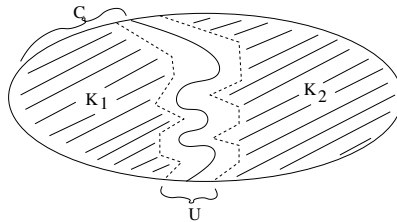


Figura 5.2: O conceito  $C$  está “preso” entre os compactos  $K_1$  e  $K_2$ .

Relembremos que todos os pontos de  $K_1$  são rotulados 1 (porque  $K_1 \subseteq C$ ), enquanto os pontos de  $K_2$  são rotulados 0. O classificador NN prediz o rótulo de um ponto  $x \in K_i$  baseando a predição sobre o rótulo do ponto  $\text{NN}_{\zeta_n}(x)$  que pertence ao conjunto  $K_i \cup U$ . Se pudermos limitar a “influência” sobre  $x$  de pontos da amostra  $\zeta_n$  que pertencem a  $U$  (por exemplo, mostrando que o valor da probabilidade  $P[\text{NN}_{\zeta_n}(X) \in U]$  é proporcional à medida de  $U$ ), teríamos controle sobre o erro de classificação. No espaço euclidiano um tal controle é devido ao lema importante de Stone (aqui, na versão  $k = 1$ ).

**Lema 5.1.24** (Lema geométrico de Stone, caso  $k = 1$ ). *Para todo  $d$  natural, existe uma constante absoluta  $C = C(d)$  com a propriedade seguinte. Seja*

$$\sigma = (x_1, x_2, \dots, x_n), \quad x_i \in \mathbb{R}^d, \quad i = 1, 2, \dots, n,$$

*uma amostra finita qualquer em  $\mathbb{R}^d$  (possivelmente com repetições), e seja  $x \in \mathbb{R}^d$  qualquer. O número de  $i$  tais que  $x \neq x_i$  e  $x$  é o vizinho mais próximo de  $x_i$  dentro da amostra*

$$x, x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n$$

*é majorado por  $C$ .*

*Observação 5.1.25.* A estratégia de desempate não importa para a conclusão do lema.

*Observação 5.1.26.* O caso onde  $x_i = x$  e por conseguinte tem  $x$  como o vizinho mais próximo não nos preocupa, pois isso só é possível com uma probabilidade positiva se  $x$  for um átomo sob a distribuição  $\mu$ , neste caso o classificador  $NN$  já aprende o rótulo de  $x$  perfeitamente bem.

Relembremos que a *distância geodésica* na esfera euclidiana com o centro na origem é o ângulo entre dois vetores,  $\vec{x}$  e  $\vec{y}$ . A distância geodésica é equivalente à distância euclidiana, por exemplo, na esfera unitária temos

$$\|x - y\| \leq \angle(x, y) \leq \frac{\pi}{2} \|x - y\|.$$

Mais ainda, temos que cada uma delas é um chamado *transformado métrico* da outra, por exemplo, a distância euclidiana pode ser expressa assim:

$$\forall x, y \in \mathbb{S}, \quad \|x - y\| = 2 \sin\left(\frac{\angle(x, y)}{2}\right).$$

Isso implica que as bolas abertas com relação a uma distância são as bolas com relação à outra.

*Demonstração do lema 5.1.24.* Como a distância euclidiana é invariante pelas translações, podemos supor sem perda de generalidade que  $x = 0$ . Um cone com o vértice na origem é definido assim:

$$C(\vec{v}, \alpha) = \{\vec{y} \in \mathbb{R}^d : \angle(\vec{y}, \vec{v}) < \alpha\},$$

onde  $\vec{v} \in \mathbb{R}^d$  e  $\alpha > 0$  são fixos. A interseção de um cone com a esfera unitária em torno de origem é uma bola aberta na esfera de raio  $\alpha$  formada com ajuda da distância geodésica, e por conseguinte, uma bola na esfera relativo à distância euclidiana. Como a esfera é um conjunto compacto, qualquer seja  $\alpha > 0$ , o espaço  $\mathbb{R}^d$  pode ser coberto por uma família finita de cones da forma  $C(\vec{v}, \alpha)$ . Seja  $\alpha = \pi/6$ . Escolhemos os cones  $C_1, C_2, \dots, C_m$  cobrindo o espaço. (O número  $m$  só depende de  $d$ , é a nossa constante  $C$ ).

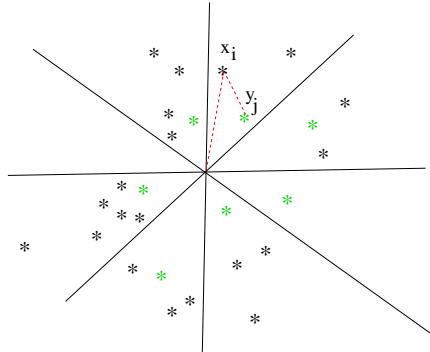


Figura 5.3: Prova do lema geométrico de Stone (caso  $k = 1$ ) em  $\mathbb{R}^d$ .

Para cada cone, se existirem pontos da amostra  $x_i$  que pertencem ao interior do cone, escolhamos entre eles o vizinho mais próximo de zero, e no caso de empates, qualquer um deles. Denotemos  $Y$  o conjunto de todos os pontos escolhidos,  $m$  deles no máximo. Seja  $x_i \notin Y$ ,  $x_i \neq 0$ . Existe  $j$  tal que  $x_i \in C_j$ . Neste caso, existe  $y = y_j \in Y \cap C_j$ . Temos  $\|x_i\| \geq \|y_j\|$ . Agora é um exercício simples da planimetria básica, mostrar que  $\|x_i - y_j\| < \|x_i\|$ . Por conseguinte, o vizinho mais próximo de  $x_i$  no conjunto  $x_1, x_2, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n$  nunca é igual a 0.  $\square$

**Lema 5.1.27.** *Sejam  $U$  um subconjunto boreliano qualquer de  $\mathbb{R}^d$ , e  $\mu$  uma medida de probabilidade boreliana sobre  $\mathbb{R}^d$ . Então, para todo  $n$ ,*

$$\limsup_{n \rightarrow \infty} P[X \notin U \text{ e } NN_{\sigma_n}(X) \in U] \leq C(d)\mu(U),$$

ou, um pouco mais exatamente e na notação conjuntística,

$$(\mu \otimes \mu^{\otimes n})\{(x, \sigma_n) \in \mathbb{R}^d \times (\mathbb{R}^d)^n : x \notin U \text{ e } NN_{\sigma_n}(x) \in U\} \leq C(d)\mu(U) + \frac{C}{n}.$$

*Demonstração.* Apliquemos uma simetrização pelas transposições  $\tau_i$  que trocam  $X \leftrightarrow X_i$ . Toda permutação de coordenadas, incluindo  $\tau_i$ , conserva a medida produto  $\mu \otimes \mu^{\otimes n}$ , e por conseguinte

$$\begin{aligned} P[X \notin U \text{ e } NN_{\sigma_n}(X) \in U] &= P[X_i \notin U \text{ e } NN_{(X_1, X_2, \dots, X_{i-1}, X, X_{i+1}, \dots, X_n)}(X_i) \in U] \\ &= \frac{1}{n} \sum_{i=1}^n P[X_i \notin U \text{ e } NN_{(X_1, \dots, X_{i-1}, X, X_{i+1}, \dots, X_n)}(X_i) \in U] \\ &= \mathbb{E} \frac{1}{n} \sum_{i=1}^n \chi\{(x, \sigma_n) : x_i \notin U \text{ e } NN_{(x_1, \dots, x_{i-1}, x, x_{i+1}, \dots, x_n)}(x_i) \in U\}. \end{aligned}$$



A soma é um “contador” que registra o número de  $i$  tais que  $x_i \notin U$ , e ao mesmo tempo o seu vizinho mais próximo no resto da amostra  $(x, \sigma)$  pertence a  $U$ . Entre os  $n + 1$  pontos  $x, x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n$ , ao máximo  $n\mu_{\sigma_n}(U) + 1$  pertencem a  $U$ , onde 1 é adicionado por causa de  $x$ . Cada um destes pontos é, no máximo, o vizinho mais próximo de  $C$  pontos distintos dele, em particular, de pontos fora de  $U$ . Por conseguinte, o número dos índices  $i$  tais que a função indicadora não se anula em  $(x, \sigma_n)$  é limitado por  $C(n\mu_{\sigma_n}(U) + 1)$ . Continuamos a avaliação:

$$\begin{aligned} P[X \notin U \text{ e } \text{NN}_{\sigma_n}(X) \in U] &\leq \mathbb{E} \frac{1}{n} C(n\mu_{\sigma_n}(U) + 1) \\ &= C \mathbb{E} \mu_{\sigma_n}(U) + \frac{C}{n} \\ &= C\mu(U) + \frac{C}{n}. \end{aligned}$$

□

Agora podemos terminar a prova do teorema 5.1.18. Suponha que  $K_1, K_2$  são escolhidos como acima. O fato 5.1.23 implica que, para  $n$  bastante grande, com a confiança  $\geq 1 - \delta$ , onde  $\delta > 0$  é o risco desejado, o vizinho mais próximo de todo ponto de  $K_1$  não pertence a  $K_2$ , e reciprocamente. A predição errado do rótulo no ponto  $x$  só pode ocorrer em dois casos: seja  $x \in U$ , seja  $x \in K_i, i = 1, 2$  e  $\text{NN}_{\sigma_n}(x) \in U$ . Então, a probabilidade de uma predição errada é limitada assim:

$$\begin{aligned} \mathbb{E}_{\sigma \sim \mu^n} \text{erro}_C \mathcal{L}_n^{\text{NN}}(C \upharpoonright \sigma_n) &= P[\mathcal{L}_n^{\text{NN}}(C \upharpoonright \sigma_n)(X) \neq \chi_C(X)] \\ &\leq \mu(U) + P[X \notin U \text{ e } \text{NN}_{\sigma_n}(X) \in U] \\ &< \varepsilon + C(d)\mu(U) + \frac{C}{n} \\ &< (C(d) + 1)\varepsilon + \frac{C}{n}. \end{aligned}$$

O último valor pode ser tão pequeno quanto quiser.

## 5.2 Erro de Bayes

Por que precisamos, então, do classificador de  $k$  vizinhos mais próximos, se já o classificador 1-NN aprende os conceitos? Esta parte da teoria de aprendizagem tem origem na estatística, e o modelo de aprendizagem é um pouco mais sofisticado do que o usado na informática teórica. O modelo previamente estudado é *determinístico* no sentido que um ponto  $x \in \Omega$  sempre recebe o mesmo rótulo,  $\chi_C(x)$ . O modelo estatístico leva em consideração a possibilidade de ruído aleatório que pode corromper as observações. Deste modo, o modelo é mais realístico, e a aprendizagem na presença de ruído, mais difícil. Vamos ver em breve que o classificador 1-NN falha na presença de ruído.

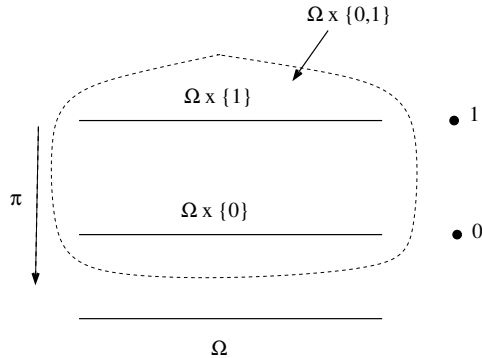


Figura 5.4: O domínio rotulado e a projeção  $\pi : \Omega \times \{0, 1\} \rightarrow \Omega$ .

Dado um ponto  $x$  do domínio, o modelo atribui um rótulo aleatório, segundo o valor da probabilidade de obter o rótulo 1, denotado  $\eta(x) \in [0, 1]$ . A função  $\eta : \Omega \rightarrow [0, 1]$  é chamada na estatística de *função de regressão*. No espírito da *lógica contínua*, pode-se dizer que  $\eta(x)$  é o valor de verdade (“grau de verdade”) da proposição “o rótulo de  $x$  é igual a 1”, cujos valores possíveis preenchem o intervalo  $[0, 1]$ .

No caso determinístico, a função de regressão é binária, sendo simplesmente a função indicadora do conceito a ser aprendido:

$$\eta(x) = \chi_C(x).$$

Vamos agora descrever o modelo correspondente, com todas as modificações necessárias. O domínio  $\Omega$ , como sempre, é um espaço boreliano padrão. O ponto rotulado  $(x, \epsilon)$ , onde  $x \in \Omega$ ,  $\epsilon \in \{0, 1\}$ , é modelado por uma variável aleatória  $(X, Y)$  com valores no produto  $\Omega \times \{0, 1\}$ . Aqui,  $X \in \Omega$  representa um ponto no domínio, e  $Y \in \{0, 1\}$ , o rótulo marcando o ponto. A lei conjunta de  $(X, Y)$  é uma medida de probabilidade,  $\tilde{\mu}$ , sobre  $\Omega \times \{0, 1\}$ . Agora, o ponto  $x \in \Omega$  é uma *instância* da v.a.  $X$ , e o rótulo  $\epsilon$  é uma instância da v.a.  $Y$ .

Denotemos  $\mu_1$  a restrição de  $\tilde{\mu}$  sobre  $\Omega \times \{1\}$ , ou, mais exatamente, uma medida sobre  $\Omega$  definida por

$$\mu(A) = \tilde{\mu}(A \times \{1\}).$$

Esta não é mais necessariamente uma medida de probabilidade: o volume total de  $\mu_1$  é igual a probabilidade de um ponto ser rotulado 1. Semelhantemente, define a medida  $\mu_0$  sobre  $\Omega$ .

Seja  $\pi : \Omega \times \{0, 1\} \rightarrow \Omega$  a projeção canônica de  $\Omega \times \{0, 1\}$  sobre  $\Omega$ ,  $(x, \epsilon) \mapsto x$ . A imagem direita de  $\tilde{\mu}$  sobre  $\pi$  é uma medida de probabilidade sobre  $\Omega$ ,

$$\mu = \pi_*(\tilde{\mu}),$$

definida por

$$\mu(A) = \mu_0(A) + \mu_1(A).$$

A medida  $\mu$  define a distribuição de pontos não rotulados.

É claro que a medida  $\mu_1$  é absolutamente contínua com relação à medida  $\mu$ , ou seja, se  $N \subseteq \Omega$  e  $\mu(N) = 0$ , então  $\mu_1(N) = 0$ . De fato, ela satisfaz a condição mais forte: para cada  $A$ ,  $\mu_1(A) \leq \mu(A)$ . Segundo o caso particular do teorema de Radon-Nikodým [H.3.30](#), existe uma derivada de Radon-Nikodým de  $\mu_1$  com relação a  $\mu$ , ou seja, uma função mensurável

$$\eta(x) = \frac{d\mu_1(x)}{d\mu}, \quad \eta: \Omega \rightarrow \mathbb{R},$$

tal que para todo  $A \subseteq \Omega$ ,

$$\mu_1(A) = \int_A \eta(x) d\mu(x).$$

Segue-se que

$$\mu_0(A) = \int_A (1 - \eta(x)) d\mu(x).$$

Na linguagem probabilística,  $\eta$  é a probabilidade condicional para  $X = x$  estar rotulado 1:

$$\eta(x) = P[Y = 1 | X = x].$$

O par  $(\mu, \eta)$  descreve completamente a distribuição  $\tilde{\mu}$  de pontos rotulados, como segue:  $X \in \Omega$  é uma variável aleatória com a lei  $\mu$ , e uma vez que a instância  $x$  de  $X$  é escolhida, o valor de  $Y$  é escolhido lançando a moeda com a probabilidade  $\eta(x)$  de dar “coroa”.

Dado um classificador (função boreliana),  $T: \Omega \rightarrow \{0, 1\}$ , o seu *erro de classificação* é definido por

$$\begin{aligned} \text{erro}_{\tilde{\mu}}(T) &= \text{erro}_{\eta, \mu}(T) \\ &= P[T(X) \neq Y] \\ &= \tilde{\mu}\{(x, y) \in \Omega \times \{0, 1\} : T(x) \neq y\}. \end{aligned}$$

**Proposição 5.2.1.**  $\text{erro}_{\eta, \mu}(T) = \|T - \eta\|_{L^1(\mu)} = \int_{\Omega} |T - \eta| d\mu.$

*Demonstração.*

$$\begin{aligned} \text{erro}_{\eta, \mu}(T) &= P[T(X) \neq Y] \\ &= \int_{\{T=1\}} P[Y = 0 | X = x] d\mu(x) + \int_{\{T=0\}} P[Y = 1 | X = x] d\mu(x) \\ &= \int_{\{T=1\}} (1 - \eta(x)) d\mu(x) + \int_{\{T=0\}} \eta(x) d\mu(x) \\ &= \int_{\{T=1\}} |T - \eta| d\mu + \int_{\{T=0\}} |T - \eta| d\mu \\ &= \int_{\Omega} |T - \eta| d\mu. \end{aligned}$$

□

*Observação 5.2.2.* Se  $\eta = \chi_C$  é uma função de regressão determinística, então obtemos a expressão bem familiar:

$$\text{erro}_{\eta, \mu}(T) = \|T - \chi_C\|_{L^1(\mu)} = \mu(C \Delta \{T = 1\}).$$

**Corolário 5.2.3.** Denote  $Z_\eta = Z(\eta - 1/2) = \{x \in \Omega : \eta(x) = 1/2\}$ . Então,

$$\text{erro}_{\eta, \mu}(T) = \int_{\Omega \setminus Z_\eta} |T - \eta| d\mu.$$

*Demonstração.* Basta notar que, qualquer seja o classificador  $T$ , a função  $|T - \eta|$  toma o mesmo valor constante sobre  $Z_\eta$ :

$$|T - \eta|_{Z_\eta} \equiv \frac{1}{2}.$$

□

**Corolário 5.2.4.** Sejam  $T, T'$  dois classificadores satisfazendo

$$\forall x \in \Omega, \eta(x) \neq \frac{1}{2} \Rightarrow T(x) = T'(x).$$

Então,

$$\text{erro}_{\tilde{\mu}}(T) = \text{erro}_{\tilde{\mu}}(T').$$

O *erro de Bayes* é o ínfimo de erros de classificação de todos os classificadores possíveis sobre  $\Omega$ :

$$\ell^* = \ell^*(\tilde{\mu}) = \ell^*(\mu, \eta) = \inf_T \text{erro}_{\tilde{\mu}}(T).$$

Com efeito, o ínfimo é o mínimo, atingido pelo *classificador de Bayes*:

$$T_{\text{bayes}}(x) = \begin{cases} 0, & \text{se } \eta(x) < \frac{1}{2}, \\ 1, & \text{se } \eta(x) \geq \frac{1}{2}. \end{cases}$$

**Exercício 5.2.5.** Mostre que

$$\text{erro}_{\tilde{\mu}}(T_{\text{bayes}}) = \ell^*(\tilde{\mu}).$$

[*Sugestão:* suponha que  $T$  e  $T_{\text{bayes}}$  sejam essencialmente diferentes fora do conjunto  $Z_\eta$  do exercício 5.2.4. Então, existe  $A, \mu(A) > 0, A \cap Z = \emptyset$ , tal que  $T|_A \neq T_{\text{bayes}}|_A$ . Por exemplo, suponha que  $T|_A \equiv 1$  e  $T_{\text{bayes}}|_A \equiv 0$ . Mostre diretamente que  $\text{erro}_{\tilde{\mu}}(T) > \text{erro}_{\tilde{\mu}}(T_{\text{bayes}})$ . ]

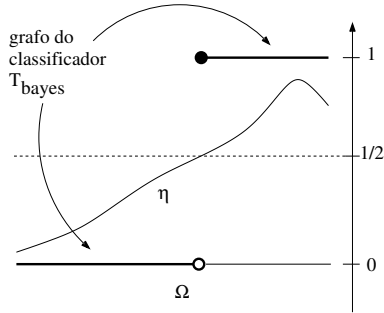


Figura 5.5: O classificador de Bayes

*Observação 5.2.6.* Segue-se do exercício 5.2.4 que em pontos  $x$  onde  $\eta(x) = 1/2$  o classificador de Bayes pode tomar qualquer valor, 0 ou 1. Por isso, talvez seria mais correto de falar de *um classificador de Bayes*.

**Exercício 5.2.7.** Mostre que o erro de Bayes é igual a zero,  $\ell^*(\tilde{\mu}) = 0$ , se e somente se a função de regressão  $\eta$  é determinística (só toma os valores 0 e 1 fora de um conjunto  $\mu$ -negligenciável).

O significado do classificador de Bayes é puramente teórico, porque a função de regressão,  $\eta$ , é desconhecida, assim como a lei  $\tilde{\mu}$ .

A amostra rotulada  $(x_1, x_2, \dots, x_n, \epsilon_1, \dots, \epsilon_n)$  é modelada pela sequência

$$(X_1, Y_1), (X_2, Y_2), \dots, (X_n, Y_n)$$

das variáveis independentes com valores em  $\Omega \times \{0, 1\}$ , seguindo a lei fixa, porém desconhecida,  $\tilde{\mu}$ .

A regra de aprendizagem  $\mathcal{L}$  no domínio  $\Omega$  é chamada *consistente* se o erro de classificação converge para o erro de Bayes (o menor possível) em probabilidade quando  $n \rightarrow \infty$ :

$$\forall \varepsilon > 0, P [\text{erro}_\mu \mathcal{L}_n > \ell^*(\tilde{\mu}) + \varepsilon] \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Como não conhecemos a lei subjacente,  $\tilde{\mu}$ , precisamos que a regra de aprendizagem seja consistente para todas as leis possíveis. Isto leva à seguinte definição.

**Definição 5.2.8.** A regra  $\mathcal{L}$  é *universalmente consistente* se ela é consistente para cada medida de probabilidade  $\tilde{\mu}$  sobre  $\Omega \times \{0, 1\}$ .

Em particular, uma regra universalmente consistente PAC aprende cada conceito  $C$  sob cada lei  $\mu$  sobre o domínio. Porém, a afirmação recíproca não é verdadeira. Ocorre que o classificador de um vizinho mais próximo não é consistente já numa situação simplíssima.

**Exemplo 5.2.9.** O domínio é um conjunto unitário,  $\Omega = \{*\}$ , munido da medida de probabilidade  $\mu$  evidente. O único caminho amostral é constante,  $*, *, \dots$ . A função de regressão toma o valor  $2/3$  sobre o único ponto do domínio. Isso significa que com a probabilidade  $2/3$ , o ponto  $*$  obteve o rótulo 1, e com a probabilidade  $1/3$ , o rótulo será 0. Como  $\eta(*) = 2/3$ , o classificador de Bayes toma o valor 1, e o erro de Bayes é igual a  $1/3$ .

Nesta situação, precisamos uma regra de desempate, e ela pode ser qualquer, uma vez ela não depende dos rótulos. Qualquer seja a regra de desempate, a probabilidade de que  $NN(*)$  tenha o rótulo  $\epsilon_i = 1$  é sempre igual a  $2/3$ . É fácil fazer o cálculo seguinte:

Rótulo de $NN(*)$	Probabilidade dele	Erro
1	$\frac{2}{3}$	$\frac{1}{3}$
0	$\frac{1}{3}$	$\frac{2}{3}$

Concluimos, usando a probabilidade condicional:

$$\text{erro}_{\mu, \eta}(\mathcal{L}^{NN}) = \frac{2}{3} \cdot \frac{1}{3} + \frac{1}{3} \cdot \frac{2}{3} = \frac{4}{9} > \frac{1}{3}.$$

Se você olha este exemplo com malícia, pode modificá-lo e substituir  $\Omega$  por um espaço probabilístico não atômico, onde quase certamente todo ponto terá um único vizinho mais próximo, munido da função de regressão  $\eta \equiv 2/3$ . O mesmo argumento se aplica para concluir que o classificador 1-NN não é consistente.

Agora imaginemos que ao invés de escolher o rótulo de  $x$  nos baseando sobre o único vizinho mais próximo de  $x$ , levamos em consideração os rótulos de  $k$  vizinhos, onde  $k \rightarrow \infty$ . Segundo a lei dos grandes números, quando  $k$  for bastante grande, com alta confiança aproximadamente  $(2/3 \pm \epsilon)k$  pontos teriam o rótulo 1, e o voto majoritário entre  $k$  vizinhos mais próximos produziria, com alta confiança, o rótulo 1 para  $x$ . No limite assintótico  $n, k \rightarrow \infty$ , o erro de aprendizagem vai convergir para o erro de Bayes,  $1/3$ .

## 5.3 Classificador $k$ -NN

Dado  $k$  e  $n \geq k$ , definemos o valor  $r_{k\text{-NN}}^{\mathcal{S}_n}(x)$  como o menor raio de uma bola fechada em torno de  $x$  que contém  $k$  vizinhos mais próximos de  $x$  em  $\mathcal{S}_n$ :

$$r_{k\text{-NN}}^{\mathcal{S}_n}(x) = \min\{r \geq 0: \#\{i = 1, 2, \dots, n: x_i \in \bar{B}_r(x)\} \geq k\}.$$

**Exercício 5.3.1.** Verificar que a função real  $r_{k\text{-NN}}^{\mathcal{S}_n}: \Omega \rightarrow \mathbb{R}$  é Lipschitz contínua de constante  $L = 1$ .

Eis, o lema de Cover-Hart na sua versão completa.

**Teorema 5.3.2** (Lema de Cover-Hart [Cover e Hart 1967]). *Seja  $\Omega$  um espaço métrico separável qualquer, e seja  $\mu$  uma medida de probabilidade boreliana sobre  $\Omega$ . Quase certamente, a função  $r_{k\text{-NN}}^{\zeta n}$  converge para zero uniformemente sobre conjuntos precompactos  $K \subseteq \text{supp } \mu$ .*

*Demonstração.* Seja  $A$  um subconjunto enumerável e denso de  $\text{supp } \mu$ . Seja  $\varepsilon > 0$  qualquer. Um argumento já conhecido mostra que, dado  $x \in A$  e  $\epsilon > 0$ , quase certamente, a bola  $B_\epsilon(x)$  contém um número infinito de elementos do caminho amostral (exercício; usemos o fato que a medida da bola não é nula). Aplicando esta observação à sequência de valores  $\varepsilon = 1/m$ , concluímos: para quase todos caminhos amostrais,  $\zeta$ , para todos  $\varepsilon > 0$  e  $x \in A$ , a bola  $B_\varepsilon(x)$ ,  $x \in A$ , contém um número infinito de elementos de  $\zeta$ .

Sejam  $\zeta$  um caminho amostral qualquer tendo a propriedade acima,  $K$  um subconjunto precompacto qualquer do suporte da medida, e  $\varepsilon > 0$ . Cubramos  $K$  com uma família finita de bolas abertas de raio  $\varepsilon$  com centros em  $A$ :

$$K \supseteq \bigcup_{i=1}^k B_\varepsilon(x_i), \quad x_i \in K.$$

Existe  $N$  tal que, se  $n \geq N$ , cada bola  $B_\varepsilon(x_i)$ ,  $i = 1, 2, \dots, k$  contém pelo menos  $k$  elementos de  $\zeta$ . A desigualdade triangular implica que a partir de  $N$ , temos para todo  $x \in K$

$$r_{k\text{-NN}}^{\zeta n}(x) < 2\varepsilon.$$

Concluímos:

$$r_{k\text{-NN}}^{\zeta n} \xrightarrow{K} 0 \text{ quando } n \rightarrow \infty.$$

□

Dado um ponto  $x$  e uma amostra (não rotulada)  $\sigma$ , pode acontecer que existam vários pontos de  $\sigma$  à mesma distância de  $x$ , ou seja, que existam estritamente mais do que  $k$  pontos na bola fechada  $\bar{B}_{r_{k\text{-NN}}^\sigma(x)}(x)$ . Com isto em mente, precisamos de uma estratégia de desempate. Para defini-la, vamos usar a notação seguinte: se  $\sigma \in \Omega^n$  e  $\sigma' \in \Omega^k$ ,  $k \leq n$ , o símbolo

$$\sigma' \sqsubset \sigma$$

significa que existe uma injeção  $f: [k] \rightarrow [n]$  tal que

$$\forall i = 1, 2, \dots, k, \quad \sigma'_i = \sigma_{f(i)}.$$

Uma aplicação de desempate é uma aplicação

$$k\text{-NN}^\sigma: \Omega^n \times \Omega \rightarrow \Omega^k$$

que possui as propriedades

$$k\text{-NN}^\sigma(x) \sqsubset \sigma$$

e

$$\sigma \cap \bar{B}_{r_{k\text{-NN}}^\sigma(x)}(x) \subseteq k\text{-NN}^\sigma(x) \subseteq \bar{B}_{r_{k\text{-NN}}^\sigma(x)}(x).$$

A aplicação  $k\text{-NN}^\sigma$  pode ser determinística ou estocástica, dependendo de uma variável aleatória  $Z$ , independente da lei  $\mu$  de dados.

**Exemplo 5.3.3.** Uma escolha determinística possível é usar a ordem na amostra,  $x_1 < x_2 < \dots < x_n$ . Neste caso,  $k$ -NN $^\sigma(x)$  consiste de todos os pontos de  $\sigma$  na bola aberta,  $B_{r_{k\text{-NN}^\sigma}(x)}(x)$ , mais o número necessário de pontos de  $\sigma \cap S_{r_{k\text{-NN}^\sigma}(x)}(x)$  que têm os menores índices.

**Exemplo 5.3.4.** A escolha de uma ordem de desempate pode ser também estocástica. Neste caso a fonte de aleatoriedade,  $Z$ , pode ser convertida numa variável aleatória  $Z'$  com valores no grupo  $S_n$  de permutações, seguindo a lei uniforme.

Agora a regra de classificação  $k$ -NN pode ser formalizada como segue:

$$\begin{aligned} \mathcal{L}_n^{k\text{-NN}}(\sigma, \epsilon)(x) &= \theta \left[ \frac{1}{k} \sum_{x_i \in k\text{-NN}^\sigma(x)} \epsilon_i - \frac{1}{2} \right] \\ &= \theta \left[ \mathbb{E}_{\mu_{k\text{-NN}^\sigma(x)}} \epsilon - \frac{1}{2} \right]. \end{aligned}$$

Aqui,  $\theta$  é a função de Heaviside, o sinal do argumento:

$$\theta(t) = \begin{cases} 1, & \text{se } t \geq 0, \\ 0, & \text{se } t < 0. \end{cases}$$

A medida empírica  $\mu_{k\text{-NN}^\sigma(x)}$  é suportada sobre o conjunto de  $k$  vizinhos mais próximos de  $x$  na amostra  $\sigma$ , e  $\epsilon$  é a rotulagem, uma função  $\epsilon: \{x_1, x_2, \dots, x_n\} \rightarrow \{0, 1\}$ . Deste modo, a esperança tem sentido.

A aplicação  $\mathcal{L}_n^{k\text{-NN}}$  pode ser determinística ou estocástica, dependendo da natureza do desempate, porém ela não depende da medida  $\tilde{\mu}$  sobre  $\Omega \times \{0, 1\}$ .

Começamos a análise com um resultado preliminar estabelecendo a consistência do classificador  $k$ -NN em espaço métrico qualquer, sob uma hipótese adicional, a de continuidade da função de regressão,  $\eta(x) = d\mu_1(x)/d\mu(x)$ .

**Teorema 5.3.5.** *Seja  $\Omega$  um espaço métrico separável munido de uma medida de probabilidade  $\mu$ . Suponha que a função de regressão  $\eta$  é contínua. Então, quando  $n, k \rightarrow \infty$  e  $k/n \rightarrow 0$ , o erro de classificador  $k$ -NN converge quase certamente para o erro de Bayes:*

$$\text{erro}_{\mu, \eta}(\mathcal{L}_n^{k\text{-NN}}) \xrightarrow{q.c.} \ell^*(\mu, \eta).$$

No caso de desempate determinístico (ou, por exemplo, se a probabilidade de empates é nula), quase certamente significa em relação aos pares  $(\zeta, \epsilon) \in \Omega^\infty \times \{0, 1\}^\infty = (\Omega \times \{0, 1\})^\infty$ , seguindo a lei  $\tilde{\mu}^\infty$ .

No caso de desempate aleatório, temos que adicional uma variável aleatória auxiliar,  $Z$ , tomando valores num espaço boreliano padrão,  $\Upsilon$ , com a lei  $\nu$ . Por exemplo, se usamos



uma ordem aleatória sobre a amostra  $\sigma$  para desempatar,  $Z$  pode tomar valores no produto  $\prod_{n=1}^{\infty} S_n$  de grupos simétricos, com a lei sendo a medida produto das medidas uniformes correspondentes. Neste caso, “quase certamente” se aplica às triplas  $(\zeta, \epsilon, z)$ , onde  $z \in \mathcal{Y}^{\infty}$ , um elemento aleatório de  $\mathcal{Y}$  para desempatar cada amostra  $\zeta_n$  (caso for necessário). O espaço boreliano

$$(\Omega \times \{0, 1\})^{\infty} \times \mathcal{Y}^{\infty}$$

é munido da lei  $\tilde{\mu}^{\infty} \otimes \nu^{\infty}$ .

*Observação 5.3.6.* Graças ao teorema de convergência dominada, o teorema 5.3.5 implica, em particular, que o classificador  $k$ -NN é consistente sobre  $\Omega$  se a função de regressão  $\eta$  é contínua. (Veja a observação 5.2.6).

Como adicionar a variável  $Z$  não causa dificuldades, frequentemente vamos a suprimir e trabalhar principalmente com o caso de desempate determinístico (mesmo se o desempate aleatório é o mais comum, pelo menos na teoria).

As vezes é cômodo expressar a lei  $\tilde{\mu}^{\infty} \otimes \mu$  de modo diferente. Seja  $\mu$  a projeção da medida  $\tilde{\mu}$  de  $\Omega \times \{0, 1\}$  sobre  $\Omega$ . O caminho aleatório não rotulado,  $\zeta$ , segue a lei  $\mu^{\infty}$ . Agora seja  $\zeta$  (para qual usamos a mesma letra) uma realização fixa do caminho aleatório,

$$\zeta = (x_1, x_2, \dots, x_n, \dots) \in \Omega^{\infty}.$$

A sequência de rótulos  $Y = (Y_1, Y_2, \dots, Y_n, \dots)$  para os pontos do caminho  $\zeta$  é uma variável aleatória com valores no produto infinito  $\{0, 1\}^{\infty}$  (um espaço de Cantor) munido da medida produto

$$\tilde{\mu}^{\zeta} = \{\eta(x_1), 1 - \eta(x_1)\} \otimes \{\eta(x_2), 1 - \eta(x_2)\} \otimes \dots \otimes \{\eta(x_n), 1 - \eta(x_n)\} \otimes \dots$$

Aqui, usamos a notação bastante comum,  $\{p, q\}$ , significando um espaço probabilístico padrão com apenas dois pontos, 0 e 1, tendo as probabilidades  $p$  e  $q$  respectivamente,  $p + q = 1$ .

A medida  $\tilde{\mu}^{\zeta}$  da “fibra”  $\{0, 1\}^{\infty}$  sobre o caminho  $\zeta$  (que consiste de todas as rotulagens possíveis  $\epsilon$  de  $\zeta$ ) é diferente para caminhos diferentes. Na linguagem probabilística,  $\tilde{\mu}^{\zeta}$  é a distribuição condicional dado  $\zeta$ . A família de medidas  $\tilde{\mu}^{\zeta}$ ,  $\zeta \in (\Omega^{\infty}, \mu^{\infty})$  é um exemplo de *desintegração* da medida  $\tilde{\mu}^{\infty}$  (veja seção H.4). A medida  $\tilde{\mu}^{\zeta}$  pode ser vista também como uma medida de probabilidade sobre o espaço  $\Omega^{\infty} \times \{0, 1\}^{\infty}$ , suportada sobre a fibra  $\{\zeta\} \times \{0, 1\}^{\infty}$ .

**Exercício 5.3.7.** Mostrar que, qualquer seja o conjunto boreliano  $B \subseteq \Omega^{\infty} \times \{0, 1\}^{\infty}$ , temos

$$\tilde{\mu}^{\infty}(B) = \int_{\Omega^{\infty}} \tilde{\mu}^{\zeta}(B) d\mu^{\infty}(\zeta).$$

[*Sugestão:* basta mostrar o resultado no caso onde  $B$  é um conjunto cilíndrico, e o teorema de Fubini permite reduzir tudo ao caso  $n = 1$ , onde a definição da função de regressão deve ser usada...]

Precisamos também re-examinar alguns resultados sobre a concentração de medida no cubo de Hamming.

**Exercício 5.3.8.** Deduzir dos teoremas 3.2.12 e E.2.1 a forma seguinte, formalmente mais geral, da lei geométrica de grandes números. Sejam  $(\Omega_i, \mu_i)$  espaços probabilísticos padrão, e seja  $f : (\prod_{i=1}^n \Omega_i, \mathcal{d}) \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua com relação a distância de Hamming normalizada, e mensurável com relação a estrutura boreliana do produto. Então para todo  $\varepsilon > 0$  temos

$$(\otimes_{i=1}^n \mu_i) \left\{ x \in \prod_{i=1}^n \Omega_i : |f(x) - \mathbb{E} f| \geq \varepsilon \right\} \leq 2e^{-2\varepsilon^2 n}.$$

**Exercício 5.3.9.** Sejam  $(p_i, q_i), i = 1, 2, \dots, n$  espaços de Bernoulli,  $p_i, q_i \geq 0, p_i + q_i = 1$ . Coloquemos sobre o cubo de Hamming  $\{0, 1\}^n$  a medida produto

$$\mu = \otimes_{i=1}^n \{p_i, q_i\}.$$

Então, a esperança do peso normalizado  $\bar{w}$  sobre o cubo satisfaz

$$\mathbb{E}_\mu \bar{w} = \frac{p_1 + p_2 + \dots + p_n}{n}.$$

[ *Sugestão:* usar a definição de  $\bar{w}$  junto com a da medida produto... ]

O teorema 5.3.5 vai seguir da afirmação mais forte.

**Lema 5.3.10.** *Sob a hipótese do teorema 5.3.5 ( $(\Omega, \mu)$  é um espaço métrico munido de uma medida de probabilidade,  $\eta$  é uma função de regressão contínua), há convergência quase certa:*

$$\frac{1}{k} \sum_{x_i \in k\text{-NN}^\sigma(x)} \epsilon_i \rightarrow \eta(x).$$

*Observação 5.3.11.* A expressão a esquerda é a *função de regressão empírica*.

*Observação 5.3.12.* “Quase certamente” neste contexto significa com relação às triplas  $(\zeta, \epsilon, x) \in \Omega^\infty \times \{0, 1\}^\infty \times \Omega = (\Omega \times \{0, 1\})^\infty \times \Omega$ , seguindo a lei  $\tilde{\mu}^\infty \otimes \mu$ . O resultado não depende da estratégia do desempate.

No caso de desempate aleatório, automaticamente segue-se a convergência certa com relação com os quadrúplos  $(\zeta, \epsilon, x, z) \in \Omega \times \{0, 1\}^\infty \times \Omega \times \Upsilon^\infty$ , seguindo a lei  $\tilde{\mu}^\infty \otimes \mu \otimes \nu^\infty$ , onde  $\nu$  é a lei da v.a.  $Z$  usado para desempatar quando for necessário.

Dada a afirmação do lema acima, segue-se que, quase certamente,

$$\theta \left[ \frac{1}{k} \sum_{x_i \in k\text{-NN}^\sigma(x)} \epsilon_i - \frac{1}{2} \right] \rightarrow \theta \left[ \eta(x) - \frac{1}{2} \right] = T_{\text{Bayes}}(x)$$

quando  $\eta \in \Omega \setminus Z_\eta$  (ou seja,  $\eta(x) \neq 1/2$ ), e agora o teorema de Lebesgue de convergência dominada, junto com o corolário 5.2.3 e a definição do classificador  $k$ -NN, implicarão que, quase certamente (com relação só ao caminho amostral, esta vez),

$$\begin{aligned} \text{erro}_{\mu, \eta} \mathcal{L}_n^{k\text{-NN}}(\sigma, \epsilon) &= \int_{\Omega \setminus Z_\eta} \left| \theta \left[ \frac{1}{k} \sum_{x_i \in k\text{-NN}^\sigma(x)} \epsilon_i - \frac{1}{2} \right] - \eta(x) \right| d\mu(x) \\ &\rightarrow \int_{\Omega \setminus Z_\eta} |T_{\text{bayes}}(x) - \eta(x)| d\mu(x) \\ &= \text{erro}_{\mu, \eta} T_{\text{bayes}} \\ &= \ell^*(\mu, \eta). \end{aligned}$$

*Prova do lema 5.3.10.* Segue-se do lema de Cover–Hart e da continuidade de  $\eta$  que, quase certamente em  $(\zeta, x)$ , o conjunto de valores  $\eta(k\text{-NN}(x))$  converge para  $\eta(x)$  no sentido óbvio: dado  $\epsilon > 0$ , existe  $N$  tal que quando  $n \geq N$ ,

$$\eta(k\text{-NN}(x)) \subseteq (\eta(x) - \epsilon, \eta(x) + \epsilon).$$

Seja  $\epsilon > 0$  qualquer fixo, e seja  $(\zeta, x)$  um par qualquer tendo a propriedade acima. Segundo os exercícios 5.3.8 e 5.3.9, a probabilidade do evento

$$\frac{\sum_{i=1}^k \epsilon_i}{k} \notin (\eta(x) - 2\epsilon, \eta(x) + 2\epsilon)$$

é exponencialmente pequena, limitada por  $2 \exp(-4\epsilon_0^2 k)$ . Como  $\sum_{k=1}^{\infty} 2 \exp(-4\epsilon_0^2 k) < \infty$ , o 1º lema de Borel–Cantelli (exercício E.2.27) implica (no mesmo espírito que na prova da lei geométrica forte de grandes números, lema E.2.26) que,  $\otimes_{n=1}^{\infty} \{\eta(x_i), 1 - \eta(x_i)\}$ -quase certamente em  $\epsilon$ , o evento acima só vai ocorrer para um número finito de  $k$ . Aplicando-o à sequência  $\epsilon = 1/m$ , concluímos:  $\otimes_{n=1}^{\infty} \{\eta(x_i), 1 - \eta(x_i)\}$ -quase certamente,

$$\frac{\sum_{i=1}^k \epsilon_i}{k} \rightarrow \eta(x).$$

□

A fim de se livrar da hipótese de continuidade de  $\eta$ , precisamos do lema geométrico de Stone para  $k$  qualquer.

**Lema 5.3.13** (Lema geométrico de Stone para  $\mathbb{R}^d$ ). *Para todo  $d$  natural, existe uma constante absoluta  $C = C(d)$  com a propriedade seguinte. Seja*

$$\sigma = (x_1, x_2, \dots, x_n), \quad x_i \in \mathbb{R}^d, \quad i = 1, 2, \dots, n,$$

uma amostra finita qualquer em  $\mathbb{R}^d$  (possivelmente com repetições), e seja  $x \in \mathbb{R}^d$  qualquer. Dado  $k \in \mathbb{N}_+$ , o número de  $i$  tais que  $x \neq x_i$  e  $x$  fica entre os  $k$  vizinhos mais próximos de  $x_i$  dentro da amostra

$$x, x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n$$

é majorado por  $Ck$ .

*Observação 5.3.14.* A desigualdade  $x \neq x_i$  é entendida no sentido conjuntístico. Teoricamente, no caso dos empates, pode ocorrer que a amostra inteira consiste do mesmo ponto,  $x_i = 0$ , repetido  $n$  vezes, e  $x = 0$  também. Porém, a conclusão resta verdadeira, de modo trivial.

*Demonstração.* O argumento é quase idêntico ao no caso  $k = 1$  (lema 5.1.24). Podemos supor que  $x = 0$ . Cubramos  $\mathbb{R}^d$  com  $C$  cones, e dentro de todo cone escolhemos o máximo número possível de vizinhos mais próximos de 0 diferentes de 0 próprio, até  $k$ . (Alguns deles podem ser repetidos, se tiver repetições dentro da amostra, mas nenhum é igual a 0). No caso dos empates, fazemos a escolha de modo qualquer, é não importa. Desta maneira,  $\leq Ck$  pontos estão marcados. Seja agora  $i$  qualquer. Se  $x_i$  é diferente de 0 e não foi marcado, então o cone que contém  $x_i$  já tem exatamente  $k$  pontos marcados, e para cada um deles,  $x_j$ , temos  $\|x_i - x_j\| < \|x_i\|$ . Isso implica que  $0 \notin k\text{-NN}(x_i)$ , qualquer seja a estratégia de desempate.  $\square$

Finalmente, o resultado clássico, cuja prova ocupa o resto da seção.

**Teorema 5.3.15** (Charles J. Stone). *O classificador  $k$ -NN é universalmente consistente no espaço euclidiano  $\mathbb{R}^d$ , sob a estratégia de desempate qualquer.*

Vamos escrever  $\mu_{k\text{-NN}^n(x)}$  para a medida uniforme suportada pelos  $k$  vizinhos mais próximos de  $x$  na amostra  $\zeta_n$ .

**Lema 5.3.16.** *Em  $\mathbb{R}^d$ ,*

$$\mathbb{E} \left| \mathbb{E}_{\mu_{k\text{-NN}^n(x)}} \eta - \eta \right| \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Seja  $\varepsilon > 0$ . Segundo o teorema de Luzin E.2.14, existe um compacto  $K \subseteq \Omega$  com  $\mu(K) > 1 - \varepsilon$  tal que a restrição  $\eta|_K$  é contínua. Os dois exercícios a seguir permitem estender  $f|_K$  até uma função (uniformemente) contínua,  $g$ , sobre  $\Omega$ , com valores em  $[0, 1]$ .

**Exercício 5.3.17.** *Seja  $f$  uma função 1-Lipschitz contínua com valores em  $[0, 1]$  sobre um subespaço métrico  $Y$  de um espaço métrico  $X$ . Mostrar que a função  $\tilde{f}$  sobre  $X$ , dada por*

$$\tilde{f}(x) = \max\{1, \inf\{f(y) - d(x, y) : y \in Y\}\}$$

é uma função 1-Lipschitz contínua bem definida, com valores em  $[0, 1]$ , que estende  $f$ .

[ Para uma solução, veja a prova do lema 7.1.3. ]

**Exercício 5.3.18.** Seja  $f$  uma função uniformemente contínua sobre um subespaço métrico  $Y$  de um espaço métrico  $(X, d)$ . Mostrar que existe uma métrica  $\rho$  sobre  $X$ , uniformemente equivalente a  $d$ , tal que  $f$  é 1-Lipschitz contínua com relação a  $\rho|_Y$ .

[ *Sugestão:* a métrica  $\rho$  pode ser obtida como uma *transformação métrica* de  $d$ , ou seja, sob a forma  $\rho(x, y) = h(d(x, y))$ , onde  $h: \mathbb{R}_+ \rightarrow \mathbb{R}_+$  é uma função estritamente monótona e côncava, com  $h(0) = 0 \dots$  ]

Segue-se que  $\|\eta - g\|_{L^1(\mu)} < \varepsilon$ . Podemos escrever:

$$\mathbb{E} \left| \mathbb{E}_{\mu_{k\text{-NN}\leq n}(x)} \eta - \eta \right| \leq \underbrace{\mathbb{E} \left| \mathbb{E}_{\mu_{k\text{-NN}\leq n}(x)} (\eta - g) \right|}_I + \underbrace{\mathbb{E} \left| \mathbb{E}_{\mu_{k\text{-NN}\leq n}(x)} g - g \right|}_II + \underbrace{\mathbb{E} |g - \eta|}_III.$$

O termo *(III)* é limitado por  $\varepsilon$  graças à escolha de  $g$ . O termo *(II)* é uma sequência convergente para zero quando  $n \rightarrow \infty$  graças ao teorema de convergência dominada de Lebesgue, porque

$$\mathbb{E}_{\mu_{k\text{-NN}\leq n}(x)} g \rightarrow g$$

quase certamente (lema 5.3.10). Note que até agora, tudo funciona para um espaço métrico separável e completo qualquer, não só em  $\mathbb{R}^d$ .

Falta somente estimar o termo *(I)*. Para isso, precisamos do lema geométrico de Stone, que garante que o “conjunto ruim”,  $U = \Omega \setminus K$ , não exerce uma influência indevida sobre os valores preditos pelo classificador  $k$ -NN. Temos:

$$\begin{aligned} (I) &\leq \mathbb{E} \mathbb{E}_{\mu_{k\text{-NN}\leq n}(X)} |\eta - g| \\ &= \mathbb{E} \frac{1}{k} \sum_{X_i \in k\text{-NN}(X)} |\eta(X_i) - g(X_i)| \\ &= \mathbb{E} \frac{1}{k} \sum \{|\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X)\} \\ &= \underbrace{\mathbb{E} \frac{1}{k} (\dots | X \in U)}_A + \underbrace{\mathbb{E} \frac{1}{k} (\dots | X \in K)}_B. \end{aligned}$$

O termo *(A)* é limitado por  $\varepsilon$ , pois  $\mu(U) < \varepsilon$ . Para avaliar o termo *(B)*, note que se  $X_i \in K$ , então o valor sob esperança se anula. Por conseguinte,

$$\begin{aligned} (B) &= \mathbb{E} \frac{1}{k} \sum \{|\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X), X \in K, X_i \notin K\} \\ &\leq \mathbb{E} \frac{1}{k} \sum \{|\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X), X_i \neq X\}. \end{aligned}$$

A transposição de coordenadas  $\tau_i: X \leftrightarrow X_i$  conserva a medida  $\mu$ , logo:

$$\begin{aligned}
(B) &\leq \mathbb{E} \frac{1}{k} \sum \{|\eta(X) - g(X)| : X \in k\text{-NN}(X_i), X_i \neq X\} \\
&= \mathbb{E} \frac{1}{k} [|\eta(X) - g(X)| \#\{i = 1, 2, \dots, n : X \in k\text{-NN}(X_i), X_i \neq X\}] \\
&\leq \mathbb{E} |\eta(X) - g(X)| \frac{1}{k} C(d)k \\
&< \varepsilon C(d),
\end{aligned}$$

usando o lema geométrica de Stone. Isso termina a prova do lema 5.3.16.

Agora a prova do teorema de Stone 5.3.15 é finalizada usando um argumento parecido ao da prova do teorema 5.3.5, com as modificações necessárias usando a convergência em probabilidade ao invés da convergência quase certa.

O teorema de Stone permanece válido para qualquer norma sobre  $\mathbb{R}^d$ .

**Exercício 5.3.19.** Modificar a prova do lema geométrico de Stone para mostrar que o classificador  $k$ -NN é universalmente consistente em todo espaço normado de dimensão finita. (Uma prova pode ser achada em [Duan 2014].)

*Observação 5.3.20.* Intuitivamente, quando mais dados temos, podemos escolher um classificador melhor. Isso é, espera-se que o erro de classificação esperado ao nível  $n + 1$  seja menor do que ao nível  $n$ . Mais formalmente, uma regra de classificação  $\mathcal{L} = (\mathcal{L}_n)$ ,

$$\mathcal{L}_n : \Omega \times (\Omega \times \{0, 1\})^n \rightarrow \{0, 1\},$$

é dita *inteligente* (*smart* [Devroye, Györfi e Lugosi 1996]) se para todas as medidas de probabilidade  $\mu$  sobre  $\Omega \times \{0, 1\}$  a seqüência de valores de erros de classificação

$$\mathbb{E}_\mu \{L(\mathcal{L}_n)\}, \quad n = 1, 2, 3, \dots$$

é não crescente, onde  $L(\mathcal{L}_n) = P\{\mathcal{L}_n(X, \sigma_n) \neq Y \mid \sigma_n\}$ .

Surpreendentemente, as regras consistentes mais comuns (incluindo o classificador  $k$ -NN) não são inteligentes.

*Conjetura em aberto:* nenhuma regra de aprendizagem universalmente consistente é inteligente ([*ibid.*], Problem 6.16, p. 109).

**Exercício 5.3.21.** Mostre que o classificador  $k$ -NN em geral não é “inteligente”.

[ *Sugestão:* faça o cálculo do erro de classificação no domínio  $\Omega = [-1, 1]$  munido da lei seguinte:  $\mu_0$  é a medida uniforme sobre o intervalo, com a massa total de  $p$ , e  $\mu_1$  é puramente atômica, com  $\mu_1\{0\} = q$ ,  $p + q = 1$ . Para valores apropriadas de  $p$  e  $q$ , o erro de classificador 1-NN é menor do que o do classificador 2-NN (em relação à distância euclidiana). ] O exemplo foi emprestado de [*ibid.*].

## 5.4 Dimensão de Nagata

Comecemos a seção com dois exemplos de espaços normados de dimensão infinita, onde o classificador  $k$ -NN não é universalmente consistente. O primeiro exemplo pertence a Roy O. Davis, e o segundo, onde o espaço é um espaço de Hilbert  $\ell^2$ , a David Preiss. Ambos exemplos são elegantes, bastante simples, e muito pouco conhecidos.

Os dois exemplos, juntamente com o teorema de Stone, sugerem que um espaço métrico no qual o classificador  $k$ -NN é universalmente consistente, deve ter dimensão finita em algum sentido intuitivo. A noção relevante de dimensão finita para espaços métricos será considerada a seguir, é a chamada dimensão de Nagata.

### 5.4.1 Um espaço de Banach onde o classificador $k$ -NN não é consistente

Nesta sub-seção, vamos mostrar um exemplo fino, devido a Roy O. Davis [Davies 1971].

#### Panorâmica da situação

O exemplo original de [ibid.] é um espaço métrico compacto  $\Omega$  de diâmetro um e duas medidas borelianas  $\mu_1, \mu_2$  sobre  $\Omega$  tais que  $\mu_0(\Omega) = 2/3$ ,  $\mu_1(\Omega) = 1/3$ , e ao mesmo tempo para todo  $0 < r < 1$  temos  $\mu_0(\bar{B}_r(x)) = \mu_1(\bar{B}_r(x))$  qualquer seja  $x \in \Omega$ . (Exercício: deduzir a mesma propriedade para bolas abertas correspondentes, assim como para esferas).

Vamos apresentar o exemplo na subseção 5.4.1, bem como observar que esse espaço pode ser imerso isometricamente no espaço de Banach  $c_0$  de seqüências convergentes para zero.

**Exercício 5.4.1.** Seja  $\mu = \mu_0 + \mu_1$ . Interpretemos  $\mu_i$  como a distribuição de pontos de  $\Omega$  tendo rótulo  $i$ ,  $i = 0, 1$ . Segue-se que  $\int_0^1 \eta(x) d\mu(x) = 1/3$ , e  $\ell^*(\mu, \eta) \leq 1/3$  (testemunhado pelo classificador  $T \equiv 0$ ). Mostrar que no limite  $n \rightarrow \infty$  o classificador  $k$ -NN (com desempate digamos mais comum, aleatório e uniforme) vai assinar o rótulo 1 a metade de pontos:

$$P[\mathcal{L}_n^{k-NN}(X) = 1] \rightarrow \frac{1}{2} \text{ quando } n \rightarrow \infty. \quad (5.5)$$

Concluir que

$$\text{erro}_\mu(\mathcal{L}_n^{k-NN}) \rightarrow \frac{1}{2} > \frac{1}{3} \geq \ell^*.$$

[ *Sugestão:* re-escrever a probabilidade na eq. (5.5) com ajuda do jeito de condicionamento (veja subseção H.4.1),

$$\mathbb{E}\mathcal{L}_n^{k-NN}(X) = \mathbb{E}_r [\mathbb{E}\mathcal{L}_n^{k-NN}(X) \mid r_{k-NN}(X) = r],$$

e usar o lema de Cover–Hart. ]

### Exemplo de Roy O. Davis

Seja  $(N_n)$  uma sequência de inteiros positivos, a ser escolhida recursivamente mais tarde. Denotemos  $E_n$  o conjunto dos elementos  $(i, j)$ ,  $1 \leq i \leq N_n$ ,  $0 \leq j \leq N_n$ ; os elementos  $(i, 0)$  sendo chamados *centrais*, os elementos  $(i, j)$ ,  $j \geq 1$ , *periféricos*.

Definamos uma estrutura de grafo,  $G_n$ , sobre  $E_n$ , onde todos os elementos centrais são adjacentes (ou seja, formam um grafo completo com  $N_n$  vértices), e todo elemento periférico  $(i, j)$  é adjacente ao elemento central correspondente  $(i, 0)$ . Definamos uma métrica,  $d_n$ , sobre  $E_n$  como segue: para  $x, y \in E_n$ ,

$$d_n(x, y) = \begin{cases} \frac{1}{2^n}, & \text{se } x, y \text{ são adjacentes,} \\ \frac{1}{2^{n-1}}, & \text{senão.} \end{cases}$$

**Exercício 5.4.2.** Dado um conjunto  $\Gamma$ , o espaço normado  $\ell^\infty(\Gamma)$  consiste de todas funções limitadas  $f: \Gamma \rightarrow \mathbb{R}$  munidas da estrutura canônica de um espaço vetorial e da norma

$$\|f\|_\infty = \sup_{\gamma \in \Gamma} |f(\gamma)|.$$

Verificar que  $\ell^\infty(\Gamma)$  é um espaço de Banach, e que  $\ell^\infty(\Gamma)$  é isometricamente isomorfo ao espaço  $\ell^\infty(n)$  no caso  $\#\Gamma = n$ .

**Exercício 5.4.3.** Seja  $X = \{x_1, x_2, \dots, x_n\}$  um espaço métrico finito. Mostrar que a aplicação

$$X \ni x \mapsto [f: y \mapsto d(x, y)] \in \ell^\infty(n) = \ell^\infty(\{x_1, x_2, \dots, x_n\}),$$

é uma imersão isométrica (a *imersão de Kuratowski*, veja subseção C.2.16).

Seja  $\Omega = \prod_{n=1}^\infty E_n$ . A métrica sobre  $\Omega$  é definida pela regra: dado  $x = (x_i)$ ,  $y = (y_i) \in \Omega$ ,  $x \neq y$ ,

$$d(x, y) = d_n(x_n, y_n),$$

onde  $n$  é o menor índice tal que  $x_n \neq y_n$ . Como o diâmetro de  $E_n$  é igual a  $2^{n-1}$ , e assim menor ou igual à distância entre dois elementos distintos quaisquer em  $E_{n-1}$ , a definição da distância  $d$  pode se escrever assim:

$$d(x, y) = \max_n d_n(x_n, y_n). \quad (5.6)$$

**Exercício 5.4.4.** Verificar que o espaço métrico  $\Omega$  é compacto, e que a métrica  $d$  induz a topologia produto (veja subseção C.2.14).

**Exercício 5.4.5.** O espaço de Banach  $c_0$  consiste de todas as sequências de números reais convergentes para zero,  $x = (x_n)$ ,  $x_n \rightarrow 0$ , munidos da norma uniforme (induzida de  $\ell^\infty$ ):

$$\|x\| = \sup_n |x_n|$$

(de fato, sobre  $c_0$  é o máximo). Mostrar que  $\Omega$  admite uma imersão isométrica no espaço de Banach  $c_0$ .



Seja  $B$  uma bola fechada em  $\Omega$ . Pode-se supor que  $B = \bar{B}_{1/2^n}(x)$ , onde  $n \geq 1$  e  $x = (x_i)$ . Então  $B$  consiste de todos  $x'$  tais que  $x'_i = x_i$  para todos  $1 \leq i < n$ , e  $x'_n$  é adjacente a  $x_n$  em  $G_n$ , ou  $x'_n = x_n$ . Se  $x_n$  é de gênero  $(i, 0)$ , então todos os elementos possíveis  $x'_n$  são

$$(i, 1), \dots, (i, N_n), (1, 0), \dots, (N_n, 0),$$

enquanto se  $x_n$  é de forma  $(i, j)$ ,  $1 \leq j \leq N_n$ , então todos os elementos possíveis  $x'_n$  são  $(i, j)$  mesmo e  $(i, 0)$ . Isso implica que a projeção de  $B$  sobre  $E_n$  tem o número igual dos elementos centrais e periféricos.

Formamos o conjunto cilíndrico:

$$\Omega(x_1, \dots, x_n) = \{x_1\} \times \{x_2\} \times \dots \times \{x_n\} \times E_{n+1} \times E_{n+2} \times \dots$$

(onde  $\Omega(\emptyset) = \Omega$ ). Vamos definir duas seqüências de números  $\alpha_n, \beta_n$ ,  $n = 0, 1, 2, \dots$ , com  $\alpha_n > \beta_n > 0$ , e  $\alpha_0 = \frac{2}{3}$ ,  $\beta_0 = \frac{2}{3}$ , bem como duas medidas borealianas  $\mu_0, \mu_1$  sobre  $\Omega$ , tendo a propriedade: quando tiver o número dos inteiros  $1 \leq i \leq n$  tais que  $x_i$  é central em  $E_i$ , então

$$\mu_0(\Omega(x_1, \dots, x_n)) = \alpha_n, \quad \mu_1(\Omega(x_1, \dots, x_n)) = \beta_n, \quad (5.7)$$

embora no caso contrário

$$\mu_0(\Omega(x_1, \dots, x_n)) = \beta_n, \quad \mu_1(\Omega(x_1, \dots, x_n)) = \alpha_n. \quad (5.8)$$

As medidas  $\mu_0, \mu_1$  são não atômicas e satisfazem  $\mu_0(\Omega) = \frac{2}{3}$ ,  $\mu_1(\Omega) = \frac{1}{3}$ . Em vista de texto em itálico acima, toda bola fechada  $B$  de raio  $r < 1$  é igual à união de um número igual de conjuntos cilíndricos de ambos tipos, e por conseguinte, satisfaz  $\mu_0(B) = \mu_1(B)$ .

Segundo o teorema de extensão de Carathéodory E.1.15, basta verificar a condição seguinte:

$$\mu_k(\Omega(x_1, x_2, \dots, x_{n-1})) = \sum_{x_n \in E_n} \mu_k(\Omega(x_1, x_2, \dots, x_{n-1}, x_n)), \quad k = 0, 1. \quad (5.9)$$

Vamos definir  $\alpha_n, \beta_n, N_n$  recursivamente, começando com  $\alpha_0 = \frac{2}{3}$ ,  $\eta_0 = \frac{1}{3}$ , como segue. Suponhamos que  $\alpha_{n-1} > \beta_{n-1} > 0$ , escolhamos  $N_n > 1$  tão grande que o sistema das equações lineares

$$\begin{cases} N_n^2 a + N_n b &= \alpha_{n-1}, \\ N_n^2 b + N_n a &= \beta_{n-1} \end{cases}$$

tem uma solução em números positivos  $a, b$ .

**Exercício 5.4.6.** Verificar que uma tal solução existe se  $N_n > \alpha_{n-1}/\beta_{n-1}$ .

**Exercício 5.4.7.** Verificar que  $a > b$  e  $4a < \alpha_{n-1}$ .

Definamos  $\alpha_n = a$ ,  $\beta_n = b$ . As seqüências  $(\alpha_n)$ ,  $(\beta_n)$  tem as propriedades desejadas. Para verificar eq. (5.9), suponha que o número dos inteiros  $i$ ,  $1 \leq i \leq n-1$ , tais que  $x_i$  é um elemento central, é par. Então, (5.7) tem lugar para os elementos periféricos  $x_n \in E_n$  e (5.8) para os elementos centrais. Para  $k = 1$ , o valor de lado direito da eq. (5.9) é igual a  $N_n^2 \alpha_n + N_n \beta_n = \alpha_{n-1}$ , igual ao valor de lado esquerda. Os três casos restantes são parecidos.

## 5.4.2 Classificador $k$ -NN não é consistente no espaço de Hilbert $\ell^2$

Aqui, vamos reproduzir o exemplo de David Preiss [Preiss 1979].

Seja  $Q = \prod_{k=1}^{\infty} [N_k]$  um espaço de Cantor com a topologia produto (subs. C.2.14), onde adotemos uma notação combinatória para  $[n] = \{1, 2, \dots, n\}$ , e  $(N_k)$  é uma seqüência de números naturais  $\geq 2$ . Denotemos  $\pi_k$  a projeção canônica de  $Q$  sobre o cubo de dimensão  $k$ ,  $Q_k = \prod_{i=1}^k [N_i]$ . Seja  $\mathcal{H} = \ell^2(\cup_{k=1}^{\infty} Q_k)$  um espaço de Hilbert cuja base ortonormal é indexada com elementos da união dos cubos  $Q_k$  (veja exemplo F.1.7).

Para todo  $\bar{n} = (n_1, \dots, n_k)$  em cada cubo  $Q_k$  define

$$f(\bar{n}) = \sum_{i=1}^k 2^{-i} e_{(n_1, \dots, n_i)} \in \mathcal{H}.$$

**Exercício 5.4.8.** Mostrar que a aplicação  $f$  se estende por continuidade sobre a união  $Q^*$  de cubos sobre o espaço de Cantor  $Q$ .

Denote  $\mu_1 = f_*(\nu)$  a imagem direta da medida de Haar sobre  $Q$  (o produto de medidas uniformes sobre cada conjunto finito  $[N_k]$ ).

**Exercício 5.4.9.** Verificar que para todo  $r > 0$  satisfazendo  $2^{-k} \leq r^2 < 2^k$ , e para todo  $\bar{n} = (n_1, n_2, \dots) \in Q$ ,

$$\mu_1(B_r(\bar{n})) = (N_1 N_2 \dots N_{k+1})^{-1}.$$

Agora define uma medida puramente atômica  $\mu_0$ , suportada na imagem de  $Q^*$ :

$$\mu_0 = \sum_k \sum_{\bar{n} \in Q_k} a_k \delta_{\bar{n}},$$

onde  $a_k > 0$  estão escolhidos de modo que a medida seja finita:

$$\sum_{k=1}^{\infty} a_k N_1 N_2 \dots N_k < \infty. \quad (5.10)$$

Para  $r$  e  $\bar{n} \in Q$  como acima a bola  $B_r(\bar{n})$  contém  $f(n_1 n_2, \dots, n_k)$ , logo

$$\mu_1(B_r(\bar{n})) \geq a_k.$$

Supondo, além disso, que

$$a_k N_1 N_2 \dots N_k N_{k+1} \rightarrow \infty \text{ as } k \rightarrow \infty, \quad (5.11)$$

concluimos:

$$\frac{\mu_1(B_r(\bar{n}))}{\mu_0(B_r(\bar{n}))} \rightarrow 0 \text{ when } r \downarrow 0.$$

**Exercício 5.4.10.** Mostrar que as condições (5.10) e (5.11) podem ser satisfeitos pela escolha recursiva de  $(N_k)$  e  $(a_k)$ .

Now renormalizemos as medidas  $\mu_0$  e  $\mu_1$  de modo que  $\mu = \mu_0 + \mu_1$  é uma medida de probabilidade, e interpretemos  $\mu_i$  como a distribuição de pontos rotulados  $i = 0, 1$ . Deste modo, a função de regressão,  $\eta$ , é determinística, e estamos aprendendo o conceito  $C = f(Q) = \text{supp } \mu_1, \mu_1(C) > 0$ .

Para um elemento aleatório  $X \in \mathcal{H}$ ,  $X \sim \mu$ , a distância  $r_{k,NN}(X)$  converge para zero quase certamente pelo lema de Cover e Hart.

**Exercício 5.4.11.** Deduzir das observações acima que a probabilidade condicional para qualquer dos  $k$  vizinhos mais próximos de  $X = x$  a ser rotulado 1 converge para zero quase certamente.

A regra de  $k$  vizinhos mais próximos vai quase certamente prever um classificador identicamente zero, logo não é consistente.

Um exemplo mesmo mais natural no espaço  $\ell^2$ , porém não trivial (com  $\mu$  sendo uma medida de Wiener e o conceito  $C$  não aprendizável, um elipsóide), foi apresentado em [Preiss 1981].

### 5.4.3 Dimensão de Nagata

Relembremos que uma família  $\gamma$  de subconjuntos de um conjunto  $\Omega$  tem *multiplicidade*  $\leq \delta$  se a interseção de mais de  $k$  elementos distintos de  $\gamma$  é sempre vazia. Em outras palavras,

$$\forall x \in \Omega, \quad \sum_{V \in \gamma} \chi_V(x) \leq \delta.$$

**Definição 5.4.12.** Sejam  $\delta \in \mathbb{N}$ ,  $s \in (0, +\infty]$ . Digamos que um espaço métrico  $(\Omega, d)$  tem *dimensão de Nagata*  $\leq \delta$  na escala  $s > 0$ , se toda família *finita* de bolas fechadas  $\gamma$  de raios  $< s$  tem uma sub-família  $\gamma'$  de multiplicidade  $\leq \delta + 1$  que cobre todos os centros de bolas de  $\gamma$ .

Um espaço  $\Omega$  tem dimensão de Nagata  $\delta$  se ele tem dimensão de Nagata  $\delta$  em uma escala apropriada  $s \in (0, +\infty]$ . Vamos denotar:  $\text{dim}_{Nag}^s(\Omega) = \delta$ , ou simplesmente  $\text{dim}_{Nag}(\Omega) = \delta$ .

**Exercício 5.4.13.** Mostre que a noção acima é equivalente à propriedade seguinte de  $\Omega$ . Dado uma sequência  $x_1, \dots, x_{\delta+2} \in \bar{B}_r(x)$ ,  $r < s$ , existem  $i, j$  tais que  $d(x_i, x_j) \leq \max\{d(x, x_i), d(x, x_j)\}$ .

[ *Sugestão:* usar contraposição para necessidade, e um argumento recursivo para suficiência. ]

**Exercício 5.4.14.** Deduzir que todo espaço métrico não arquimediano (isto é, satisfazendo a desigualdade triangular forte  $d(x, z) \leq \max\{d(x, y), d(y, z)\}$ ) tem dimensão de Nagata 0 na escala  $+\infty$ .

**Exercício 5.4.15.** Mostrar (também usando o exercício 5.4.13) que  $\dim_{Nag}(\mathbb{R}) = 1$ , e  $\dim_{Nag}(\mathbb{R}^2) = 2$ .

**Exercício 5.4.16.** Mostrar que todo espaço normado de dimensão finita  $n$  tem a dimensão de Nagata finita, mais não necessariamente  $n$ . (Estudar o exemplo de  $\ell^\infty(n)$ ), bem como os espaços euclidianos de dimensão  $n > 2$ ).

**Exercício 5.4.17.** Construir uma métrica equivalente na reta  $\mathbb{R}$  cuja dimensão de Nagata é infinita, em qualquer escala  $s > 0$ .

[ *Sugestão:* realizar  $\mathbb{R}$  como uma curva contínua e sem auto-interseções no espaço de Hilbert  $\ell^2$ , passando pelo zero e todos vetores de uma base ortogonal, e induzir a distância de lá. ]

Modificar o exemplo para construir uma métrica equivalente sobre uma sequência convergente com limite, que tem a dimensão de Nagata infinita em qualquer escala.

*Observação 5.4.18.* Pode se mostrar que um espaço topológico metrizável,  $X$ , tem a dimensão de Lebesgue  $n$  se e somente se a topologia de  $X$  pode ser gerada por uma métrica de dimensão de Nagata  $n$ . (Teorema de Nagata–Ostrand [Ostrand 1965]).

Espaços métricos de dimensão de Nagata finita admitem uma versão do lema geométrico de Stone, pelo menos no caso onde a amostra não tem empates, ou seja, os valores das distâncias  $d(x_i, x_j)$ ,  $i \neq j$ , são todas dois a dois diferentes.

**Lema 5.4.19** (Lema geométrico de Stone, dimensão de Nagata finita, sem empates). *Seja  $X$  um espaço métrico da dimensão de Nagata  $\delta < \infty$ . Seja*

$$\sigma = (x_1, x_2, \dots, x_n), \quad x_i \in \mathbb{R}^d, \quad i = 1, 2, \dots, n,$$

*uma amostra finita em  $X$ , e seja  $x \in X$  qualquer. Suponha que não tem empates na amostra*

$$x, x_1, x_2, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n.$$

*Dado  $k$ , o número de  $i$  tais que  $x \neq x_i$  e  $x$  fica entre os  $k$  vizinhos mais próximos de  $x_i$  dentro da amostra acima é majorado por  $(k + 1)(\delta + 1)$ .*

*Demonstração.* Suponha que  $x_i$ ,  $i = 1, 2, \dots, m$  tem  $x$  entre os  $k$  vizinhos mais próximos. A família  $\gamma$  das bolas fechadas  $B_{r_{k\text{-NN}}(x_i)}(x_i)$ ,  $i \leq m$ , admite uma sub-família  $\gamma'$  de

multiplicidade  $\leq \delta + 1$  que cobre todos pontos  $x_i$ ,  $i \leq m$ . Porque não há empates, cada bola em  $\gamma$  contem  $\leq k + 1$  pontos. Segue-se que  $\#\gamma' \geq m/(k + 1)$ . Todas bolas em  $\gamma'$  contem  $x$ , e como a multiplicidade de  $\gamma'$  é limitada por  $\delta + 1$ , concluímos:  $\#\gamma' \leq \delta + 1$ . O resultado se segue.  $\square$

Agora o mesmo argumento que na prova de Stone mostra que o classificador  $k$ -NN é consistente sob cada distribuição  $\mu$  sobre  $\Omega \times \{0, 1\}$  tal que a probabilidade de empates é nula. (Em outras palavras, se cada esfera de raio estritamente positivo é  $\mu$ -negligenciável).

Ao contrário do caso euclidiano, a afirmação do lema 5.4.19 é falsa na presença dos empates.

**Exemplo 5.4.20.** A conclusão do lema geométrico de Stone é falsa se a amostra  $\sigma$  com  $n > k$  pontos dois a dois distintos está munida de uma métrica zero-um. Por exemplo, o desempate baseado sobre a ordem na amostra escolherá  $x_1, x_2, \dots, x_k$  como vizinhos mais próximos de todo outro ponto.

Ao mesmo tempo, a dimensão de Nagata de um espaço  $X$  munido da métrica zero-um é igual a  $\delta = 0$ . Se a família  $\gamma$  de bolas fechadas contém uma bola de raio  $\geq 1$ , esta bola já cobre  $X$ . Se não, escolha de  $\gamma$  uma bola de raio  $< 1$  para cada centro de  $\gamma$ . As bolas escolhidas tem a mesma união que  $\gamma$  e são duas a duas disjuntas, ou seja, da multiplicidade 1.

Vale a pena observar que no caso euclidiano um tal exemplo é impossível: o tamanho de uma amostra cuja métrica induzida é a métrica zero-um é limitada pela dimensão do espaço!

Poderia-se esperar que a conclusão do lema geométrico de Stone seja válida no caso de dimensão de Nagata finita no sentido probabilístico, se o desempate for feito com ajuda de uma ordem aleatória e uniforme sobre a amostra. Mesmo assim, o resultado é falso.

**Exemplo 5.4.21.** Dado  $N \in \mathbb{N}$ , existe um espaço métrico finito  $\sigma = \{x_1, \dots, x_n\}$  de dimensão de Nagata 0, tal que a esperança de número de pontos  $x_i$  tais que o ponto  $x_1$  é o vizinho mais próximo deles sob um desempate aleatório uniforme é pelo menos  $N$ .

Vamos construir  $\sigma$  por recorrência. Começamos com  $x_1$  qualquer, e seja  $\sigma_1 = \{x_1\}$ . Adicionemos  $x_2$  à distância 1 de  $x_1$ , de modo que  $\sigma_2 = \{x_1, x_2\}$ . Se  $\sigma_n$  foi definido, adicionemos  $x_{n+1}$  à distância  $2^n$  de todos os pontos  $x_i$ ,  $i \leq n$ , e definemos  $\sigma_{n+1} = \sigma_n \cup \{x_{n+1}\}$ . Verifiquemos indutivamente que  $\dim_{Nag}(\sigma_n) = 0$ . Para  $n = 1$  é trivial. Suponhamos que a conclusão seja válida para  $\sigma_n$ , e seja  $\mathcal{F}$  uma família qualquer de bolas fechadas em  $\sigma_{n+1}$ . Se existe uma bola que contém todos os pontos, há nada a mostrar. Supondo que não, ou seja, todas as bolas têm raios menos de  $2^{n+1}$ , escolhemos uma família de multiplicidade 1 da sub-família de bolas centradas em elementos de  $\sigma_n$ , e adicionemos a bola centrada em  $x_{n+1}$  (um ponto isolado).

Finalmente, mostremos que se  $n$  é bastante grande, então o número esperado de  $i$  tais que  $x_1$  é um vizinho mais próximo de  $x_i$  sob um desempate uniforme é tão grande quanto desejado. Com este propósito, para todo  $i \geq 2$  calculemos a esperança do evento  $x_1 \in NN(x_i)$ . Para  $x_2$ , o único vizinho mais próximo é  $x_1$ , então  $\mathbb{E}[x_1 \in NN(x_2)] = 1$ . Para  $x_3$ , temos dois pontos à distância 2, que podem ser escolhidos com a probabilidade

$1/2$  cada um,  $x_1$  e  $x_2$ , então  $\mathbb{E}[x_1 \in NN(x_3)] = 1/2$ . Para  $i$  qualquer, temos  $\mathbb{E}[x_1 \in NN(x_i)] = 1/i$ . Concluimos:

$$\mathbb{E}[\#\{i = 1, \dots, n : x_1 \in NN(x_i)\}] = \sum_{i=1}^n \frac{1}{i},$$

que converge para  $+\infty$  quando  $n \rightarrow \infty$ .

Poderíamos considerar que empates não ocorrem na prática? Ou seja, pode ser que pelo menos para espaços métricos “não degenerados” de dimensão métrica finita a probabilidade de um empate é assintoticamente zero, quando  $n \rightarrow \infty$ ? Mesmo essa esperança é infundada.

**Exemplo 5.4.22.** Dado um valor  $\delta > 0$  e uma sequência  $n'_k \uparrow +\infty$ , existe um espaço métrico compacto de dimensão de Nagata zero (o conjunto de Cantor munido de uma métrica compatível), munido de uma medida de probabilidade, não atômica, e uma sequência  $n_k \uparrow \infty$ ,  $n_k \geq n'_k$ ,  $k/n_k \rightarrow 0$ , tendo a propriedade seguinte. Seja  $X$  um elemento aleatório de  $\Omega$ , e  $W$  um caminho amostral. Com probabilidade  $> 1 - \delta$ , para todos os valores  $k \in \mathbb{N}_+$ ,  $X$  tem  $\geq n_k$  empates entre seus  $k$ -vizinhos mais próximos dentro da amostra  $W_{n_{k+1}}$ .

O espaço  $\Omega$  é o produto direto  $\prod_{k=1}^{\infty} [N_k]$  de espaços topológicos finitos discretos, onde  $N_k$  são escolhidos recursivamente e  $[N_k] = \{1, 2, \dots, N_k\}$ . A distância é não arqui-mediana:

$$d(\sigma, \tau) = \begin{cases} 0, & \text{se } \sigma = \tau, \\ 2^{-\min\{i : \sigma_i \neq \tau_i\}}, & \text{caso contrário.} \end{cases}$$

Ela induz a topologia compacta de produto sobre  $\Omega$ . A medida  $\mu$  sobre  $\Omega$  é a medida-produto de medidas uniformes  $\mu_{N_k}$  sobre os  $[N_k]$ . Essa medida é não atômica, e em particular, quase todos os empates ocorrem à distância estritamente positiva de um ponto aleatório  $X$ .

Seja  $(\delta_i)$  uma sequência, tal que  $\delta_i > 0$ ,  $2 \sum_i \delta_i = \delta$ . Escolha  $N_1$  tão grande que, com a probabilidade  $> 1 - \delta_1$ ,  $n_1 = n'_1$  elementos escolhidos aleatoriamente e independentemente entre  $[N_1]$  (segundo a medida uniforme) são todos dois a dois distintos. Agora, escolha  $n_2 \geq n'_2$  tão grande que, se  $n_2$  elementos estão escolhidos aleatoriamente em  $[N_1]$ , então com a probabilidade  $> 1 - \delta_1$  cada elemento de  $[N_1]$  é escolhido pelo menos  $n_1$  vezes. Suponha que  $n_1, N_1, n_2, N_2, \dots, n_k$  foram escolhidas. Seja  $N_k$  tão grande que, com a probabilidade  $> 1 - \delta_k$ ,  $n_k$  elementos escolhidos aleatoriamente dentro  $[N_k]$  são dois a dois distintos. Escolha  $n_{k+1}$  tão grande que, com a probabilidade  $> 1 - \delta_k$ , se  $n_{k+1}$  elementos são escolhidos uniformemente dentro  $\prod_{i=1}^k [N_i]$ , então todo elemento de  $\prod_{i=1}^k [N_i]$  será escolhido pelo menos  $n_k$  vezes.

Agora seja  $(X, W)$  um elemento aleatório de  $\Omega \times \Omega^\infty$ . Com a probabilidade  $> 1 - \delta$ , o seguinte ocorre:

1. Para todo  $k$ , as  $k + 1$ -ésimas coordenadas de todos elementos de  $W_{n_{k+1}}$  são duas a duas distintas, logo as distâncias entre  $X$  e o resto da amostra  $W_{n_{k+1}}$  são  $\geq 2^{-k-1}$ ;

2. Para todo  $k$ , existem  $n_k$  elementos na amostra  $W_{n_{k+1}}$  que têm as mesmas  $i$ -ésimas coordenadas que  $X$ , para todos  $i = 1, 2, 3, \dots, k$ . Concluimos: eles são à distância exatamente  $2^{-k-1}$  de  $X$  e são os vizinhos mais próximos de  $X$  dentro da amostra.

Temos  $n_k$  empates entre  $k$  vizinhos mais próximos de  $X$  dentro  $W_{n_{k+1}}$ , qualquer que seja  $k$ .

Os exemplos acima mostram que, na presença de empates, a prova clássica não se generaliza sobre os espaços métricos de dimensão de Nagata finita. A fim de tratar dos empates, precisa-se uma abordagem técnica diferente.

Para começar, vamos estender o nosso cenário até o mais geral possível.

**Definição 5.4.23.** Um sub-espaço métrico  $X$  de um espaço métrico  $\Omega$  tem *dimensão de Nagata*  $\leq \delta \in \mathbb{N}$  na escala  $s > 0$  dentro de  $\Omega$  se toda família finita de bolas fechadas em  $\Omega$  com centros em  $X$  admite uma sub-família tendo multiplicidade  $\leq \delta + 1$  em  $\Omega$  que cobre os centros de bolas originais. Diz-se que  $X$  tem dimensão de Nagata finita em  $\Omega$  se  $X$  tem dimensão finita em  $\Omega$  em uma escala  $s > 0$ . Notação:  $\dim_{Nag}^s(X, \Omega)$  ou  $\dim_{Nag}(X, \Omega)$ .

**Exercício 5.4.24.** Digamos que uma família de bolas é *desconexa* (segundo Preiss), se o centro de toda bola da família não pertence às outras bolas. Mostrar que

$$\dim_{Nag}^s(X, \Omega) \leq \beta$$

se e somente se toda família desconexa de bolas fechadas em  $\Omega$  de raios  $< s$  com centros em  $X$  tem multiplicidade  $\leq \beta + 1$ .

**Exercício 5.4.25.** Mostrar que na definição 5.4.23, bem como no exercício 5.4.24, as bolas fechadas podem ser substituídas pelas bolas abertas. De fato, as afirmações restam válidas para famílias de bolas algumas das quais são abertas, algumas fechadas.

**Exercício 5.4.26.** Mostrar que se  $\dim_{Nag}^s(X, \Omega) \leq \delta$ , então  $\dim_{Nag}^s(\bar{X}, \Omega) \leq \delta$ , onde  $\bar{X}$  é a aderência de  $X$  em  $\Omega$ .

**Exercício 5.4.27.** Mostrar que se  $X$  e  $Y$  são dois sub-espaços de um espaço métrico  $\Omega$  que tem dimensão finita em  $\Omega$ , então  $X \cup Y$  tem dimensão finita em  $\Omega$ , com  $\dim_{Nag}(X \cup Y, \Omega) \leq \dim_{Nag}(X, \Omega) + \dim_{Nag}(Y, \Omega)$ .

**Definição 5.4.28.** Um espaço  $\Omega$  tem *dimensão de Nagata sigma-finita* se  $\Omega = \cup_{i=1}^{\infty} X_n$ , onde cada sub-espaço métrico  $X_n$  tem dimensão de Nagata finita em  $\Omega$  (com escalas  $s_n > 0$  possivelmente todas diferentes).

*Observação 5.4.29.* Graças ao exercício 5.4.26, na definição acima pode-se supor que  $X_n$  são fechados, em particular borelianos.

Eis a ferramenta técnica que permite manejar os empates nos espaços métricos mais gerais.

**Lema 5.4.30.** *Seja  $\sigma = \{x_1, x_2, \dots, x_n\}$  uma amostra finita num espaço métrico  $\Omega$ , e seja  $X$  um sub-espaço de dimensão de Nagata finita  $\delta$  em  $\Omega$  na escala  $s > 0$ . Seja  $\alpha \in (0, 1]$  qualquer. Seja  $\sigma' \sqsubseteq \sigma$  uma sub-amostra com  $m$  pontos. Assinemos a todo ponto  $x_i$  da amostra uma bola (fechada ou aberta),  $B_i$ , em torno de  $x_i$ , de raio  $< s$ . Então no máximo  $\alpha^{-1}(\delta + 1)m$  pontos  $x_i$  pertencendo a  $X$  tem a fração de  $\geq \alpha$  pontos de  $\sigma'$  nas bolas  $B_i$ :*

$$\#\{i = 1, 2, \dots, n: x_i \in X, \#(B_i \cap \sigma') \geq \alpha \#B_i\} \leq \alpha^{-1}(\delta + 1)m.$$

*Demonstração.* A família de todas as bolas  $B_i$  tendo as propriedades  $x_i \in X$  e

$$\#(B_i \cap \sigma') \geq \alpha \#B_i$$

admite uma sub-família de multiplicidade  $\leq \delta + 1$  que contem todos os centros. Cada ponto de  $\sigma'$  pertence, no máximo, aos  $\delta + 1$  bolas da sub-família. A soma de cardinalidades de bolas dessa sub-família, vez  $\alpha$ , não excede a cardinalidade de  $\sigma'$  vez  $\delta + 1$  (pois cada ponto de  $\sigma'$  está contado, no máximo,  $\delta + 1$  vezes), de onde concluímos.  $\square$

*Observação 5.4.31.* Nas aplicações do lema,  $B_i = B_{\epsilon_{k-\text{NN}}}(x)$  (as vezes abertas, as vezes fechadas).

**Lema 5.4.32.** *Sejam  $\alpha, \alpha_1, \alpha_2 \geq 0$ ,  $t_1, t_2 \in [0, 1]$ ,  $t_2 \leq 1 - t_1$ . Suponha que  $\alpha_1 \leq \alpha$  e*

$$t_1\alpha_1 + (1 - t_1)\alpha_2 \leq \alpha.$$

*Então,*

$$\frac{t_1\alpha_1 + t_2\alpha_2}{t_1 + t_2} \leq \alpha.$$

*Demonstração.* Se  $\alpha_2 \leq \alpha$ , a conclusão é imediata. Caso contrário,  $\alpha_2 \geq \alpha$ , segue-se da hipótese que

$$t_1\alpha_1 + t_2\alpha_2 \leq \alpha - (1 - t_1 - t_2)\alpha_2 \leq (t_2 + t_2)\alpha.$$

$\square$

**Lema 5.4.33.** *Seja  $x, x_1, x_2, \dots, x_n$  uma amostra finita (talvez com repetições), e  $\sigma' \sqsubseteq \sigma$  uma sub-amostra. Seja  $\alpha \geq 0$ , e seja  $B$  uma bola fechada em torno de  $x$  de raio  $r_{k-\text{NN}}(x)$  que contem  $K$  elementos da amostra,*

$$\#\{i = 1, 2, \dots, n: x_i \in B\} = K.$$

*Suponha que a fração de pontos de  $\sigma'$  contidos em  $B$  seja menor ou igual a  $\alpha$ ,*

$$\#\{i: x_i \in \sigma', x_i \in B\} \leq \alpha K,$$



e que da mesma forma, para a bola aberta,  $B^\circ$ ,

$$\#\{i : x_i \in \sigma', x_i \in B^\circ\} \leq \alpha \#\{i : x_i \in B^\circ\}.$$

Sob um desempate uniformemente aleatório de  $k$  vizinhos mais próximos, a fração esperada de pontos de  $\sigma'$  entre os  $k$  vizinhos mais próximos de  $x$  é menor ou igual a  $\alpha$ .

*Demonstração.* Aplica-se o lema 5.4.32 com  $\alpha_1$  e  $\alpha_2$  as frações de pontos de  $\sigma'$  na bola  $B$  e na esfera  $S = B \setminus B^\circ$  respectivamente,  $t_1 = \#\{B^\circ\}/\#\{B\}$ , e  $t_2$  a fração de pontos da esfera  $S = B \setminus B^\circ$  que temos de escolher aleatoriamente como vizinhos mais próximos de  $x$  faltados na bola aberta. Basta observar que a fração esperada de pontos de  $\sigma'$  entre os vizinhos mais próximos que pertencem à esfera é também igual a  $\alpha_2$  pois são escolhidos aleatoriamente seguindo uma distribuição uniforme.  $\square$

Agora chegamos ao resultado principal desta seção.

**Teorema 5.4.34.** *O classificador  $k$ -NN sob um desempate uniformemente aleatório de  $k$  vizinhos mais próximos é universalmente consistente em qualquer espaço métrico de dimensão de Nagata sigma-finita.*

*Demonstração.* Seja  $\Omega = \cup_{l=1}^{\infty} Y_n$ , onde  $Y_n$  tem dimensão de Nagata finita em  $\Omega$ . Segundo o exercício 5.4.27, pode-se supor que as  $Y_n$  formam uma cadeia crescente, e o exercício 5.4.26 permite supor que  $Y_n$  são borelianos. Sejam  $\mu$  e  $\eta$  quaisquer. Dado  $\epsilon > 0$ , existe  $l$  tal que  $\mu(Y_l) \geq 1 - \epsilon/2$ , e existe  $K$  compacto,  $K \subseteq Y_l$ , tal que  $\eta|_K$  é contínua e  $\mu(K) \geq 1 - \epsilon$ . A função  $\eta|_K$  se estende a uma função uniformemente contínua  $g$  sobre  $\Omega$ .

No espírito da prova do teorema de Stone 5.3.15, basta estimar por cima o termo

$$\begin{aligned} (B) &= \mathbb{E} \frac{1}{k} \sum \{|\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X), X \in K, X_i \notin K\} \\ &= \mathbb{E} \mathbb{E}_{j \sim \mu_{\#}} \frac{1}{k} \sum \{|\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X_j), X_j \in K, X_i \notin K, \\ &\quad i \in \{0, 1, \dots, n\} \setminus \{j\}\}, \end{aligned}$$

onde  $\mu_{\#}$  é a medida uniforme sobre o conjunto  $\{0, 1, 2, \dots, n\}$ , e  $X_0 = X$ . Vamos tratar do termo  $(B)$  como a soma de duas esperanças condicionais,  $(B_1)$  e  $(B_2)$ , segundo  $k$  vizinhos mais próximos de  $X_j$  dentro da amostra  $\{X_0, X_1, \dots, X_n\}$  contém mais ou menos de  $\sqrt{\epsilon}k$  elementos de  $U = \Omega \setminus K$ .

Usando o lema 5.4.30, aplicado às bolas fechadas de raio  $k\text{-NN}(X_j)$  bem como às

bolas abertas correspondentes, junto com lema 5.4.33, no primeiro caso temos

$$\begin{aligned}
 (B_1) &= \mathbb{E} \mathbb{E}_{j \sim \mu_{\#}} \left[ \frac{1}{k} \sum \{ |\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X_j), X_j \in K, X_i \notin K, \right. \\
 &\quad \left. i \in \{0, 1, \dots, n\} \setminus \{j\} \} \mid \#\{i : X_i \in k\text{-NN}(X_j), X_i \notin K\} \geq k\sqrt{\epsilon} \right] \\
 &\leq \mathbb{E} \frac{1}{k} 2\epsilon^{-1/2} (\delta + 1) \frac{1}{n} \#\{i = 0, 1, \dots, n : X_i \notin K\} \\
 &\leq 2\epsilon^{-1/2} (\delta + 1) \epsilon = 2\sqrt{\epsilon} (\delta + 1),
 \end{aligned}$$

onde usamos o fato e que a soma não excede  $k$ , e depois a Lei dos Grandes Números. No segundo caso,

$$\begin{aligned}
 (B_2) &= \mathbb{E} \mathbb{E}_{j \sim \mu_{\#}} \left[ \frac{1}{k} \sum \{ |\eta(X_i) - g(X_i)| : X_i \in k\text{-NN}(X_j), X_j \in K, X_i \notin K, \right. \\
 &\quad \left. i \in \{0, 1, \dots, n\} \setminus \{j\} \} \mid \#\{i : X_i \in k\text{-NN}(X_j), X_i \notin K\} \leq k\sqrt{\epsilon} \right] \\
 &\leq \frac{1}{k} k \sqrt{\epsilon} = \sqrt{\epsilon}.
 \end{aligned}$$

□

*Observação 5.4.35.* Uma boa referência para uma grande variedade de dimensões métricas, inclusive a de Nagata, é o artigo [Assouad e Quentin de Gromard 2006].

*Observação 5.4.36.* Teorema 5.4.34 inicialmente resultou de uma combinação dos resultados de [Preiss 1983] e [Cérou e Guyader 2006].

Um espaço métrico munido de uma medida de probabilidade,  $(\Omega, d, \mu)$ , satisfaz a *propriedade de Lebesgue–Besicovitch (forte)* se para toda  $f \in L^1(\mu)$

$$\frac{1}{\mu(B_\epsilon(x))} \int_{B_\epsilon(x)} f(x) d\mu(x) \rightarrow f(x)$$

em probabilidade (respectivamente, em quase toda parte).

Foi mostrado em [ibid.] que a propriedade de Lebesgue–Besicovitch implica que o classificador  $k$ -NN é consistente. (A prova estende a de [Devroye 1981], onde a ideia foi elaborada para  $\mathbb{R}^d$ .)

E segundo [Preiss 1983], um espaço métrico  $\Omega$  satisfaz a propriedade de Lebesgue–Besicovitch forte para cada medida de probabilidade  $\mu$  se e somente se  $\Omega$  tem a dimensão de Nagata sigma-finita. Isto implica o teorema 5.4.34.

(Mencionemos que a prova de Preiss foi muito curta, apenas um esboço. A suficiência foi elaborada de modo detalhado em [Assouad e Quentin de Gromard 2006], e a necessidade, em [Kumari 2018].)

A prova atual do teorema 5.4.34, assim como diversos exemplos do capítulo, aparecem na tese [ibid.].

*Observação 5.4.37.* Seja  $X$  um espaço métrico (separável e completo) tal que o classificador  $k$ -NN é universalmente consistente em  $X$ . Segue-se que  $X$  tinha dimensão de Nagata sigma finita?

A resposta positiva, modulo o resultado de [Cérou e Guyader 2006] mencionado acima, implicaria uma resposta positiva a uma pergunta da análise real, já bastante antiga [Preiss 1983]: não se sabe se  $\Omega$  tem a propriedade de Lebesgue–Besicovitch para cada medida de probabilidade se e somente se  $\Omega$  tem dimensão de Nagata sigma-finita.

*Observação 5.4.38.* Não enfrentamos aqui o problema de consistência universal forte do classificador  $k$ -NN. A consistência universal forte no espaço euclidiano foi estabelecida em [Devroye e Györfi 1985] e [Zhao 1987]. O argumento é o seguinte. Supondo que a medida  $\mu$  sobre  $\mathbb{R}^d$  (ou um espaço métrico qualquer) não admite empates (ou seja, cada esfera é  $\mu$ -neglenciável), para cada  $\alpha > 0$  e cada  $x$  existe o mínimo  $r = r(\alpha)(x) > 0$  tal que  $\mu(B_r(x)) = \alpha$ . Definamos a regra de aprendizagem  $\mathcal{L}_n$  em  $x$  pelo voto majoritário entre os rótulos de todos os pontos  $\sigma \cap B_{r(k/n)}(x)$ . Não é difícil a verificar que a regra  $\mathcal{L}_n$  e a regra  $k$ -NN são *mutualmente fortemente consistentes*, ou seja,

$$\text{erro}_{\mu,\eta} k\text{-NN} - \text{erro}_{\mu,\eta} \mathcal{L} \rightarrow 0$$

ao longo de quase todo caminho amostral. Segue-se em particular que  $\mathcal{L}$  é universalmente consistente. Usando o lema geométrico de Stone mais alguns argumentos topológicos, pode-se mostrar que o erro de classificação da regra  $\mathcal{L}_n$  é uma função Lipschitz contínua sobre  $\Omega^n \times \{0, 1\}^n$ , com a constante de Lipschitz uniformemente limitada. Usando o lema E.2.28, concluímos que  $\mathcal{L}$  é fortemente consistente, logo o mesmo vale para a regra  $k$ -NN.

O mesmo argumento se generaliza para espaços métricos de dimensão de Nagata sigma-finita na ausência de empates [Kumari 2018].

A condição de ausência de empates foi removida para espaço euclidiano em [Devroye, Györfi, Krzyżak et al. 1994].

*Observação 5.4.39.* Seja  $\mathcal{M}$  uma família de métricas sobre um espaço boreliano padrão, todas gerando a sua estrutura boreliana. Suponha que o classificador  $k$ -NN seja universalmente consistente em cada espaço métrico  $(\Omega, \rho)$ ,  $\rho \in \mathcal{M}$ . Formemos a regra de aprendizagem seguinte: dado uma amostra rotulada  $\sigma$ , seja  $\mathcal{L}_n(\sigma)$  o valor do classificador  $k$ -NN sobre  $\sigma$ , em relação à métrica  $\rho \in \mathcal{M}$  minimizando o erro empírico de classificador  $k$ -NN. Sobre quais condições sobre a família  $\mathcal{M}$  a tal regra será universalmente consistente? Intuitivamente, é o caso quando  $\mathcal{M}$  tiver uma “complexidade baixa”, ou, talvez, num sentido apropriado, estiver “uniformemente de dimensão de Nagata sigma-finita”. Seria interessante tentar e desenvolver uma pequena teoria, justificando a otimização do classificador  $k$ -NN sobre uma família de métricas (ou outras distâncias).

Algun trabalho nesta direção foi feito em [Hatko 2015].

O problema é importante porque já existem algoritmos deste tipo, tais como o classificador LMNN (*Large Margin Nearest Neighbour classifier*) nos espaços euclidianos [Weinberger e Saul 2009]. A pergunta que parece ficar em aberto é a seguinte: o classificador LMNN é universalmente consistente?

*Observação 5.4.40.* Tradicionalmente, o classificador de vizinhos mais próximos é estudado e usado no contexto dos espaços métricos (como neste capítulo), e sobretudo num espaço euclidiano  $\ell^2(d)$  de dimensão finita. Todavia, nenhum axioma de métrica é necessária para definir o classificador. Por outro lado, as “medidas de semelhança”  $d(x, y)$  intrínsecos a alguns domínios (por exemplo, biologia molecular) não são necessariamente simétricas, nem satisfazem a desigualdade triangular [Pestov e Stojmirović 2006]. A razão principal para a teoria ser quase exclusivamente desenvolvida para espaços métricos, é que ela é baseada sobre a teoria bem estabelecida das medidas de probabilidade em tais espaços, praticamente inexistente para conjuntos munidos de distâncias mais gerais (quasimétricas, etc.) Como já mencionamos, o âmbito natural para estudar e analisar os classificadores de vizinhos mais próximos seria um espaço boreliano padrão  $\Omega$  munido de uma família de pré-ordens  $\prec_x$ , uma para cada ponto  $x \in \Omega$ , compatíveis com a estrutura boreliana padrão separável no sentido que os intervalos geram a estrutura, onde a interpretação de  $y \prec_x z$  é que  $y$  fica mais perto de  $x$  que  $z$ . A única propriedade desejável seria  $y \prec_x x \Rightarrow y = x$ . Na presença de uma métrica (ou outra medida de semelhança),  $d$ , a pré-ordem é definida por

$$y \prec_x z \iff d(x, y) \leq d(x, z). \quad (5.12)$$

Pode-se argumentar que a teoria de classificadores de vizinhos mais próximos desta generalidade merece, seguramente, atenção.

É fácil verificar que, dado uma família de pré-ordens  $\prec_x$ ,  $x \in \Omega$  com a propriedade  $y \prec_x x \Rightarrow y = x$ , existe uma métrica  $d$  sobre  $\Omega$  que satisfaz Eq. (5.12). Deixemos isso como um exercício. Porém, tipicamente uma tal métrica vai gerar a topologia discreta, a uma estrutura boreliana não separável, e por isso vai ser inútil. Não é claro se a pergunta seguinte já foi tratada: sob quais condições existe uma tal métrica  $d$  que gera a estrutura boreliana original de  $\Omega$ ?

# 6

## *Redução de dimensionalidade*

---

Nos domínios de alta dimensão  $d \gg 1$ , vários algoritmos da ciência de dados muitas vezes levam muito tempo e tornam-se ineficientes. Por exemplo, nenhum classificador padrão vai funcionar se aplicado diretamente ao conjunto de dados seguinte.<sup>1</sup> Os dados são sequências genômicas,

$$X \subseteq \{A, T, G, C\}^d,$$

onde a “dimensão” (número de características)  $d \sim 870,000$ , enquanto a tamanho do conjunto não é muito grande ( $n \sim 6,000$ , os dados correspondem aos pacientes individuais). No entanto, já em dimensões baixas a médias (tais como 7) alguns algoritmos tornam-se visivelmente menos eficientes que em dimensões 1 ou 2. Este fenômeno é conhecido como a *maldição de dimensionalidade*.

Para remediar a situação, são usados vários algoritmos sob o nome comum de *redução de dimensionalidade*. Isto significa escolher uma função  $f: \Omega \rightarrow \Upsilon$  do domínio de dimensão alta,  $\Omega$ , para um domínio  $\Upsilon$  de dimensão mais baixa, transferindo o problema para lá. No contexto da aprendizagem supervisionada, a fim de classificar um ponto de dados  $x \in \Omega$  baseado sobre amostra rotulada  $\sigma$ , aplicamos um algoritmo de classificação no espaço  $\Upsilon$  ao ponto  $f(x)$  e à amostra  $f(\sigma)$ , esperando que o desempenho do algoritmo em  $\Upsilon$  seja mais eficaz de que em  $\Omega$  por causa da baixa dimensão, e que a função  $f$  conserve os padrões presentes no domínio  $\Omega$ .

Existem vários métodos de redução de dimensionalidade. Para alguns aspectos da teoria, a chamada extração de características, veja a coleção de artigos [Guyon et al. 2006].

---

<sup>1</sup>O do Instituto de Cardiologia da Universidade de Ottawa.

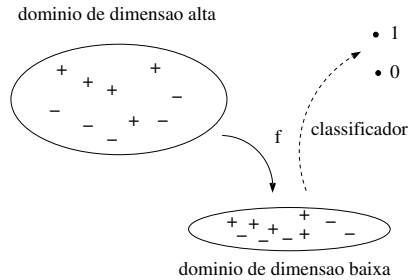


Figura 6.1: Redução de dimensionalidade

Ao mesmo tempo, parece que ainda não existe muita base teórica deste procedimento no contexto de aprendizagem de máquina. Isto é, em parte, porque o fenômeno de maldição de dimensionalidade em si mesmo é ainda mal entendido. (Considere, por exemplo, a “conjetura de maldição de dimensionalidade” em aberto, mencionada na subseção 3.2.5). Até mesmo não é ainda claro o que significa “dimensão alta” de um conjunto de dados: a teoria de dimensão correspondente não foi ainda elaborada. Por esta razão, qualquer apresentação do assunto será necessariamente inconclusiva, disjunta, e teoricamente insatisfatória. Porém, dado que o desafio é muito interessante do ponto de vista teórico bem como prático, arrisquemos incluir este capítulo.

Discutimos alguns aspectos da maldição de dimensionalidade, em particular o que pode significar uma “dimensão intrínseca alta” de dados, e as ligações com a concentração de medida. Depois, descrevemos um dos importantes algoritmos de redução de dimensionalidade, o método de projeções aleatórias baseado sobre o lema de Johnson–Lindenstrauss. Vamos discutir possíveis ligações do lema com aprendizagem supervisionada. Concluímos com a descrição de um novo algoritmo para redução de dimensionalidade, usando as funções injetoras borelianas, descontínuas em cada ponto – um resultado simples, que no entanto pode tornar-se uma ferramenta importante.

## 6.1 Maldição de dimensionalidade

Como nós já mencionamos, a natureza geométrica e algorítmica da maldição de dimensionalidade ainda resta um desafio teórico interessante. Nesta seção tentaremos entender um pouco, pelo menos ao nível intuitivo, a origem de alguns problemas que afetam o classificador  $k$ -NN. Por isso, o domínio vai ser um espaço métrico com medida de probabilidade,  $(\Omega, d, \mu)$ .

### 6.1.1 Geometria de busca por semelhança

O classificador  $k$ -NN precisa de um algoritmo eficaz para buscar os  $k$  vizinhos mais próximos do qualquer ponto  $x$  do domínio dentro da amostra,  $\sigma$ . Isto é onde os problemas começam nas altas dimensões, e intuitivamente, a origem de dificuldades é bastante clara.

Seja  $(\Omega, d, X)$  um domínio munido de uma métrica,  $d$ , e de uma amostra finita  $X = \{x_1, x_2, \dots, x_n\}$  (conjunto, ou *instância*, de dados). O triplo  $(\Omega, d, \sigma)$  é conhecido na teoria de busca por semelhança como uma *carga de trabalho de semelhança* (*similarity workload*). O que nos interessa, é a pesquisa de  $k$  vizinhos mais próximos (consulta  $k$ -NN) dentro de  $X$ , dado um ponto de consulta (*query point*),  $q$ . (A nossa notação aqui vai ser um pouco diferente da usada na aprendizagem estatística, porque nos passamos por uma parte diferente da informática).

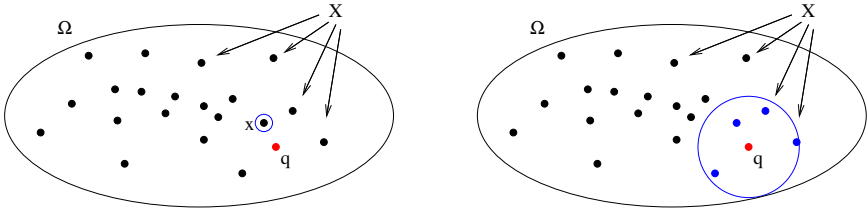


Figura 6.2: Consulta do vizinho mais próximo (esq.) e consulta de  $\varepsilon$ -intervalo (dir.)

Uma possibilidade é a busca completa sequencial de  $X$ , calculando todos os valores  $d(x_i, q)$ ,  $i = 1, 2, \dots, n$ , ordenando-os, e escolhendo  $k$  menores. Por exemplo, no caso de  $k = 1$ , o algoritmo pode ser definido como segue:

$$i = \arg \min_i d(x_i, q).$$

A complexidade temporal deste algoritmo é de  $O(n)$ , o número de passos a executar sendo proporcional a  $n$ . Frequentemente, é o mais rápido algoritmo conhecido. No entanto, ele se torna devagar demais se o número de pontos,  $n$ , é grande, ou a métrica é difícil a calcular. É desejável construir um *esquema de indexação*, ou seja, uma estrutura sobre  $(\Omega, d, X)$  capaz de executar uma busca mais rápida: de maneira ideal, no tempo  $\text{poly } \log n$ , ou  $\text{poly } d$ , onde  $d$  é a “dimensão”.

Um esquema de indexação permite executar *consultas de intervalo* (*range queries*): dado  $q \in \Omega$  e  $\varepsilon > 0$ , retornar todos  $x \in \bar{B}_\varepsilon(q) \cap X$ . (Depois, a busca binária permite reduzir a consulta  $k$ -NN a uma série de consultas de intervalo da maneira mais ou menos evidente e eficaz.) Um esquema de indexação tradicional, cingido ao essencial, consiste de uma família de funções reais  $f_i$ ,  $i \in I$  sobre  $\Omega$ , definidas totalmente ou parcialmente, que satisfazem a propriedade de Lipschitz com constante  $L = 1$ :

$$|f_i(x) - f_i(y)| \leq d(x, y). \quad (6.1)$$

(Por exemplo, os chamados esquemas baseados sobre pivôs usam como as funções  $f_i$  as da distância  $d(p_i, -)$  até os *pivôs* escolhidos, ou seja, pontos do domínio  $p_i \in \Omega$ .)

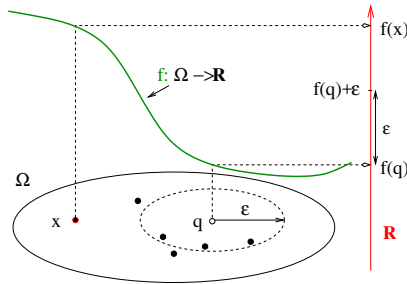


Figura 6.3: O ponto  $x$  pode ser descartado.

Dado uma consulta  $(q, \epsilon)$ , onde  $q \in \Omega$  e  $\epsilon > 0$ , o algoritmo escolhe recursivamente uma série de índices  $i_n$ , onde cada  $i_{n+1}$  está determinado pelos valores  $f_{i_m}(q)$ ,  $m \leq n$ . As funções  $f_i$  servem para descartar os pontos  $x_i$  que não podem responder à consulta. A saber, se  $|f_i(q) - f_i(x)| \geq \epsilon$ , então, segundo a propriedade 1-lipschitziana de  $f_i$ , temos  $d(q, x) \geq \epsilon$ . Assim, o ponto  $x$  é irrelevante e não precisa ser considerado (Figura 6.3).

Após o cálculo terminar, o algoritmo retorna todos os pontos que não podem ser descartados, e verifica cada um deles contra a condição  $d(x, q) < \epsilon$ .

Figura 6.4 ilustra o funcionamento do esquema onde as funções  $f_i$  são distâncias até pivôs. Apenas os pontos na região verde terão que ser examinadas.

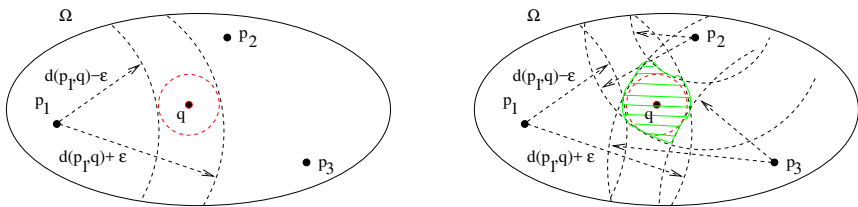


Figura 6.4: Busca do vizinho mais próximo com pivôs.

Uma observação importante aqui é que as funções  $f_i$ ,  $i \in I$  que formam um esquema de indexação geralmente exigem uma certa quantidade de pré-computação e armazenamento, principalmente os ponteiros para dados a ser descartados. Por isso, o tamanho do esquema,  $\#I$ , não pode ser ilimitado.

Por causa de concentração de medida, sobre as estruturas de alta dimensão, as funções lipschitzianas são concentradas em torno de seus valores médios (ou medianas). Esse efeito já é pronunciado em dimensões moderadas, tais como  $d = 14$  na Figura 6.5. Aqui a função é a distância de um pivô  $p$  escolhido aleatoriamente. As linhas verticais marcam



a distância média normalizada  $1 \pm \epsilon_{NN}$ , onde  $\epsilon_{NN}$  é a distância média do vizinho mais próximo. Supondo que o ponto de consulta  $q$  esteja a uma distância  $\approx 1$  de  $p$ , apenas os pontos fora da região marcada por barras verticais podem ser descartados.

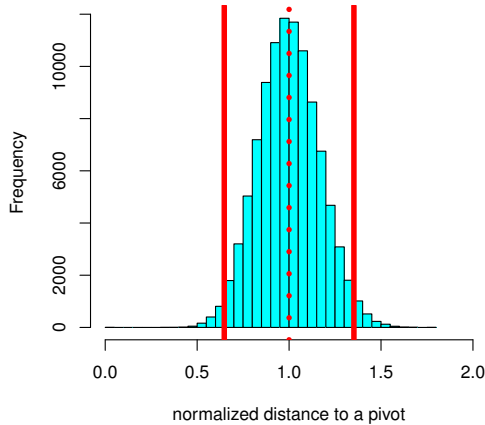


Figura 6.5: Histograma das distâncias a um ponto escolhido aleatoriamente em um conjunto de dados  $X$  com  $n = 10^5$  pontos, tirados de uma distribuição gaussiana em  $\mathbb{R}^{14}$ .

Isto conduz em particular ao efeito conhecido na ciência de dados como o “paradoxo do espaço vazio”, que afirma que a distância média  $\mathbb{E}(\epsilon_{NN})$  para o vizinho mais próximo aproxima-se à distância média  $\mathbb{E}(d)$  entre dois pontos de dados, quando a dimensão  $d$  cresce, desde que o número de dados,  $n$ , cresce apenas subexponencialmente em  $d$ . Figura 6.6 é auto-explicativa.

O fenômeno está também ilustrado na Figura 6.7 com o número de pontos constante ( $n = 10^3$  e  $n = 10^5$ ), e as distâncias normalizadas de modo que o *tamanho característico* do espaço gaussiano ( $\mathbb{R}^n, \gamma^n$ ),

$$\text{CharSize}(X) = \mathbb{E}_{\mu \otimes \mu}(d(x, y)), \quad (6.2)$$

seja igual a 1.

As duas propriedades combinadas implicam que, como  $d \rightarrow \infty$ , cada vez menos pontos podem ser descartados durante a execução de uma consulta de intervalo, e o desempenho de um esquema de indexação degrada rapidamente.

No entanto, já apenas o paradoxo de espaço vazio em si mesmo tem consequências imediatas para o classificador  $k$ -NN. Seja  $x \in \Omega$  um ponto qualquer. Denotemos  $r_{NN}(x)$  a distância de  $x$  para o seu vizinho mais próximo na amostra  $\sigma$ . Na consequência do

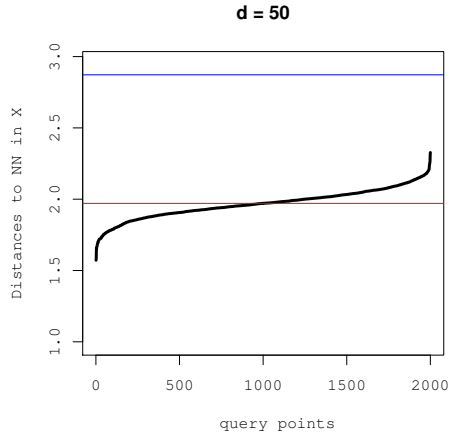


Figura 6.6: Distâncias de 2,000 pontos de busca aleatórios até seus vizinhos mais próximos dentro de um conjunto de 10,000 pontos aleatórios no cubo euclidiano  $[0, 1]^{50}$ . A linha horizontal inferior marca o valor mediano  $(r_{\text{NN}})_M = 1.9701$ , a linha vertical,  $\mathbb{E}d(x, y) = 2.872$ .

paradoxo de espaço vazio, uma grande quantidade de pontos de  $\sigma$  estão quase a mesma distância de  $x$  que o seu vizinho mais próximo. Mais formalmente, seja  $c > 0$ , e digamos, seguindo Beyer et al. 1999, que a consulta de vizinho mais próximo de  $x$  é  $c$ -instável se a bola de raio  $(1 + c)r_{\text{NN}}(x)$  centrada em  $x$  contém pelo menos metade dos pontos de  $\sigma$ . (Figura 6.8.)

Usando a concentração da medida, não é difícil de mostrar que, pelo  $c > 0$  fixo, no limite  $d \rightarrow \infty$  a maioria das buscas serão  $c$ -instáveis.

Nas dimensões baixas, o fenômeno está fraco (Figura 6.9, a esquerda, o conjunto de dados *Segment* da *UCI data repository*<sup>2</sup>), mas nas dimensões médias, é já pronunciado (Figura 6.9, a direita, o subconjunto aleatório da distribuição gaussiana em  $\mathbb{R}^{14}$ ). Aqui,  $k = 20$  e  $c = 0.5$ . A linha esquerda vertical corresponde ao valor médio de raio da bola que contém  $k$  vizinhos mais próximos,  $r_{k\text{-NN}}$ , e a segunda linha corresponde a  $(1 + c)r_{k\text{-NN}}$ . Para o conjunto *Segment*, a segunda bola contém em média 60 pontos. Para o gaussiano, o valor correspondente já é de 1,742 pontos.

O fenômeno da instabilidade significa uma perda da importância do fato de ser o vizinho mais próximo. Por exemplo, no caso de um erro quase inevitável de recuperação do vizinho mais próximo exato, o rótulo do vizinho substituído será mais ou menos aleatório. Além disso, a convergência de raio  $r_{k\text{-NN}}$  para zero, como no lema de Cover–Hart, será muito devagar. O desempenho do classificador  $k$ -NN (e de qualquer outro algoritmo

<sup>2</sup><http://archive.ics.uci.edu/ml/>

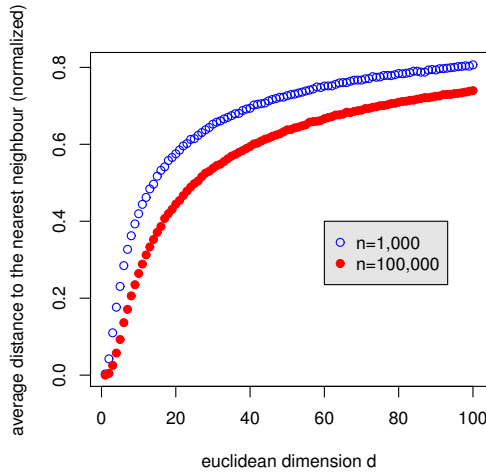


Figura 6.7: A distância média normalizada até o vizinho mais próximo dentro da amostra com  $n$  pontos tirada aleatoriamente da distribuição gaussiana em  $\mathbb{R}^d$ .

baseado sobre vizinhos mais próximos) degrada especialmente em dimensões altas, mas também em dimensões médias, mesmo se não tão notoriamente.

Apoiemos alguns dos argumentos empíricos acima com resultados concretos.

### 6.1.2 Paradóxo de espaço vazio e instabilidade da busca

Relembramos que a notação assintótica  $f(n) = O(g(n))$  significa que existe uma constante  $C > 0$  e um número natural  $N$  tais que  $|f(n)| \leq C|g(n)|$  para todos  $n \geq N$ . Neste caso também escrevemos  $g(n) = \Omega(f(n))$ . O fato  $f = O(g)$  e  $g = O(f)$  é expresso pela notação  $f = \Theta(g)$ . A notação  $f(n) = \omega(g(n))$  significa que  $f(n) = \Omega(g(n))$  e  $f(n) \neq O(g(n))$ , ou seja,  $f$  cresce estritamente mais rápido que  $g$ .

A fim de executar a análise assintótica, vamos trabalhar com uma *sequência infinita* de domínios,  $\Omega_d$ , bem como de conjuntos de dados  $X_d \subseteq \Omega_d$ ,  $d = 1, 2, \dots$ . Isso equivale a tirar um ponto único (caminho amostral),  $\bar{x}$ , no produto infinito

$$\Omega_1^{n_1} \times \Omega_2^{d_2} \times \dots \times \Omega_d^{n_d} \times \dots,$$

em relação ao produto infinito de medidas de probabilidade:

$$\bar{X} \sim \mu_1^{\otimes n_1} \otimes \mu_2^{\otimes d_2} \otimes \dots \otimes \mu_d^{\otimes n_d} \otimes \dots$$

A *confiança* neste contexto significa a medida de produto acima. Especificamente, a afirmação  $Q(d, \bar{x})$ , parametrizado pela dimensão  $d$  e aceitando como uma variável o caminho

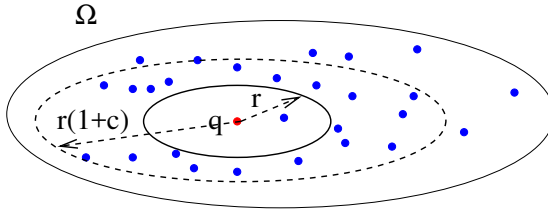


Figura 6.8: Instabilidade da busca do vizinho mais próximo.

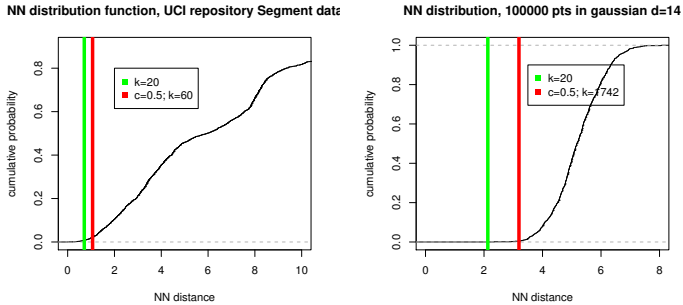


Figura 6.9: A fração média dos pontos de dados nas bolas de raio  $(1 + c)r_{k\text{-NN}}$ .

amostral, *ocorre assintoticamente com alta confiança* se para todo  $\delta > 0$  existe  $D$  tal que

$$P[Q(d, \bar{X}) \text{ é verdadeiro} ] > 1 - \delta$$

quando  $d \geq D$ .

Ao mesmo tempo, a fim de manter a notação simples, vamos suprimir o índice  $d$  e falar apenas de um domínio único  $\Omega$  e um conjunto de dados  $X \subseteq \Omega$ .

A fim de provar formalmente um resultado geral, aceitemos as seguintes hipóteses.

### Domínio como um espaço métrico com medida

O domínio métrico  $(\Omega, d)$  é munido de uma medida de probabilidade  $\mu$ , e dados estão tirados de  $\Omega$  de maneira i.i.d., seguinte a lei  $\mu$ .

### Normalização da distância

A distância  $d$  sobre o domínio é normalizada de modo que o *tamanho característico* de  $\Omega$  é constante:

$$\text{CharSize}(\Omega) = \mathbb{E}_{\mu \otimes \mu}(d) = \Theta(1).$$

### Dimensão intrínseca crescente

O domínio  $\Omega = \Omega_d$  tem “dimensão intrínseca  $\Omega(d)$ ” no sentido que a função de concentração de  $(\Omega, d, \mu)$  admite uma cota superior gaussiana

$$\alpha_\Omega(\varepsilon) = \exp(-\Omega(\varepsilon^2 d)).$$

### Tamanho de conjunto de dados

O número de pontos,  $n = \sharp X_d$ , cresce mais rápido do que alguma função polinomial em  $d$ , é mais devagar do que alguma função exponencial em  $d$ :

$$n = d^{\omega(1)}, \quad d = \omega(\log n). \quad (6.3)$$

*Observação 6.1.1.* A última hipótese é padrão na análise assintótica de esquemas de indexação para pesquisa de semelhança, veja [Indyk 2004]. Um exemplo da tal taxa de crescimento é  $n = 2^{\sqrt{d}}$ .

**Teorema 6.1.2.** *Sob as hipóteses acima, para cada  $\varepsilon > 0$ , assintoticamente com alta confiança todos pontos  $q \in \Omega$  exceto um conjunto de medida demasiado pequena  $\exp(-\Omega(\varepsilon^2 d))$ , satisfazem*

$$\left| r_{\text{NV}}^X(q) - \text{CharSize}(\Omega) \right| < \varepsilon.$$

**Corolário 6.1.3.** *Sob as hipóteses acima, para cada  $\varepsilon > 0$  e  $c > 0$ , assintoticamente com alta confiança, para todos pontos  $q \in \Omega$  exceto um conjunto de medida demasiado pequena  $\exp(-\Omega(\varepsilon^2 d))$ , a busca de intervalo de raio  $\varepsilon$  em ponto  $q$  é  $c$ -instável.*

Como um outro sub-produto da técnica, obtemos:

**Proposição 6.1.4.** *Sob as mesmas hipóteses, para todo  $\varepsilon > 0$  as distâncias dois a dois entre pontos de  $X$  são todos no intervalo  $\text{CharSize}(\Omega) \pm \varepsilon$ , assintoticamente com alta confiança.*

Sem perda de generalidade, normalizemos o tamanho característico de  $\Omega$  para 1. Para cada  $q \in \Omega$ , a função distância,  $d(q, -)$ , é 1-Lipschitz contínua, logo concentrada em torno do seu valor mediano,  $R(q)$ . Para evitar incerteza, escolhemos o *mínimo* valor mediano, que sempre existe (exercício).

**Exercício 6.1.5.** Mostrar que a função  $R: \Omega \rightarrow \mathbb{R}$ ,  $q \mapsto R(q)$  é Lipschitz contínua também, de constante 1.

Por conseguinte,  $R(q)$  concentra-se em torno do seu valor mediano, que denotemos por  $R_M$ .

**Exercício 6.1.6.** Deduza que para todos pontos  $q \in \Omega$  fora de um conjunto de medida demasiado pequena,  $\exp(-\Omega(\varepsilon^2 d))$ , a casca esférica,

$$\{x \in \Omega : R_M - \varepsilon \leq d(q, x) \leq R_M + \varepsilon\},$$

tem medida  $1 - \exp(-\Omega(\varepsilon^2 d))$ .

A probabilidade para pelo menos um ponto de  $X$  não pertencer à casca esférica como acima é limitada por

$$n \exp(-\Omega(\varepsilon^2 d)) = \exp(-\Omega(\varepsilon^2 d))$$

pois  $n$  cresce sub-exponencialmente em  $d$ . Para concluir a prova do teorema 6.1.2, precisamos do exercício seguinte.

**Exercício 6.1.7.** Mostre que, com a confiança  $1 - \exp(-\Omega(\varepsilon^2 d))$ ,

$$1 - R_M < \varepsilon.$$

Consideremos o conjunto  $A$  de todos pares  $(q, \bar{x})$  que satisfazem a conclusão do teorema 6.1.2. Nós estabelecemos que para todos  $q$  fora de um conjunto de medida  $\exp(-\Omega(\varepsilon^2 d))$ , a “faixa vertical” sobre  $q$ ,

$$\{\bar{x} : (q, \bar{x}) \in A\},$$

tem medida  $1 - \exp(-\Omega(\varepsilon^2 d))$ . O teorema de Fubini H.4.13 permite concluir que a medida de produto de  $A$  é  $1 - \exp(-\Omega(\varepsilon^2 d))$ . Por conseguinte, para todos caminhos amostrais  $\bar{x}$  fora de um conjunto de medida  $\exp(-\Omega(\varepsilon^2 d))$ , a “faixa horizontal”, ou seja, o conjunto de  $q \in \Omega$  tais que  $(q, \bar{x}) \in A$ , tem medida  $1 - \exp(-\Omega(\varepsilon^2 d))$ . Isso é exatamente a afirmação do teorema 6.1.2.

Segue-se que, qualquer que seja  $c > 0$ , para todos os pontos  $q$  fora de um conjunto da medida demasiado pequena, assintoticamente, a medida da bola de raio  $(1+c)r_{\text{NN}}^X(q)$  com centro em  $q$  converge para 1, como  $1 - \exp(-\Omega(c^2 d))$ . Isto estabelece a instabilidade de busca e o corolário 6.1.3.

Para mostrar proposição 6.1.4, fixemos  $\varepsilon > 0$ . Para dois elementos aleatórios de  $\Omega$ ,  $X_1$  e  $X_2$ , temos com confiança  $1 - n \exp(-O(d)\varepsilon^2)$  a propriedade  $|d(X_1, X_2) - R(X_1)| < \varepsilon/2$  (condicionando sobre  $X_1$ ). Dado uma amostra aleatória  $X$  com  $n$  pontos, concluímos que, com confiança  $1 - n^2 \exp(-O(d)\varepsilon^2)$ ,  $|d(x, y) - R(x)| < \varepsilon/2$  para todos  $x, y \in X$ . Ao mesmo tempo, com a confiança  $1 - n \exp(-O(d)\varepsilon^2)$ , temos  $|R(x) - 1| < \varepsilon/2$  para todos  $x \in X$ . Como  $n$  é subexponencial em  $d$ , o resultado segue-se.

### 6.1.3 Funções de dimensão intrínseca

Formular precisamente o que é a “dimensão intrínseca de dados” resta um desafio teórico na ciência de dados, tendo um significado prático bastante óbvio. Eis alguns objetivos que uma tal noção deveria cumprir.

1. Queremos que um valor elevado de dimensão intrínseca seja indicativo da presença da maldição da dimensionalidade.
2. O conceito não deve fazer qualquer distinção entre objetos contínuos e discretos, e a dimensão intrínseca de uma amostra discreta aleatória deve estar próxima da do domínio subjacente munido da lei de distribuição.
3. A dimensão intrínseca deve concordar com a nossa intuição geométrica e devolver valores usuais para objetos familiares, tais como esferas euclidianas ou cubos de Hamming.
4. Nós queremos o conceito ser insensível ao ruído aleatório da amplitude moderada.
5. Por fim, para ser útil, a dimensão intrínseca deve ser computacionalmente viável.

Vamos discutir uma abordagem, concentrando sobre os objetivos 1–3, que vão ser formalizados e transformados em três axiomas.

Para formalizar o objetivo 2, precisamos de uma noção de proximidade entre espaços métricos com medida, que concorde bem com o fenômeno de concentração. Sejam  $X = (X, d_X, \mu_X)$  e  $Y = (Y, d_Y, \mu_Y)$  dois espaços métricos (separáveis e completos) munidos de medidas borelianas de probabilidade. A ideia da distância de Gromov [Gromov 1999] é que  $X$  e  $Y$  serão próximos se toda função 1-Lipschitz contínua sobre  $X$  pode ser emparelhada com uma tal função sobre  $Y$ , e vice-versa. Relembramos (teorema E.2.1) que todo espaço probabilístico padrão,  $\Omega$ , pode ser *parametrizado* pelo intervalo unitário,  $[0, 1]$ : existe uma aplicação boreliana  $\phi: [0, 1] \rightarrow \Omega$  tal que a medida  $\mu$  é a imagem direta da medida de Lebesgue (uniforme),  $\lambda$ , sobre o intervalo:

$$\mu = \phi_*(\lambda),$$

ou seja, para todo subconjunto boreliano  $A \subseteq X$ ,

$$\mu_X(A) = \lambda(\phi^{-1}(A)).$$

Introduzimos a distância  $\text{me}_1$  sobre o espaço de funções borelianas sobre  $[0, 1]$  como segue:

$$\text{me}_1(f, g) = \inf \{ \epsilon > 0 : \lambda \{ t \in [0, 1] : |f(t) - g(t)| > \epsilon \} < \epsilon \}.$$

**Exercício 6.1.8.** Mostrar que  $\text{me}_1$  é uma pseudométrica, determinando a convergência em medida. (Releia a discussão no início da sub-seção 3.3.1).

Agora definemos a distância de Gromov,  $d_{\text{conc}}(X, Y)$ , como o ínfimo de todos  $\epsilon > 0$  admitindo algumas parametrizações  $\phi_X$  e  $\phi_Y$  de  $X$  e de  $Y$  respetivamente, tendo a propriedade seguinte. Para cada  $f \in \text{Lip}_1(X)$  existe  $g \in \text{Lip}_1(Y)$  tal que

$$\text{me}_1(f \circ \phi_X, g \circ \phi_Y) < \epsilon, \tag{6.4}$$

e vice versa: para cada  $g \in \text{Lip}_1(Y)$  existe  $f \in \text{Lip}_1(X)$  satisfazendo eq. (6.4).

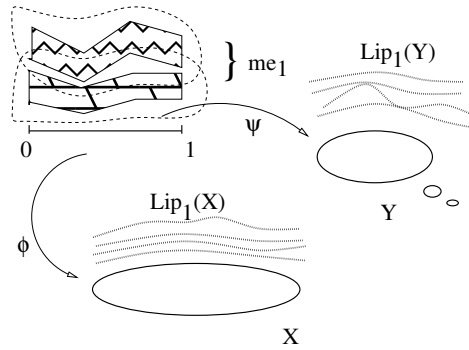


Figura 6.10: A noção da distância de Gromov

**Exercício 6.1.9.** Verificar que a distância  $d_{conc}$  é uma pseudométrica.

**Exercício 6.1.10.** Verificar que se  $d_{conc}(X, Y) = 0$ , então os espaços métricos com medida  $X = (X, d_X, \mu_X)$  e  $Y = (Y, d_Y, \mu_Y)$  são isomorfos, a saber: existe uma isometria  $f : \text{supp } \mu_X \rightarrow \text{supp } \mu_Y$  tal que  $f_*(\mu_X) = \mu_Y$ . (Este exercício é difícil, veja Th. 5.16 em [Shioya 2016]).

**Proposição 6.1.11.** *Seja  $X$  um espaço métrico com medida. Então,*

$$(d_{conc}(X, \{*\}) \leq \epsilon/2) \Rightarrow (\alpha(\epsilon) \leq \epsilon/2) \Rightarrow (d_{conc}(X, \{*\}) \leq \epsilon).$$

*Demonstração.* Suponha que  $d_{conc}(X, \{*\}) \leq \epsilon/2 < 1/2$  e seja  $A \subseteq X$  qualquer, com  $\mu(A) \geq 1/2$ . A função distância  $d_A(x) = d(A, x) = \inf\{d(a, x) : a \in A\}$  é 1-Lipschitz contínua, logo ela difere de uma função constante,  $c$ , pelo menos de  $\epsilon/2$  sobre um conjunto de medida  $> 1 - \epsilon/2$ . É claro que  $c \leq \epsilon/2$ , logo  $d_A$  apenas pode tomar valor  $> \epsilon$  sobre um conjunto da medida  $\leq \epsilon/2$ , significando  $\alpha(\epsilon) \leq \epsilon/2$ . Inversamente, se  $d_{conc}(X, \{*\}) \geq \epsilon$ , existe uma função 1-Lipschitz contínua,  $f$ , sobre  $X$ , que difere do seu valor mediano  $M = M_f$  pelo menos por  $\epsilon$  sobre um conjunto de medida  $\geq \epsilon$ . Por conseguinte, existem dois conjuntos,  $A$  e  $B$ , tais que  $\mu(A) \geq 1/2$ ,  $\mu(B) \geq \epsilon/2$ , e para todos  $a \in A$ ,  $b \in B$  temos  $|f(a) - f(b)| \geq \epsilon$ , ou seja,  $\alpha(\epsilon) \geq \epsilon/2$ .  $\square$

**Exercício 6.1.12.** Mostre que, para as esferas euclidianas, a distância de Gromov até um conjunto unitário é exatamente a solução da equação  $\alpha(S^n, \epsilon) = \epsilon/2$ , Fig. 6.11.

**Exercício 6.1.13.** Deduza que uma família  $(X_n)$  de espaços métricos com medida é uma família de Lévy se e somente se ela converge para o espaço unitário  $\{*\}$  em relação à métrica de Gromov:  $d_{conc}(X_n, \{*\}) \rightarrow 0$  quando  $n \rightarrow \infty$ .

*Observação 6.1.14.* A explicação intuitiva é a seguinte: quando uma sequência de conjuntos de dados mais se aproximar do conjunto unitário na distância de Gromov, mais se



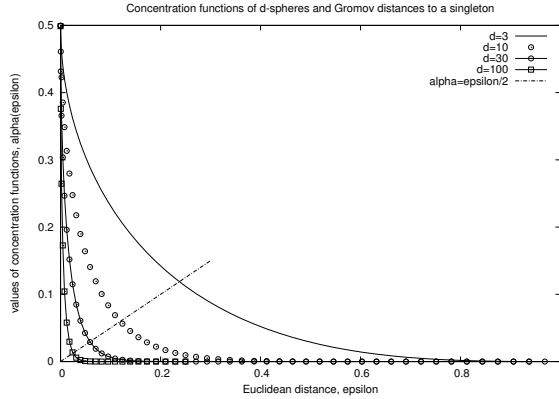


Figura 6.11: Funções de concentração das esferas  $\mathbb{S}^n$ ,  $n = 3, 10, 30, 100$ , e a reta  $\alpha = \epsilon/2$ .

assemelhar a um “buraco negro” do ponto de vista da ciência de dados, porque as “características” (funções Lipschitz contínuas) concentram-se e tornam-se cada vez menos discriminantes.

Agora seja  $\vartheta$  uma função assinando a cada espaço métrico com medida  $(X, d, \mu)$  ou um número real não negativo ou o símbolo  $+\infty$ . Digamos que  $\vartheta$  é uma *função de dimensão intrínseca* se ela satisfaz os três axiomas.

### Axioma de concentração

Dada uma família  $(X_n)$  de espaços métricos com medida,  $\vartheta(X_n) \uparrow \infty$  se e somente se  $(X_n)$  é uma família de Lévy.

Isto axioma formaliza o requerimento que a dimensão intrínseca é alta se e somente se o conjunto de dados sofre a maldição de dimensionalidade.

### Axioma de dependência suave de dados

Se  $d_{conc}(X_n, X) \rightarrow 0$ , então  $\vartheta(X_n) \rightarrow \vartheta(X)$ .

Este axioma garante, por exemplo, que a dimensão intrínseca de uma amostra aleatória é próxima à do domínio subjacente.

### Axioma de normalização

$$\vartheta(\mathbb{S}^n) = \Theta(n).$$

Relembremos que  $f(n) = \Theta(g(n))$  se existem constantes  $0 < c < C$  e  $N$  com  $c|f(n)| \leq |g(n)| \leq C|f(n)|$  para todos  $n \geq N$ . Neste caso, dizemos que  $f$  e  $g$  assintoticamente têm a mesma ordem de grandeza.

Este axioma serve para calibrar propriamente os valores da dimensão intrínseca.

*Observação 6.1.15.* Ao invés das esferas, podem ser usadas os hipercubos normalizados,  $\mathbb{I}^n$ , os cubos de Hamming normalizados, os espaços euclidianos munidas das medidas gaussianas, etc. — pode-se mostrar que as definições resultantes sejam equivalentes.

Os axiomas levam imediatamente a uma conclusão paradoxal. Como, por exemplo, as esferas euclidianas  $\mathbb{S}^n$  de raio um munidas da medida de probabilidade invariante pelas rotações formam uma família de Lévy normal (Apêndice I), eles convergem para o espaço trivial  $\{*\}$  na distância de Gromov, e os axiomas 1 e 2 (ou 2 e 3) implicam que

$$\partial(\{*\}) = +\infty.$$

O converso é também verdadeiro.

**Teorema 6.1.16.** *Seja  $\partial$  uma função de dimensão intrínseca. Então  $\partial(X) = +\infty$  se e somente se  $X$  é isomorfo a um espaço trivial,  $X \simeq \{*\}$ , ou seja, a medida  $\mu_X$  é uma medida de Dirac, suportada em um ponto.*

*Demonstração.* Se  $\partial(X) = +\infty$ , então a sequência constante  $X_n = X$  é uma família de Lévy. Por conseguinte,  $\alpha_X(\varepsilon) = 0$  para todos  $\varepsilon > 0$ , o que é apenas possível quando  $\mu$  é uma medida de Dirac (exercício).  $\square$

Assim, o único objeto de dimensão infinita em uma teoria é um espaço trivial, um conjunto unitário! Este paradoxo parece ser inevitável se alguém quer uma noção de dimensão intrínseca capaz de detectar a maldição da dimensionalidade. No entanto, isto não parece levar a quaisquer problemas ou inconvenientes.

Talvez ainda mais surpreendente é o fato de que uma função de dimensão satisfazendo os requisitos acima realmente existe.

**Exemplo 6.1.17.** Para um espaço métrico com medida  $(X, d, \mu)$ , definimos

$$\partial_{conc}(X) = \frac{1}{\left[2 \int_0^1 \alpha_X(\varepsilon) d\varepsilon\right]^2}. \quad (6.5)$$

**Exercício 6.1.18.** Verifique o axioma 1.

[ *Sugestão:* usar o teorema de convergência dominada de Lebesgue. ]

**Exercício 6.1.19.** Mostrar que se  $d_{conc}(X, Y) \leq \gamma$ , então para cada  $\varepsilon > 0$ ,

$$|\alpha(X, \varepsilon) - \alpha(Y, \varepsilon)| \leq 2\gamma.$$

[ *Sugestão:* mostrar e usar o fato que  $\alpha(X, \varepsilon)$  é o supremo de todos os valores de forma  $\mu_X\{x \in X : f(x) \geq M_f + \varepsilon\}$ , onde  $f$  é uma função 1-Lipschitz contínua. ] Deduzir o axioma 2.

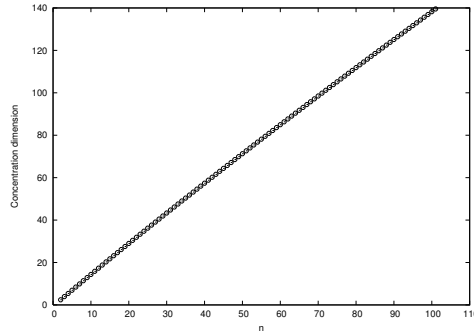


Figura 6.12: Dimensão  $\partial_{conc}$  de  $n$ -esferas para  $2 \leq n \leq 101$ .

**Exercício 6.1.20.** Verificar o axioma 3.

[ *Sugestão:* usar várias propriedades geométricas das esferas estabelecidas por Paul Lévy, do Apêndice I. ]

Eis uma ilustração do axioma de normalização.

**Exercício 6.1.21.** Seja  $(\Omega, d, \mu)$  um espaço métrico com medida de probabilidade. Mostre que, quando  $n \rightarrow \infty$ , temos as convergências quase certas:

1. Para cada  $\varepsilon > 0$ ,  $\alpha((\zeta_n, d|_{\zeta_n}, \mu_n), \varepsilon) \rightarrow \alpha(\Omega, \varepsilon)$ ,
2.  $d_{conc}((\zeta_n, d|_{\zeta_n}, \mu_n), \Omega) \rightarrow 0$ ,
3. se  $\partial$  é uma função de dimensionalidade intrínseca,  $\partial(\zeta_n, d|_{\zeta_n}, \mu_n) \rightarrow \partial\Omega$ .

[ *Sugestão:* use o lema de Cover–Hart. ]

*Observação 6.1.22.* A versão de dimensão intrínseca apresentada acima, como sugerida em [Pestov 2007], [Pestov 2008], foi desenvolvida recentemente em um cenário mais refinado e realista em [Hanika, Schneider e Stumme 2018].

## 6.1.4 Maldição de dimensionalidade para alguns esquemas de indexação

Obtenhamos alguns resultados mostrando a maldição de dimensionalidade para esquemas de indexação discutidos na subseção 6.1.1. O modelo consiste de:

1. Uma família  $\mathcal{F}$  de funções reais 1-Lipschitz contínuas sobre o domínio métrico  $\Omega$ , definidas parcialmente ou totalmente. As funções de tal família são aquelas funções 1-Lipschitz contínuas que podem ser computados da maneira eficaz.

2. Dado um conjunto de dados  $X \subseteq \Omega$ , constroi-se uma *esquema de indexação* para  $X$ . O esquema consiste de uma sub-família  $\mathcal{F}_X \subseteq \mathcal{F}$  de funções, submetidas à pré-computação, permitindo a execução do seguinte algoritmo. Dado uma subsequência finita de funções  $f_1, f_2, \dots, f_k \in \mathcal{F}_X$  e a correspondente sequência de valores  $f_i(q)$ , o algoritmo devolve ou uma nova função  $f_{k+1} \in \mathcal{F}_X$  para calcular  $f_{k+1}(q)$ , ou uma lista de pontos de  $X$  a examinar.
3. A lista de pontos devolvidos no final do cálculo deve incluir todos os pontos  $x \in X$  tais que, para todos  $f_1, \dots, f_k \in \mathcal{F}$  indicadas pelo algoritmo,  $|f_i(q) - f_i(x)| \leq \varepsilon$ , onde  $\varepsilon > 0$  é o raio de busca de intervalo inicial.
4. Para todos os pontos  $x$  na lista, a condição  $d(x, q) < \varepsilon$  é verificada, e os pontos satisfazendo-a são devolvidos pelo algoritmo.

Este tipo de esquema não é exclusivo, mas sim é muito comum. Para uma discussão mais detalhada com exemplos, consulte [Pestov e Stojmirović 2006], e para várias implementações na engenharia de dados, consulte [Chavez et al. 2001], [Samet 2006], [Santini 2001], [Yianilos 1993], [Zezula et al. 2006].

Precisamos de alguns resultados adicionais sobre a dimensão VC e a concentração de medida.

**Exercício 6.1.23.** Seja  $\mathcal{C}$  uma classe de conceitos, e  $k$  um número natural. Então a dimensão da classe

$$\mathcal{C}^{k \cdot \cap} = \{\cap \mathcal{A} : \mathcal{A} \subseteq \mathcal{C}, \#\mathcal{A} \leq k\},$$

que consiste de todas as interseções de  $\leq k$  conceitos de  $\mathcal{C}$ , satisfaz

$$\text{VC-dim}(\mathcal{C}^{k \cdot \cap}) \leq 2k \text{VC-dim}(\mathcal{C}) \log(k \text{VC-dim}(\mathcal{C})).$$

[ *Sugestão*: comece com o lema de Sauer–Shelah, e depois imite o jeito na página 69 baseado sobre lema 2.3.23. ]

**Proposição 6.1.24.** *Seja  $C$  um subconjunto boreliano não negligenciável de um espaço métrico com medida de probabilidade,  $(\Omega, d, \mu)$ . Denote  $\alpha_C$  a função de concentração de  $C$  em relação a métrica induzida  $d|_C$  e a medida de probabilidade induzida  $\mu|_C$ . Então para todos  $\varepsilon > 0$*

$$\alpha_C(\varepsilon) \leq \frac{\alpha_\Omega(\varepsilon/2)}{\mu(C)}.$$

*Demonstração.* Sejam  $\varepsilon > 0$  e  $\delta < \alpha_C(\varepsilon)$  quaisquer. Existem subconjuntos  $D, E \subseteq C$  a distância  $\geq \varepsilon$  um de outro, satisfazendo  $\mu(D) \geq \mu(C)/2$  e  $\mu(E) \geq \delta\mu(C)$ . Em particular, a medida de qualquer deles é pelo menos  $\delta\mu(C)$ . As  $\varepsilon/2$ -vizinhanças de  $D$  e  $E$  em  $\Omega$  não se encontram pela desigualdade triangular. Por conseguinte, uma deles tem a medida  $\leq 1/2$ , e o seu complemento em  $\Omega$ , denote-o  $F$ , tem a propriedade  $\mu(F) \geq 1/2$ .

Ao mesmo tempo,  $\mu(F_{\varepsilon/2}) \leq 1 - \delta\mu(C)$ , porque  $F_{\varepsilon/2}$  não encontra um de dois conjuntos,  $D$  ou  $E$ . Concluimos:  $\alpha_{\Omega}(\varepsilon/2) \geq \delta\mu(C)$ , e, formando o supremo sobre todos  $\delta < \alpha_C(\varepsilon)$ ,

$$\alpha_{\Omega}(\varepsilon/2) \geq \alpha_C(\varepsilon)\mu(C).$$

Em outras palavras,  $\alpha_C(\varepsilon) \leq \alpha_{\Omega}(\varepsilon/2)/\mu(C)$ , como desejado.  $\square$

**Corolário 6.1.25.** *Sejam  $C$  um subconjunto boreliano não negligenciável de um espaço métrico com medida de probabilidade,  $(\Omega, d, \mu)$ , e  $f : C \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua. Seja  $M$  um valor mediano de  $f$  sobre  $C$ . Então, para cada  $\varepsilon > 0$ ,*

$$\mu\{x \in C : |f(x) - M| > \varepsilon\} \leq 2\alpha(\Omega, \varepsilon/2).$$

*Demonstração.*

$$\begin{aligned} \frac{1}{\mu(C)}\mu\{x \in C : |f(x) - M| > \varepsilon\} &= \mu_C\{x \in C : |f(x) - M| > \varepsilon\} \\ &\leq 2\alpha(C, \varepsilon) \\ &\leq \frac{2}{\mu(C)}\alpha(\Omega, \varepsilon/2). \end{aligned}$$

$\square$

Seja  $\mathcal{F}$  uma classe de funções reais sobre  $\Omega$  (possivelmente parcialmente definidas). Denote  $\mathcal{F}_{\geq}$  a família de todos os subconjuntos

$$\{\omega \in \text{dom } f : f(\omega) \geq a\}, \quad a \in \mathbb{R}.$$

O resultado seguinte é uma variação sobre os resultados de [Pestov 2012, 2013b].

**Teorema 6.1.26.** *Suponha que o domínio  $\Omega$ , munido de uma métrica  $d$  e uma medida de probabilidade  $\mu$ , tem o tamanho característico  $\mathbb{E}_{\mu^2}d(X, Y) = 1$  e a função de concentração subgaussiana com expoente  $\Theta(d)$ :*

$$\alpha_{\Omega}(\varepsilon) = \exp(-\Theta(\varepsilon^2 d)). \quad (6.6)$$

*Seja  $\mathcal{F}$  a família de todas as funções 1-Lipschitz contínuas sobre  $\Omega$  usadas para escolher as funções de decisão para um esquema particular. Suponha que  $VC\text{-dim}(\mathcal{F}_{\geq}) = \text{poly}(d)$  é polinomial em  $d$ . Seja  $X$  uma amostra aleatória i.i.d. com  $n$  pontos de  $\Omega$  seguindo a lei  $\mu$ , onde  $n$  é superpolinomial e subexponencial em  $d$ ,  $d = n^{o(1)}$  e  $d = \omega(\log n)$ . Então cada esquema de indexação para busca de vizinho mais próximo em  $X$  de tipo descrito acima, usando as funções de decisão de uma sub-família  $\mathcal{F}_X \subseteq \mathcal{F}$  de tamanho  $\text{poly}(n)$ , tem o tempo esperado médio da execução superpolinomial em  $d$ ,  $d^{\omega(1)}$ .*

Fixemos um valor  $0 < \varepsilon_0 < 1$  estritamente positivo qualquer, por exemplo,  $\varepsilon_0 = 1/2$ . Para cada  $f \in \mathcal{F}$  definimos os conjuntos

$$\begin{aligned} \text{Out}_f &= \left\{ x \in \text{dom } f : |f(x) - M_f| > \frac{\varepsilon}{4} \right\}, \\ \text{In}_f &= \text{dom } f \setminus \text{Out}_f, \end{aligned}$$

onde  $M_f$  é o valor mediano de  $f$  sobre o seu domínio de definição.

**Exercício 6.1.27.** Deduza que a dimensão de Vapnik–Chervonenkis da classe  $\mathcal{D} = \{\text{In}_f : f \in \mathcal{F}\}$  é polinomial em  $d$ .

Seja  $k$  o comprimento esperado da sequência  $f_1, \dots, f_i$  de funções geradas pelo algoritmo de busca sobre todos os conjuntos de dados  $X$  e todos os centros de busca  $q$  de raio  $\varepsilon$ . Se  $k$  é superpolinomial em  $d$ , não tem nada a mostrar. Senão, segue-se do exercício 6.1.23 que a dimensão VC da classe  $\mathcal{D}^{k \cap}$  de todas as interseções de  $\leq k$  elementos de  $\mathcal{D}$  é  $\text{poly } d$  também. Segundo o teorema de Glivenko–Cantelli, quando  $d, n \rightarrow \infty$ , com confiança  $1 - \exp(-\Theta(-\varepsilon^2 d))$ , a medida empírica de todos os elementos de  $\mathcal{D}^{k \cap}$  difere da medida  $\mu$  por menos de  $\varepsilon/4$ .

Agora seja  $X$  um conjunto de dados qualquer fixo tendo a propriedade acima. Um esquema de indexação está escolhida neste momento. Segundo a nossa hipótese, a subclasse  $\mathcal{F}_X \subseteq \mathcal{F}$  satisfaz  $\#\mathcal{F}_X = \text{poly}(n)$ . Um centro de busca  $q$ , um elemento aleatório de  $\Omega$ , satisfaz

$$\begin{aligned} P \left[ q \in \bigcup_{f \in \mathcal{F}_X} \text{Out}_f \right] &\leq \#\mathcal{F}_X \cdot \alpha(\Omega, \varepsilon/8) \\ &= \exp(-\Theta(-\varepsilon^2 d)). \end{aligned}$$

Em outras palavras, com confiança  $1 - \exp(-\Theta(-\varepsilon^2 d))$ , qualquer seja  $f \in \mathcal{F}_X$ , se  $q$  pertence a  $\text{dom } f$ , então  $q \in \text{In}_f$ . Além disso, com alta confiança, a vizinho mais próximo de  $q$  dentro de  $X$  vai ser a distância  $\geq \varepsilon_0$ . Fixemos um  $q$  qualquer com estas duas propriedades.

A série de buscas de intervalo para determinar o vizinho mais próximo vai necessariamente incluir a busca de intervalo com o centro  $q$  e um raio  $\geq \varepsilon_0/4$ . Executemos uma tal busca. Sejam  $f_i, i = 1, \dots, k$  funções elementos de  $\mathcal{F}_X$  escolhidos pelo algoritmo para calcular os valores em  $q$ . Como  $q \in \text{dom } f_i$  para todos  $i$ , temos

$$|f_i(q) - M_f| < \frac{\varepsilon}{4}, \quad i = 1, 2, \dots, k.$$

Os pontos de  $X$  que não pertencem ao conjunto  $\cup\{\text{Out}_{f_i} : i = 1, 2, \dots, k\}$  têm que ser

devolvidos. Temos:

$$\begin{aligned} \#\{x \in X : x \notin \cup_{i=1}^k \text{Out}_{f_i}\} &= n \mu_{\#} \left[ \Omega \setminus \cup_{i=1}^k \text{Out}_{f_i} \right] \\ &\geq n \left( \mu \left[ \Omega \setminus \cup_{i=1}^k \text{Out}_{f_i} \right] - \varepsilon/2 \right) \\ &\geq \frac{n}{2} \\ &= d^{\omega(1)}. \end{aligned}$$

□

O resultado seguinte (que mencionemos sem demonstração) sugere que, para todos os fins práticos, a hipótese  $\text{VC-dim}(\mathcal{F}_{\geq}) = \text{poly}(d)$  é razoável.

**Teorema 6.1.28** (Goldberg e Jerrum [1995], Theorem 2.3). *Seja*

$$\mathcal{F} = \{x \mapsto f(\theta, x) : \theta \in \mathbb{R}^s\}$$

*uma classe parametrizada de funções binárias. Suponha que, para todo input  $x \in \mathbb{R}^n$ , existe um algoritmo calculando  $f(\theta, x)$ , e o cálculo precisa ao máximo  $t$  operações dos seguintes tipos:*

- *os operações aritméticas  $+$ ,  $-$ ,  $\times$  e  $/$  sobre reais,*
- *saltos condicionados sobre  $>$ ,  $\geq$ ,  $<$ ,  $\leq$ ,  $=$ , e  $\neq$  comparações de reais, e*
- *saida 0 ou 1.*

*Então  $\text{VC-dim}(\mathcal{F}) \leq 4s(t + 2)$ .*

□

Aliás, a dimensão  $s$  do espaço de parâmetros  $\mathbb{R}^s$  não pode ser superpolinômio em  $d$ , pois neste caso já lendo o parâmetro vai demorar o tempo  $d^{\omega(1)}$ .

**Exercício 6.1.29.** Tente mostrar o teorema de Goldberg e Jerrum usando as técnicas desenvolvidas na prova do teorema 2.3.20.

## 6.2 Lema de Johnson–Lindenstrauss

### 6.2.1 Formulação do resultado e discussão preliminar

**Teorema 6.2.1** (Lema de Johnson–Lindenstrauss). *Seja  $X$  um subconjunto com  $n$  elementos num espaço de Hilbert  $\mathcal{H}$ , e seja  $0 < \epsilon \leq 1$  qualquer. Existe um operador linear  $T : \mathcal{H} \rightarrow \ell^2(k)$ , onde*

$$k = O(\epsilon^{-2} \log n),$$

*tal que*

$$(1 - \epsilon) \|x - y\| < \|T(x) - T(y)\| < (1 + \epsilon) \|x - y\|$$

*para todos  $x, y \in X$ .*

Vamos deduzir valores concretos das constantes na nossa demonstração. A saber, o nosso argumento em particular vai mostrar que se  $n \geq 96$ , então a dimensão  $k$  é no máximo

$$k \leq \left\lceil \frac{65 \log n}{\epsilon^2} \right\rceil.$$

(Certamente, as cotas não são ótimas e podem ser melhoradas).

Obviamente, pode-se supor que  $\dim \mathcal{H} \leq n$ , substituindo  $\mathcal{H}$  pelo espaço linear gerado por  $X$ . No entanto, o espaço  $T(\mathcal{H})$  tem dimensão logarítmica em  $n$ . O resultado, originalmente motivado pelas necessidades da análise funcional, tornou-se uma ferramenta importante na informática teórica bem como prática. O lema é sujeito a muita pesquisa contemporânea.

Chama a atenção a consequência seguinte do resultado, bastante surpreendente. Se um espaço de Hilbert  $\mathcal{H}$  contiver um sistema ortogonal de  $n$  vetores, então, obviamente, a dimensão de  $\mathcal{H}$  seria maior ou igual à  $n$ . Agora, chamamos um sistema de vetores  $\epsilon$ -quase ortogonal se o ângulo entre quaisquer dois vetores distintos pertence ao intervalo  $\pi/2 \pm \epsilon$ . O lema de Johnson–Lindenstrauss, aplicada aos vetores básicos  $e_1, e_2, \dots, e_n$ , implica a existência de sistemas  $\epsilon$ -quase ortogonais de tamanho *exponencial* em dimensão do espaço de Hilbert, para um  $\epsilon > 0$  fixo.

Agora fazemos algumas preparações para a demonstração. Substituamos  $\mathcal{H}$  por  $\ell^2(n)$ . Vamos reduzir o problema para um de geometria da esfera euclidiana. Com esta finalidade, formemos o conjunto

$$Y = \left\{ \frac{x - y}{\|x - y\|} : x, y \in X, x \neq y \right\}. \quad (6.7)$$

Temos:  $Y \subseteq \mathbb{S}^{n-1}$  e  $|Y| = n(n-1)/2$ . É claro que basta mostrar a existência de um operador linear  $T$  tendo a propriedade seguinte:

$$\forall y \in Y, \quad 1 - \epsilon < \|Ty\| < 1 + \epsilon. \quad (6.8)$$

Em outras palavras,  $T$  envia  $Y$  dentro a casca esférica de espessura  $2\epsilon$ . De fato, basta mostrar que existe uma constante  $M > 0$  tal que

$$\forall y \in Y, \quad (1 - \epsilon)M < \|Ty\| < (1 + \epsilon)M. \quad (6.9)$$

Neste caso, podemos substituir  $T$  pelo operador linear  $M^{-1}T$  e obter (6.8).

Denotemos por  $p_k$  a projeção ortogonal de  $\mathcal{H} = \ell^2(n)$  sob o sub-espaço gerado pelas  $k$  primeiras coordenadas. Como  $p_k$  é um operador linear de norma um, a função  $f = \|\cdot\| \circ p_k$  é 1-Lipschitz contínua. A prova clássica do lema de Johnson–Lindenstrauss é baseada sobre a concentração dessa função, restrita sobre a esfera, em torno do seu valor mediano:

$$\mathbb{S}^{n-1} \ni x \mapsto f(x) = \|p_k(x)\| = \left( \sum_{i=1}^k x_i^2 \right)^{1/2} \in \mathbb{R}. \quad (6.10)$$



Aqui, a medida na esfera unitária é a medida de Haar, ou seja, a única medida boreliana de probabilidade invariante pelas rotações da esfera, veja seção (I.2.2). A distância na esfera é euclidiana.

Vamos estimar o valor mediano  $M_f$ , fazendo isso em poucas etapas. Primeiramente, note que a esperança do quadrado de  $f$  pode ser calculada exatamente:

$$\begin{aligned}\mathbb{E}(f^2) &= \mathbb{E}\left(\sum_{i=1}^k x_i^2\right) \\ &= \sum_{i=1}^k \mathbb{E}(x_i^2) \\ &= \frac{k}{n},\end{aligned}$$

porque para  $n = k$  temos

$$\mathbb{E}(f^2) = 1 = \sum_{i=1}^n \mathbb{E}(x_i^2) = n\mathbb{E}(x_i^2)$$

e  $\mathbb{E}(x_i^2)$  são todas iguais para  $i = 1, 2, \dots, n$  por consideração de simetria.

Como  $f \geq 0$ , temos  $(M_f)^2 = M_{f^2}$ . Então, bastaria estimar o valor mediano de  $f^2$ . Isso parece ser possível graças à observação feita no exercício 4.1.3: sobre as estruturas de alta dimensão, o valor mediano e o valor médio são próximos. Infelizmente, a diferença entre dois valores dada pelo exercício é da ordem de grandeza maior do que a esperança! Esse argumento sim se aplica à função  $f$ , e não a  $f^2$ . E não se pode limitar  $\mathbb{E}(f)$  por baixo através de  $\mathbb{E}(f^2)$  de modo útil. Segundo a desigualdade de Jensen,  $|\mathbb{E}(f)| \leq (\mathbb{E}(f^2))^{1/2}$ , mas este é o sentido errado. A desigualdade de Hölder implica que  $\mathbb{E}f^2 \leq \mathbb{E}f \cdot \sup f = \mathbb{E}f$ , mas esta estimativa é fraca demais, como será visto.

A solução será fornecida pelo fato que sobre as estruturas de alta dimensão, a variância de uma função Lipschitz contínua,

$$\text{var } f = \mathbb{E}(f - \mathbb{E}f)^2 = \mathbb{E}(f^2) - \mathbb{E}(f)^2,$$

é pequena. Então, o nosso plano de trabalho é o seguinte: de  $\mathbb{E}(f^2)$  para  $\mathbb{E}(f)$ , e depois para  $M_f$ .

## 6.2.2 Mais resultados sobre a concentração de medida

Começemos com a prova do exercício 4.1.3.

**Lema 6.2.2.** *Seja  $(X, d, \mu)$  um espaço métrico separável munido de uma medida boreliana de probabilidade, e seja  $f : X \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua. Então,*

$$|\mathbb{E}f - M_f| \leq \int_0^\infty \alpha_X(\epsilon) d\epsilon. \quad (6.11)$$

*Demonstração.* Denotemos

$$A_{\pm} = \{x \in X : f(x) \gtrless M_f\}.$$

Agora,

$$\begin{aligned} |\mathbb{E}f - M_f| &= \left| \int_{A_+} (f - M_f) d\mu - \int_{A_-} (M_f - f) d\mu \right| \\ &\leq \max \left\{ \left| \int_{A_+} (f - M_f) d\mu \right|, \left| \int_{A_-} (M_f - f) d\mu \right| \right\}, \end{aligned}$$

porque ambas integrais são positivas. Basta estimar uma delas, por exemplo  $A_+$ . Como  $M_f$  é um valor mediano de  $f$ , o valor da medida de  $A_{\pm}$  é pelo menos  $1/2$ . Como a função  $f$  é 1-Lipschitz contínua, temos

$$\{x : f(x) \geq M_f + \epsilon\} \subseteq \{x : x \notin (A_-)_{\epsilon}\},$$

e por conseguinte

$$\mu\{x : f(x) \geq M_f + \epsilon\} \leq \alpha_X(\epsilon). \tag{6.12}$$

Para calcular a integral, dividimos o volume entre o gráfico de  $f$  e o nível  $M_f$  acima do conjunto  $A_+$  em faixas horizontais infinitesimais (Fig. 6.13).

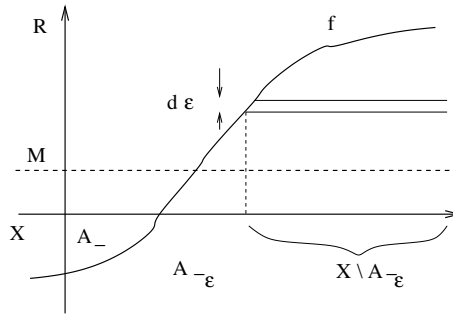


Figura 6.13: Estimando  $\int_{A_+} (f - M_f) d\mu$ .

Segue-se que o volume da cada faixa é aproximada (menos as quantidades de alta ordem) por  $\alpha(\epsilon) d\epsilon$ . □

**Corolário 6.2.3.** *Suponha que a função de concentração admita uma cota superior gaussiana,*

$$\alpha_X(\epsilon) \leq C_1 \exp(-C_2 \epsilon^2 n). \tag{6.13}$$

Então para toda função  $f$  1-Lipschitz contínua sobre  $X$  temos

$$|\mathbb{E}f - M_f| \leq \frac{C_1\sqrt{\pi}}{2\sqrt{C_2n}}. \quad (6.14)$$

*Demonstração.*

$$\begin{aligned} \int_0^\infty \exp(-C_2\epsilon^2n) d\epsilon &= \frac{1}{\sqrt{C_2n}} \int_0^\infty \exp(-C_2\epsilon^2n) d(\sqrt{C_2n}\epsilon) \\ &= \frac{\sqrt{\pi}}{2\sqrt{C_2n}}. \end{aligned}$$

□

**Corolário 6.2.4.** *Se  $f$  é uma função real 1-Lipschitz contínua sobre a esfera euclidiana  $\mathbb{S}^{n-1}$ , então*

$$|\mathbb{E}f - M_f| \leq \frac{5\sqrt{2\pi}}{2\sqrt{n}}. \quad (6.15)$$

De mesma maneira, pode-se estimar a variância de uma função 1-Lipschitz contínua sobre um espaço de alta dimensão.

**Lema 6.2.5.** *Seja  $(X, d, \mu)$  um espaço métrico separável munido de uma medida boreliana de probabilidade, e seja  $f : X \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua. Então,*

$$\text{var } f \leq 2 \int_0^\infty \alpha_X(\sqrt{\epsilon}) d\epsilon \quad (6.16)$$

*Demonstração.*

$$\begin{aligned} \text{var } f &= \mathbb{E}((f - \mathbb{E}f)^2) \\ &= \mathbb{E}(f - M_f + M_f - \mathbb{E}f)^2 \\ &= \mathbb{E}((f - M_f)^2) + 2\mathbb{E}(f - M_f)(M_f - \mathbb{E}f) + (M_f - \mathbb{E}f)^2 \\ &= \mathbb{E}((f - M_f)^2) - (M_f - \mathbb{E}f)^2 \\ &\leq \mathbb{E}((f - M_f)^2). \end{aligned}$$

Dividamos de novo a imagem em faixas infinitesimais de altura  $d\epsilon$  para notar que

$$\mu\{x \in X : (f(x) - M_f)^2 \geq \epsilon\} \leq \mu\{x \in X : |f(x) - M_f| \geq \sqrt{\epsilon}\} \leq 2\alpha_X(\sqrt{\epsilon}).$$

Isso nos dá a estimativa

$$\mathbb{E}((f - M_f)^2) \leq 2 \int_0^\infty \alpha_X(\sqrt{\epsilon}) d\epsilon.$$

□

**Corolário 6.2.6.** *Temos, para uma função 1-Lipschitz contínua  $f$  qualquer sobre a esfera  $\mathbb{S}^{n-1}$ :*

$$\text{var } f \leq \frac{20}{n}.$$

*Demonstração.*

$$\begin{aligned} \int_0^\infty \alpha_X(\sqrt{\epsilon}) d\epsilon &\leq 5 \int_0^\infty \exp(-\epsilon n/2) d\epsilon \\ &= \frac{10}{n} \int_0^\infty \exp(-\epsilon n/2) d(\epsilon n/2) \\ &= \frac{10}{n}. \end{aligned}$$

□

### 6.2.3 Estimativa do valor mediano de $f$

Reunindo nossas observações sobre a função  $f$  definida na eq. (6.10), obtemos:

$$\mathbb{E}(f^2) = \frac{k}{n}, \quad |\mathbb{E}f - M_f| \leq \frac{5\sqrt{2\pi}}{2\sqrt{n}}, \quad \text{var } f \leq \frac{20}{n}.$$

A última significa:

$$|\mathbb{E}(f^2) - (\mathbb{E}f)^2| \leq \frac{20}{n}.$$

Por conseguinte,

$$(\mathbb{E}f)^2 \geq \frac{k-20}{n}, \quad \mathbb{E}f \geq \frac{\sqrt{k-20}}{\sqrt{n}}$$

e

$$M_f \geq \frac{\sqrt{k-20} - (5/2)\sqrt{2\pi}}{\sqrt{n}}.$$

Assumindo que  $k$  seja bastante grande de modo que

$$\sqrt{k-20} - (5/2)\sqrt{2\pi} > \frac{\sqrt{k}}{4}$$

(este será o caso a partir de  $k \geq 96$ ), chegamos a uma cota inferior razoável:

$$M_f > \frac{\sqrt{k}}{4\sqrt{n}}. \tag{6.17}$$

### 6.2.4 Prova do lema de Johnson–Lindenstrauss

Seja  $f$  a função definida na eq. (6.10), e  $u \in O(n)$  uma transformação ortogonal.

**Exercício 6.2.7.** Verificar que o valor  ${}^u f(x)$  é igual à norma da imagem de  $x$  pela projeção ortogonal sobre o espaço de dimensão  $k$  de  $\ell^2(n)$  gerado pelas imagens  $u(e_1), u(e_2), \dots, u(e_k)$ . Em outras palavras,

$${}^u f(x) = \|u^* p_k u(x)\|.$$

É claro que todo sub-espaço de dimensão  $k$  pode ser obtido desse modo.

Vamos aplicar o lema I.3.21 à função  ${}^u f$ , ao conjunto finito  $Y \subseteq \mathbb{S}^{n-1}$  definido na eq. (6.7), assim que ao valor

$$\epsilon' = \epsilon M_f.$$

A condição (I.10) sobre a cardinalidade de  $F = Y$  no lema torna-se assim:

$$\frac{n(n-1)}{2} = |Y| < \frac{1}{4} \exp(\epsilon^2 M_f^2 n/2),$$

e, tendo em vista eq. (6.17), a cota será verificada uma vez temos

$$\begin{aligned} \frac{n^2}{2} &< \frac{1}{4} \exp\left(\epsilon^2 \left(\frac{\sqrt{k}}{4\sqrt{n}}\right)^2 n/2\right) \\ &= \frac{1}{4} \exp(\epsilon^2 k/32). \end{aligned}$$

Aplicando o logaritmo natural, resolvemos a desigualdade para obter

$$2 \log n < \frac{\epsilon^2 k}{32} - \log 2,$$

ou

$$k > \frac{64 \log n}{\epsilon^2} + 32 \log 2.$$

Isso é satisfeito, por exemplo, quando

$$k > \frac{65 \log n}{\epsilon^2}.$$

Obtemos a eq. (6.9) com  $T = u^{-1} p_k u$ , módulo a observação no exercício 6.2.7.  $\square$

**Exercício 6.2.8.** Implemente o algoritmo das projeções aleatórias em R e aplique ao conjunto de dados *Phoneme* (página 6), combinando com o classificador  $k$ -NN, ou melhor, um ensemble de classificadores  $k$ -NN combinados com várias projeções. (Se você conseguiu melhorar o desempenho do classificador, você fez melhor do que eu ou meus alunos).

## 6.2.5 Discussão: projeções aleatórias e aprendizagem

O lema de Johnson–Lindenstrauss foi mostrada em artigo [Johnson e Lindenstrauss 1984]. O resultado tornou-se desde então uma ferramenta maior na análise funcional assim que na informática, onde ele é usado para projetar os algoritmos aleatorizados, incluindo os da redução de dimensionalidade. A pesquisa moderna é amplamente dedicada aos meios de escolher o operador aleatório  $T$  de uma maneira computacionalmente eficaz.

De fato,  $T$  não precisa ser uma projeção (normaizada) aleatória, como na prova acima. Por exemplo, uma matriz aleatória do tamanho  $n \times k$  com coeficientes gaussianos bastaria também. Ainda mais, os coeficientes podem ser zeros e uns, e além disso, a matriz pode ser esparsa (conter mais zeros do que uns). Para leituras futuras, eu recomendo [Matoušek 2008] e [Vempala 2004], bem como [Naor 2018].

O exemplo seguinte mostra que a única projeção aleatória seguida pelo classificador qualquer não vai dar certo. No espaço euclidiano  $\mathbb{R}^N$  de uma alta dimensão  $N \gg 1$  sejam  $\mu_0$  e  $\mu_1$  duas medidas invariantes pelas rotações, da massa total  $1/2$  cadauma, suportadas nas esferas concêntricas  $(1/2)\mathbb{S}^{N-1}$  e  $\mathbb{S}^{N-1}$ , respetivamente, em torno de zero. Criemos o problema de aprendizagem, cujo lei subjacente é a medida de probabilidade  $\mu = \mu_0 + \mu_1$  e a função de regressão é igual a  $\eta = \chi_{\mathbb{S}^{N-1}}$ .

Seja  $\pi_k$  uma projeção de  $\mathbb{R}^N$  sobre um sub-espaço de uma menor dimensão  $k \ll N$ . Segundo um resultado de Poincaré, as imagens diretas  $\pi_*\mu_i$ ,  $i = 0, 1$ , depois da renormalização do argumento por  $\sqrt{N-k}$  (o que não vai afeitar o desempenho do classificador), são aproximadamente gaussianas, centradas e com variância  $1/2$  e  $1$ , respetivamente. A regra composta  $\mathcal{L} \circ \pi_k$  vai possuir aproximadamente o mesmo erro de aprendizagem que a regra  $\mathcal{L}$  aprendendo o problema cuja lei tem a densidade

$$\frac{1}{2} \left[ \frac{1}{\sqrt{2\pi}} e^{-\|x\|^2/2} + \frac{1}{\sqrt{\pi}} e^{-\|x\|^2} \right]$$

e a função de regressão

$$\eta(x) = \frac{\frac{1}{\sqrt{2\pi}} e^{-\|x\|^2/2}}{\frac{1}{\sqrt{2\pi}} e^{-\|x\|^2/2} + \frac{1}{\sqrt{\pi}} e^{-\|x\|^2}},$$

a norma sendo a de  $\ell^2(k)$ . É claro que o erro de Bayes vai ser estritamente positivo, e por conseguinte o conceito  $C = \mathbb{S}^{N-1}$  não pode ser aprendido com qualquer regra composta  $\mathcal{L} \circ \pi_k$ .

Ao mesmo tempo, o teorema de Cramér–Wold 7.2.4, que vamos mostrar no próximo capítulo, diz que uma medida boreliana de probabilidade sobre  $\mathbb{R}^d$  é unicamente definida pelas suas imagens diretas sob todas as projeções unidimensionais. Por conseguinte, qualquer problema de aprendizagem no espaço  $\mathbb{R}^d$ , ou até mesmo no espaço de Hilbert  $\ell^2$ , é unicamente definido, e pode ser aprendido, pelas suas imagens sob as projeções unidimensionais. Pode ser que aprendizagem ensemble de um conjunto de regras  $k$ -NN combinadas com  $m$  projeções aleatórias unidimensionais é universalmente consistente, quando  $m$  é de tamanho razoável, por exemplo  $m = O(\log n)$ ?

A ideia de usar aprendizagem ensemble de classificadores  $k$ -NN combinados com projeções aleatórias unidimensionais foi sugerida em [Fraiman, Justel e Svarc 2010].

O algoritmo sugerido no artigo depende de três parâmetros:  $k$  (o número de vizinhos mais próximos),  $r > 1$ , e  $N$ . Dado uma amostra rotulada,  $\sigma$ , no espaço euclidiano  $\mathbb{R}^d$ , e um ponto  $x \in \mathbb{R}^d$ , sugere-se escolher  $\lfloor rk \rfloor$  vizinhos mais próximos de  $x$  em  $\sigma$ , depois aplicar a eles, assim que a  $x$ ,  $N$  projeções aleatórias uni-dimensionais (segundo a medida de Haar sobre a esfera),  $\pi_1, \pi_2, \dots, \pi_N$ , depois executar o algoritmo  $k$ -NN para todas as imagens, e escolher o rótulo de  $x$  pelo voto majoritário. O resultado principal do artigo (teorema 3) afirma que o algoritmo é universalmente consistente quando  $k/n \rightarrow \infty$ . Porém, o teorema não contém algumas hipóteses sobre os valores dos parâmetros  $r$  e  $N$ , assim que seu comportamento assintótico. A única condição mencionada é que  $k, n \rightarrow \infty$ ,  $k/n \rightarrow 0$ . Por isso, não parece possível verificar a validade do resultado. Além disso, o algoritmo não resolve uma das dificuldades principais em altas dimensões, que é a busca de vizinhos mais próximos, e assim, em nossa opinião, vai um pouco contra a lógica.

Para um panorâmico do estado-do-arte na área de redução métrica aleatorizada de dimensionalidade, veja [Naor 2018]. Combinar esta teoria avançada com a aprendizagem supervisionada pode ser uma direção promissora.

## 6.3 Redução boreliana

### 6.3.1

Geralmente, as aplicações  $f$  que realizam a redução de dimensionalidade em várias áreas da informática são contínuas, por exemplo Lipschitz contínuas, como no método de projeções aleatórias. No contexto de aprendizagem de máquina, esta é uma condição bastante restritiva. O problema pode ser intuitivamente descrito como segue.

Sejam  $\Omega$  e  $\Upsilon$  dois domínios, e seja  $f: \Omega \rightarrow \Upsilon$  uma função contínua, realizando a redução de dimensionalidade. Dado uma amostra rotulada  $\sigma$  em  $\Omega$  e um ponto  $x \in \Omega$ , apliquemos uma regra de aprendizagem  $\mathcal{L}$  ao domínio  $\Upsilon$  às imagens  $f(\sigma)$  da amostra, afim de determinar o rótulo do ponto  $f(x)$ , que será devolvido pela regra composta  $\mathcal{L} \circ f$  como rótulo de  $x$ . Agora suponha que a dimensão topológica do domínio  $\Omega$  é mais alta do que a de  $\Upsilon$  (a situação comum).

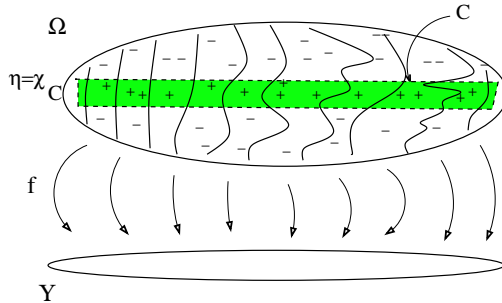


Figura 6.14: Fibração produzida por uma função contínua.

Pelas razões topológicas, as fibras  $f^{-1}(y)$  tipicamente têm a dimensão topológica estritamente positiva,  $\dim \Omega - \dim \Upsilon$ . Em particular, eles estão altamente não triviais. A regra  $\mathcal{L}$  não faz distinção entre os pontos  $x \in \Omega$  tendo a mesma imagem,  $f(x)$ , devolvendo o mesmo rótulo para todos. Deste modo, se, por exemplo, o conceito  $C \subseteq \Omega$  a ser aprendido passa a ser transversal à foliação definida por  $f$ , o resultado vai ser péssimo.

O erro da regra  $\mathcal{L} \circ f$  vai ser próximo ao erro de Bayes se e somente se a função de regressão toma valores aproximadamente constantes ao longo das fibras  $f^{-1}(y)$ . De modo equivalente, precisamos das garantias que as imagens diretas  $f_*(\mu_0)$  e  $f_*(\mu_1)$  das distribuições de pontos rotulados 0 e 1 respectivamente sejam tão bem separadas em  $\Upsilon$  que em  $\Omega$ . A este respeito, o exemplo na subseção 6.2.5 mostra que há restrições sobre a validade de resultados deste gênero.

### 6.3.2

No entanto, analisando de perto o modelo teórico da aprendizagem estatística, pode notar-se que a noção da consistência universal é na verdade insensível a estrutura métrica ou mesmo topológica no domínio, enquanto a estrutura *boreliana* permanece intacta. Isto permite, através de uma injeção boreliana, reduzir os dados para um caso de baixa dimensão, até mesmo unidimensional, após o qual o algoritmo de aprendizagem composto continua a ser universalmente consistente.

Relembramos que uma aplicação  $f: \Omega \rightarrow W$  entre dois espaços borelianos é dita *isomorfismo boreliano* se  $f$  é bijetiva, e  $f$  e  $f^{-1}$  são borelianas. Isso significa que  $f$  estabelece uma bijeção entre a estrutura boreliana  $\mathcal{B}_\Omega$  e  $\mathcal{B}_W$ .



Cada aplicação contínua é boreliana, e cada homeomorfismo (isso é, uma bijeção contínua, com o inverso contínuo) é um isomorfismo boreliano. Mas existem muito mais aplicações borelianas do que aplicações contínuas, e muito mais isomorfismos borelianos do que homeomorfismos.

**Exercício 6.3.1.** Mostre que não existe alguma injeção contínua do quadrado  $[0, 1]^2$  dentro do intervalo  $[0, 1]$ .

[ *Sugestão:* uma injeção contínua sobre um espaço compacto é um homeomorfismo... ]

Ao mesmo tempo, existe uma injeção boreliana do quadrado no intervalo. Ela pode ser obtido usando o “entrelaçamento” dos dígitos nas expansões binárias de  $x$  e de  $y$  num par  $(x, y) \in [0, 1]^2$  (sujeito as precauções habituais sobre as seqüências infinitas de uns):

$$[0, 1]^2 \ni (0.a_1a_2 \dots, 0.b_1b_2 \dots) \mapsto (0.a_1b_1a_2b_2 \dots) \in [0, 1]. \quad (6.18)$$

Para uma representação geométrica desta injeção, veja a figura 6.15.

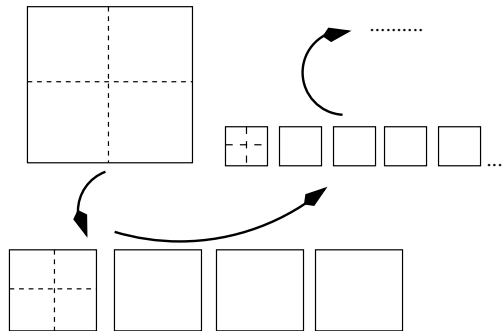


Figura 6.15: Construindo uma injeção boreliana do quadrado para o intervalo.

**Exercício 6.3.2.** Mostrar que a aplicação acima é injetora e boreliana.

[ *Sugestão:* basta mostrar que as imagens recíprocas dos intervalos abertos formando uma base da topologia do intervalo são conjuntos borelianos. ]

A aplicação  $f$  acima não é sobrejetora, por exemplo o ponto  $0.10101010\dots$  não é na imagem de  $f$ . Mas ela pode ser modificada a fim de obter um isomorfismo boreliano entre  $[0, 1]^2$  e  $[0, 1]$ . No lugar da base 2, pode ser uma base qualquer. Ademais, esta construção pode ser generalizada para mostrar que não há muita diversidade entre os espaços borelianos padrão. Eis um resultado clássico (teorema D.0.2).

**Teorema 6.3.3.** *Dois espaços borelianos padrão são isomorfos se e somente se eles tem a mesma cardinalidade.*  $\square$

**Corolário 6.3.4.** *Sejam  $\Omega$  e  $W$  dois espaços métricos separáveis e completos, de cardinalidade  $c = 2^{\aleph_0}$  cada um. (Por exemplo, isso é o caso se eles não contêm os pontos isolados). Então os espaços borelianos correspondentes são isomorfos.  $\square$*

Este será o caso da maioria dos domínios de interesse na teoria. Por exemplo, o conjunto de Cantor, o intervalo unitário, o espaço euclidiano  $\mathbb{R}^d$ , o espaço de Hilbert separável de dimensão infinita  $\ell^2$ , e na verdade todos espaços de Fréchet (espaços lineares topológicos localmente convexos, metrizáveis e completos) separáveis não triviais são todos isomorfos entre eles como espaços borelianos. A estrutura de Borel de todos estes espaços é a mesma do *espaço de Borel padrão* com cardinalidade de contínuo.

### 6.3.3

Agora, sejam  $\Omega$  e  $\mathcal{Y}$  dois espaços borelianos padrão, e seja  $f: \Omega \rightarrow W$  uma injeção boreliana. Esta  $f$  pode ser canonicamente estendida a uma injeção boreliana de  $\Omega \times \{0, 1\}$  em  $\mathcal{Y} \times \{0, 1\}$ :

$$f(x, \epsilon) = (f(x), \epsilon),$$

onde  $\epsilon \in \{0, 1\}$ . Usemos a mesma letra  $f$  pela prolongação.

Suponha agora que  $\mathcal{L}$  seja um classificador qualquer no domínio  $\mathcal{Y}$ . Definiremos um novo classificador,  $\mathcal{L}^f$ , no domínio  $\Omega$ , como a composição de  $\mathcal{L}$  com a injeção boreliana  $f$ :

$$\mathcal{L}_n^f(\sigma)(x) = \mathcal{L}_n(f(\sigma))(f(x)).$$

(Como na Figura 6.1).

Seja  $\mu$  uma medida de probabilidade qualquer sobre  $\Omega \times \{0, 1\}$ . Definamos a imagem direta  $f_*\mu$  da medida  $\mu$  ao longo de  $f$ : qualquer seja um conjunto boreliano  $B \subseteq \mathcal{Y} \times \{0, 1\}$ , posemos

$$(f_*\mu)(B) = \mu(f^{-1}(B)).$$

É uma medida de probabilidade boreliana sobre  $\mathcal{Y} \times \{0, 1\}$ .

**Exercício 6.3.5.** Mostre que se

$$X_1, X_2, \dots, X_n, \dots$$

é uma sequência de variáveis aleatórias i.i.d. com valores em  $\Omega \times \{0, 1\}$  segundo a lei  $\mu$ , então

$$f(X_1), f(X_2), \dots, f(X_n), \dots$$

é uma sequência das variáveis aleatórias i.i.d. com valores em  $\mathcal{Y} \times \{0, 1\}$  seguindo a lei  $f_*(\mu)$ .

Definemos  $\iota$  a função de regressão da medida  $f_*(\mu)$  sobre  $\mathcal{Y} \times \{0, 1\}$ .

**Exercício 6.3.6.** Verifique que

$$\eta = \iota \circ f.$$

Por conseguinte, o classificador de Bayes (“o melhor classificador possível”),  $T_{bayes}^\Omega$ , para  $\Omega$ , e o classificador de Bayes,  $T_{bayes}^\Upsilon$ , para  $\Upsilon$ , satisfazem:

$$\forall x \in \Omega, \quad T_{bayes}^\Omega(x) = T_{bayes}^\Upsilon(f(x)).$$

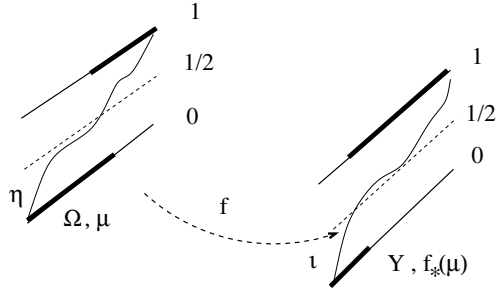


Figura 6.16: Gráficos de classificadores de Bayes em dois domínios.

**Exercício 6.3.7.** Mostre que, para  $\mu^{\otimes n}$ -quase todo  $\sigma$ ,

$$\text{erro}_{\mu, \eta} \mathcal{L}_n^f(\sigma) = \text{erro}_{f_*(\mu), \theta} \mathcal{L}_n(f(\sigma)).$$

Segue-se imediatamente que qualquer injeção boreliana fornece uma redução de dimensionalidade que conserva a consistência universal de regras de aprendizagem. O resultado seguinte oferece uma nova perspectiva da redução de dimensionalidade em teoria da aprendizagem automática estatística.

**Teorema 6.3.8.** *Sejam  $\Omega$  e  $\Upsilon$  dois domínios (espaços borelianos padrão), e seja  $f : \Omega \rightarrow \Upsilon$  uma injeção boreliana. Seja  $\mathcal{L}$  é um classificador universalmente consistente em  $\Upsilon$ . Então o classificador  $\mathcal{L}^f$ , obtido pela redução de dimensionalidade  $f$  de  $\Omega$  para  $\Upsilon$ , seguida da aplicação do classificador  $\mathcal{L}$ , é universalmente consistente em  $\Omega$  também. Se  $\mathcal{L}$  é universalmente fortemente consistente em  $\Upsilon$  (a saber, o erro de aprendizagem converge para o erro de Bayes quase certamente), então  $\mathcal{L}^f$  é universalmente fortemente consistente em  $\Omega$ .  $\square$*

Em particular, pelo menos teoricamente, sempre existe a redução com uma injeção boreliana do problema de aprendizagem em qualquer domínio para o no intervalo,  $[0, 1]$ , ou até o no conjunto de Cantor, com a dimensão topológica  $d = 0$ .

*Observação 6.3.9.* Injeções borelianas para redução de dimensionalidade foram sugeridas em [Pestov 2013a], e aplicadas com sucesso na competição CDMC’2013 pela equipe consistente do autor destas notas e de três alunos dele: Gaël Giordano, Hubert Duan, e

Stan Hatko. O erro de classificação pelo problema de detecção de intrusos numa rede (uma amostra rotulada em  $\mathbb{R}^7$ ) foi reduzido de 0.3 até 0.1 por cento. Veja [Duan et al. s.d.] para uma descrição de algoritmos mais detalhada, assim como [Hatko 2013].

As nossas experiências até agora mostram que os melhores resultados são obtidos quando a dimensão é reduzida por um fator constante (por exemplo, entre 4 e 7), que depende do conjunto de dados.

**Exercício 6.3.10.** Escrever o código em R para redução de dimensionalidade usando as injeções borelianas, e combiná-lo com o classificador  $k$ -NN para melhorar o erro de classificação no problema do reconhecimento de voz (o conjunto de dados *Phoneme*). Tentar as bases diferentes de expansão dos números.

*Observação 6.3.11.* A teoria está no seu início. O que é necessário do ponto de vista teórico, é desenvolver alguma noção de capacidade, talvez no espírito de dimensão de Vapnik–Chervonenkis ou médias de Rademacher, para uma família  $\mathcal{F}$  de injeções de Borel  $f$  entre dois domínios,  $\Omega$  e  $W$ . Quando esta noção for finita, isto garantiria que o classificador  $\mathcal{L}^f$  seja universalmente consistente, quando  $f$  é selecionado dentro de  $\mathcal{F}$  dependendo da amostra  $\sigma$ , a fim de otimizar o desempenho empírico de  $\mathcal{L}^f$ . Em outras palavras,  $f$  é um elemento aleatório de  $\mathcal{F}$ .

A perspectiva mais promissora será de combinar a redução boreliana com aprendizagem ensemble.

# 7

## *Aproximação universal*

---

O perceptron produz uma coleção de conceitos realmente simples, eles são semi-espços, e suas habilidades de classificação são claramente muito limitadas. O que ocorre se permitirmos redes de arquitetura mais complexa? Quão complicada é possível que seja uma classe de funções gerada por uma rede neural? Podemos esperar gerar todos os conceitos? A resposta é positiva: que se juntarmos apenas alguns unidades de computação, podemos aproximar cada conceito (ou até cada função) que queremos.

O primeiro resultado deste capítulo é o teorema clássico de Kolmogorov obtido em resposta a um dos problemas na famosa lista de David Hilbert, logo antes da emergência da aprendizagem automática. O resultado pode ser interpretado assim: para cada  $d$  existe uma rede fixa de unidades de computação que, para vários valores de parâmetros, gera todas as funções contínuas de  $d$  variáveis.

No entanto, o significado deste resultado é sobretudo metafísico. O resultado “pé no chão” nesta direção é o Teorema de Aproximação Universal de Cybenko, afirmando, em particular, que já uma rede de perceptrons sem realimentação que tem apenas uma camada interior pode aproximar qualquer conceito boreliano se o número de unidades é bastante grande (aqui, ao contrário ao teorema de Kolmogorov, o tamanho da rede depende da função e de grau de aproximação desejado).

Finalmente, discutimos o princípio de minimização de risco estrutural que combina algumas vantagens da teoria de Vapnik–Chervonenkis com as de consistência universal.

## 7.1 Problema 13 de Hilbert e teorema da superposição de Kolmogorov

### 7.1.1

Em sua palestra plenária no 1900 Congresso Internacional de Matemáticos (ICM), realizado em Paris, David Hilbert formulou uma lista de 23 problemas abertos que tiveram, ao todo, um profundo impacto sobre os desenvolvimentos matemáticos no século XX. (Um livro altamente recomendado é [Yandell 2002]). O décimo terceiro da lista foi o problema seguinte.

Nomography deals with the problem: to solve equations by means of drawings of families of curves depending on an arbitrary parameter. It is seen at once that every root of an equation whose coefficients depend upon only two parameters, that is, every function of two independent variables, can be represented in manifold ways according to the principle lying at the foundation of nomography. Further, a large class of functions of three or more variables can evidently be represented by this principle alone without the use of variable elements, namely all those which can be generated by forming first a function of two arguments, then equating each of these arguments to a function of two arguments, next replacing each of those arguments in their turn by a function of two arguments, and so on, regarding as admissible any finite number of insertions of functions of two arguments. So, for example, every rational function of any number of arguments belongs to this class of functions constructed by nomographic tables; for it can be generated by the processes of addition, subtraction, multiplication and division and each of these processes produces a function of only two arguments. One sees easily that the roots of all equations which are solvable by radicals in the natural realm of rationality belong to this class of functions; for here the extraction of roots is adjoined to the four arithmetical operations and this, indeed, presents a function of one argument only. Likewise the general equations of the 5-th and 6-th degrees are solvable by suitable nomographic tables; for, by means of Tschirnhausen transformations, which require only extraction of roots, they can be reduced to a form where the coefficients depend upon two parameters only.

Now it is probable that the root of the equation of the seventh degree is a function of its coefficients which does not belong to this class of functions capable of nomographic construction, i. e., that it cannot be constructed by a finite number of insertions of functions of two arguments. In order to prove this, the proof would be necessary that the equation of the seventh degree  $f^7 + xf^3 + yf^2 + zf + 1 = 0$  is not solvable with the help of any continuous functions of only two arguments. I may be allowed to add that I have satisfied myself by a rigorous process that there exist analytical functions of three arguments  $x, y, z$  which cannot be obtained by a finite chain of functions of only two arguments.

By employing auxiliary movable elements, nomography succeeds in constructing functions of more than two arguments, as d'Ocagne has recently proved in the case of the

equation of the 7-th degree.

A essência do problema 13 era então comumente interpretada como a conjectura de que nem todas as funções contínuas em três variáveis podem ser expressas por meio de composições finitas de funções contínuas em duas variáveis.

Em 1957, Vladimir Arnold, então um aluno de graduação de 3o ano e depois um dos mais influentes matemáticos russos, mostrou que, na verdade, a conjectura de Hilbert era falsa: cada função contínua de três variáveis pode ser expressa usando um número finito de substituições de funções contínuas de duas variáveis.

Desenvolvendo a prova de Arnold ainda mais, seu orientador de pesquisa Andreï Kolmogorov estabeleceu [Kolmogorov 1963] o resultado seguinte, que se tornou clássico.

**Teorema 7.1.1** (Teorema da Superposição de Kolmogorov). *Para todo  $n \geq 2$  existem funções contínuas  $\psi^{pq}$ ,  $p = 1, 2, \dots, n$ ,  $q = 1, 2, \dots, 2n + 1$ , definidas sobre  $[0, 1]$ , tais que cada função contínua  $f : [0, 1]^n \rightarrow \mathbb{R}$  pode ser representada assim:*

$$f(x_1, x_2, \dots, x_n) = \sum_{q=1}^{2n+1} g_q \left[ \sum_{p=1}^n \psi^{pq}(x_p) \right], \quad (7.1)$$

onde  $g_q$ ,  $q = 1, 2, \dots, 2n + 1$  são funções reais contínuas, que dependem de  $f$ .

Desde então, o resultado tem atraído uma atenção considerável e foi melhorado muitas vezes. Em particular, aqui está uma forma dada por G. Lorentz [Lorentz 1976].

**Teorema 7.1.2.** *Seja  $f : [0, 1]^d \rightarrow \mathbb{R}$  uma função contínua, e  $\epsilon > 0$  um número racional. Então*

$$f = \sum_{i=1}^{2d+1} g(z_k), \quad (7.2)$$

onde  $g : \mathbb{R} \rightarrow \mathbb{R}$  é uma função contínua apropriada (dependendo de  $f$  e de  $\epsilon$ ), e para todo  $k$ ,

$$z_k = \sum_{j=1}^d \lambda^k \psi(x_j + \epsilon k) + k. \quad (7.3)$$

Aqui,  $\lambda \in \mathbb{R}$ ,  $\psi$  é uma função real Lipschitz contínua crescente, e  $\lambda$ ,  $\psi$  não dependem de  $f$  e  $\epsilon$ .  $\square$

O teorema acima pode ser interpretado para dizer que uma rede neural artificial relativamente simples (a “rede neural de Kolmogorov–Lorentz”) pode gerar uma função contínua qualquer em  $d$  variáveis:

O único “parâmetro” da rede a ser treinado é a função  $g$  de uma variável. Em seu tempo a ideia acima atraiu o interesse de tais pesquisadores na comunidade da aprendizagem da máquina como Robert Hecht-Nielsen [Hecht-Nielsen 1987]. Houve também publicações argumentando que a rede de Kolmogorov–Lorentz não pode possivelmente ter algum valor

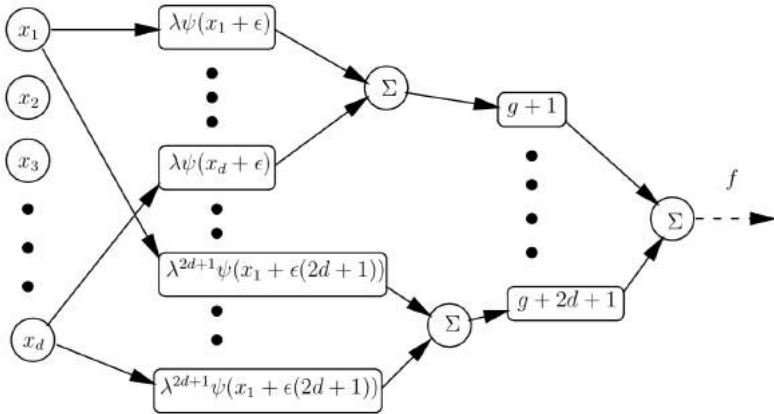


Figura 7.1: A “rede neural de Kolmogorov–Lorentz”.

prático [Girosi e Poggio 1989], e pelo contrário, alguns resultados mais recentes [Braun e Griebel 2009; Igel'nik 2003; Kurková 1991] demonstram que as funções  $\psi$ ,  $\lambda$  e  $g$  podem ser recuperadas de forma algorítmica eficiente.

Apesar de tudo isso, a observação acima tem principalmente um significado filosófico: é tranquilizador estar ciente do fato que as redes neurais artificiais, em teoria pelo menos, são onipotentes. O teorema de Kolmogorov é assim mencionado em muitas fontes que tratam de redes neurais.

### 7.1.2

Na sua revista [Lorentz 1976] do problema 13 de Hilbert, G.G. Lorentz oferece a perspectiva seguinte do teorema de Kolmogorov.

Let us take a good Calculus text and examine what genuine functions of two or three variables can we find. The function  $x + y$  will be found, but the product  $xy$  is already nothing new, it reduces to the sum and functions of one variable,  $xy = e^{\log x + \log y}$ , similarly for  $x + y + z = (x + y) + z$ . So perhaps there do not exist any other functions?

The astonishing result of Kolmogorov (1957) confirms this.

Nesta seção vamos apresentar a prova do Teorema de Superposição de Kolmogorov devida a Jean-Pierre Kahane [Kahane 1975], que é provavelmente a mais curta prova conhecida. Embora possa ser a menos construtiva, porém todas as ideias originais são conservadas e podem ser vistas claramente, e as tecnicidades são reduzidas ao mínimo dos mínimos.



### 7.1.3 Estendendo as funções Lipschitz contínuas

**Lemma 7.1.3.** *Seja  $f$  uma função real Lipschitz contínua de constante  $L \geq 0$ , definida sobre um sub-espaço  $A$  de um espaço métrico  $(X, d)$ . Então  $f$  admite uma extensão,  $\tilde{f}$ , sobre todo  $X$ , que é Lipschitz contínua da mesma constante  $L$ .*

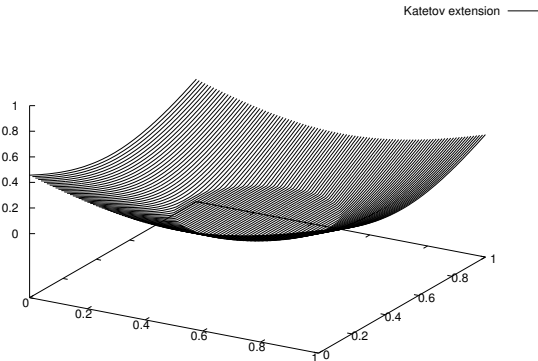


Figura 7.2: Extensão  $\tilde{f}$  de uma função identicamente zero sobre o disco de raio  $1/4$  em torno do meio do quadrado unitário.

*Demonstração.* Sem perda de generalidade e substituindo  $f$  por  $f/L$  se for necessário, podemos supor que  $f$  é 1-Lipschitz contínua. Além disso, suponhamos que  $A$  não é vazio. Para todo  $x \in X$ , definamos

$$\tilde{f}(x) = \inf \{ f(a) + d(a, x) : a \in A \}. \quad (7.4)$$

O valor  $\tilde{f}(x)$  é bem-definido: escolhendo um  $a_0 \in A$  qualquer, a desigualdade triangular e a condição  $L = 1$  implicam que

$$\forall a \in A, \quad f(a) + d(a, x) \geq f(a_0) - d(x, a_0).$$

A segunda observação é que se  $x \in A$ , então para todo  $a \in A$ , pela mesma razão que acima,

$$f(a) + d(a, x) \geq f(x),$$

ou seja, o ínfimo na Eq. (7.4) é atingido em  $a = x$ , é por isso a função  $\tilde{f}$  é uma extensão de  $f$ .

Basta mostrar que  $\tilde{f}$  é 1-Lipschitz contínua. Sejam  $x, z \in \Omega$  e  $\epsilon > 0$  quaisquer. Escolha  $y_1, y_2 \in Y$  de modo que o valor de  $f(x)$ , respetivamente  $f(z)$ , seja a distância  $< \epsilon$  do valor  $f(y_1) + d(x, y_1)$ , respetivamente  $f(y_2) + d(z, y_2)$ . Então  $|f(x) - f(z)|$  é a menor de  $2\epsilon$  de  $|f(y_1) + d(x, y_1) - f(y_2) - d(z, y_2)|$ , e além disso,

$$f(y_1) + d(x, y_1) \leq f(y_2) + d(x, y_2) + \epsilon,$$

embora, como é óbvio,

$$d(x, y_2) \leq d(x, z) + d(z, y_2).$$

Por conseguinte,

$$f(y_1) + d(x, y_1) \leq f(y_2) + d(x, z) + d(z, y_2) + \epsilon,$$

ou seja

$$f(y_1) + d(x, y_1) - f(y_2) - d(z, y_2) \leq d(x, z) + \epsilon.$$

Isso implica

$$f(x) - f(z) \leq d(x, z) + 3\epsilon$$

e como  $\epsilon > 0$  foi qualquer, enviando  $\epsilon \downarrow 0$ ,

$$f(x) - f(z) \leq d(x, z).$$

Um argumento simétrico mostra que

$$f(z) - f(x) \leq d(x, z).$$

□

*Observação 7.1.4.* A função  $\tilde{f}$  se chama *extensão de Katétov*. É claro que a extensão  $\tilde{f}$  é, em geral, longe de ser única. A função estendida,  $\tilde{f}$ , é a *maior* de todas as extensões Lipschitz contínuas de  $f$  tendo a constante Lipschitz determinada. (Exercício.) Considere também Fig. 7.2, onde essa extensão é grafada para a função  $f$  tomando identicamente o valor zero no círculo  $(x - 0.5)^2 + (y - 0.5)^2 = 1/16$ . Os valores da função  $\tilde{f}$  estão subindo na taxa mais rápida permitida pela constante de Lipschitz 1.

Pode-se, por exemplo, considerar em vez disso a *menor* extensão possível, dada por

$$\tilde{f}(x) = \sup \{f(a) - d(a, x) : a \in A\}.$$

## 7.1.4 A prova de Kahane do teorema da superposição de Kolmogorov

### Formulação do teorema dada por Kahane

Denotemos  $\Phi$  o conjunto de todas as funções contínuas não decrescentes do intervalo fechado  $\mathbb{I} = [0, 1]$  nele mesmo, visto como um sub-conjunto de  $C[0, 1]$ .

**Exercício 7.1.5.** Mostrar que  $\Phi$  é fechado em  $C[0, 1]$ , então é um espaço métrico completo relativo à métrica uniforme.

**Exercício 7.1.6.** Mostrar que uma função genérica  $\varphi \in \Phi$  (veja subseção C.4.4) é estritamente crescente.

[ *Sugestão:* basta verificar que se  $x, y \in \mathbb{Q} \cap [0, 1]$  e  $x < y$ , então a propriedade  $\phi(x) < \phi(y)$  é genérica. ]

Para todo inteiro  $k$ , a potência  $k$ -ésima  $\Phi^k$  é um espaço métrico completo quando munido da distância

$$d((\varphi_1, \dots, \varphi_n), (\psi_1, \psi_2, \dots, \psi_n)) = \max_{i=1}^n \|\varphi_i - \psi_i\|,$$

e assim pode-se falar de  $k$ -tuplos genéricos de elementos de  $\Phi$ .

**Teorema 7.1.7** (Teorema da superposição de Kolmogorov, versão de Kahane). *Sejam  $\lambda_1, \lambda_2, \dots, \lambda_n$  reais estritamente positivos, dois a dois distintos, de soma um. Então, para uma  $(2n + 1)$ -tupla genérica  $(\varphi_1, \varphi_2, \dots, \varphi_{2n+1}) \in \Psi^{2n+1}$ , toda função contínua real  $f_0$  sobre o cubo unitário  $\mathbb{I}^n$  pode ser representada como*

$$f_0(x_1, \dots, x_n) = \sum_{q=1}^{2n+1} g \left( \sum_{p=1}^n \lambda_p \varphi_q(x_p) \right), \quad (7.5)$$

onde  $g$  é uma função contínua sobre o intervalo  $\mathbb{I}$  (que depende de  $f$ ).

Seja  $\epsilon > 0$  um número bastante pequeno, a ser especificado mais tarde. Para cada  $f \in C[0, 1]^n$  não identicamente igual a zero, definamos o conjunto  $\Omega(f)$  de todas as  $(2n + 1)$ -tuplas  $(\varphi_1, \varphi_2, \dots, \varphi_{2n+1})$  de funções de  $\Phi$  tais que existe um  $h \in C[0, 1]$  tendo as propriedades:

$$(i) \|h\| \leq \|f\|, \\ (ii) \left\| f(x_1, x_2, \dots, x_n) - \sum_{q=1}^{2n+1} h \left( \sum_{p=1}^n \lambda_p \varphi_q(x_p) \right) \right\| < (1 - \epsilon) \|f\|. \quad (7.6)$$

(As normas são normas uniformes em  $C[0, 1]$  e em  $C(\mathbb{I}^n)$ , respectivamente).

É claro que  $\Omega(f)$  é aberto em  $\Phi^{2n+1}$ . De fato, a norma da expressão na parte esquerda em (ii) é estritamente menor que  $(1 - \epsilon) \|f\|$ ; denote a diferença entre dois valores da

norma por  $\gamma$ . Se o valor de  $h$  em todas  $2n + 1$  expressões dentro dos parênteses muda por menos de  $\gamma/(2n + 1)$ , a norma da diferença muda por  $< \gamma$ , e a desigualdade vai ser válida. Como  $h$  é contínua sobre o intervalo fechado unitário, ela é uniformemente contínua. Pode-se escolher um  $\gamma_1 > 0$  com a propriedade que se dois valores do argumento de  $h$  diferem por menos de  $\gamma_1$ , então os valores correspondentes de  $h$  diferem por  $< \gamma/(2n + 1)$ . Concentremo-nos sobre a soma de  $n$  termos dentro do argumento de  $h$ . Se todo termo muda por  $< \gamma_1/n$ , então o argumento de  $h$  muda por  $< \gamma_1/n$ . Todo  $\lambda_p$  é limitado por um, logo basta verificar que os valores de cada  $\varphi_q$  mudam por  $< \gamma_1/n$ . Mas isso é o caso se for permitido que a  $(2n + 1)$ -tupla  $(\varphi_q)$  varie dentro da bola aberta de raio  $\gamma_1/n$  em torno do valor original.

Pretendamos mostrar que o conjunto  $\Omega(f)$  é denso em  $\Phi^{2n+1}$ . Suponha, por enquanto, que isso foi estabelecido. A prova do teorema segue assim.

Como o espaço  $C[0, 1]^n$  é separável (proposição H.2.32), ele contém um subconjunto enumerável denso,  $F$ . Pode-se ainda supor que  $0 \notin F$ . De acordo com o teorema da categoria de Baire C.4.24, o conjunto  $\Omega = \bigcap_{f \in F} \Omega(f)$  é um conjunto  $G_\delta$  denso em  $\Phi^{2n+1}$ . Logo, um elemento genérico  $(\varphi_1, \varphi_2, \dots, \varphi_{2n+1})$  de  $\Phi^{2n+1}$  pertence a  $\Omega$ .

**Exercício 7.1.8.** Mostrar que sob nossas hipóteses, dado  $f_0 \in C(\mathbb{I}^n)$ , existe  $f \in F$  com as propriedades  $\|f\| \leq \|f_0\|$  e  $\|f - f_0\| < (\epsilon/2)\|f_0\|$ .

Escolha uma função  $f \in F$  como acima. Seja  $(\varphi_1, \varphi_2, \dots, \varphi_{2n+1})$  uma tupla qualquer de elementos de  $\Omega$ . Agora escolhamos uma função  $h$  verificando as condições (7.6). Nós iremos expressar este fato simplesmente escrevendo  $h = \gamma(f_0)$ . Defina também  $\gamma(0) = 0$ .

Agora definamos recursivamente para  $j = 0, 1, \dots$ , as funções  $h_j = \gamma(f_j)$ , onde

$$f_{j+1}(x_1, x_2, \dots, x_n) = f_j(x_1, x_2, \dots, x_n) - \sum_{q=1}^{2n+1} h_j \left( \sum_{p=1}^n \lambda_p \varphi_q(x_p) \right).$$

**Exercício 7.1.9.** Verifique que a série de funções  $\sum_{j=0}^{\infty} h_j$  converge (até mesmo absolutamente) no espaço normado  $C[0, 1]$ .

**Exercício 7.1.10.** Verifique que a soma da série acima,  $h = \sum_{j=0}^{\infty} h_j$  (que é também uma função contínua), satisfaz a conclusão do teorema de Kolmogorov (7.5).

[ *Sugestão:* use as somas telescópicas. ]

Agora concentremos nossos esforços para estabelecer que  $\Omega(f)$  é denso em  $\Phi^{2n+1}$ .

Seja  $G$  um subconjunto aberto não vazio qualquer de  $\Phi^{2n+1}$ , e seja  $\delta = \delta(G, F, \epsilon)$  um valor positivo bastante pequeno, a ser especificado quase no final da prova.

Para todo  $q = 1, 2, \dots, 2n + 1$  considere a sequência de intervalos fechados dois a dois disjuntos  $\mathbb{I}_q(j)$ ,  $j \in \mathbb{Z}$ , de comprimento  $2n\delta$  cada um, separados entre si por sucessivas lacunas de comprimento  $\delta$ . Eis a fórmula:

$$\mathbb{I}_q = \mathbb{I}_q(j) = [q\delta + (2n + 1)j\delta, q\delta + (2n + 1)j\delta + 2n\delta].$$

Observe que, como o valor de  $q$  aumenta por um, todos os intervalos  $\mathbb{I}_q$  mover para a direita por  $\delta$  unidades, de modo que depois de  $2n + 1$  passos o arranjo de intervalos  $\mathbb{I}_q$  novamente parece como no início.

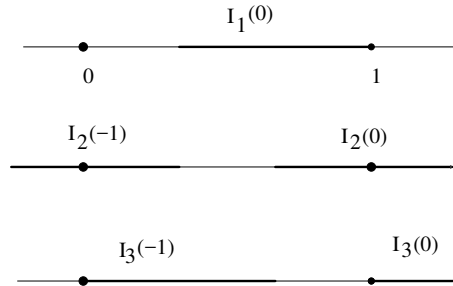


Figura 7.3: Intervalos  $\mathbb{I}_q(j)$  no caso mais simples onde  $\delta = 1/3$  e  $n = 1$ , de modo que  $2n + 1 = 3$ .

Por conseguinte, todo ponto  $x \in [0, 1]$  pertence à união de todos os intervalos  $\mathbb{I}_q$  para todos os valores de  $q$  exceto no máximo um.

Denote por  $P_q$  o cubo da forma

$$P_q = P_q(j_1, j_2, \dots, j_n) = \mathbb{I}_q(j_1) \times \mathbb{I}_q(j_2) \times \dots \times \mathbb{I}_q(j_n).$$

Se  $x \in \mathbb{I}^n$ , então toda coordenada  $x_i$  pertence a um dos intervalos  $\mathbb{I}_q$  para todos  $q$  exceto no máximo um valor. Por conseguinte,  $x$  pertence à união de todos os cubos  $P_q$  para todos os valores  $q = 1, 2, \dots, 2n + 1$  exceto no máximo  $n$  valores (o número de coordenadas do cubo). Então,  $x$  pertence à união de cubos  $P_q$  para pelo menos  $n + 1$  valores diferentes de  $q$ .

*Observação 7.1.11.* Este é um ponto importante que cada elemento do cubo  $\mathbb{I}^n$  pertence aos cubos pequenos “mais frequentemente do que não”, e este ponto sutil vai cumprir um papel crucial na estimativa final da prova. Isso explica o número de funções,  $2n + 1$ , na afirmação do teorema. Foi mostrado (veja por exemplo [Sternfeld 1985]), que o número  $2n + 1$  das funções  $\varphi_q$  é de fato o mínimo possível e não pode ser melhorado.

Agora denote por  $\Delta$  a coleção de todas as  $(2n + 1)$ -tuplas de funções em  $\Phi$  tais que  $\varphi_q$  é constante sobre os intervalos  $\mathbb{I}_q$  e afim entre eles. Escolha  $\delta$  de modo que

1. a oscilação de  $f$  sobre todo cubo  $P_q$  é limitada por  $\epsilon \|f\|$  (isso é certamente possível, pois  $f$  é uniformemente contínua sobre o cubo  $\mathbb{I}^n$ ), e
2.  $G \cap \Delta = \emptyset$ . Observe que, como o tamanho dos intervalos de  $\mathbb{I}_q$  se aproxima de zero, as funções constantes sobre estes intervalos e afins entre eles se tornarem cada vez mais flexíveis e podem aproximar as funções contínuas dadas cada vez melhor. Se nós escolhermos qualquer  $(2n + 1)$ -tupla de funções  $\varphi_1, \dots, \varphi_{2n+1}$  de  $G$ , e um  $\gamma > 0$  de tal modo que o  $\gamma$ -bola em torno deste  $(2n + 1)$ -tupla está contida em  $G$ , então, escolhendo o tamanho dos intervalos de  $\mathbb{I}_q$  bastante pequeno, podemos garantir que existem  $(2n + 1)$ -tuplas de funções de  $\Delta$  que estão  $\gamma$ -próximas de  $\varphi_1, \dots, \varphi_{2n+1}$ .

**Exercício 7.1.12.** Mostre que se pode escolher de modo recursivo uma sequência de números suficientemente pequenos  $\mu_{q,j}$  de modo que, adicionando  $\mu_i$  ao valor de todo  $\varphi_q$  sobre o  $j$ -ésimo cubo, obtemos que as funções

$$\chi_q(x_1, x_2, \dots, x_n) = \sum_{p=1}^n \lambda_p \phi_1(x_p), \quad q = 1, 2, 3, \dots, 2n + 1$$

assumem valores dois a dois diferentes sobre todos os cubos diferentes,  $P_q(j_1, \dots, j_n)$  e  $P_{q'}(j'_1, j'_2, \dots, j'_n)$ . Em outras palavras, a aplicação

$$(q, j_1, j_2, \dots, j_n) \mapsto \chi_q(P_q(j_1, \dots, j_n))$$

é injetora.

[ *Sugestão:* escolher todos os  $\mu_{q,j}$  linearmente independentes sobre o corpo gerado por todos os  $\lambda_i$  e, em seguida, usar o fato de que  $\lambda_i$  são todos dois a dois distintos. ]

### 7.1.5

Denote  $M(P_q)$  o valor médio de  $f$  sobre o cubo  $P_q = P_q(j_1, \dots, j_n)$ , ou seja,

$$M(P_q) = \int_{P_q} f(x) dx.$$

Para todos os cubos, defina

$$h(\chi_q(P_q)) = 2\epsilon M(P_q).$$

Lembre-se de que o valor da função  $\chi_q$  é constante sobre cada cubo  $P_q$ , e não há dois valores iguais entre si. Claramente, o valor máximo de  $h$  nos cubos é limitado por  $2\epsilon \|f\|$ .

Estenda esse  $h$  sobre  $\mathbb{R}$  de modo que a norma de  $h$  é limitada pela mesma quantidade  $2\epsilon \|f\|$ :

$$\|h\| \leq 2\epsilon \|f\|. \quad (7.7)$$

Pode-se, por exemplo, usar o lema 7.1.3 e cortar os grandes valores da função resultante usando  $\max\{-, 2\epsilon\|f\|\}$  e  $\min\{-, 2\epsilon\|f\|\}$ .

Para todo valor  $x \in P_q$ , pode-se escrever, segundo a definição de  $h$ ,

$$h(\chi_q(P_q)) = 2\epsilon f(x) + \rho, \quad (7.8)$$

onde  $|\rho| \leq 2\epsilon^2\|f\|$ .

Como todo  $x \in \mathbb{I}^n$  pertence, ao mínimo, aos  $n+1$  cubos que correspondem aos valores distintos de  $q$ , podemos, quando

$$\epsilon < \frac{n+1}{2},$$

usar a estimativa fina (7.8) para esses  $n+1$  valores de  $q$ , bem como a estimativa grosseira (7.7) para os  $\leq n$  cubos restantes, a fim de obter o seguinte,

$$\begin{aligned} \left| f(x) - \sum_{q=1}^{2n+1} h(\chi_q(x)) \right| &\leq (1 - 2(n+1)\epsilon)|f(x)| + 2(n+1)\epsilon^2\|f\| + 2n\epsilon\|f\| \\ &\leq (1 - 2\epsilon + 2(n+1)\epsilon^2)\|f\| \\ &\leq (1 - \epsilon)\|f\|, \end{aligned}$$

como desejado. Nós mostramos que  $\Omega(f)$  tem uma interseção não vazia com  $G$ , terminando a prova.  $\square$

*Observação 7.1.13.* Observe novamente que a estimativa na última cadeia de desigualdades está vãida pela mais magra das margens: ela depende do fato que  $n+1 > n!$

## 7.2 Teorema da aproximação universal de Cybenko

### 7.2.1

A rede de Kolmogorov–Lorentz ainda está distante demais daquelas que ocorrem na prática. O que pode ser dito sobre a capacidade de aproximação das redes mais realistas, por exemplo, de uma rede binária sem realimentação feita de perceptrons, de tipo estudado na subseção 2.3.4? Teorema 2.3.20 afirma que uma tal rede de arquitetura fixa tem dimensão VC finita, logo ela apenas pode aproximar uma classe própria de conceitos. E se permitirmos que o número de unidades cresça? Acontece que neste caso, até mesmo as redes da arquitetura a mais simples podem aproximar cada conceito arbitrariamente bem.

**Teorema 7.2.1.** *Seja  $\mathcal{N}$  uma rede neural sem realimentação com valor limiar linear, cujas unidades de computação são perceptrons. Suponha que  $\mathcal{N}$  só tem uma camada de entrada com  $k$  unidades, uma camada escondida com  $m$  unidades, e uma unidade de saída. Então, quando  $m$  é bastante grande,  $\mathcal{N}$  pode aproximar qualquer conceito boreliano  $C \subseteq \mathbb{R}^k$ . Em outras palavras, dado uma medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , um conjunto boreliano  $C \subseteq \mathbb{R}^k$  e  $\epsilon > 0$ , existem  $m$  e uma escolha de  $(k+1)m + (m+1)$  parâmetros da rede gerando um conceito  $C'$  com  $\mu(C' \Delta C) < \epsilon$ .*

Para mostrar o resultado, é necessário colocá-lo numa perspectiva ligeiramente mais geral, onde a unidade de saída é linear, e deste modo, a rede produz funções ao invés de conceitos.

**Teorema 7.2.2.** *Seja  $\mathcal{N}$  uma rede neural sem realimentação tendo uma camada de entrada com  $k$  unidades, uma camada escondida com  $m$  unidades, e uma unidade de saída. Suponha que todas as unidades tenham funções de modelagem afins, e as da camada escondida são perceptrons, enquanto a unidade de saída é linear. Então, para cada medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , quando  $m$  é bastante grande,  $\mathcal{N}$  pode aproximar qualquer função  $g \in L^1(\mathbb{R}^k, \mu)$ . Em outras palavras, dado uma medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , uma função  $g \in L^1(\mathbb{R}^k, \mu)$  e  $\varepsilon > 0$ , existem  $m$  e uma escolha de  $(k + 1)m + m$  parâmetros da rede gerando uma função  $g'$  com  $\|g' - g\|_{L^1(\mu)} < \varepsilon$ .*

Fornecemos algumas clarificações. A função gerada pela unidade computacional da camada 1 é da forma

$$u(x) = \eta \left( \sum_{i=1}^k a_i x_i - \theta \right),$$

onde  $a_i, \theta \in \mathbb{R}$  são os parâmetros (pesos e o valor limiar) e  $\eta$  a função de Heaviside. Deste modo, a função gerada pela rede é da forma

$$\sum_{j=1}^m \beta_j \eta \left( \sum_{i=1}^k a_{ij} x_i - \theta_j \right). \quad (7.9)$$

O teorema diz que um espaço vetorial gerado pelas composições da função de Heaviside  $\eta$  com todas as funções afins  $z: \mathbb{R}^k \rightarrow \mathbb{R}$ ,

$$z(x) = \langle a, x \rangle - \theta,$$

é denso em  $L^1(\mathbb{R}^k, \mu)$ , qualquer seja  $\mu \in P(\mathbb{R}^k)$ . Note que todas as composições  $\eta \circ z$  são funções borelianas e limitadas, logo pertencem ao espaço  $L^1(\mu)$ .

**Exercício 7.2.3.** Deduza teorema 7.2.1 do teorema 7.2.2.

A demonstração do teorema 7.2.2 é baseada sobre o resultado seguinte.

**Teorema 7.2.4** (Cramér–Wold). *Uma medida boreliana de probabilidade sobre  $\mathbb{R}^d$  é unicamente definida pelas suas imagens diretas sob todas as projeções unidimensionais.*

Em outras palavras, se  $\mu_1$  e  $\mu_2$  são duas medidas de probabilidade sobre  $\mathbb{R}^d$  tais que, qualquer seja uma projeção ortogonal  $\pi: \mathbb{R}^d \rightarrow \mathbb{R}$ , temos  $\pi_*(\mu_1) = \pi_*(\mu_2)$ . Então,  $\mu_1 = \mu_2$ .



Para mostrar o resultado, relembra que a *função caraterística*,  $\phi_\mu$ , de uma medida de probabilidade,  $\mu$ , sobre  $\mathbb{R}^d$  é uma função de  $\mathbb{R}^d$  para  $\mathbb{C}$ , dada por

$$\begin{aligned}\mathbb{R}^d \ni t \mapsto \phi_\mu(t) &= \mathbb{E}_\mu(\exp i \langle t, X \rangle) \\ &= \int_{\mathbb{R}^d} \exp i \langle t, x \rangle d\mu(x) \in \mathbb{C}.\end{aligned}$$

A função caraterística permite de reconstruir a medida  $\mu$  unicamente (teorema H.1.22).

**Exercício 7.2.5.** Seja  $V$  um sub-espaço linear do espaço vetorial  $\ell^2(d)$ , com a projecção ortogonal correspondente  $\pi: \ell^2(d) \rightarrow V$ . Seja  $\mu$  uma medida de probabilidade sobre  $\ell^2(d)$ . Verifique que para todo  $t \in V$ ,

$$\phi_{\pi_*(\mu)}(t) = \phi_\mu(t).$$

[ *Sugestão:* aplicando uma transformação unitária, pode-se supor que  $V$  é gerado pelos primeiros  $\dim V$  vetores de base... ]

Teorema 7.2.4 de Cramér–Wold segue imediatamente modulo teorema H.1.22 e o fato que os sub-espaços de dimensão um cobram  $\mathbb{R}^d$ .

*Observação 7.2.6.* O argumento estabelece, de fato, um resultado mais geral (teorema de Rényi): cada medida de probabilidade sobre  $\mathbb{R}^d$  é determinada unicamente pelas suas imagens sob projecções sobre uma família de sub-espaços lineares cuja união é  $\mathbb{R}^d$ .

*Observação 7.2.7.* Geometricamente, o teorema de Cramér–Wold diz que uma medida de probabilidade sobre  $\mathbb{R}^d$  é definida unicamente pelos valores sobre semi-espaços.

**Exercício 7.2.8.** Deduza que a conclusão do teorema de Cramér–Wold resta válida para quaisquer medidas borelianas *finitas* sobre  $\mathbb{R}^d$ .

*Prova do teorema 7.2.2.* Seja  $\mu$  uma medida de probabilidade boreliana sobre  $\mathbb{R}^k$ . Denotemos  $V$  um subespaço linear fechado de  $L^1(\mu)$  gerado pelas composições de  $\eta$  com todas as funções afins  $\mathbb{R}^k \rightarrow \mathbb{R}$ . Seja  $\phi$  um funcional linear limitado sobre  $L^1(\mu)$  qualquer, que se anula sobre  $V$ . Vamos mostrar que  $\phi$  é necessariamente trivial,  $\phi \equiv 0$ , o que implica, graças ao teorema de Hahn–Banach F.2.1, que  $V = L^1(\mu)$ .

Cada funcional linear limitado sobre  $L^1(\mu)$  pode ser identificado com uma função  $g \in L^\infty(\mu)$ , essencialmente limitada em relação com a medida  $\mu$ , pela fórmula:

$$\phi(h) = \int_{\mathbb{R}^k} g(x)h(x) d\mu(x). \quad (7.10)$$

(Teorema H.3.34). Segundo a escolha de  $\phi$ , para toda função afim  $z: \mathbb{R}^k \rightarrow \mathbb{R}$ , temos

$$\begin{aligned}\int \int_{\mathbb{R}^k} g(x)\eta(z(x)) d\mu(x) &= \phi(\eta \circ z) \\ &= 0.\end{aligned} \quad (7.11)$$

Consideremos a parte positiva e a parte negativa de  $g$ :

$$g_+(x) = \max\{g(x), 0\}, \quad g_-(x) = -\min\{g(x), 0\},$$

de modo que

$$g = g_+ - g_-.$$

Dado qualquer subconjunto boreliano,  $B \subseteq \mathbb{R}^k$ , definamos

$$\nu_{\pm}(B) = \int_B g_{\pm}(x) d\mu(x).$$

Estas  $\nu_{\pm}$  são medidas finitas, satisfazendo  $\nu_{\pm}(\mathbb{R}^k) \leq \text{ess sup } g$ . Vamos mostrar que  $\nu_+ = \nu_-$ , o que terminará a demonstração, pois para todas funções borelianas  $h$ ,

$$\phi(h) = \int_{\mathbb{R}^k} h(x) d\nu_+(x) - \int_{\mathbb{R}^k} h(x) d\nu_-(x). \quad (7.12)$$

Segue-se da eq. (7.11) que, qualquer seja função afim  $z: \mathbb{R}^k \rightarrow \mathbb{R}$ ,

$$\int_{\mathbb{R}^k} \eta(z(x)) d\nu_+(x) = \int_{\mathbb{R}^k} \eta(z(x)) d\nu_-(x). \quad (7.13)$$

Segundo o teorema de Cramér–Wold 7.2.4, uma medida de probabilidade (logo, uma medida finita) sobre  $\mathbb{R}^d$  é unicamente definida pelas imagens diretas sob todas as projeções unidimensionais. Basta mostrar que, dado um funcional linear  $\psi: \mathbb{R}^k \rightarrow \mathbb{R}$ , as medidas  $\psi_*(\nu_+)$  e  $\psi_*(\nu_-)$  são idênticas. Por sua vez, isto vai seguir se mostrarmos que as funções de distribuição de  $\psi_*(\nu_{\pm})$ ,

$$F_{\pm}(t) = \psi_*(\nu_{\pm})(-\infty, t],$$

são iguais para todos valores  $t$ . Seja  $t$  qualquer. Definemos a função afim  $z: \mathbb{R}^k \rightarrow \mathbb{R}$  por  $z(x) = -\psi(x) + t$ . Agora,

$$\psi(x) \leq t \iff z(x) \geq 0 \iff (\eta \circ z)(x) = 1,$$

de onde concluímos, usando eq. (7.12):

$$\begin{aligned} F_+(t) - F_-(t) &= \nu_+(\psi^{-1}(-\infty, t)) - \nu_-(\psi^{-1}(-\infty, t)) \\ &= \int (\eta \circ z) d\nu_+ - \int (\eta \circ z) d\nu_- \\ &= \int_{\mathbb{R}^k} g(x)(\eta \circ z) d\mu \\ &= \phi(\eta \circ z) \\ &= 0. \end{aligned} \quad (7.14)$$

□

Com pouco esforço adicional, podemos substituir a função de Heaviside  $\eta$  por qualquer função sigmóide  $f$  como função de ativação. Digamos que uma função  $f: \mathbb{R} \rightarrow \mathbb{R}$  é sigmóide se

$$\lim f(x) = \begin{cases} 0, & \text{quando } x \rightarrow -\infty, \\ 1, & \text{quando } x \rightarrow +\infty. \end{cases}$$

(Aqui, omitamos a condição para  $\eta$  ser monótona).

**Exercício 7.2.9.** Seja  $f: \mathbb{R} \rightarrow \mathbb{R}$  uma função boreliana, limitada e sigmóide. Mostre que existe uma sequência  $(z_n)$  de funções afins,  $z_n: \mathbb{R} \rightarrow \mathbb{R}$ , tais que, para cada medida de probabilidade  $\mu$  sobre  $\mathbb{R}$ ,  $\|f \circ z_n - \eta\|_{L^1(\mu)} \rightarrow 0$ .

[ *Sugestão:* dado  $\varepsilon > 0$ , pode-se escolher uma função afim  $z$  de modo que, se  $x \notin (0, \varepsilon)$ , temos  $|f(z(x)) - \eta(x)| < \varepsilon$ . Escolha recursivamente uma tal sequência  $z_n$ , verifique a convergência simples, e use o teorema de Lebesgue de convergência dominada. ]

**Exercício 7.2.10.** Adaptar a prova do teorema 7.2.2 acima (nomeadamente, a parte em torno da eq. (7.14) exige um pouco de trabalho) para mostrar que ao invés da função de Heaviside  $\eta$ , pode-se substituir qualquer função limitada, boreliana, e sigmóide,  $f$ .

Chegamos ao seguinte resultado.

**Teorema 7.2.11** (Teorema da Aproximação Universal [Cybenko 1989]). *Seja  $f: \mathbb{R} \rightarrow \mathbb{R}$  uma função boreliana e limitada sigmóide qualquer. Seja  $\mathcal{N}$  uma rede neural sem realimentação tendo uma camada de entrada com  $k$  unidades, uma camada escondida com  $m$  unidades, e uma unidade de saída. Suponha que todas as unidades tenham funções de modelagem afins, e as da camada escondida tenham a função de ativação  $\eta$ , enquanto a unidade de saída é linear. Então, para cada medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , quando  $m$  é bastante grande,  $\mathcal{N}$  pode aproximar qualquer função  $g \in L^1(\mathbb{R}^k, \mu)$ . Em outras palavras, dado uma medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , uma função  $g \in L^1(\mathbb{R}^k, \mu)$  e  $\varepsilon > 0$ , existem  $m$  e uma escolha de  $(k+1)m + m$  parâmetros da rede gerando uma função  $g'$  com  $\|g' - g\|_{L^1(\mu)} < \varepsilon$ .*

Neste caso, a função gerada pela unidade computacional da camada 1 é da forma

$$u(x) = f\left(\sum_{i=1}^k a_i x_i - \theta\right),$$

enquanto a função gerada pela rede é

$$\sum_{j=1}^m \beta_j f\left(\sum_{i=1}^k a_{ij} x_i - \theta_j\right). \quad (7.15)$$

O teorema diz que um espaço vetorial gerado pelas composições da função de ativação sigmóide  $f$  fixa com todas as funções afins  $z : \mathbb{R}^k \rightarrow \mathbb{R}$ ,

$$z(x) = \langle a, x \rangle - \theta,$$

é denso em  $L^1(\mathbb{R}^k, \mu)$ .

## 7.2.2 Discussão

Nós escolhemos de fórmular os resultados para norma  $L^1(\mu)$ , por causa de sua relevância para a nossa abordagem, mas de fato eles valem para qualquer  $L^p(\mu)$ ,  $1 \leq p < \infty$ , sem esforço extra. (Exercício).

O leitor pode querer modificar os argumentos acima para provar uma versão do teorema 7.2.11 para funções contínuas, que Cybenko [Cybenko 1989] considerou como mais importante.

**Teorema 7.2.12** (George Cybenko, 1989). *Seja  $f : \mathbb{R} \rightarrow \mathbb{R}$  uma função contínua e limitada sigmóide qualquer. Seja  $\mathcal{N}$  uma rede neural sem realimentação tendo uma camada de entrada com  $k$  unidades, uma camada escondida com  $m$  unidades, e uma unidade de saída. Suponha que todas as unidades tenham funções de modelagem afins, e as da camada escondida tenham a função de ativação  $\eta$ , enquanto a unidade de saída é linear. Então, quando  $m$  é bastante grande,  $\mathcal{N}$  pode aproximar qualquer função contínua  $g : \mathbb{R}^k \rightarrow \mathbb{R}$  na topologia de convergência uniforme sobre compactos. Em outras palavras, dado uma função  $g : \mathbb{R}^k \rightarrow \mathbb{R}$  contínua e limitada, um compacto  $K \subseteq \mathbb{R}^k$ , e  $\varepsilon > 0$ , existem  $m$  e uma escolha de  $(k + 1)m + m$  parâmetros da rede gerando uma função  $g'$  com  $\max_{x \in K} |g(x) - g'(x)| < \varepsilon$ .*

A prova deve usar uma forma mais forte do teorema de representação de Riesz do que nós estabelecemos no teorema H.2.1: para qualquer espaço compacto metrizável  $K$ , a fórmula

$$\phi(f) = \int_X f(x) d\mu(x)$$

estabelece uma correspondência bijetora entre os funcionais lineares limitados,  $\phi : C(K) \rightarrow \mathbb{R}$ , e medidas finitas com sinal, que tomam valores reais quaisquer, positivos assim como negativos.

Refinando ainda mais o mesmo círculo de ideias (teoria da transformada de Fourier, que está escondida em nossa prova ao disfarce da função característica de uma medida),

foi mostrado por Hornik [Hornik 1991] que, bastante surpreendentemente, a função de ativação pode ser qualquer função não essencialmente constante em relação à medida de Lebesgue,  $\lambda$ . (Uma função  $f: \mathbb{R} \rightarrow \mathbb{R}$  é essencialmente constante se  $f(x) = f(y)$  para quase todos  $x, y \in \mathbb{R}$ , ou seja, existe  $c \in \mathbb{R}$  tão que  $\lambda\{x \in \mathbb{R}: f(x) \neq c\} = 0$ .)

**Teorema 7.2.13** (Kurt Hornik, 1991). *Seja  $f: \mathbb{R} \rightarrow \mathbb{R}$  uma função boreliana qualquer, limitada e não essencialmente constante, em relação à medida de Lebesgue. Seja  $\mathcal{N}$  uma rede neural sem realimentação tendo uma camada de entrada com  $k$  unidades, uma camada escondida com  $m$  unidades, e uma unidade de saída. Suponha que todas as unidades tenham funções de modelagem afins, e as da camada escondida tenham a função de ativação  $\eta$ , enquanto a unidade de saída é linear. Então, para cada medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , quando  $m$  é bastante grande,  $\mathcal{N}$  pode aproximar qualquer função  $g \in L^1(\mathbb{R}^k, \mu)$ . Em outras palavras, dado uma medida de probabilidade  $\mu$  sobre  $\mathbb{R}^k$ , uma função  $g \in L^1(\mathbb{R}^k, \mu)$  e  $\varepsilon > 0$ , existem  $m$  e uma escolha de  $(k + 1)m + m$  parâmetros da rede gerando uma função  $g'$  com  $\|g' - g\|_{L^1(\mu)} < \varepsilon$ .*

A prova do teorema de Hornik necessita o uso de um teorema de Wiener na Análise Harmônica, oferecendo uma classificação completa de todos os sub-espços lineares fechados de  $L^1(\mathbb{R}, \lambda)$ , invariantes pelas translações. No mesmo artigo [ibid.] Hornik mostrou também uma versão contínua do resultado, parecida ao teorema 7.2.12, onde a função de ativação  $f: \mathbb{R} \rightarrow \mathbb{R}$  pode ser qualquer função contínua e limitada não constante.

*Observação 7.2.14.* Mencionemos uma pergunta de Hornik [ibid.] que pode ser ainda em aberto. Quais são as condições (necessárias e suficientes) sobre uma função de ativação  $f: \mathbb{R} \rightarrow \mathbb{R}$  (não necessariamente boreliana) para garantirem que a classe de funções  $g'$  geradas pela rede como acima aproxime todas as funções contínuas  $g: \mathbb{R}^k \rightarrow \mathbb{R}$  na topologia de convergência uniforme sobre compactos? (Esta topologia tem sentido para espaço linear de todas as funções de  $\mathbb{R}^k$  para  $\mathbb{R}$  limitadas sobre cada compacto).

É claro que algumas condições sejam necessárias, pois se, por exemplo,  $f$  é a função indicadora de um ponto, a conclusão é falsa.

## 7.3 Minimização de risco estrutural

Até agora, estudamos dois conceitos de aprendizagem: a dentro da classe, e a universalmente consistente. Ambos têm vantagens e desvantagens. Aprendizagem dentro da classe permite estimar o erro de generalização, porém não pode aproximar qualquer conceito. De outro lado, regras de aprendizagem universalmente consistentes podem aprender qualquer conceito, mas a taxa de aprendizagem pode ser arbitrariamente devagar.

Nós discutiremos agora um conceito de aprendizagem que pertence a [Vapnik 1998] e que combina alguns bons aspectos das duas abordagens: o princípio de minimização de risco estrutural.

Senti-me tentado de desenvolver uma apresentação diferente, e quaisquer erros e mal-entendidos surgiram, são certamente os meus próprios.

### 7.3.1 Re-examinando o erro empírico de aprendizagem

Dada uma classe de conceitos  $\mathcal{C}$  e uma amostra rotulada  $(\sigma, \epsilon)$ , o princípio de minimização do erro empírico exige minimizar sobre  $C \in \mathcal{C}$  o erro empírico de aprendizagem do conceito desconhecido,  $D$ ,

$$\text{erro}_{\mu_\sigma, D}(C) = \mu_\sigma(C \Delta D).$$

Note que a expressão pode ser re-escrita evitando  $D$ , pois somente usamos a rotulagem  $D \upharpoonright \sigma$  produzida sobre  $\sigma$  por  $D$ , or, de modo equivalente, a sub-amostra  $\sigma_+ \sqsubset \sigma$  formada pelos pontos  $x_i$  com o rótulo correspondente  $\epsilon_i = 1$ :

$$\text{erro}_{\mu_\sigma, \sigma_+}(C) = \mu_\sigma(\sigma_+ \Delta C).$$

Reinterpretemos o erro empírico  $\text{erro}_{\mu_\sigma, \sigma_+}(C)$  no contexto do problema de aprendizagem  $(\mu, \eta)$  no domínio  $\Omega$ , onde  $\mu \in P(\Omega)$  e  $\eta: \Omega \rightarrow [0, 1]$  é uma função de regressão.

Recordemos o teorema 4.1.10: dado uma classe de conceitos  $\mathcal{C}$  qualquer, com confiança  $1 - \delta$ ,

$$\sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| \leq 2R_n(\mathcal{C}) + \sqrt{\frac{\ln(2/\delta)}{2n}}.$$

Nos lemas seguintes, a amostra rotulada  $(\sigma, \sigma_+)$  segue a lei conjunta dada por  $(\mu, \eta)$ .

**Lema 7.3.1.** *Seja  $\mathcal{C}$  uma classe de conceitos. Para todos  $C \in \mathcal{C}$ , com confiança  $1 - \delta$ ,*

$$\begin{aligned} \mu_\sigma(\sigma_+ \cap C) &\stackrel{\varepsilon}{\approx} \mu_1(C) \\ &= \int_C \eta d\mu, \end{aligned}$$

onde

$$\varepsilon = 2R_n(\mathcal{C}) + \sqrt{\frac{\ln(2/\delta)}{2n}}. \quad (7.16)$$

*Demonstração.* Basta aplicar o teorema 4.1.10 à medida empírica  $\mu_{(\sigma, \epsilon)}$  no domínio rotulado  $\Omega \times \{0, 1\}$ , substituindo  $C \times \{1\}$  em vez de  $C$ . A complexidade de Rademacher da classe de conjuntos  $C \times \{1\}$ ,  $C \in \mathcal{C}$ , é limitada por cima pela complexidade da classe  $\mathcal{C}$ .  $\square$

Do modo parecido, usando o teorema 4.1.10 com a classe de conceitos  $C \times \{0\}$ , obtemos

**Lema 7.3.2.** *Para todos  $C \in \mathcal{C}$ , com confiança  $1 - \delta$ ,*

$$\begin{aligned} \mu_\sigma(\sigma_- \cap C) &\stackrel{\varepsilon}{\approx} \mu_0(C) \\ &= \int_C (1 - \eta) d\mu, \end{aligned}$$

onde  $\varepsilon$  é como na eq. (7.16).

**Exercício 7.3.3.** Mostre que a complexidade de Rademacher da classe  $\mathcal{C}^c$ , formada pelos conceitos complementares  $\Omega \setminus C$ ,  $C \in \mathcal{C}$ , é igual a complexidade de Rademacher de  $\mathcal{C}$ .

**Lema 7.3.4.** Para todos  $C \in \mathcal{C}$ , com confiança  $1 - 2\delta$ ,

$$\begin{aligned} \text{erro}_{\mu_\sigma, \sigma_+}(C) &\stackrel{\varepsilon}{\approx} \int_{\Omega} |\chi_C - \eta| d\mu \\ &= \text{erro}_{\mu, \eta}(C), \end{aligned}$$

onde

$$\varepsilon = 4R_n(\mathcal{C}) + 2\sqrt{\frac{\ln(2/\delta)}{2n}}.$$

*Demonstração.*

$$\begin{aligned} \int_{\Omega} |\chi_C - \eta| d\mu &= \int_C (1 - \eta) d\mu + \int_{\Omega \setminus C} \eta d\mu \\ &\stackrel{2\varepsilon}{\approx} \mu_\sigma(\sigma_- \cap C) + \mu_\sigma(\sigma_+ \cap (\Omega \setminus C)) \\ &= \mu_\sigma[(C \setminus \sigma_+) \cup (\sigma_+ \setminus C)] \\ &= \mu_\sigma(C \Delta \sigma_+) \\ &= \text{erro}_{\mu_\sigma, \sigma_+}(C). \end{aligned}$$

□

Por conseguinte, mesmo quando apenas ambicionarmos a minimizar o erro de aprendizagem dentro de um problema determinístico (sob a hipótese  $\eta = \chi_C$ ), na realidade, estamos minimizando o erro de aprendizagem no problema com ruído aleatório também.

### 7.3.2 Classes filtradas

Seja  $\mathcal{C}$  uma classe de conceitos num domínio  $\Omega$ , munido de uma *filtração*, ou seja, representado como união de uma cadeia crescente de sub-classes,

$$\mathcal{C} = \bigcup_{m=1}^{\infty} \mathcal{C}_m,$$

$$\mathcal{C}_1 \subseteq \mathcal{C}_2 \subseteq \dots \subseteq \mathcal{C}_m \subseteq \dots$$

Para  $C \in \mathcal{C}$  escrevamos

$$\text{gr}(C) = \min\{m \in \mathbb{N} : C \in \mathcal{C}_m\}.$$

Suponhamos também que

1. Dimensão de Vapnik–Chervonenkis de cada classe  $\text{VC-dim}(\mathcal{C}_m) = d_m < \infty$  é finita,
2.  $\mathcal{C}$  tem a propriedade de aproximação universal: para cada medida de probabilidade  $\mu$  sobre  $\Omega$ , cada conceito boreliano  $D \subseteq \Omega$ , e cada  $\varepsilon > 0$ , existe  $C \in \mathcal{C}$  tal que  $\mu(C \Delta D) < \varepsilon$ .

Vamos chamar uma tal classe *classe filtrada*.

*Observação 7.3.5.* Segue-se que a sequência  $(d_m)$  é monótona e converge para infinito,  $d_m \uparrow +\infty$ .

**Exemplo 7.3.6.** Seja  $\mathcal{C}_m$  a classe de conceitos gerada pela rede neural sem realimentação, com valor limiar linear, tendo uma camada interior com  $m$  unidades. Teoremas 2.3.20 e 7.2.11 servem a verificar que a classe de conceitos filtrada  $\mathcal{C} = \bigcup_{m=1}^{\infty} \mathcal{C}_m$  satisfaz as duas condições.

**Exemplo 7.3.7.** Definemos  $\mathcal{C}_m$  a classe de todos os conceitos da forma  $\eta \circ p_m$ , onde  $\eta$  é a função de Heaviside e  $p_m$  é um polinômio qualquer de grau  $\leq m$ . As duas condições acima seguem do teorema 2.1.14 (imediato) e do teorema de Stone–Weierstrass F.3.1 (isto exige um pouco de trabalho, exercício).

**Exemplo 7.3.8.** Seja  $\Omega = \{0, 1\}^{\mathbb{N}}$  um espaço de Cantor (as vezes chamado o “cubo de Cantor”), ou seja, um espaço compacto metrizável totalmente desconexo sem pontos isolados, cuja topologia é gerada pela métrica

$$d(x, y) = 2^{-\min\{i : x_i \neq y_i\}}.$$

Dado  $m \in \mathbb{N}$ , definemos  $\mathcal{C}_m$  a classe de todos os conjuntos cilíndricos  $\mathcal{C}_m$  com a base nas primeiras  $m$  coordenadas:

$$\mathcal{C}_m = \{\pi_m^{-1}(A) : A \subseteq \{0, 1\}^m\},$$

once  $\pi_m$  é a projeção canônica de  $\{0, 1\}^{\mathbb{N}}$  sobre  $\{0, 1\}^m$ . Tais conjuntos são abertos e fechados. A classe  $\mathcal{C}_m$  é finita, com  $2^m$  elementos, e  $\text{VC-dim}(\mathcal{C}_m) = m$ . A propriedade de aproximação universal da classe  $\mathcal{C} = \bigcup_{m=1}^{\infty} \mathcal{C}_m$  segue das duas afirmações seguintes, deixadas como exercícios.

1. Dado um conjunto boreliano  $C \subseteq \{0, 1\}^{\mathbb{N}}$ , uma medida de probabilidade  $\mu$ ,  $\mu, \varepsilon > 0$ , existe um conjunto aberto e fechado  $V \subset \{0, 1\}^{\mathbb{N}}$  tal que  $\mu(C \Delta V) < \varepsilon$ . (Usar teorema E.2.11 sobre regularidade de  $\mu$ , mais um pouco da topologia geral).
2. Cada conjunto aberto e fechado  $V \subset \{0, 1\}^{\mathbb{N}}$  é necessariamente da forma  $\pi_m^{-1}(A)$  para  $m$  e  $A \subseteq \{0, 1\}^m$  apropriados. (Use compacidade). Assim,  $\mathcal{C}$  é exatamente a classe de todos subconjuntos abertos e fechados do cubo de Cantor.



**Exercício 7.3.9.** Mostre que para cada classe de conceitos  $\mathcal{C}$ ,

$$\hat{R}_n(\mathcal{C}) \leq \sqrt{2d \frac{\log n}{n}},$$

onde  $d = \text{VC-dim}(\mathcal{C})$ .

[ *Sugestão:* combinar as estimativas na prova da implicação (2)  $\Rightarrow$  (1), página 131, a desigualdade na subseção 4.3.3, e o lema de Sauer–Shelah. ]

**Lema 7.3.10.** *Sejam  $\mathcal{C}$  uma classe filtrada. Dada uma sequência  $(\delta_m)$ ,  $\delta_m > 0$ , a um número  $\delta > 0$  tais que  $\delta = \sum_{m=1}^{\infty} \delta_m$ , temos para cada problema de aprendizagem  $(\mu, \eta)$  em  $\Omega$ , com confiança  $1 - 2\delta$ ,*

$$\begin{aligned} \forall C \in \mathcal{C}, \quad |erro_{\mu_{\sigma}, \sigma_+}(C) - erro_{\mu, \eta}(C)| &\leq 4R_n(\mathcal{C}_{\text{gr}}(C), \mu) + 2\sqrt{\frac{\ln(2/\delta_{\text{gr}}(C))}{2n}} \\ &\leq 4\sqrt{2d_{\text{gr}}(C) \frac{\log n}{n}} + 2\sqrt{\frac{\ln(2/\delta_{\text{gr}}(C))}{2n}}. \end{aligned}$$

*Demonstração.* Para todo  $m$ , pelo lema 7.3.4 temos com confiança  $1 - 2\delta_m$ ,

$$\forall C \in \mathcal{C}_m, \quad |erro_{\mu_{\sigma}, \sigma_+}(C) - erro_{\mu, \eta}(C)| \leq 4R_n(\mathcal{C}_m, \mu) + 2\sqrt{\frac{\ln(2/\delta_m)}{2n}},$$

e a primeira desigualdade segue com risco  $2\delta = \sum_{i=1}^{\infty} 2\delta_m$  pela cota da união. A segunda desigualdade segue do exercício 7.3.9.  $\square$

**Definição 7.3.11.** *Seja  $\mathcal{C}$  uma classe filtrada,  $(\mu, \eta)$  um problema de aprendizagem, e  $(\delta_m)_{m=1}^{\infty}$  uma sequência somável de reais,  $\delta_m > 0$ . O risco estrutural é a função*

$$erro_{\mu_{\sigma}, \sigma_+}(C) + 4\sqrt{2d_{\text{gr}}(C) \frac{\log n}{n}} + 2\sqrt{\frac{\ln(2/\delta_{\text{gr}}(C))}{2n}}.$$

A regra de aprendizagem  $\mathcal{L}$  segue o *princípio de minimização do risco estrutural* se para todo  $n$ ,  $\mathcal{L}_n$  escolha a hipótese  $H$  minimizando a expressão acima.

*Observação 7.3.12.* É claro que a escolha de uma tal hipótese  $H$  é sempre possível. Mostrar que tal escolha é sempre possível em uma forma Borel mensurável exige trabalho adicional, no espírito da subseção 4.5.3. Por exemplo, isto é sempre possível se a classe  $\mathcal{C}$  é universalmente separável (exercício).

**Exercício 7.3.13.** Mostrar que as classes filtradas nos exemplos 7.3.6, 7.3.7, e 7.3.8 são universalmente separáveis.

**Teorema 7.3.14.** *Cada regra de aprendizagem seguindo o princípio de minimização do risco estrutural numa classe filtrada é universalmente consistente.*

*Demonstração.* Dada uma classe filtrada  $\mathcal{C}$ , escolhemos uma sequência  $(m_n)$  que cresce,  $m_n \uparrow +\infty$ , mas bastante devagar, da maneira que a sequência

$$4\sqrt{2d_{m_n} \frac{\log n}{n}} + 2\sqrt{\frac{\ln(2/\delta_{m_n})}{2n}}$$

converge para zero monotonicamente. Lema 7.3.10 implica que, com confiança  $1 - 2\sum_{i=m_n}^{\infty} \delta_i$ ,

$$\forall C \in \mathcal{C}, \quad |\text{erro}_{\mu\sigma, \sigma_+}(C) - \text{erro}_{\mu, \eta}(C)| \leq 4\sqrt{2d_{m_n \wedge \text{gr}}(C) \frac{\log n}{n}} + 2\sqrt{\frac{\ln(2/\delta_{m_n \wedge \text{gr}}(C))}{2n}}.$$

Seja  $\varepsilon > 0$  qualquer. Existe  $M$  tão grande que a classe  $\mathcal{C}_M$  contém um conceito  $C$  com  $\|\chi_C - T_{\text{Bayes}}\|_1 < \varepsilon$ . Este  $C$  pertence a todas as classes  $\mathcal{C}_m$ ,  $m \geq M$ . Segundo lema 7.3.4, com confiança  $1 - 2\sum_{i=m_n}^{\infty} \delta_i$ , a regra  $\mathcal{L}_n$  vai escolher uma hipótese  $H$  satisfazendo

$$|\text{erro}_{\mu\sigma, \sigma_+}(H) - \text{erro}_{\mu, \eta}(H)| \leq 4\sqrt{2d_{m_n \wedge \text{gr}}(H) \frac{\log n}{n}} + 2\sqrt{\frac{\ln(2/\delta_{m_n \wedge \text{gr}}(H))}{2n}}.$$

Combinando duas desigualdades, concluímos: com confiança  $1 - 4\sum_{i=m_n}^{\infty} \delta_i$ ,

$$\text{erro}_{\mu, \eta} \mathcal{L}_n(\sigma, \sigma_+) \leq \ell^*(\mu, \eta) + \varepsilon + 8\sqrt{2d_{m_n \wedge \text{gr}}(H) \frac{\log n}{n}} + 4\sqrt{\frac{\ln(2/\delta_{m_n \wedge \text{gr}}(H))}{2n}}.$$

Quando  $n \rightarrow \infty$ , as duas raízes e o risco  $\sum_{i=m_n}^{\infty} \delta_i$  convergem para zero, e  $\varepsilon > 0$  foi qualquer. Deduzimos a convergência em probabilidade

$$\text{erro}_{\mu, \eta} \mathcal{L}_n(\sigma, \sigma_+) \rightarrow \ell^*(\mu, \eta).$$

□



# Compressão amostral

---

## 8.1 Compressão, descompressão, e aprendizagem

### 8.1.1

O assunto do último capítulo é esquemas de compressão amostral. Denotemos por  $[\Omega]^d$  o conjunto de todos os subconjuntos com  $d$  elementos,  $[\Omega]^{\leq d}$  o conjunto de todos os subconjuntos com  $\leq d$  elementos, e  $[\Omega]^{\leq \infty}$  o conjunto de todos os subconjuntos finitos. Na sua versão mais básica e pura, uma *aplicação de descompressão amostral de tamanho  $d$*  é qualquer aplicação

$$\mathcal{H}: [\Omega]^{\leq d} \rightarrow 2^\Omega,$$

associando a cada subconjunto com  $\leq d$  elementos uma hipótese, ou seja, um subconjunto de  $\Omega$ . A aplicação de descompressão pode ser também codificada assim:

$$\mathcal{H}: [\Omega]^{\leq d} \times \Omega \rightarrow \{0, 1\}. \quad (8.1)$$

Deste modo, os subconjuntos finitos de  $\Omega$ ,  $\sigma = \{x_1, x_2, \dots, x_n\}$ , estão vistos como “amostras” num sentido um pouco diferente: nós descartamos a ordem nas amostras, bem como repetições de pontos.

**Exemplo 8.1.1.** Seja  $\Omega = \mathbb{R}$  e  $d = 2$ . A cada conjunto  $\sigma$  com  $\leq 2$  pontos associemos o menor intervalo fechado,  $I(\sigma)$ , que contém  $\sigma$ , ou seja, a envoltória fechada convexa de  $\sigma$  na reta. A mesma construção se aplica a qualquer conjunto  $\Omega$  totalmente ordenado.

**Exemplo 8.1.2.** Seja  $\Omega = \mathbb{R}^2$  e  $d = 4$ . A cada conjunto  $\sigma$  com  $\leq 4$  pontos associemos o menor retângulo fechado,  $\Pi(\sigma)$ , cujos lados são paralelos aos eixos coordenados e que contém  $\sigma$ .

Dado uma aplicação de descompressão amostral,  $\mathcal{H}$ , definimos a classe  $\mathcal{C}_{\mathcal{H}}$ , que consiste de todos os subconjuntos  $C \subseteq \Omega$  satisfazendo

$$\forall \sigma \in [\Omega]^{\leq \infty}, \exists \tau \subseteq \sigma, \tau \in [\Omega]^{\leq d}, \mathcal{H}(\tau) \cap \sigma = C \cap \sigma. \quad (8.2)$$

Em outras palavras, a rotulagem induzida por  $C$  sobre qualquer amostra finita,  $\sigma$ , pode ser também induzida pela descompressão de uma subamostra apropriada de  $\sigma$  de tamanho  $\leq d$ .

**Exercício 8.1.3.** Seja  $\mathcal{H}$  uma aplicação de descompressão amostral de tamanho  $d$ . Mosrar que a classe  $\mathcal{C}_{\mathcal{H}}$  tem dimensão de Vapnik–Chervonenkis  $\leq d$ .

[ *Sugestão*: contar as rotulagens diferentes sobre  $\sigma$ . ]

Um problema maior em aberto é o seguinte. Seja  $\mathcal{C}$  uma classe de conceitos. Existe uma aplicação de descompressão de tamanho  $d = \text{VC-dim}(\mathcal{C})$  tal que  $\mathcal{C} \subseteq \mathcal{C}_{\mathcal{H}}$ ?

*Observação 8.1.4.* Os exemplos 8.1.1 e 8.1.2 fornecem uma boa ilustração simples.

Para esquemas de compressão, a ordem dos elementos numa amostra, bem como as repetições, não importam. Por isso, uma *amostra* significa um subconjunto finito do domínio,  $\Omega$ , enquanto uma *amostra rotulada* vai significar um subconjunto finito  $\sigma$  do domínio  $\Omega$ , munido de uma rotulagem, ou seja, um subconjunto  $\tau \subseteq \sigma$  de pontos rotulados 1, no pressuposto de que os pontos de  $\sigma \setminus \tau$  são rotulados 0. Denotemos por  $[\Omega]^{\leq d \ 0|1}$  o conjunto de todas as amostras rotuladas de tamanho  $\leq d$ , e da mesma maneira  $[\Omega]^{\leq \infty \ 0|1}$ .

Dado uma aplicação de descompressão amostral,  $\mathcal{H}$ , na definição da classe  $\mathcal{C}_{\mathcal{H}}$  fica implícita uma *aplicação de compressão amostral de tamanho  $d$* ,

$$\kappa: [\Omega]^{\leq \infty \ 0|1} \rightarrow [\Omega]^{\leq d}, \quad (8.3)$$

tendo as propriedades

$$\kappa(\sigma, \tau) \subseteq \sigma \quad (8.4)$$

e, para cada  $C \in \mathcal{C}_{\mathcal{H}}$ ,

$$\mathcal{H}(\kappa(\sigma, C \cap \sigma)) \cap \sigma = C \cap \sigma. \quad (8.5)$$

**Definição 8.1.5.** Um *esquema de compressão amostral de tamanho  $d$*  para uma classe de conceitos  $\mathcal{C}$  é um par  $(\mathcal{H}, \kappa)$ , onde  $\mathcal{H}$  é uma aplicação de descompressão de tamanho  $d$  tal que  $\mathcal{C} \subseteq \mathcal{C}_{\mathcal{H}}$ , e  $\kappa$  é uma aplicação de compressão de tamanho  $d$  correspondente.

*Observação 8.1.6.* De modo equivalente, um esquema de compressão amostral de tamanho  $d$  pode ser definido como um par  $(\mathcal{H}, \kappa)$  de aplicações

$$\mathcal{H}: [\Omega]^{\leq d} \rightarrow 2^{\Omega},$$

$$\kappa: [\Omega]^{\leq \infty \ 0|1} \rightarrow [\Omega]^{\leq d},$$

tendo as propriedades nas eq. (8.4) e (8.5).

Em particular,  $\mathcal{H} \circ \kappa$  é uma regra de aprendizagem consistente com a classe  $\mathcal{C}$ , o que conduz-nos ao assunto de aprendizagem. Por esta razão, estamos mais interessados no caso onde a aplicação de descompressão na eq. (8.1) é boreliana. O tópico de mensurabilidade de esquemas de compressão é praticamente inexplorado (no entanto, veja a dissertação [Kalajdziewski 2012]).

**Exercício 8.1.7.** Seja  $\Omega$  um espaço boreliano padrão e  $k \in \mathbb{N}$ . Mostrar que o espaço  $[\Omega]^k$  tem uma estrutura boreliana padrão induzida do produto  $\Omega^k$ .

[ *Sugestão:* identificar  $\Omega$  com o intervalo  $\mathbb{I}$ . ] Deduzir que  $[\Omega]^{\leq k}$  e  $[\Omega]^{\leq \infty}$  também admitem estruturas borelianas padrão naturais.

A pergunta seguinte está mais forte, e vemos que uma resposta positiva implicaria a resposta positiva na pergunta na página 242. Seja  $\mathcal{C}$  uma classe de conceitos. Suponha que  $\mathcal{C}$  seja munido de uma estrutura boreliana padrão tal que  $\{(x, C) : x \in C \in \mathcal{C}\}$  é um subconjunto boreliano de  $\Omega \times \mathcal{C}$ . Existe uma aplicação de descompressão boreliana de tamanho  $d = \text{VC-dim}(\mathcal{C})$  tal que  $\mathcal{C} \subseteq \mathcal{C}_{\mathcal{H}}$ ? Por exemplo, se  $\mathcal{C}$  é universalmente separável?

**Exercício 8.1.8.** Mostre que a classe  $\mathcal{C}_{\mathcal{H}}$  gerado por uma função de descompressão  $\mathcal{H}$  é fechado na topologia de convergência simples. Deduza que se  $\mathcal{C}'$  é universalmente denso em  $\mathcal{C}$ , então cada esquema de compressão amostral para  $\mathcal{C}'$  é automaticamente um esquema de compressão amostral para  $\mathcal{C}$  também.

Aqui é a ligação com a aprendizagem supervisionada. Definemos a aplicação canónica  $\iota$  que esquece a ordem e as repetições numa amostra rotulada,

$$\iota: \bigcup_{n=1}^{\infty} \Omega^n \times \{0, 1\}^n \rightarrow [\Omega]^{\leq \infty} \times [\Omega]^{\leq \infty},$$

$$\sigma = (x_1, x_2, \dots, x_n, \epsilon_1, \epsilon_2, \dots, \epsilon_n) \mapsto (\{x_1, x_2, \dots, x_n\}, \{x_i : \epsilon_i = 1\}).$$

Agora, cada esquema de compressão amostral para uma classe  $\mathcal{C}$  defina uma regra de aprendizagem como segue: dado uma amostra rotulada  $(\sigma, \epsilon)$ ,

$$\mathcal{L}(\sigma, \epsilon) = \mathcal{H}(\kappa(\iota(\sigma, \epsilon))).$$

Segue-se das definições que a regra é consistente com a classe  $\mathcal{C}$ , logo, PAC aprende  $\mathcal{C}$  (teorema 4.4.6 e exercício 8.1.3).

Existe uma prova direta e muito simples, sem usar as classes de Glivenko–Cantelli. O resultado seguinte foi um dos principais no trabalho original [Littlestone e Warmuth 1986], onde a teoria de esquemas de compressão amostral foi lançada. Curiosamente, o manuscrito nunca foi publicado, porém resta um das referências mais importantes nesta área.

**Teorema 8.1.9** (Littlestone–Warmuth). *Seja  $(\mathcal{H}, \kappa)$  um esquema de compressão amostral de tamanho  $d$  para uma classe  $\mathcal{C}$  de conceitos borelianos, tal que a aplicação  $\mathcal{H}: [\Omega]^{\leq d} \times$*

$\Omega \rightarrow \{0, 1\}$  é boreliana. Então a regra  $\mathcal{L} = \mathcal{H} \circ \kappa \circ \iota$  PAC aprende a classe  $\mathcal{C}$  com erro  $\varepsilon > 0$  e confiança

$$\geq 1 - \sum_{j=0}^d \binom{n}{j} (1 - \varepsilon)^{n-j} > 1 - \left(\frac{en}{d}\right)^d (1 - \varepsilon)^{n-d},$$

onde  $n$  é o tamanho da amostra.

No seguinte, identifiquemos o espaço boreliano padrão  $\Omega$  com o intervalo  $\mathbb{I} = [0, 1]$ . Fixemos o tamanho da amostra,  $n$ . Seja  $J$  um subconjunto de  $[n] = \{1, 2, 3, \dots, n\}$ . Dado uma amostra  $\sigma \in [\mathbb{I}]^d$ , escrevamos-la  $\sigma = \{x_1, x_2, \dots, x_n\}$ , onde  $x_1 < x_2 < \dots < x_n$ , e formemos uma amostra  $\sigma_J$  com  $d$  elementos pela regra

$$x_i \in \sigma_\tau \iff i \in J.$$

A aplicação

$$[\mathbb{I}]^n \ni \sigma \mapsto \sigma_J \in [\mathbb{I}]^{\#J}$$

é contínua com relação à topologia de produto, em particular boreliana.

**Exercício 8.1.10.** Verificar que na presença de uma lei  $\mu$  os elementos aleatórios  $\sigma_J$  e  $\sigma_{[n] \setminus J}$  são independentes.

Cada escolha de um conjunto de índices  $J \in [[n]]^{\leq d}$  de tamanho  $j \leq d$  define a hipótese aleatória  $\mathcal{H}(\sigma_J)$ . (A noção tem sentido porque a aplicação  $\mathcal{H}$  é boreliana). Segue-se que o elemento aleatório  $\mathcal{H}(\sigma_J)$  é independente de  $\sigma_{[n] \setminus J}$ .

Agora seja  $C \in \mathcal{C}$  qualquer, induzindo uma rotulagem  $C \upharpoonright \sigma$  sobre  $\sigma$ . Usamos o truque de condicionamento. Para  $J$  e  $\sigma_J$  fixos, se  $\mu(\mathcal{H}(\sigma_J) \Delta C) > \varepsilon$ , então a probabilidade que  $\mu_{\sigma_{[n] \setminus J}}(\mathcal{H}(\sigma_J) \Delta C) = 0$  é menos de  $(1 - \varepsilon)^{n-j}$ . Isso significa que a probabilidade do evento  $\sigma_J = \kappa(C \upharpoonright \sigma)$  é também  $< (1 - \varepsilon)^{n-j}$ . A cota de união termina a prova da primeira desigualdade. A segunda segue do lema 1.2.6.  $\square$

**Exercício 8.1.11.** Estimar acima a complexidade amostral da regra  $\mathcal{L} = \mathcal{H} \circ \kappa \circ \iota$  no teorema 8.1.9. Por exemplo, tentar deduzir a estimativa de [Moran e Yehudayoff 2016] (Th. 1.2):

$$s(\varepsilon, \delta) \leq \frac{8}{\varepsilon} \left( d \log \left( \frac{2}{\varepsilon} \right) + \log \left( \frac{1}{\delta} \right) \right).$$

## 8.1.2 Dimensão VC um

Mostremos que toda classe de dimensão VC um admite um esquema de compressão amostral de tamanho um, com boas propriedades de mensurabilidade.

**Exercício 8.1.12.** Mostrar que a diferença simétrica

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

é associativa,

$$(A \Delta B) \Delta C = A \Delta (B \Delta C)$$

e distributiva sobre interseção:

$$A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C).$$

**Lema 8.1.13.** *Seja  $\mathcal{C}$  uma classe de conceitos, e  $D \subseteq \Omega$  um conceito qualquer. A dimensão de Vapnik–Chervonenkis da classe*

$$\mathcal{C} \Delta D = \{C \Delta D : C \in \mathcal{C}\}$$

é igual à de  $\mathcal{C}$ .

*Demonstração.* Sejam  $A$  um subconjunto fragmentado por  $\mathcal{C}$ , e  $B \subseteq A$ . Existe  $C \in \mathcal{C}$  tal que  $C \cap A = B \Delta (D \cap A)$ . Agora temos:

$$\begin{aligned} A \cap (C \Delta D) &= (A \cap C) \Delta (A \cap D) \\ &= (B \Delta (D \cap A)) \Delta (D \cap A) \\ &= B \Delta \emptyset \\ &= B. \end{aligned}$$

Segue-se que  $\text{VC-dim}(\mathcal{C}) \leq \text{VC-dim}(\mathcal{C} \Delta D)$ . Como  $(\mathcal{C} \Delta D) \Delta D = \mathcal{C}$ , obtemos a igualdade.  $\square$

**Lema 8.1.14.** *Seja  $\mathcal{H}$  uma aplicação de descompressão de tamanho  $d$ , e  $D \subseteq \Omega$  um conceito qualquer. A formula*

$$[\Omega]^{\leq d} \ni \tau \mapsto \mathcal{H}(\tau) \Delta D \subseteq \Omega$$

defina uma aplicação de descompressão de tamanho  $d$  cuja classe de conceitos associada é

$$\mathcal{C}_{\mathcal{H} \Delta D} = \mathcal{C}_{\mathcal{H}} \Delta D. \quad (8.6)$$

*Demonstração.* Seja  $\kappa$  uma aplicação de compressão correspondente a  $\mathcal{H}$ . Definemos a aplicação

$$\begin{aligned} D_{\kappa} : [\Omega]^{< \infty} \times [\Omega]^{< \infty} &\rightarrow [\Omega]^{\leq d}, \\ D_{\kappa}(\sigma, \tau) &= \kappa(\sigma, \tau \Delta (D \cap \sigma)). \end{aligned}$$

Para qualquer elemento  $C \Delta D \in \mathcal{C}_{\mathcal{H}} \Delta D$  e qualquer  $\sigma \in [\Omega]^{<\infty}$ , temos

$$\begin{aligned} \sigma \cap [\mathcal{H}({}^D \kappa(\sigma, \sigma \cap (C \Delta D)) \Delta D)] &= \sigma \cap [\mathcal{H}(\kappa(\sigma, (\sigma \cap C) \Delta (\sigma \cap D)) \Delta (D \cap \sigma)) \Delta D] \\ &= \sigma \cap [\mathcal{H}(\kappa(\sigma, \sigma \cap C) \Delta D)] \\ &= [\sigma \cap \mathcal{H}(\kappa(\sigma, \sigma \cap C))] \Delta (\sigma \cap D) \\ &= (\sigma \cap C) \Delta (\sigma \cap D) \\ &= \sigma \cap (C \Delta D). \end{aligned}$$

Isto estabelece a inclusão  $\supseteq$  na eq. (8.6). Mas a situação é simétrica:  $(\mathcal{H} \Delta D) \Delta D = \mathcal{H}$ .  $\square$

**Lema 8.1.15.** *Seja  $\mathcal{C}$  uma classe de conceitos tal que  $\emptyset \in \mathcal{C}$  e  $VC\text{-dim}(\mathcal{C}) = 1$ . Formemos a classe  $\mathcal{C}^\cap$  que consiste de todas as interseções de sub-famílias não vazias de  $\mathcal{C}$ :*

$$\mathcal{C}^\cap = \{\cap \mathcal{C}' : \emptyset \neq \mathcal{C}' \subseteq \mathcal{C}\}.$$

Então,

$$VC\text{-dim}(\mathcal{C}^\cap) = 1.$$

*Demonstração.* Suponha que existe um conjunto,  $\{a, b\}$ , com dois pontos distintos fragmentado pela classe  $\mathcal{C}^\cap$ . Em particular, existem  $C'_1, C'_2, C'_3 \in \mathcal{C}^\cap$  tais que  $C'_1 \cap \{a, b\} = \{a\}$ ,  $C'_2 \cap \{a, b\} = \{b\}$ , e  $C'_3 \supseteq \{a, b\}$ . A definição da classe  $\mathcal{C}^\cap$  implica imediatamente que existem  $C_1, C_2, C_3 \in \mathcal{C}$  tais que  $C_1 \cap \{a, b\} = \{a\}$ ,  $C_2 \cap \{a, b\} = \{b\}$ , e  $C_3 \supseteq \{a, b\}$ . Como  $\emptyset \in \mathcal{C}$ , concluímos:  $\mathcal{C}$  fragmenta  $\{a, b\}$ , o que é impossível.  $\square$

**Teorema 8.1.16.** *Cada classe  $\mathcal{C}$  de dimensão  $VC\text{-dim}(\mathcal{C}) = 1$  admite um esquema de compressão amostral de tamanho 1.*

*Demonstração.* Segundo lema 8.1.14, podemos supor sem perda de generalidade que  $\emptyset \in \mathcal{C}$ ; se não for o caso, substituiremos a classe  $\mathcal{C} \Delta D$  para  $D \in \mathcal{C}$  qualquer. Segundo lema 8.1.15, a classe maior  $\mathcal{C}^\cap \supseteq \mathcal{C}$  tem dimensão VC um e é fechado pelas interseções.

A esquema de descompressão  $\mathcal{H}$  vai associar a cada ponto  $x$  a interseção de todos os conceitos que contém  $x$ :

$$\mathcal{H}_x = \cap \{C : C \in \mathcal{C}^\cap\}.$$

Seja  $C \in \mathcal{C}^\cap$  qualquer. A relação entre elementos de  $C$ ,

$$\begin{aligned} x < y &\iff \mathcal{H}_x \subseteq \mathcal{H}_y \\ &\iff x \in \mathcal{H}_y \end{aligned}$$

é uma pré-ordem. Seja  $\sigma$  uma amostra finita qualquer. Escolhamos um elemento maximal,  $x \in C \cap \sigma$ , com relação à preordem  $<$ . Supondo que  $C_x \cap \sigma \neq C \cap \sigma$ , existe  $y \in C \cap \sigma$  que é incomparável com  $x$ . Mas neste caso o conjunto  $\{x, y\}$  é fragmentado por  $\mathcal{C}^\cap$ :

$$\{x, y\} \subseteq C, \quad C_x \cap \{x, y\} = \{x\}, \quad C_y \cap \{x, y\} = \{y\}, \quad \emptyset \cap \{x, y\} = \emptyset,$$

uma contradição.  $\square$



*Observação 8.1.17.* Parece que o resultado deve ser creditado a [Floyd e Warmuth 1995], veja p. 295. Ele foi redescoberto algumas vezes, inclusive pelo autor e Damjan Kalajdzievski em 2011 (nunca publicado).

*Observação 8.1.18.* Seja  $\mathcal{C}$  uma classe universalmente separável de dimensão de Vapnik–Chervonenkis um. Verifique que a construção acima resulta em um esquema de compressão boreliano. Neste caso, a solução do problema é, então, completamente satisfatória.

### 8.1.3 Teorema de compacidade: redução aos domínios finitos

O resultado seguinte mostra que, se esquecermos da mensurabilidade, o problema de existência dos esquemas de compressão pode ser reduzida ao problema finito. Para uma classe  $\mathcal{C}$  de conceitos de um domínio  $\Omega$  e um sub-domínio  $\Upsilon \subseteq \Omega$ , denotemos por  $\mathcal{C} \upharpoonright \Upsilon$  a classe de todos os conceitos  $C \cap \Upsilon$ ,  $C \in \mathcal{C}$ .

**Teorema 8.1.19** (Teorema de Compacidade [Ben-David e Litman 1998]). *Seja  $\mathcal{C}$  uma classe de conceitos num domínio  $\Omega$  e  $d \in \mathbb{N}$ . Suponha que para cada sub-domínio finito  $F \subseteq \Omega$ , a classe  $\mathcal{C} \upharpoonright F$  admite um esquema de compressão amostral de tamanho  $d$  no domínio  $F$ . Então,  $\mathcal{C}$  admite um esquema de compressão amostral de tamanho  $d$ .*

*Demonstração.* Para cada  $F \subseteq \Omega$  finito, escolhamos uma aplicação de descompressão de tamanho  $d$  para domínio  $F$ ,

$$\mathcal{H}_F: [F]^{\leq d} \times F \rightarrow \{0, 1\}.$$

Suponhamos que  $\Omega$  é infinito (caso contrário, há nada a mostrar). Neste caso, a família de todos os intervalos superiores semi-infinitos,

$$I_F = \{G \in [\Omega]^{<\infty} : F \subseteq G\},$$

é facilmente verificada para ser centrada. Segundo proposição B.3.23, existe um ultrafiltro (família centrada maximal),  $\mathcal{U}$ , sobre o conjunto  $[\Omega]^{<\infty}$  que contém todos os intervalos  $I_F$ ,  $F \in [\Omega]^{<\infty}$ .

Agora sejam  $\sigma \in [\Omega]^d$  uma amostra finita qualquer com  $\leq d$  elementos em  $\Omega$ , e  $x \in \Omega$ . O conjunto  $[\Omega]^{<\infty}$  admite uma partição em três subconjuntos:

$$\begin{aligned} A_1 &= \{F \in [\Omega]^{<\infty} : \mathcal{H}_F(\sigma \cap F)(x) = 1\}, \\ A_0 &= \{F \in [\Omega]^{<\infty} : \mathcal{H}_F(\sigma \cap F)(x) = 0\}, \\ A_? &= \{F \in [\Omega]^{<\infty} : x \notin F\}. \end{aligned}$$

Segundo a escolha do ultrafiltro  $\mathcal{U}$ , ele contém o intervalo  $I_{\{x\}} = \Omega \setminus A_?$ , e segundo teorema B.3.25,  $A_0 \cup A_1 \in \mathcal{U}$ . Corolário B.3.28 implica que exatamente uma das duas possibilidades tem lugar: seja  $A_0 \in \mathcal{U}$ , seja  $A_1 \in \mathcal{U}$ .

Definemos o valor da aplicação de descompressão

$$\mathcal{H}: [\Omega]^{\leq d} \times \Omega \rightarrow \{0, 1\}$$

assim:

$$\mathcal{H}(\sigma)(x) = \begin{cases} 1, & \text{se } \{F \in [\Omega]^{< \infty} : \mathcal{H}_F(\sigma \cap F)(x) = 1\} \in \mathcal{U}, \\ 0, & \text{se } \{F \in [\Omega]^{< \infty} : \mathcal{H}_F(\sigma \cap F)(x) = 1\} \in \mathcal{U}. \end{cases}$$

Resta mostrar que todo  $C \in \mathcal{C}$  verifica eq. (8.2). Seja  $\sigma \in [\Omega]^{< \infty}$  qualquer, e  $x \in \sigma$ . Para todo  $F \in I_\sigma$ , a hipótese implica que pode escolher  $\tau_F \subseteq \sigma$ ,  $\#\tau_F \leq d$ , tal que

$$\mathcal{H}_F(\tau_F)(x) = \chi_C(x).$$

Dado  $\tau \in [\sigma]^{\leq d}$ , definemos a família

$$X_\tau = \{F \in I_\sigma : \tau_F = \tau\}.$$

Os conjuntos  $X_\tau$ ,  $\tau \in [\sigma]^{\leq d}$ , junto com o conjunto  $\Omega \setminus I_\sigma$ , formam uma cobertura finita de  $[\Omega]^{< \infty}$ , e o mesmo argumento que acima permite concluir que existe o único  $\tau$  tal que  $X_\tau \in \mathcal{U}$ . Segue-se da nossa definição de  $\mathcal{H}$  que

$$\mathcal{H}(\tau)(x) = \chi_C.$$

□

*Observação 8.1.20.* Seja  $\mathcal{C}$  uma classe universalmente separável, e suponha que para cada sub-domínio finito  $F \subseteq \Omega$ , a classe  $\mathcal{C} \upharpoonright F$  admite um esquema de compressão amostral de tamanho  $d$  em  $F$ . Segue-se que  $\mathcal{C}$  admite um esquema de compressão *boreliana* de tamanho  $d$ ? A resposta é positiva para classes *d-máximas* [Kalajdziewski 2012].

## 8.2 Classes extremais

A existência de esquemas de compressão de tamanho  $d$  foi estabelecida em [Kuzmin e Warmuth 2007] para classes de conceitos ditas *d-máximas*. Uma classe  $\mathcal{C}$  é *d-máxima* se para cada amostra  $\sigma \in [\Omega]^{< \infty}$  a cota no lema de Sauer–Shelah está atingida:

$$\#\mathcal{C} \upharpoonright \sigma = \sum_{j=0}^d \binom{n}{j}.$$

Em particular,  $\mathcal{C}$  tem dimensão de Vapnik–Chervonenkis  $d$ .

Como a prova é um pouco técnica, vamos apresentar ao invés disso um resultado bem mais transparente: cada classe *d-máxima* admite um esquema de compressão *rotulado* de tamanho  $d$ . Um esquema de compressão rotulado tem, como o domínio da aplicação de

descompressão  $\mathcal{H}$  (e o co-domínio da aplicação de compressão  $\kappa$ ) o conjunto de todas as amostras rotuladas de tamanho  $\leq d$ . Deste modo, a compressão torna-se mais fácil.

O resultado para esquemas rotulados, mostrado originalmente em [Floyd e Warmuth 1995], foi recentemente generalizado por [Moran e Warmuth 2016] para classes de conceitos mais gerais, chamadas *classes extremais*. Neste contexto de geometria combinatória, a prova torna-se muito elegante, e forma o assunto desta seção.

### 8.2.1 Classes máximas

**Definição 8.2.1.** Seja  $\mathcal{C}$  uma classe de conceitos de dimensão  $VC \leq d$ . Diz-se que a classe  $\mathcal{C}$  é

- *d-maximal* se ela não está contida numa classe estritamente maior de dimensão  $VC$   $d$ , e
- *d-máxima* se para cada amostra  $\sigma \in [\Omega]^{<\infty}$  a cota no lema de Sauer–Shelah está atingida:

$$\#\mathcal{C} \upharpoonright \sigma = \sum_{j=0}^d \binom{n}{j}.$$

Nenhuma propriedade implica a outra.

**Exemplo 8.2.2.** (Emprestado de [Floyd e Warmuth 1995]). Definemos  $\Omega = \{1, 2, 3, 4\}$ , e

$$\mathcal{C} = \{\{1\}, \{2\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}\}.$$

É fácil verificar que a classe  $\mathcal{C}$  é 2-maximal, porém não é 2-máxima, pois  $\#\mathcal{C} = 11$ , enquanto  $\sum_{j=0}^2 \binom{4}{j} = 12$ .

Segue-se que nem cada classe de dimensão  $VC$   $d$  é contida numa classe *d-máxima*.

**Exercício 8.2.3.** Use lema de Zorn (B.3.6) para mostrar que cada classe de dimensão  $VC$   $d$  é contida numa classe *d-maximal*.

**Exemplo 8.2.4.** A classe que consiste de todos os intervalos fechados em  $\mathbb{R}$  é 2-máximo, mas não é 2-maximal.

Portanto, em domínios *finitos* cada classe *d-máxima* é *d-maximal*.

**Exercício 8.2.5.** Seja  $\Omega$  um domínio finito com  $n$  elementos, e seja  $\mathcal{C}$  uma classe de dimensão  $VC$   $d$ . Verifique que  $\mathcal{C}$  é *d-máxima* se e somente se

$$\#\mathcal{C} = \sum_{j=0}^d \binom{n}{j}.$$

[ *Sugestão*: para suficiência, usar indução em  $n$  junto com as propriedades de base dos coeficientes binomiais. ] Em particular, segue-se do lema de Sauer–Shelah que uma classe  $d$ -máxima num domínio finito é  $d$ -maximal.

**Definição 8.2.6.** Seja  $\mathcal{H}: [\Omega]^{\leq d} \rightarrow 2^\Omega$  uma aplicação de descompressão. Diz-se que  $\mathcal{H}$  evite embates se, dado  $\tau_1, \tau_2 \in [\Omega]^{\leq d}$ ,  $\tau_1 \neq \tau_2$ , as hipóteses  $\mathcal{H}(\tau_1)$  e  $\mathcal{H}(\tau_2)$  são distintas já na união  $\tau_1 \cup \tau_2$ :

$$\mathcal{H}(\tau_1) \cap (\tau_1 \cup \tau_2) \neq \mathcal{H}(\tau_2) \cap (\tau_1 \cup \tau_2).$$

A prova do teorema de [Kuzmin e Warmuth 2007] sobre a existência de um esquema de compressão para classes  $d$ -máximas é baseada sobre a seguinte observação-chave.

**Exercício 8.2.7.** Seja  $\mathcal{H}: [\Omega]^{\leq d} \rightarrow \mathcal{C}$  uma aplicação qualquer, onde  $\mathcal{C}$  é uma classe  $d$ -máximo. Se  $\mathcal{H}$  evite embates, mostre que  $\mathcal{C} \subseteq \mathcal{C}_{\mathcal{H}}$ .

No entanto, deixemos o resultado mencionado acima, e provemos um resultado menos tecnicamente desafiador, porém muito instrutivo.

## 8.2.2 Esquemas de compressão rotulados

Relembremos que  $[\Omega]^{\leq d \ 0|1}$  denota o conjunto de todas as amostras rotuladas de tamanho  $\leq d$ , e de mesmo jeito é definido  $[\Omega]^{\leq \infty \ 0|1}$ .

**Definição 8.2.8.** Um esquema de compressão amostral rotulado é um par  $(\mathcal{H}, \kappa)$ , onde

$$\mathcal{H}: [\Omega]^{\leq d \ 0|1} \rightarrow 2^\Omega$$

é a aplicação de descompressão, e

$$\kappa: [\Omega]^{\leq \infty \ 0|1} \rightarrow [\Omega]^{\leq d \ 0|1},$$

a aplicação de compressão, que tem as propriedades:  $\kappa(\sigma, \tau)$  é uma sub-amostra de  $\sigma$  cujo rotudo é induzido por  $\tau$ , e

$$\forall C \in \mathcal{C}, \forall \sigma \in [\Omega]^\infty, \mathcal{H}(\kappa(\sigma, C \cap \sigma)) \cap \sigma = C \cap \sigma. \quad (8.7)$$

*Observação 8.2.9.* Da maneira equivalente, a partir de uma aplicação  $\mathcal{H}$  como acima, pode-se definir a classe  $\mathcal{C}_{\mathcal{H}}$ , como na eq. (8.2), e depois terminar a definição requiring que  $\kappa(\sigma, \tau)$  seja uma sub-amostra rotulada de  $(\sigma, \tau)$ , e  $\mathcal{C} \subseteq \mathcal{C}_{\mathcal{H}}$ .

*Observação 8.2.10.* Cada esquema de compressão amostral  $(\mathcal{H}, \kappa)$  não rotulada defina um esquema de descompressão amostral rotulada, cuja aplicação de descompressão é a composição de  $\mathcal{C}$  com a aplicação esquecendo a rotulagem:

$$[\Omega]^{\leq \infty \ 0|1} \ni (\sigma, \tau) \mapsto \sigma \in [\Omega]^{< \infty}.$$

A aplicação de compressão simplesmente adiciona o rótulo induzido de  $\sigma$ :

$$[\Omega]^{\leq \infty \ 0|1} \ni (\sigma, \tau) \mapsto (\kappa(\sigma, \tau), \tau \cap \kappa(\sigma, \tau)).$$

*Observação 8.2.11.* Agora os resultados sobre os esquemas não rotulados se generalizam para esquemas rotulados. Alguns deles (como teorema 8.1.16) valem trivialmente. O leitor pode ser interessado de mostrar os resultados análogos ao exercício 8.1.3, teorema 8.1.9, e Teorema de Compacidade 8.1.19.

*Observação 8.2.12.* O exemplo motivador de um esquema de compressão rotulada é o famoso classificador de Máquina de Vetores de Suporte (Support Vector Machine, SVM). Deste ponto de vista, ele está discutido em [von Luxburg, Bousquet e Schölkopf 2003/04].

### 8.2.3 Cubos de conceitos

Teorema de Compacidade 8.1.19 permite apenas trabalhar com domínios finitos, e isto vai ser a nossa hipótese até o final da seção.

**Definição 8.2.13.** Seja  $\mathcal{C}$  uma classe de conceitos num domínio  $\Omega$ . Um *cubo* em  $\mathcal{C}$  com o conjunto de coordenadas  $D \subseteq \Omega$  é uma classe  $\mathcal{B} \subseteq \mathcal{C}$  tal que:

1.  $\mathcal{B}$  fragmenta  $D$ , e
2.  $\mathcal{B}|_{\Omega \setminus D}$  consiste de único conceito, que vamos denotar  $\text{tag}(\mathcal{B})$ .

Em outras palavras, se pensamos do cubo  $\mathcal{B}$  como um subconjunto do cubo de Hamming  $\{0, 1\}^{\Omega}$ , ele pode ser escrito assim:

$$\mathcal{B} = \{0, 1\}^D \times \{\chi_{\text{tag}(\mathcal{B})}\}.$$

As restrições dos elementos do cubo sobre  $D$  podem tomar quaisquer valores, mas sobre  $\Omega \setminus D$ , é sempre apenas uma função binária fixa. Deste modo,  $\mathcal{B}$  pode ser identificado com o cubo de Hamming,  $\{0, 1\}^D$ : a aplicação

$$\mathcal{B} \ni C \mapsto [D \ni x \mapsto \chi_C(x)] \in \{0, 1\}^D$$

é bijetora.

**Definição 8.2.14.** Um conjunto  $D \subseteq \Omega$  é *fortemente fragmentado* por uma classe  $\mathcal{C}$  se existe um cubo  $\mathcal{B} \subseteq \mathcal{C}$  tendo  $D$  como conjunto de coordenadas.

Obviamente, um conjunto fortemente fragmentado é fragmentado por  $\mathcal{C}$ .

**Exercício 8.2.15.** Construir um exemplo simples (com o domínio  $\Omega$  de dois pontos) de um conjunto fragmentado mas não fortemente fragmentado por uma classe.

**Teorema 8.2.16.** *Seja  $\mathcal{C}$  uma classe de conceitos num domínio finito,  $\Omega$ . Denotemos por  $\text{sh}(\mathcal{C})$  a família de subconjuntos de  $\Omega$  fragmentados por  $\mathcal{C}$ , e  $\text{ssh}(\mathcal{C})$  a família de subconjuntos fortemente fragmentados por  $\mathcal{C}$ . Então,*

$$\#\text{ssh}(\mathcal{C}) \leq \#\mathcal{C} \leq \#\text{sh}(\mathcal{C}).$$

A segunda desigualdade é o teorema de Pajor 2.2.3. Cada das desigualdades pode ser de fato deduzida da outra (aplicada à classe complementar).

**Exercício 8.2.17.** Mostre que para um conjunto  $A \subseteq \Omega$  uma e uma só condição é verdadeira:

- $\mathcal{C}$  fragmenta  $A$ ,
- $2^\Omega \setminus \mathcal{C}$  fortemente fragmenta  $\Omega \setminus A$ .

**Exercício 8.2.18.** Deduza do exercício 8.2.17 o seguinte: a primeira desigualdade (chamada em [Bollobás e Radcliffe 1995] a desigualdade de Sauer reversa) vale para uma classe  $\mathcal{C}$  se e somente se a segunda desigualdade vale para a classe complementar  $2^\Omega \setminus \mathcal{C}$ . De mesmo, para igualdades.

Isto termina a prova do teorema 8.2.16.

**Definição 8.2.19.** Uma classe  $\mathcal{C}$  é dita *extremal* se todo subconjunto fragmentado por  $\mathcal{C}$  é fortemente fragmentado, ou seja, se as duas desigualdades no teorema 8.2.16 são igualdades.

Mostremos que toda classe  $d$ -máximo é extremal. Com este propósito, verifiquemos que as duas igualdades são de fato equivalentes já quando aplicadas à mesma classe (e não apenas à complementar). Vamos usar a técnica da prova original [Sauer 1972] do lema de Sauer–Shelah 2.2.1, um pouco mais complicada do que a prova do teorema de Pajor 2.2.3.

## 8.2.4 Compressão para baixo

Para cada família  $\mathcal{C}$  de subconjuntos de  $\sigma$  e cada  $x \in \sigma$ , definemos a família  $T_x(\mathcal{C})$  como segue. O operador  $T_x$  remove o ponto  $x$  de todo conjunto  $A \in \mathcal{C}$ , exceto quando  $A \setminus \{x\}$  já pertence a  $\mathcal{C}$ . Neste caso,  $T_x$  devolve  $A$ . Formalmente,

$$T_x(\mathcal{C}) = \{A \setminus \{x\} : A \in \mathcal{H}\} \cup \{A : A \in \mathcal{C} \text{ e } A \setminus \{x\} \in \mathcal{C}\}. \quad (8.8)$$

**Lema 8.2.20.** O operador  $T_x$  é injetor sobre  $\mathcal{C}$ .

*Demonstração.* As imagens de  $A$  e de  $B$  são iguais apenas se um deles é obtido do outro deletando  $x$ , por exemplo,  $B = A \setminus \{x\}$ . Porém, neste caso  $T_x(A) = A$  e  $T_x(B) = B$ .  $\square$

Definamos o *peso* da família  $\mathcal{C}$  como a soma de cardinalidades de todos os conjuntos:

$$w(\mathcal{C}) = \sum_{C \in \mathcal{C}} \#C.$$

O seguinte é óbvio.

**Lema 8.2.21.**

$$w(\mathcal{C}) \leq w(T_x(\mathcal{C})). \quad (8.9)$$

Só há igualdade no caso  $T_x(\mathcal{C}) = \mathcal{C}$ .

**Lema 8.2.22.**  $sh(T_x(\mathcal{C})) \subseteq sh(\mathcal{C})$ . Em particular,  $VC\text{-dim}(T_x(\mathcal{C})) \leq VC\text{-dim}(\mathcal{C})$ .

*Demonstração.* Suponha  $A \subseteq \sigma$  é fragmentado por  $T_x(\mathcal{C})$ . Mostremos que  $A$  é fragmentado por  $\mathcal{C}$ . Seja  $B \subseteq A$ . Procureremos  $C \in \mathcal{C}$  tal que  $A \cap C = B$ .

*Caso 1.*  $x \notin A$ .

Existe  $C \in T_x(\mathcal{C}^*)$  com  $A \cap C = B$ , e pela definição de  $T_x(\mathcal{C}^*)$ , ou  $C \cup \{x\} \in \mathcal{C}$  ou  $C \in \mathcal{C}$ . A interseção de qualquer conjunto com  $A$  é igual a  $B$ .

*Caso 2.*  $x \in B$ .

Fixe  $C \in T_x(\mathcal{C}^*)$  com  $A \cap C = B$ . Neste caso,  $x \in C$ , significando que  $C \in \mathcal{C}$ .

*Caso 3.*  $x \in A \setminus B$ .

Como  $B \cup \{x\} \subseteq A$  e  $A$  é fragmentado por  $T_x(\mathcal{C}^*)$ , esta família contém  $C$  tal que  $A \cap C = B \cup \{x\}$ . Este  $C$  contém  $x$ , o que implica que  $C$  e  $C \setminus \{x\}$  pertencem a  $\mathcal{C}$ . Como  $(C \setminus \{x\}) \cap A = B$ , concluímos.  $\square$

O comportamento de conjuntos fortemente fragmentados é dual.

**Lema 8.2.23.**  $ssh(T_x(\mathcal{C})) \supseteq ssh(\mathcal{C})$ .

*Demonstração.* Seja  $A \subseteq \sigma$  um conjunto fortemente fragmentado por  $\mathcal{C}$ . De modo equivalente,  $\sigma \setminus A$  não é fragmentado por  $2^\sigma \setminus \mathcal{C}$  (exercício 8.2.17): existe  $B \subset \sigma$ ,  $B \cap A = \emptyset$ , tal que para qualquer  $C \in \mathcal{C}$ ,  $C \setminus A \neq B$ . Suponha, para obter uma contradição, que  $\sigma \setminus A$  é fragmentado pela classe  $2^\sigma \setminus T_x \mathcal{C}$ . Em particular, existe  $C \in \mathcal{C}$  tal que  $T_x(C) \setminus A = B$ . Cado conceito  $C$  com esta propriedade deve satisfazer as propriedades seguintes:

1.  $x \notin B$ ,
2.  $x \notin A$ ,
3.  $x \in C$ ,
4.  $C \setminus \{x\} \notin \mathcal{C}$ .

Ao mesmo tempo, existe  $C' \in \mathcal{C}$  tal que  $T_x(C') \setminus A = B \cup \{x\}$ . Isso implica que  $C' \setminus \{x\} \in \mathcal{C}$ , e  $C' \setminus \{x\} \setminus A = B$ , a contradição.  $\square$

Agora denotemos por  $T = T_{x_n} T_{x_{n-1}} \dots T_{x_2} T_{x_1}$ , onde  $\sigma = \{x_1, x_2, \dots, x_n\}$ . Apliquemos  $T$  recursivamente à família de conjuntos  $\mathcal{C}$  até tal iteração  $N$  que o peso de  $\mathcal{C}$  se estabilize.

**Lema 8.2.24.** Já uma iteração basta, ou seja, a família  $T(\mathcal{C})$  atinge o peso minimal.

*Demonstração.* Chamemos uma família  $\mathcal{C}$   $x$ -estável para  $x \in \Omega$  se  $T_x(\mathcal{C}) = \mathcal{C}$ . De modo equivalente, como  $\mathcal{C}$  é finita, para todo  $C \in \mathcal{C}$  temos  $T_x(C) = C$ . Por exemplo, cada família da forma  $T_x(\mathcal{C})$  é  $x$ -estável. Mostremos que se  $\mathcal{C}$  é  $x$ -estável, então para cada  $y \in \Omega$  a família  $T_y(\mathcal{C})$  é  $x$ -estável também, o que termina a prova pela indução finita.

Seja  $C \in \mathcal{C}$ . Basta mostrar que a imagem de  $C$  por  $T_y$  tem a propriedade  $T_y(C) \setminus \{x\} \in T_y(\mathcal{C})$ . É verdadeiro de modo trivial se  $x \notin C$ . Suponhamos que  $x \in C$ . A  $x$ -estabilidade de  $\mathcal{C}$  implica  $C \setminus \{x\} \in \mathcal{C}$ . Tem dois casos a estudar.

*Caso 1.*  $T_y(C) = C$ . Isso significa  $C \setminus \{y\} \in \mathcal{C}$ , logo o conjunto  $C \setminus \{y\}$  é fixo pelo operador  $T_x$ . Concluimos:  $C \setminus \{x, y\} \in \mathcal{C}$ , e por conseguinte  $T_y(C \setminus \{x\}) = C \setminus \{x\}$ , como desejado.

*Caso 2.*  $T_y(C) = C \setminus \{y\}$ . Se  $T_y(C \setminus \{x\}) = C \setminus \{x, y\}$ , então  $T_y(C) \setminus \{x\} = C \setminus \{x, y\} \in T_y(\mathcal{C})$  e tudo está bem. Se, ao contrário,  $T_y(C \setminus \{x\}) = C \setminus \{x\}$ , então  $C \setminus \{x, y\} \in \mathcal{C}$ , logo  $C \setminus \{x, y\} \in T_y(\mathcal{C})$ , e chegamos à mesma conclusão.  $\square$

*Observação 8.2.25.* Exemplos simples (com  $\sigma$  tendo apenas três pontos distintos) mostram que a família  $T(\mathcal{C})$  é altamente não única: ela depende da ordem de atuação dos operadores  $T_x$ ,  $x \in \sigma$ . Dado uma permutação  $\tau \in S_n$  de  $[n]$ , escrevemos

$$T_\tau = T_{x_{\tau(n)}} T_{x_{\tau(n-1)}} \cdots T_{x_{\tau(2)}} T_{x_{\tau(1)}}.$$

Como o operador  $T_x$ ,  $x \in \sigma$ , não muda mais a família  $T_\tau(\mathcal{C})$ , concluimos: para cada  $x \in \sigma$  e  $A \in T_\tau(\mathcal{C})$ ,

$$A \setminus \{x\} \in T_\tau(\mathcal{C}).$$

Por conseguinte, se  $C \in T_\tau(\mathcal{C})$  e  $B \subseteq A$ , então  $B \in T_\tau(\mathcal{C})$ . A família  $T_\tau(\mathcal{C})$  é fechada para baixo. Em particular, ela não contém algum conjunto  $A$  de cardinalidade  $d + 1$  ou mais, e deste modo, é contida na bola de Hamming fechada de raio  $d$ . (Isto traz imediatamente a estimativa do lema de Sauer–Shelah).

**Lema 8.2.26.** *Seja  $\mathcal{C}$  uma classe de conceitos no domínio  $\sigma = \{x_1, \dots, x_n\}$ . Sejam  $I = \{x_{i_1}, x_{i_2}, \dots, x_{i_k}\} \subseteq \sigma$ , e  $\sigma \setminus I = \{x_{j_1}, \dots, x_{j_{n-k}}\}$ . Então*

1.  *$I$  é fragmentado por  $\mathcal{C}$  se e somente se  $I \in T_{(i_1, i_2, \dots, i_k, j_1, j_2, \dots, j_{n-k})}(\mathcal{C})$ ,*
2.  *$I$  é fortemente fragmentado por  $\mathcal{C}$  sse  $I \in T_{(j_1, j_2, \dots, j_{n-k}, i_1, i_2, \dots, i_k)}(\mathcal{C})$ .*

*Demonstração.* (1) O conjunto  $I$  sendo fragmentado por  $\mathcal{C}$  significa que para cada  $A \subseteq I$  existe conjunto  $C_A \in \mathcal{C}$  tal que  $C_A \cap I = A$ . A aplicação de operadores  $T_x$  com  $x$  fora de  $I$  não afeta as interseções com  $I$ , e denotando  $T_J = T_{x_{j_1}} \cdots T_{x_{j_{n-k}}}$ , ainda temos  $T_J(C_A) \cap I = A$ . Como a classe  $T_J(\mathcal{C})$  é fechado pelas remoções de pontos  $x \in \sigma \setminus I$ , para cada  $A \subseteq I$ , existe  $C'_A \in \mathcal{C}$  tal que  $T_J(C'_A) = A$ . Em outras palavras, os elementos de  $T_J(\mathcal{C})$  que são subconjuntos de  $I$  formam uma família fechada por baixo, e por conseguinte eles pertencem à classe  $T_{IJ}(\mathcal{C})$  também. Isto estabelece a necessidade



( $\Rightarrow$ ). A suficiência ( $\Leftarrow$ ) segue de fato que  $T_{IJ}(\mathcal{C})$  é fechado por baixo, e a inclusão  $\text{sh}(T_{IJ}(\mathcal{C})) \subseteq \text{sh}(\mathcal{C})$  (lema 8.2.22).

(2) Agora suponha que  $I$  é fortemente fragmentado por  $\mathcal{C}$ . Existe um conjunto  $C \subseteq J = \sigma \setminus I$  tal que, qual quer seja  $A \subseteq I$ , o conjunto  $C \cap A$  pertence a  $\mathcal{C}$ . É claro que os operadores  $T_x$ ,  $x \in I$  não mudam os elementos do cubo  $\{C\} \times 2^I$ . Depois da aplicação de operadores  $T_x$ ,  $x \in J$ , obtemos uma família de conjuntos  $T_{JI}(\mathcal{C})$ , fechada por baixo, que ainda fragmenta  $I$ , logo  $I \in T_{JI}(\mathcal{C})$ . A necessidade é mostrada. Para suficiência, suponha que  $I \in T_{JI}(\mathcal{C})$ . Então,  $T_{JI}(\mathcal{C})$  fragmenta  $I$ , e por isso já  $T_I(\mathcal{C})$  fragmenta  $I$ , logo  $T_I(\mathcal{C}) = \mathcal{C}$ . Em particular, existe  $C' \in \mathcal{C}$  tal que  $I \subseteq C'$ . Definemos  $C = C' \setminus I$ . Como a família  $\mathcal{C}$  é fechada sob operadores  $T_x$ ,  $x \in I$ , concluimos que, qualquer seja  $A \subseteq I$ , o conjunto  $C \cup A$  pertence a  $\mathcal{C}$ .  $\square$

**Teorema 8.2.27 (Bollobás e Radcliffe [1995]).** *Para uma classe de conceitos  $\mathcal{C}$  num domínio finito  $\sigma$ , as condições seguintes são equivalentes.*

1.  $\mathcal{C}$  é extremal, ou seja,  $\sharp\text{ssh}(\mathcal{C}) = \sharp(\mathcal{C}) = \sharp\text{sh}(\mathcal{C})$ .
2.  $\sharp\mathcal{C} = \sharp\text{sh}(\mathcal{C})$ .
3.  $\sharp\text{ssh}(2^\sigma \setminus \mathcal{C}) = \sharp(2^\sigma \setminus \mathcal{C})$ .
4.  $\mathcal{C}$  tem a única compressão para baixo. Em outras palavras, quaisquer sejam permutações  $\tau, \tau' \in S_n$ ,  $T_\tau(\mathcal{C}) = T_{\tau'}(\mathcal{C})$ .
5.  $\sharp\text{ssh}(\mathcal{C}) = \sharp(\mathcal{C})$ .

*Demonstração.* (1)  $\Rightarrow$  (2) é trivial, e a equivalência (2)  $\iff$  (3) já foi estabelecida (exercício 8.2.17).

Assuma (2), ou seja,  $\sharp\mathcal{C} = \sharp\text{sh}(\mathcal{C})$ . Para qualquer permutação  $\tau \in S_n$ ,  $\text{sh}(T_\tau(\mathcal{C})) = T_\tau(\mathcal{C})$  e  $T_\tau$  é injetora. Temos:

$$\sharp\text{sh}(T_\tau(\mathcal{C})) = \sharp T_\tau(\mathcal{C}) = \sharp\mathcal{C} = \sharp\text{sh}(\mathcal{C}).$$

Lema 8.2.22 implica que  $\text{sh}(T_\tau(\mathcal{C})) \subseteq \text{sh}(\mathcal{C})$ , e por conseguinte

$$T_\tau(\mathcal{C}) = \text{sh}(T_\tau(\mathcal{C})) = \text{sh}(\mathcal{C})$$

qualquer seja permutação  $\tau \in S_n$ , estabelecendo (4).

Assumamos a condição (4). Usando o lema 8.2.26, concluimos que um conjunto  $I$  é fragmentado por  $\mathcal{C}$  se e somente se  $I$  é fortemente fragmentado por  $\mathcal{C}$ , o que estabelece (1) e em particular (5). Neste momento, as condições (1)–(4) são dois a dois equivalentes.

Finalmente, assumamos a validade de (5). Usando a implicação já mostrada, (3) $\Rightarrow$ (1), aplicada à classe complementar  $2^\sigma \setminus \mathcal{C}$ , concluimos que esta classe é extremal, ou seja,  $\sharp\text{ssh}(2^\sigma \setminus \mathcal{C}) = \sharp(2^\sigma \setminus \mathcal{C})$ . Exercício 8.2.18 implica condição (2) para  $\mathcal{C}$ .  $\square$

**Corolário 8.2.28.** *Cada classe  $d$ -máxima é extremal.*

*Demonstração.* Para uma classe  $d$ -máxima,  $\#\mathcal{C} = \sum_{j=0}^d \binom{n}{j}$ , o que é exatamente o número de subconjuntos com  $\leq d$  elementos de  $\sigma$ , ou seja, subconjuntos fragmentados. Temos a igualdade  $\#\mathcal{C} = \#\text{sh}(\mathcal{C})$ , e concluímos pelo teorema 8.2.27.  $\square$

**Exemplo 8.2.29.** Nem cada classe extremal de dimensão VC  $d$  é  $d$ -máxima. O exemplo mais simples é o de qualquer bola de Hamming em torno de zero que é estritamente intermediária entre a bola aberta e a bola fechada de raio  $d$ . Outra exemplo é qualquer cubo  $\mathcal{B}$  cujo conjunto de coordenadas é um subconjunto próprio do domínio,  $D \subsetneq \Omega$ .

**Lema 8.2.30.** *Seja  $\mathcal{C}$  uma classe extremal, e seja  $\sigma \subseteq \Omega$ . Então a classe  $\mathcal{C} \upharpoonright \sigma$  é extremal.*

*Demonstração.* Um subconjunto  $A \subseteq \sigma$  fragmentado por  $\mathcal{C} \upharpoonright \sigma$  é fragmentado por  $\mathcal{C}$ , logo fortemente fragmentado por  $\mathcal{C}$ . Existe um cubo  $\{C\} \times \{0, 1\}^A \subseteq \mathcal{C}$ , onco  $C \subseteq \Omega \setminus A$ . Por conseguinte, o cubo  $\{C \cap \sigma\} \times \{0, 1\}^A$  é uma subfamília de  $\mathcal{C} \upharpoonright \sigma$ , ou seja,  $A$  é fortemente fragmentado por  $\mathcal{C} \upharpoonright \sigma$ .  $\square$

**Definição 8.2.31.** Dado uma classe  $\mathcal{C}$  e um subconjunto  $D$  do domínio  $\Omega$ , definemos a *redução* de  $\mathcal{C}$  modulo  $D$  como uma classe no domínio  $\Omega \setminus D$  que consiste de todos os conceitos da forma  $\text{tag}(\mathcal{B})$  onde  $\mathcal{B} \subseteq \mathcal{C}$  é um cubo com conjunto de coordenadas exatamente  $D$ . Notação:  $\mathcal{C} \setminus D$ .

**Lema 8.2.32.** *A redução de uma classe extremal é uma classe extremal.*

*Demonstração.* Seja  $I \subseteq \Omega \setminus D$  um subconjunto fragmentado por  $\mathcal{C} \setminus D$ . Segue-se que  $D \cup I$  é fragmentado por  $\mathcal{C}$ , logo fortemente fragmentado. Concluímos da definição de  $\mathcal{C} \setminus D$  que esta classe fortemente fragmenta  $I$  em  $\Omega \setminus D$ .  $\square$

**Lema 8.2.33.** *Seja  $\mathcal{B}$  um cubo e  $\mathcal{C}$  uma classe extremal, ambos no domínio  $\Omega$ . Então  $\mathcal{B} \cap \mathcal{C}$  é uma classe extremal.*

*Demonstração.* Seja  $D$  o conjunto de coordenadas do cubo  $\mathcal{B}$ . Podemos supor que  $\mathcal{B} \cap \mathcal{C}$  não é vazia. Suponha que  $I \subseteq \Omega$  é fragmentado por  $\mathcal{B} \cap \mathcal{C}$ . Então, em particular,  $I \subseteq D$ . Como  $I$  é fragmentado por  $\mathcal{C}$ , ele é fortemente fragmentado, e segundo lema 8.2.26,  $I$  pertence a  $T_{\Omega \setminus D, D \setminus I, I}(\mathcal{C})$ . É claro que  $T_{D \setminus I, I}(\mathcal{C} \cap \mathcal{B}) \cap D = T_{D \setminus I, I}(\mathcal{C}) \cap D$ , logo este conjunto contém  $I$  (8.2.26, (2)). Como  $\mathcal{C} \cap \mathcal{B} \setminus D$  consiste de único conceito  $\text{tag}(\mathcal{B})$ , e  $T_{\Omega \setminus D, D \setminus I, I}(\mathcal{C} \cap \mathcal{B})$  é fechado por baixo, concluímos que  $I \in T_{\Omega \setminus D, D \setminus I, I}(\mathcal{C} \cap \mathcal{B})$  também.  $\square$

**Definição 8.2.34.** Cada classe de conceitos  $\mathcal{C}$  suporta uma estrutura natural de grafo, nomeadamente, dois conceitos  $C$  e  $C'$  são adjacentes se e somente se eles só diferem em um ponto:  $\#(C \Delta C') = 1$ . Em outras palavras, quando pensamos de  $\mathcal{C}$  como um subconjunto do cubo de Hamming  $\{0, 1\}^\Omega$ , a distância de Hamming (não normalizada) entre  $C$  e  $C'$  é exatamente 1. Este grafo chama-se *grafo de 1-inclusão* (1-inclusion graph).

**Definição 8.2.35.** Um grafo (simples) é dito *conexo* se para cada par  $x, y$  de vértices, existe um *caminho* que junta  $x$  e  $y$ , ou seja, uma sequência finita

$$x = x_0, x_1, x_2, \dots, x_n = y,$$

onde dois pontos consequentes são adjacentes. O mínimo  $n$  com esta propriedade (o comprimento do caminho) é dito a *distância de caminho* entre  $x$  e  $y$ .

**Exercício 8.2.36.** Verifique que a distância de caminho é uma métrica.

Eis um resultado importante sobre a geometria de classes extremais.

**Teorema 8.2.37.** *Seja  $\mathcal{C}$  uma classe extremal. A distância de caminho entre dois conceitos é igual à distância de Hamming. Em particular, a grafo de 1-inclusão de  $\mathcal{C}$  é conexo.*

*Demonstração.* Suponhamos que a afirmação é falsa, e escolhamos dois conceitos,  $C$  e  $C'$ , cuja distância de caminho não é igual a distância de Hamming, e tais que a distância de Hamming é menor entre todos os pares com esta propriedade. Seja  $D$  o conjunto de todos  $x$  onde  $\chi_C(x) \neq \chi_{C'}(x)$ , e seja  $\mathcal{B}$  o menor cubo que contém  $C$  e  $C'$ , ou seja, o cubo dom conjunto de coordenadas  $D$  e  $\text{tag}(\mathcal{B}) = C \setminus D = C' \setminus D$ . Segue-se da nossa hipótese que  $\#D \geq 2$ . No cubo  $\mathcal{B} \cong \{0, 1\}^D$  existe um elemento  $C'' \neq C, C'$  com a propriedade

$$d_{\text{Hamming}}(C, C'') + d_{\text{Hamming}}(C', C'') = d_{\text{Hamming}}(C, C'),$$

e a escolha de  $C, C'$  garante que

$$\begin{aligned} d_{\text{caminho}}(C, C') &\leq d_{\text{caminho}}(C, C'') + d_{\text{caminho}}(C', C'') \\ &= d_{\text{Hamming}}(C, C'') + d_{\text{Hamming}}(C', C'') \\ &= d_{\text{Hamming}}(C, C'), \end{aligned}$$

uma contradição. □

Digamos que um cubo  $\mathcal{B} \subseteq \mathcal{C}$  é *maximal* se ele não está contido num cube estritamente maior dentro de  $\mathcal{C}$ .

**Lema 8.2.38.** *Sejam  $\mathcal{B}_1, \mathcal{B}_2$  dois cubos dentro de uma classe extremal,  $\mathcal{C}$ , tendo os conjuntos de coordenadas  $D_1$  e  $D_2$ . Se  $\mathcal{B}_1$  é maximal e  $D_1 \subseteq D_2$ , então  $\mathcal{B}_1 = \mathcal{B}_2$ .*

*Demonstração.* Suponha que  $D_2 \setminus D_1 \neq \emptyset$  e  $\mathcal{B}_1 \neq \mathcal{B}_2$ . A redução  $\mathcal{B}_1^{\setminus D}$  é um conjunto unitário com o único elemento  $\text{tag } \mathcal{B}_1$ , e a redução  $\mathcal{B}_2^{\setminus D}$  é um cubo com o conjunto de coordenadas  $D_2 \setminus D_1$ , que não contém  $\text{tag } \mathcal{B}_1$  por causa da maximalidade de  $\mathcal{B}_1$ . Como o grafo de 1-inclusão de  $\mathcal{C}^{\setminus D}$  é conexo (lema 8.2.32 e teorema 8.2.37), existe um caminho que junta  $\text{tag } \mathcal{B}_1$  com algum elemento do cubo  $\mathcal{B}_2^{\setminus D}$ . O elemento do caminho adjacente a  $\text{tag } \mathcal{B}_1$  difere de  $\text{tag } \mathcal{B}_1$  em um ponto  $x \in \Omega \setminus D$ , e está da forma  $\text{tag } \mathcal{B}_3$ , onde  $\mathcal{B}_3$  tem  $D$  como o conjunto de coordenadas. Segue-se das definições que  $\mathcal{B}_1 \cup \mathcal{B}_3$  é um cubo com conjunto de coordenadas  $D \cup \{x\}$ , contradizendo a maximalidade de  $\mathcal{B}_1$ . □

Agora podemos mostrar o resultado central da seção.

**Teorema 8.2.39** (Moran e Warmuth [2016]). *Cada classe extremal de dimensão de Vapnik–Chervonenkis  $d$  admite um esquema de compressão amostral rotulado de tamanho  $d$ .*

*Demonstração.* Teorema de Compacidade 8.1.19 reduz o teorema ao caso de domínios finitos. O esquema de compressão tem a descrição seguinte.

1. A descompressão  $\mathcal{H}(\tau, \gamma)$  de uma amostra rotulada  $(\tau, \gamma)$  é qualquer conceito  $C$  consistente com a rotulagem (isto é,  $C \cap \tau = \gamma$ ) que pertence a um cubo  $\mathcal{B} \subseteq \mathcal{C}$  com o conjunto de coordenadas  $\tau$ .
2. A compressão  $\kappa(\sigma, \tau)$  de uma amostra rotulada  $(\sigma, \tau)$  é da forma  $(\delta, \tau \cap \delta)$ , onde  $\delta$  é o conjunto de coordenadas de um cubo maximal em  $\mathcal{C} \cap \sigma$ , que contém  $\tau$ .

Se a amostra  $(\delta, \alpha)$  pertence à imagem da aplicação de compressão,  $\kappa$ , então  $\delta$  é fortemente fragmentada pela classe  $\mathcal{C} \upharpoonright \sigma$ , logo fragmentado por  $\mathcal{C}$ , logo fortemente fragmentado por  $\mathcal{C}$ . Existe um cubo  $\mathcal{B}$  em  $\mathcal{C}$  com o conjunto de coordenadas  $\delta$ , em particular existe um conceito  $C \in \mathcal{B}$  que induz sobre  $\delta$  a rotulagem  $\alpha$ . Então, a hipótese  $\mathcal{H}(\tau, \gamma)$  para tais amostras é bem definida.

Resta só verificar a condição na eq. (8.7). Seja  $(\sigma, C \cap \sigma)$  uma amostra rotulada por um elemento da classe  $\mathcal{C}$ , seja  $\mathcal{B}$  um cubo maximal da classe  $\mathcal{C} \upharpoonright \sigma$  que contém  $C \cap \sigma$ , com o conjunto de coordenadas  $\delta$ . Seja  $\mathcal{B}'$  um cubo da classe  $\mathcal{C}$  com coordenadas  $\delta$ , e seja  $C' \in \mathcal{B}'$  um conceito que induz sobre  $\delta$  a rotulagem  $C \cap \sigma = C \cap \delta$ . Basta verificar que  $C'$  é consistente com  $C$  também sobre o resto de  $\sigma$ , ou seja, que  $C' \cap (\sigma \setminus \delta) = C \cap (\sigma \setminus \delta)$ .

O cubo  $\mathcal{B}' \upharpoonright \sigma$  tem  $\delta$  como coordenadas, e como o cubo  $\mathcal{B}$  é maximal, lema 8.2.38 implica que  $\mathcal{B} = \mathcal{B}' \upharpoonright \sigma$ . Como  $\delta$  é o conjunto de coordenadas de  $\mathcal{B}$ , a restrição  $\mathcal{B} \upharpoonright \sigma \setminus \delta$  consiste apenas de um conceito,  $\text{tag}(\mathcal{B})$ . O mesmo vale para a restrição  $\mathcal{B}' \upharpoonright \sigma \setminus \delta$ , e o resultado segue.  $\square$

## 8.3 Teorema de Moran–Yehudayoff

O mais forte resultado geral concernendo a existência dos esquemas de compressão até o momento é um avanço notável recente por [Moran e Yehudayoff 2016], que mostram que cada classe de conceitos  $\mathcal{C}$  de dimensão  $\text{VC-dim}(\mathcal{C}) = d$  admite um esquema de compressão de tamanho exponencial em  $d$ . Aqui a noção de um esquema é relaxado ainda mais: não somente o esquema é rotulado, mas além disso o argumento do esquema permite um número exponencial em  $d$  de bits de “informação adicional”. O tamanho do esquema no teorema de Moran–Yehudayoff não depende apenas da dimensão de Vapnik–Chervonenkis, mas também da dimensão de Vapnik–Chervonenkis *dual*, que, por seu turno, admite uma cota exponencial em  $d$ .

### 8.3.1 Dimensão de Vapnik–Chervonenkis dual

Seja  $(\Omega, \mathcal{C})$  uma classe de conceitos, isto é,  $\Omega$  é um conjunto e  $\mathcal{C}$  é uma família de subconjuntos de  $\Omega$ . A *classe de conceitos dual* a  $(\Omega, \mathcal{C})$  tem  $\mathcal{C}$  como o domínio e  $\Omega$  como a classe de conceitos, onde cada  $x \in \Omega$  determina uma função binária,  $\hat{x}$ , sobre  $\mathcal{C}$  como segue:

$$\hat{x}(C) = \begin{cases} 1, & \text{se } x \in C, \\ 0, & \text{senão.} \end{cases}$$

A dimensão VC da classe dual é chamada *dimensão VC dual* de  $\mathcal{C}$ . Notemos:

$$\text{VC-dim}^*(\mathcal{C}) = \text{VC-dim}(\mathcal{C}, \Omega).$$

**Teorema 8.3.1.** *Suponha que  $\text{VC-dim}((\Omega, \mathcal{C}) = d$  seja finita. Então, a dimensão VC dual de  $\mathcal{C}$  é estritamente limitada por  $2^{d+1} - 1$ ,*

$$\text{VC-dim}^*(\mathcal{C}) < 2^{d+1},$$

*é a desigualdade é exata.*

*Demonstração.* Suponha que  $\text{VC-dim}(\Omega, \mathcal{C}) \geq 2^{d+1}$ . Então existe uma subfamília finita  $\mathcal{A} \subseteq \mathcal{C}$  de cardinalidade  $|\mathcal{A}| = 2^{d+1}$  fragmentada por  $\Omega$ . O que significa: para todo  $\mathcal{B} \subseteq \mathcal{A}$  existe  $x = x_{\mathcal{B}} \in \Omega$  que pertence aos todos  $B \in \mathcal{B}$  e não pertence a nenhum  $A \in \mathcal{A} \setminus \mathcal{B}$ .

Vamos agora selecionar um subconjunto de  $\Omega$  com  $d + 1$  elementos fragmentado por  $\mathcal{A}$ , acabando o argumento por contraposição. Indexamos os elementos de  $\mathcal{A}$  com elementos do cubo de Hamming  $\{0, 1\}^{d+1}$ . Para cada  $i = 1, 2, \dots, d + 1$ , escolhemos um ponto  $x_i \in \Omega$  que pertence a um conjunto  $A_\sigma$  indexado com a palavra  $\sigma = \sigma_1 \sigma_2 \dots \sigma_{d+1}$  se e somente se  $\sigma_i = 1$ . Isso é possível porque  $\mathcal{A}$  é fragmentado por  $\Omega$ .

Se agora  $I$  é um subconjunto de  $\{1, 2, \dots, d + 1\}$ , seja  $\sigma$  um elemento do cubo de Hamming que tem 1 nas todas as posições que pertencem a  $I$ , e 0 em outras partes. O conjunto correspondente  $A_\sigma$  contém  $x_i$  se e somente se  $i \in I$ .

Resta mostrar que o valor  $2^{d+1} - 1$  pode ser atingido. Seja  $\Omega = \{0, 1\}^k$ , e seja  $\mathcal{C}$  uma classe que consiste de todos os subconjuntos cilíndricos do cubo de Hamming da forma

$$\pi_i^{-1}(1), \quad i = 1, 2, \dots, k.$$

Em outras palavras,

$$\mathcal{C} = \{C_i : i = 1, 2, \dots, k\},$$

onde  $C_i$  consiste de todas as palavras cuja  $i$ -ésima coordenada é um.

É claro que  $\mathcal{C}$  é fragmentado por  $\Omega$ , logo a dimensão VC dual desta classe é exatamente  $k$ . No mesmo tempo, a dimensão VC de  $\mathcal{C}$  é menor ou igual a  $\lfloor \log k \rfloor$ , pelas considerações da cardinalidade.

Defina  $k = 2^{d+1} - 1$ . A construção acima resulta em uma classe de dimensão VC dual  $2^{d+1} - 1$  e de dimensão VC  $\leq d$ . A dimensão VC de  $\mathcal{C}$  não pode ser estritamente menor que  $d$  por causa da desigualdade já estabelecida. Portanto,  $\text{VC-dim}(\mathcal{C}) = d$ .  $\square$

**Corolário 8.3.2.** *Se  $d = \text{VC-dim}(\mathcal{C})$  e  $d^* = \text{VC-dim}^*(\mathcal{C})$ ,*

$$\log_2 d - 1 < d^* < 2^{d+1}.$$

*Em particular,  $d^* = O(\exp d) \cap \Omega(\log d)$ .*  $\square$

### 8.3.2 Complexidade amostral de classes de Glivenko–Cantelli

Dado uma classe de Glivenko–Cantelli de dimensão VC  $d$ , precisamos obter algumas estimativas para a complexidade amostral de  $\mathcal{C}$ , ou seja, um valor de  $n$  garantindo que o erro uniforme da estimativa empírica de medidas de todos os elementos de  $\mathcal{C}$  seja menor que  $\varepsilon > 0$  com confiança  $1 - \delta$ . A complexidade amostral é de ordem  $O(d/\varepsilon^2)$ , e para deduzir-a, vamos usar o resultado técnico importante.

#### Lema de separação de Dudley

**Lema 8.3.3** (Lema de Separação (Dudley)). *Seja  $K$  um subconjunto  $\varepsilon$ -separado do cubo de Hamming  $\Sigma^n$  (com a distância normalizada). Suponha*

$$\text{VC-dim}(K) \leq d.$$

*Então,*

$$|K| \leq \left( 2e^2 \log \left( \frac{2e}{\varepsilon} \right) \right)^d \left( \frac{1}{\varepsilon} \right)^d. \quad (8.10)$$

*Observação 8.3.4.* Note que a cota sobre o tamanho de  $K$  não depende da dimensão  $n$  do cubo de Hamming em questão.

**Lema 8.3.5.** *Seja  $K$  um subconjunto  $\varepsilon$ -separado de  $\Sigma^n$ . Então existe um subconjunto de coordenadas*

$$I \subseteq \{1, 2, \dots, n\}$$

*com*

$$|I| \leq \frac{2 \log |K|}{\varepsilon}, \quad (8.11)$$

*tendo a propriedade que cada duas palavras distintas  $\eta, \tau \in K$  diferem entre elas sobre pelo menos uma coordenada de  $I$ . Em outras palavras, a aplicação de restrição*

$$K \ni \sigma \mapsto \sigma \upharpoonright I \in \{0, 1\}^I$$

*é injetora.*

*Demonstração.* Se  $|K| \leq 2$ , a afirmação é óbvia, e por isto assumamos que  $|K| \geq 3$ , e por conseguinte

$$\log|K| \geq 1. \quad (8.12)$$

Formemos o subconjunto  $V \subseteq \{-1, 0, 1\}^n$  por

$$V = \{\eta - \tau : \eta, \tau \in K, \eta \neq \tau\}.$$

(Aqui a subtração é feita em  $\mathbb{R}^n$ , nem modulo 2.)

Claro,  $|V| \leq |K|^2$ . Como para cada  $\eta \neq \tau$  temos  $\bar{d}(\eta, \tau) \geq \epsilon$ , cada  $v \in V$  difere de zero sobre pelo menos  $n\epsilon$  coordenadas.

Sejam  $X_i, i = 1, 2, \dots, t$  variáveis aleatórias i.i.d. tomando valores em  $[n] = \{1, 2, \dots, n\}$  e distribuídas uniformemente: para todos  $i = 1, 2, \dots, t$  e  $j = 1, 2, \dots, n$ ,

$$\Pr\{X_i = j\} = \frac{1}{n}.$$

Para todo  $v \in V$ , a probabilidade do que uma coordenada aleatória não é nula é pelo menos  $\epsilon$ , logo

$$\Pr\{\forall i = 1, 2, \dots, t, v(X_i) = 0\} = \prod_{i=1}^t \Pr\{v(X_i) = 0\} < (1 - \epsilon)^t.$$

Segundo a cota de união,

$$\begin{aligned} \Pr\{\exists v \in V, \forall i = 1, 2, \dots, t, v(X_i) = 0\} &\leq \sum_{v \in V} \Pr\{\forall i = 1, 2, \dots, t, v(X_i) = 0\} \\ &\leq |K|^2 (1 - \epsilon)^t. \end{aligned}$$

Por conseguinte, para o evento complementar,

$$\Pr\{\forall v \in V, \exists i = 1, 2, \dots, t, v(X_i) \neq 0\} \geq 1 - |K|^2 (1 - \epsilon)^t.$$

Desde que

$$1 - |K|^2 (1 - \epsilon)^t > 0, \quad (8.13)$$

existe um subconjunto  $I \subseteq [n]$  com  $t$  elementos e a propriedade desejada. A eq. (8.13) é equivalente a

$$(1 - \epsilon)^t < \frac{1}{|K|^2},$$

ou seja, o tamanho de  $I$  que garante a conclusão do lema, é

$$t > -\frac{2 \log|K|}{\log(1 - \epsilon)}. \quad (8.14)$$

Para todos  $\epsilon$  estritamente entre 0 e  $t$  temos, usando a série de Taylor,

$$-\log(1 - \epsilon) = \epsilon + \frac{\epsilon^2}{2} + \frac{\epsilon^3}{3} + \dots + \frac{\epsilon^n}{n} + \dots \quad (8.15)$$

Em particular,

$$-\log(1 - \epsilon) > \epsilon$$

logo

$$-\frac{2 \log |K|}{\log(1 - \epsilon)} < \frac{2 \log |K|}{\epsilon}.$$

Tomando em consideração (8.15) e (8.12),

$$\begin{aligned} \frac{2 \log |K|}{\epsilon} - \left( -\frac{2 \log |K|}{\log(1 - \epsilon)} \right) &= 2 \log |K| \frac{\log(1 - \epsilon) + \epsilon}{\epsilon \log(1 - \epsilon)} \\ &= 2 \log |K| \frac{\frac{1}{2} + \frac{\epsilon}{3} + \dots + \frac{\epsilon^{n-2}}{n} + \dots}{1 + \frac{\epsilon}{2} + \frac{\epsilon^2}{3} + \dots + \frac{\epsilon^{n-1}}{n} + \dots} \\ &\geq \frac{1 + \frac{2\epsilon}{3} + \dots + \frac{2\epsilon^{n-2}}{n} + \dots}{1 + \frac{\epsilon}{2} + \frac{\epsilon^2}{3} + \dots + \frac{\epsilon^{n-2}}{n-1} + \dots} \\ &> 1. \end{aligned}$$

Por conseguinte, existe pelo menos um número inteiro  $t$  estritamente entre os dois números:

$$-\frac{2 \log |K|}{\log(1 - \epsilon)} < t < \frac{2 \log |K|}{\epsilon}.$$

Este  $t$  satisfaz (8.14), bem como (8.11), e nós concluímos.  $\square$

**Exercício 8.3.6.** Mostre que

$$e^x > x^e$$

para todos  $x > e$ .

**Lema 8.3.7.** Suponhamos que  $\beta > e^2$  e  $\alpha \geq 1$ .

(1) Se  $\alpha \geq e\beta \log \beta$ , então  $\alpha > \beta \log \alpha$ . De modo equivalente,

(2) se  $\alpha \leq \beta \log \alpha$ , então  $\alpha < e\beta \log \beta$ .

*Demonstração.* Estabeleçamos a primeira parte do lema, de onde a segunda parte segue pela contraposição. Defina a função  $\phi(\alpha) = \alpha - \beta \log \alpha$ , e seja  $\alpha_0 = e\beta \log \beta$ . Como  $\beta > e^2$ , temos  $\alpha_0 > e\beta$ . Além disso,

$$\begin{aligned} \phi(\alpha_0) &= e\beta \log \beta - \beta(1 + \log \beta + \log \log \beta) \\ &> \beta(\log \beta - 1 - \log \log \beta) \\ &> 0, \end{aligned}$$



sob a condição que

$$\log \beta > 1 + \log \log \beta,$$

isto é,

$$\beta > e \log \beta,$$

ou

$$e^\beta > \beta^e,$$

depois de exponenciar duas vezes. A última desigualdade é válida se  $\beta > e^2$  (exercício 8.3.6), de onde concluímos:  $\phi(\alpha_0) > 0$  quando  $\beta > e^2$ . Como  $\phi'(\alpha) = 1 - \beta/\alpha > 0$  para  $\alpha > \alpha_0$ , temos  $\phi(\alpha) > 0$  para todos  $\alpha > \alpha_0$ .  $\square$

*Prova do Lema de Separação 8.3.3.* Escolhamos um subconjunto  $I$  como no lema 8.3.5. Obviamente,

$$\text{VC-dim}(K \upharpoonright I) \leq d,$$

e pelo lema de Sauer–Shelah,

$$\begin{aligned} |K| &= |K \upharpoonright I| \\ &\leq \left(\frac{e|I|}{d}\right)^d \\ &\leq \left(\frac{e2 \log |K|}{\epsilon d}\right)^d, \end{aligned}$$

ou seja,

$$|K|^{1/d} \leq \frac{2e \log |K|}{\epsilon d} = \frac{2e}{\epsilon} \log(|K|^{1/d}).$$

Aplicando lema 8.3.7, parte (2), com valores

$$\alpha = |K|^{1/d} \text{ (o que é } \geq 1)$$

e

$$\beta = \frac{2e}{\epsilon} \text{ (o que é } > e^2 \text{ se } \epsilon < 2/e),$$

concluímos

$$|K|^{1/d} < e \frac{2e}{\epsilon} \log \left(\frac{2e}{\epsilon}\right) = \frac{2e^2}{\epsilon} \log \left(\frac{2e}{\epsilon}\right),$$

or, de modo equivalente,

$$|K| < \left(2e^2 \log \left(\frac{2e}{\epsilon}\right)\right)^d \left(\frac{1}{\epsilon}\right)^d,$$

como desejado. Só basta notar que se  $\epsilon \geq 2/e$ , então  $K$  contém ao máximo dois pontos, e a conclusão é verdadeira também.  $\square$

Relembramos que  $\mu_n$  é a medida empírica suportada pela amostra aleatória  $X_1, X_2, \dots, X_n$  (então,  $\mu_n$  é uma medida aleatória). A distância  $L^1(\mu_n)$  entre duas funções reais  $f$  e  $g$  é dada por

$$\|f - g\|_{L^1(\mu_n)} = \frac{1}{n} \sum_{i=1}^n |f(X_i) - g(X_i)|,$$

é ela é uma distância aleatória. Esta distância não é, geralmente, uma métrica, mas uma pseudométrica.

**Exercício 8.3.8.** O que é  $\mathbb{E}_\mu \|f - g\|_{L^1(\mu_n)}$ ?

Seja  $\sigma = \{x_1, x_2, \dots, x_n\}$  uma instância de amostra aleatória, e suponhamos que todos os pontos  $x_i$  são dois a dois distintos. Então a distância  $L^1(\mu_n)$  sobre funções binárias com valores em  $\{0, 1\}$  é simplesmente a distância de Hamming normalizada entre as restrições das funções sobre a amostra:

$$\|\chi_C - \chi_D\|_{L^1(\mu_n)} = \bar{d}(\chi_C \upharpoonright \sigma, \chi_D \upharpoonright \sigma).$$

Para uma classe de conceitos  $\mathcal{C}$  sobre um domínio  $\Omega$ , nos denotamos  $N(\epsilon, \mathcal{C}, L^1(\mu_n))$  ou, mais precisamente,  $N(\epsilon, \mathcal{C}, L^1(\mu_\sigma))$ , o número de cobertura de  $\mathcal{C}$  em relação à medida empírica suportada na amostra  $\sigma$ . Essencialmente, isso é o número de cobertura da imagem de  $\mathcal{C}$  no cubo de Hamming correspondente  $\{0, 1\}^\sigma$ . O seguinte é uma consequência imediata do lema de Dudley.

**Teorema 8.3.9** (Dudley). *Seja  $VC\text{-dim}(\mathcal{C}) \leq d$ . Então para todo  $\epsilon > 0$*

$$N(\epsilon, \mathcal{C}, L^1(\mu_n)) \leq \left(2e^2 \log\left(\frac{2e}{\epsilon}\right)\right)^d \left(\frac{1}{\epsilon}\right)^d. \quad (8.16)$$

□

**Exercício 8.3.10.** Seja  $\mathcal{C}$  uma classe de conceitos de dimensão VC finita  $d$ . Mostre que as cotas no teorema de Dudley valem para distância  $L^1(\mu)$  em relação a *qualquer* medida de probabilidade boreliana  $\mu$  sobre  $\Omega$ .

[ *Sugestão:* assumamos que existe um subconjunto finito  $\epsilon$ -separado em  $\mathcal{C}$  em relação a distância  $L^1(\mu)$ , cuja cardinalidade é estritamente maior do que a cota no teorema, e obtenha a contradição usando amostragem aleatória junto com o fato que  $\mathcal{C}$  é uma classe de Glivenko–Cantelli. ]

### Complexidade amostral de classes de Glivenko–Cantelli

Segundo teorema 4.1.10, dada uma classe de conceitos  $\mathcal{C}$  qualquer, com confiança  $1 - \delta$ ,

$$\sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| \leq 2R_n(\mathcal{C}) + \sqrt{\frac{\ln(2/\delta)}{2n}}. \quad (8.17)$$

A prova da implicação (2)  $\Rightarrow$  (1) no teorema 4.3.1 (página 131) contém a desigualdade seguinte: para qualquer  $\varepsilon > 0$ ,

$$\hat{R}_n(\mathcal{C})(\sigma) \leq \sqrt{\frac{2 \log N(\varepsilon, \mathcal{C}, L^1(\mu_\sigma))}{n}} + \varepsilon. \quad (8.18)$$

Combinando a desigualdade acima e o teorema de Dudley para o valor  $\varepsilon/8$  ao invés de  $\varepsilon$ , obtemos:

$$\begin{aligned} \hat{R}_n(\mathcal{C})(\sigma) &= \sqrt{\frac{2 \log N(\varepsilon/8, \mathcal{C}, L^1(\mu_\sigma))}{n}} + \frac{\varepsilon}{8} \\ &\leq \sqrt{\frac{2 \log (2e^2 \log (\frac{16e}{\varepsilon}))^d (\frac{8}{\varepsilon})^d}{n}} + \frac{\varepsilon}{8} \\ &\leq \frac{\varepsilon}{8} + \frac{\varepsilon}{8} = \frac{\varepsilon}{4}, \end{aligned}$$

quando

$$n \geq \frac{128}{\varepsilon^2} \left( d \log \frac{8}{\varepsilon} + d \log \log \frac{16e}{\varepsilon} + \log 2 + 2 \right).$$

Para o segundo termo na eq. (8.17), temos

$$\sqrt{\frac{\ln(2/\delta)}{2n}} < \frac{\varepsilon}{4}$$

quando

$$n > \frac{8}{\varepsilon^2} \log \frac{2}{\delta}.$$

Deduzemos o resultado seguinte.

**Teorema 8.3.11** (Vapnik–Chervonenkis). *Seja  $\mathcal{C}$  uma classe satisfazendo  $VC\text{-dim}(\mathcal{C}) = d < \infty$ . Dado  $\varepsilon, \delta > 0$ , temos com confiança  $1 - \delta$  para cada medida de probabilidade  $\mu$  no domínio  $\Omega$ ,*

$$\sup_{C \in \mathcal{C}} |\mu_\sigma(C) - \mu(C)| \leq \varepsilon$$

quando

$$\begin{aligned} n &\geq \frac{128}{\varepsilon^2} \max \left\{ d \log \frac{8}{\varepsilon} + d \log \log \frac{16e}{\varepsilon} + \log 2 + 2, 16 \log \frac{2}{\delta} \right\} \\ &= O \left( \frac{d}{\varepsilon^2} \log \frac{1}{\delta} \right). \end{aligned}$$

Em outras palavras, a complexidade amostral de  $\mathcal{C}$  satisfaz

$$s(\mathcal{C}, \varepsilon, \delta) \leq \frac{128}{\varepsilon^2} \max \left\{ d \log \frac{8}{\varepsilon} + d \log \log \frac{16e}{\varepsilon} + \log 2 + 2, 16 \log \frac{2}{\delta} \right\}. \quad (8.19)$$

*Observação 8.3.12.* Como sempre, as constantes podem ser melhoradas consideravelmente.

Tendo em vista corolário 4.2.1, concluímos:

**Corolário 8.3.13.** *Seja  $\mathcal{C}$  uma classe de conceitos de Glivenko–Cantelli. Então  $\mathcal{C}$  é consistentemente PAC aprendizável com a complexidade amostral  $s(\mathcal{C}, \varepsilon, \delta)$  da eq. (8.19). A saber, se  $\mathcal{L}$  é uma regra de aprendizagem consistente com a classe  $\mathcal{C}$ , então para todos  $\varepsilon, \delta > 0$  e cada  $n \geq s(\mathcal{C}, \varepsilon, \delta)$ , dado um conceito  $C \in \mathcal{C}$ , temos para toda medida de probabilidade  $\mu$  sobre  $\Omega$  que, com confiança  $1 - \delta$ ,*

$$\text{erro}_{\mu, \mathcal{C}} \mathcal{L}_n(C \upharpoonright \sigma) \leq \varepsilon.$$

Eis um corolário imediato para classes duais.

**Corolário 8.3.14.** *Seja  $\mathcal{C}$  uma classe de dimensão VC dual  $VC\text{-dim}^*(\mathcal{C}) = d^* < \infty$  num domínio  $\Omega$ . Dado  $\varepsilon, \delta > 0$ , para  $n$  bastante grande da ordem  $O(\frac{d^*}{\varepsilon^2} \log \frac{1}{\delta})$  e cada medida de probabilidade  $\mu$  sobre  $\Omega$ , temos que com confiança  $1 - \delta$*

$$\forall x \in \Omega, \mu\{C \in \mathcal{C} : x \in C\} \approx \frac{\#\{i = 1, 2, \dots, n : x \in C_i\}}{n},$$

onde  $C_1, C_2, \dots, C_n$  é uma amostra i.i.d. de conceitos, seguindo a distribuição  $\mu$ .

*Observação 8.3.15.* Todos os três resultados exigem hipóteses adicionais de mensurabilidade. Por exemplo, teorema 8.3.11 e corolário 8.3.13 são válidos sob a hipótese usual que  $\mathcal{C}$  é universalmente separável bastaria em ambos casos. A hipótese mais geral, que se aplica a todas as três situações e que não estudamos neste texto, seria a seguinte: a classe  $\mathcal{C}$  admite uma estrutura boreliana tal que o conjunto  $\{(x, C) : x \in \Omega, C \in \mathcal{C}\}$  é um subconjunto boreliano do produto  $\Omega \times \mathcal{C}$ . Todavia, só vamos usar o corolário 8.3.14 para classes  $\mathcal{C}$  finitas, naquele caso todas as condições da mensurabilidade estão verificadas.

### 8.3.3 Esquemas de compressão com informação adicional

A seguinte definição já aparece na obra original [Littlestone e Warmuth 1986].

**Definição 8.3.16.** Um esquema de compressão amostral rotulado com informação adicional  $I$ , onde  $I$  é um conjunto finito, é um par  $(\mathcal{H}, \kappa)$ , onde

$$\mathcal{H} : [\Omega]^{\leq d} \times I \rightarrow 2^\Omega$$

é a aplicação de descompressão, e

$$\kappa : [\Omega]^{\leq \infty 0|1} \rightarrow [\Omega]^{\leq d 0|1} \times I,$$

a aplicação de compressão, satisfazendo as propriedades usuais:  $\kappa(\sigma, \tau)$  é uma sub-amostra de  $\sigma$  cujo rotudo é induzido por  $\tau$ , e

$$\forall C \in \mathcal{C}, \forall \sigma \in [\Omega]^\infty, \mathcal{H}(\kappa(\sigma, C \cap \sigma)) \cap \sigma = C \cap \sigma. \quad (8.20)$$

*Observação 8.3.17.* Da maneira equivalente, a definição pode ser modificada usando a classe  $\mathcal{C}_H$ .

Temos a versão seguinte do teorema 8.1.9.

**Teorema 8.3.18 (Littlestone e Warmuth [ibid.]).** *Seja  $(\mathcal{H}, \kappa)$  um esquema de compressão amostral rotulado com informação adicional para uma classe  $\mathcal{C}$  de conceitos borelianos, tal que a aplicação  $\mathcal{H} : [\Omega]^{\leq d} \times I \times \Omega \rightarrow \{0, 1\}$  é boreliana. Então a regra  $\mathcal{L} = \mathcal{H} \circ \kappa \circ \iota$  PAC aprende a classe  $\mathcal{C}$  com erro  $\varepsilon > 0$  e confiança*

$$\geq 1 - \#I \sum_{j=0}^d \binom{n}{j} (1 - \varepsilon)^{n-j},$$

onde  $n$  é o tamanho da amostra. □

Daqui, pode-se deduzir a mesma estimativa da complexidade amostral que no exercício 8.1.11, onde  $d$  é substituído por  $k = d + \log \#I$ :

$$s(\varepsilon, \delta) \leq \frac{8}{\varepsilon} \left( k \log \left( \frac{2}{\varepsilon} \right) + \log \left( \frac{1}{\delta} \right) \right).$$

**Exercício 8.3.19.** Tentar deduzir a estimativa acima.

O resultado justifica a definição seguinte.

**Definição 8.3.20.** O tamanho de um esquema rotulado com informação adicional é definido como

$$d + \log_2 \#I.$$

**Teorema 8.3.21 (Moran e Yehudayoff [2016]).** *Cada classe  $\mathcal{C}$  com  $VC\text{-dim}(\mathcal{C}) = d$  e  $VC\text{-dim}^*(\mathcal{C}) = d^*$  admite um esquema de compressão rotulado com informação adicional de tamanho  $O(d \cdot d^*)$ , em particular,  $\exp(O(d))$ .*

A prova ocupa o resto do capítulo e conclui a parte principal das nossas notas.

Fixemos qualquer regra de aprendizagem

$$\mathcal{L}: \bigcup_{n=1}^{\infty} \Omega^n \times \{0, 1\}^n \rightarrow \mathcal{C}$$

consistente com a classe  $\mathcal{C}$ , com valores em  $\mathcal{C}$ . Podemos supor que  $\mathcal{L}$  é invariante pelas permutações das amostras (não depende da ordem dos elementos  $x_1, \dots, x_n \in \sigma$ ), bem como não depende das repetições dos elementos: se  $\sigma = (x_1, \dots, x_n)$  e  $\sigma' = (y_1, \dots, y_m)$  são tais que  $\{x_1, \dots, x_n\} = \{y_1, \dots, y_m\}$ , então para cada  $C \in \mathcal{C}$ , temos  $\mathcal{L}(\sigma, C \upharpoonright \sigma) = \mathcal{L}(\sigma', C \upharpoonright \sigma')$ .

Seja  $s = s(\mathcal{C}, 1/3, 1/3)$  o valor da complexidade amostral de aprendizagem da classe  $\mathcal{C}$  para  $\varepsilon = \delta = 1/3$ . Segue-se do corolário 8.3.14 que  $s = O(d)$ .

### Aplicação de compressão

Seja  $(\sigma, \tau) \in [\Omega]^{\leq \infty 011}$  uma amostra rotulada com um conceito da classe  $\mathcal{C}$ , a saber,  $\sigma \in [\Omega]^n$ ,  $n \in \mathbb{N}$ , e existe  $C \in \mathcal{C}$  com  $\tau = C \cap \sigma$ . Procuremos a imagem de  $(\sigma, \tau)$  pela aplicação de compressão  $\kappa$ . Note que  $C$  é desconhecido.

Formemos a classe (finita),  $\mathcal{C}'$ , de todas as hipóteses da forma  $\mathcal{L}(\zeta, \tau \cap \zeta) \in \mathcal{C}$ , onde  $\zeta \in [\sigma]^{\leq s}$ . (Formalmente,  $(\zeta, \tau)$  não pertence ao domínio de  $\mathcal{L}$ , no entanto, podemos fixar uma ordem boreliana sobre  $\Omega$ , por exemplo, identificá-lo com  $[0, 1]$ , tornando todas as amostras ordenadas, ou seja, elementos de  $\Omega^n$ ). Eis o coração da prova e um novo discernimento importante.

**Lema 8.3.22.** *Existem  $T = O(d^*)$  elementos  $\zeta_1, \dots, \zeta_T \in [\sigma]^{\leq s}$  tais que, para cada  $x \in \sigma$ , o rótulo de  $x$  é adivinhado corretamente pela maioria das hipóteses  $\mathcal{L}(\zeta_i, \tau \cap \zeta_i)$ :*

$$\forall x \in \sigma, \#\{i = 1, 2, \dots, T : x \in \tau \Delta \mathcal{L}(\zeta_i, \tau \cap \zeta_i)\} < T/2. \quad (8.21)$$

*Demonstração.* Definemos uma matriz binária (com coeficientes em  $\{0, 1\}$ ), de tamanho  $[n]^{\leq s} \times n$ , cujas linhas correspondem às amostras  $\zeta \in [\sigma]^{\leq s}$ , e colunas, aos elementos  $x \in \sigma$ . O coeficiente  $(\zeta, x)$  é igual a 0 se e somente se

$$x \in \tau \Delta \mathcal{L}(\zeta_i, \tau \cap \zeta_i),$$

ou seja, o coeficiente é igual a 1 se e somente se os rótulos gerados para  $x$  por  $\tau$  e pela hipótese  $\mathcal{L}(\zeta_i, \tau \cap \zeta_i)$  são iguais.

Segundo corolário 8.3.14 e a escolha de  $s$ , dada uma medida de probabilidade  $\mu$  sobre a amostra  $\sigma$ , com confiança  $2/3$ , o erro de aprendizagem da hipótese  $\mathcal{L}(\tilde{\zeta}, \tau \cap \tilde{\zeta})$ ,  $\tilde{\zeta} \in \sigma^s$ , é menor que  $1/3$ :

$$\mu^{\otimes s} \{\tilde{\zeta} \in \sigma^s : \mu(\mathcal{L}(\tilde{\zeta}, \tau \cap \tilde{\zeta}) \Delta \tau) < 1/3\} \geq 2/3.$$

Em particular, existe  $\tilde{\zeta} \in \sigma^s$  tal que o erro de aprendizagem de  $\mathcal{L}(\tilde{\zeta}, \tau \cap \tilde{\zeta})$  é menor que  $1/3$ . Segundo a nossa escolha de  $\mathcal{L}$ , a amostra  $\zeta \in [\sigma]^{\leq s}$  obtida de  $\tilde{\zeta}$  pela eliminação de repetições e a ordem tem a mesma propriedade:

$$\mu(\mathcal{L}(\zeta, \tau \cap \zeta)\Delta\tau) < 1/3. \quad (8.22)$$

O teorema Minimax de von Neumann J.0.1 diz o seguinte. Pensemos de uma medida de probabilidade sobre  $[n]$  como um  $n$ -vetor,  $p$ , com coordenadas (pesos) não negativas, cuja soma é igual a 1. Seja  $M$  uma matriz com coeficientes reais, de formato  $m \times n$ . Então,

$$\max_{p \in P[m]} \min_{q \in P[n]} p^t M q = \min_{q \in P[n]} \max_{p \in P[m]} p^t M q.$$

(Veja também uma reformulação mais pertinente na eq. (J.1)). Para  $\zeta \in [\sigma]^{\leq s}$ , denotemos por  $\delta_\zeta$  a medida de Dirac suportada em ponto  $\zeta$ , ou seja, o vetor de base cuja coordenada  $\zeta$ -esima é 1, e o resto são zeros. Agora o erro na eq. (8.22) pode ser escrito assim:

$$\mu(\mathcal{L}(\zeta, \tau \cap \zeta)\Delta\tau) = \delta_\zeta^t M \mu.$$

Por conseguinte, o que acabamos de mostrar, é que

$$\max_{\zeta} \min_{\mu \in P(\sigma)} \delta_\zeta^t M \mu \geq 2/3.$$

Segue-se que a expressão a direita no teorema Minimax seja  $\geq 2/3$  também. Por conseguinte, para cada elemento  $x \in \sigma$ , existe uma distribuição  $p$  sobre o conjunto de hipóteses  $\mathcal{C}'$  (ou: o conjunto de  $\zeta$ ), tal que

$$p\{\zeta : x \in \tau \Delta \mathcal{L}(\zeta, \tau \cap \zeta)\} \geq 2/3.$$

Deduzimos do corolário 8.3.14 que existe um conjunto finito de  $T = O(d^*)$  subamostras  $\zeta_i, i = 1, 2, \dots, T$ , tal que para cada  $x \in \sigma$ ,

$$p\{\zeta : x \in \tau \Delta \mathcal{L}(\zeta, \tau \cap \zeta)\} \stackrel{1/8}{\approx} \frac{1}{T} \#\{i = 1, 2, \dots, T : x \in \tau \Delta \mathcal{L}(\zeta_i, \tau \cap \zeta_i)\},$$

e por conseguinte

$$\begin{aligned} \frac{1}{T} \#\{i = 1, 2, \dots, T : x \in \tau \Delta \mathcal{L}(\zeta_i, \tau \cap \zeta_i)\} &\geq p\{\zeta : x \in \tau \Delta \mathcal{L}(\zeta, \tau \cap \zeta)\} - \frac{1}{8} \\ &> \frac{1}{2}, \end{aligned}$$

estabelecendo o lema. □

Agora a imagem  $\kappa(\sigma, \tau)$  é definido como o par consistindo da subamostra

$$\alpha = \bigcup_{t=1}^T \zeta_t$$

de  $\sigma$ , rotulada com  $\tau$ , assim como a palavra binária  $I \in \{0, 1\}^{2^T}$ , para identificar todas as subamostras de  $\alpha$  que correspondem às amostras  $\zeta_t$ . Pense dos elementos de  $I$  como rotulagens de  $\alpha$  com subconjuntos de  $[T]$ , onde cada ponto  $x$  é marcado com o conjunto  $\{t \in T : x \in \zeta_t\}$ .

**Exercício 8.3.23.** Mostrar que o número de tais rotulagens é  $O(d^* \cdot d)$ .

### Aplicação de descompressão

Dado um par que consiste de uma amostra rotulada  $(\alpha, \tau)$  junto com a informação adicional  $i$ , recupere as amostras rotuladas  $(\zeta_t, \tau_t)$ ,  $t \in [T]$ . O rótulo de um ponto  $x \in \Omega$  pela hipótese  $\mathcal{H}((\alpha, \tau), i)$  é definido pelo voto majoritário entre os rótulos

$$\mathcal{L}(\zeta_t, \tau_t)(x), \quad t \in [T].$$

Como  $\alpha$  é uma subamostra rotulada de  $\sigma$ , apenas temos que verificar a condição (8.20). Sejam  $C \in \mathcal{C}$  e  $\sigma \in [\Omega]^{<\infty}$  quaisquer. Consideremos a hipótese  $\mathcal{H}(\kappa(\sigma, C \cap \sigma))$ . Para cada  $x$ , o rótulo é determinado pelo voto majoritário entre as hipóteses  $\mathcal{L}((\zeta_t, \tau_t)$ , e lema 8.3.22 garante que este rótulo é correto.





# Variáveis aleatórias: a primeira passagem

---

Ambicionamos dar sentido à frase seguinte: *os dados são modelados por uma sequência  $X_1, X_2, \dots, X_n, \dots \in \Omega$  de elementos aleatórios independentes e identicamente distribuídos de um espaço boreliano padrão,  $\Omega$* . Essa é uma tarefa que será plenamente concretizada apenas no Apêndice H. O presente Apêndice tem um caráter bastante informal e principalmente motivador.

## A.0.1 De variáveis usuais para variáveis aleatórias

Dado um domínio  $\Omega$ , os dados são modelados pelas *variáveis aleatórias* com valores em  $\Omega$ , ou *elementos aleatórios* de  $\Omega$ . Recordemos primeiramente a noção bem conhecida de uma *variável*, muito comum na matemática pura (geometria, álgebra, análise...) Eis alguns contextos típicos onde as variáveis fazem a sua aparição.

(1) Determinar os valores de  $x$  por quais

$$5x^2 - x + 3 = 0.$$

(2) Suponha que  $t \in [0, 1]$ . Então ....

(3) Sejam  $x, y, z \in \mathbb{R}$  quaisquer. Suponha que  $x < y$ . Então  $x + z > y + z$ .

(4) Seja  $z$  um número complexo qualquer. O valor absoluto de  $z$  ....

Uma variável é um elemento qualquer (desconhecido) de um conjunto ( $\mathbb{R}$  nos casos (1) e (3),  $[0, 1]$  no (2),  $\mathbb{C}$  no (4), etc.). As variáveis na teoria de probabilidade são de uma natureza ligeiramente diferente. Elas são denotadas habitualmente pelas letras *maiúsculas*,  $X, Y, Z, \dots$ , a fim de distinguir das variáveis “usuais”. Se  $X$  é uma variável aleatória (abreviamos: v.a.) real, isso significa duas coisas. Primeiramente, como no caso de uma variável usual,

-  $X$  é um número real cujo valor exato é desconhecido:  $X \in \mathbb{R}$ .

Mas há mais informações adicionais disponíveis. Mesmo com o valor exato de  $X$  sendo desconhecido, se sabe

- a probabilidade de  $X$  pertencer à cada parte  $A$  de  $\mathbb{R}$ .

Em outras palavras, se  $A \subseteq \mathbb{R}$  é uma parte de  $\mathbb{R}$ , então existe um número real entre 0 e 1 que fornece a probabilidade do evento  $X \in A$ . Este número é denotado por

$$P[X \in A],$$

e o conjunto de valores  $P[X \in A]$  para todos  $A$  se chamam a *lei de probabilidade*, ou simplesmente a *lei* de  $X$ . Então, uma variável aleatória é uma variável “usual” munida de uma lei. Por exemplo, se  $a, b \in \mathbb{R}$ ,  $a \leq b$  quaisquer, então se sabe a probabilidade

$$P[a < X < b]$$

de que o valor de  $X$  esteja entre  $a$  e  $b$ . A lei de uma variável aleatória se denota por uma letra grega, por exemplo,  $\mu$  ou  $\nu$ . É uma aplicação associando a cada parte  $A$  de  $\mathbb{R}$  um número real,

$$\mathbb{R} \supseteq A \mapsto \mu(A) = P[X \in A] \in [0, 1].$$

Eis alguns exemplos.

1. Uma variável aleatória de Bernoulli toma dois valores: 0 e 1, cada uma com a probabilidade  $1/2$ :

$$P[X = 0] = \frac{1}{2} = P[X = 1].$$

Para calcular a lei de  $X$ , seja  $A \subseteq \mathbb{R}$  um conjunto qualquer. Obviamente, se  $A$  contém ambos 0 e 1, então a probabilidade que  $X \in A$  é igual a 1, é um evento certo. Se  $A$  não contém nem 0 nem 1, então o evento  $X \in A$  é improvável, a sua probabilidade é 0. Afinal, se  $A$  contém exatamente um dos pontos  $\{0, 1\}$ , então a probabilidade do evento  $X \in A$  é  $1/2$ :

$$P[X \in A] = \begin{cases} 1, & \text{se } 0, 1 \in A, \\ \frac{1}{2}, & \text{se } 0 \in A \text{ e } 1 \notin A, \\ \frac{1}{2}, & \text{se } 0 \notin A \text{ e } 1 \in A, \\ 0, & \text{se } 0 \notin A, 1 \notin A. \end{cases}$$

Uma variável de Bernoulli modela uma jogada única de uma moeda justa, onde a probabilidade de dar “coroa” (o valor 1) é  $1/2$ , a mesma que a probabilidade de dar “cara” (o valor 0).

De maneira mais geral, se a moeda não é justa, então a probabilidade de dar “coroa” pode ser um valor qualquer  $p \in [0, 1]$ ,

$$P[X = 1] = p,$$

é a probabilidade de dar “cara” é

$$P[X = 0] = 1 - p = q.$$

A lei de probabilidade de uma variável aleatória real,  $X$ , é completamente determinada pela sua *função de distribuição*,  $\Phi$ . É uma função real dada por

$$\Phi(t) = P[X < t].$$

É fácil calcular a função de distribuição de uma v.a. de Bernoulli, veja Figura A.1.

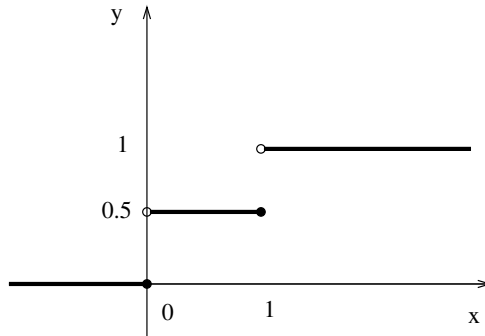


Figura A.1: Função de distribuição de uma variável aleatória de Bernoulli.

Se o conjunto dos valores da função de distribuição de uma variável aleatória  $X$  é enumerável, então  $X$  é dita *discreta*. Por exemplo, a variável aleatória de Bernoulli é discreta.

2. Uma variável aleatória de lei *uniforme* com valores no intervalo  $[0, 1]$  é dada pela fórmula seguinte: quaisquer sejam  $a, b \in \mathbb{R}$ ,  $a < b$ ,

$$P[X \in (a, b)] = \int_a^b \chi_{[0,1]}(t) dt. \quad (\text{A.1})$$

Aqui,  $\chi_{[0,1]}$  nota a *função indicadora* do intervalo  $[0, 1]$  (Figura A.2):

$$\chi_{[0,1]}(t) = \begin{cases} 1, & \text{se } x \in [0, 1], \\ 0, & \text{caso contrário.} \end{cases}$$

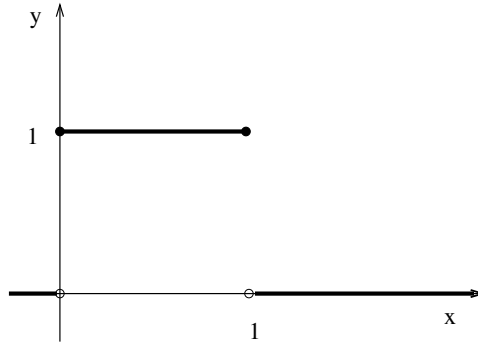


Figura A.2: Grafo da função indicadora do intervalo  $[0, 1]$ .

Por exemplo,

$$P[0 \leq X \leq 1] = \int_0^1 \chi_{[0,1]}(t) dt = 1,$$

e

$$P\left[-\frac{1}{2} \leq X \leq \frac{1}{2}\right] = \int_{-\frac{1}{2}}^{\frac{1}{2}} \chi_{[0,1]}(t) dt = \frac{1}{2}.$$

Se um intervalo  $(a, b)$  está contido em  $[0, 1]$ , então

$$\begin{aligned} P[X \in (a, b)] &= \int_a^b \chi_{[0,1]}(t) dt \\ &= \int_a^b 1 \cdot dt \\ &= b - a. \end{aligned}$$

Em outras palavras, neste caso a probabilidade de que  $X$  pertença ao intervalo  $(a, b)$  é igual ao comprimento do intervalo.

Se a lei de uma variável aleatória é dada pela integral, como na fórmula (A.1), então a função sob a integral é chamada a *densidade* de  $X$ . A densidade de uma v.a. uniforme é a função indicadora:

$$\chi_{[0,1]}(t).$$

**Exercício A.0.1.** Mostrar que a lei de Bernoulli não possui densidade.

A função de distribuição de uma v.a. uniforme é calculada facilmente (Figura A.3).

Uma variável aleatória real  $X$  é dita *contínua* se valores da sua função de distribuição preenchem o intervalo  $[0, 1]$ . A v.a. uniforme é obviamente contínua.

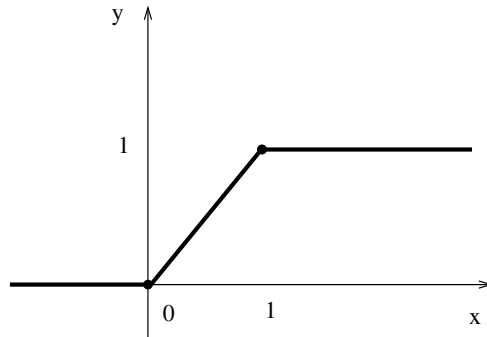


Figura A.3: A função de distribuição de uma variável aleatória uniforme.

**Exercício A.0.2.** Seja  $X$  uma v.a. que possui densidade. Mostrar que  $X$  é contínua.

**Exercício A.0.3 (\*)**. Construir um exemplo de v.a. que é contínua e não possui densidade.  
[ *Sugestão*: deve-se usar o conjunto de Cantor 5.1. ]

**Exercício A.0.4.** Construir um exemplo de v.a. nem discreta nem contínua.

Uma variável aleatória real é *gaussiana* (ou: segue a lei *normal centrada e reduzida*), se  $X$  possui densidade dada por

$$\frac{1}{\sqrt{2\pi}} e^{-t^2/2}.$$

Em outras palavras, quais quer sejam  $a, b \in \mathbb{R}$ ,

$$P[a < X < b] = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2} dt.$$

A lei *semi-circular* é dada pela função de densidade

$$f(t) = \begin{cases} \frac{2}{\pi} \sqrt{1-t^2}, & \text{se } |t| \leq 1, \\ 0, & \text{se não.} \end{cases}$$

Estritamente falando, o gráfico da densidade não é um semi-círculo, mas, melhor, uma semi-elipse – o fator normalizador  $2/\pi \approx 0.637$  é necessário para que a probabilidade de um evento certo seja igual a 1.

A noção de uma variável aleatória não é apenas o único conceito mais fundamental da teoria de probabilidade, mas é, sem dúvida, uma das mais importantes noções em todas as ciências matemáticas. Alguns matemáticos eminentes argumentam que, eventualmente, os fundamentos da matemática devem ser alterados de modo que as variáveis aleatórias sejam tão básicos quanto os conjuntos [Mumford 2000].

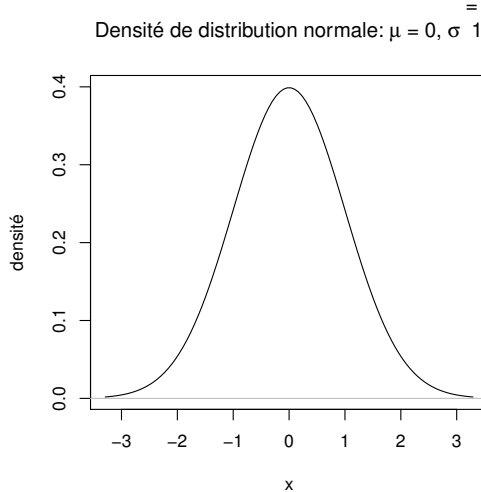


Figura A.4: A função de densidade da lei gaussiana.

## A.0.2 Álgebra de conjuntos borealianos

Até agora, só vimos as variáveis aleatórias reais, com valores em  $\mathbb{R}$ . Mas elas podem assumir valores em domínios  $\Omega$  mais gerais.

Seja  $\Omega$  um domínio geral. Quais são as propriedades desejadas da lei,  $\mu$ , de uma variável aleatória  $X$  com valores em  $\Omega$ ? Claro, os valores da lei pertencem no intervalo  $[0, 1]$ , e a probabilidade que  $X \in \Omega$  deve ser 1:

$$(P1) \quad P[X \in \Omega] = \mu(\Omega) = 1.$$

A probabilidade de  $x$  pertencer a união de uma família disjunta dos conjuntos  $A_i, i \in I$  deve ser igual à soma das probabilidades de que  $x \in A_i$  para todos  $i$ :

$$Pr \left[ X \in \bigcup A_i \right] = \sum Pr[X \in A_i].$$

Qual é o tamanho de tais famílias que devemos considerar? Se nós restringimos a propriedade às uniões finitas, a noção de probabilidade resultante é muito geral e fraca demais. Neste caso, trata-se das *medidas de probabilidade finitamente aditivas*. Elas são bastante importantes em várias partes da matemática, mas não são suficientes para abranger as necessidades da teoria de probabilidade. Vários teoremas fundamentais são falsos neste contexto.

Se, pelo contrário, permitimos as uniões de famílias *quaisquer*, a noção de probabilidade que obtemos é demasiado restritiva.

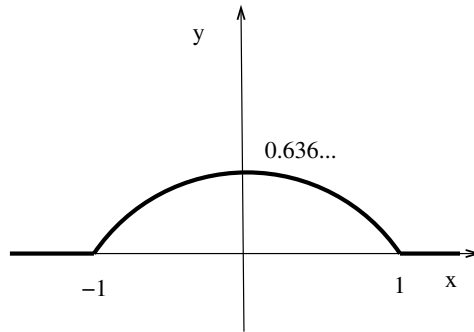


Figura A.5: A densidade da lei semi-circular.

**Exercício A.0.5.** Suponha que a lei de uma variável aleatória  $X$  com valores em  $\Omega$  lei possui a propriedade: qualquer seja uma família dos conjuntos  $A_i \subseteq \Omega$ ,  $i \in I$  dois a dois disjuntos,  $A_i \cap A_j = \emptyset$  para todos  $i, j$ ,  $i \neq j$ , temos

$$P[X \in \cup_{i \in I} A_i] = \sum_{i \in I} P[X \in A_i].$$

Mostrar que isso é o caso se e somente se  $X$  é puramente atômica, ou seja, existe uma sequência (finita ou infinita) de pontos dois-a-dois distintos  $a_j \in \Omega$ ,  $j = 1, 2, 3, \dots$  (átomos de medida  $\mu$ ), com  $\mu\{a_j\} = p_j > 0$ , tal que o valor da medida de um subconjunto  $A \subseteq \Omega$  é dado por

$$\mu(A) = \sum \{p_j : a_j \in A\} = \sum_{j=1}^{\infty} \chi_A(a_j) p_j = \int_{\Omega} \chi_A d\mu.$$

Em particular,

$$\sum_{j=1}^{\infty} p_j = 1.$$

**Exercício A.0.6.** Mostrar que uma variável aleatória real é discreta se e somente se ela é puramente atômica.

A escolha mais natural e frutífera (ditada pela prática da pesquisa matemática) é a das famílias *enumeráveis*.

(P2) Se  $A_i$ ,  $i = 1, 2, 3, \dots$  são disjuntos dois-a-dois, então  $\mu(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mu(A_i)$ .

Como um corolário imediato, obtemos, no caso onde  $A_1 = A$  e  $A_2 = A^c = X \setminus A$ :

(P2') Se  $A \subseteq \Omega$ , então  $P(A^c) = 1 - P(A)$ .

Se  $\mu$  é a lei de uma variável puramente atômica, então o valor

$$\mu(A) = P[X \in A]$$

é bem definido qualquer seja um subconjunto  $A \subseteq \Omega$  do domínio. Podemos esperar o mesmo para cada variável aleatória? A resposta é negativa.

A *Hipótese do Contínuo* (Apêndice B) diz que cada subconjunto infinito de  $\mathbb{R}$  ou tem a cardinalidade de  $\mathbb{N}$ , ou tem a cardinalidade de  $\mathbb{R}$ . Pode-se mostrar [Banach e Kuratowski 1929] que, assumindo a validade da Hipótese do Contínuo, as únicas medidas definidas sobre a família de todos os subconjuntos de  $\mathbb{R}$  é satisfazendo as propriedades (P1) e (P2) acima são puramente atômicas. Como não queremos que a teoria dependa de hipóteses conjuntísticas adicionais, somos forçados a restringir a coleção  $\mathcal{B}$  dos subconjuntos  $A \subseteq \Omega$ , para as quais o valor  $P[X \in A]$  é bem definido. Tentemos definir esta família usando algum senso comum.

O axioma (P1) implica que  $\Omega$  sempre pertence à família  $\mathcal{B}$ . Segundo o axioma (P2), se uma sequência de conjuntos pertence a  $\mathcal{B}$ ,

$$A_1, A_2, \dots \in \mathcal{B},$$

então a sua união pertence a  $\mathcal{B}$  também:

$$\bigcup_i A_i \in \mathcal{B}.$$

Tendo em conta o axioma (P2'), concluímos que, se  $A \in \mathcal{B}$ , então  $A^c \in \mathcal{B}$ . Segue-se que a família  $\mathcal{B}$  deve conter  $\Omega$ , os complementares de todos os seus membros, e as uniões de sub-famílias enumeráveis. Uma família com estas propriedades é dita uma *sigma-álgebra* de subconjuntos de  $\Omega$ .

Se  $\Omega$  é um espaço métrico, é razoável exigir que a lei seja bem-definida para todas as bolas abertas:

$$B_r(x) = \{y \in \Omega : d(x, y) < r\}.$$

Isso é necessário, por exemplo, para conhecer a probabilidade do evento

$$[d(X, x) < r].$$

Mais geralmente, exigimos que a lei seja bem-definida para todos os conjuntos *abertos*, ou seja, os conjuntos que são uniões das bolas:

$$V \text{ é aberto} \iff \forall x \in V, \exists \epsilon > 0, B_\epsilon(x) \subseteq V.$$

**Exercício A.0.7.** Seja  $\Omega$  um espaço métrico. Mostrar que existe a menor sigma-álgebra que contem todos os conjuntos abertos de  $\Omega$ .



**Definição A.0.8.** Seja  $\Omega$  um espaço métrico qualquer. A menor família  $\mathcal{B}$  que contém todos os conjuntos abertos e é fechada com relação aos complementares e uniões de subfamílias enumeráveis, se chama a família de subconjuntos *borelianos* de  $\Omega$ .

Um espaço métrico  $\Omega$  é dito *separável* se existe um subconjunto enumerável  $A$  cujo fecho é  $\Omega$ :

$$\bar{A} = \Omega.$$

**Exercício A.0.9.** Seja  $\Omega$  um espaço métrico separável. Mostrar que a família de conjuntos borelianos é a menor sigma-álgebra que contém todas as bolas abertas.

É claro que todo subconjunto fechado de  $\Omega$  é boreliano também. De fato, os conjuntos borelianos são muito mais numerosos do que os abertos ou fechados.

**Exercício A.0.10.** Mostrar exemplos de subconjuntos borelianos de  $[0, 1]$  que não são nem abertos nem fechados.

**Definição A.0.11.** Um conjunto  $\Omega$  munido de uma sigma-álgebra  $\mathcal{B}$  de subconjuntos é dito um *espaço boreliano* se existe uma métrica  $d$  sobre  $\Omega$  tal que  $\mathcal{B}$  é exatamente a família de todos os conjuntos borelianos do espaço métrico  $(\Omega, d)$ .

**Exercício A.0.12.** Seja  $\Upsilon$  um subconjunto de um espaço boreliano  $(\Omega, \mathcal{B})$ . Mostrar que  $\Upsilon$  se torna um espaço boreliano se munido da sigma-álgebra

$$\mathcal{B}|_{\Upsilon} = \{B \cap \Upsilon : B \in \mathcal{B}\}.$$

[ *Sugestão:* escolha uma métrica  $d$  sobre  $\Omega$  que gera a estrutura boreliana  $\mathcal{B}$ , e verifique que a estrutura  $\mathcal{B}|_{\Upsilon}$  é gerada pela restrição  $d|_{\Upsilon \dots}$  ]

O espaço boreliano  $(\Upsilon, \mathcal{B}|_{\Upsilon})$  se chama um *sub-espaço boreliano* de  $\Omega$ .

### A.0.3 Medidas de probabilidade borealianas

**Definição A.0.13.** Uma função  $\mu$  na classe  $\mathcal{B}$  dos conjuntos borelianos de  $\Omega$  com valores em  $[0, 1]$  que satisfaz (P1) e (P2) é uma *medida de probabilidade boreliana*.

**Definição A.0.14.** Um espaço boreliano  $\Omega$  munido de uma medida boreliana de probabilidade  $\mu$  é dito *espaço probabilístico*.

**Exemplo A.0.15.** Se  $\Omega = \Sigma^n$  é o cubo de Hamming, então a estrutura boreliana do cubo  $\Sigma^n$  consiste de todos os seus subconjuntos, e a medida de contagem normalizada  $\mu_{\#}$  é uma medida de probabilidade boreliana.

**Exemplo A.0.16.** Mais geralmente, seja  $\Omega$  um domínio qualquer, seja

$$x_1, x_2, \dots, x_n, \dots$$

uma sequência (finita ou infinita) dos elementos de  $\Omega$ , e seja

$$p_1, p_2, \dots, p_n, \dots$$

uma sequência do mesmo tamanho dos valores positivos,  $p_i > 0$ , com a propriedade

$$\sum_i p_i = 1.$$

Então a regra

$$\mu(A) = \sum \{p_i : x_i \in A\}$$

define uma medida de probabilidade boreliana sobre  $\Omega$ . De fato, esta medida é definida para todo subconjunto  $A \subseteq \Omega$ , boreliano ou não. Os conjuntos unitários  $\{x_i\}$  tem a medida positiva:

$$\mu\{x_i\} = p_i.$$

**Definição A.0.17.** Uma medida  $\mu$  sobre  $\Omega$  é *discreta*, ou *puramente atômica*, se existe um subconjunto enumerável de  $\Omega$  cuja medida é um.

**Exercício A.0.18.** Mostrar que cada medida discreta tem a mesma forma que a medida no exemplo A.0.16.

Afim de dar exemplos matematicamente rigorosos de medidas de probabilidade não-discretas, tais como a distribuição uniforme sobre o intervalo  $[0, 1]$ , já precisamos mais trabalho técnico. Vamos fazer isso no apêndice E.

## A.0.4 Funções borelianas

Cada medida de probabilidade sobre  $\Omega$  é a lei de uma variável aleatória com valores em  $\Omega$ . Vamos mostrar agora que pode-se compor variáveis aleatórias e funções para obter novas variáveis aleatórias.

Sejam  $\Omega$  e  $W$  dois espaços métricos, e  $f : \Omega \rightarrow W$  uma função. Seja  $X$  uma variável aleatória com valores em  $\Omega$ . Então  $f(X)$  é uma variável aleatória com valores em  $W$ . A lei,  $\nu$ , de  $f(X)$  é a *imagem direta* da lei  $\mu$  de  $X$  por  $f$ : se  $B \subseteq W$ , então

$$\nu(B) = \mu(f^{-1}(B)).$$

Isso significa:

$$P[f(X) \in B] = P[X \in f^{-1}(B)].$$

A lei  $\nu$  é as vezes denotada

$$\nu = f_*(\mu).$$

Para esta definição funcionar, a única condição necessária sobre  $f$  é que a imagem recíproca de cada subconjunto boreliano  $B \subseteq W$  por  $f$  seja um conjunto boreliano. Uma tal função se chama *função boreliana*, ou *Borel mensurável*. Pode se verificar que  $f : \Omega \rightarrow W$  é boreliana se e somente se a imagem recíproca de cada subconjunto *aberto* de  $W$  é boreliana. Em particular, cada função contínua é boreliana, mas as funções borelianas são muito mais numerosas.

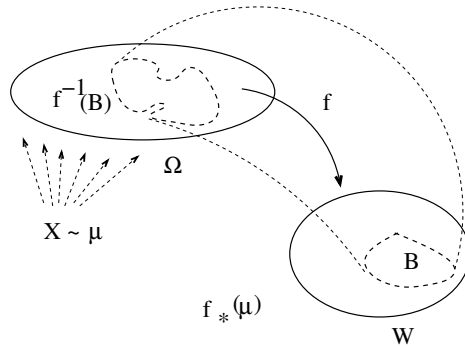


Figura A.6: Imagem direta de uma lei.

**Exercício A.0.19.** Construir uma função boreliana descontínua.

**Exercício A.0.20.** Sejam  $\Omega$  e  $W$  dois espaços métricos,  $f: \Omega \rightarrow W$  uma função boreliana, e  $\mu$  uma medida de probabilidade boreliana sobre  $\Omega$ . Mostrar que a imagem direta  $f_*(\mu)$  é uma medida de probabilidade boreliana sobre  $W$ .

É neste sentido que cada função  $f$  sobre um espaço de probabilidade  $(\mathcal{X}, \nu)$  com valores num espaço boreliano  $\Omega$  pode ser tratada como uma variável aleatória. A saber,  $\nu$  é a lei de uma variável aleatória, digamos  $X$ , com valores em  $\mathcal{X}$ . Então,  $f(X)$  é uma variável aleatória com valores em  $\Omega$ , tendo a lei  $f_*(\nu)$ . Foi neste sentido que falamos da esperança de uma função real  $f$  sobre o cubo de Hamming munido da medida de contagem normalizada.

**Definição A.0.21.** Uma *realização* de variável aleatória  $X$  com valores em  $\Omega$  e a lei  $\mu$  é uma função boreliana  $f$  de um espaço de probabilidade  $(\mathcal{X}, \nu)$  com valores em  $\Omega$  tal que a imagem direta  $f_*(\nu)$  é igual a  $\mu$ .

Cada variável aleatória pode ser representada desta forma. Por exemplo, se  $X \in \Omega$  é uma v.a. com a lei  $\mu$ , podemos definir  $\mathcal{X} = \Omega$ ,  $\nu = \mu$ , e  $f(x) = x$ .

## A.0.5 Espaços borelianos padrão

A aprendizagem estatística – pelo menos, dentro do paradigma atual – ou não é factível nos domínios não separáveis, ou se reduz a um sub-domínio separável. Por isso, vamos supor que  $\Omega$  seja separável. Uma outra restrição natural é que o domínio seja metrizável com uma métrica completa. Isto leva-nos ao conceito seguinte.

**Definição A.0.22.** Um *espaço boreliano padrão* é um par  $(\Omega, \mathcal{B})$  que consiste de um conjunto  $\Omega$  e uma sigma-álgebra  $\mathcal{B}$ , que é a estrutura boreliana gerada por uma métrica completa e separável sobre  $\Omega$ .

Relembramos que um espaço métrico  $(X, d)$  é *separável* se existe um subconjunto enumerável  $Y$  denso em  $X$ :

$$\bar{Y} = X.$$

**Exercício A.0.23.** Mostrar que um subespaço de um espaço métrico separável é separável. [ Para uma prova, veja teorema C.2.74. ]

Acontece que os espaços borelianos padrão distintos são muito poucos e admitem uma classificação completa simples.

**Definição A.0.24.** Um *isomorfismo* entre dois espaços borelianos  $(\Omega_i, \mathcal{B}_i)$ ,  $i = 1, 2$  é uma bijeção  $f: \Omega_1 \rightarrow \Omega_2$  conservando os conjuntos borelianos: qual quer seja  $B \subseteq \Omega_1$ , temos

$$B \in \mathcal{B}_1 \iff f(B) \in \mathcal{B}_2.$$

**Teorema A.0.25.** *Dois espaços borelianos padrão são isomorfos se e somente se eles tem a mesma cardinalidade.*

A prova do teorema ocupa o Apêndice D. Em particular, vamos ver que cada espaço boreliano enumerável é isomorfo ao espaço discreto da mesma cardinalidade cuja estrutura boreliana consiste de todos os subconjuntos; enquanto cada espaço boreliano padrão não enumerável é isomorfo a  $\mathbb{R}$  com a sua estrutura boreliana canônica.

## A.0.6 Independência

**Definição A.0.26.** Se  $\Omega$  é um espaço boreliano padrão e  $\mu$  é uma medida de probabilidade boreliana (ou seja, definida para todos elementos da estrutura boreliana  $\mathcal{B}$  de  $\Omega$ ), então  $(\Omega, \mu)$  é dito *espaço probabilístico padrão*.

Se temos mais de uma variável aleatória,

$$X_1, X_2, \dots, X_n, \dots,$$

tomando os valores, respectivamente, nos espaços  $\Omega_1, \Omega_2, \dots, \Omega_n, \dots$ , então elas podem ser combinadas numa única variável aleatória, tomando os valores no produto dos espaços  $\Omega_i$ :

$$X = (X_1, X_2, \dots, X_n, \dots) \in \Omega_1 \times \Omega_2 \times \dots \times \Omega_n.$$

A lei  $\mu$  da variável  $X$  é chamada a *lei conjunta* das variáveis  $X_1, X_2, \dots, X_n, \dots$

As variáveis aleatórias  $X_1, X_2, \dots, X_n, \dots$  são ditas *independentes* se, cada vez que  $A_i$  é um subconjunto boreliano de  $\Omega_i$ ,  $i = 1, 2, \dots$ , temos

$$\begin{aligned} Pr[X_1 \in A_1, X_2 \in A_2, \dots, X_n \in A_n, \dots] = \\ Pr[X_1 \in A_1] \times Pr[X_2 \in A_2] \times \dots \times Pr[X_n \in A_n] \times \dots \end{aligned}$$

Notação:

$$\mu = \otimes_{i=1}^{\infty} \mu_i.$$

Esta  $\mu$  é também chamada a medida produto das medidas de probabilidade  $\mu_1, \mu_2, \dots$ .

Por exemplo, sejam  $X$  e  $Y$  duas v.a., cada uma de lei uniforme sobre o intervalo  $[0, 1]$ . Se  $X$  e  $Y$  são independentes, isso significa que a variável aleatória  $Z = (X, Y)$  com valores no quadrado  $[0, 1]^2$  tem lei,  $\mu$ , que é uniforme no quadrado: quaisquer sejam  $a, b, c, d, a \leq b, c \leq d$ , temos

$$\mu([a, b] \times [c, d]) = (b - a)(d - c).$$

Por outro lado, se por exemplo  $Y = X$ , então a lei da variável  $Z = (X, Y)$  é concentrada na diagonal do quadrado: se  $A_1, A_2 \subseteq [0, 1]$  são disjuntos, então, obviamente,

$$P[X \in A_1, Y \in A_2] = 0,$$

de onde é fácil de concluir que

$$\mu(\Delta) = 1,$$

onde

$$\Delta = \{(x, x) : x \in [0, 1]\}.$$

Se  $X_1, X_2, \dots, X_n$  é uma sequência das variáveis aleatórias independentes distribuídas segundo a lei gaussiana em  $\mathbb{R}$ , então sua lei conjunta é a lei gaussiana  $n$ -dimensional em  $\mathbb{R}^d$ , determinada pela densidade

$$\frac{1}{(2\pi)^{n/2}} e^{-(t_1^2 + t_2^2 + \dots + t_n^2)/2}.$$

Isso significa que, qualquer que seja um subconjunto boreliano  $A \subseteq \mathbb{R}^d$ ,

$$P[X \in A] = \frac{1}{(2\pi)^{n/2}} \int_A e^{-(t_1^2 + t_2^2 + \dots + t_n^2)/2} dt_1 \dots dt_n.$$

# B

## Elementos da teoria de conjuntos

---

### B.1 Cardinalidade e ordens

#### B.1.1 Cardinalidade

**Definição B.1.1.** Sejam  $X$  e  $Y$  dois conjuntos quaisquer. Eles são *equipotentes*, ou *têm a mesma cardinalidade*, se existe uma aplicação bijetora entre eles:

$$f: X \rightarrow Y,$$

ou seja,  $f$  é injetora ( $\forall x, y \in X, x \neq y \rightarrow f(x) \neq f(y)$ ) e sobrejetora ( $\forall y \in Y, \exists x \in X$  tal que  $f(x) = y$ ). Notação:

$$|X| = |Y|.$$

Para conjuntos finitos, num contexto combinatório usamos também a notação

$$\sharp X = \sharp Y.$$

*Observação B.1.2.* A relação da equipotência é uma relação da equivalência entre conjuntos. Ela é

1. reflexiva:  $|X| = |X|$ ,
2. simétrica: se  $|X| = |Y|$ , então  $|Y| = |X|$ , e

3. transitiva: se  $|X| = |Y|$  e  $|Y| = |Z|$ , então  $|X| = |Z|$ .

Todas as três propriedades são fáceis a verificar.

**Definição B.1.3.** Seja  $X$  um conjunto. A classe de equivalência de  $X$  relativo à relação de equipotência é denotado  $|X|$ . Ela é chamado a *cardinalidade* de  $X$ .

Em particular, a cardinalidade do conjunto  $\mathbb{N}$  dos números naturais é denotado  $\aleph_0$  (lê: álef zero):

$$|\mathbb{N}| = \aleph_0.$$

A cardinalidade do conjunto  $\mathbb{R}$  dos números reais é denotado ou  $c$  ou  $2^{\aleph_0}$ .

**Definição B.1.4.** Seja  $X$  e  $Y$  dois conjuntos. Digamos que a cardinalidade de  $X$  é maior ou igual à cardinidade de  $Y$ ,

$$|X| \geq |Y|,$$

se existe uma injeção de  $Y$  em  $X$ .

**Definição B.1.5.** Digamos que a cardinalidade de  $X$  é estritamente maior que a cardinalidade de  $Y$ ,

$$|X| > |Y|,$$

se  $|X| \geq |Y|$  e não é verdadeiro que  $|X| = |Y|$ .

**Teorema B.1.6** (Cantor–Bernstein). *Sejam  $X$  e  $Y$  dois conjuntos tais que  $|X| \leq |Y|$  e  $|Y| \leq |X|$ . Então*

$$|X| = |Y|.$$

*Demonstração.* Definemos  $X_1 = X \setminus g(Y)$ ,  $Y_1 = Y \setminus f(X)$ , e depois, da maneira recursiva,

$$X_{n+1} = g(Y_n),$$

$$Y_{n+1} = f(X_n),$$

para todos  $n \in \mathbb{N}_+ = \{1, 2, \dots\}$ .

Os conjuntos  $X_n$ ,  $n = 1, 2, 3, \dots$  são dois a dois disjuntos, bem como os conjuntos  $Y_n$ . Definemos

$$X_\infty = X \setminus \bigcup_{n=1}^{\infty} X_n,$$

$$Y_\infty = Y \setminus \bigcup_{n=1}^{\infty} Y_n.$$

Para cada  $x \in X$ , seja

$$h(x) = \begin{cases} f(x), & \text{si } x \in X_{2n+1}, n = 1, 2, 3, \dots, \\ g^{-1}(x), & \text{si } x \in X_{2n}, n = 1, 2, 3, \dots, \\ f(x), & \text{si } x \in X_\infty. \end{cases} \quad (\text{B.1})$$

Agora não é difícil verificar que  $h: X \rightarrow Y$  é uma função bijetora.  $\square$

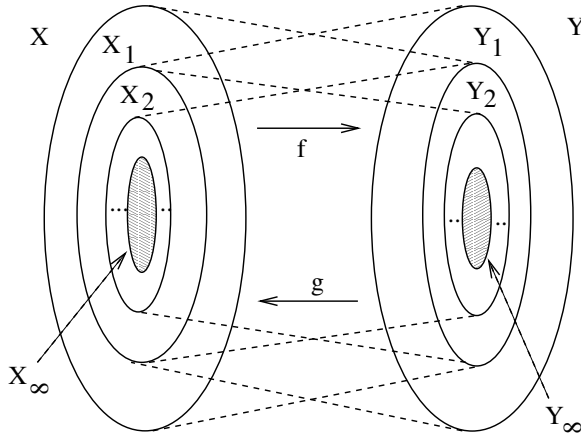


Figura B.1: Prova do teorema de Cantor–Bernstein.

**Exercício B.1.7.** Verifique que  $h : X \rightarrow Y$  na eq. (B.1) é bijetora. (Sugestão: mostre que a aplicação  $h^\ddagger : Y \rightarrow X$  definida por

$$h^\ddagger(y) = \begin{cases} g(y), & \text{si } y \in Y_{2n+1}, n = 1, 2, 3, \dots, \\ f^{-1}(y), & \text{si } y \in Y_{2n}, n = 1, 2, 3, \dots, \\ f^{-1}(x), & \text{si } y \in Y_\infty. \end{cases}$$

é a aplicação inversa de  $h$ , em outras palavras,  $h \circ h^\ddagger = \text{Id}_Y$  e  $h^\ddagger \circ h = \text{Id}_X$ .)

**Teorema B.1.8.** *Sejam  $X$  e  $Y$  dois conjuntos quaisquer. Então, ou  $|X| \leq |Y|$ , ou  $|Y| \leq |X|$ .*

Deixemos a prova do teorema B.1.8 como exercício B.3.10 (uma aplicação do lema de Zorn, a ser discutido mais tarde).

**Corolário B.1.9.** *Sejam  $X$  e  $Y$  dois conjuntos quaisquer. Então uma e uma só possibilidade entre as seguintes tem lugar:*

- $|X| < |Y|$ ,
- $|X| = |Y|$ , ou
- $|X| > |Y|$ .

**Definição B.1.10.** Seja  $X$  um conjunto. Denotaremos  $2^X$  o conjunto de todas as partes de  $X$ :

$$2^X = \{Y : Y \subseteq X\}.$$



**Teorema B.1.11.** *Seja  $X$  um conjunto qualquer. Então,*

$$|X| < |2^X|.$$

*Demonstração.* Para começar, a aplicação  $H : X \rightarrow 2^X$  dada por

$$H(x) = \{x\}$$

é obviamente injetora, de onde concluímos:

$$|X| \leq |2^X|.$$

Resta mostrar que

$$|X| \neq |2^X|.$$

Suponha, para uma contradição, que os dois cardinais sejam iguais:

$$|X| = |2^X|. \tag{B.2}$$

Isto significa que existe uma aplicação bijetora

$$F : X \xrightarrow{\sim} 2^X.$$

Definemos

$$A = \{x \in X : x \notin F(x)\}.$$

Como  $F$  é sobrejetora, existe  $x_0 \in X$  tal que

$$F(x_0) = A.$$

Perguntamos:  $x_0 \in A$ ? Segundo a definição do conjunto  $A$ , temos  $x_0 \in A$  se e somente se  $x_0 \notin A$ . É obviamente uma afirmação auto-contraditória. Deduzimos: a hipótese inicial (B.2) é falsa.  $\square$

**Exemplo B.1.12.** Mostremos que  $|2^{\mathbb{N}}| = |\mathbb{R}|$ .

Associamos a cada subconjunto  $A$  de  $\mathbb{N}$  a sua função característica, ou seja, uma sequência dos zeros e uns da maneira que se  $n \in A$ , então na  $n$ -ésima posição temos 1, e se  $n \notin A$ , temos 0. Por exemplo, ao subconjunto dos números naturais pares associamos a sequência

$$0, 1, 0, 1, 0, 1, \dots$$

Desta maneira, pensaremos de  $2^{\mathbb{N}}$  como o conjunto de todas as sequências binárias.

A aplicação que associa à uma sequência

$$\epsilon_1 \epsilon_2 \epsilon_3 \dots, \quad \epsilon_i \in \{0, 1\},$$

o único número real

$$\sum_{n=1}^{\infty} 10^{-n} \epsilon_n$$

cuja expansão decimal é esta sequência, é injetora. Logo,

$$|2^{\mathbb{N}}| \leq |\mathbb{R}|.$$

De outro lado, definemos uma injeção de  $\mathbb{R}$  em  $2^{\mathbb{N}}$  como a composição de uma bijeção qualquer entre  $\mathbb{R}$  e o intervalo  $(0, 1)$  e a aplicação que envia  $x \in (0, 1)$  na sequência dos dígitos da sua expansão binária,

$$x = \sum_{n=1}^{\infty} 2^{-n} \epsilon_n \mapsto (\epsilon_1, \epsilon_2, \epsilon_3, \dots), \quad \epsilon_n \in \{0, 1\}.$$

Esta injeção  $\mathbb{R} \rightarrow 2^{\mathbb{N}}$  estabelece que

$$|\mathbb{R}| \leq |2^{\mathbb{N}}|.$$

Concluimos usando o teorema de Cantor–Bernstein. ▲

**Corolário B.1.13.**  $\aleph_0 < c$ .

A hipótese do contínuo (Continuum Hypothesis, CH) afirma que não existem cardinalidades estritamente intermediárias entre  $\aleph_0$  e  $c$ . Vamos discutir a CH em mais detalhes no final do Apêndice.

## B.1.2 Ordens e permutações

**Definição B.1.14.** Sejam  $X$  um conjunto e  $R$  uma relação binária sobre  $X$ :  $R \subseteq X^2$ . Diz-se que  $R$  é uma *relação de ordem parcial*, ou simplesmente um *ordem parcial*, se ela verifica as condições seguintes:

1.  $R$  é reflexiva:  $xRx$  para todos  $x \in X$ .
2.  $R$  é antisimétrica: se  $xRy$  e  $yRx$ , então  $x = y$ .
3.  $R$  é transitiva: se  $xRy$  e  $yRz$ , então  $xRz$ .

Habitualmente, uma relação de ordem parcial é denotada pelo símbolo  $\leq$ . Um par  $(X, \leq)$  que consiste de um conjunto  $X$  munido de uma ordem parcial  $\leq$  é dito *conjunto parcialmente ordenado*.

**Definição B.1.15.** Uma ordem parcial  $\leq$  sobre um conjunto  $X$  é dita *ordem total* se todos elementos de  $X$  são comparáveis dois a dois entre eles:

$$\forall x, y \in X, \quad \text{ou bem } x \leq y, \text{ ou bem } y \leq x.$$

Nesto caso, diz-se que o conjunto  $(X, \leq)$  é *totalmente ordenado*, ou *linearmente ordenado*.

**Definição B.1.16.** Uma relação é dita *pré-ordem* (*parcial*) se ela satisfaz os axiomas (1) e (3) da definição B.1.14. Usamos as pré-ordens algumas vezes no texto principal. Usualmente, *pré-ordem* significa uma pré-ordem total, ou seja, todos elementos de  $X$  são dois a dois comparáveis.

**Exemplo B.1.17.** A reta  $\mathbb{R}$ , munida da ordem usual, é totalmente ordenada.

**Exemplo B.1.18.** Seja  $X$  um conjunto qualquer. A família  $2^X$  das todas as partes de  $X$  é parcialmente ordenada pela relação da inclusão:

$$A \leq B \iff A \subseteq B.$$

Se  $|X| \geq 2$ , esta ordem não é total: existem sempre pelo menos dois sub-conjuntos  $A, B \subseteq X$  que não são comparáveis entre eles:

$$A \not\subseteq B \text{ e } B \not\subseteq A.$$

**Definição B.1.19.** Um conjunto totalmente ordenado  $(X, \leq)$  é dito ser *bem ordenado* se cada subconjunto não vazio,  $A \subseteq X$ , tem um elemento mínimo: existe  $a \in A$  tal que  $a \leq y$  para todos  $y \in A$ .

**Exemplo B.1.20.** O conjunto  $\mathbb{N}$  de números naturais é bem ordenado. Se  $A$  é um subconjunto não vazio de números naturais, escolha  $n \in A$  qualquer; o conjunto de todos  $a \in A$  com  $a \leq n$  é finito e não vazio, e um simples argumento indutivo mostra que ele contém o elemento menor,  $m$ . Este  $m$  é também o elemento menor de  $A$ .

**Exemplo B.1.21.** O conjunto  $\mathbb{Z}$  de números inteiros, munido da ordem usual, não é bem ordenado, porque o próprio  $\mathbb{Z}$  não tem um elemento mínimo.

**Exemplo B.1.22.** O conjunto vazio  $\emptyset$  munido da sua única ordem (uma relação vazia) é bem ordenado.

**Definição B.1.23.** Seja  $E$  um conjunto qualquer (finito ou infinito). Uma *permutação de  $E$*  é uma bijeção de  $E$  sobre si mesmo:

$$\sigma: E \rightarrow E.$$

O conjunto de todas as permutações de  $E$  é noté  $S_E$ . Se  $E$  é um conjunto finito da cardinalidade  $n$ , as permutações de  $E$  são ditas as *do posto  $n$* .

**Definição B.1.24.** Seja  $n$  um número inteiro natural. Na tradição combinatória, nota-se

$$[n] = \{1, 2, 3, \dots, n\}.$$

**Definição B.1.25.** O conjunto de permutações de  $[n]$  se nota  $S_n$ .

Dado uma permutação  $\sigma$  de  $[n]$ , obtemos uma ordem  $\preceq$  sobre  $[n]$ , definindo

$$i \preceq j \iff \sigma(i) \leq \sigma(j).$$

É fácil ver que  $\preceq$  é uma ordem total. O resultado seguinte mostra que toda ordem total sobre  $[n]$  vem deste modo da ordem usual, permutando os elementos de  $[n]$  entre eles.

**Teorema B.1.26.** *Dada uma ordem total qualquer,  $\preceq$ , sobre  $[n]$ , existe uma e uma só permutação  $\sigma \in S_n$  tal que, quaisquer sejam  $i, j \in [n]$ , temos*

$$i \preceq j \iff \sigma(i) \leq \sigma(j), \quad (\text{B.3})$$

onde  $\leq$  é a ordem usual sobre os números inteiros.

*Demonstração.* A propriedade na eq. (B.3) pode ser re-escrita da maneira equivalente como segue: quaisquer sejam  $i, j \in [n]$ ,

$$\sigma^{-1}(i) \preceq \sigma^{-1}(j) \iff i \leq j. \quad (\text{B.4})$$

Como 1 é o menor elemento de  $[n]$  na ordem usual,  $\sigma^{-1}(1)$  dever ser o menor elemento de  $[n]$  em relação à ordem  $\preceq$ . Então, não há escolha para  $\sigma^{-1}(1)$ : deve ser  $\sigma^{-1}(1) = \min\{[n], \preceq\}$ . Comme cada conjunto totalmente ordenado finito possui o mínimo, definemos

$$\sigma^{-1}(1) = \min\{[n], \preceq\}.$$

O número 2 é o mínimo de  $\{2, 3, \dots, n\}$ , e usando eq. (B.4), concluímos que  $\sigma^{-1}$  deve ser o menor elemento do conjunto ordenado  $([n], \preceq)$  menos  $\sigma^{-1}(1)$ . Definemos

$$\sigma^{-1}(2) = \min\{[n] \setminus \{\sigma^{-1}(1)\}, \preceq\}.$$

De modo recursivo, se as imagens de  $1, 2, \dots, k$  por  $\sigma^{-1}$  tinham sido escolhidas, definemos

$$\sigma^{-1}(k+1) = \min\{[n] \setminus \{\sigma^{-1}(1), \sigma^{-1}(2), \dots, \sigma^{-1}(k)\}, \preceq\}.$$

É claro que a função  $\sigma^{-1}: [n] \rightarrow [n]$  escolhida deste modo é injetora, porque a cada passo a imagem de  $k+1$  por  $\sigma^{-1}$  foi diferente dos valores já escolhidos para  $1, 2, 3, \dots, k$ . Como  $[n]$  é um conjunto finito,  $\sigma^{-1}$  é bijetora, é possui a aplicação inversa, que denotemos por  $\sigma$ .

Esta  $\sigma$  é uma permutação de  $[n]$ , que, segundo a sua definição, verifica a propriedade (B.4), logo a propriedade (B.3) também.

Para mostrar a unicidade de  $\sigma$ , notemos que a escolha de cada valor por  $\sigma^{-1}$  possuindo a propriedade (B.4) foi única.  $\square$

**Definição B.1.27.** Dado um número natural,  $n$ , o *fatorial* de  $n$ , denotado  $n!$ , é um número natural definido recursivamente como segue:

1.  $1! = 1$ , et

$$2. (n + 1)! = (n + 1)n!$$

Então, pode-se escrever:

$$n! = n(n - 1)(n - 2) \dots 3 \cdot 2 \cdot 1 = \prod_{i=1}^n i.$$

**Exercício B.1.28.**  $\#S_n = n!$ .

*Observação B.1.29.* O problema seguinte, chamado o *problema do caixeiro-viajante* (em inglês: *travelling salesman problem*, ou *TSP*), é provavelmente o mais importante problema em aberto da informática teórica moderna.

Dado  $n$  pontos (as “cidades”) e as distâncias dois a dois entre eles, o problema é, calcular, em tempo polinomial em  $n$ , a rota mais curta que visita todas as cidades uma única vez.

É claro que o problema pode ser resolvido enumerando todos os  $(n - 1)!$  caminhos possíveis e comparando-os dois a dois para escolher o mais curto. Mas este algoritmo vai exigir o tempo (número de operações) proporcional a  $(n - 1)!$ , que é uma quantidade enorme. Segundo a *fórmula de Stirling*,

$$n! \approx \sqrt{2\pi n} \left(\frac{n}{e}\right)^n.$$

Por exemplo,

$$100! \approx 9.3326 \cdot 10^{157}.$$

O algoritmo mais eficaz conhecido exige o tempo da ordem de grandeza  $2^n n^2$ , o que é exponencial em  $n$ .

## B.2 Sobre o sistema axiomático ZFC

### B.2.1 Sistema ZF

O que isso significa, provar um teorema? Na compreensão moderna, significa: deduzi-lo a partir de um conjunto de axiomas, usando uma coleção de ferramentas lógicas exatamente especificadas.

Os axiomas que têm mais ou menos toda a matemática atual baseada sobre eles, são os chamados axiomas ZFC da teoria dos conjuntos axiomática. Este axiomática remonta ao trabalho de Cantor, que foi o primeiro a propor uma coleção de axiomas que regem a teoria dos conjuntos. Mais tarde, sua axiomática foi corrigida e atualizada por Zermelo, Fraenkel, e Skolem. A origem da sigla ZFC é:

- **Z** para Ernst Zermelo,
- **F** para Adolf Abraham Fraenkel,

- C para Axioma de Escolha (Axiom of Choice).

Para dar uma ideia de como esses axiomas se parecem, deixe-me declarar alguns axiomas da lista original de 7 axiomas da teoria dos conjuntos propostos pelo próprio Georg Cantor.

**Axioma do Conjunto Vazio** Existe um conjunto, denotado  $\emptyset$ , que contém nenhum elemento:

$$\forall x, \neg(x \in \emptyset).$$

Aqui o símbolo  $\neg$  significa negação lógica. A notação mais familiar para  $\neg(x \in \emptyset)$  seria  $x \notin \emptyset$ .

**Axioma da Extensão** Dois conjuntos,  $x$  e  $y$ , são iguais se e somente se eles consistem dos mesmos elementos:

$$\forall x \forall y (x = y) \leftrightarrow \forall z (z \in x) \leftrightarrow (z \in y)$$

**Axioma do Par** Este axioma permite, a partir de dois conjuntos  $x, y$ , criar um novo conjunto,  $\{x, y\}$ , que contém exatamente dois elementos,  $x$  e  $y$ :

$$\forall x \forall y \exists z \forall t (t \in z) \leftrightarrow (t = x) \vee (t = y)$$

**Axioma da Potência** Dado um conjunto  $X$ , pode-se formar um novo conjunto cujos elementos são todos os subconjuntos de  $X$ . Este conjunto é chamado *conjunto potência* de  $X$  e denotado  $2^X$  ou  $2^X$ . Em notação lógica,

$$\forall x \exists y \forall z (z \in y) \leftrightarrow (z \subseteq x).$$

Aqui  $y \subseteq x$  é uma substituição para

$$\forall z (z \in y) \rightarrow (z \in x).$$

Um dos axiomas originais de Cantor tinha postulado que se pode formar novos conjuntos por suas propriedades. Isso é realmente o que estamos fazendo todos os dias quando fazemos matemática, e assim um axioma deste tipo é vital.

**Axioma de Compreensão** Seja  $\mathcal{P}$  uma propriedade de conjuntos que pode se exprimir em uma língua formal apropriada. Então a coleção de todos os conjuntos  $x$  que possuem a propriedade  $\mathcal{P}$ ,

$$\{x : \mathcal{P}(x)\},$$

é um conjunto.

No entanto, este axioma leva a problemas, que foi notado pela primeira vez em 1902 por Bertrand Russell. Esta contradição, conhecida como a *antinomia de Russell*, causou alguns problemas para as fundações axiomáticas nascentes da teoria dos conjuntos. Em essência, é simplesmente uma reformulação do bem-conhecido paradoxo do barbeiro.

**Antinomia de Russell** Seja  $\mathcal{P}$  a propriedade de um conjunto  $x$  seguinte:

$$x \notin x.$$

O Axioma de Compreensão permite formar o conjunto

$$A = \{x : x \notin x\}.$$

Pergunta:  $A$  é um elemento de si-mesmo? É claro que ambas possíveis respostas levam a uma contradição.

A antinomia levou à necessidade de formular a Axioma de Compreensão em uma maneira mais exata. Além disso, alguns outros axiomas foram adicionados. A primeira versão do axiomas que estava livre da antinomia de Russell e alguns outros paradoxos foi proposta por Zermelo em 1908. Foram introduzidas novas melhorias por Fraenkel em 1919 e Skolem em 1922. Observe que Cantor já morreu em 1918.

Os nove axiomas atuais incluem os axiomas que vimos acima, incluindo uma versão corrigida do Axioma da Compreensão (que não discutiremos), bem como, por exemplo, o seguinte.

**Axioma da Regularidade** Cada conjunto não vazio  $x$  contém um elemento que, visto como um conjunto, é disjunto de  $x$ :

$$\forall x, (\neg(x = \emptyset) \rightarrow \exists y (y \in x \wedge y \cap x = \emptyset)).$$

Pode-se mostrar que o Axioma da Regularidade é equivalente à não-existência de cadeias infinitas da forma

$$x_1 \ni x_2 \ni x_2 \ni \dots \ni x_n \ni \dots$$

Em particular, nenhum conjunto pode ser o seu próprio elemento:

$$\forall x, x \notin x.$$

**Axioma do Infinito** Existe um conjunto infinito. Eis uma forma econômica para exprimir isso:

$$\exists x (\emptyset \in x \wedge \forall y (y \in x \rightarrow \{y\} \in x)).$$

Em outras palavras, existe um conjunto  $X$  tendo a propriedade:

$$\emptyset \in X, \{\emptyset\} \in X, \{\{\emptyset\}\} \in X, \dots$$

## B.2.2 Axioma da Escolha

Axioma da escolha (AC) é, provavelmente, o mais controverso de todos os axiomas do sistema ZFC, e definitivamente o mais conhecido de todos: mesmo se um matemático for duramente pressionado para declarar exatamente os 8 axiomas restantes, ninguém vai ter qualquer problema afirmando o axioma da escolha.

AC afirma uma coisa muito simples: dada uma família de conjuntos não-vazios e dois a dois disjuntos,  $A_i$ , indexada com um conjunto de índices,  $I$ , pode-se formar um novo conjunto,  $B$ , que intercepta cada conjunto em nossa família em exatamente um ponto.

**Axioma da Escolha** Seja  $A_i, i \in I$  uma família de conjuntos não vazios, tal que  $A_i \cap A_j = \emptyset$  quando  $i \neq j$ . Existe um conjunto  $B$  tal que para cada  $i \in I$ , a interseção  $B \cap A_i$  é um conjunto unitário.

**Axioma da Escolha** (Forma B) Seja  $\gamma$  uma família qualquer dos conjuntos não vazios. Então existe uma função  $f: \gamma \rightarrow \cup \gamma$  (uma função de escolha) tal que, para todos  $A \in \gamma$ ,

$$f(A) \in A.$$

**Exercício B.2.1.** Verifique que as duas formas do Axioma da Escolha são equivalentes.

**Exercício B.2.2.** Verifique o Axioma da Escolha no caso onde  $\gamma$  é enumerável, usando a indução matemática.

O axioma da escolha parece tão natural que ele estava sendo usado implicitamente no século XIX, sem ser declarado explicitamente. No entanto, para conjuntos infinitos quaisquer AC não, de fato, siga do resto dos axiomas da ZF!

A primeira formulação de AC possivelmente pertence a Peano. Em 1904 o Axioma da Escolha foi “legitimada” por Zermelo, que provou o princípio da boa ordem (teorema B.3.14) usando Axioma da Escolha.

Assim, o sistema axiomático ZFC, em certo sentido, serve como base da matemática moderna. Quão sólido é essa base? Por exemplo, como podemos acertar que o sistema ZFC não leve a contradições, alguns resultados tipo  $0 = 1$ ? Em outras palavras, o sistema ZFC é *consistente*?

Paradoxalmente, não só não sabemos a resposta a esta pergunta, mas mesmo assumindo que ZFC é consistente, nunca seremos capazes de provar este fato! É uma consequência do famoso *teorema de Incompletude*, uma das contribuições fundamentais para a matemática do século XX feitas por Kurt Gödel. O teorema da incompletude diz que, dado um sistema axiomático, a afirmação “este sistema é consistente” (isto é, não leva a contradições) não pode ser provada *dentro do próprio sistema*.

E pode o axioma da escolha causar problemas por conta própria? Surpreendentemente — e este foi outra grande contribuição de Gödel — apesar de sua natureza controversa, a AC não acrescenta problemas adicionais aos fundamentos da matemática. É *relativamente consistente*:

**Teorema de Gödel da Consistência Relativa da AC** (1935) Se ZF é consistente, então ZFC é consistente.

Em outras palavras, se não houver contradição em ZF, então ZF mais o Axioma da Escolha também levará a nenhuma contradição. Se houver problemas com fundamentos da matemática, então é um problema com ZF, e o Axioma da Escolha não tem nada a ver com isso.



### B.2.3 Hipótese do Contínuo (CH)

Aqui está a famosa conjectura de Georg Cantor, um dos problemas mais famosos e influentes em toda a história da matemática:

**Hipótese do Contínuo (Continuum Hypothesis, CH)** (Georg Cantor, 1878). *Não existem números cardinais estritamente entre  $\aleph_0$  e  $c$ . A saber, se  $A$  é um subconjunto infinito da reta,  $\mathbb{R}$ , então ou  $|A| = \aleph_0$  ou  $|A| = c$ .*

David Hilbert considerou o problema da validade do CH para ser de tal grande importância que ele incluiu-o como problema 1 em sua lista de problemas matemáticos em seu discurso ao segundo Congresso Internacional de Matemáticos (ICM) em Paris em 1900.

Em 1937 Gödel provou talvez o seu maior resultado.

**Consistência da Hipótese do Contínuo.** (Kurt Gödel) *A Hipótese do Contínuo é consistente com ZFC. Em outras palavras, se ZF é consistente, então a lista dos axiomas de ZFC mais CH é consistente (não leva a contradições).*

Este resultado excluiu a possibilidade de que a Hipótese do Contínuo pudesse ser refutada. É geralmente considerado como “a primeira metade da solução para a Hipótese do Contínuo”.

A fim de ver a “segunda metade”, os matemáticos tiveram que esperar até 1963.

**Independência da Hipótese do Contínuo.** (Paul Cohen) *A Hipótese do Contínuo não pode ser provada a partir de axiomas ZFC. Em outras palavras, supondo que ZFC é consistente, se um acrescenta à lista de axiomas de ZFC a negação da Hipótese do Contínuo, então a lista resultante de axiomas,*

$$ZFC + \neg(CH),$$

*também é consistente.*

Assim, a Hipótese do Contínuo não pode ser provada nem desprovada no sistema axiomático ZFC. É *independente* de ZFC.

## B.3 Lema de Zorn

### B.3.1 Formulação

**Definição B.3.1.** Um elemento  $x$  de um conjunto parcialmente ordenado  $X$  é dito *maximal* se não existem nenhumas elementos estritamente maiores do que  $x$ :

$$\forall y \in X, \quad x \leq y \Rightarrow x = y.$$

**Exemplo B.3.2.** O elemento 1 é maximal no segmento  $[0, 1]$  munido da ordem usual.

**Exemplo B.3.3.** Seja  $V$  um espaço vetorial sobre um corpo  $\mathbb{K}$  qualquer. Fazemos  $\mathfrak{B}$  a família dos todos os sub-conjuntos linearmente independentes de  $V$ :

$$\begin{aligned} X \in \mathfrak{B} \iff X \subseteq V \text{ e } \forall n \in \mathbb{N}_+, \forall \lambda_i \in \mathbb{R}, \forall x_i \in X, \\ i = 1, 2, \dots, n, x_i \neq x_j \text{ para } i \neq j, \\ \text{se } \sum_{i=1}^n \lambda_i x_i = 0, \text{ então } \lambda_1 = \lambda_2 = \dots = \lambda_n = 0. \end{aligned}$$

O conjunto  $\mathfrak{B}$ , munido da relação da relação de inclusão, é parcialmente ordenado. Um elemento  $X \in \mathfrak{X}$  é maximal se e somente se  $X$  é uma base (isso é,  $X$  não é contido em nenhum conjunto linearmente independente estritamente maior).

*Observação B.3.4.* A noção de um elemento maximal é diferente desta de um elemento máximo. No exemplo precedente, não existe nenhuma elemento máximo.

**Definição B.3.5.** Um conjunto parcialmente ordenado e não vazio  $\mathfrak{X}$  é chamado *indutivo* se ele possui a propriedade seguinte. Seja  $\mathfrak{C} \subseteq \mathfrak{X}$  um sub-conjunto de  $\mathfrak{X}$  tal que a restrição da ordem sobre  $\mathfrak{C}$  é uma ordem total. Então  $\mathfrak{C}$  é majorado em  $\mathfrak{X}$ :

$$\exists x \in X \quad \forall c \in \mathfrak{C}, \quad c \leq x.$$

O resultado seguinte encontra-se entre aos instrumentos mais potentes e frequentemente utilizados da matemática moderna. A demonstração é deduzida do Axioma de Escolha (e é, de fato, uma forma equivalente dele).

**Teorema B.3.6** (Lema de Zorn). *Seja  $\mathfrak{X}$  conjunto não vazio parcialmente ordenado indutivo. Então  $\mathfrak{X}$  contém pelo menos um elemento maximal.*  $\square$

## B.3.2 Dedução do lema de Zorn do Axioma da Escolha

A nossa prova é uma das mais curtas em existência, seguindo [Weston 1957].

Seja  $\mathfrak{X}$  um conjunto parcialmente ordenado não vazio e indutivo. Mostremos a existência de um elemento maximal em  $\mathfrak{X}$ .

Para cada cadeia  $\mathcal{C} \subseteq \mathfrak{X}$ , denotemos por  $\widehat{\mathcal{C}}$  o conjunto des todos os majorantes de  $\mathcal{C}$  dentro  $\mathfrak{X}$  que não pertencem a  $\mathcal{C}$ :

$$\widehat{\mathcal{C}} = \{x \in \mathfrak{X} \setminus \mathcal{C} : \forall y \in \mathcal{C} \quad y \leq x\}.$$

Por exemplo,  $\widehat{\emptyset} = \mathfrak{X}$  (onde  $\emptyset$  é uma cadeia vazia). Com certeza, não pode se excluir a possibilidade do que  $\widehat{\mathcal{C}}$  seja vazio para algumas cadeias  $\mathcal{C}$ .

Denotemos

$$\gamma = \{\widehat{C}: C \text{ é uma cadeia dentro } \mathcal{X} \text{ t.q. } \widehat{C} \neq \emptyset\}.$$

Segundo AC, existe uma função de escolha

$$f: \gamma \rightarrow \bigcup \gamma,$$

tal que

$$\forall \widehat{C} \in \gamma, f(\widehat{C}) \in \widehat{C}.$$

Notemos que, se  $C$  é uma cadeia e  $\mathcal{H} \subseteq C$ , então  $\mathcal{H}$  é uma cadeia também. Digamos que uma cadeia  $C$  é uma  $f$ -cadeia se ela possui a propriedade seguinte. Qualquer seja  $\mathcal{H} \subseteq C$ , se  $\widehat{\mathcal{H}} \cap C \neq \emptyset$ , então  $f(\widehat{\mathcal{H}}) \in C$  e  $f(\widehat{\mathcal{H}})$  é o menor majorante de  $\mathcal{H}$  dentro  $C \setminus \mathcal{H}$ .

Por exemplo, pois  $\widehat{\emptyset} \cap C = C$ , toda  $f$ -cadeia contém o elemento  $f(\widehat{\emptyset})$ , que é o menor elemento de  $C$ . Existe sempre pelo menos uma  $f$ -cadeia não-vazia: o conjunto unitário  $\{f(\widehat{\emptyset})\}$ .

Se  $C$  é uma  $f$ -cadeia tal que  $\widehat{C} \neq \emptyset$ , então  $C \cup \{f(\widehat{C})\}$  é uma  $f$ -cadeia.

◁ Denotemos  $x = f(\widehat{C})$ . Seja  $\mathcal{H} \subseteq C$  um sub-conjunto tal que  $\widehat{\mathcal{H}} \cap (C \cup \{x\}) \neq \emptyset$ . Há dois casos a considerar. Se  $\mathcal{H} \cap C \neq \emptyset$ , então, como  $C$  é uma  $f$ -cadeia, temos  $f(\widehat{\mathcal{H}}) \in C \subseteq C \cup \{x\}$  e  $f(\widehat{\mathcal{H}})$  é o menor majorante de  $\mathcal{H}$  dentro  $C \setminus \mathcal{H}$ , logo dentro  $C \cup \{x\}$  também. Se  $\mathcal{H} \cap C = \emptyset$ , então  $\widehat{\mathcal{H}} \cap (C \cup \{x\}) = \{x\}$ , de onde concluímos:  $\widehat{\mathcal{H}} = \widehat{C}$ . Por conseguinte,  $f(\widehat{\mathcal{H}}) = f(\widehat{C}) = x$ , e a condição de ser uma  $f$ -cadeia é satisfeita. ▷

Sejam  $C$  e  $C'$  duas cadeias quaisquer. Então, ou  $C' \subseteq C$ , ou  $C \subseteq C'$ . No primeiro caso,  $C'$  é um segmento inicial de  $C$ , ou seja, se  $y, z \in C$ ,  $z \leq y$ , e  $y \in C'$ , então  $z \in C'$ .

◁ Suponha que  $C \setminus C' \neq \emptyset$ , e seja  $x \in C \setminus C'$  qualquer. Definemos

$$\mathcal{H} = \{y \in C \cap C': y \leq x\} \equiv \{y \in C \cap C': y < x\}.$$

Como  $x \in \widehat{\mathcal{H}} \cap C$ , temos  $\mathcal{H} \cap C \neq \emptyset$  e  $f(\widehat{\mathcal{H}}) \in C$  e por conseguinte  $f(\widehat{\mathcal{H}}) \leq x$ . Como  $\widehat{\mathcal{H}} \cap C' = \emptyset$ , temos  $f(\widehat{\mathcal{H}}) \notin C'$ , logo  $f(\widehat{\mathcal{H}}) \notin C'$ . Isso implica que necessariamente

$\widehat{\mathcal{H}} \cap \mathcal{C}' = \emptyset$ . Como nenhum elemento de  $\mathcal{C}'$  majora  $\mathcal{H}$ , e  $\mathcal{C}'$  é uma cadeia, concluímos que  $\mathcal{H}$  é *cofinal* dentro  $\mathcal{C}'$ , a saber,

$$\forall y \in \mathcal{C}' \exists z \in \mathcal{H} \ y \leq z,$$

et por conseguinte,

$$\forall y \in \mathcal{C}' \ y \leq x.$$

Concluímos:  $\mathcal{C}' \subseteq \mathcal{C}$ . Além disso, o argumento implica que  $y \in \mathcal{C}'$  e  $z \leq y$ , então  $z$  não pode pertencer a  $\mathcal{C} \setminus \mathcal{C}'$ . Por conseguinte,  $\mathcal{C}'$  é um segmento inicial de  $\mathcal{C}$ .  $\triangleright$

Em particular, a família de todas as  $f$ -cadeias é totalmente ordenada: em outras palavras, todas as  $f$ -cadeias são comparáveis duas a duas. Logo, a união

$$\mathcal{C}_0 = \bigcup \{ \mathcal{C} : \mathcal{C} \text{ est une } f\text{-cadeia} \}$$

é uma cadeia.

Cada  $f$ -cadeia  $\mathcal{C}$  é um segmento inicial da cadeia  $\mathcal{C}_0$ .

$\triangleleft$  Sejam  $x \in \mathcal{C}$  e  $y \in \mathcal{C}_0$  tais que  $y \leq x$ . Existe uma  $f$ -cadeia  $\mathcal{C}'$  tal que  $y \in \mathcal{C}'$ . Segundo B.3.2, uma das  $f$ -cadeias  $\mathcal{C}$  e  $\mathcal{C}'$  contém a outra. Se  $\mathcal{C}' \subseteq \mathcal{C}$ , então  $y \in \mathcal{C}' \subseteq \mathcal{C}$  e não tem nada a mostrar. Se  $\mathcal{C} \subseteq \mathcal{C}'$ , então, mais uma vez segundo B.3.2,  $\mathcal{C}$  forma um segmento inicial de  $\mathcal{C}'$ , de onde concluímos:  $y \in \mathcal{C}$ .  $\triangleright$

A cadeia  $\mathcal{C}_0$  é uma  $f$ -cadeia.

$\triangleleft$  Seja  $\mathcal{H} \subseteq \mathcal{C}_0$  uma cadeia tal que  $\widehat{\mathcal{H}} \cap \mathcal{C}_0 \neq \emptyset$ . Então, existe uma  $f$ -cadeia  $\mathcal{C}$  que tem uma interseção não-vazia com  $\widehat{\mathcal{H}}$ . Deduzimos duas coisas: primeiramente,  $\mathcal{H} \subseteq \mathcal{C}$  (graças a B.3.2), e além disso,  $\widehat{\mathcal{H}} \cap \mathcal{C} \neq \emptyset$ . Pois  $\mathcal{C}$  é uma  $f$ -cadeia, temos  $f(\widehat{\mathcal{H}}) \in \mathcal{C} \subseteq \mathcal{C}_0$ , e  $f(\widehat{\mathcal{H}})$  é o elemento menor de  $\widehat{\mathcal{H}} \cap \mathcal{C}$ . Como  $\mathcal{C}$  é um segmento inicial de  $\mathcal{C}h_0$ , concluímos que  $\widehat{\mathcal{H}} \cap \mathcal{C}h$  é um segmento inicial de  $\widehat{\mathcal{H}} \cap \mathcal{C}_0$ , e por conseguinte  $f(\widehat{\mathcal{H}})$  é o menor elemento de  $\widehat{\mathcal{H}} \cap \mathcal{C}$ .  $\triangleright$

$$\widehat{\mathcal{C}}_0 = \emptyset.$$

$\triangleleft$  Redução para o absurdo. Suponha que  $\widehat{\mathcal{C}}_0 \neq \emptyset$ , e notemos  $x = f(\widehat{\mathcal{C}}_0)$ . Segundo B.3.2,  $\mathcal{C}_0 \cup \{x\}$  é uma  $f$ -cadeia. Pois  $\mathcal{C}$  é a união de todas as  $f$ -cadeias, temos  $\mathcal{C} \cup \{x\} \subseteq \mathcal{C}$ , ou seja,  $x \in \mathcal{C}$ . Ao mesmo tempo,  $x \in \widehat{\mathcal{C}}_0$ , qual conjunto é disjuncto de  $\mathcal{C}_0$ .  $\triangleright$

Porque  $\mathcal{X}$  é indutivo, existe um majorante,  $x$ , para a cadeia  $\mathcal{C}_0$ . De acordo com B.3.2,  $x \in \mathcal{C}_0$ . Cada  $y$  tal que  $y > x$  seria um majorante para  $\mathcal{C}_0$  que não pertence a  $\mathcal{C}_0$ , o que é impossível segundo B.3.2. Isso significa que  $x$  é um elemento maximal de  $\mathcal{X}$ .  $\square$

**Exercício B.3.7.** Deduza o Axioma da Escolha do lema de Zorn.

[ *Sugestão:* considere o conjunto parcialmente ordenado  $\mathcal{X}$  que consiste de todas as funções de escolha parcialmente definidas sobre  $\gamma$ . ]

### B.3.3 Ilustração: existência de uma base num espaço vetorial

**Exemplo B.3.8.** O conjunto  $\mathfrak{B}$  dos sub-espços vetoriais do exemplo B.3.3 é indutivo.

Eis a verificação. Seja  $\mathfrak{C}$  uma família dos elementos de  $\mathfrak{B}$  totalmente ordenada pela relação de inclusão:

$$\forall A, B \in \mathfrak{C}, \quad A \subseteq B \text{ ou } B \subseteq A.$$

Portanto,  $A \cup B$  pertence a  $\mathfrak{C}$  para todos  $A, B \in \mathfrak{C}$ . Pela indução finita, qualquer sejam  $n \in \mathbb{N}$  e  $A_1, A_2, \dots, A_n \in \mathfrak{C}$ , temos  $\bigcup_{i=1}^n A_i \in \mathfrak{C}$ .

Fazemos  $X = \bigcup \mathfrak{C} = \bigcup \{A : A \in \mathfrak{C}\}$ . Vamos mostrar que  $X \in \mathfrak{B}$ , isso é,  $X$  é linearmente independente. Sejam  $n \in \mathbb{N}$ ,  $\lambda_i \in \mathbb{K}$ ,  $x_i \in X$ ,  $i = 1, 2, \dots, n$ , tais que  $x_i \neq x_j$  para  $i \neq j$ . Suponhamos que  $\sum_{i=1}^n \lambda_i x_i = 0$ . Existe  $A_i \in \mathfrak{C}$  tais que  $x_i \in A_i$ ,  $i = 1, 2, \dots, n$ . O conjunto  $A = \bigcup_{i=1}^n A_i$  pertencem a  $\mathfrak{C}$ , e por conseguinte  $A$  é linearmente independente. Deduzimos:  $\lambda_i = 0$  para todos  $i = 1, 2, \dots, n$ .

Eis uma aplicação do lema de Zorn.

**Teorema B.3.9.** *Cada espaço vetorial possui uma base.*

*Demonstração.* Seja  $V$  um espaço vetorial qualquer. A família  $\mathfrak{B}$  definida como o exemplo B.3.3 é indutiva (exemplo B.3.8). De acordo com o lema de Zorn, ele possui pelo menos um elemento maximal,  $X$ . Isto  $X$  é uma base de  $V$ .  $\square$

**Exercício B.3.10.** Mostrar teorema B.1.8. (*Sugestão:* aplique o lema de Zorn à família de todos as injeções parciais de  $X$  para  $Y$ , bem como de  $Y$  para  $X$ .)

### B.3.4 Princípio da boa ordem

Mesmo se  $\mathbb{Z}$  não é bem ordenado com sua ordem natural (usual), podemos dê-lhe uma boa ordem. Para obter essa ordem,  $<$ , organize os inteiros da seguinte maneira: primeiro, coloque todos os números naturais em sua ordem habitual, e depois disso, colocar todos os inteiros negativos em um ordem inversa:

$$0 < 1 < 2 < 3 < \dots < 10^{10} < \dots < -1 < -2 < -3 < \dots < -10^{10} < \dots$$

**Exercício B.3.11.** Mostre que a ordem  $<$  como acima é uma boa ordem, isto é,  $(\mathbb{Z}, <)$  é bem-ordenado.

Acontece que se pode construir uma boa ordem sobre qualquer conjunto, mesmo tendo uma propriedade mais forte.

**Definição B.3.12.** Seja  $(X, <)$  um conjunto totalmente ordenado. Um *segmento inicial* de  $X$  é qualquer subconjunto  $Y$  munida da ordem induzida de  $X$  e tal que, se  $y \in Y$  e  $z < y$ , então  $z \in Y$ .

**Definição B.3.13.** Uma boa ordem  $<$  sobre um conjunto  $X$  chama-se *minimal* se cada próprio segmento inicial de  $(X, <)$  tem a cardinalidade menor do que  $X$ .

**Teorema B.3.14** (Princípio da Boa Ordem; Zermelo, 1904). *Dado um conjunto qualquer,  $X$ , existe uma boa ordem minimal  $<$  sobre  $X$ .*  $\square$

**Exercício B.3.15.** Seja  $X$  um conjunto bem-ordenado. Mostrar que não existe nenhuma bijeção que preserva ordem entre  $X$  e um próprio segmento inicial de  $X$ .

**Exercício B.3.16.** Mostre a existência de uma boa ordem sobre qualquer conjunto usando o Lema de Zorn.

[ *Sugestão:* considere a família de todos os boas ordens (minimais) sobre sub-conjuntos de  $X$ , definindo uma ordem parcial entre eles de uma maneira cuidada, para usar o exercício acima. ]

**Exercício B.3.17.** Deduza que todo conjunto admite uma boa ordem minimal.

### B.3.5 Ultrafiltros

**Definição B.3.18.** Um *filtro* sobre um conjunto  $X$  qualquer é uma família  $\mathcal{F}$  (não vazia) dos subconjuntos não vazios de  $X$  tal que

1. se  $A, B \in \mathcal{F}$ , então  $A \cap B \in \mathcal{F}$ , e
2. se  $A \in \mathcal{F}$  e  $A \subseteq B \subseteq X$ , então  $B \in \mathcal{F}$ .

**Exemplo B.3.19.** Sejam  $X$  um espaço métrico (ou, mais geralmente, espaço topológico),  $x$  um ponto de  $X$ . A família  $\mathcal{N}(x)$  de todas as vizinhanças de  $x$  em  $X$  é um filtro.

**Exemplo B.3.20.** O *filtro de Fréchet* sobre um conjunto infinito  $X$  qualquer consiste de todos os subconjuntos de  $X$  cofinitos.

**Definição B.3.21.** Seja  $X$  um conjunto não vazio qualquer. Uma família  $\mathcal{F}$  de subconjuntos de  $X$  é chamada *centrada* se a interseção de cada sub-família finita de  $\mathcal{F}$  é não vazia:

$$\forall n, \forall F_1, F_2, \dots, F_n \in \mathcal{F}, \bigcap_{i=1}^n F_i \neq \emptyset.$$

**Exemplo B.3.22.** Cada filtro é uma família centrada.

É fácil verificar que a coleção das todas as famílias centradas sobre um conjunto não vazio  $X$ , ordenada pela inclusão, é indutiva. Como corolário de lema de Zorn, obtemos:

**Proposição B.3.23.** *Cada sistema centrado sobre um conjunto  $X$  qualquer é contido num sistema centrado maximal.*

**Definição B.3.24.** Uma sistema centrado maximal é dito *ultrafiltro*.

Eis um critério maior.

**Teorema B.3.25.** *Seja  $\mathcal{F}$  um sistema centrado sobre um conjunto não vazio  $X$ . Então  $\mathcal{F}$  é um ultrafiltro se e somente se, qualquer seja  $A \subseteq X$ , temos  $A \in \mathcal{F}$  ou  $A^c \in \mathcal{F}$ .*

*Demonstração.*  $\Rightarrow$ : suponhamos que  $\mathcal{F}$  é um ultrafiltro, e seja  $A \subseteq X$  um sub-conjunto qualquer. Se  $A$  encontra a interseção de cada sub-coleção finita de  $\mathcal{F}$ , então o sistema  $\mathcal{F} \cup \{A\}$  é centrada, e como  $\mathcal{F}$  é maximal, temos  $A \in \mathcal{F}$ . De mesmo modo, se  $A^c$  encontra a interseção de cada sub-coleção finita de  $\mathcal{F}$ , temos  $A^c \in \mathcal{F}$ . O caso onde nem  $A$ , nem  $A^c$  encontram a interseção de cada sub-coleção finita de  $\mathcal{F}$  é impossível: suponha a existência dos  $A_1, A_2, \dots, A_n, A_{n+1}, \dots, A_{n+m}$  tais que

$$A \cap A_1 \cap \dots \cap A_n = \emptyset, \quad A^c \cap A_{n+1}, \dots, A_{n+m} = \emptyset,$$

logo

$$\bigcap_{i=1}^n A_i \subseteq A^c, \quad \bigcap_{i=n+1}^{n+m} A_i \subseteq A,$$

e finalmente

$$\bigcap_{i=1}^{n+m} A_i \subseteq A \cap A^c = \emptyset,$$

a contradição com a hipótese que  $\mathcal{F}$  é centrada.

$\Leftarrow$ : Seja  $\mathcal{F}$  uma sistema centrada com a propriedade que para cada  $A \subseteq X$ , ou  $A \in \mathcal{F}$ , ou  $A^c \in \mathcal{F}$ . Seja  $\mathcal{F}'$  uma sistema centrada tal que  $\mathcal{F} \subseteq \mathcal{F}'$ . Se a inclusão é própria, obtemos uma contradição imediata: existe  $A \in \mathcal{F}' \setminus \mathcal{F}$ , e como  $A \notin \mathcal{F}$ , temos  $A^c \in \mathcal{F}$ . Os conjuntos  $A$  e  $A^c$  ambos pertencem ao sistema centrada  $\mathcal{F}'$ , que é impossível.  $\square$

*Observação B.3.26.* Evidentemente, “ou” no teorema B.3.25 é exclusivo.

**Corolário B.3.27.** *Seja  $\mathcal{U}$  um ultrafiltro sobre um conjunto  $X$ . Sejam  $A, B \subseteq X$  tais que  $A \cup B = X$ . Então ou  $A \in \mathcal{U}$ , ou  $B \in \mathcal{U}$ .*

*Demonstração.* Suponha que  $A \notin \mathcal{U}$  e  $B \notin \mathcal{U}$ . Segundo o teorema B.3.25, temos  $A^c \in \mathcal{U}$  e  $B^c \in \mathcal{U}$ , e por conseguinte

$$\emptyset = A^c \cap B^c \in \mathcal{U},$$

uma contradição.  $\square$

Pela indução matemática finita óbvia, obtemos:

**Corolário B.3.28.** *Sejam  $\gamma$  uma cobertura finita de um conjunto  $X$  e  $\mathcal{U}$  um ultrafiltro sobre  $X$ . Então existe  $A \in \gamma$  tal que  $A \in \mathcal{U}$ . Em outras palavras,*

$$\gamma \cap \mathcal{U} \neq \emptyset.$$

**Corolário B.3.29.** *Cada ultrafiltro é um filtro.*

*Demonstração.* Seja  $\mathcal{U}$  um ultrafiltro sobre um conjunto  $X$ . Sejam  $A, B \in \mathcal{U}$ . Se  $A \cap B \notin \mathcal{U}$ , então

$$A^c \cup B^c = (A \cap B)^c \in \mathcal{U},$$

e obtemos uma contradição com o fato que  $\mathcal{U}$  é uma família centrada, porque

$$A \cap B \cap (A^c \cup B^c) = \emptyset.$$

Concluimos:  $A \cap B \in \mathcal{U}$ .

De maneira semelhante, sejam  $A \in \mathcal{U}$  e  $A \subseteq B \subseteq X$ . Suponhamos que  $B \notin \mathcal{U}$ . Logo  $B^c \in \mathcal{U}$ , e  $A \cap B^c = \emptyset$ , a contradição.  $\square$





# *Espaços métricos. Teorema da categoria de Baire*

---

## C.1 Números reais

### C.1.1 Corpos ordenados

**Definição C.1.1.** Seja  $F$  um conjunto munido de duas operações binárias,  $+$  e  $\cdot$ , assim como dois elementos distinguidos,  $0$  e  $1$ . O sistema  $\langle F, +, \cdot, 0, 1 \rangle$  é dito um *corpo* se ele satisfaz os axiomas seguintes.

(F1)  $\forall a, b, c \in F, a + (b + c) = (a + b) + c$  (associatividade de adição).

(F2)  $\forall a, b \in F, a + b = b + a$  (comutatividade de adição).

(F3)  $\forall a \in F, a + 0 = a$ .

(F4)  $\forall a \in F, \exists -a : a + (-a) = 0$ .

(F5)  $\forall a, b, c \in F, a(bc) = (ab)c$  (associatividade de multiplicação)

(F6)  $\forall a, b \in F, ab = ba$  (comutatividade de multiplicação)

(F7)  $\forall a \in F, a \cdot 1 = a$ .

(F8)  $\forall a \neq 0, \exists a^{-1} : a \cdot a^{-1} = 1$ .

(F9)  $\forall a, b, c \in F, a(b + c) = ab + ac$  (distributividade)

**Exemplo C.1.2.** O sistema de números reais  $\mathbb{R}$  é um corpo.

**Exemplo C.1.3.** A totalidade de números racionais, ou seja, os reais que podem ser representados como um rácio de inteiros,  $p/q$ ,  $p, q \in \mathbb{Z}$ ,  $q \neq 0$ , forma um corpo sobre as operações usuais, o corpo de números racionais, denotado  $\mathbb{Q}$ .

**Exemplo C.1.4.** Para todo número primo  $p$ , pode-se formar um corpo, denotado  $\mathbb{Z}_p$  e chamado o *corpo de resíduos módulo  $p$* , ou simplesmente um *corpo finito com  $p$  elementos*. Os elementos de  $\mathbb{Z}_p$  são denotados  $0, 1, 2, \dots, p - 1$ , e a adição e multiplicação são executadas módulo  $p$ .

Relembramos que dois inteiros,  $m$  e  $n$ , são *iguais módulo  $p$*  (notação:  $m \equiv n \pmod{p}$ ), se  $m - n$  é um múltiplo de  $p$ .

**Exemplo C.1.5.** O corpo de números complexos,  $\mathbb{C}$ , consiste de todos os polinómios em uma variável  $i$  da forma  $z = a + bi$ , com coeficientes reais, e  $i$  é a *unidade imaginária*, tendo a propriedade  $i^2 = -1$ . O coeficiente  $a$  é dito a *parte real* de  $z$ , e  $b$  é a *parte imaginária* de  $z$ .

Adição e multiplicação dos números complexos são executadas como as dos polinómios, e a expressão  $i^2$  está depois substituída por  $-1$ . Para executar a divisão, definemos o *conjugado* de  $z$ ,  $\bar{z} = a - bi$ . Temos:

$$z\bar{z} = (a + bi)(a - bi) = a^2 + b^2 = |z|^2,$$

onde  $|z|$  à a norma euclidiana de  $z$ . Agora

$$\frac{z}{w} = \frac{z\bar{w}}{w\bar{w}} = \frac{1}{|w|^2}z\bar{w}.$$

**Exemplo C.1.6.** Dado um corpo  $F$  qualquer, formemos um novo corpo, denotado  $F(t)$  é chamado uma *extensão transcendental simples* de  $F$ , ou um *corpo de funções racionais sobre  $F$* . O corpo  $F(t)$  consiste de todas as expressões da forma

$$\frac{p(t)}{q(t)} \equiv \frac{a_0 + a_1t + a_2t^2 + \dots + a_mt^m}{b_0 + b_1t + b_2t^2 + \dots + b_nt^n},$$

onde  $p(t)$  e  $q(t)$  são (relativamente primos) polinómios em uma variável  $t$  com coeficientes de  $F$ . Em outras palavras, elementos de  $F(t)$  são *funções racionais* sobre  $F$ . As operações são executadas de modo usual.

**Definição C.1.7.** Seja  $F = \langle F, +, \cdot, 0, 1 \rangle$  um corpo, e seja  $\leq$  uma relação de ordem total sobre  $F$  (definição B.1.15). O sistema  $F = \langle F, +, \cdot, 0, 1, \leq \rangle$  é chamado um *corpo ordenado* se ele satisfaz

(OF1)  $\forall a, b, c \in F$ , se  $a \leq b$  então  $a + c \leq b + c$ .

(OF2)  $\forall a, b, c \in F$ , se  $a \leq b$  e  $0 \leq c$  então  $ac \leq bc$ .

**Exercício C.1.8.** Deduza dos axiomas de um corpo ordenado que, se  $a > 0$  e  $b > 0$ , então  $a + b > 0$ .

**Exemplo C.1.9.**  $\mathbb{R}$  é um corpo ordenado.

**Exemplo C.1.10.** O corpo de racionais,  $\mathbb{Q}$ , é um *sub-corpo ordenado* de  $\mathbb{R}$ .

**Exercício C.1.11.** Mostre que o corpo de números complexos,  $\mathbb{C}$ , não admite uma estrutura de corpo ordenado.

*Observação C.1.12.* Um corpo  $F$  é *formalmente real* se existe uma ordem  $\leq$  sobre  $F$  tornando-lo um corpo ordenado. O corpo  $\mathbb{C}$  não é formalmente real, enquanto o corpo  $\mathbb{R}$  é. Pode-se mostrar que um corpo  $F$  é formalmente real se e somente se  $-1$  não pode ser representado como uma soma finita de quadrados de elementos de  $F$  (teorema de Artin-Schreier, resolvendo um dos problemas de Hilbert, o décimo sétimo).

**Exercício C.1.13.** Um corpo finito  $F$  qualquer, inclusive  $\mathbb{Z}_p$ , não é formalmente real.

**Exemplo C.1.14.** O corpo  $F(t)$  de funções racionais com coeficientes em um corpo formalmente real,  $F$ , é formalmente real. Mostremos uma tal construção para o corpo  $\mathbb{Q}(t)$ .

Definamos o sinal de um polinômio,

$$p \equiv p(t) \equiv a_0 + a_1t + a_2t^2 + \cdots + a_nt^n,$$

como o sinal de  $p$  é igual ao sinal do primeiro coeficiente não nulo. Por exemplo,  $t > 0$ ,  $-2 + t + t^{11} < 0$ . O sinal de  $x = p/q$  é igual ao produto dos sinais de  $p$  e  $q$ . Por exemplo,

$$\frac{3 + t}{-11 - t + t^2 + t^{25}} < 0,$$

pois  $3 + t > 0$  e  $-11 - t + t^2 + t^{25} < 0$ .

Finalmente,  $x < y$  se e somente se  $y - x > 0$ .

**Exercício C.1.15.** Mostrar que a ordem linear definido sobre o corpo  $\mathbb{Q}(t)$  como acima satisfaz os axiomas de um corpo ordenado.

Quando munido da ordem acima, o corpo  $\mathbb{Q}(t)$  é as vezes denotado  $\mathbb{Q}(\alpha)$ , onde  $\alpha = t$ , mas este símbolo enfatiza o fato de que o campo está ordenado em um modo particular. O elemento  $\alpha$  é positivo ( $a_0 = 0, a_1 = 1 > 0$ ). e ao mesmo tempo, para todo número racional estritamente positivo  $\epsilon > 0$  temos

$$\alpha < \epsilon,$$

pois  $\alpha - \epsilon < 0$ , com  $a_0 = -\epsilon < 0$ ). De fato,  $|\alpha|$  é menor do que qualquer racional estritamente positivo. Tais elementos são chamados *infinitesimais*.

O elemento  $\alpha^{-1}$  é *infinitamente grande*: qualquer que seja um número racional  $r$ , temos  $\alpha^{-1} > r$ ;

$$\alpha^{-1} - r = \frac{1}{\alpha} - \frac{r}{1} = \frac{1 - r\alpha}{\alpha} > 0.$$

## C.1.2 Axioma de Dedekind

**Definição C.1.16.** Um conjunto  $X$  totalmente ordenado satisfaz a *propriedade de completude de Dedekind*, ou é *completo no sentido de Dedekind*, se todo subconjunto de  $X$  não vazio e limitado por cima tem um supremo.

Em outras palavras, se  $\emptyset \neq A \subseteq X$  e existe  $x \in X$  tal que

$$\forall a \in A, a \leq x,$$

então existe  $y = \sup A$ :

$$\forall a \in A, a \leq y, \text{ e se } \forall a \in A, a \leq z, \text{ então } y \leq z.$$

**Exemplo C.1.17.** O corpo  $\mathbb{Q}(\alpha)$  não é completo no sentido de Dedekind. O conjunto  $\mathbb{N}$  de números naturais é um subconjunto limitado por cima, por exemplo,

$$\forall n \in \mathbb{N}, n < \frac{1}{\alpha}.$$

Suponha agora que existe o supremo de  $\mathbb{N}$ ,  $s = \sup \mathbb{N}$ . Em particular,  $s$  é uma cota superior para  $\mathbb{N}$ , a saber,

$$\forall n \in \mathbb{N}, n \leq s,$$

logo

$$\forall n \in \mathbb{N}, n + 1 \leq s,$$

ou, de modo equivalente,

$$\forall n \in \mathbb{N}, n \leq s - 1 < s,$$

contradizendo a definição do supremo.

**Exemplo C.1.18.** O corpo  $\mathbb{Q}$  não é completo no sentido de Dedekind. O conjunto  $A$  de todos os elementos da forma

$$0, 0.1, 0.101, 0.101001, 0.1010010001, 0.101001000100001, \dots$$

é limitado por cima, porém não tem o supremo em  $\mathbb{Q}$ . É fácil a verificar que se o supremo existisse, sua expansão digital seria da forma

$$r = 0.101001000100001\dots,$$

um número irracional.

**Definição C.1.19.** Um *isomorfismo* entre dois corpos ordenados,  $K$  e  $F$ , é uma bijeção  $f: K \rightarrow F$  tal que  $f$  conserva adição, ou seja, para cada  $x, y \in K$  temos  $f(x + y) = f(x) + f(y)$ , multiplicação, ou seja, para  $f(xy) = f(x)f(y)$ , e a ordem, ou seja, se  $x < y$ , então  $f(x) < f(y)$ .

**Definição C.1.20.** Dois corpos ordenados,  $F$  e  $K$ , são *isomorfos* se existe um isomorfismo  $f: F \rightarrow K$ .

**Teorema C.1.21.** *A menos de isomorfismo, existe um e apenas um corpo ordenado completo no sentido de Dedekind. Ele é chamado o corpo dos reais e denotado  $\mathbb{R}$ .*

Idealmente, teríamos que começar com uma teoria de números naturais, definidos pelos axiomas de Peano:

**Definição C.1.22.** O sistema de números naturais,  $\mathbb{N}$ , é definido pelos *axiomas de Peano* seguintes.

1. Existe um elemento de  $\mathbb{N}$  denotado 0.
2. Cada elemento  $n \in \mathbb{N}$ , possui o *sucessor*,  $Sn \in \mathbb{N}$ .
3. Se  $m \neq n$ , então  $Sm \neq Sn$ .
4. O elemento 0 não é o sucessor de algum elemento.
5. (*Axioma de recorrência*). Seja  $P$  um subconjunto de  $\mathbb{N}$  tal que  $0 \in P$  e para cada  $n \in P$ ,  $Sn \in P$ . Então  $P = \mathbb{N}$ .

No entanto, só vamos esboçar uma construção de  $\mathbb{R}$  a partir de números racionais. Definamos

$$\mathbb{Q}_{>0} = \{r \in \mathbb{Q} : r > 0\},$$

o conjunto de números racionais estritamente positivos.

**Definição C.1.23.** O conjunto  $\mathbb{R}_{>0}$  consiste de todos os subconjuntos  $A$  de  $\mathbb{Q}_{>0}$  tais que

1. Quaisquer que sejam  $a \in A$  e  $x \in X$  com  $x \leq a$ , temos  $x \in A$  ( $A$  é um *intervalo inicial* de  $X$ ),
2.  $\emptyset \neq A \neq X$  ( $A$  é um subconjunto *próprio* de  $X$ ).
3.  $A$  não possui o máximo ( $A$  é um intervalo aberto).

**Exercício C.1.24.** Verifique que  $\mathbb{R}_{>0}$  é totalmente ordenado pela relação de inclusão:

$$A \leq A' \iff A \subseteq A'.$$

**Exercício C.1.25.** Sejam  $A, B \in \mathbb{R}_{>0}$ . Mostre que a soma conjuntística

$$A + B = \{a + b : a \in A, b \in B\}$$

pertence a  $\mathbb{R}_{>0}$ .

**Exercício C.1.26.** Verifique que a soma conjuntística define uma operação de adição comutativa e associativa.

**Exercício C.1.27.** Se  $A \leq B$ , então  $A + C \leq B + C$ .

**Exercício C.1.28.** Mostre que, se  $A \leq B$ , pode se definir a subtração

$$B - A = \mathbb{Q}_{>0} \cap \{b - a : b \in B, a \in A^c\},$$

de modo que

$$(B - A) + A = B.$$

**Definição C.1.29.** Definamos o produto conjuntístico dentro de  $\mathbb{R}_{>0}$  por

$$AB = \{ab : a \in A, b \in B\}.$$

**Exercício C.1.30.** Verifique que o produto  $AB$  pertence a  $\mathbb{R}_{>0}$  (satisfaz as propriedades na definição C.1.23). Depois, verifique que a multiplicação é comutativa e associativa, bem como distributiva em relação à adição:

$$\begin{aligned} A(B + C) &= \{a(b + c) : a \in A, b \in B, c \in C\} \\ &= \{ab + ac : a \in A, b \in B, c \in C\} \\ &= AB + AC. \end{aligned}$$

Finalmente, se  $A \leq B$  e  $C \in \mathbb{R}_{>0}$ , então

$$AC \leq BC.$$

O conjunto  $(0, 1)$  pertence a  $\mathbb{R}_{>0}$  e joga o papel da identidade multiplicativa.

**Exercício C.1.31.** Qualquer que seja  $A \in \mathbb{R}_{>0}$ ,

$$(0, 1) \cdot A = A.$$

A construção do inverso multiplicativo é um pouco mais complicada. Dado  $A \in \mathbb{R}_{>0}$ , formamos o conjunto de inversos do conjunto complementar,

$$(A^c)^{-1} = \{b^{-1} : b \in A^c\},$$

e removamos o mínimo deste conjunto (que sempre existe). Denotemos o conjunto resultante  $A^\S$ .

**Exercício C.1.32.**  $A \cdot A^\S = (0, 1)$ .

Agora definamos o sistema  $\mathbb{R}_{<0}$  de números estritamente negativos como uma cópia formal de  $\mathbb{R}_{>0}$ ,

$$\mathbb{R}_{<0} = \{-x : x \in \mathbb{R}_{>0}\}.$$

Munamos  $\mathbb{R}_{>0}$  de uma ordem,

$$-r < -t \iff t < r,$$

uma adição,

$$(-r) + (-t) = -(r + t),$$

assim como uma *multiplicação externa* que toma seus valores dentro de  $\mathbb{R}_{>0}$ :

$$(-r) \cdot (-t) = rt.$$

Finalmente, definamos o sistema  $\mathbb{R}$  como a união disjunta de  $\mathbb{R}_{>0}$ ,  $\mathbb{R}_{<0}$ , e o zero:

$$\mathbb{R} = \mathbb{R}_{<0} \cup \{0\} \cup \mathbb{R}_{>0}.$$

A ordem total é definido sobre  $\mathbb{R}$  por

$$-r < 0 < t.$$

A multiplicação é estendida sobre  $\mathbb{R}$  pela regra

$$r \cdot (-t) = -rt.$$

A adição será definida assim. Se  $r < t$ , então

$$(-r) + t = t - r$$

(a subtração sendo bem definida), e se  $r > t$ ,

$$(-r) + t = -(r - t).$$

Finalmente,

$$1 = (0, 1) \in \mathbb{R}_{>0}.$$

A verificação do que o sistema  $\mathbb{R} = \langle \mathbb{R}, +, \times, 0, 1, \leq \rangle$  forme um corpo ordenado não é difícil, é uma cadeia dos exercícios puramente técnicos. Verifiquemos o seguinte.

**Teorema C.1.33.** *O sistema  $\mathbb{R} = \langle \mathbb{R}, +, \times, 0, 1, \leq \rangle$  satisfaz o axioma de Dedekind.*

Seja  $X$  um subconjunto não vazio é limitado por cima: existe  $b \in \mathbb{R}$  tal que para todos  $x \in X$ , temos  $x \leq b$ . Escolhamos um elemento  $x_0 \in X$  qualquer. Denotemos

$$\hat{X} = \{x - x_0 + 1 : x \in X\}.$$

O conjunto  $\hat{X}$  contém o elemento  $x_0 - x_0 + 1 = 1$ , de onde concluímos

$$\hat{X} \cap \mathbb{R}_{>0} \neq \emptyset.$$

Além disso,  $\hat{X}$  é majorado por  $b' = b - x_0 + 1$ . Basta mostrar que  $\hat{X}$  possui um supremo,  $s$ , pois neste caso  $s + x_0 - 1$  será o supremo de  $X$ .

Referindo à nossa definição de  $\mathbb{R}_{>0}$ , definamos o conjunto

$$S = \bigcup_{A \in \hat{X}} A.$$

Este  $S$  é um subconjunto de  $\mathbb{Q}_{>0}$ . Como  $\hat{X} \neq \emptyset$ , concluímos que  $S \neq \emptyset$ . O conjunto  $\hat{X}$  est majorado por  $b'$ . Na interpretação conjuntística dos reais,

$$A \subseteq b'. \quad (\text{C.1})$$

Por conseguinte,  $\emptyset \neq (b')^c \subseteq A^c$ , de onde concluímos que  $A^c \neq \emptyset$ .

Sejam  $s \in S$  e  $x \in \mathbb{Q}_{>0}$  quaisquer tais que  $x \leq s$ . Existe  $A \in \hat{X}$  com  $s \in A$ . Este  $A$  é um intervalo inicial de  $\mathbb{Q}_{>0}$ , e por conseguinte

$$x \in A \subseteq S.$$

Agora suponha que  $S$  contém o elemento maximal,  $d \in \mathbb{Q}_{>0}$ :

$$d \in S \text{ e } \forall s \in S, s \leq d.$$

Então, existe  $A \in \hat{X}$  tal que  $d \in A$ , e como  $A \subseteq S$ , concluímos que  $d$  é o elemento máximo de  $A$ , o que é impossível.

As propriedades acima significam que  $S$  é um número real.

Qualquer que seja  $A \in \hat{X}$ ,

$$A \subseteq \bigcup \{B : B \in \hat{X}\} = S,$$

o que significa

$$A \leq S,$$

ou seja,  $S$  é um majorante de  $\hat{X}$ . Agora seja  $C$  um majorante qualquer de  $\hat{X}$ . Para todos  $A \in \hat{X}$ ,  $A \leq C$ , ou seja,  $A \subseteq C$ . Concluímos:

$$S = \bigcup \{A : A \in \hat{X}\} \subseteq C,$$

o que é interpretado como  $S \leq C$ . A demonstração do teorema [C.1.33](#) é terminada.

A unicidade de  $\mathbb{R}$  no teorema [C.1.21](#) a menos de um isomorfismo mais ou menos reproduz o argumento acima, a partir do fato seguinte.

**Exercício C.1.34.** Mostre que cada corpo ordenado contém o corpo de racionais,  $\mathbb{Q}$ , como um sub-corpo ordenado.



### C.1.3 Axioma de Arquimedes e propriedade de Cantor

**Definição C.1.35.** Um corpo ordenado  $K$  satisfaz o *axioma de Arquimedes*, ou é *arquimediano*, se, quaisquer que sejam  $x$  e  $y$  estritamente positivos, existe um número natural  $n$  tal que  $nx > y$ , ou seja,

$$\underbrace{x + x + x + \cdots + x}_{n \text{ vezes}} > y.$$

Se  $K$  não satisfaz o axioma de Arquimedes, ele é dito *não arquimediano*.

**Teorema C.1.36.** *Um corpo completo no sentido de Dedekind é arquimediano.*

**Exercício C.1.37.** Mostre o teorema pela contraposição, usando a mesma ideia que no exemplo C.1.17.

**Exemplo C.1.38.** O corpo  $\mathbb{Q}(\alpha)$  é não arquimediano: para cada  $n \in \mathbb{N}$ ,  $n\alpha < 1$ .

**Exemplo C.1.39.** Como o exemplo de  $\mathbb{Q}$  mostra, o axioma de Arquimedes não implica o axioma de Dedekind.

**Teorema C.1.40.** *O corpo de números reais possui a propriedade de interseção de Cantor: cada seqüência encaixada de intervalos fechados finitos tem a interseção não vazia. Se o comprimento dos intervalos converge para zero, a interseção consiste de um ponto.*

*Demonstração.* Seja  $[a_n, b_n]$ ,  $n \in \mathbb{N}_+$  uma seqüência encaixada,

$$a_1 \leq a_2 \leq \dots \leq a_n \dots \leq \dots b_n \dots b_2 \leq b_1.$$

O conjunto  $A = \{a_n : n \in \mathbb{N}\}$  é limitado por cima, logo possui o supremo  $c = \sup A$ . Em particular,  $c \leq b_n$  para todos  $n \in \mathbb{N}$ . Isso significa

$$\forall n \in \mathbb{N}, \quad a_n \leq c \leq b_n,$$

como desejado. Supondo que  $b_n - a_n \rightarrow 0$ , se  $d \in \bigcap_{n \in \mathbb{N}} [a_n, b_n]$ , então

$$|c - d| \leq b_n - a_n$$

para todos  $n$ , logo  $c = d$ . □

**Exemplo C.1.41.** O corpo ordenado  $\mathbb{Q}$  não satisfaz a propriedade de interseção de Cantor, como testemunhado pela seqüência de intervalos

$[0, 2]$ ,  $[0.1, 0.2]$ ,  $[0.101, 0.102]$ ,  $[0.101001, 0.101002]$ ,  $[0.1010010001, 0.1010010002]$ , ...

**Exemplo C.1.42.** O corpo ordenado  $\mathbb{Q}(\alpha)$  não satisfaz a propriedade de interseção de Cantor também: a interseção da seqüência encaixada

$$\left[ n\alpha, \frac{1}{n} \right], \quad n = 1, 2, \dots$$

é vazia.

*Observação C.1.43.* A propriedade de interseção de Cantor é mais fraca do que o axioma de Dedekind. Pode-se construir alguns corpos ordenados não-arquimedianos onde cada sequência encaixada de intervalos fechados tem uma interseção não vazia (tais corpos são ditos *esfericamente completos*), e ademais, nenhuma sequência enumerável converge para zero.

**Exercício C.1.44.** Mostre que o axioma de Dedekind é equivalente à propriedade de interseção de Cantor junto com o axioma de Arquimedes.

## C.2 Métricas, topologias, funções

### C.2.1 Espaços métricos

**Definição C.2.1.** Seja  $X$  um conjunto não vazio. Uma *métrica* sobre  $X$  é uma função

$$d: X \times X \rightarrow \mathbb{R}_+$$

que verifica os axiomas seguintes:

1.  $\forall x, y \in X, d(x, y) = 0$  se e somente se  $x = y$ .
2. (Simetria)  $\forall x, y \in X, d(x, y) = d(y, x)$ .
3. (Desigualdade triangular)  $\forall x, y, z \in X, d(x, z) \leq d(x, y) + d(y, z)$ .

**Exercício C.2.2.** Mostre que a positividade de valores de uma métrica é uma consequência imediata dos três axiomas.

**Definição C.2.3.** Um conjunto  $X$  não vazio qualquer, munido duma distância  $d$ , é chamado um *espaço métrico*. Em outros termos, um espaço métrico é um par  $(X, d)$ , onde  $d$  é uma métrica sobre o conjunto não vazio  $X$ .

Habitualmente, um espaço métrico é notado pela única letra  $X$ .

Os elementos de um espaço métrico são chamados os *pontos*, a fim de sublinhar a natureza geométrica dos objetos desse tipo.

**Exemplo C.2.4.** A distância dita *usual* sobre  $\mathbb{R}$  é dada pela fórmula

$$d(x, y) = |x - y|.$$

**Exemplo C.2.5.** Seja  $X$  um conjunto não vazio. A *métrica discreta*, ou *métrica zero-um*, sobre  $X$  é dada pela regra

$$d_{discr}(x, y) = \begin{cases} 1, & \text{se } x \neq y, \\ 0, & \text{se } x = y. \end{cases}$$

**Definição C.2.6.** Sejam  $X = (X, d)$  um espaço métrico,  $Y \subseteq X$  um sub-conjunto de  $X$  não vazio. A *restrição* de  $d$  sobre  $Y$ , notada  $d|_Y$ , é, com efeito, a restrição de  $d$  sobre o produto cartesiano  $Y \times Y$ , ou seja,

$$\forall x, y \in Y, \quad d|_Y(x, y) = d(x, y).$$

É óbvio que  $d|_Y$  é uma métrica sobre  $Y$ , chamada a *métrica* (ou *distância*) *induzida* sobre  $Y$  (de  $X$ ). O espaço métrico  $(Y, d|_Y)$  é dito *um sub-espaço métrico* de  $X$ . Cada sub-conjunto não vazio de um espaço métrico  $X$  define um sub-espaço métrico da maneira única.

**Exemplo C.2.7.** O espaço

$$\alpha\mathbb{N} = \left\{ \frac{1}{n} : n = 1, 2, 3, \dots \right\} \cup \{0\}$$

é munido da distância induzida da reta  $\mathbb{R}$ , ou seja, a distância entre dois pontos  $x, y \in \alpha\mathbb{N}$  é a mesma que no  $\mathbb{R}$ . Isso espaço consiste dos membros duma sequência convergente com o seu limite. Ele é chamado a *compactificação de Alexandroff* (ou a *compactificação por um ponto*) *de um conjunto enumerável*.

**Exemplo C.2.8.** O intervalo fechado

$$[0, 1] = \{x \in \mathbb{R} : 0 \leq x \leq 1\},$$

munida da distância usual (induzida da reta  $\mathbb{R}$ ), encontra-se entre aos exemplos mais importantes dos espaços métricos.

**Exemplo C.2.9.** O espaço métrico dos números racionais,

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0 \right\}$$

munido da função distância usual, é um sub-espaço métrico da reta.

**Exemplo C.2.10.** O espaço vetorial real da dimensão  $n$ ,

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \dots \times \mathbb{R}}_{n \text{ vezes}}$$

munido da *distância euclideana usual*:

$$d(x, y) = \sqrt{\sum_{i=1}^n |x_i - y_i|^2}.$$

Os axiomas 1 e 2 são óbvios, enquanto o axioma 3 exige uma démonstração.

**Definição C.2.11.** Recordemos que o *produto escalar padrão* de dois vetores no  $\mathbb{R}^n$  é dado pela fórmula

$$(x, y) = \sum_{i=1}^n x_i y_i.$$

O produto escalar tem as propriedades seguintes verificadas facilmente.

**Proposição C.2.12.** 1.  $(x, x) \geq 0$  e  $(x, x) = 0$  se e somente se  $x = 0$ .

2.  $(x, y) = (y, x)$ .

3.  $(x + y, z) = (x, z) + (y, z)$ .

4.  $(\lambda x, y) = \lambda(x, y)$ .

Quaisquer que sejam  $x, y \in \mathbb{R}^n$ , temos

$$d(x, y) = \sqrt{(x - y, x - y)}.$$

A desigualdade triangular pela distância euclideana é uma consequência imediata do teorema seguinte.

**Teorema C.2.13** (Desigualdade de Minkowski). *Para todos  $x, y \in \mathbb{R}^n$  temos*

$$\sqrt{(a + b, a + b)} \leq \sqrt{(a, a)} + \sqrt{(b, b)}.$$

A fim de mostrar a desigualdade de Minkowski, precisamos de um outro resultado.

**Teorema C.2.14** (Desigualdade de Cauchy–Schwarz). *Para todos  $x, y \in \mathbb{R}^n$  temos*

$$|(x, y)|^2 \leq (x, x)(y, y).$$

*Demonstração.* Sejam  $x, y \in \mathbb{R}^n$  dois vetores quaisquer. Para todos  $t \in \mathbb{R}$  temos

$$0 \leq (tx + y, tx + y) = t^2(x, x) + 2t(x, y) + (y, y).$$

Por conseguinte, o polinômio do grau 2 em  $t$ ,

$$t^2(x, x) + 2t(x, y) + (y, y),$$

tem um raiz no máximo. Isto quer dizer que o discriminante do polinômio é negativo,

$$[2(x, y)]^2 - 4(x, x)(y, y) \leq 0,$$

ou seja

$$|(x, y)|^2 = (x, y)^2 \leq (x, x)(y, y).$$

□

Demonstração do teorema C.2.13.

$$\begin{aligned}
 (x + y, x + y) &= (x, x) + (x, y) + (y, x) + (y, y) \\
 &= (x, x) + (x, y) + (x, y) + (y, y) \\
 &= (x, x) + 2(x, y) + (y, y) \\
 &\leq (x, x) + 2|(x, y)| + (y, y) \\
 (\text{após Cauchy-Schwarz}) &\leq (x, x) + 2\sqrt{(x, x)}\sqrt{(y, y)} + (y, y) \\
 &= [\sqrt{(x, x)} + \sqrt{(y, y)}]^2,
 \end{aligned}$$

o que implica o resultado desejado.  $\square$

**Exemplo C.2.15.** Notaremos  $\ell^\infty$  o conjunto de todas as seqüências limitadas dos números reais,  $x = (x_n)_{n \in \mathbb{N}_+}$ ,  $x_n \in \mathbb{R}$ . (Recordemos que uma seqüência infinita  $(x_n)$  é dita *limitada* se existe um número real  $L \geq 0$  tal que para todos  $n = 1, 2, 3, \dots$  temos  $|x_n| \leq L$ ).

O valor da distância

$$d_\infty(x, y) = \sup_{n \in \mathbb{N}_+} |x_n - y_n|$$

entre duas seqüências  $x, y \in \ell^\infty$  é bem definido porque  $x$  e  $y$  são limitadas, bem como a sua diferença  $x - y$ . A verificação dos axiomas de uma métrica para  $d_\infty$  será deixada como exercício. Esta métrica  $d_\infty$  é chamada a métrica do tipo  $\ell^\infty$ , ou a métrica uniforme.

**Exemplo C.2.16.** O espaço de Baire, notado  $\mathbb{Z}^\omega$ , consiste de todas as seqüências infinitas dos números inteiros  $x = (x_1, x_2, \dots, x_n, \dots)$ , onde  $x_i \in \mathbb{Z}$ ,  $i = 1, 2, \dots$ . O valor da distância entre as duas seqüências,

$$x = (x_1, x_2, \dots, x_n, \dots)$$

e

$$y = (y_1, y_2, \dots, y_n, \dots),$$

é dado pela expressão seguinte:

$$d(x, y) = \begin{cases} 0, & \text{se } x = y, \\ 2^{-\min\{i: x_i \neq y_i\}}, & \text{se } x \neq y. \end{cases}$$

Por exemplo, a distância entre os elementos

$$(1, 2, 3, 4, 5, \dots, n, \dots)$$

e

$$(1, 2, 3, 0, 0, 0, 0, \dots, 0, \dots)$$

é igual a  $1/8$ .

Os axiomas 1 e 2 são praticamente evidentes. A fim de verificar a desigualdade triangular, sejam  $x, y, z$  três pontos em  $\mathbb{Z}^\omega$ . O nosso objetivo é mostrar que

$$d(x, z) \leq d(x, y) + d(y, z). \quad (\text{C.2})$$

Se pelo menos dois entre os elementos  $x, y, z$  são iguais, então a desigualdade (C.2) é verificada da maneira trivial. Por conseguinte, pode-se supor que todas as seqüências  $x, y, z$  são distintas.

Denotemos  $i$  o menor número inteiro tal que (i) para todos  $j < i$  temos  $x_j = y_j = z_j$ , e (ii) os inteiros  $x_i, y_i, z_i$  não são todos iguais. Um tal  $i$  existe após a hipótese. Agora é óbvio o que  $d(x, z) \leq 2^{-i}$ . Logo, o número à esquerda da equação (C.2) é menor ou igual a  $2^{-i}$ . Ao mesmo tempo, pelo menos um entre os números  $d(x, y)$  e  $d(y, z)$  à direita é igual a  $2^{-i}$ . (Se não, então  $x_i = y_i$  e  $y_i = z_i$ , por conseguinte  $x_i = y_i = z_i$ , o que contradiz a escolha de  $i$ ).

## C.2.2 Espaços ultramétricos

*Observação C.2.17.* Com efeito, o argumento acima mostra que a métrica sobre o espaço de Baire satisfaz a *desigualdade triangular forte*:

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}. \quad (\text{C.3})$$

**Definição C.2.18.** Uma métrica é chamada *ultramétrica* se ela satisfaz a desigualdade (C.3). Um conjunto munido de uma ultramétrica é dito *espaço ultramétrico*.

**Exemplo C.2.19.** O espaço métrico cuja métrica é a métrica zero-um é ultramétrico.

**Exemplo C.2.20.** Segundo observação C.2.17, o espaço de Baire é um espaço ultramétrico.

## C.2.3 Conjuntos abertos

**Definição C.2.21.** Sejam  $(X, d)$  um espaço métrico,  $x$  um ponto no  $X$ , e  $\epsilon > 0$ . A *bola aberta de centro  $x$  e raio  $\epsilon$*  é o conjunto

$$B_\epsilon(x) := \{y \in X : d(x, y) < \epsilon\} \subseteq X.$$

**Exemplo C.2.22.** Num espaço métrico  $(X, d)$  munido da distância zero-um, cada bola aberta é igual ou ao espaço inteiro ou a um conjunto unitário.

**Definição C.2.23.** Seja  $X$  um espaço métrico. Um sub-conjunto  $V$  de  $X$  é dito *aberto* no  $X$  se para cada ponto  $x$  de  $V$  existe um valor  $\epsilon > 0$  tal que a bola  $B_\epsilon(x)$  é contida no  $V$ .

**Exercício C.2.24.** Cada bola aberta é um conjunto aberto.

**Proposição C.2.25.** *Seja  $(X, d)$  um espaço métrico. Então:*

1. O conjunto vazio  $\emptyset$  e o espaço  $X$  são abertos no  $(X, d)$ .
2. A interseção de dois abertos é aberto. Por conseguinte, se  $V_1, \dots, V_k$  são abertos, então  $\bigcap_{i=1}^k V_i$  é aberto.
3. A união  $V = \bigcup_{\alpha \in A} V_\alpha$  dum família dos abertos é aberta.

*Observação C.2.26.* A família  $\mathcal{T}$  de todos os abertos de um espaço métrico  $X$  é chamada a *topologia* de  $X$ . As três propriedades acima são escolhidas como os axiomas de um *espaço topológico*, que é uma noção mais geral do que a noção de espaço métrico.

**Definição C.2.27.** Sejam  $X = (X, d)$  um espaço métrico,  $A$  um sub-conjunto de  $X$ , e  $x$  um ponto no  $A$ . Suponhamos que existe um  $\epsilon > 0$  tal que  $x \in B_\epsilon(x) \subseteq A$ . Então  $x$  é chamado um *ponto interior* de  $A$ , enquanto  $A$  é chamado uma *vizinhança* de  $x$ .

*Observação C.2.28.* A vizinhança de um ponto não é necessariamente um conjunto aberto em  $X$ .

**Definição C.2.29.** Uma parte  $A$  de um conjunto  $X$  é chamada de *cofinita* se o seu complemento  $A^c = X \setminus A$  é finito.

**Proposição C.2.30.** Cada parte cofinita de um espaço métrico qualquer é aberta.

*Demonstração.* Exercício. □

**Proposição C.2.31.** Cada bola aberta num espaço ultramétrico é um conjunto fechado.

*Demonstração.* Sejam  $X$  um espaço ultramétrico,  $x \in X$ , e  $\epsilon > 0$ . Se  $y \notin B_\epsilon(x)$ , escolhemos  $\delta > 0$  qualquer tal que  $\delta < \epsilon$ . Suponhamos que existe  $z \in B_\epsilon(x) \cap B_\delta(y)$ . Então temos

$$d(x, y) \leq \max\{d(x, y), d(y, z)\} \leq \max\{d(x, y), \delta\} < \epsilon,$$

logo  $y \in B_\epsilon(x)$ , a contradição. Concluímos:  $B_\epsilon(x)$  e  $B_\delta(y)$  são disjuntas, isto é, o complemento da bola  $B_\epsilon(x)$  é uma vizinhança de  $y$ . □

**Exercício C.2.32.** Verdadeiro ou falso: cada bola fechada num espaço ultramétrico é um conjunto aberto?

**Definição C.2.33.** Seja  $X$  um espaço métrico. Um ponto  $x \in X$  é dito *isolado* se o conjunto unitário  $\{x\}$  é aberto no  $X$ .

**Exemplo C.2.34.** Num espaço métrico  $X$  munido da distância zero-um cada ponto é isolado.

**Exemplo C.2.35.** Cada elemento com exceção de 0 é isolado no espaço métrico  $\alpha\mathbb{N}$ .

**Exercício C.2.36.** Mostre que um subconjunto,  $A$ , de  $\alpha\mathbb{N}$  é aberto se é somente se ou  $A$  não contem zero, ou  $A$  é cofinito. (As duas propriedades não são mutualmente exclusivas). C.2.30.

## C.2.4 Interior

**Definição C.2.37.** Sejam  $(X, d)$  um espaço métrico e  $A$  um subconjunto de  $X$ . O *interior* de  $A$ , notado  $\text{Int}_X A$  ou simplesmente  $\text{Int } A$ , é um sub-conjunto de  $X$  que consiste de todos os pontos interiores de  $A$ :

$$\text{Int}_X A = \{x \in A : \exists \epsilon > 0 \ B_\epsilon(x) \subseteq A\}.$$

Às vezes utiliza-se o símbolo  $\overset{\circ}{A}$ .

*Observação C.2.38.* Seja  $X$  um espaço métrico. Uma parte  $A$  de  $X$  é aberta se e somente se  $A = \text{Int}_X A$ . É uma consequência imediata das definições.

**Exemplo C.2.39.** O interior de cada espaço métrico  $X$  em si mesmo é  $X$ :

$$\text{Int}_X X = X.$$

Por exemplo,

$$\text{Int}_{\mathbb{Q}} \mathbb{Q} = \mathbb{Q}.$$

**Exemplo C.2.40.** O interior do mesmo conjunto  $\mathbb{Q}$  formado no espaço métrico  $\mathbb{R}$  é vazio:

$$\text{Int}_{\mathbb{R}} \mathbb{Q} = \emptyset.$$

Em outras palavras, nenhum intervalo aberto não vazio,  $(a, b)$ , dos números reais não está contido em  $\mathbb{Q}$ : existe pelo menos um ponto irracional no intervalo  $(a, b)$ .

## C.2.5 Métricas equivalentes

**Definição C.2.41.** Duas métricas  $d$  e  $d'$  sobre um conjunto  $X$  são *equivalentes* se elas geram a mesma topologia: um subconjunto  $A$  de  $X$  é aberto no espaço métrico  $(X, d)$  se e somente se ele é aberto no espaço  $(X, d')$ .

**Exemplo C.2.42.** A métrica zero-um sobre  $\mathbb{R}$  não é equivalente à métrica usual, por que o conjunto unitário  $\{0\}$  é aberto no espaço  $(\mathbb{R}, d_{0-1})$ , mas não é aberto no espaço  $\mathbb{R}$  relativo à métrica usual.

**Exercício C.2.43.** A métrica usual (induzida do  $\mathbb{R}$ ) sobre o espaço  $\alpha\mathbb{N}$  não é uma ultramétrica:

$$d(0, 1) = 1 > \frac{1}{2} = \max\{d(0, 1/2), d(1/2, 1)\}.$$

Verifique que a regra seguinte define uma ultramétrica equivalente:  $d(x, x) = 0$  para cada  $x$ , e se  $x \neq y$ , então  $d(x, y) = \max\{x, y\}$ .

**Exercício C.2.44.** Seja  $(X, d)$  um espaço métrico qualquer. Mostre que a fórmula

$$\tilde{d}(x, y) = \min\{d(x, y), 1\}$$

define uma métrica equivalente sobre  $X$ .



## C.2.6 Conjuntos fechados

**Definição C.2.45.** Digamos que uma parte  $F$  de um espaço métrico  $X$  é *fechada* em  $X$  (ou:  $F$  é um *fechado*), se o complemento  $F^c = X \setminus F$  é aberto.

**Exemplo C.2.46.** Cada conjunto unitário  $\{x\}$ ,  $x \in X$  é fechado num espaço métrico  $X$  qualquer.

**Exemplo C.2.47.** No espaço métrico  $\mathbb{R}$  dos números reais munido da distancia usual  $d(x, y) = |x - y|$ , todo intervalo fechado

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}$$

é um sub-conjunto fechado de  $\mathbb{R}$ .

*Observação C.2.48.* Uma parte  $A$  de um espaço métrico pode ser ao mesmo tempo aberta e fechada, as dual propriedades não são mutualmente exclusivas.

**Exercício C.2.49.** Sejam  $X$  um espaço métrico qualquer,  $Y \subseteq X$  um sub-espaço métrico de  $X$ . Se  $V \subseteq X$  é aberto (fechado) em  $X$ , então a interseção  $V \cap Y$  é aberta (respectivamente, fechada) em  $Y$ .

**Exemplo C.2.50.** Sejam  $a, b \in \mathbb{R} \setminus \mathbb{Q}$ ,  $a < b$ . No espaço  $\mathbb{Q}$  dos números racionais, denotemos

$$A = \{x \in \mathbb{Q} : a < x < b\}.$$

Então a parte  $A$  é ao mesmo tempo aberta e fechada em  $\mathbb{Q}$ . Ela é aberta por que

$$A = \mathbb{Q} \cap (a, b),$$

graças ao Exercício C.2.49. Da mesma maneira, como

$$A = \mathbb{Q} \cap [a, b],$$

concluimos que  $A$  é fechado em  $\mathbb{Q}$ .

**Definição C.2.51.** Seja  $X = (X, d)$  um espaço métrico. A *bola fechada* de raio  $r > 0$  em torno de  $x \in X$  é o conjunto definido por

$$\bar{B}_r(x) = \{y \in X : d(x, y) \leq r\}.$$

**Exercício C.2.52.** Cada bola fechada é um conjunto fechado.

**Teorema C.2.53.** *Seja  $X = (X, d)$  um espaço métrico qualquer.*

1.  $X$  é o conjunto vazio  $\emptyset$  são fechados.
2. A união de dois conjuntos fechados é fechado.

3. A interseção de uma família não vazia qualquer de fechados é um fechado.

**Definição C.2.54.** A esfera de raio  $r > 0$  centrada em  $x \in X$  é o conjunto

$$S_r(x) = \{y \in X : d(x, y) = r\}.$$

**Exemplo C.2.55.** Cada esfera é um conjunto fechado, sendo a interseção de dois fechados:

$$S_r(x) = \bar{B}_r(x) \cap B_r(x)^c.$$

## C.2.7 Aderência

**Definição C.2.56.** Uma sequência  $(x_n)$  de pontos de um espaço métrico  $(X, d)$  é dita convergente para o limite  $x \in X$  se

$$\forall \epsilon > 0 \exists n_0 \forall n \geq n_0 \quad d(x_n, x) < \epsilon.$$

Em outras palavras, cada bola aberta em torno de  $x$  contém todos os membros da sequência excepto um número finito. Simbolicamente:

$$\lim_{n \rightarrow \infty} x_n = x,$$

ou

$$x_n \xrightarrow{n \rightarrow \infty} x.$$

**Definição C.2.57.** Sejam  $X$  um espaço métrico,  $A$  um subconjunto de  $X$ . Um ponto  $x$  de  $X$  é chamado um ponto aderente de  $A$  (em  $X$ ) se existe uma sequência  $(a_n)$  dos pontos de  $A$  que converge para  $x$ :

$$\lim_{n \rightarrow \infty} a_n = x.$$

**Exemplo C.2.58.** Seja  $A$  um subconjunto não vazio qualquer da reta  $\mathbb{R}$ . Suponhamos que  $A$  seja limitado superiormente. Então o supremo  $b = \sup A$  de  $A$  é um ponto aderente a  $A$ . De mesmo para o ínfimo  $\inf A$ .

**Proposição C.2.59.** Um ponto  $x$  de um espaço métrico qualquer  $X$  é um ponto aderente de uma parte  $A$  de  $X$  se e somente se toda vizinhança de  $x$  tem pontos em comum com  $A$ .

*Demonstração.* Exercício. □

**Definição C.2.60.** A aderência, ou o fecho, de uma parte  $A$  de um espaço métrico  $X$  é o conjunto de todos os pontos aderentes de  $A$ . A aderência é denotada por  $\bar{A}$  ou, se quer-se sublinhar o espaço âmbito, por  $\bar{A}^X$ . (A notação alternativa e bastante popular:  $\text{cl } A$ , ou  $\text{cl}_X(A)$ , da palavra inglesa "closure" para a aderência.)

**Teorema C.2.61.** O "operador da aderência" possui as propriedades seguintes:

1.  $\bar{\emptyset} = \emptyset.$

2.  $A \subseteq \bar{A}.$

3. se  $A \subseteq B$ , então  $\bar{A} \subseteq \bar{B}.$

4.  $\bar{\bar{A}} = \bar{A}.$

*Demonstração.* Exercício. □

*Observação C.2.62.* As propriedades (1)-(4) podem ser usados como axiomas de um espaço topológico (axiomas de Kuratowski).

**Teorema C.2.63.** *Uma parte  $A$  de um espaço métrico é fechada se e somente se  $\bar{A} = A$ .*

*Demonstração.*  $\Rightarrow$ : se a parte  $A$  é fechada, então o complemento  $A^c$  é aberto e para cada  $x \in A^c$  existe  $\epsilon > 0$  com a propriedade  $B_\epsilon(x) \subseteq A^c$ . Logo, a bola  $B_\epsilon(x)$  não contém nenhum ponto de  $A$ , e por conseguinte  $x$  não é aderente a  $A$ . Concluimos: todos os pontos aderentes a  $A$  já pertencem a  $A$ . De acordo com a afirmação (2) do teorema C.2.61,  $\bar{A} = A$ .

$\Leftarrow$ : Suponhamos que  $\bar{A} = A$ . Seja  $x \in A^c$  um ponto qualquer. Então  $x$  não é aderente a  $A$ , e pode-se escolher um número real  $\epsilon > 0$  tal que  $B_\epsilon(x) \cap A = \emptyset$ . Segue-se que o complemento  $A^c$  é aberto. □

**Corolário C.2.64.** *A aderência  $\bar{A}$  de qualquer conjunto  $A$  é um conjunto fechado.*

*Demonstração.* De acordo com o teorema C.2.61(3), temos  $\bar{\bar{A}} = \bar{A}$ . □

**Corolário C.2.65.** *A aderência de um conjunto  $A$  é o menor fechado contendo  $A$ .*

*Demonstração.* Se  $A$  é um sub-conjunto de fechado qualquer,  $F$ , então

$$\bar{A} \subseteq \bar{F} = F$$

(teorema C.2.63).

Ao mesmo tempo,  $\bar{A}$  é fechado (corolário C.2.64). Concluimos:  $\bar{A}$  é um fechado que contém  $A$  e que é contido em cada fechado contendo  $A$ . □

### C.2.8 Partes densas

**Definição C.2.66.** Uma parte  $A$  de um espaço métrico qualquer  $X$  é dita *densa*, se

$$\bar{A} = X.$$

*Observação C.2.67.* As condições seguintes são (evidentemente) equivalentes:

1.  $A$  é denso em  $X$ .
2. Cada ponto de  $X$  é aderente a  $A$ .
3. Cada aberto não vazio de  $X$  encontra  $A$ , ou seja, contém algum ponto de  $A$ .
4. Para todos  $x \in X$  e todos  $\epsilon > 0$ , a bola  $B_\epsilon(x)$  contém algum ponto de  $A$ .

**Exemplo C.2.68.** O conjunto  $\mathbb{Q}$  dos números racionais é denso na reta  $\mathbb{R}$ . Este fato é conhecido como *teorema da densidade*. Sejam  $a, b \in \mathbb{R}$ ,  $a < b$ . De acordo com a propriedade de Arquimedes, existe um  $n \in \mathbb{N}_+$  tal que

$$\frac{1}{n} < b - a.$$

Por conseguinte, entre os números racionais

$$\frac{k}{n}, \quad k \in \mathbb{Z},$$

ao menos um é contido no intervalo  $(a, b)$ . Se não, podem escolher dois números consecutivos,  $\frac{k}{n}$  e  $\frac{k+1}{n}$ , tais que

$$\frac{k}{n} \leq a, \quad \text{enquanto} \quad \frac{k+1}{n} \geq b,$$

que não é possível graças a escolha de  $n$ : a quantidade  $1/n$  é demasiado pequena para “atravessar a racha (o intervalo  $[a, b]$ ) de um salto”!

### C.2.9 Espaços separáveis

**Definição C.2.69.** Um espaço métrico  $X$  é dito *separável* se existe um sub-conjunto  $A \subseteq X$  enumerável e denso:

$$A = \{a_n : n = 1, 2, \dots\}, \quad \bar{A} = X.$$

**Exemplo C.2.70.** Cada espaço métrico enumerável tal que  $\alpha\mathbb{N}$  ou  $\mathbb{Q}$  é obviamente separável.

**Exemplo C.2.71.** A reta  $\mathbb{R}$  é separável: o conjunto enumerável  $\mathbb{Q}$  dos números racionais é denso em  $\mathbb{R}$ .

**Exemplo C.2.72.** O espaço euclidiano  $\mathbb{R}^n$  é separável: por exemplo, o conjunto  $\mathbb{Q}^n$  que consiste de todos os vetores cujas coordenadas são racionais é enumerável e denso.

**Exemplo C.2.73.** Um espaço métrico munido com a função distância zero-um é separável se e somente se  $X$  é enumerável. (Exercício.)

**Teorema C.2.74.** Cada sub-espaço métrico de um espaço métrico separável é separável.

*Demonstração.* Seja  $X$  um espaço separável e seja  $Y \subseteq X$  um sub-espaço. Escolhamos uma parte denumerável e denso em  $X$ ,

$$A = \{a_n : n = 1, 2, 3, \dots\}.$$

Seja  $y_0 \in Y$  um elemento qualquer. Para cada  $m = 1, 2, 3, \dots$ , escolhamos um ponto  $b_{n,m}$ , onde

$$\begin{cases} b_{n,m} \in B_{1/m}(a_n) \cap Y, & \text{se a bola } B_{1/m}(a_n) \text{ encontra } Y, \\ b_{n,m} = y_0, & \text{se não.} \end{cases}$$

O conjunto

$$B = \{b_{n,m} : n, m = 1, 2, 3, \dots\}$$

é contido em  $Y$ . Ele é evidentemente enumerável. Basta verificar que  $B$  é denso em  $Y$ . Sejam  $y \in Y$  e  $\epsilon > 0$ . Existe  $m$  tal que

$$\frac{1}{m} < \frac{\epsilon}{2}.$$

Como  $A$  é denso em  $X$ , existe  $n$  tal que  $a_n \in B_{1/m}(y)$ . Por conseguinte, a bola  $B_{1/m}(a_n)$  encontra  $Y$  (ela contém  $y$ , por exemplo). Concluimos: o ponto  $b_{n,m} \in B$  é contido em  $B_{1/m}(a_n)$ , e portanto

$$d(y, b_{n,m}) \leq d(y, a_n) + d(a_n, b_{n,m}) < \frac{1}{m} + \frac{1}{m} = \frac{2}{m} < \epsilon.$$

Isto significa que a interseção  $B_\epsilon(y) \cap B$  é não vazia.  $\square$

*Observação C.2.75.* O resultado acima (teorema C.2.74) não é verdadeiro para os espaços topológicos mais gerais.

**Proposição C.2.76.** O espaço métrico  $\ell^\infty$  contém um subespaço métrico  $A$  de cardinalidade do contínuo e tal que a métrica induzida sobre  $A$  é uma métrica zero-um.

*Demonstração.* Cada sequência binária

$$\epsilon_1 \epsilon_2 \epsilon_3 \dots, \quad \epsilon_i \in \{0, 1\},$$

é obviamente limitada, logo pertence a  $\ell^\infty$ . Denotemos  $A$  o conjunto de todas tais sequências. Sejam  $a, b \in A$ ,  $a \neq b$ . Existe  $n$  tal que  $a_n \neq b_n$ , de onde

$$|a_n - b_n| = 1,$$

e por conseguinte

$$d_\infty(a, b) = \sup_{i \in \mathbb{N}} |a_i - b_i| = 1.$$

De acordo com Exemplo B.1.12, a cardinalidade de  $A$  é igual à cardinalidade de  $\mathbb{R}$ .  $\square$

**Corollary C.2.77.** *O espaço métrico  $\ell^\infty$  não é separável.*

*Demonstração.* Combinemos exemplo C.2.73 com teorema C.2.74.  $\square$

**Exercício C.2.78.** Mostrar que cada sequência num espaço métrico possui no máximo um limite.

**Teorema C.2.79.** *Seja  $X$  um espaço métrico separável. Então*

$$|X| \leq 2^{\aleph_0}.$$

*Demonstração.* Escolhamos um sub-espaço  $Y$  denso e enumerável. Denotemos  $\mathcal{C}$  o conjunto de todas as sequências dos pontos de  $Y$  que são convergentes em  $X$ . A aplicação que associa à sequência  $(y_n)$  o seu único limite é uma sobrejeção de  $\mathcal{C}$  sobre  $X$ . O conjunto  $Y^{\mathbb{N}}$  de todas as sequências dos pontos de  $Y$  (convergentes e não) contém  $\mathcal{C}$  como um subconjunto. Então,

$$|X| \leq |\mathcal{C}| \leq |Y^{\mathbb{N}}|.$$

Basta mostrar que  $|Y^{\mathbb{N}}| \leq |\mathbb{R}|$ . Como o conjunto  $Y$  é enumerável, ele pode ser identificado com um subconjunto de  $\mathbb{N}$ , e a nossa tarefa é de mostrar que

$$|\mathbb{N}^{\mathbb{N}}| \leq |\mathbb{R}|.$$

Basta produzir uma injeção de  $\mathbb{N}^{\mathbb{N}}$  em  $2^{\mathbb{N} \times \mathbb{N}}$ . Associemos a cada sequência  $(n_1, n_2, \dots, n_k, \dots)$  de números naturais o seu gráfico:

$$A = \{(n, a_n) : n \in \mathbb{N}\}.$$

É evidente que a correspondência acima é injetora: cada função é unicamente determinada pelo seu gráfico.  $\square$

### C.2.10 Imagens diretas e imagens recíprocas

*Observação C.2.80.* Sejam  $f: X \rightarrow Y$  uma aplicação entre dois conjuntos quaisquer,  $A \subseteq X$  e  $B \subseteq Y$  sub-conjuntos quaisquer. A *imagem* de  $A$  por  $f$  é o conjunto

$$f(A) = \{f(a) : a \in A\} \subseteq Y,$$

e a *imagem inversa*, ou *recíproca*, de  $B$  por  $f$  é o conjunto

$$f^{-1}(B) = \{x \in X : f(x) \in B\} \subseteq X.$$

*Observação C.2.81.* A imagem inversa  $f^{-1}(B)$  é o maior subconjunto  $A$  de  $X$  que possui a propriedade seguinte:

$$f(A) \subseteq B.$$

### C.2.11 Aplicações contínuas em um ponto

**Definição C.2.82.** Seja  $f$  uma aplicação entre dois espaços métricos,  $X$  e  $Y$ , e seja  $x \in X$ . Digamos que  $f$  é *contínua em  $x$*  se

$$\forall \epsilon > 0, \exists \delta > 0, \forall y \in X, (d_X(x, y) < \delta) \Rightarrow (d_Y(f(x), f(y)) < \epsilon,$$

ou, da maneira equivalente e um pouco mais econômica,

$$\forall \epsilon > 0, \exists \delta > 0, f(B_\delta(x)) \subseteq B_\epsilon(f(x)).$$

**Proposição C.2.83** (Critério sequencial da continuidade). *Uma aplicação  $f: X \rightarrow Y$  é contínua em um ponto  $x \in X$  se e somente se para cada seqüência  $(x_n)$  de pontos de  $X$  que converge para  $x$ , a seqüência das imagens  $(f(x_n))$  converge para  $f(x)$ .*

*Demonstração.*  $\Rightarrow$ : suponhamos que  $f$  é contínua no ponto  $x$ , e seja  $(x_n)$  uma seqüência tal que  $x_n \rightarrow x$  quando  $n \rightarrow \infty$ . Seja  $\epsilon > 0$  qualquer. Escolhamos  $\delta > 0$  da maneira que

$$f(B_\delta(x)) \subseteq B_\epsilon(f(x)).$$

Como  $(x_n)$  tenha  $x$  com o limite, existe um número natural,  $N$ , tal que

$$\forall n \geq N, x_n \in B_\delta(x).$$

Concluimos:

$$f(x_n) \rightarrow f(x) \text{ quando } n \rightarrow \infty.$$

$\Leftarrow$ : por contraposição. Suponhamos que  $f$  é descontínua no ponto  $x$ . Logo,

$$\exists \epsilon > 0, \forall \delta > 0, \exists y \in B_\delta(x), f(y) \notin B_\epsilon(f(x)).$$

Fixemos um tal  $\epsilon > 0$ . Para cada  $n = 1, 2, 3 \dots$  encontremos um ponto  $x_n \in X$  tal que

$$d_X(x_n, x) < \frac{1}{n} \text{ e } f(x_n) \notin B_\epsilon(f(x)).$$

A seqüência  $(x_n)$  converge para  $x$ , enquanto a seqüência  $(f(x_n))$  não converge para  $f(x)$ .  $\square$

## C.2.12 Aplicações contínuas

**Definição C.2.84.** Uma aplicação  $f$  entre dois espaços métricos  $X$  e  $Y$  é dita *contínua* se  $f$  é contínua em cada ponto  $x \in X$ . Em outras palavras,

$$\forall x \in X, \forall \epsilon > 0, \exists \delta > 0, \forall y \in X, (d_X(x, y) < \delta) \Rightarrow (d_Y(f(x), f(y)) < \epsilon).$$

**Teorema C.2.85.** *Seja  $f: X \rightarrow Y$  uma aplicação entre dois espaços métricos quaisquer. As condições seguintes são equivalentes:*

1.  $f$  é contínua.
2. Para cada  $x \in X$  e cada vizinhança  $V$  de  $f(x)$ , a imagem inversa  $f^{-1}(V)$  é uma vizinhança de  $x$ .
3. A imagem inversa,  $f^{-1}(V)$ , de cada aberto,  $V$ , de  $Y$  é aberta em  $X$ .
4. A imagem inversa,  $f^{-1}(F)$ , de cada fechado,  $F$ , de  $Y$  é fechada em  $X$ .
5. Para cada parte  $A \subseteq X$ , temos

$$f(\overline{A}) \subseteq \overline{f(A)}.$$

*Demonstração do Teorema C.2.85 “em sentido anti-horário”.* (1)  $\Rightarrow$  (5): Seja  $x \in \overline{A}$ . Então  $x$  é um ponto de aderência de  $A$ , logo existe uma sequência  $(a_n)$  dos pontos de  $A$  convergente para  $x$ . A função  $f$  é contínua em ponto  $x$ , e devido ao critério sequencial da continuidade, temos

$$f(a_n) \rightarrow f(x).$$

Concluimos:  $f(x)$  pertence à aderência de  $f(A)$  pois  $f(a_n) \in f(A)$ .

(5)  $\Rightarrow$  (4): seja  $G$  um subconjunto fechado de  $Y$ . Seja  $B = f^{-1}(G)$ . Então  $B$  é o maior subconjunto de  $X$  tal que  $f(B) \subseteq G$  (Observação 3.3.2). Segundo (4), temos

$$f(\overline{B}) \subseteq \overline{f(B)} \subseteq \overline{G} = G,$$

logo  $\overline{B} \subseteq B$ , e  $B = f^{-1}(G)$  é fechado em  $X$ .

(4)  $\Rightarrow$  (3): se  $V$  é um subconjunto aberto de  $Y$ , então

$$f^{-1}(V) = f^{-1}(Y \setminus V) = X \setminus f^{-1}(Y \setminus V),$$

e o conjunto  $f^{-1}(Y \setminus V)$  é fechado em  $X$  graças à hipótese (4).

(3)  $\Rightarrow$  (2): Seja  $V$  uma vizinhança de  $f(x)$  em  $Y$ . Escolhamos  $\epsilon > 0$  tal que  $B_\epsilon(f(x)) \subseteq V$ . O conjunto  $f^{-1}(B_\epsilon(f(x)))$  é aberto em  $X$  e contém  $x$ , logo é uma vizinhança de  $x$  em  $X$ .

(2)  $\Rightarrow$  (1): A bola  $B_\epsilon(f(x))$  é uma vizinhança de  $f(x)$  em  $Y$ , logo  $f^{-1}(B_\epsilon(f(x)))$  é uma vizinhança de  $x$  em  $X$ . Existe  $\delta > 0$  com  $B_\delta(x) \subseteq f^{-1}(B_\epsilon(f(x)))$ . Concluimos:

$$f(B_\delta(x)) \subseteq B_\epsilon(f(x)),$$

o que implica a continuidade de  $f$  em  $x$ . □



### C.2.13 Aplicações Lipschitz contínuas

**Definição C.2.86.** Uma função  $f : X \rightarrow Y$  entre dois espaços métricos é dita *Lipschitz contínua* se existe uma constante  $L \geq 0$  (*constante de Lipschitz de  $f$* ) tal que

$$\forall x, y \in X \quad d_Y(f(x), f(y)) \leq L \cdot d_X(x, y).$$

*Observação C.2.87.* Cada aplicação Lipschitz contínua é contínua. (Exercício.)

**Exemplo C.2.88.** A função contínua

$$f(x) = x^2$$

de  $\mathbb{R}$  a  $\mathbb{R}$  não é Lipschitz contínua. Seja  $L \geq 0$  qualquer. Seja  $x > L$  e  $y = x + 1$ . Temos

$$|f(x) - f(y)| = y^2 - x^2 = (x + 1)^2 - x^2 = 2x + 1 > L.$$

Concluimos: nenhum valor  $L \in \mathbb{R}$  é uma constante de Lipschitz para  $f$ .

**Exemplo C.2.89.** Sejam  $X$  um espaço métrico e  $x_0 \in X$ . A *função distância* de  $x_0$ , dada por

$$d_{x_0}(y) = d(x_0, y),$$

é Lipschitz contínua, com a constante de Lipschitz 1. (Exercício.)

**Exercício C.2.90.** Mais geralmente, sejam  $X$  um espaço métrico e  $A \subseteq X$  um subconjunto não vazio qualquer. A *função distância* de  $A$ , notada  $d_A$ , é dada pela fórmula seguinte:

$$d_A(x) = \inf_{a \in A} d(x, a).$$

Mostrar que a função  $d_A : X \rightarrow \mathbb{R}$  é Lipschitz contínua, com a constante de Lipschitz 1. (Para solução, veja a prova do lema 1.1.27.)

### C.2.14 Topologia produto

**Definição C.2.91.** Dada uma família de conjuntos  $X_i, i \in I$ , definamos o produto cartesiano como o conjunto de todas as funções

$$\begin{aligned} x : I &\rightarrow \cup_{i \in I} X_i, \\ i &\mapsto x_i \end{aligned}$$

tais que

$$\forall i \in I, \quad x_i \in X_i.$$

Notação do produto cartesiano:  $\prod_{i \in I} X_i$ .

**Definição C.2.92.** Dado  $i \in I$ , definamos a  $i$ -ésima projeção do produto  $\prod_{i \in I} X_i$  sobre  $X_i$  pela formula

$$\pi_i(x) = x_i.$$

**Definição C.2.93.** Se  $X_i, i \in I$  é uma família enumerável (finita ou infinita) de espaços métricos,  $|I| \leq \aleph_0$ , digamos que uma métrica  $d$  sobre o produto cartesiano  $\prod_{i \in I} X_i$  induz a topologia produto se qualquer sequência  $(x_n)$  de elementos do produto converge para um elemento  $x$  se e somente se, para todo  $i \in I$ ,

$$\pi_i(x_n) \rightarrow \pi_i(x).$$

**Exercício C.2.94.** Mostre que a condição acima é equivalente à condição seguinte: a família de conjuntos abertos do espaço métrico  $(\prod_{i \in I} X_i, d)$  é a menor topologia (família de conjuntos satisfazendo as propriedades na proposição C.2.25) tal que todas as projeções  $\pi_i, i \in I$  são contínuas.

Em outras palavras, a topologia produto é a menor topologia que contém todos os conjuntos da forma

$$\pi_i^{-1}(V), \quad i \in I, \quad V \text{ é aberto em } X_i.$$

**Exercício C.2.95.** Sejam  $(X_i, d_i), i \in I$  espaços métricos,  $|I| \leq \aleph_0$ . Mostrar que a métrica no produto dada por

$$d(x, y) = \sum_{i \in I} \frac{1}{2^n} \min\{d_i(x_i, y_i), 1\}$$

gera a topologia produto sobre  $\prod_{i \in I} X_i$ .

**Exercício C.2.96.** Sejam  $X_i, i \in \mathbb{N}$  espaços métricos finitos quaisquer (logo, discretos). Mostra que a métrica no produto dada por

$$d(x, y) = \begin{cases} 0, & \text{se } x = y, \\ 2^{-\min\{i : x_i \neq y_i\}}, & \text{se } x \neq y, \end{cases}$$

gera a topologia produto sobre  $\prod_{i \in \mathbb{N}} X_i$ .

### C.2.15 Imersões isométricas

**Definição C.2.97.** Uma aplicação  $i : X \rightarrow Y$  entre dois espaços métricos é dita *imersão isométrica* quando para quaisquer  $x, y \in X$  tivermos

$$d_Y(i(x), i(y)) = d_X(x, y).$$

*Observação C.2.98.* Sejam  $X$  um espaço métrico qualquer e  $Y \subseteq X$  um sub-espaço métrico dele. Então, como no exemplo precedente, a aplicação idêntica

$$Y \ni y \mapsto i(y) = y \in X$$

é uma imersão isométrica de  $Y$  em  $X$ .

### C.2.16 Imerção de Kuratowski

**Lema C.2.99.** Se  $X$  é um espaço métrico qualquer e  $x, y \in X$  dois pontos de  $X$ , então

$$\sup_{z \in X} |d_x(z) - d_y(z)| = d(x, y),$$

onde  $d_x$  é a função distância de  $x$ .

*Demonstração.* A desigualdade  $\leq$  é uma consequência da desigualdade triangular: para cada  $z \in X$ , temos

$$|d_x(z) - d_y(z)| = \max\{d_x(z) - d_y(z), d_y(z) - d_x(z)\} \leq d(x, y).$$

Para mostrar a desigualdade  $\geq$ , notemos que a igualdade é atingida no ponto  $z = x$ :

$$|d_x(x) - d_y(x)| = |0 - d(y, x)| = d(x, y).$$

□

**Exemplo C.2.100.** Seja  $\Gamma$  um conjunto qualquer. Generalizemos o exemplo C.2.15, e definamos o espaço métrico  $\ell^\infty(\Gamma)$  como o conjunto de todas as aplicações limitadas

$$x: \Gamma \ni \gamma \mapsto x_\gamma \in \mathbb{R},$$

munido da métrica

$$d_\infty(x, y) = \sup_{\gamma \in \Gamma} |x_\gamma - y_\gamma|.$$

Por exemplo, se  $\Gamma = \mathbb{N}_+$ , então  $\ell^\infty(\Gamma) = \ell^\infty$ .

*Observação C.2.101.* Se  $X = (X, d)$  é um espaço métrico, vamos denotar o espaço  $\ell^\infty(\Gamma)$  onde  $\Gamma = X$  por  $\ell^\infty(|X|)$ , para sublinhar que o conjunto de coordenadas do espaço é o conjunto subjacente do espaço  $X$ .

**Definição C.2.102.** Seja  $A$  um sub-conjunto de um espaço métrico  $X$  qualquer. O *diâmetro* de  $A$  é dado pela fórmula

$$\text{diam}(A) = \inf\{r \in [0, +\infty]: \forall a, b \in A, d(a, b) \leq r\}.$$

**Exercício C.2.103.** Mostrar que para cada sub-conjunto  $A$  não vazio temos

$$\text{diam}(A) = \sup_{a,b \in A} d(a, b).$$

**Exercício C.2.104.** Mostrar que para um espaço métrico  $X$  as definições seguintes são equivalentes:

1.  $X$  é limitado, ou seja, o diâmetro de  $X$  é finito.
2. Para cada  $x \in X$ , a função distância  $d_x: X \rightarrow \mathbb{R}$  é limitada.
3. Existe  $x \in X$  tal que a função distância  $d_x: X \rightarrow \mathbb{R}$  é limitada.

**Definição C.2.105.** Um sub-conjunto  $A$  de um espaço métrico  $X$  é dito *limitado* se  $A$  satisfaz uma das condições equivalentes de exercício C.2.104.

**Proposição C.2.106.** *Seja  $X$  um espaço métrico limitado. Então a fórmula seguinte define uma imersão isométrica de  $X$  em  $\ell^\infty(|X|)$ :*

$$X \ni x \mapsto i(x) = d_x \in \ell^\infty(|X|).$$

(Essa imersão é chamada a imersão de Kuratowski.)

*Demonstração.* Graças ao exercício C.2.104, cada função  $d_x$  pertence a  $\ell^\infty(|X|)$ . E graças ao lema C.2.99, temos, para quaisquer que sejam  $x, y \in X$ ,

$$\begin{aligned} d_\infty(i(x), i(y)) &= \sup_{z \in X} |d_x(z) - d_y(z)| \\ &= d_X(x, y). \end{aligned}$$

□

*Observação C.2.107.* Em caso geral, a função  $d_x$  não é limitada, e a construção acima deve ser modificada.

**Teorema C.2.108.** *Seja  $X$  um espaço métrico qualquer. Escolhamos um ponto  $x_0 \in X$ . A fórmula seguinte define uma imersão isométrica de  $X$  em  $\ell^\infty(|X|)$ :*

$$X \ni x \mapsto i(x) = d_x - d_{x_0} \in \ell^\infty(|X|).$$

(Esta imersão é também uma versão da imersão de Kuratowski.)

*Demonstração.* Seja  $x \in X$ . A função  $i(x) = d_x - d_{x_0}$  é limitada, graças à desigualdade triangular: qualquer que seja  $z \in M$ , temos

$$|d_x(z) - d_{x_0}(z)| \leq d(x, x_0).$$

Agora, sejam  $x, y \in X$  quaisquer. Temos:

$$\begin{aligned} d_\infty(i(x), i(y)) &= \sup_{z \in X} |(d_x(z) - d_{x_0}(z)) - (d_y(z) - d_{x_0}(z))| \\ &= \sup_{z \in X} |d_x(z) - d_y(z)| \\ &= d(x, y) \end{aligned}$$

(lema C.2.99). □

**Lema C.2.109.** *Sejam  $f$  uma função real limitada sobre um espaço métrico  $X$  e  $Y$  um subespaço denso de  $X$ . Então temos*

$$\sup_{x \in X} f(x) = \sup_{y \in Y} f(y).$$

*Demonstração.* A desigualdade  $\geq$  é óbvia. Denotemos  $b = \sup_{x \in X} f(x)$ . Seja  $\epsilon > 0$ . Existe  $x \in X$  tal que  $f(x) > b - \frac{\epsilon}{2}$ . A função  $f$  é contínua em  $x$ , logo existe  $\delta > 0$  tal que, se  $d(x, y) < \delta$ , temos  $|f(x) - f(y)| < \epsilon/2$ . Como  $Y$  é denso em  $X$ , existe  $y \in Y \cap B_\delta(x)$ . Por conseguinte,

$$f(y) > f(x) - \frac{\epsilon}{2} > b - \epsilon,$$

o que implica a desigualdade  $\leq$ . □

Isto nos leva a mais uma versão da imersão de Kuratowski.

**Teorema C.2.110.** *Sejam  $X$  um espaço métrico e  $Y$  um subespaço denso de  $X$ . Escolhamos um ponto  $x_0 \in X$  qualquer. A fórmula seguinte define uma imersão isométrica de  $X$  em  $\ell^\infty(|Y|)$ :*

$$X \ni x \mapsto i(x) = (d_x - d_{x_0})|_Y \in \ell^\infty(|Y|).$$

## C.3 Espaços completos, compactos, e precompactos

### C.3.1 Sequências de Cauchy

**Definição C.3.1.** Uma sequência de elementos de um espaço métrico  $X$  é chamada *sequência de Cauchy* se para cada  $\epsilon > 0$  existe um  $N$  tal que

$$d(x_m, x_n) < \epsilon$$

quaisquer que sejam  $m, n \geq N$ .

*Observação C.3.2.* Cada sequência convergente é uma sequência de Cauchy.

A recíproca é falsa em geral.

**Exemplo C.3.3.** Eis um exemplo de uma sequência de Cauchy no espaço métrico  $\mathbb{Q}$  que não converge neste espaço:

$$0, 0.1, 0.101, 0.101001, 0.1010010001, \dots$$

**Lema C.3.4.** *Uma sequência  $(x_n)$  é uma sequência de Cauchy se e somente se*

$$\forall \epsilon > 0 \exists N \forall n \geq N \quad x_n \in B_\epsilon(x_N).$$

*Demonstração.* Exercício. □

### C.3.2 Espaços métricos completos

**Definição C.3.5.** Um espaço métrico  $X$  é dito *completo* quando cada sequência de Cauchy tiver um limite (no mesmo espaço  $X$ ).

**Exemplo C.3.6.** O espaço métrico  $(X, d)$  munido de uma distância zero-um  $d = d_{0-1}$  é completo. Toda sequência de Cauchy  $(x_n)$  em  $X$  é *eventualmente constante*, ou seja, existem  $x \in X$  e  $N \in \mathbb{N}$  tais que para cada  $n \geq N$  temos  $x_n = x$ .

**Lema C.3.7.** *Seja  $X$  em espaço métrico. As condições seguintes são equivalentes:*

1.  $X$  é completo.
2. A interseção de cada sequência das bolas fechadas encaixadas de  $X$ , cuja o raio converge para zero, é não vazia.

*Demonstração.* (1)  $\Rightarrow$  (2): esta direção é praticamente evidente por que os centros das bolas formam uma sequência de Cauchy. Mais exatamente, seja  $(\bar{B}_{\epsilon_n}(x_n))_{n=1}^\infty$  uma sequência qualquer das bolas fechadas encaixadas em  $X$  cujas raios convergem para zero. Dado  $\epsilon > 0$ , existe  $N$  tal que  $\epsilon_n \leq \epsilon/2$  quando  $n \geq N$ . Se  $m, n \geq N$ , então  $x_m, x_k \in \bar{B}_{\epsilon_N}(x_N)$ , e assim teríamos

$$d(x_m, x_n) \leq d(x_m, x_N) + d(x_k, x_N) < 2\epsilon_N \leq \epsilon.$$

A sequência dos centros é uma sequência de Cauchy, e como  $X$  é completo, existe um limite

$$x = \lim_{n \rightarrow \infty} x_n.$$

Esto  $x$  é aderente a cada bola fechada  $\bar{B}_{\epsilon_n}(x_n)$ , logo  $x \in \bar{B}_{\epsilon_n}(x_n)$  e por conseguinte,

$$x \in \bigcap_{n=1}^\infty \bar{B}_{\epsilon_n}(x_n).$$

(2)  $\Rightarrow$  (1): seja  $(x_n)$  uma sequência de Cauchy em  $X$ . Para todo  $k = 1, 2, 3, \dots$  escolhamos  $N = N(k)$  de modo que

$$\forall m, n \geq N(k), \quad d(x_m, x_n) < 2^{-k-1}.$$

Se  $k \leq m$ , então para cada  $y \in \bar{B}_{2^{-m}}(x_{N(m)})$  temos

$$d(x_k, y) \leq d(x_k, x_m) + d(x_m, y) \leq 2^{-k-1} + 2^{-m} \leq 2^{-k-1} + 2^{-k-1} = 2^{-k},$$

logo  $y \in \bar{B}_{2^{-k}}(x_{N(k)})$ . Por conseguinte,

$$\bar{B}_{2^{-m}}(x_{N(m)}) \subseteq \bar{B}_{2^{-k}}(x_{N(k)}).$$

Concluimos: as bolas  $\bar{B}_{2^{-k}}(x_{N(k)})$  formam uma sequência das bolas fechadas encaixadas, cujos raios convergem para zero. De acordo com a hipótese, a interseção das bolas é não vazia, e como os raios convergem para zero, a interseção consiste de um ponto só, denotemos-o  $x$ :

$$\bigcap_{k=1}^{\infty} \bar{B}_{2^{-k}}(x_{N(k)}) = \{x\}.$$

Para cada  $k$  temos

$$d(x, x_{N(k)}) \leq 2^{-k-1}.$$

Concluimos que  $x$  é o limite da sequência  $(x_{N(k)})_{k=1}^{\infty}$ . □

**Exemplo C.3.8.** Para o espaço  $\mathbb{R}$  munido da distância usual a propriedade (2) do Lema C.3.7 é exatamente a propriedade dos intervalos fechados encaixados (Teorema de Cantor). Concluimos que  $\mathbb{R}$  é completo como um espaço métrico.

**Exemplo C.3.9.** O critério acima (lema C.3.7) acima mostra mais ou menos imediatamente a completude do espaço normado  $\ell^{\infty}(\Gamma)$  de todas as funções reais limitadas sobre um conjunto  $\Gamma$  qualquer, munido da norma uniforme

$$\|f\| = \sup_{\gamma \in \Gamma} |f(\gamma)|$$

e a distância correspondente,

$$d(f, g) = \|f - g\|.$$

(Exercício.)

**Teorema C.3.10.** *Seja  $Y$  um sub-espaço métrico de um espaço métrico  $X$ . Se  $Y$  é completo, então ele é fechado em  $X$ .*

*Demonstração.* Seja  $x$  um ponto aderente qualquer de  $Y$  em  $X$ :

$$x \in \bar{Y}^X.$$

Existe uma sequência  $(y_n)$  de pontos de  $Y$  convergente para  $x$  em  $X$ . Por conseguinte,  $(y_n)$  é uma sequência de Cauchy em  $X$ , logo ela resta uma sequência de Cauchy no sub-espaço  $Y$ , e possui o limite,  $y$ , em  $Y$ , porque  $Y$  é completo. Certamente,  $y_n \rightarrow y$  em  $X$  também. A unicidade do limite implica que  $x = y$ , e portanto

$$x = y \in Y.$$

□

**Teorema C.3.11.** *Cada sub-espaço fechado de um espaço métrico completo é completo.*

*Demonstração.* Exercício. □

**Exemplo C.3.12.** Um exemplo importante é o espaço  $C[0, 1]$  de todas as funções contínuas reais sobre o intervalo fechado unitário, munido da norma uniforme

$$\|f\| = \max_{x \in [0, 1]} |f(x)|.$$

A maneira mais fácil de verificar a completude de  $C[0, 1]$  é perceber que este espaço é fechado no espaço métrico ambiente  $\ell^\infty([0, 1])$ . (Exercício. Veja uma prova um pouco mais tarde, teorema C.3.23.)

**Exercício C.3.13.** Deduzir do lema C.3.7 o resultado seguinte. Um espaço métrico  $X$  é completo se e somente se cada sequência de *conjuntos fechados* encaixados, cujos diâmetros convergem para zero, tem uma interseção não vazia.

### C.3.3 Completamento de um espaço métrico: existência

**Definição C.3.14.** Seja  $X$  um espaço métrico qualquer. O *completamento* de  $X$  é um par  $(\hat{X}, i)$ , que consiste de um espaço métrico completo  $\hat{X}$  e uma imersão isométrica  $i: X \hookrightarrow \hat{X}$ , onde  $i(X)$  é denso em  $\hat{X}$ .

**Exemplo C.3.15.** O completamento do espaço  $\mathbb{Q}$  munido da distância usual é (isométrico ao) espaço métrico  $\mathbb{R}$ .

**Teorema C.3.16.** *Cada espaço métrico,  $X$ , possui um completamento.*

*Demonstração.* De acordo com Teorema C.2.108, existe uma imersão isométrica,  $i$ , de  $X$  num espaço métrico  $\ell^\infty(|X|)$ . Definamos

$$\hat{X} = \overline{i(X)}.$$

O espaço  $\ell^\infty(|X|)$  é completo (exercício C.3.9), e como o subespaço  $\hat{X}$  é fechado em  $\ell^\infty(|X|)$ , ele é completo também (teorema C.3.11). A imagem  $i(X)$  é densa em  $\hat{X}$ . □



### C.3.4 Espaços isométricos

**Definição C.3.17.** Uma *isometria* entre dois espaços métricos  $X$  e  $Y$  e uma imersão isométrica sobrejetiva do  $Y$  em  $X$ .

**Exemplo C.3.18.** A função

$$\mathbb{R} \ni x \mapsto i(x) = x + 1 \in \mathbb{R}$$

é uma isometria da reta com si própria.

**Definição C.3.19.** Dois espaços métricos  $X$  e  $Y$  são chamados *isométricos* se existe uma isometria

$$i: X \rightarrow Y.$$

Notação:  $X \cong Y$ .

**Exercício C.3.20.** A relação da isometria entre espaços métricos é uma relação de equivalência, ou seja,

1. Reflexividade: cada espaço  $X$  é isométrico a si mesmo:  $X \cong X$ .
2. Simetria: se  $X \cong Y$ , então  $Y \cong X$ .
3. Transitividade: se  $X \cong Y$  e  $Y \cong Z$ , então  $X \cong Z$ .

### C.3.5 Completamento de um espaço métrico: unicidade

**Teorema C.3.21.** O completamento  $\hat{X}$  de um espaço métrico  $X$  é único a menos de isometria. Sejam  $(\hat{X}, i)$  e  $(\tilde{X}, j)$  dois completamentos de  $X$ . Então existe uma isometria  $\kappa: \hat{X} \rightarrow \tilde{X}$  tal que

$$\kappa \circ i = j.$$

*Demonstração.* Escolhamos um ponto  $x_0 \in X$  qualquer. Segundo Teorema C.2.110, a fórmula

$$\hat{X} \ni x \mapsto i'(x) = (d_{i(x)} - d_{i(x_0)}) \circ i \in \ell^\infty(|X|)$$

define uma imersão isométrica

$$i': \hat{X} \hookrightarrow \ell^\infty(|X|),$$

e a fórmula semelhante

$$\tilde{X} \ni x \mapsto j'(x) = (d_{j(x)} - d_{j(x_0)}) \circ j \in \ell^\infty(|X|)$$

define uma imersão isométrica

$$j': \tilde{X} \hookrightarrow \ell^\infty(|X|).$$

Temos

$$i' \circ i = j' \circ j,$$

e por essa razão as imagens de  $\hat{X}$  para  $i'$  e de  $\tilde{X}$  para  $j'$  são iguais (cada uma delas é o fecho em  $\ell^\infty(|X|)$  do conjunto  $i'(i(X)) = j'(j(X))$ ).

As aplicações

$$i': \hat{X} \rightarrow i'(\hat{X}) \text{ e } j': \tilde{X} \rightarrow j'(\tilde{X})$$

são isometrias sobre as suas imagens, logo possuem as aplicações recíprocas. Definamos

$$\kappa = (j')^{-1} \circ i'.$$

É uma isometria entre  $\hat{X}$  e  $\tilde{X}$ . Além disso, temos

$$\begin{aligned} \kappa \circ i &= (j')^{-1} \circ i' \circ i \\ &= (j')^{-1} \circ j' \circ j \\ &= j. \end{aligned}$$

□

### C.3.6 Teorema de Weierstrass sobre a convergência uniforme

**Definição C.3.22.** Seja  $X$  um espaço métrico qualquer. Denotemos  $CB(X)$  o conjunto de todas as funções reais limitadas e contínuas sobre  $X$ , munido da distância induzida de  $\ell^\infty(X)$ .

**Teorema C.3.23.** *Seja  $X$  um espaço métrico qualquer. O espaço métrico  $CB(X)$  é completo.*

*Demonstração.* Mostremos que  $CB(X)$  é fechado em  $\ell^\infty(X)$ , ou seja, que o complemento de  $CB(X)$  em  $\ell^\infty(X)$  é aberto. Seja  $f \in CB(X)^c = \ell^\infty(X) \setminus CB(X)$  uma função qualquer. Como  $f$  é descontínua, existem  $x_0 \in CB(X)$  e  $\epsilon_0 > 0$  tais que

$$\forall \delta > 0 \exists y \in K \quad d(x_0, y) < \delta \wedge |f(x_0) - f(y)| \geq \epsilon_0.$$

Mostremos que a bola aberta  $B_{\epsilon_0/3}(g)$  não encontra  $CB(X)$ . Sejam  $g \in B_{\epsilon_0/3}(x_0)$  e  $\delta > 0$  quaisquer. Escolhamos  $y \in K$  como acima. Agora estabeleçamos a desigualdade

$$|g(x_0) - g(y)| \geq \frac{\epsilon_0}{3}, \tag{C.4}$$

de onde a descontinuidade de  $g$  seguir.

Para obter uma contradição, suponhamos que (C.4) não é verdadeiro. Temos

$$|g(x_0) - g(y)| < \frac{\epsilon_0}{3},$$

e, seguindo a desigualdade triangular,

$$\begin{aligned} |f(x_0) - f(y)| &= |f(x_0) - g(x_0) + g(x_0) - g(y) + g(y) - f(y)| \\ &\leq |f(x_0) - g(x_0)| + |g(x_0) - g(y)| + |g(y) - f(y)| \\ &< \frac{\epsilon_0}{3} + \frac{\epsilon_0}{3} + \frac{\epsilon_0}{3} \\ &= \epsilon, \end{aligned}$$

uma contradição. □

**Definição C.3.24.** Seja  $(f_n)$  uma seqüência das funções de um conjunto  $X$  para  $\mathbb{R}$ . Diz-se que a seqüência  $(f_n)$  converge uniformemente para uma função  $f: X \rightarrow \mathbb{R}$  se

$$d_\infty(f_n, f) \rightarrow 0 \text{ quando } n \rightarrow \infty,$$

onde  $d_\infty$  é a distância no espaço  $\ell^\infty(X)$ . Notação:

$$f_n \rightrightarrows f.$$

Eis uma reformulação equivalente do teorema C.3.23.

**Teorema C.3.25** (Teorema de Weierstrass sobre a convergência uniforme). *O limite uniforme de uma seqüência de funções contínuas é contínua.* □

### C.3.7 Espaços compactos

**Definição C.3.26.** Um subconjunto  $K$  de um espaço métrico  $X$  é dito *compacto* se cada seqüência dos pontos de  $K$  contém uma subsequência que converge e tem o seu limite em  $K$ .

**Exemplo C.3.27.**  $\mathbb{R}$  não é compacto: a seqüência

$$1, 2, 3, 4, \dots, n, \dots$$

não contém nenhuma subsequência convergente.

**Exemplo C.3.28.** Cada espaço métrico finito,  $X$ , é compacto.

**Exercício C.3.29.** Mostre que o produto de uma família enumerável de espaços métricos compactos, munido de uma métrica que gera a topologia de produto, é compacto.

**Teorema C.3.30.** *Seja  $K$  um sub-conjunto compacto de um espaço métrico  $X$  qualquer. Então  $K$  é fechado em  $X$ .*

*Demonstração.* Seja  $x \in X$  um ponto aderente a  $K$ . Existe uma sequência  $(x_n)$  dos elementos de  $K$  que converge para  $x$ :

$$x_n \rightarrow x.$$

Como  $K$  é compacto, a sequência  $(x_n)$  tem uma sub-sequência convergente  $(x_{n_k})_{k=1}^{\infty}$  cujo limite é contido em  $K$ :

$$\exists \mathcal{x} \in K \quad x_{n_k} \rightarrow \mathcal{x} \text{ quando } k \rightarrow \infty.$$

Ao mesmo tempo, a sub-sequência certamente converge para  $x$ , todo como a sequência original:

$$x_{n_k} \rightarrow x \text{ quando } k \rightarrow \infty.$$

Concluimos:  $x = \mathcal{x} \in K$ . □

**Teorema C.3.31.** *Cada espaço métrico compacto é completo.*

*Demonstração.* Seja  $(x_n)$  uma sequência de Cauchy no espaço métrico compacto  $K$ . Existem uma sub-sequência  $(x_{n_k})$  convergente para um limite  $x \in K$ . Verifica-se facilmente que com efeito

$$\lim_{n \rightarrow \infty} x_n = x.$$

□

**Teorema C.3.32.** *Cada sub-conjunto fechado de um espaço métrico compacto é compacto.*

*Demonstração.* Exercício. □

### C.3.8 Teoremas de Weierstrass

**Teorema C.3.33.** *A imagem de um conjunto compacto por uma aplicação contínua é compacta.*

*Demonstração.* Sejam  $X$  e  $Y$  dois espaços métricos,  $K \subseteq X$  um sub-conjunto compacto, e  $f : X \rightarrow Y$  uma aplicação contínua. Seja  $(y_n)$  uma sequência qualquer dos pontos de  $f(K)$ . Para cada  $n$  escolhamos  $x_n \in K$  tal que  $f(x_n) = y_n$ . Como  $K$  é compacto, existe uma subsequência  $(x_{n_k})_{k=1}^{\infty}$  convergente em  $K$  para um limite  $\mathcal{x} \in K$ . Como a aplicação  $f$  é contínua, concluimos

$$y_n = f(x_n) \rightarrow f(\mathcal{x}) \in f(K) \text{ quando } n \rightarrow \infty.$$

□

Eis um corolário importante que, pelas razões históricas, habitualmente é cortado em duas partes de maneira um pouco grotesca.

**Teorema C.3.34** (Primeiro teorema de Weierstrass). *Cada função real contínua sobre um espaço métrico compacto é limitada...*

**Teorema C.3.35** (Segundo teorema de Weierstrass). *...e atinge os seus limites.*

*Demonstração.* Seja  $K$  um espaço métrico compacto (em especial, não vazio), e seja  $f : K \rightarrow \mathbb{R}$  uma função contínua. A imagem  $f(K)$  é compacto graças ao teorema C.3.33, logo limitado em  $\mathbb{R}$  (teorema de Heine-Borel C.3.51). Como  $f(K)$  não é vazio, o supremo  $b = \sup f(K)$  existe e pertence a  $\mathbb{R}$ . Evidentemente,  $b$  é um ponto aderente de  $f(K)$ . Como  $f(K)$  é fechado em  $\mathbb{R}$ , temos  $b \in f(K)$ , de onde concluímos.  $\square$

### C.3.9 Aplicações fechadas

**Definição C.3.36.** Uma aplicação contínua  $f : X \rightarrow Y$  entre dois espaços métricos quaisquer  $X$  e  $Y$  é dita *fechada* se para cada parte fechada  $G$  de  $X$  a sua imagem,  $f(G)$ , por  $f$  é fechada em  $Y$ .

**Exemplo C.3.37.** Sejam  $X = \mathbb{R}^2$  munido da distância usual,  $Y = \mathbb{R}$ ,  $G \subseteq \mathbb{R}^2$  o gráfico da função  $y = 1/x$ , ou seja,

$$G = \left\{ \left( x, \frac{1}{x} \right) : x \in \mathbb{R} \setminus \{0\} \right\},$$

e  $p : \mathbb{R}^2 \rightarrow \mathbb{R}$  a projeção:

$$p(x, y) = x.$$

Verifica-se facilmente que a aplicação  $p$  é contínua e que o conjunto  $G$  é fechado em  $\mathbb{R}^2$ , mas ao mesmo tempo a imagem não é:

$$p(G) = \mathbb{R} \setminus \{0\}$$

**Proposição C.3.38.** *Cada aplicação contínua de um espaço métrico compacto  $K$  para um espaço métrico  $Y$  qualquer é fechada.*

*Demonstração.* Seja  $F \subseteq K$  uma parte fechada qualquer. Logo  $F$  é compacto, e a sua imagem  $f(F)$  pela aplicação contínua  $f$  é compacto em  $Y$ . Cada sub-conjunto compacto de um espaço métrico é fechado.  $\square$

**Corolário C.3.39.** *Seja  $f : K \rightarrow Y$  uma aplicação contínua e bijetiva entre dois espaços métricos, onde  $K$  é compacto. Então a aplicação inversa  $f^{-1}$  é contínua. (Como diz-se,  $f$  é um homeomorfismo.)*

*Demonstração.* A fim de mostrar que a aplicação  $g = f^{-1} : Y \rightarrow K$  é contínua, seja  $G \subseteq K$  uma parte fechada qualquer. Temos

$$g^{-1}(G) = f(G),$$

e  $f(G)$  é fechado em  $Y$  porque a aplicação  $f$  é fechada segundo a proposição C.3.38. Concluímos: a imagem inversa de cada parte fechada de  $K$  por  $g$  é fechada em  $Y$ , e portanto  $g = f^{-1}$  é contínua.  $\square$

### C.3.10 Espaços precompactos

**Definição C.3.40.** Um sub-conjunto  $A$  de um espaço métrico  $X$  é dito *precompacto*, ou *totalmente limitado*, se para cada valor  $r > 0$  existe uma cobertura finita de  $A$  pelas bolas abertas de raio  $r$ :

$$\exists n, \exists x_1, x_2, \dots, x_n \in X, \text{ tais que } A \subseteq \cup_{i=1}^n B_r(x_i).$$

Em outras palavras, para cada  $r > 0$  existe uma coleção finita  $x_1, x_2, \dots, x_n$  dos pontos de  $X$  tal que cada  $a \in A$  é a distância  $< r$  de algum deles:

$$\forall a \in A, \exists i = 1, 2, 3, \dots, n \text{ tal que } d(a, x_i) < r.$$

**Exemplo C.3.41.** Um subconjunto  $A$  de  $\mathbb{R}$  é precompacto se e somente se  $A$  é limitado (contido num intervalo finito).

**Definição C.3.42.** Um espaço métrico  $X$  é dito *precompacto* se  $X$  é um sub-conjunto precompacto de si mesmo.

Com efeito, a noção da precompactidade de um sub-espaço métrico  $A$  é “absoluta”, ou seja, não depende de um espaço ambiental,  $X$ .

**Proposição C.3.43.** *Seja  $A$  um sub-conjunto precompacto não vazio de um espaço métrico  $X$ , ou seja, para cada  $r > 0$  existe uma cobertura finita de  $A$  pelas bolas abertas de raio  $r$  centradas em  $X$ . Então,  $A$  é precompacto em si mesmo, ou seja, para cada  $r > 0$  existe uma cobertura finita de  $A$  pelas bolas abertas de raio  $r$  centradas em  $A$ .*

*Demonstração.* Seja  $r > 0$ . Podemos escolher uma coleção finita dos pontos  $x_1, x_2, \dots, x_n \in X$  tal que para cada  $a \in A$  existe  $i$  com a propriedade

$$d(x_i, a) < r/2.$$

Sem perda da generalidade, podemos supor que cada bola aberta  $B_{r/2}(x_i)$  encontra  $A$ . Para cada  $i$ , escolhamos um ponto

$$a_i \in B_{r/2}(x_i) \cap A.$$

Seja  $a \in A$  um ponto qualquer. Existe  $i$  tal que  $d(a, x_i) < r/2$ . Temos finalmente, graça à desigualdade triangular:

$$d(a, a_i) \leq d(a, x_i) + d(x_i, a_i) < \frac{r}{2} + \frac{r}{2} = r.$$

Portanto,  $A$  é contido na união das bolas abertas  $B_r(a_i)$ ,  $i = 1, 2, \dots, n$ , onde as bolas podem ser consideradas em  $A$  em vez de em  $X$ . □

**Corolário C.3.44.** *Um sub-espaço métrico de um espaço métrico precompacto é precompacto.* □

### C.3.11 Compacidade e precompacidade

**Teorema C.3.45.** *Cada conjunto compacto é precompacto.*

*Demonstração.* Vamos mostrar a contraposição: se  $X$  não é precompacto, então  $X$  não é compacto.

Suponhamos que  $X$  é um sub-conjunto não precompacto de um espaço métrico. A negação da precompacidade significa que existe  $r > 0$  com a propriedade que para cada coleção finita  $x_1, x_2, \dots, x_n \in X$ , existe  $x_{n+1} \in X$  tal que

$$d(x_i, x_{n+1}) \geq r, \quad i = 1, 2, \dots, n.$$

Utilizando esta propriedade, escolhamos pela recorrência uma sequência infinita dos pontos de  $X$ ,

$$x_1, x_2, \dots, x_n, \dots,$$

de modo que

$$\forall i, j, \quad (i \neq j) \Rightarrow d(x_i, x_j) \geq r.$$

Evidentemente, cada sub-sequência de  $(x_n)$  tem a mesma propriedade, logo não é convergente. Concluimos: o conjunto  $X$  não é compacto.  $\square$

*Observação C.3.46.* Existem espaços precompactos não compactos, por exemplo, o intervalo  $(0, 1)$ .

**Teorema C.3.47.** *Um espaço métrico  $X$  é compacto se e somente se  $X$  é precompacto é completo.*

*Demonstração.* A necessidade ( $\Rightarrow$ ) foi mostrada nos teoremas C.3.45 et C.3.31.

A fim de verificar a suficiência ( $\Leftarrow$ ), seja  $X$  um espaço precompacto e completo, e seja  $(x_n)$  uma sequência qualquer dos pontos de  $X$ . Cobremos  $X$  com uma família finita das bolas abertas de raio um. Como esta coleção é finita, existe pelo menos uma bola entre elas, denotaremos-a  $B_1(a_1)$ , que contém uma infinidade dos membros da sequência  $(x_n)$ .

De acordo com o corolário C.3.44, a bola  $B_1(a_1)$  é precompacta, logo ela pode ser coberta por uma família finita das bolas abertas de raio  $1/2$  (formadas no sub-espaço métrico  $B_1(a_1)$ ). Entre elas, pelo menos uma bola contém uma infinidade dos membros da sequência  $(x_n)$ .

Continuando pela recorrência, escolhamos uma sequência infinita das bolas abertas  $B_1(a_1), B_{1/2}(a_2), \dots, B_{1/n}(a_n), \dots$ , cujas cada uma contém uma infinidade dos membros da sequência  $(x_n)$ .

Finalmente, escolhamos uma sequência dos números inteiros

$$n_1 < n_2 < \dots < n_k < \dots$$

de tal modo que cada elemento  $x_{n_k}, k = 1, 2, 3, \dots$  pertence à bola  $B_{1/k}(a_k)$ . Esta sub-sequência é uma sequência de Cauchy: cada vez que  $i, j > k$ , temos

$$d(x_{n_i}, x_{n_j}) < 2/k.$$

Como o espaço métrico  $X$  é completo, a sequência extrata  $(x_{n_k})_{k=1}^{\infty}$  converge em  $X$ . Concluimos:  $X$  é compacto.  $\square$

*Observação C.3.48.* Com efeito, temos mostrado que se  $X$  é um espaço precompacto, então cada sequência  $(x_n)$  dos pontos de  $X$  contém uma subsequência de Cauchy. Prova-se facilmente que esta propriedade caracteriza os espaços precompactos (exercício).

*Observação C.3.49.* O critério da compacidade acima (teorema C.3.47) é muito conveniente porque, geralmente, é mais fácil de verificar a precompacidade de um espaço métrico que a compacidade dele.

**Exercício C.3.50.** Deduza o resultado clássico seguinte.

**Teorema C.3.51** (Teorema de Heine-Borel). *Uma parte  $K$  de  $\mathbb{R}$  é compacta se e somente se  $K$  é fechada e limitada.*

**Teorema C.3.52.** *Seja  $X$  um sub-espaço denso de um espaço métrico  $Y$ . Se  $X$  é precompacto, então  $Y$  é precompacto.*

*Demonstração.* Seja  $r > 0$  um número real qualquer. Escolhamos uma coleção finita  $x_1, x_2, \dots, x_n \in X$  da tal maneira que

$$X \subseteq \cup_{i=1}^n B_{r/2}(x_i).$$

(Aqui  $B_{r/2}(x_i)$  pode denotar as bolas abertas seja em  $X$ , seja em  $Y$ , isso não importe).

Vamos verificar agora que

$$Y \subseteq \cup_{i=1}^n B_r(x_i).$$

Seja  $y \in Y$ . Como  $X$  é denso em  $Y$ , existe  $x \in X \cap B_{r/2}(y)$ . O ponto  $x$  é contido na bola  $B_{r/2}(x_i)$  por um  $i$ . Concluimos, utilizando a desigualdade de triângulo:

$$d(y, x_i) \leq d(y, x) + d(x, x_i) < \frac{r}{2} + \frac{r}{2} = r.$$

(Aqui  $B_r(x_i)$  denota uma bola aberta em  $Y$ .)  $\square$

*Observação C.3.53.* Se  $X$  é denso em  $Y$ , a condição  $X \subseteq \cup_{i=1}^n B_r(x_i)$  não implica, em geral, que  $Y \subseteq \cup_{i=1}^n B_r(x_i)$ . Queiram olhar o exemplo seguinte:  $Y = (0, 1)$ ,  $X = (0, 1) \setminus \{1/2\}$ ,  $x = 1/4$ ,  $y = 3/4$ ,  $r = 1/4$ .  $\square$

**Corolário C.3.54.** *Um espaço métrico  $X$  é precompacto se e somente se o seu completamento  $\hat{X}$  é compacto.*  $\square$



### C.3.12 Aplicações uniformemente contínuas

*Observação C.3.55.* Lembremos que a imagem de um espaço compacto por uma função contínua é compacto. É *falso* para os espaços precompactos.

Por exemplo, a função contínua

$$\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) \ni x \mapsto \tan x \in \mathbb{R}$$

é sobrejetiva, o intervalo limitado é precompacto, e a imagem não é precompacta.

**Definição C.3.56.** Uma função  $f: X \rightarrow Y$  entre dois espaços métricos é dita *uniformemente contínua* se

$$\forall \epsilon > 0 \exists \delta > 0 \forall x, y \in X (d_X(x, y) < \delta) \Rightarrow (d_Y(f(x), f(y)) < \epsilon).$$

O valor de  $\delta = \delta(\epsilon)$  pode ser escolhido “uniformemente” em relação a  $x$ . Certamente, cada função uniformemente contínua é contínua.

**Exemplo C.3.57.** A função

$$f(x) = x^2$$

de  $\mathbb{R}$  para  $\mathbb{R}$  é contínua mas não uniformemente contínua, porque, dados  $\epsilon > 0$  e  $x \in \mathbb{R}$ , o valor de  $\delta > 0$  correspondente é da ordem da grandeza

$$\delta \sim \frac{\epsilon}{2|x|}.$$

Por conseguinte,  $\delta$  depende de  $x$  de maneira essencial.

**Teorema C.3.58.** *Cada função contínua sobre um espaço métrico compacto é uniformemente contínua.*

*Demonstração.* Vamos mostrar a contraposição: seja  $f: X \rightarrow Y$  uma função contínua entre dois espaços métricos. Suponhamos que  $f$  não é uniformemente contínua. Existe  $\epsilon_0 > 0$  tal que para cada  $n = 1, 2, 3, \dots$  pode-se encontrar os pontos  $x_n, y_n \in X$  que satisfazem

$$d_X(x_n, y_n) < \frac{1}{n} \tag{C.5}$$

e

$$d_Y(f(x_n), f(y_n)) \geq \epsilon_0. \tag{C.6}$$

A sequência  $(x_n)$  contém uma subsequência convergente

$$x_{n_i} \rightarrow x \text{ quando } i \rightarrow \infty.$$

Graça à hipótese (C.5),

$$d_X(x, y_{n_i}) \leq d_X(x, x_{n_i}) + d_X(x_{n_i}, y_{n_i}) \rightarrow 0 \text{ quando } i \rightarrow \infty.$$

Por conseguinte,

$$y_{n_i} \rightarrow x.$$

Por causa de (C.6), não temos

$$f(x_{n_i}) \rightarrow f(x) \leftarrow f(y_{n_i}),$$

o que significa que  $f$  não é contínua.  $\square$

**Exercício C.3.59.** Mostre que a imagem de um espaço métrico precompacto para uma aplicação uniformemente contínua é precompacto.

## C.4 Teorema da categoria de Baire

### C.4.1 Conjuntos nunca densos

Eis uma forte negação da propriedade de um sub-conjunto de ser denso num espaço métrico.

**Definição C.4.1.** Um sub-conjunto  $A$  de um espaço métrico  $X$  é dito *nunca denso*<sup>1</sup> se cada bola aberta,  $B_\epsilon(x)$ , de  $X$  conta uma bola  $B_\delta(y)$  disjunta de  $A$ :

$$\forall x \in A, \forall \epsilon > 0 \exists y \in X, \exists \delta > 0, \text{ tais que } B_\delta(y) \subseteq B_\epsilon(x) \text{ e } B_\delta(y) \cap A = \emptyset.$$

*Observação C.4.2.* Um sub-conjunto de um conjunto nunca denso é nunca denso.

*Observação C.4.3.*  $A$  é nunca denso se e somente se  $\bar{A}$  é nunca denso.

A implicação  $\Leftarrow$  segue-se da observação C.4.2. A fim de mostrar a implicação  $\Rightarrow$ , suponhamos que  $A$  é um sub-conjunto nunca denso de  $X$ . Sejam  $x \in X$  e  $\epsilon > 0$  quaisquer. Como  $A$  é nunca denso, existem  $y \in X$  e  $\delta > 0$  tais que  $B_\delta(y) \subseteq B_\epsilon(x)$  e  $B_\delta(y) \cap A = \emptyset$ . Mas toda bola aberta disjunta de um conjunto,  $A$ , é disjunta da aderência  $\bar{A}$ .

*Observação C.4.4.* Um conjunto fechado,  $F$ , é nunca denso se e somente se  $\text{Int } F = \emptyset$ .

A implicação “somente se” ( $\Rightarrow$ ) é evidentemente verdadeira para todos sub-conjuntos, fechados ou não. A fim de verificar a implicação “se” ( $\Leftarrow$ ), seja  $F$  um conjunto fechado de interior vazio, e sejam  $x \in X$  e  $\epsilon > 0$  quaisquer. A bola  $B_\epsilon(x)$  não é contida em  $F$  de acordo com a hipótese, por que  $\text{Int } F = \emptyset$ . Logo a diferença  $B_\epsilon(x) \setminus F$  é não vazia. De outro lado, esta diferença é aberta como a interseção de dois abertos:

$$B_\epsilon(x) \setminus F = B_\epsilon(x) \cap F^c.$$

Como todo aberto não vazio,  $B_\epsilon(x) \setminus F$  contém uma bola aberta,  $B_\delta(y)$ . Ela é contida na bola original,  $B_\epsilon(x)$ , e disjunta de  $F$ .

<sup>1</sup>*Nowhere dense* (ingles), *rare* (francês).

As observações C.4.3 e C.4.4 implicam imediatamente:

**Proposição C.4.5.** *Um sub-conjunto  $A$  de um espaço métrico  $X$  é nunca denso em  $X$  se e somente se a aderência de  $A$  possui o interior vazio.*  $\square$

**Exemplo C.4.6.** Cada conjunto unitário  $\{x\}$ , onde  $x$  não é isolado, é nunca denso.

**Exemplo C.4.7.** A reta  $y = 0$  (o eixo coordenado  $Ox$ ) é nunca denso no plano euclidiano  $\mathbb{R}^2$ .

**Exemplo C.4.8.** O conjunto  $\mathbb{Q}$  não é nunca denso em  $\mathbb{R}$ , porque  $\mathbb{Q}$  é denso.

**Exemplo C.4.9.**  $\mathbb{Z}$  é nunca denso em  $\mathbb{R}$  mas não é nunca denso em si mesmo.

**Lema C.4.10.** *A união de uma família finita dos conjuntos nunca densos é nunca densa.*

*Demonstração.* Basta mostrar o resultado para dois conjuntos nunca densos,  $A$  e  $B$ . Seja  $B_\epsilon(x)$  uma bola aberta qualquer. Ela contém uma bola aberta  $B_\delta(y)$  disjunta de  $A$ , e por sua vez, a bola  $B_\delta(y)$  contém uma bola aberta ainda menor,  $B_\gamma(z)$ , disjunta de  $B$ . Evidentemente, a bola  $B_\gamma(z)$  é disjunta de  $A \cup B$ .  $\square$

## C.4.2 Conjuntos magros

**Definição C.4.11.** Uma parte  $A$  de um espaço métrico  $X$  é dita um conjunto *magro*,<sup>2</sup> ou um conjunto *da primeira categoria*<sup>3</sup> se ela é igual à união de uma família enumerável de sub-conjuntos nunca densos:

$$A = \bigcup_{i=1}^{\infty} A_i,$$

onde  $A_i$  são nunca densos em  $X$ .

*Observação C.4.12.* Evidentemente, cada sub-conjunto de um conjunto magro é magro. Por conseguinte, um sub-conjunto magro pode ser definido como um conjunto *contido* na união de uma família enumerável de sub-conjuntos nunca densos (ou: nunca densos e fechados).

**Exemplo C.4.13.** Cada conjunto nunca denso é magro.

**Exemplo C.4.14.**  $\mathbb{Q}$  é magro em  $\mathbb{R}$ , assim como em si mesmo.

**Exemplo C.4.15.**  $\mathbb{Z}$  é magro em  $\mathbb{R}$ , mas não é magro em si mesmo: todos os conjuntos unitários são abertos em  $\mathbb{Z}$ , logo não nunca densos.

<sup>2</sup>Como em francês, *maigre*.

<sup>3</sup>Set of first category (ingles).

### C.4.3 Teorema da categoria de Baire

O teorema a seguir encontra-se entre as ferramentas mais úteis.

**Teorema C.4.16** (Teorema da categoria de Baire). *Cada sub-conjunto magro de um espaço métrico completo tem o interior vazio.*

*Demonstração.* Basta mostrar que a união de uma sequência de sub-conjuntos fechados e nunca densos,  $(F_n)$ , tem o interior vazio. Seja  $B_\epsilon(x)$  uma bola aberta qualquer em  $X$ . Vamos provar que

$$B_\epsilon(x) \not\subseteq \bigcup_{n=1}^{\infty} F_n.$$

Definamos  $x_1 = x$ ,  $\epsilon_1 = \epsilon$ . Escolhamos uma bola fechada contida em  $B_\epsilon(x)$ , por exemplo  $\bar{B}_{\epsilon/2}(x)$ . Como  $F_1$  é nunca denso, existem  $x_2 \in X$  e  $\epsilon_2 > 0$  tais que

$$B_{\epsilon_2}(x_2) \subseteq B_{\epsilon/2}(x) \text{ e } B_{\epsilon_2}(x_2) \cap F_1 = \emptyset.$$

Reduzamos o raio a fim de obter uma bola fechada contida em  $B_{\epsilon_2}(x_2)$ :

$$\bar{B}_{\epsilon_2/2}(x_2) \subseteq B_{\epsilon_2}(x_2).$$

Escolhamos  $x_3$  e  $\epsilon_3 > 0$  de tal modo que

$$B_{\epsilon_3} \subseteq \bar{B}_{\epsilon_2/2}(x_2) \text{ e } B_{\epsilon_3} \cap F_3 = \emptyset.$$

Continuemos da maneira recorrente a fim de obter uma sequência das bolas fechadas encaixadas,  $B_1, B_2, \dots$ , cujas raio aproximam-se de zero e que possuem a propriedade seguinte: cada bola  $B_n$  é disjunta dos conjuntos nunca densos  $F_1, F_2, \dots, F_n$ .

De acordo com lema C.3.7, a interseção  $\bigcap B_n$  é não vazia. É óbvio que o ponto comum de todas as bolas pertence à bola original, e ao mesmo tempo pertence ao nenhum conjunto  $F_n$ ,  $n = 1, 2, 3, \dots$   $\square$

**Exemplo C.4.17.** A conclusão do teorema é falsa sem a hipótese que  $X$  seja completo. Consideremos o espaço  $\mathbb{Q}$  munido da distância usual. Os conjuntos unitários  $\{q\}$ ,  $q \in \mathbb{Q}$  são fechados, e o interior deles é vazio. Apesar disso,

$$\mathbb{Q} = \bigcup_{q \in \mathbb{Q}} \{q\}$$

é a união de uma família *enumerável* dos sub-conjuntos nunca densos.

**Definição C.4.18.** Um sub-conjunto de um espaço métrico  $X$  é dito um *sub-conjunto do tipo  $G_\delta$*  (ou simplesmente *um  $G_\delta$* ), se  $G$  é igual à interseção de uma família enumerável de abertos de  $X$ :

$$G = \bigcap_{i=1}^{\infty} U_i, \text{ onde } U_i \text{ são abertos.}$$

**Exemplo C.4.19.** Cada aberto,  $U$ , em um espaço métrico qualquer é um  $G_\delta$ :

$$U = \bigcap \{U\},$$

ou, se não convencer ainda,

$$U = \bigcap_{i=1}^{\infty} U_n, \text{ ou } U_n = U \text{ para todos } n.$$

**Exemplo C.4.20.** O conjunto dos números irracionais é um  $G_\delta$  na reta  $\mathbb{R}$ :

$$\mathbb{R} \setminus \mathbb{Q} = \bigcap_{q \in \mathbb{Q}} (\mathbb{R} \setminus \{q\}).$$

**Exemplo C.4.21.** Cada conjunto unitário  $\{x\}$  em um espaço métrico qualquer  $X$  é um  $G_\delta$ : verifica-se simplesmente que

$$\{x\} = \bigcap_{n=1}^{\infty} B_{1/n}(x).$$

**Exercício C.4.22.** Mais geralmente, cada sub-conjunto fechado de um espaço métrico é um  $G_\delta$ .

Existem numerosos corolários e formas equivalentes do teorema de Baire.

**Lema C.4.23.** *Se  $U$  é uma parte aberta densa num espaço métrico  $X$ , então o complemento  $U^c$  é nunca denso em  $X$ .*

*Demonstração.* Como o complemento  $U^c$  é fechado, basta mostrar que o seu interior é vazio. Se não, então existem  $x \in X$  e  $\epsilon > 0$  tais que  $B_\epsilon(x) \subseteq \text{Int } U^c$ . Em particular,  $B_\epsilon(x)$  é disjunta de  $U$ , uma contradição por que  $U$  é denso em  $X$ .  $\square$

Deduz-se imediatamente:

**Teorema C.4.24** (Forma equivalente do teorema de Baire). *Sejam  $X$  um espaço métrico completo e  $(U_n)$  uma família enumerável de partes abertas de  $X$  que são densas em  $X$ . Então a interseção*

$$\bigcap_{n=1}^{\infty} U_n$$

*é densa em  $X$ .*

*Demonstração.* O complemento

$$\left(\bigcap_{n=1}^{\infty} U_n\right)^c = \bigcup_{n=1}^{\infty} U_n^c$$

é a união de uma família enumerável dos conjuntos nunca densos, de acordo com o lema C.4.23. Logo, o complemento acima é magro em  $X$ , e pelo teorema de Baire, o seu interior é vazio. Em outras palavras, esta união não contém nenhuma bola aberta. Portanto, o seu complemento,  $\bigcap_{n=1}^{\infty} U_n$ , encontra cada bola aberta.  $\square$

### C.4.4 Genericidade

**Definição C.4.25.** Um sub-conjunto  $G$  de um espaço métrico  $X$  é dito *co-magro*, ou *genérico*, se  $A$  contém um sub-conjunto  $B$  do tipo  $G_\delta$  que é denso em  $X$ .

Eis uma justificação do nome “co-magro”.

**Lema C.4.26.** *Uma parte  $A$  de um espaço métrico  $X$  é co-magro se e somente se o complemento  $A^c$  é magro.*

*Demonstração.*  $\Rightarrow$ : Seja  $A$  uma parte co-magra. Escolhamos um  $G_\delta$  denso,  $G$ , contido em  $A$ . Então

$$G = \bigcap_{n=1}^{\infty} U_n,$$

onde todos os  $U_n$  são abertos e evidentemente densos em  $X$  (por que  $G \subseteq U_n$  e já  $G$  é denso). Temos

$$A^c \subseteq G^c = \bigcup_{n=1}^{\infty} U_n^c,$$

e de acordo com o lema C.4.23, os sub-conjuntos  $U_n^c$  são nunca densos. Concluimos:  $A^c$  é magro.

$\Leftarrow$ : a prova é semelhante. □

**Exemplo C.4.27.** O conjunto dos números racionais não é um  $G_\delta$  em  $\mathbb{R}$ . Suponhamos o contrario: que  $\mathbb{Q}$  é um  $G_\delta$ . Então  $\mathbb{Q}$  é co-magro e o seu complemento, o conjunto  $\mathbb{R} \setminus \mathbb{Q}$  dos números irracionais, é magro. Como  $\mathbb{Q}$  é si mesmo magro em  $\mathbb{R}$ , a união  $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$  é magro assim, logo o interior em  $\mathbb{R}$  é vazio, que é absurdo.

Eis uma outra reformulação do teorema de Baire.

**Teorema C.4.28** (Mais uma forma equivalente do teorema de Baire). *A interseção de uma família enumerável de partes genéricas de um espaço métrico completo é uma parte genérica.*

*Demonstração.* Seja  $A_n$ ,  $n = 1, 2, \dots$  uma família enumerável de sub-conjuntos genéricos de  $X$ . Os complementos deles,  $A_1^c, A_2^c, \dots, A_n^c, \dots$  são magros, de acordo com o lema C.4.26. Evidentemente, a união de uma família enumerável das partes magros,

$$\bigcup_{n=1}^{\infty} A_n^c,$$

é magra. Logo, o complemento desta união,

$$\left( \bigcup_{n=1}^{\infty} A_n^c \right)^c = \bigcap_{n=1}^{\infty} A_n,$$

é co-magro (= genérico). □

*Observação C.4.29.* Na matemática, uma *propriedade* dos elementos de um conjunto  $X$  é mais ou menos sinônimo com uma *parte* de  $X$ , mesmo se habitualmente uma “propriedade” significa uma parte que pode ser definida por uma formula lógica.

**Corolário C.4.30.** *Seja*

$$\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_n, \dots$$

*uma sequência de propriedades de elementos de um espaço métrico completo,  $X$ . Suponhamos que todas as propriedades  $\mathcal{P}_n$  são genéricas. Então, a conjunção infinita delas,*

$$\mathcal{P}_1 \wedge \mathcal{P}_2 \wedge \dots \wedge \mathcal{P}_n \wedge \dots$$

*é uma propriedade genérica. Em particular, existe pelo menos um elemento  $x \in X$  que verifica todas as propriedades  $\mathcal{P}_n$ .*

Este resultante potente se aplica frequentemente às propriedades diversas de funções, por exemplo umas funções contínuas, diferenciáveis, e cetera. Neste caso, o espaço métrico em questão consiste de funções.

**Exemplo C.4.31.** A família das todas as funções contínuas  $f: [0, 1] \rightarrow \mathbb{R}$  que são não diferenciáveis em todos os pontos  $t \in [0, 1]$  do intervalo é co-magro no espaço métrico  $C[0, 1]$  das todas as funções contínuas reais sobre o intervalo, munido da distância uniforme:

$$d(f, g) = \sup_{t \in [0, 1]} |f(t) - g(t)|.$$

Em outras palavras, uma função contínua genérica sobre o intervalo fechado é não diferenciável em todos os pontos do intervalo. A demonstração é não completamente óbvia, mas eu acho que ela pode ser reconstruída diretamente, sem utilizar os livros.

# D

## *Espaços borelianos padrão. Teorema de isomorfismo*

---

Recordemos a definição seguinte da subseção [A.0.5](#).

**Definition D.0.1.** Um *espaço boreliano padrão* é um par  $(\Omega, \mathcal{B})$  que consiste de um conjunto  $\Omega$  e uma sigma-álgebra  $\mathcal{B}$ , que é uma estrutura boreliana gerada por uma métrica completa e separável sobre  $\Omega$ .

Neste apêndice, vamos mostrar o teorema seguinte (teorema [A.0.25](#) do Apêndice A).

**Teorema D.0.2.** *Dois espaços borelianos padrão são isomorfos se e somente se eles tem a mesma cardinalidade.*

Necessidade é trivial. Para mostrar a suficiência, notemos que se  $\Omega$  é enumerável, então a estrutura boreliana correspondente consiste de todos os subconjuntos de  $\Omega$ :

$$\mathcal{B} = 2^\Omega.$$

De fato, todo conjunto unitário de um espaço métrico é fechado, logo boreliano, e num espaço enumerável cada subconjunto é a união de uma família enumerável de conjuntos



unitários. Por isso,  $\Omega$  é Borel isomorfo ao (único) espaço métrico da mesma cardinalidade munido da distância zero-um.

Eis um exercício para ilustrar a noção de um isomorfismo boreliano (definição A.0.24).

**Exercício D.0.3.** Seja  $\Omega$  um espaço boreliano não enumerável, e seja  $A \subseteq \Omega$  um subconjunto enumerável. Mostrar que os espaços borelianos  $\Omega$  e  $\Omega \setminus A$  são isomorfos (compare o exercício A.0.12).

[ *Sugestão:* escolha um subconjunto enumerável infinito qualquer  $Z \subseteq \Omega \setminus A$ , assim que uma bijeção qualquer  $\phi: A \cup Z \rightarrow Z$ . Agora verifica que a bijeção entre  $\Omega$  e  $\Omega \setminus A$ , dada por

$$\Omega \ni x \mapsto \begin{cases} x, & \text{se } x \in \Omega \setminus (A \cup Z), \\ \phi(x), & \text{se } x \in A \cup Z, \end{cases}$$

é um isomorfismo boreliano. ]

Relembremos que o *espaço de Baire* (exemplo C.2.16) é o conjunto  $\mathbb{N}^{\mathbb{N}}$  de todas as seqüências de números naturais, munido da métrica

$$d(x, y) = \begin{cases} 0, & \text{se } x = y, \\ 2^{-\min\{i : x_i \neq y_i\}}, & \text{caso contrário.} \end{cases}$$

(Assim, a topologia do espaço de Baire é a topologia produto, no sentido da sub-seção C.2.14, sobre a potência infinita enumerável de  $\mathbb{Z}$  munido da topologia discreta.)

**Exercício D.0.4.** Mostrar que o espaço de Baire é completo e separável.

**Exercício D.0.5.** (\*) Mostrar que, como espaço topológico, o espaço de Baire é homeomorfo ao espaço  $\mathbb{R} \setminus \mathbb{Q}$  de números irracionais.

Agora basta mostrar o resultado seguinte.

**Teorema D.0.6.** *Cada espaço boreliano padrão não enumerável é isomorfo ao espaço de Baire  $\mathbb{N}^{\mathbb{N}}$  com a sua estrutura boreliana canônica.*

Segue-se que, como espaços borelianos,  $\mathbb{R}$ ,  $\mathbb{R}^d$ ,  $\ell^2$ , o espaço de Cantor  $C$ , todos os espaços de Banach separáveis não triviais, etc., são dois a dois isomorfos. A prova do teorema D.0.6 ocupa o resto do apêndice.

**Definição D.0.7.** Um subconjunto  $G$  de um espaço métrico  $(X, d)$  é dito um *subconjunto  $G_\delta$*  se existe uma família enumerável de conjuntos abertos  $U_n, n \in \mathbb{N}$ , tal que

$$G = \bigcap_{i \in \mathbb{N}} U_n.$$

Por exemplo, todo subconjunto aberto é  $G_\delta$ .

**Exercício D.0.8.** Mostrar que todo subconjunto fechado de um espaço métrico é um conjunto  $G_\delta$ .

**Teorema D.0.9.** *Seja  $(X, d)$  um espaço métrico, e seja  $Y$  um sub-espaço que admite uma métrica  $\rho$  completa e equivalente a  $d|_Y$  (isto é,  $\rho$  e  $d$  induzem a mesma topologia sobre  $Y$ ). Então  $Y$  é um subconjunto  $G_\delta$  em  $X$ .*

**Exercício D.0.10.** Mostre que um subconjunto  $Y$  de um espaço métrico  $X$  é um  $G_\delta$  em  $X$  se e somente se  $Y$  é um  $G_\delta$  na sua aderência  $\bar{Y}^X$ .

Portanto, na prova do teorema D.0.9 suponha sem perda de generalidade que  $Y$  é denso em  $X$ . Seja  $x \in X \setminus Y$  qualquer. Para cada  $\varepsilon > 0$ , a bola aberta  $B_\varepsilon(x)$  encontra  $Y$ , então o conjunto  $\bar{B}_\varepsilon(x) \cap Y$  é fechado e não vazio. Se  $\varepsilon_n \downarrow 0$ , a sequência de fechados  $\bar{B}_{\varepsilon_n}(x) \cap Y$  em  $Y$  é encaixada e tem a interseção vazia. Exercício C.3.13 implica que os diâmetros destes conjuntos em relação à métrica  $\rho$  não convergem para zero. Denotemos

$$\begin{aligned} D(x) &= \inf_{\varepsilon > 0} \text{diam}_\rho \bar{B}_{\varepsilon_n}(x) \cap Y \\ &= \lim_{\varepsilon \downarrow 0} \text{diam}_\rho \bar{B}_{\varepsilon_n}(x) \cap Y, \end{aligned}$$

onde os diâmetros são calculados em  $(Y, \rho)$ . Para cada  $\delta > 0$ , denotemos

$$A_\delta = \{x \in X : D(x) \geq \delta\}.$$

**Exercício D.0.11.** Mostre que

$$X \setminus Y = \bigcup_{\delta > 0} A_\delta.$$

**Exercício D.0.12.** Mostre que  $A_\delta$  é fechado em  $X$ .

Para estabelecer o teorema D.0.9, é bastante observar que se  $\delta \leq \delta'$ , então  $A_\delta \supseteq A_{\delta'}$ , e combinar os exercícios acima.  $\square$

**Teorema D.0.13.** *Seja  $(X, d)$  um espaço métrico completo, e seja  $Y$  um subconjunto  $G_\delta$  de  $X$ . Então  $Y$  admite uma métrica equivalente completa,  $\rho$ . Além disso,  $\rho$  pode ser escolhida da maneira que  $\rho \geq d|_Y$ , ou seja, quais quer sejam  $x, y \in Y$ ,*

$$d(x, y) \leq \rho(x, y).$$

Começamos com um passo intermediário, o caso onde  $Y$  é aberto em  $X$ .

**Exercício D.0.14.** Seja  $f$  uma função real sobre um conjunto  $X$ . Mostre que a fórmula

$$d(x, y) = |f(x) - f(y)|$$

defina uma pseudométrica sobre  $X$  (ou seja, uma função real de dois argumentos que satisfaz os axiomas 2 e 3 de uma métrica).

**Exercício D.0.15.** Seja  $U$  um subconjunto aberto de um espaço métrico completo  $X = (X, d)$ . Mostre que a métrica  $\rho_U$  sobre  $U$ , definida pela fórmula

$$\rho_U(x, y) = d(x, y) + \min \left\{ 1, \left| \frac{1}{d(x, X \setminus U)} - \frac{1}{d(y, X \setminus U)} \right| \right\},$$

é equivalente a  $d$  e completa.

Agora escolhamos uma sequência de abertos  $(U_n)$  tal que  $\bigcap_n U_n = Y$ . Para cada  $n$  escolhamos uma métrica equivalente e completa sobre  $U_n$ , limitada por 1.

**Exercício D.0.16.** Mostre que espaço métrico  $\prod_{n=1}^{\infty} U_n$ , munido da métrica

$$d(x, y) = \sum_{n=1}^{\infty} 2^{-n} d_n(x_n, y_n),$$

é completo.

**Exercício D.0.17.** Mostre que a aplicação diagonal

$$Y \ni y \mapsto \Delta(y) = (y, y, y, \dots, y, \dots) \in \prod_n U_n,$$

é um homeomorfismo de  $Y$  com um sub-espaço do produto.

**Exercício D.0.18.** Mostre que a imagem de  $Y$  é fechado dentro de produto.

[ *Sugestão:* se  $x = (x_n)$  não pertence à imagem, então a sequência  $(x_n)$  não é constante.... ]

**Exercício D.0.19.** Deduza o teorema [D.0.13](#).

**Exercício D.0.20.** Seja  $\Omega$  um espaço métrico separável. Denotemos por  $A$  o conjunto de  $x \in \Omega$  com a propriedade que existe  $r > 0$  tal que a bola  $B_r(x)$  é enumerável. Mostrar que  $A$  é enumerável.

**Lema D.0.21.** *Seja  $X$  um espaço métrico separável e completo e não enumerável. Então, dado  $\epsilon > 0$ , existe um subconjunto enumerável  $A \subseteq X$  e uma partição enumerável infinita de  $X \setminus A$ ,*

$$X \setminus A = \bigcup_{i \in \mathbb{N}} G_i, \quad G_i \cap G_j = \emptyset \text{ quando } i \neq j,$$

onde para todo  $i$ ,  $G_i$  é um conjunto  $G_\delta$  não enumerável de diâmetro  $< \epsilon$ .

*Demonstração.* Formemos o conjunto enumerável  $A_1$  como no exercício [D.0.20](#), e definamos  $X' = X \setminus A_1$ . Seja  $0 < \gamma < \epsilon/2$ . Escolha uma sequência densa em  $X'$ ,  $(x_n)$ . Temos  $\bigcup_{i=1}^{\infty} B_\gamma(x_n) = X'$ . Escolha recursivamente uma subsequência, eliminando um ponto  $x_n$  se e somente se  $x_n \in \bigcup_{i=1}^{n-1} \bar{B}_\gamma(x_i)$ , onde as bolas são formadas em  $X'$ . Para

todo  $n$ , defina  $X_n = \bar{B}_\gamma(x_n) \setminus \bigcup_{i=1}^n \bar{B}_\gamma(x_i)$ . Pode ocorrer que esta família seja infinita ou finita, mas ela consiste de conjuntos de diâmetro  $\leq 2\gamma < \epsilon$ , que cobrem  $X'$ .

Agora dividimos  $X_1 = \bar{B}_\gamma(x_1)$ , em “aneis”, a saber: existe uma sequência infinita  $\gamma_m \downarrow 0$ ,  $\gamma_1 = \gamma$ , tal que todo conjunto  $Y_m = \bar{B}_{\gamma_m}(x_1) \setminus \bar{B}_{\gamma_{m+1}}(x_1)$  não é enumerável.

Denotemos por  $G_n$ ,  $n \in \mathbb{N}$  a família infinita que consiste de todos os conjuntos  $Y_m$ ,  $m = 1, 2, \dots$ , e  $X_n$ ,  $n = 2, 3, \dots$ . Para cada um deles, o conjunto  $A_n \subseteq G'_n$  de pontos  $x \in G'_n$  que admitem uma bola  $B_r(x) \cap G'_n$  enumerável é enumerável. Denotaremos  $A_2 = \bigcup_{n \in \mathbb{N}} A_n$ ,  $A = A_1 \cup A_2$ , e  $G_n = G'_n \setminus A$ . Se alguns conjuntos  $G_n$  foram vazios, envelamos-los. Os restantes, junto com  $A$ , satisfazem as conclusões do lema.  $\square$

Vamos terminar a prova do teorema [D.0.6](#).

Denotemos por  $\mathbb{N}^{<\omega}$  o conjunto de todos as sequências finitas dos números naturais. Recursivamente no comprimento  $k = \ell(\bar{n})$  de uma sequência  $\bar{n} \in \mathbb{N}^{<\omega}$  definamos para todo  $\bar{n}$  um subconjunto  $G_{\bar{n}} \subseteq \Omega$ , uma métrica  $\rho_{\bar{n}}$  sobre  $G_{\bar{n}}$ , e um conjunto enumerável  $A_{\bar{n}} \subseteq \Omega$  tais que:

- $G_\emptyset = \Omega$ ,  $\rho_\emptyset = d$ ,
- $G_{\bar{n}}$  é um conjunto  $G_\delta$  em  $\Omega$ ,
- $G_{\bar{n}}$  não é enumerável,
- se o comprimento de  $\bar{n}$  é igual a  $k$ , então para todo  $m \in \mathbb{N}$ ,  $\text{diam}_{\rho_{\bar{n}}}(G_{\bar{n}m}) < 1/k$ ,
- para todo  $\bar{n} \in \mathbb{N}^{<\omega}$ , os conjuntos da forma  $G_{\bar{n}m}$ , onde  $m \in \mathbb{N}$ , formam uma partição de  $G_{\bar{n}} \setminus A_{\bar{n}}$ ,
- a métrica  $\rho_{\bar{n}}$  sobre  $G_{\bar{n}}$  é completa (e automaticamente separável),
- se  $\bar{n} \in \mathbb{N}^{<\omega}$  e  $m \in \mathbb{N}$ , então  $\rho_{\bar{n}m} \geq \rho_{\bar{n}}|_{G_{\bar{n}m}}$ .

Denotemos  $A = \bigcup A_{\bar{n}}$ . Dado um elemento qualquer do espaço de Baire,

$$x = (n_1, n_2, \dots) \in \mathbb{N}^{\mathbb{N}},$$

a sequência encaixada de conjuntos  $G_{(n_1, n_2, \dots, n_k)} \subseteq \Omega$ ,  $k = 1, 2, \dots$ , que correspondem aos prefixos de  $x$ , tem a propriedade  $\text{diam}_d(G_{(n_1, n_2, \dots, n_k)}) \rightarrow 0$ . Segue-se que a sequência de fechos destes conjuntos tem um e apenas um ponto em comum, que denotemos por  $f(x)$  (exercício [C.3.13](#)). Deste modo, a função  $f: \mathbb{N}^{\mathbb{N}} \rightarrow \Omega$  é bem definida. De fato,  $f(x) \in \Omega \setminus A$ : se  $\bar{k}$  é um prefixo de  $x$  qualquer, então os diâmetros de  $G_{\bar{n}}$  convergem para zero relativo a métrica completa  $\rho_{\bar{k}}$ . Por isso,  $f(x) \in G_{\bar{k}}$ . Segue-se que  $f(x) \notin A$ .

A função  $f$  é sobrejetora: se  $y \in \Omega \setminus A$ , então para cada  $k$  existe a única sequência finita  $(n_1, \dots, n_k) \in \mathbb{N}^{<\omega}$ , tal que  $y \in G_{(n_1, \dots, n_k)}$ , e além disso, se  $k < \ell$ , então a sequência do comprimento  $\ell$  começa com os elementos  $n_1, \dots, n_k$ . Deste modo, obtemos uma sequência infinita  $n_1, n_2, \dots, n_k, \dots, n_\ell, \dots$ , cuja imagem por  $f$  é igual a  $y$ .

A função  $f$  é injetora: se dois elementos,  $x$  e  $y$ , de  $\mathbb{N}^{\mathbb{N}}$  são diferentes, existe  $k$  tal que os  $k$ -prefixos de sequências,  $\bar{n}$  e  $\bar{m}$ , não são iguais. Então,  $f(x)$  e  $f(y)$  pertencem aos

dois espaços métricos completos disjuntos,  $(G_{\bar{n}}, \rho_{\bar{n}})$  e  $(G_{\bar{m}}, \rho_{\bar{m}})$ . Graças às propriedades das métricas escolhidas, concluímos que  $f(x) \in G_{\bar{n}}$  e  $f(y) \in G_{\bar{m}}$ , logo  $f(x) \neq f(y)$ .

A função  $f$  é boreliana. Isso é uma consequência imediata dos resultados seguintes.

**Exercício D.0.22.** Sejam  $(\Omega_i, \mathcal{B}_i)$ ,  $i = 1, 2$ , dois espaços borelianos, e  $f: \Omega_1 \rightarrow \Omega_2$  uma função. Suponha que  $\mathcal{B}_2$  seja gerada pela família  $\mathcal{D}$  de subconjuntos de  $\Omega_2$ , ou seja,  $\mathcal{B}_2$  é a menor sigma-álgebra que contém a família  $\mathcal{D}$ . Suponha que para todo  $D \in \mathcal{D}$  o conjunto  $f^{-1}(D)$  é boreliano. Então  $f$  é uma função boreliana.

**Exercício D.0.23.** Mostrar que cada bola aberta de  $\Omega$  é a união de uma (necessariamente enumerável) família de conjuntos da forma  $G_{\bar{n}}$ ,  $\bar{n} \in \mathbb{N}^{<\omega}$ . Deduzir que a família de tais conjuntos gera a estrutura boreliana de  $\Omega$ .

Como  $f^{-1}(G_{\bar{n}})$  é o conjunto aberto de todas as sequências que tem o prefixo  $\bar{n}$ , segue-se que  $f$  é boreliana.

Finalmente,  $f^{-1}$  é boreliana, usando o mesmo resultado e a observação que a imagem por  $f$  de conjunto aberto de todas as sequências que tem o prefixo  $\bar{n}$  do comprimento  $k$  (ou seja, uma bola aberta de raio  $2^{-k+1}$ ) é igual ao conjunto  $G_{\bar{n}} \setminus A$ .

Temos um isomorfismo boreliano  $f: \mathbb{N}^{\mathbb{N}} \rightarrow \Omega \setminus A$ , onde  $A$  é enumerável. O exercício D.0.3 diz que  $\Omega \setminus A$  é isomorfo a  $\Omega$ , o que termina a demonstração.  $\square$

O livro [Kechris 1995] é uma referência padrão da teoria de conjuntos descritiva.

# E

## *Medidas de probabilidade. Teorema de Carathéodory*

---

Neste Apêndice vamos desenvolver alguns ferramentas técnicas necessárias para mostrar a existência de medidas não-atômicas (difusas) e algumas de suas propriedades, assim como definir o produto de uma família de medidas, uma noção indispensável para estudar a independência de variáveis aleatórias.

### E.1 Teorema de extensão de medida

Relembramos a definição seguinte.

**Definição E.1.1.** Seja  $\Omega$  um conjunto não vazio. Uma *sigma-álgebra* de subconjuntos de  $\Omega$  é uma família de subconjuntos de  $\Omega$ ,

$$\mathcal{F} \subseteq 2^\Omega,$$

tal que

1.  $\Omega \in \mathcal{F}$ ,
2. se  $A \in \mathcal{F}$ , então  $A^c \in \mathcal{F}$  (onde  $A^c = \Omega \setminus A$ ).
3. se  $A_1, \dots, A_n, \dots \in \mathcal{F}$  são elementos de  $\mathcal{F}$ , então  $\bigcup_{i=1}^{\infty} A_i \in \mathcal{F}$ .

*Observação E.1.2.* Segue-se que uma sigma-álgebra contem as interseções enumeráveis de seus membros também, assim como o conjunto vazio.

Todavia, vamos começar com uma noção auxiliar de um campo de conjuntos. Os campos são mais fácil a manipular do que as sigma-álgebras.

**Definição E.1.3.** Seja  $\Omega$  um conjunto. Um *campo (field)* de subconjuntos de  $\Omega$  é uma família de subconjuntos de  $\Omega$ ,

$$\mathcal{F}_0 \subseteq 2^\Omega,$$

tal que

1.  $\Omega \in \mathcal{F}_0$ ,
2. se  $A \in \mathcal{F}_0$ , então  $A^c \in \mathcal{F}_0$ ,
3. se  $n \in \mathbb{N}$  e  $A_1, \dots, A_n \in \mathcal{F}_0$  são dois a dois disjuntos, então  $\cup_{i=1}^n A_i \in \mathcal{F}_0$ .

**Exemplo E.1.4.** A família  $\mathcal{F}_0$  de todos os subconjuntos  $A$  do intervalo semi-aberto  $(0, 1]$  que podem ser representados como unões finitas de intervalos semi-abertos,

$$A = (a_1, b_1] \cup (a_2, b_2] \cup \dots \cup (a_k, b_k], \quad k \in \mathbb{N},$$

forma um campo.

**Definição E.1.5.** Un subconjunto  $A$  de  $\{0, 1\}^{\mathbb{N}}$  chama-se um *conjunto cilíndrico* se ele é definido pelo um conjunto finito de coordenadas,  $I$ . Precisamente, existe um conjunto finito  $I \subset \mathbb{N}$  e um conjunto  $B \subseteq \{0, 1\}^I$  tais que

$$A = \pi_I^{-1}(B). \tag{E.1}$$

Aqui,

$$\pi_I: \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^I$$

é a projecção usual, definida por

$$\{0, 1\}^{\mathbb{N}} \ni \omega \mapsto [I \ni i \mapsto \pi_I(\omega)_i := \omega_i \in \{0, 1\}] \in \{0, 1\}^I.$$

**Exemplo E.1.6.** O conjunto

$$A = \{\omega \in \{0, 1\}^{\mathbb{N}} \mid \omega_1 = 0\}$$

é cilíndrico. Neste caso, podemos tomar  $I = \{1\}$  e

$$B = \{0\} \subseteq \{0, 1\} = \{0, 1\}^I.$$

**Exercício E.1.7.** A família de todos os conjuntos cilíndricos de  $\{0, 1\}^{\mathbb{N}}$  é um corpo de conjuntos.

**Definição E.1.8.** Seja  $\mathcal{F}_0$  um corpo de subconjuntos de um conjunto  $\Omega$ . Digamos que a função

$$\mu: \mathcal{F}_0 \rightarrow \mathbb{R}_+$$

é uma medida de probabilidade sobre o corpo  $\mathcal{F}_0$  se ela satisfaz as condições seguintes.

1.  $\mu(\Omega) = 1$ ,
2. se  $A_1, \dots, A_n, \dots \in \mathcal{F}_0$  são elementos de  $\mathcal{F}_0$  dois a dois disjuntos, tais que sua união  $\cup_{i=1}^{\infty} A_i$  pertence a  $\mathcal{F}_0$ , então  $\mu(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mu(A_i)$ .

Tais medidas são fáceis a construir à mão.

**Exemplo E.1.9.** Sobre o corpo  $\mathcal{F}_0$  de subconjuntos de  $(0, 1]$  do exemplo E.1.4, definamos a medida de probabilidade  $P$  por

$$\begin{aligned} \mu(A) &= \mu((a_1, b_1] \cup (a_2, b_2] \cup \dots \cup (a_k, b_k]) \\ &:= l(a_1, b_1] + l(a_2, b_2] + \dots + l(a_k, b_k] \\ &= \sum_{i=1}^k (b_i - a_i), \end{aligned}$$

onde os subintervalos  $(a_i, b_i]$  são dois a dois disjuntos. Todo elemento de  $\mathcal{F}_0$  pode ser representado desta maneira (*exercício*).

**Exercício E.1.10.** Verificar que a definição da medida no exemplo E.1.9 é consistente, ou seja, independente da representação de um conjunto  $A$  como acima, e que trata-se de uma medida de probabilidade no sentido da definição E.1.8.

**Exemplo E.1.11.** Dado um conjunto cilíndrico  $A$  (definição E.1.3), definamos a sua medida por

$$\mu(A) = \frac{\#(B)}{2^{|I|}},$$

onde  $A$  é representado como em Eq. (E.1).

Em outras palavras,  $\mu(A)$  é igual à medida de contagem normalizada do conjunto  $B$  no cubo de Hamming  $\{0, 1\}^I$ .

Precisamos verificar que a definição não depende da escolha de um conjunto de índices  $I$  e um subconjunto  $B \subseteq \{0, 1\}^I$ . Com esta finalidade, notemos que entre todos os  $I$  que permitem uma representação de  $A$  como em Eq. (E.1), então existe o menor conjunto de índices,  $I_0$ . O resto é mais ou menos evidente. (*Exercício*).



É menos óbvio que a medida  $\mu$  é sigma-aditiva. Precisamos demonstrar que, cada vez que um conjunto cilíndrico  $A$  for representado como a união de uma sequência de cilindros disjuntos,  $A_1, A_2, \dots, A_n, \dots$ , temos necessariamente

$$\mu(A) = \sum_i \mu(A_i).$$

Se a sequência terminar, isso é fácil: neste caso basta mostrar a igualdade para  $i = 2$ . Sejam  $A_1, A_2$  dois conjuntos cilíndricos disjuntos, suportados sobre os conjuntos de índices  $I_1$  e  $I_2$  respectivamente. Neste caso, o conjunto  $A_1 \cup A_2$  é um cilindro suportado pelo conjunto de índices  $I = I_1 \cup I_2$ . De fato, temos conjuntos  $B_1, B_2 \subseteq \{0, 1\}^I$  tais que

$$A_1 = \pi_I^{-1}(B_1), \quad A_2 = \pi_I^{-1}(B_2),$$

e por conseguinte  $A_1 \cup A_2 = \pi_I^{-1}(B_1 \cup B_2)$ . Agora temos

$$\begin{aligned} \mu(A_1 \cup A_2) &= \frac{\#(B_1 \cup B_2)}{2^{|I|}} \\ &= \frac{\#(B_1)}{2^{|I|}} + \frac{\#(B_2)}{2^{|I|}} \\ &= \mu(A_1) + \mu(A_2), \end{aligned}$$

como evidentemente  $B_1$  e  $B_2$  são disjuntos.

É o caso difícil onde todos os cilindros  $A_1, A_2, \dots, A_n, \dots$  são dois a dois disjuntos e não vazios? O fato é que este caso nunca ocorre. Com efeito, isso é uma consequência da propriedade fundamental da compacidade do espaço  $\{0, 1\}^{\mathbb{N}}$  munido da topologia padrão de produto, ou seja, a topologia do espaço (ou: cubo) de Cantor.

Para mostrar este fato, vamos reexpressar-o numa forma equivalente.

**Lema E.1.12.** *Se*

$$B_1 \supseteq B_2 \supseteq \dots \supseteq B_n \supseteq \dots$$

*é uma sequência encaixada de subconjuntos cilíndricos não vazias de  $\{0, 1\}^{\mathbb{N}}$ , então*

$$\bigcap_{i=1}^{\infty} B_i \neq \emptyset.$$

Para notar que isso é exatamente o que precisamos, dado uma família  $A_1, A_2, \dots$  de conjuntos cilíndricos dois a dois disjuntos e não vazios, cuja união,  $A$ , é um conjunto cilíndrico, renomeie  $B_i = A \setminus (\bigcup_{j=1}^n A_j)$  e aplica o lema E.1.12.

*Prova do lema E.1.12.* Vamos escolher recursivamente um elemento comum  $\omega$  contido em todos os conjuntos  $B_i$ . Tem um elemento  $\omega_1 \in \{0, 1\}$  com a propriedade seguinte: cada  $A_i$  contem uma palavra que começa com  $\omega_1$ . (Exercício de 30 segundos). Defina  $\omega_1 = \epsilon_1$ . Agora, existe um elemento  $\omega_2$ , igual a 0 ou a 1, com a propriedade: cada  $A_i$ ,  $i \geq 2$ , contem uma palavra cuja primeira coordenada é igual a  $\omega_1$  e a segunda, a  $\omega_2$ . (Porque se não, então...?)

Continuando a repetir este procedimento, obtemos uma sequência  $\omega_1, \omega_2, \omega_3, \dots$  que pertence à interseção de todos os  $A_i$ 's.  $\square$

Os campos em si são pouco importantes, mas eles geram as sigma-álgebras.

**Lema E.1.13.** *Cada campo (e de fato, cada família de subconjuntos de  $\Omega$ ),  $\mathcal{F}_0$ , é contida em uma única menor sigma-álgebra. Em outras palavras, existe uma sigma-álgebra  $\mathcal{F}$  tal que*

$$\mathcal{F}_0 \subseteq \mathcal{F} \subseteq 2^\Omega,$$

e se  $\mathcal{F}_1$  é uma sigma-álgebra qualquer que contem  $\mathcal{F}_0$ , então

$$\mathcal{F} \subseteq \mathcal{F}_1.$$

*Demonstração.* A família, dizemos  $\Phi$ , de todas as sigma-álgebras  $\mathcal{E}$  de subconjuntos de  $\Omega$  com a propriedade  $\mathcal{F}_0 \subseteq \mathcal{E}$  não é vazia (ela contem sempre o conjunto  $2^\Omega$  de partes de  $\Omega$ ), e por conseguinte a interseção,

$$\mathcal{F} := \bigcap \Phi = \bigcap_{\mathcal{E} \in \Phi} \mathcal{E},$$

é uma família bem-definida de subconjuntos de  $\Omega$ . É fácil a verificar que a interseção de uma família de sigma-álgebras é uma sigma-álgebra. E pela definição,  $\mathcal{F}$  é contido em toda sigma-álgebra que contem  $\mathcal{F}_0$ .  $\square$

**Exemplo E.1.14.** Os subconjuntos borelianos de  $\left\{ \begin{array}{l} (0, 1] \\ \{0, 1\}^{\mathbb{N}} \end{array} \right\}$  são exatamente os elementos da menor sigma-álgebra que contem  $\left\{ \begin{array}{l} \text{todo intervalo semi-aberto} \\ \text{todo conjunto cilíndrico} \end{array} \right\}$ , respetivamente.  $\square$

Aqui um resultado extremamente poderoso e útil para construir as medidas.

**Teorema E.1.15** (Teorema de Carathéodory). *Seja  $\mathcal{F}_0$  um corpo de subconjuntos de um conjunto  $\Omega$ , e seja  $\mu: \mathcal{F}_0 \rightarrow \mathbb{R}_+$  uma função tendo as propriedades:*

1.  $\mu(\Omega) = 1$ .
2. Se  $A \in \mathcal{F}_0$ , então  $\mu(A^c) = 1 - \mu(A)$ .
3. Se  $A_1, A_2, \dots, A_n, \dots \in \mathcal{F}_0$  são dois a dois disjuntos e tais que  $\cup_{i=1}^{\infty} A_i \in \mathcal{F}_0$ , então  $\mu(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mu(A_i)$ .

Então existem uma sigma-álgebra  $\mathcal{F}$  que contem  $\mathcal{F}_0$ , e uma medida de probabilidade  $\tilde{\mu}$  definida sobre  $\mathcal{F}$ , de modo que a restrição de  $\tilde{\mu}$  a  $\mathcal{F}_0$  é igual a  $\mu$ :

$$\forall A \in \mathcal{F}_0, \quad \tilde{\mu}(A) = \mu(A).$$

Além disso, a medida de probabilidade  $\tilde{\mu}$  sobre  $\mathcal{F}$  com esta propriedade é única.

O resto da secção é dedicado à demonstração do teorema.

### E.1.1 Medida exterior e conjuntos mensuráveis

**Definição E.1.16.** Seja  $A \subseteq \Omega$  um subconjunto qualquer. A *medida exterior* de  $A$  é o valor

$$\mu^*(A) = \inf \sum_{i=1}^{\infty} \mu(A_i),$$

onde o ínfimo é tomado sobre todas as coberturas enumeráveis  $\{A_i : i \in \mathbb{N}\}$  do conjunto  $A$  com elementos do campo  $\mathcal{F}_0$ :

$$A \subseteq \cup_{i \in \mathbb{N}} A_i, \quad A_i \in \mathcal{F}_0.$$

O ínfimo ao lado direita é bem definido pois todo subconjunto  $A \subseteq \Omega$  admite uma cobertura enumerável pelos elementos de  $\mathcal{F}_0$ , por exemplo,  $A \subseteq \cup \{\Omega\}$ . Além disso, é claro que a soma ao lado direita é sempre menor ou igual a 1.

**Proposição E.1.17.** *A medida exterior tem as propriedades seguintes.*

1.  $\mu^*(\emptyset) = 0$ .
2. (Monotonicidade.) Se  $A \subseteq B$ , então  $\mu^*(A) \leq \mu^*(B)$ .
3. (Subaditividade.) Se  $A_i, i = 1, 2, \dots$  é uma família enumerável de subconjuntos de  $\Omega$ , então

$$\mu^*(\cup_i A_i) \leq \sum_i \mu^*(A_i).$$

*Demonstração.* As duas primeiras propriedades são mais ou menos óbvias. A terceira é uma conseqüência do fato que a soma de uma série absolutamente convergente não é afetada pelos rearranjos dos termos. Seja  $\epsilon > 0$  qualquer. Para cada  $n \in \mathbb{N}_+$ , escolhamos os elementos  $B_{ni} \in \mathcal{F}_0$  da maneira que

$$A_n \subseteq \bigcup_{i=1}^{\infty} B_{ni} \text{ e } \sum_{i=1}^{\infty} \mu(B_{ni}) \leq \mu^*(A_n) + \frac{\epsilon}{2^n}.$$

A família  $(B_{ni})_{n,i=1}^{\infty}$  de elementos do campo  $\mathcal{F}_0$  é enumerável e satisfaz

$$\sum_{n,i=1}^{\infty} \mu(B_{ni}) = \sum_{n=1}^{\infty} \sum_{i=1}^{\infty} \mu(B_{ni}) \leq \sum_{n=1}^{\infty} \mu^*(B_{ni}) + \epsilon.$$

Tomando o ínfimo sobre todos  $\epsilon > 0$ , obtemos a propriedade desejada.  $\square$

Em geral, a medida exterior até não é finitamente aditiva (pelo menos, assumindo o axioma de escolha). Vamos definir uma subclasse de conjuntos sobre qual  $\mu^*$  é sigma-aditiva. Estes conjuntos formam uma sigma-álgebra que contém  $\mathcal{F}_0$ , e são chamados *conjuntos mensuráveis*.

**Definição E.1.18.** Um subconjunto  $A \subseteq \Omega$  diz-se  $\mu$ -mensurável, ou simplesmente *mensurável*, se para todo subconjunto  $B \subseteq \Omega$

$$\mu^*(B) = \mu^*(B \cap A) + \mu^*(B \setminus A).$$

*Observação E.1.19.* Como a medida exterior é subaditiva (proposição E.1.17), sempre temos a desigualdade

$$\mu^*(B) \leq \mu^*(B \cap A) + \mu^*(B \setminus A),$$

quaisquer que sejam  $A$  e  $B$ . Então, um subconjunto  $A \subseteq \Omega$  é mensurável se e somente se, qualquer que seja subconjunto  $B \subseteq \Omega$ , temos a desigualdade

$$\mu^*(B) \geq \mu^*(B \cap A) + \mu^*(B \setminus A).$$

Denotaremos  $\mathcal{M}$  a família de todos os subconjuntos  $\mu$ -mensuráveis de  $\Omega$ .

Substituindo  $B \leftarrow A \cup B$  na definição de um conjunto mensurável, obtemos:

**Proposição E.1.20.** *A medida exterior é finitamente aditiva sobre os conjuntos mensuráveis: se  $A$  e  $B$  são disjuntos e mensuráveis, então  $\mu^*(A \cup B) = \mu^*(A) + \mu^*(B)$ .  $\square$*

Esta propriedade estende-se indutivamente às uniões finitas.

**Proposição E.1.21.** *Todo elemento do campo original  $\mathcal{F}_0$  é um conjunto mensurável, ou seja,*

$$\mathcal{F}_0 \subseteq \mathcal{M}.$$

*Demonstração.* Seja  $A \in \mathcal{F}_0$ , e seja  $B \subseteq \Omega$  qualquer. Dado  $\epsilon > 0$  qualquer, escolhemos uma sequência enumerável  $(A_i)_{i=1}^{\infty}$  de elementos de  $\mathcal{F}_0$  tal que

$$B \subseteq \bigcup_{i=1}^{\infty} A_i$$

e

$$\sum_{i=1}^{\infty} \mu(A_i) \leq \mu^*(B) + \epsilon.$$

Definamos  $A'_i = A_i \cap A$  e  $A''_i = A_i \setminus A$ . Os conjuntos  $A'_i, A''_i$  pertencem ao corpo  $\mathcal{F}_0$ , e

$$B \cap A \subseteq \bigcup_{i=1}^{\infty} A'_i, \quad B \setminus A \subseteq \bigcup_{i=1}^{\infty} A''_i.$$

Por conseguinte,

$$\mu^*(B \cap A) \leq \sum_{i=1}^{\infty} \mu(A'_i) \text{ e } \mu^*(B \setminus A) \leq \sum_{i=1}^{\infty} \mu(A''_i).$$

Notemos que para todo  $i$ ,

$$\mu(A_i) = \mu(A'_i) + \mu(A''_i).$$

Deduzimos das desigualdades acima:

$$\begin{aligned} \mu^*(B) &\geq \sum_{i=1}^{\infty} \mu(A_i) - \epsilon \\ &= \sum_{i=1}^{\infty} \mu(A'_i) + \sum_{i=1}^{\infty} \mu(A''_i) - \epsilon \\ &\geq \mu^*(B \cap A) + \mu^*(B \setminus A) - \epsilon. \end{aligned}$$

Enviando  $\epsilon \rightarrow 0$ , obtemos

$$\mu^*(B) \geq \mu^*(B \cap A) + \mu^*(B \setminus A),$$

o que significa, considerando a observação E.1.19, que  $A$  é mensurável.  $\square$

**Proposição E.1.22.** *A restrição da medida exterior  $\mu^*$  sobre o campo  $\mathcal{F}_0$  é igual à medida  $\mu$ :*

$$\forall A \subseteq \mathcal{F}_0, \quad \mu^*(A) = \mu(A).$$

*Demonstração.* Tomando a cobertura de  $A$  com o único elemento  $A \in \mathcal{F}_0$ , concluímos

$$\mu^*(A) \leq \mu(A).$$

Seja  $\epsilon > 0$  qualquer. Existe uma cobertura enumerável de  $A$  pelos elementos  $A_1, A_2, \dots \in \mathcal{F}_0$  tal que

$$\sum_{i=1}^{\infty} \mu(A_i) \leq \mu^*(A) + \epsilon. \quad (\text{E.2})$$

Os conjuntos

$$A'_i = (A_i \setminus \cup_{j=1}^{i-1} A_j) \cap A$$

pertencem ao campo  $\mathcal{F}_0$ , são dois a dois disjuntos, e a sua união é igual a  $A$ , que é um elemento de  $\mathcal{F}_0$ . Segundo as propriedades de  $P$ ,

$$\mu(A) = \sum_{i=1}^{\infty} \mu(A'_i).$$

Como  $A'_i \subseteq A_i$ , temos

$$\sum_{i=1}^{\infty} \mu(A'_i) \leq \sum_{i=1}^{\infty} \mu(A_i),$$

e graças à Eq. (E.2),

$$\mu(A) \leq \mu^*(A) + \epsilon.$$

Como isso é verdadeiro para todos  $\epsilon > 0$ , concluímos, enviando  $\epsilon \downarrow 0$ , que

$$\mu(A) \leq \mu^*(A).$$

□

**Teorema E.1.23.** *A família  $\mathcal{M}$  de todos os conjuntos mensuráveis forma uma sigma-álgebra.*

*Demonstração.* Somente a sigma-aditividade precisa uma prova, pois as primeiras duas propriedades são mais ou menos evidentes.

Vamos mostrar inicialmente que as uniões finitas de conjuntos mensuráveis são mensuráveis. Basta mostrar para dois conjuntos mensuráveis,  $A_1$  e  $A_2$ . Com esta finalidade, seja  $B \subseteq \Omega$  qualquer. Temos, como  $A_1$  é mensurável,

$$\mu^*(B) = \mu^*(B \cap A_1) + \mu^*(B \setminus A_1),$$

e como  $A_2$  é mensurável,

$$\mu^*(B \setminus A_1) = \mu^*((B \setminus A_1) \cap A_2) + \mu^*(B \setminus A_1 \setminus A_2).$$

Por conseguinte,

$$\begin{aligned} \mu^*(B) &= \mu^*(B \cap A_1) + \mu^*(B \cap (A_2 \setminus A_1)) + \mu^*(B \setminus (A_1 \cup A_2)) \\ &= \mu^*(B \cap (A_1 \cup A_2)) + \mu^*(B \setminus (A_1 \cup A_2)), \end{aligned} \quad (\text{E.3})$$

o que estabelece a mesurabilidade de  $A_1 \cup A_2$ .

Em consequência disso, as interseções finitas e as diferenças de conjuntos mensuráveis são mensuráveis. Concluímos:  $\mathcal{M}$  é um campo.

Seja  $(A_i)_{i=1}^{\infty}$  uma sequência infinita de subconjuntos mensuráveis de  $\Omega$ . Sem perda de generalidade e substituindo para  $A_i$  o conjunto mensurável  $A_i \setminus (\cup_{j=1}^i A_j)$  se for necessário, podemos supor que os conjuntos  $A_i$  são dois a dois disjuntos. Denotemos  $A = \cup_{i=1}^{\infty} A_i$ . Vamos mostrar que  $A$  é mensurável.

Seja  $B \subseteq \Omega$  qualquer. Temos, para todo  $i$ ,

$$\mu^*(B) = \mu^*(\cup_{j=1}^i A_j \cap B) + \mu^*(B \setminus \cup_{j=1}^i A_j).$$

Como a medida exterior é monótona, concluímos

$$\mu^*(B) \geq \mu^*(\cup_{j=1}^i A_j \cap B) + \mu^*(B \setminus A).$$

Como os conjuntos são dois a dois disjuntos e mensuráveis, podemos reescrever a última expressão assim:

$$\mu^*(B) \geq \sum_{j=1}^i \mu^*(A_j \cap B) + \mu^*(B \setminus A).$$

No limite  $i \rightarrow \infty$  temos

$$\mu^*(B) \geq \sum_{j=1}^{\infty} \mu^*(A_j \cap B) + \mu^*(B \setminus A). \quad (\text{E.4})$$

Como  $\mu^*(A \cap B) \leq \sum_{j=1}^{\infty} \mu^*(A_j \cap B)$  (subaditividade de  $\mu^*$ ), temos

$$\mu^*(B) \geq \mu^*(A \cap B) + \mu^*(B \setminus A).$$

A outra desigualdade segue-se da subaditividade da medida exterior:

$$\mu^*(B) \leq \mu^*(A \cap B) + \mu^*(B \setminus A).$$

Combinamos as duas para concluir:

$$\mu^*(B) = \mu^*(A \cap B) + \mu^*(B \setminus A).$$

Isso estabelece que  $A = \cup_{i=1}^{\infty} A_i$  é mensurável.  $\square$

De fato, na prova mostramos algo mais. Substituindo na Eq. (E.4)  $B = A$ , obtemos

$$\mu^*(A) \geq \sum_{j=1}^{\infty} \mu^*(A_j),$$

a junto com a subaditividade, esta desigualdade implica

$$\mu^*(A) = \sum_{j=1}^{\infty} \mu^*(A_j). \quad (\text{E.5})$$

A restrição,  $\tilde{\mu}$ , da medida exterior  $\mu^*$  sobre a sigma-álgebra  $\mathcal{M}$  de conjuntos mensuráveis é uma medida de probabilidade. A restrição de  $\tilde{\mu}$  sobre  $\mathcal{F}_0$  é igual a  $\mu$ .

## E.1.2 Unicidade de extensão

Seja  $\mu_1$  uma medida de probabilidade qualquer, definida sobre a sigma-álgebra  $\mathcal{M}$  e tal que a restrição de  $\mu_1$  sobre  $\mathcal{F}_0$  é igual a  $\mu$ :

$$\forall A \in \mathcal{F}_0, \quad \mu(A) = \mu_1(A).$$

**Lema E.1.24.** *Para todo  $A \in \mathcal{M}$ ,  $\mu_1(A) \leq \tilde{\mu}(A)$ .*

*Demonstração.* Seja  $\epsilon > 0$  qualquer. Segundo a definição de uma medida exterior, existe uma cobertura de  $A$  por elementos de  $\mathcal{F}_0$ ,

$$A \subseteq \cup_{i=1}^{\infty} A_i, \quad A_i \in \mathcal{F}_0,$$

tal que

$$\sum_{i=1}^{\infty} \mu(A_i) \leq \tilde{\mu}(A) + \epsilon.$$

Usando a monotonicidade e  $\sigma$ -subaditividade da medida  $\mu_1$ , obtemos

$$\begin{aligned} \mu_1(A) &\leq \mu_1\left(\bigcup_{i=1}^{\infty} A_i\right) \\ &\leq \sum_{i=1}^{\infty} \mu_1(A_i) \\ &= \sum_{i=1}^{\infty} \mu(A_i) \\ &\leq \tilde{\mu}(A) + \epsilon. \end{aligned}$$

Enviando  $\epsilon \downarrow 0$ , concluímos

$$\mu_1(A) \leq \tilde{\mu}(A).$$

□

Seja  $A \in \mathcal{M}$  qualquer. Lema E.1.24 diz que

$$\mu_1(A) \leq \tilde{\mu}(A),$$

e no mesmo tempo,

$$\mu_1(A^c) \leq \tilde{\mu}(A^c).$$

Por conseguinte,

$$\begin{aligned} \mu_1(A) &= 1 - \mu_1(A^c) \\ &\geq 1 - \tilde{\mu}(A^c) \\ &= \tilde{\mu}(A), \end{aligned}$$

o que significa

$$\mu_1(A) = \tilde{\mu}(A).$$

Concluímos: a extensão da medida é única. Isso termina a demonstração do teorema E.1.15.

Com efeito, nos demonstramos mais. No argumento acima, basta supor que a medida de probabilidade  $\mu_1$  seja definida sobre uma sigma-álgebra, dizemos  $\mathcal{F}_1$ , presa entre  $\mathcal{F}_0$  e  $\mathcal{M}$ ,

$$\mathcal{F} \subseteq \mathcal{F}_1 \subseteq \mathcal{M}.$$

O que nos demonstramos, é o resultado seguinte, uma forma um pouco mais exata do teorema de extensão.



**Teorema E.1.25** (Teorema de Carathéodory). *Seja  $\mathcal{F}_0$  um campo de conjuntos de um conjunto  $\Omega$ , e seja  $\mu: \mathcal{F}_0 \rightarrow \mathbb{R}_+$  uma função com as propriedades*

1.  $\mu(\Omega) = 1$ .

2. se  $A_1, A_2, \dots, A_n, \dots \in \mathcal{F}_0$  são dois a dois disjuntos e  $\cup_{i=1}^{\infty} A_i \in \mathcal{F}_0$ , então  $\mu(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} \mu(A_i)$ .

Denotaremos  $\tilde{\mu}$  a medida de probabilidade sobre a sigma-álgebra  $\mathcal{M}$  de todos os conjuntos  $\mu$ -mensuráveis de  $\Omega$ . Seja  $\mathcal{F}_1$  uma sigma-álgebra qualquer de subconjuntos de  $\Omega$  que satisfaz

$$\mathcal{F}_0 \subseteq \mathcal{F}_1 \subseteq \mathcal{M},$$

e seja  $\mu_1$  uma medida de probabilidade sobre  $\mathcal{F}_1$ , cuja restrição sobre  $\mathcal{F}_0$  é igual a  $\mu$ . Então  $\mu_1$  é igual à restrição de  $\tilde{\mu}$  sobre  $\mathcal{F}_1$ .  $\square$

Este resultado diz que usar a notação  $\tilde{\mu}$  não tem sentido, pois usando a letra  $\mu$  para a medida estendida vai nunca resultar numa ambiguidade.

### E.1.3 Dois exemplos

**Exemplo E.1.26.** O espaço é o espaço de Cantor  $\Omega = \{0, 1\}^{\mathbb{N}}$  de seqüências binárias infinitas. Aqui, o campo  $\mathcal{F}_0$  é formado por todos conjuntos cilíndricos de  $\Omega$ , e os elementos da sigma-álgebra correspondente são os conjuntos borelianos. Os elementos da sigma-álgebra  $\mathcal{M}$  são ditos conjuntos *Haar mensuráveis*. A medida de probabilidade resultante é chamada *medida de Haar*.

*Observação E.1.27.* A maneira de ligá-la com a medida de Haar construída na esfera na seção 1.2, é notar que esta medida vai resultar da mesma construção se  $\{0, 1\}^{\mathbb{N}}$  é visto como um grupo compacto sob adição módulo 1 munida da métrica  $\sum_{i=1}^{\infty} 2^{-i} |\sigma_i - \tau_i|$  (compare também as observações 1.2.4 e 1.2.6). É um exercício interessante.

**Exemplo E.1.28.** O espaço é o intervalo  $(0, 1]$ . Aqui,  $\mathcal{F}_0$  consiste de todos os uniões finitos de intervalos semi-abertos. A sigma-álgebra gerada por  $\mathcal{F}_0$  consiste de conjuntos borelianos do intervalo. Os elementos da família  $\mathcal{M}$  são conjuntos *mensuráveis no sentido de Lebesgue*. A medida de probabilidade estendida é frequentemente denotada  $\lambda$  ou as vezes  $\lambda^{(1)}$ , é dita a *medida de Lebesgue*, ou *medida uniforme* sobre o intervalo.

### E.1.4 $\mathcal{F}$ contra $\mathcal{M}$

Nossa próxima tarefa é mostrar que, de certa forma, a sigma-álgebra gerada por  $\mathcal{F}_0$  já basta para dar vazão às necessidades da probabilidade e teoria de medida.

Estamos sempre no âmbito delineado em E.1.15. Seja  $A \in \mathcal{M}$  um conjunto mensurável qualquer de  $\Omega$ . Para todo  $n \in \mathbb{N}_+$ , podemos cobrir  $A$  com uma família enumerável de elementos de  $\mathcal{F}_0$ ,

$$A \subseteq \cup_{i=1}^{\infty} A_i, \quad A_i \in \mathcal{F}_0$$

de modo que

$$\sum_{i=1}^{\infty} \mu(A_i) \leq \mu(A) + \frac{1}{n}.$$

(Lembra que  $\mu(A)$  é igual à medida exterior  $\mu^*(A)$  para todo conjunto mensurável,  $A$ .)  
Se denota-se

$$B_n = \cup_{i=1}^{\infty} A_i,$$

então

$$A \subseteq B_n$$

e

$$\mu(A) \leq \mu(B_n) \leq \mu(A) + \frac{1}{n}.$$

Além disso,  $B_n \in \mathcal{F}$ . Agora definiremos

$$B = \cap_{i=1}^{\infty} B_n.$$

Claro,  $B \in \mathcal{F}$ . Também,

$$A \subseteq B.$$

Qual quer seja  $n$ ,

$$\mu(B) \leq \mu(B_n) \leq \mu(A) + \frac{1}{n}.$$

De fato, temos

$$\mu(B) \leq \mu(A),$$

e

$$\mu(B) = \mu(A).$$

Ademais,

$$A \Delta B = (A \setminus B) \cup (B \setminus A) = B \setminus A,$$

e como

$$\mu(A) = \mu(B) = \mu(A) + \mu(B \setminus A),$$

concluimos:

$$\mu(A \Delta B) = \mu(B \setminus A) = 0.$$

**Definição E.1.29.** Um conjunto mensurável  $N$  de  $\Omega$  é dito um *conjunto nulo*, ou *conjunto negligenciável*, se  $\mu(N) = 0$ .

Demonstramos o seguinte.

**Teorema E.1.30.** *Sobre as hipóteses do teorema E.1.15, seja  $A$  um subconjunto mensurável de  $\Omega$ . Então existe um subconjunto  $B \in \mathcal{F}$  tal que a diferença simétrica  $A \Delta B$  é negligenciável.*

*Mais exatamente, cada conjunto mensurável  $A \subseteq \Omega$  pode ser representado ou como*

$$A = B \setminus N,$$

*onde  $B \in \mathcal{F}$  e  $N$  é negligenciável, ou como*

$$A = B \cup N,$$

*onde de novo  $B \in \mathcal{F}$  e  $N$  é negligenciável. □*

(A última representação é obtida pela aplicação do resultado ao complemento  $A^c$ .)

**Exercício E.1.31.** *Seja  $N$  um conjunto negligenciável. Mostre que qualquer subconjunto  $A \subseteq N$  é mensurável (logo, certamente, negligenciável).*

*Observação E.1.32.* Tipicamente, há muito mais conjuntos mensuráveis do que elementos de  $\mathcal{F}$  (por exemplo, conjuntos borelianos). Por exemplo, no caso do intervalo unitário  $(0, 1]$  assim como do espaço de Cantor  $\{0, 1\}^{\mathbb{N}}$ , pode-se mostrar que a cardinalidade da família de todos os conjuntos borelianos (elementos de  $\mathcal{F}$ ) é a do contínuo,  $c = 2^{\aleph_0}$ , enquanto a cardinalidade da família de todos os conjuntos mensuráveis é igual a

$$2^c = 2^{2^{\aleph_0}}.$$

(Deixemos ambas afirmações como exercícios para os leitores interessados). Em qualquer caso, segundo o teorema E.1.30, um conjunto mensurável só difere de um elemento apropriado de  $\mathcal{F}$  por uma parte negligenciável, que não importa. □

**Exercício E.1.33.** *Deduzir, sobre as hipóteses do teorema E.1.15, o resultado seguinte. Seja  $f$  uma função  $\mathcal{M}$ -mensurável com valores reais, ou seja, dado  $a, b \in \mathbb{R}$ ,  $a < b$ , a imagem recíproca  $f^{-1}(a, b)$  pertence a  $\mathcal{M}$ . Então existe uma função  $g$   $\mathcal{F}$ -mensurável (para todos  $a, b$ ,  $g^{-1}(a, b)$  pertence a  $\mathcal{F}$ ) tal que  $f$  e  $g$  só diferem sobre um conjunto  $\mu$ -negligenciável:*

$$\mu\{x \in \Omega : f(x) \neq g(x)\} = 0.$$

[ *Sugestão:* aplicar o teorema E.1.30 recursivamente a cada conjunto da forma  $f^{-1}(a, b)$  com  $a, b$  racionais... ]

## E.1.5 Completamento de um espaço probabilístico

Seja  $(\Omega, \mathcal{F}, \mu)$  um espaço probabilístico qualquer. Então, a sigma-álgebra  $\mathcal{F}$  é, em particular, um campo, e o procedimento acima pode se aplicar ao espaço  $(\Omega, \mathcal{F}, \mu)$  também. A sigma-álgebra  $\mathcal{F}$  é estendida até uma sigma-álgebra  $\mathcal{M}$  de todos os conjuntos  $\mu$ -mensuráveis, e a medida de probabilidade  $\mu$  se estende para uma medida de probabilidade (notada normalmente pela mesma letra) sobre  $\mathcal{M}$ .

**Definição E.1.34.** O espaço de probabilidade  $(\Omega, \mathcal{M}, \mu)$ , chama-se o *completamento* de  $(\Omega, \mathcal{F}, \mu)$ .

**Definição E.1.35.** Um espaço de probabilidade  $(\Omega, \mathcal{F}, P)$  é dito *completo* se ele coincide com o seu próprio completamento, ou seja, se todo subconjunto  $\mu$ -measurável de  $\Omega$  é já contido em  $\mathcal{F}$ .

Ao cada espaço probabilístico  $(\Omega, \mathcal{M}, \mu)$  podemos associar um espaço pseudométrico, cujo conjunto subjacente é  $\mathcal{M}$  e a pseudométrica é dada por a expressão  $\mu(A \Delta B)$ .

**Exercício E.1.36.** Verifique que a expressão acima é uma pseudométrica (satisfaz axionas 2 e 3 de uma métrica).

A cada espaço pseudométrico pode-se associar um espaço métrico quociente, como descrito no exercício 3.3.1.

**Exercício E.1.37.** Verificar que os espaços métricos quocientes associados a um espaço probabilístico e ao seu completamento são isometricamente isomorfos, e ambos são completos.

Por isso, o nome “completamento de um espaço probabilístico” não é consistente com a estrutura (pseudo)métrica sobre a sigma-álgebra (que é importante na parte principal das nossas notas). Trata-se de completamento num sentido diferente.

Pode-se mostrar que um espaço  $(\Omega, \mathcal{F}, \mu)$  é completo — ou seja, seu completamento não adiciona novos conjuntos mensuráveis — se e somente se cada subconjunto de um conjunto negligenciável  $A \in \mathcal{F}$ ,  $\mu(A) = 0$ , já pertence a  $\mathcal{F}$ . No entanto, temos que parar em algum momento. Deixemos a prova deste critério como um (factível) exercício.

## E.1.6 Produtos de espaços probabilísticos

Seja  $\Omega_\alpha$ ,  $\alpha \in A$ , uma família de espaços probabilísticos, onde  $A$  é um conjunto de índices e para todo  $\alpha \in A$

$$\Omega_\alpha = (\Omega_\alpha, \mathcal{F}_\alpha, P_\alpha).$$

Denotemos por

$$\Omega = \prod_{\alpha \in A} \Omega_\alpha$$

o produto cartesiano da família de conjuntos  $\Omega_\alpha$ ,  $\alpha \in A$ . Em outras palavras, elementos de  $\Omega$  são aplicações  $x: A \rightarrow \cup_{\alpha \in A} \Omega_\alpha$  tendo a propriedade que para todos  $\alpha \in A$

$$x_\alpha = x(\alpha) \in \Omega_\alpha.$$

Axioma da Escolha garante que  $\Omega \neq \emptyset$  (pois os espaços  $\Omega_\alpha$  nunca são vazios).

Para um subconjunto  $I \subseteq A$ , definamos a *projeção canónica*  $\pi_I^A$ , ou simplesmente  $\pi_I$ ,

$$\pi_I: \Omega \ni x \mapsto \pi_I(x) \in \Omega_I,$$

onde

$$\Omega_I = \prod_{\beta \in I} \Omega_\beta$$

e para cada  $\beta \in I$

$$\pi_I(x)_\beta = x_\beta.$$

Por exemplo, se  $I = \{\beta\}$  é um conjunto unitário, obtemos a projeção de  $\beta$ -ésima coordenada,  $\pi_\beta$ , de  $\Omega$  sobre o fator  $\Omega_\beta$ , dada por  $\pi_\beta(x) = x_\beta$ .

Seja  $\Omega_1, \Omega_2, \dots, \Omega_n$  uma sub-coleção finita qualquer de espaços probabilísticos, tendo as sigma-álgebras de conjuntos mensuráveis  $\mathcal{F}_1, \mathcal{F}_2, \dots, \mathcal{F}_n$ , respetivamente. Chamemos um subconjunto  $A \subseteq \prod_{i=1}^n \Omega_i$  *retangular* se  $A$  é da forma

$$A = A_1 \times A_2 \times \dots \times A_n,$$

para apropriados  $A_i \in \mathcal{F}_i$ ,  $i = 1, 2, 3, \dots$ . Chamemos um subconjunto  $B \subseteq \prod_{i=1}^n \Omega_i$  *elementar* se  $B$  é a união de um número finito de subconjuntos retangulares dois a dois disjuntos. A observação seguinte é elementar, embora talvez um pouco tediosa para verificar em todos os detalhes.

**Exercício E.1.38.** Mostre que a coleção de todos os subconjuntos elementares de um produto finito  $\prod_{i=1}^n \Omega_i$  é um campo de conjuntos.  $\square$

Denotemos por  $\mathcal{F}_0$  a família de todos os subconjuntos *cilíndricos*,  $B$ , do produto cartesiano  $\Omega = \prod_{\alpha \in A} \Omega_\alpha$ , ou seja, conjuntos da forma

$$B = \pi_I^{-1}(C),$$

onde  $I \subseteq A$  é *finito*, e  $C \subseteq \prod_{\beta \in I} \Omega_\beta$  é um subconjunto elementar. O seguinte é fácil a mostrar.

**Lema E.1.39.** *A família  $\mathcal{F}_0$  é um campo de subconjuntos de  $\Omega$ .*  $\square$

Agora denotemos por  $\mathcal{F}$  a sigma-álgebra gerada por  $\mathcal{F}_0$ . De modo equivalente,  $\mathcal{F}$  é a menor sigma-álgebra que contém todos os conjuntos da forma  $\pi_\alpha^{-1}(A)$ ,  $A \in \mathcal{F}_\alpha$ ,  $\alpha \in A$ , ou também como a menor sigma-álgebra que torna todas as projeções  $\pi_\alpha$ ,  $\alpha \in A$ , mensuráveis.

Nossa tarefa será de munir  $\Omega$  com uma medida de probabilidade definida sobre a sigma-álgebra  $\mathcal{F}$ . Isto é feito em duas etapas.

**Lema E.1.40.** *Seja  $A \in \mathcal{F}_0$ . Represente  $A$  sob a forma*

$$\pi_I^{-1} \left( \bigcup_{i=1}^k \prod_{j=1}^k A_{ij} \right),$$

onde  $I \subseteq A$  é finito,  $|I| = k$ , a união é a de conjuntos dois a dois disjuntos, e  $A_{ij} \in \mathcal{F}_j$ . Então o número

$$P(A) := \sum_{i=1}^k P_1(A_{i1}) \cdot P_2(A_{i2}) \cdot \dots \cdot P_k(A_{ik})$$

não depende da escolha de uma representação para  $A$  como acima, e determina uma função sobre o campo  $\mathcal{F}_0$  tendo as propriedades

1.  $P(\Omega) = 1$ .
2. Se  $A_1, A_2, \dots, A_n, \dots \in \mathcal{F}_0$  são dois a dois disjuntos e tais que  $\cup_{i=1}^{\infty} A_i \in \mathcal{F}_0$ , então  $P(\cup_{i=1}^{\infty} A_i) = \sum_{i=1}^{\infty} P(A_i)$ .

Deixemos a primeira afirmação como exercício. Além disso, como nós apenas vamos usar produtos enumeráveis, vamos fazer a verificação da segunda afirmação só para eles, porque para os produtos não enumeráveis a sigma-álgebra resultante não é uma estrutura boreliana padrão, e nós não temos ferramentas para lidar com isso.

**Exercício E.1.41.** Suponha que  $|A| \leq \aleph_0$ , e que todos os espaços  $(\Omega_\alpha, \mathcal{F}_\alpha)$  são espaços borelianos padrão. Verificar que o produto  $(\Omega, \mathcal{F})$  é um espaço boreliano padrão. Mais exatamente, sejam  $d_\alpha$  métricas separáveis e completas sobre  $\Omega_\alpha$  gerando as estruturas  $\mathcal{F}_\alpha$ . Então,  $\mathcal{F}$  é gerada por qualquer métrica sobre o produto que gera a topologia produto correspondente.

**Definição E.1.42.** Um espaço métrico  $X$  tem *dimensão zero* se os conjuntos abertos e fechados formam uma *base*, ou seja: dado  $x \in X$  e  $\varepsilon > 0$ , existe um conjunto aberto e fechado,  $V$ , tal que

$$x \in V \subseteq B_\varepsilon(x).$$

**Exemplo E.1.43.** Todo espaço métrico finito tem dimensão zero.

**Exercício E.1.44.** Verifique que o espaço de Cantor  $\{0, 1\}^{\mathbb{N}}$  tem dimensão zero.

**Exercício E.1.45.** Mostre que o espaço  $\mathbb{Q}$  de racionais munido da distância usual tem dimensão zero.

**Exercício E.1.46.** Mostre que qualquer espaço métrico enumerável tem dimensão zero.  
[ *Sugestão:* estudar as funções contínuas  $d(x, -)$  da distância e suas imagens em  $\mathbb{R} \dots$  ]

Agora usamos o teorema de isomorfismo boreliano [D.0.2](#) para realizar cada  $\Omega_\alpha$  como um espaço métrico compacto de dimensão zero, a saber:

- Se  $\Omega$  é finito, será o espaço métrico finito correspondente com qualquer métrica (por exemplo, zero-um).

- Se  $\Omega$  é infinito e enumerável, será o espaço métrico compacto  $\alpha\mathbb{N} = \{0\} \cup \{1/n : n \in \mathbb{N}_+\}$ .
- Se  $\Omega$  tem cardinalidade  $c$ , será o espaço de Cantor  $\{0, 1\}^{\mathbb{N}}$  munido de qualquer métrica gerando a topologia produto, como, por exemplo,  $d(x, y) = 2^{-\min\{i : x_i \neq y_i\}}$ .

**Exercício E.1.47.** Mostrar que o produto de uma família enumerável de espaços métricos de dimensão zero, munido de uma métrica que gera a topologia produto, tem dimensão zero.

Agora o produto  $\Omega = \prod_{\alpha \in A} \Omega_\alpha$  é si mesmo um espaço métrico compacto (exercício C.3.29) de dimensão zero.

**Exercício E.1.48.** Mostre que a família  $\mathcal{F}_{00}$  de todos os conjuntos cilíndricos abertos e fechados forma um corpo em  $\Omega$  e gera a sigma-álgebra  $\mathcal{F}$ .

**Exercício E.1.49.** Use os mesmos argumentos topológicos que no caso particular  $\Omega = \{0, 1\}^{\mathbb{N}_+}$  tratado no exemplo E.1.11 e no lema E.1.12 para mostrar que a função  $\mu$  definida sobre  $\mathcal{F}_{00}$  como no lema E.1.40 satisfaz a conclusão do lema.

Agora apliquemos o teorema de extensão de medidas E.1.15 para concluir que  $\mu$  estende-se até a única medida de probabilidade definida sobre a sigma-álgebra  $\mathcal{F}$ . Esta medida chama-se a *medida produto* é denotada

$$\mu = \otimes_{\alpha \in A} \mu_\alpha.$$

O espaço de probabilidade padrão  $(\Omega, \mathcal{F}, \otimes_{\alpha \in A} P_\alpha)$  se chama o *produto* de espaços de probabilidade padrão  $\Omega_\alpha$ ,  $\alpha \in A$ . No caso onde  $\Omega_\alpha$  são dois a dois isomorfos,  $\Omega_\alpha = \Omega$ , trata-se de uma *potência* de um espaço de probabilidade,  $\Omega^A$ , e a medida produto é denotada  $\mu^{\otimes A}$ .

**Exemplo E.1.50.** O espaço de Cantor munido da medida de Haar,  $\Omega = \{0, 1\}^{\mathbb{N}_+}$ , é a potência infinita enumerável do espaço de Bernulli,  $\{0, 1\}$ , munido da medida de contagem normalizada.

**Exemplo E.1.51.** Se  $\Omega$  é o intervalo unitário  $\mathbb{I} = [0, 1]$  munido da medida de Lebesgue  $\lambda$ , então a potência finita  $\mathbb{I}^n$ ,  $n \in \mathbb{N}$ , é o cubo de dimensão  $n$ , e a medida produto  $\lambda^{\otimes n}$  é a medida de Lebesgue de dimensão  $n$ , denotada  $\lambda^{(n)}$ .

## E.1.7 Realizações de variáveis aleatórias e independência

Já discutimos brevemente a noção de independência de uma família de variáveis aleatórias na seção A.0.6. Relembramos a definição.

**Definição E.1.52.** Uma família  $(X_i)_{i \in I}$  de variáveis aleatórias com valores respetivos em espaços borelianos padrão  $\Omega_i$ ,  $i \in I$  é *independente* se para cada coleção finita de índices,

$i_1, i_2, \dots, i_k$ , é cada coleção de conjuntos borelianos (ou mensuráveis),  $A_1 \in \Omega_{i_1}, A_2 \in \Omega_{i_2}, \dots, A_k \in \Omega_{i_k}$ , temos

$$P(X \in A_1, X_{i_2} \in A_2, \dots, X_{i_k} \in A_k) = P(X_{i_1} \in A_1) \cdot P(X_{i_2} \in A_2) \cdot \dots \cdot P(X_{i_k} \in A_k).$$

Em outras palavras, a lei da variável aleatória

$$(X_i)_{i \in I} \in \prod_{i \in I} \Omega_i$$

é o produto  $\otimes_{i \in I} \mu_i$  das leis  $\mu_i$  de  $X_i$ .

A abordagem comum para tratar as variáveis aleatórias da maneira matematicamente rigorosa e de falar das suas *realizações*.

**Definição E.1.53.** Seja  $X$  uma variável aleatória tomando valores em um espaço boreliano padrão  $\Omega$ , com a lei  $\mu$ . Uma *realização* de  $X$  sobre um espaço probabilístico  $(\mathcal{X}, \nu)$  é qualquer função mensurável  $f: \mathcal{X} \rightarrow \Omega$ , tendo a propriedade

$$f_*(\nu) = \mu.$$

**Exemplo E.1.54.** Toda variável aleatória  $X \in \Omega$  possui a realização canônica que é uma aplicação de identidade:

$$\text{id}_\Omega: \Omega \ni x \mapsto x \in \Omega.$$

*Observação E.1.55.* Temos que uma família de v.a.  $X_i \in \Omega, i \in I$  é independente se e somente se as variáveis  $X_i$  podem ser realizadas simultaneamente como projeções coordenadas

$$\pi_i: \left( \prod_{i \in I} \Omega_i, \otimes_{i \in I} \mu_i \right) \rightarrow \Omega_i.$$

Frequentemente, nenhuma distinção é feita entre uma variável e sua realização, e a mesma letra  $X$  está usada para denotar a última.

A seguinte consequência imediata da existência da medida produto fornece uma fonte rica de variáveis aleatórias independentes.

**Teorema E.1.56.** *Sejam  $\mu_n$  medidas de probabilidade borelianas em espaços borelianos padrão  $\Omega_n, n = 1, 2, 3, \dots$ . Então existe uma sequência independente de v.a.  $X_1, X_2, X_3, \dots$  tais que a lei de cada  $X_n$  é  $\mu_n$ .*  $\square$

*Demonstração.* Cada v.a.  $X_n$  é realizada como a  $n$ -ésima projeção coordenada,  $\pi_n$ , sobre o espaço probabilístico padrão  $(\prod_{n=1}^{\infty} \Omega_n, \otimes_{n=1}^{\infty} \mu_n)$ .  $\square$



*Observação E.1.57.* Uma das perguntas mais intrigantes para o autor — e possivelmente, absurda — é a seguinte. Pode-se dar o significado à frase “os dados são modelados com uma sequência de variáveis aleatórias livres no sentido de Voiculescu”?

As variáveis aleatórias reais limitadas podem ser realizadas como funções mensuráveis sobre um espaço probabilístico padrão  $(\Omega, \mu)$ , ou seja, elementos da álgebra comutativa de funções  $L^\infty(\mu)$ . As variáveis aleatórias livres não são variáveis aleatórias, mas sim, elementos de uma álgebra de operadores *não comutativa* [Voiculescu, Dykema e Nica 1992].

## E.2 Parametrização, regularidade, convergência

### E.2.1 Parametrização de espaços probabilísticos padrão

**Teorema E.2.1.** *Seja  $(\Omega, \mu)$  um espaço probabilístico padrão. Então existe uma aplicação boreliana  $f: [0, 1] \rightarrow \Omega$  tal que a medida  $\mu$  é a imagem direta da medida de Lebesgue (uniforme),  $\lambda$ , sobre o intervalo:*

$$\mu = f_*(\lambda).$$

*Observação E.2.2.* A parametrização é nunca única: por exemplo, o intervalo admite um grupo  $\text{Aut}(\lambda)$  de automorfismos borelianos conservando a medida de Lebesgue, qual grupo é muito rico e interessante.

**Exemplo E.2.3.** O espaço de Bernoulli  $\Omega = \{0, 1\}$  com  $\mu(1) = p, \mu(0) = q, p + q = 1$ , pode ser parametrizado assim:

$$f = \chi_{[0,p]}.$$

**Exercício E.2.4.** Mostre o teorema E.2.1 no caso onde  $\mu$  é puramente atômica. Deduza que será bastante mostrar o teorema para medidas  $\mu$  não atômicas.

**Lema E.2.5.** *Seja  $f: A \rightarrow [0, 1]$  uma função monotona (ou seja, não crescente ou não decrescente), onde  $A \subseteq [0, 1]$  é um subconjunto boreliano. Mostre que  $f$  é boreliana. Se  $A = [0, 1]$ , então a imagem de  $f$  é um espaço boreliano padrão.*

*Demonstração.* A imagem inversa de cada intervalo por  $f$  é a interseção de um intervalo (aberto, semi-aberto, ou fechado) com  $A$ , logo, um conjunto boreliano. Agora suponha que o domínio de  $f$  seja  $[0, 1]$ . A função  $f$  possui, ao máximo, uma família enumerável de discontinuidades de salto, e a cada tal discontinuidade corresponde um intervalo removido do intervalo  $[f(0), f(1)]$ . Um intervalo (seja aberto, semi-aberto, ou fechado) é um conjunto  $F_\sigma$ , ou seja, a união de uma família enumerável de subconjuntos fechados de  $[0, 1]$ . A sua união é um  $F_\sigma$  também, portanto o complemento desta união, que é exatamente a imagem de  $f$ , é um  $G_\delta$ . A topologia de um subconjunto  $G_\delta$  de um espaço métrico completo é gerada por uma métrica completa (que e, claro, separável), segundo o teorema D.0.13, logo o mesmo se aplica à estrutura boreliana de  $f([0, 1])$ .  $\square$

Seja  $\Omega$  um espaço boreliano padrão munido de uma medida de probabilidade  $\mu$  não atômica. Segue-se que  $\Omega$  tem cardinalidade  $c$ . Segundo teorema D.0.2, existe um isomorfismo boreliano  $\phi: \Omega \rightarrow [0, 1]$ . A imagem direta da medida  $\mu$  por  $\phi$  é uma medida de probabilidade não atômica,  $\phi_*(\mu)$ , sobre o intervalo  $[0, 1]$ . A função de distribuição de  $\phi_*(\mu)$ , dada por

$$\Phi(t) = \phi_*(\mu)[0, t) = \mu(\phi^{-1}[0, t)),$$

é contínua e não decrescente,  $\Phi(0) = 0$ ,  $\Phi(1) = 1$ .

**Exercício E.2.6.** Mostrar que a função

$$\begin{aligned} \Phi^{\leftarrow}: [0, 1] &\rightarrow [0, 1], \\ \Phi^{\leftarrow}(x) &= \min\{t : \Phi(t) \geq x\} \end{aligned}$$

é (estritamente) crescente (logo boreliana), e tem a propriedade

$$\Phi_*^{\leftarrow}(\lambda) = \phi_*(\mu).$$

[ *Sugestão*: basta mostrar que para todo  $t \in [0, 1]$ ,

$$\Phi_*^{\leftarrow}(\lambda)[0, t) = \phi_*(\mu)[0, t). ]$$

Por conseguinte, a aplicação boreliana  $\phi^{-1} \circ \Phi^{\leftarrow}: [0, 1] \rightarrow \Omega$  é uma parametrização desejada do espaço probabilístico  $(\Omega, \mu)$ , no caso  $\mu$  é não atômica. O teorema E.2.1 segue-se deste resultado junto com exercício E.2.4.

**Teorema E.2.7.** *Cada espaço boreliano padrão,  $\Omega$ , munido de uma medida de probabilidade não atômica,  $\mu$ , é isomorfo ao intervalo fechado  $[0, 1]$  munido da medida de Lebesgue  $\lambda$ .*

*Observação E.2.8.* Aqui a palavra “isomorfismo” significa um isomorfismo entre dois espaços probabilísticos padrão,  $f: (\Omega, \mu) \rightarrow (\Upsilon, \nu)$ , ou seja, um isomorfismo boreliano  $f$  entre subespaços borelianos padrão  $\Omega'$  e  $\Upsilon'$ , respetivamente, cada um tendo a medida plena, tal que  $f_*(\mu) = \nu$  e  $(f^{-1})_*(\nu) = \mu$ . (Apenas uma de duas condições já basta).

**Exercício E.2.9.** Mostre o teorema E.2.7.

[ *Sugestão*: mostre que a função  $\Phi^{\leftarrow}$  no exercício E.2.6, é bijetora, logo (usando o lema E.2.5) um isomorfismo boreliano entre  $[0, 1]$  e um subespaço boreliano padrão do intervalo de medida um. ]

## E.2.2 Regularidade de medidas

**Teorema E.2.10.** *Toda medida boreliana de probabilidade,  $\mu$ , sobre um espaço métrico  $\Omega$  qualquer (não necessariamente completo ou separável) satisfaz a condição de regularidade seguinte. Seja  $A$  um subconjunto mensurável de  $\Omega$ . Para todo  $\varepsilon > 0$  existem um conjunto fechado,  $F$ , e um conjunto aberto,  $U$ , de  $\Omega$  tais que*

$$F \subseteq A \subseteq U$$

e

$$\mu(U \setminus F) < \varepsilon.$$

*Demonstração.* Consideremos a família  $\mathcal{A}$  de subconjuntos  $A$  de  $\Omega$  que tem a propriedade na conclusão do teorema: dado  $\varepsilon > 0$ , existem um conjunto fechado,  $F$ , e um conjunto aberto,  $U$ , de  $\Omega$  com  $F \subseteq A \subseteq U$  e  $\mu(U \setminus F) < \varepsilon$ . É fácil verificar que  $\mathcal{A}$  forma uma sigma-álgebra (exercício), e contém todos subconjuntos fechados (usa o fato que  $\mu(F_\varepsilon) \downarrow \mu(F)$  quando  $\varepsilon \downarrow 0$ ). Por conseguinte,  $\mathcal{A}$  contém todos os conjuntos borelianos.

Se  $A$  é mensurável, usamos o teorema E.1.30 para achar conjuntos borelianos  $B, B'$  tais que  $B \subseteq A \subseteq B'$  e  $\mu(B' \setminus B) = 0$ . Agora o resultado para conjuntos borelianos permite concluir.  $\square$

Para alguns matemáticos, a palavra “regularidade” significa uma condição mais forte, como no resultado seguinte.

**Teorema E.2.11.** *Toda medida boreliana de probabilidade,  $\mu$ , sobre um espaço métrico  $\Omega$  completo e separável (ou seja, polonês), satisfaz a condição de regularidade seguinte. Seja  $A$  um subconjunto mensurável de  $\Omega$ . Para todo  $\varepsilon > 0$  existem um conjunto compacto,  $K$ , e um conjunto aberto,  $U$ , de  $\Omega$  tais que*

$$K \subseteq A \subseteq U$$

e

$$\mu(U \setminus K) < \varepsilon.$$

Isso é uma consequência do resultado seguinte.

**Teorema E.2.12.** *Seja  $\mu$  uma medida boreliana de probabilidade sobre um espaço métrico  $\Omega$  completo e separável. Para cada  $\varepsilon > 0$ , existe um subconjunto compacto  $K \subseteq \Omega$  com  $\mu(K) > 1 - \varepsilon$ .*

**Exercício E.2.13.** Mostrar que cada espaço métrico separável,  $\Omega$ , tem a *propriedade de Lindelöf*: toda cobertura aberta de  $\Omega$  admite uma sub-cobertura enumerável. (*Advertência*: não é bastante de escolher uma sub-cobertura enumerável de um conjunto enumerável denso, ela pode não cobrir o espaço inteiro...)

*Prova do teorema E.2.12.* Seja  $k \in \mathbb{N}_+$  qualquer. Como  $\Omega$  é separável, existe uma cobertura enumerável de  $\Omega$  com as bolas de raio  $2^{-k}$ :

$$\bigcup_{i=1}^{\infty} B_{2^{-k}}(x_i) = \Omega.$$

Por causa da sigma-aditividade de  $\mu$ ,

$$\mu \left( \bigcup_{i=1}^N \bar{B}_{2^{-k}}(x_i) \right) \uparrow 1 \text{ quando } N \rightarrow \infty,$$

e pode se escolher um  $N_k$  tal que

$$\mu \left( \bigcup_{i=1}^{N_k} \bar{B}_{2^{-k}}(x_i) \right) > 1 - \frac{\varepsilon}{2^k}.$$

O conjunto

$$K = \bigcap_{k=1}^{\infty} \bigcup_{i=1}^{N_k} \bar{B}_{2^{-k}}(x_i)$$

é precompacto (qualquer que seja  $k$ , ele é coberto por uma família finita de bolas fechadas de raio  $2^{-k}$ , logo por uma família finita de bolas abertas de raio ligeiramente maior, digamos  $2^{-k+1}$ ). Ao mesmo tempo,  $K$  é fechado num espaço métrico completo, logo compacto. Finalmente,

$$\mu(\Omega \setminus K) \geq 1 - \sum_{k=1}^{\infty} \mu \left( \Omega \setminus \bigcup_{i=1}^{N_k} \bar{B}_{2^{-k}}(x_i) \right) > 1 - \sum_{k=1}^{\infty} \frac{\varepsilon}{2^k} = 1 - \varepsilon.$$

□

*Demonstração do teorema E.2.11.* Sejam  $F$  e  $U$  como no teorema E.2.10, e  $K$  como no teorema E.2.12. O subconjunto  $K \cap F$  de  $A$  é compacto, e  $\mu(U \setminus K \cap F) \leq 2\varepsilon$ . □

**Teorema E.2.14** (Teorema de Luzin). *Seja  $f$  uma função real mensurável sobre um espaço métrico completo e separável  $\Omega$  munido de uma medida de probabilidade boreliana,  $\mu$ . Dado  $\varepsilon > 0$ , existe um subconjunto compacto  $K \subseteq \Omega$  com  $\mu(\Omega \setminus K) < \varepsilon$  tal que a restrição  $f|_K$  é contínua.*

*Demonstração.* Escolhamos uma sequência somável  $(\varepsilon_n)$ ,  $\varepsilon_n > 0$ , com  $\sum_{n=1}^{\infty} \varepsilon_n = \varepsilon$ . Enumeremos a família de todos os intervalos abertos com pontos extremos racionais:  $(a_n, b_n)$ ,  $n \in \mathbb{N}$ . Para cada  $n$ , o conjunto  $f^{-1}(a_n, b_n)$  é mensurável, e segundo o teorema E.2.11, existem os conjuntos compactos  $K_n \subseteq f^{-1}(a_n, b_n)$  e  $K'_n$ ,  $K'_n \cap f^{-1}(a_n, b_n) = \emptyset$ , e tais que sua união,  $\tilde{K}_n = K_n \cup K'_n$ , satisfaz  $\mu(\tilde{K}_n) > \varepsilon_n$ . Definamos o compacto

$$K = \bigcap_{n=1}^{\infty} \tilde{K}_n.$$

Segue-se que  $\mu(K) > 1 - \sum_{n=1}^{\infty} \varepsilon_n = 1 - \varepsilon$ . Para cada  $n$ , o conjunto  $f^{-1}(a_n, b_n) \cap K$  é aberto em  $K$  porque o seu complemento,

$$K \setminus f^{-1}(a_n, b_n) = K'_n \cap K,$$

é fechado em  $K$ . □

(A prova curta acima pertence a Erik Talvila and Peter Loeb).

*Observação E.2.15.* Diz-se que uma função mensurável é “quase contínua”. Para os espaços com medida mais gerais (não separáveis), a definição acima é usada como a definição de uma função mensurável (funções mensuráveis no sentido de Bourbaki).

*Observação E.2.16.* É claro que o resultado generaliza-se para as funções com valores num espaço métrico separável qualquer, ou mesmo num espaço topológico que tem uma base enumerável de conjuntos abertos.

### E.2.3 Convergência

**Definição E.2.17.** Uma sequência  $X_i, i = 1, 2, \dots$  de variáveis aleatórias com valores em um espaço métrico  $(\Omega, d)$  converge *em probabilidade* para uma v.a.  $X$  se

$$\forall \epsilon > 0, P(d(X_n, X) \geq \epsilon) \rightarrow 0 \text{ quando } n \rightarrow \infty. \quad (\text{E.6})$$

Notação:

$$X_n \xrightarrow{P} X.$$

**Definição E.2.18.** Uma sequência  $X_i, i = 1, 2, \dots$  de variáveis aleatórias com valores em um espaço métrico  $(\Omega, d)$  converge *quase certamente* para uma v.a.  $X$  se

$$P\left(\lim_{n \rightarrow \infty} X_n = X\right) = 1. \quad (\text{E.7})$$

Notação:

$$X_n \xrightarrow{a.s.} X.$$

*Observação E.2.19.* Como interpretar a probabilidade do evento na última definição? Se realizarmos todas as variáveis  $X_n, X$  sobre um espaço probabilístico qualquer,  $(\mathcal{X}, \nu)$ , então trata-se da medida  $\nu$  do conjunto

$$\{\omega \in \mathcal{X} : \lim_{n \rightarrow \infty} X_n(\omega) = X(\omega)\}.$$

Senão, trata-se da medida do conjunto de todas as sequências  $(x, x_1, x_2, \dots, x_n, \dots)$  satisfazendo

$$\lim_{n \rightarrow \infty} x_n = x$$

em relação à medida da lei conjunta de v.a.  $X, X_1, X_2, \dots$ , sobre o espaço  $\Omega^\infty \times \Omega$ . Este espaço probabilístico realiza todas as variáveis aleatórias implicitamente, e cada outra realização delas vai fatorizar através deste espaço.

**Exercício E.2.20.** Mostre que o conjunto acima é boreliano.

**Definição E.2.21.** Uma sequência  $(X_n)$  de variáveis aleatórias converge para uma variável aleatória  $X$  quase certamente se

$$P[X_n \rightarrow X] = 1.$$

**Proposição E.2.22.** A convergência quase certa implica a convergência em probabilidade. Dizendo de outra forma, seja  $X_i, i = 1, 2, \dots$  é uma sequência de variáveis aleatórias com valores em um espaço métrico  $(\Omega, d)$ , e seja  $X$  é uma v.a. com valores em  $\Omega$ . Então a condição

$$X_n \xrightarrow{a.s.} X$$

implica

$$X_n \xrightarrow{p} X.$$

*Demonstração.* Realizemos todas as v.a.  $X_n, X$  sobre um espaço probabilístico qualquer,  $(\mathcal{X}, \nu)$ . Fixemos  $\epsilon > 0$ . Para cada  $N \in \mathbb{N}$ , denotemos

$$A_{N,\epsilon} = \{\omega \in \mathcal{X} : d(X_n(\omega), X(\omega)) < \epsilon \text{ para todos } n \geq N\}.$$

A hipótese que  $X_n$  converge para  $X$  quase certamente implica

$$P\left(\bigcup_{N=1}^{\infty} A_{N,\epsilon}\right) = 1,$$

e como os conjuntos  $A_{N,\epsilon}$  para  $\epsilon$  fixo e  $N$  indo para infinito formam uma sequência encaixada crescente,

$$P(A_{N,\epsilon}) \uparrow 1.$$

Como isto é verdadeiro para cada  $\epsilon > 0$ , concluímos que  $X_n$  convergem em probabilidade para  $X$ .  $\square$

O converso não é verdadeiro.

*Observação E.2.23.* Um *evento* é uma variável aleatória binária. Neste sentido, podemos falar da independência de uma família de eventos. Tipicamente, um evento é da forma  $[X \in A]$ , onde  $X$  é uma v.a. e  $A \subseteq \Omega$  um subconjunto boreliano. A função indicadora  $\chi_A$  uma realização deste evento. Neste sentido, pode-se falar da independência de uma família  $(A_i)$  de subconjuntos mensuráveis de um espaço probabilístico padrão,  $(\mathcal{X}, \nu)$ . Aplicando a definição da independência, concluímos que isso significa o seguinte: para toda coleção finita de índices,  $i_1, i_2, \dots, i_k$ ,

$$\mu(A_{i_1}^* \cap A_{i_2}^* \cap \dots \cap A_{i_k}^*) = \prod_{j=1}^k \mu(A_{i_j}^*),$$

onde  $A_i^*$  significa seja  $A_i$ , seja o seu complemento.

**Exercício E.2.24.** Mostrar o 2o lema de Borel–Cantelli. Seja  $(B_n)$  uma sequência de eventos *independentes* tais que a soma de probabilidades deles é infinita:

$$\sum_{i=1}^{\infty} P(B_n) < +\infty.$$

Então, quase certamente, um número infinito destes eventos ocorre:

$$P[\forall n \exists m \geq n B_m] = 1.$$

Na notação conjuntística: se  $B_1, B_2, \dots$  são independentes e  $\sum_{i=1}^{\infty} \mu(B_n) = +\infty$ , então

$$\mu\left(\bigcap_{n=1}^{\infty} \bigcup_{i=n}^{\infty} B_n\right) = 1.$$

[ *Sugestão*: a probabilidade que só  $n$  deles ocorrem é majorada pela probabilidade que todos eventos  $\bar{B}_i$  complementares a  $B_i$  ocurem para  $i \geq N$ , e agora pode-se usar a independência de  $\bar{B}_i$  e a desigualdade útil  $1 - x \leq e^{-x}$  para  $x \geq 0 \dots$  ]

**Exercício E.2.25.** Construir uma sequência de subconjuntos borelianos  $B_n$  do intervalo  $[0, 1]$  munido da medida de Lebesgue  $\lambda$  tais que  $\lambda(B_n) = 1/n$  e  $B_n$  são independentes. Concluir que as funções indicadores  $\chi_{B_n}$  convergem para zero em medida (e na distância  $L^1$ ), mas para cada  $x$ ,  $\limsup_{n \rightarrow \infty} \chi_{B_n}(x) = 1$ , então a sequência diverge quase em todo ponto.

Portanto, tem algumas situações onde a convergência em probabilidade, ou em esperança, implica a convergência quase certa. Na aprendizagem estatística, uma destas situações é particularmente útil: isso ocorre quando as variáveis aleatórias são altamente concentradas.

**Teorema E.2.26** (Lei Forte dos Grandes Números). *Sejam  $(\Omega, \mu)$  um espaço probabilístico padrão, e  $U$  um subconjunto mensurável. Quase certamente, para um caminho amostral aleatório  $\zeta \sim \mu^\infty$ , a medida empírica de  $U$  com relação ao segmento inicial de  $\zeta$  converge para o valor da medida de  $U$ :*

$$\mu_{\zeta_n}(U) \rightarrow \mu(U).$$

*Demonstração.* Como  $\zeta_n$  é um elemento aleatório de  $\Omega^n$  com a distribuição  $\mu^{\otimes n}$ , a lei

de grandes números implica

$$\begin{aligned}
 P[\mu_{\zeta_n}(U) \rightarrow \mu(U)] &\geq P\left[\exists N \forall m \left| \mu_{\zeta_{N+m}}(U) - \mu(U) \right| \leq \frac{1}{m}\right] \\
 &\geq \sup_N P\left[\forall m \left| \mu_{\zeta_{N+m}}(U) - \mu(U) \right| \leq \frac{1}{m}\right] \\
 &\geq \sup_N \left(1 - 2 \sum_{m=1}^{\infty} e^{-2\varepsilon^2(N+m)}\right) \\
 &= \sup_N \left(1 - 2 \frac{e^{-2\varepsilon^2 N}}{1 - e^{-2\varepsilon^2}}\right) \\
 &= 1.
 \end{aligned}$$

(Acima,  $P$  é a medida  $\mu$ ). □

**Exercício E.2.27.** Mostrar o *lo lema de Borel–Cantelli*. Seja  $(B_n)$  a sequência de eventos (não necessariamente independentes) tais que a soma de probabilidades deles é finita:

$$\sum_{i=1}^{\infty} P(B_n) < +\infty.$$

Então, a probabilidade da ocorrência de um número infinito destes eventos é zero:

$$P[\forall n \exists m \geq n B_m] = 0.$$

Na notação conjuntística: se  $\sum_{i=1}^{\infty} \mu(B_n) < +\infty$ , então

$$\mu\left(\bigcap_{n=1}^{\infty} \bigcup_{i=n}^{\infty} B_n\right) = 0.$$

[ *Sugestão*: o que pode se dizer da série  $\sum_{i=n}^{\infty} \mu(B_n)$ ? ]

O resultado seguinte é uma variação sobre a prova do teorema [E.2.26](#).

**Lema E.2.28.** *Seja  $(\Omega, \mu)$  um espaço probabilístico padrão, e seja  $(f_n)$  uma sequência de funções reais mensuráveis sobre  $\Omega$  satisfazendo uma concentração gaussiana uniforme: para todo  $\varepsilon > 0$  e todo  $n$ ,*

$$\mu\{x \in \Omega : |f_n - \mathbb{E}_{\mu} f_n| > \varepsilon\} \leq C e^{-c\varepsilon^2 n}.$$

*Se  $f_n \rightarrow f$  em probabilidade, então  $f_n \rightarrow f$  quase em toda parte (e  $f$  é uma função constante quase em toda parte).*

*Demonstração.* Exercício. □



# F

## Teoremas de Hahn–Banach e de Stone– Weierstrass

---

### F.1 Espaços normados e espaços de Banach

#### F.1.1 Espaços normados

**Definição F.1.1.** Seja  $E$  um espaço vetorial (real ou complexo). Uma *norma* sobre  $E$  é uma função real

$$N : E \rightarrow \mathbb{R}$$

que verifica as propriedades seguintes:

1.  $N(x) = 0$  se e somente se  $x = 0$ .
2.  $N(\lambda x) = |\lambda|N(x)$  para cada  $x \in E$  e cada  $\lambda \in \mathbb{R}$  (ou  $\lambda \in \mathbb{C}$ ).
3.  $N(x + y) \leq N(x) + N(y)$ .

**Definição F.1.2.** Um espaço vetorial  $E$  munido de uma norma é dito *espaço normado*.

*Observação F.1.3.* Geralmente, o valor de norma de um elemento  $x \in E$  é denotado  $\|x\|$  ao invés de  $N(x)$ .

**Exemplo F.1.4.** Seja  $\Gamma$  um conjunto qualquer. O espaço vetorial  $\ell^\infty(\Gamma)$  é um espaço normado.

**Exemplo F.1.5.** A reta  $\mathbb{R}$  com a sua norma usual

$$\|x\| = |x|$$

é um espaço normado da dimensão 1.

**Exemplo F.1.6.** A norma euclideana padrão sobre o espaço vetorial  $\mathbb{R}^n$ ,  $n \in \mathbb{N}$ , é dada por

$$\|x\|_2 = \sqrt{\sum_{i=1}^n |x_i|^2}.$$

Com efeito, temos já mostrados que  $\|\cdot\|_2$  é uma norma: a propriedade (3) é exatamente a desigualdade de Minkowski.

O espaço  $\mathbb{R}^n$  munido da norma euclideana  $\|\cdot\|_2$  acima é denotado  $\ell^2(n)$ .

**Exemplo F.1.7.** O espaço  $\ell^2$  consiste de todas as sequências de escalares (reais ou complexas) somáveis com quadrado:

$$\sum_{i=1}^{\infty} |x_i| < \infty,$$

munido da norma

$$\|x\|_2 = \sqrt{\sum_{i=1}^{\infty} |x_i|^2}.$$

Mostre que  $\ell^2$  é um espaço normado, desenvolvendo uma versão da desigualdade de Minkowski e imitando a prova no caso de dimensão finita. A norma acima é gerada pelo produto escalar

$$\langle x, y \rangle = \sum_{i=1}^{\infty} x_i y_i.$$

Um pouco mais geralmente, pode-se definir o espaço  $\ell^2(\Gamma)$  a partir de qualquer conjunto  $\Gamma$ . Por exemplo,  $\ell^2(n)$  é  $\ell^2([n])$ , enquanto  $\ell^2$  é  $\ell^2(\mathbb{N}_+)$ . Os vetores  $e_\gamma$ ,  $\gamma \in \Gamma$  formam uma base ortonormal canônica do espaço, onde

$$(e_\gamma)_\delta = \begin{cases} 1, & \text{se } \gamma = \delta, \\ 0, & \text{caso contrário.} \end{cases}$$

*Observação F.1.8.* Seja  $E = (E, \|\cdot\|)$  um espaço normado. Verifica-se facilmente que a fórmula

$$d(x, y) = \|x - y\|$$

define uma métrica sobre  $E$ .

**Exercício F.1.9.** Seja  $E$  um espaço métrico qualquer. Verificar que a adição,

$$E \times E \ni (x, y) \mapsto x + y \in E,$$

todo como a multiplicação escalar,

$$\mathbb{K} \times E \ni (\lambda, x) \mapsto \lambda x \in E,$$

são aplicações contínuas.

## F.1.2 Espaços de Banach

**Definição F.1.10.** Um espaço normado  $E$  é dito *espaço de Banach* se  $E$  é completo como um espaço métrico.

**Exemplo F.1.11.**  $\mathbb{R}$  é um espaço de Banach de dimensão real 1.

**Exercício F.1.12.** Mostrar que os espaços  $\ell^2(n)$  e  $\ell^2$  são espaços de Banach.

**Exemplo F.1.13.**  $\ell^\infty(\Gamma)$  é um espaço de Banach.

*Observação F.1.14.* Pode-se mostrar que cada espaço normado de dimensão finita é um espaço de Banach.

**Exemplo F.1.15.** O espaço  $C(X)$ , onde  $X$  é um compacto, é um espaço de Banach.

**Exemplo F.1.16.** Denotaremos  $c_{00}$  o conjunto de todas as seqüências  $(x_n)$  dos números reais cuja todos os membros, excepto um número finito, são iguais ao zero:

$$\{n : x_n \neq 0\} \text{ é finito.}$$

O sub-espaço vetorial  $c_{00}$  do espaço de Banach  $\ell^\infty$ , munido da norma (e distância) induzida, não é completo.

## F.1.3 Aplicações lineares

**Teorema F.1.17.** *Seja  $f : E \rightarrow F$  uma aplicação linear entre dois espaços normados. As condições seguintes são equivalentes.*

1.  $f$  é contínua.
2.  $f$  é contínua em zero.

3.  $f$  é limitada sobre a bola fechada  $\bar{B}_1(0)$ .  
 4. Existe  $K \geq 0$  tal que para todos  $x \in E$  temos

$$\|f(x)\|_F \leq K \cdot \|x\|_E.$$

5.  $f$  é Lipschitz contínua.  
 6.  $f$  é uniformemente contínua.

*Demonstração.* As implicações (1) $\Rightarrow$ (2), (5) $\Rightarrow$ (6), e (6) $\Rightarrow$ (1) são triviais.

(2) $\Rightarrow$ (3): Suponhamos que  $f$  é contínua em 0. Existe  $\delta > 0$  tal que, para todos  $x \in E$ ,

$$(\|x\|_E < \delta) \Rightarrow (\|f(x)\|_F < 1).$$

Seja  $y \in \bar{B}_\epsilon(0)$ . Então  $\|y\| \leq 1$ , e pois

$$\left\| \frac{2}{\delta} y \right\| \leq \frac{2}{\delta} < \delta,$$

temos

$$\left\| f\left(\frac{2}{\delta} y\right) \right\| < 1,$$

de onde

$$\begin{aligned} \|f(y)\| &= \left\| f\left(\frac{\delta}{2} \cdot \frac{2}{\delta} y\right) \right\| \\ &= \frac{\delta}{2} \left\| f\left(\frac{2}{\delta} y\right) \right\| \\ &< \frac{\delta}{2}. \end{aligned}$$

(3) $\Rightarrow$ (4): Suponha que existe  $K \geq 0$  tal que para todos  $y \in \bar{B}_1(0)$  temos  $\|f(y)\| \leq K$ . Seja  $x \in E$  qualquer. Temos:

$$\left\| \frac{x}{\|x\|} \right\| = \frac{1}{\|x\|} \|x\| = 1,$$

ou seja,

$$\frac{x}{\|x\|} \in \bar{B}_1(0),$$

logo

$$\begin{aligned}\|x\| &= \left\| \|x\| \frac{f(x)}{\|x\|} \right\| \\ &= \|x\| \cdot \left\| f\left(\frac{x}{\|x\|}\right) \right\| \\ &\leq \|x\| \cdot K.\end{aligned}$$

(4) $\Rightarrow$ (5): Suponhamos que existe  $K \geq 0$  tal que para todos  $x \in E$ ,

$$\|f(x)\|_F \leq K \cdot \|x\|_E.$$

Se  $x, y \in E$ , então

$$\begin{aligned}d_F(f(x), f(y)) &= \|f(x) - f(y)\| \\ &= \|f(x - y)\| \\ &\leq K \|x - y\| \\ &= K d_E(x, y).\end{aligned}$$

□

**Corolário F.1.18.** Uma aplicação linear  $f$  entre dois espaços normados é contínua se e somente se a restrição de  $f$  sobre a bola unitária  $B = \bar{B}_1(0)$  de  $E$  é contínua.

**Definição F.1.19.** Digamos que uma aplicação linear  $f: E \rightarrow F$  entre dois espaços normados é *limitada* se ela satisfaz a condição equivalente (4) no teorema F.1.17. O menor valor  $K \geq 0$  como em (4) é chamado a *norma* da aplicação  $f$  (ou: *norma operadora*) e notado  $\|f\|$ . Dito de outro modo,

$$\|f\| = \inf\{K \geq 0: f(B_1(0)) \subseteq B_K(0)\}. \quad (\text{F.1})$$

**Exercício F.1.20.** Sejam  $E$  e  $F$  dois espaços normados. Mostre que a norma operadora é uma norma sobre o espaço linear  $B(E, F)$  de todas as aplicações lineares limitadas de  $E$  para  $F$ , munido com as operações naturais.

**Exercício F.1.21.** Mostre que, se  $F$  é um espaço de Banach, então o espaço  $B(E, F)$  é um espaço de Banach também.

Relembramos que uma aplicação linear com valores no corpo de escalares é dita *funcional linear*.

**Exemplo F.1.22.** O funcional linear  $\delta_0: C[0, 1] \rightarrow \mathbb{R}$ , definido por

$$\delta_0(f) = f(0)$$

(e chamado a *função delta de Dirac*), é limitado, com  $\|\delta_0\| = 1$ .

**Exemplo F.1.23.** O funcional linear  $I : C[0, 1] \rightarrow \mathbb{R}$ , definido por

$$I(f) = \int_0^1 f(x) dx,$$

é limitado, com  $\|I\| = 1$ .

**Exercício F.1.24.** Mostre que cada aplicação linear  $f$  do espaço  $\ell^\infty(n)$  com valores num espaço normado  $F$  qualquer é limitado. Combine esta observação com proposição C.3.38 e corolário F.1.18 para mostrar que cada aplicação linear de um espaço normado de dimensão finita para um espaço normado  $F$  qualquer é limitada.

Os exemplos conduzem-nos de maneira natural à pergunta seguinte. Seja  $E$  um espaço normado de dimensão infinita qualquer. Existem sempre os funcionais lineares limitados sobre  $E$ ? A resposta positiva é dada pelo importante *teorema de Hahn-Banach*, uma das pedras angulares da Análise Funcional.

## F.2 Teorema de Hahn–Banach

### F.2.1 Formulação do teorema de Hahn–Banach

**Teorema F.2.1** (Teorema de Hahn–Banach). *Sejam  $E$  um espaço normado e  $F$  um subespaço vetorial de  $E$ . Seja  $\phi : F \rightarrow \mathbb{R}$  um funcional linear limitado qualquer. Então existe um funcional linear limitado  $\tilde{\phi} : E \rightarrow \mathbb{R}$  que estende  $\phi$ ,*

$$\tilde{\phi}|_F = \phi,$$

e tem a mesma norma,

$$\|\tilde{\phi}\| = \|\phi\|.$$

Como um corolário imediato, funcionais lineares limitados são numerosos sobre cada espaço normado.

**Corolário F.2.2.** *Sejam  $E$  um espaço normado qualquer e  $x \in E$  um vetor,  $x \neq 0$ . Então existe um funcional linear limitado  $\phi$  sobre  $E$  tal que*

- $\|\phi\| = 1$ , e
- $\phi(x) = \|x\|$ .

(Diz-se que  $\phi$  separe  $x$  de zero.)

*Demonstração.* Formemos

$$\mathbb{R}x = \{\lambda x : \lambda \in \mathbb{R}\}$$

um sub-espaço linear de  $E$  de dimensão um. Seja  $\psi : \mathbb{R}x \rightarrow \mathbb{R}$  um funcional dado pela formula seguinte:

$$\psi(\lambda x) = \lambda \|x\|.$$

Este funcional é visivelmente linear. Assim, temos

$$|\psi(\lambda x)| = |\lambda| \cdot \|x\| = \|\lambda x\|,$$

logo  $\psi$  é limitado, da norma um.

De acordo com o teorema de Hahn-Banach F.2.1, existe uma extensão,  $\phi = \tilde{\psi}$ , de  $\psi$  sobre  $E$  da norma um. Em particular,

$$\phi(x) = \psi(x) = \|x\|.$$

□

## F.2.2 Demonstração no caso da codimensão um

Suponha que  $\dim E/F = 1$ , em outras palavras, existe um vetor  $x \in E \setminus F$  tal que o conjunto  $F \cup \{x\}$  gera  $E$  com um espaço vetorial.

**Lema F.2.3.** *Sejam  $G$  um sub-espaço vetorial de um espaço normado  $E$ ,  $g$  um funcional linear limitado sobre  $F$ , e  $x \in E$ . Então existe um funcional linear limitado  $g_1$  sobre o espaço vetorial*

$$G + \mathbb{R}x = \{y + tx : y \in G, t \in \mathbb{R}\},$$

gerado pela união  $G \cup \{x\}$ , cuja restrição sobre  $G$  é igual a  $g$  e tal que  $\|g_1\| = \|g\|$ .

*Demonstração.* Para cada  $y \in G$  definemos

$$\varphi(y) = \|g\| \cdot \|x + y\| - g(y),$$

$$\psi(y) = -\|g\| \cdot \|x + y\| - g(y).$$

Qualquer que sejam  $y, z \in G$ , temos

$$\begin{aligned} \varphi(y) - \psi(z) &= \|g\| (\|x + y\| + \|x + z\|) - g(y - z) \\ &= \|g\| (\|x + y\| + \|-x - z\|) - g(y - z) \\ &\geq \|g\| (\|x + y - x - z\|) - g(y - z) \\ &= \|g\| \cdot \|y - z\| - g(y - z) \\ &\geq 0, \end{aligned}$$

de acordo com a definição da norma  $\|g\|$ . Por conseguinte,

$$\inf_{y \in G} \varphi(y) \geq \sup_{z \in G} \phi(z).$$

Escolhamos  $a \in \mathbb{R}$  de tal modo que

$$\forall y \in G \quad \varphi(y) \geq a \geq \psi(y).$$

Este  $a$  será a imagem de  $x$  por  $g_1$ . Definamos para todos  $t \in \mathbb{R}$  e  $y \in G$

$$g_1(y + tx) = g(y) + ta.$$

Evidentemente,  $g_1$  é uma forma linear sobre  $G + \mathbb{R}x$ . É óbvio que  $g_1|_G = g$ . A fim de verificar que a norma do funcional  $g_1$  não excede a de  $g$ , observemos que para cada  $t \neq 0$ ,

$$\begin{aligned} |g(y) + ta| &= |t| \cdot \left| f\left(\frac{y}{t}\right) + a \right| \\ &\leq |t| \cdot \|g\| \cdot \left\| \frac{y}{t} + a \right\| \\ &= \|g\| \cdot \|y + tx\|. \end{aligned}$$

□

### F.2.3 Demonstração no caso geral

Denotemos  $\mathcal{X}$  a coleção de todos os pares  $(V, \psi)$ , onde

- $V$  é um sub-espaço vetorial de  $E$  tal que  $F \subseteq V \subseteq E$ ,
- $\psi: V \rightarrow \mathbb{R}$  é um funcional linear limitado tal que

$$\begin{aligned} - \| \psi \| &\leq \| \phi \|, \\ - \psi|_F &= \phi. \end{aligned}$$

Digamos que  $(V, \psi) \leq (Z, \zeta)$  se e somente se

- $V \subseteq Z$ , e
- $\zeta|_V = \psi$ .

A relação  $\leq$  acima é uma relação de ordem parcial sobre  $\mathcal{X}$ . A família  $\mathcal{X}$  não é vazia: ela contém o par  $(F, \phi)$ .

Verifiquemos que o conjunto  $\mathcal{X}$  é intuitivo. Seja  $\mathcal{C}$  uma parte de  $\mathcal{X}$  (não vazia) totalmente ordenada qualquer. Definamos

$$V = \cup \{W : \exists \psi, (W, \psi) \in \mathcal{C}\}.$$



É fácil a ver queo sub-conjunto  $V$  de  $E$  é um sub-espaco vetorial. Sejam  $x, y \in V$ . Existem dois pares  $(V, \psi), (Z, \zeta) \in \mathfrak{C}$  tais que  $x \in V$  e  $Y \in Z$ . Porque  $\mathfrak{C}$  é totalmente ordenado, um dos dois é verdadeiro: ou  $(V, \psi) \leq (Z, \zeta)$ , ou  $(Z, \zeta) \leq (V, \psi)$ . Suponhamos sem perda de generalidade o primeiro. Logo  $x, y \in Z$  e, como  $Z$  é um sub-espaco vetorial de  $E$ , temos para todos  $\lambda, \mu \in \mathbb{R}$

$$\lambda x + \mu y \in Z \subseteq V.$$

Porque  $V \supset F \ni 0$ , concluímos.

Para cada  $x \in V$  definamos

$$v(x) = \psi(x),$$

onde  $\psi$  é um funcional linear tal que existe  $W$  com as propriedades  $x \in W$  e  $(W, \psi) \in \mathfrak{C}$ . Esta definição não depende da escolha do par  $(W, \psi)$ . Seja  $(Z, \xi) \in \mathfrak{C}$  tal que  $x \in W$ . Porque  $(W, \psi)$  e  $(Z, \xi)$  são comparáveis, podemos supor que  $(W, \psi) \leq (Z, \xi)$ . Então  $\xi|_W = \psi$ , e porque  $x \in W$ ,

$$\xi(x) = \psi(x).$$

Sejam  $x, y \in V, \lambda, \mu \in \mathbb{R}$ . Existem  $(W, \psi)$  e  $(Z, \xi)$  em  $\mathfrak{X}$  tais que  $x \in W$  e  $y \in Z$ . Como  $(W, \psi)$  e  $(Z, \xi)$  são comparáveis, podemos supor sem perda de generalidade que  $(W, \psi) \leq (Z, \xi)$ . Isso significa que  $x, y \in Z$  e, porque  $Z$  é um sub-espaco vetorial de  $E$  e  $\xi$  é linear sobre  $Z$ , temos

$$v(\lambda x + \mu y) = \xi(\lambda x + \mu y) = \lambda \xi(x) + \mu \xi(y) = \lambda v(x) + \mu v(y).$$

Concluímos: o funcional  $v$  sobre  $V$  é linear.

Se  $x \in F$ , logo, de acordo com a definição de  $V$  temos  $x \in V$ , e de acordo com a definição do funcional  $v$ , temos

$$v(x) = \phi(x),$$

onde conclui-se:

$$v|_F = \phi.$$

Finalmente, seja  $x \in V$  qualquer. Existe um par  $(W, \psi) \in \mathfrak{X}$  tal que  $x \in W$ . Portanto,

$$|v(x)| = |\psi(x)| \leq \|\psi\| \cdot \|x\| \leq \|\phi\| \cdot \|x\|.$$

Concluímos: o funcional  $v$  é limitado, e a sua norma satisfaz:

$$\|v\| \leq \|\phi\|.$$

O par  $(V, v)$  pertence a  $\mathfrak{X}$ , e evidentemente, para todos  $(W, \psi) \in \mathfrak{C}$ , temos

$$(W, \psi) \leq (V, v).$$

O sub-conjunto totalmente ordenado  $\mathfrak{C}$  é portanto majorado.

Graças ao lema de Zorn, existe um elemento maximal,  $(W, \psi)$ , em  $\mathfrak{X}$ . Suponha por absurdo, que  $W \neq E$ . Então existe  $x \in E \setminus W$ . O espaco vetorial  $W + \mathbb{R}x$  é estritamente

maior que  $W$ , e segundo o lema F.2.3 existe um funcional linear  $\tilde{\psi}$  sobre  $W + \mathbb{R}x$  que estende  $\psi$  e cuja norma não excede a de  $\psi$  (portanto, a de  $\phi$ ). Por conseguinte, o par  $(W + \mathbb{R}x, \tilde{\psi})$  é contida em  $\mathfrak{X}$ , e ele é estritamente maior do que  $(W, \psi)$ , uma contradição. Então,  $W = E$ , e o funcional linear  $\tilde{\phi} = \psi$  é uma extensão desejada de  $\phi$  sobre  $E$ .  $\square$

## F.3 Teorema de Stone–Weierstrass

### F.3.1 Formulação do teorema

**Teorema F.3.1** (Teorema de Stone–Weierstrass). *Seja  $X$  um espaço métrico compacto qualquer, e seja  $A$  um conjunto de funções contínuas sobre  $X$  com valores em  $\mathbb{R}$  ou  $\mathbb{C}$  tal que*

1. *A contém todas as funções constantes,*
2. *A é fechado pela adição: se  $f, g \in A$ , então  $f + g \in A$ ,*
3. *A é fechado pela multiplicação: se  $f, g \in A$ , então  $fg \in A$ ,*
4. *A é fechado pela conjugação complexa: se  $f \in A$ , então  $\bar{f} \in A$ ,*
5. *A separa os pontos de  $X$ : se  $x, y \in X$  e  $x \neq y$ , então existe  $f \in A$  tal que  $f(x) \neq f(y)$ .*

Então,  $A$  é uniformemente denso em  $C(X)$ :

$$\bar{A} = C(X).$$

Em outras palavras, cada função contínua  $f: X \rightarrow \mathbb{R}$  pode ser aproximada uniformemente sobre  $X$  por uma seqüência de elementos de  $A$ :

$$\exists g_n \in A \quad g_n \rightrightarrows f.$$

*Observação F.3.2.* No teorema,  $X$  pode ser um espaço topológico compacto qualquer: a existência de uma métrica sobre  $X$  não joga papel nenhum na demonstração.

*Observação F.3.3.* As condições (1)-(3) significam que  $A$  é uma subálgebra (real) de  $C(X)$ . O teorema de Stone-Weierstrass pode ser reformulada como segue: a única subálgebra fechada de  $C(X)$  que separa os pontos de  $C(X)$  é  $C(X)$  própria.

*Observação F.3.4.* Quando  $X = [0, 1]$  e  $A$  consiste de todas as funções polinômias, então as condições (1)-(4) se verificam, e a conclusão do teorema é conhecido como o teorema de Weierstrass.

As versões reais e complexas do teorema são equivalentes.

**Exercício F.3.5.** Mostra que a versão complexa implica a versão real.

[ *Sugestão:* note que se  $A \subseteq C(X, \mathbb{R})$  satisfaz as hipóteses do teorema, então a álgebra  $A + iA \subseteq C(X, \mathbb{C})$  satisfaz as condições também, e se agora  $f_n \in C(X, \mathbb{C})$  e  $f_n \rightarrow f$ ,  $f \in C(X, \mathbb{R})$ , então  $\operatorname{Re} f_n \in C(X, \mathbb{R})$  e  $\operatorname{Re} f_n \rightarrow f$ . ]

**Exercício F.3.6.** Mostra que a versão real implica a versão complexa.

[ *Sugestão:* primeiramente mostre que, qualquer que seja função contínua  $f : X \rightarrow \mathbb{C}$ ,  $f \in A$ , a sua parte real  $\operatorname{Re} f$  e a parte complexa  $\operatorname{Im} f$  pertencem à álgebra  $A$ . Depois mostre que as funções reais em  $A$  satisfazem as condições do teorema. ]

Por conseguinte, basta mostrar apenas a versão real do teorema. Vamos seguir a prova incomum de [Brosowski e Deutsch 1981].

### F.3.2 Alguns resultados técnicos

**Exercício F.3.7.** Mostrar a *desigualdade de Bernoulli*: se  $b \geq -1$  e  $m \geq 1$ , então

$$(1 + b)^m \geq 1 + mb.$$

[ *Sugestão:* use a indução em  $m$ . ]

**Lema F.3.8.** Sob as hipóteses do teorema de Stone-Weierstrass, seja  $x \in X$  e seja  $U$  uma vizinhança de  $x$  quaisquer. Existe uma vizinhança  $V$  de  $x$  tal que  $V \subseteq U$  e qualquer que seja  $\epsilon > 0$ , existe  $f \in A$  com as propriedades

- $f(X) \subseteq [0, 1]$ ,
- $f(V) \subseteq [0, \epsilon]$ ,
- $f(X \setminus U) \subseteq (1 - \epsilon, 1]$ .

*Demonstração.* Sem perda de generalidade e substituindo  $\operatorname{Int} U$  por  $U$  se necessário, podemos supor que  $U$  é aberto. Por conseguinte,  $X \setminus U$  é fechado em  $X$ , logo compacto. Para cada ponto  $y \in X$ , existe uma função  $f_y \in A$  tal que

$$f_y(x) \neq f_y(y).$$

A função

$$h_y = \frac{(f_y - f_y(x))^2}{\| (f_y - f_y(x))^2 \|_\infty}$$

pertence à álgebra  $A$ , toma suas valores no intervalo  $[0, 1]$ , e satisfaz

$$h_y(x) = 0, \quad h_y(y) > 0.$$

Os conjuntos abertos

$$V_y = \{z \in X : f_y(z) > 0\}, \quad y \in X \setminus U$$

cobrem o espaço compacto  $X \setminus U$ . Então, existe uma sub-cobertura finita de  $X \setminus U$ :

$$V_{y_1} \cup V_{y_2} \cup \dots \cup V_{y_m} \supseteq X \setminus U,$$

onde  $y_1, y_2, \dots, y_m \in Y \setminus U$ . A função

$$h = \frac{1}{m} \sum_{i=1}^m h_{y_i}$$

pertence a  $A$ , toma os valores no intervalo  $[0, 1]$ , e satisfaz  $h(x) = 0$ . Se  $z \in X \setminus U$  qualquer, então existe  $i = 1, 2, \dots, m$  tal que  $z \in V_{y_i}$ , e concluímos:

$$h(z) \geq \frac{1}{m} h_{y_i}(z) > 0.$$

Dévido ao segundo teorema de Weierstrass, o ínfimo de  $f$  sobre o espaço compacto  $X \setminus U$  é o mínimo, atingido num ponto  $z_0$ . Concluímos:

$$\forall z \in X \setminus U, \quad h(z) \geq h(z_0) > 0.$$

Escolhamos um valor irracional  $\delta > 0$  tal que  $\delta \leq h(z_0)$ . Temos:

$$\forall z \in X \setminus U, \quad h(z) \geq \delta > 0, \quad \delta \in \mathbb{R} \setminus \mathbb{Q}.$$

Em particular,  $\delta < 1$ . O conjunto aberto

$$V = \left\{ z \in X : h(z) < \frac{\delta}{2} \right\}$$

satisfaz  $x \in V \subseteq U$ . Definamos

$$k = \left\lceil \frac{1}{\delta} \right\rceil.$$

Como  $\delta$  é irracional,  $k > 1/\delta$ , e como  $\delta < 1$ , temos  $k \geq 2$ . Formemos uma sequência dos elementos de  $A$ :

$$q_n(z) = (1 - h^n(z))^{k^n}, \quad n = 1, 2, 3, \dots$$

É claro que os valores de  $q_n$  pertencem ao intervalo  $[0, 1]$ , e  $q_n(x) = 1$ . Analizemos o comportamento das funções  $q_n$  sobre os conjuntos  $V$  e  $X \setminus U$ , separadamente.

(a) Seja  $z \in V$  qualquer. Usando a desigualdade de Bernoulli com  $b = h^n(z)$  e  $m = k^n$ , obtemos

$$\begin{aligned} 1 &\geq q_n(z) \\ &= (1 - h^n(z))^{k^n} \\ &\geq 1 - k^n h^n(z) \\ &> 1 - (kh(z))^n. \end{aligned}$$

Como  $k - 1 < 1/\delta$ ,

$$k < \frac{1}{\delta} + 1 = \frac{\delta + 1}{\delta} < \frac{2}{\delta},$$

e por conseguinte,

$$kh(z) < \frac{2k}{\delta} < \frac{\delta}{2} \cdot \frac{2}{\delta} = 1.$$

Temos, uniformemente sobre  $V$ ,

$$|q_n(z) - 1| \leq \left(\frac{2k}{\delta}\right)^n \rightarrow 0 \text{ quando } n \rightarrow \infty.$$

Concluimos:

$$q_n \xrightarrow{V} 1,$$

uniformemente sobre  $V$ . Dado  $\epsilon > 0$ , se  $n$  é bastante grande,

$$\forall z \in V, |q_n(z) - 1| < \epsilon.$$

(b) Seja  $z \in X \setminus U$  qualquer. Usando a desigualdade de Bernoulli na outra direção, obtemos

$$\begin{aligned} 0 &\leq q_n(x) \\ &= (1 - h^n(z))^{k^n} \\ &= \frac{1}{k^n h^n(z)} \cdot k^n h^n(z) \cdot (1 - h^n(z))^{k^n} \\ &= \frac{1}{k^n h^n(z)} (1 + k^n h^n(z)) (1 - h^n(z))^{k^n} \\ &\leq \frac{1}{k^n h^n(z)} (1 + k^n h^n(z)) (1 - k^n h^n(z)) \\ &= \frac{1}{k^n h^n(z)} (1 - k^{2n} h^{2n}(z)) \\ &\leq \frac{1}{k^n h^n(z)} \\ &< \frac{1}{(k\delta)^n}. \end{aligned}$$

Como  $k > 1/\delta$ , temos

$$\frac{1}{k\delta} < 1,$$

de onde

$$q_n \xrightarrow{X \setminus U} 0,$$

uniformemente sobre  $X \setminus U$ . Dado  $\epsilon > 0$ , se  $n$  é bastante grande,

$$0 \leq q_n(z) < \epsilon$$

para todos  $z \in X \setminus U$ .

Agora, se  $\epsilon > 0$  é qualquer, para  $n$  suficientemente grande, a função

$$f = 1 - q_n$$

possui todas as propriedades desejadas la conclusão do lema.  $\square$

**Lema F.3.9.** *Sobre as hipóteses do teorema de Stone–Weierstrass, sejam  $F$  e  $G$  dois subconjuntos de  $X$  fechados e disjuntos. Seja  $\epsilon > 0$  qualquer. Existe  $f \in A$  tal que*

- $f(X) \subseteq [0, 1]$ ,
- $f(F) \subseteq [0, \epsilon]$ ,
- $f(G) \subseteq (1 - \epsilon, 1]$ .

*Demonstração.* Para cada  $x \in F$ , usando o lema precedente, escolhemos uma vizinhança  $V_x$  de  $x$  com  $U = X \setminus F$ . A cobertura aberta do subconjunto compacto  $G$  de  $X$  pelos conjuntos  $V_x$ ,  $x \in F$ , admite uma sub-cobertura finita

$$V_{x_i}, \quad i = 1, 2, \dots, m.$$

Para cada  $i = 1, 2, \dots, m$ , escolhemos a função  $f_i \in A$  com valores no intervalo  $[0, 1]$  e tal que  $f_i(V_{x_i}) \subseteq [0, \epsilon/m]$ ,  $f_i(G) \subseteq (1 - \epsilon/m, 1]$ . A função

$$f(z) = \prod_{i=1}^m f_i(z)$$

pertence a  $A$  e toma seus valores no intervalo  $[0, 1]$ . Seja  $z \in F$ . Existe  $i = 1, 2, \dots, m$  tal que  $z \in V_{x_i}$ , e por conseguinte

$$f_i(z) < \epsilon/m.$$

Concluimos:

$$f(z) = f_i(z) \times \prod_{j \neq i} f_j(z) \leq \frac{\epsilon}{m} \leq \epsilon.$$

Seja  $z \in G$ . Para cada  $i = 1, 2, \dots, m$ , temos

$$f_i(z) > 1 - \frac{\epsilon}{m},$$

de onde, usando a desigualdade de Bernoulli pela última vez, deduzimos

$$f(z) = \prod_{i=1}^m f_i(z) > \left(1 - \frac{\epsilon}{m}\right)^m \geq 1 - m \cdot \frac{\epsilon}{m} = 1 - \epsilon.$$

$\square$

### F.3.3 Demonstração do teorema de Stone-Weierstrass

É claro que bastaria aproximar uma função contínua com valores em  $[0, 1]$ . Dada uma função  $f \in C(X)$  tal que  $f(X) \subseteq [0, 1]$ , e um número natural  $n \in \mathbb{N}_+$ , para cada  $i = 0, 1, \dots, n-1$  definamos conjuntos

$$F_i = \left\{ x \in X : f(x) \leq \frac{i}{n} \right\},$$

$$G_i = \left\{ x \in X : f(x) \geq \frac{i+1}{n} \right\}.$$

Para cada  $i$ , os conjuntos  $F_i$  e  $G_i$  são fechados e disjuntos em  $X$ . Segundo lema F.3.9, existe uma função  $g_i : X \rightarrow [0, 1]$ ,  $g_i \in A$ , tal que

$$g_i(F_i) \subseteq [0, 1/n) \text{ e } g_i(G_i) \subseteq (1 - 1/n, 1].$$

Ponhamos

$$g = g(n) = \frac{1}{n} \sum_{i=0}^{n-1} g_i.$$

Obviamente,  $g \in A$  e  $g(X) \subseteq [0, 1]$ . A notação  $g(n)$  sublinha o fato que  $g$  depende de  $n$ . Deste modo, temos uma sequência  $g(n) \in A$ ,  $n = 1, 2, 3, \dots$

Seja  $x \in X$  qualquer. Existe  $i = 0, 1, \dots, n-1$  tal que

$$\frac{i}{n} \leq f(x) \leq \frac{i+1}{n}.$$

Deduzimos que

$$x \in F_j, \quad j = i+1, i+2, \dots, n-1,$$

$$x \in G_j, \quad j = 0, 1, \dots, i-1.$$

Se  $j \geq i+1$ , então  $x \in F_j$ , de onde  $0 \leq g_j(x) < 1/n$ . Se  $j \leq i-1$ , então  $x \in G_j$ , de onde  $1 - 1/n < g_j(x) \leq 1$ . O valor  $g_i(x)$  pode ser qualquer, entre 0 e 1. Somando  $n$  desigualdades e dividindo a soma por  $n$ , concluímos que a diferença entre  $g(x)$  e  $i/n$  é menor que  $2/n$ , e por conseguinte a diferença entre  $g(x)$  e  $f(x)$  é menor que  $3/n$ . Quando  $n \rightarrow \infty$ , temos

$$\| f(x) - g(n)(x) \|_\infty < \frac{3}{n} \rightarrow 0,$$

ou seja,

$$g(n) \rightrightarrows f.$$

# G

## Lema de Kronecker

---

Neste apêndice, vamos estudar os subgrupos aditivos fechados de  $\mathbb{R}^n$ . Começemos acertando que apenas existe uma “topologia natural” sobre um espaço vetorial de dimensão finita.

**Exercício G.0.1.** Verifique que a bola unitária fechada do espaço  $\ell^1(n)$  é igual à envoltória convexa do conjunto  $\pm e_i, i = 1, 2, \dots, n$ , onde  $(e_i)$  são vetores de base:

$$B_{\ell^1(n)} = \left\{ \sum_{i=1}^n \lambda_i e_i : \lambda_i \in [-1, 1], \sum |\lambda_i| \leq 1 \right\}.$$

Deduza que a norma de qualquer funcional linear  $\psi$  sobre  $\ell^1(n)$  é igual a  $\max_{i=1}^n |\psi(e_i)|$ .

**Exercício G.0.2.** Verifique que a bola unitária de  $\ell^\infty(n)$  é igual à envoltória convexa do conjunto de todas as combinações lineares da forma  $\sum_{i=1}^n \varepsilon_i e_i$ , onde  $\varepsilon_i = \pm 1$ .

**Teorema G.0.3.** *As topologias seguintes sobre  $\mathbb{R}^n$  são duas a duas iguais.*

1. *A topologia produto, ou seja, uma topologia metrizável tal que  $x_m \rightarrow x$  se e somente se a  $i$ -ésima coordenada de  $x_m$  converge para a de  $x$ ,  $i = 1, 2, \dots, n$ .*
2. *A topologia gerada por todos os funcionais lineares, ou seja, a menor topologia sobre  $\mathbb{R}^n$  tal que cada funcional linear  $\phi: \mathbb{R}^n \rightarrow \mathbb{R}$  é contínuo.*



3. A topologia gerada pela norma  $\ell^\infty(n)$ .
4. A topologia gerada por qualquer norma sobre  $\mathbb{R}^n$ .
5. A topologia gerada pela norma  $\ell^1(n)$ .

*Demonstração.* Vamos mostrar, de modo circular, que cada topologia é contida na seguinte.

(1)  $\subseteq$  (2) segue do fato que cada projeção coordenada,  $\pi_i$ , é um funcional linear.

(2)  $\subseteq$  (3): temos que mostrar que um funcional linear qualquer,  $\phi$ , sobre  $\ell^\infty(n)$  é limitado. Usando o exercício G.0.2, concluímos:

$$\begin{aligned} \|\phi\| &= \max\left\{\sum_{i=1}^n \varepsilon_i \phi(e_i) : \varepsilon_i = \pm 1\right\} \\ &\leq \sum_{i=1}^n |\phi(e_i)|. \end{aligned}$$

(3)  $\subseteq$  (4): Seja  $\|\cdot\|$  uma norma qualquer sobre  $\mathbb{R}^n$ . Mostremos que existe  $L \geq 0$  tal que a bola  $\ell^\infty(n)$  de raio  $L$  contém a bola unitária  $B_{\|\cdot\|}$ . Como a topologia  $\ell^\infty(n)$  é a de produto, a bola  $B_{\|\cdot\|}$  é compacta. Existe  $\delta > 0$  tão pequeno que os vetores  $\sum_{i=1}^n \varepsilon_i e_i$ ,  $\varepsilon_i = \pm 1$  todos pertencem à bola  $B_{\|\cdot\|}$ . Por conseguinte, o operador identidade  $\text{id}_{\mathbb{R}^n}$  de  $\ell^\infty(n)$  para  $(\mathbb{R}^n, \|\cdot\|)$  é limitado, logo contínuo, e a norma  $\|\cdot\|$  é uma aplicação contínua sobre  $\ell^\infty(n)$  também. Para cada  $N \in \mathbb{N}$  seja  $F_N$  o conjunto de todos  $x \in B_\infty$  tais que  $\|x\| \geq N$ . A continuidade da norma em  $\ell^\infty(n)$  implica que  $F_N$  são compactos. A sequência  $(F_N)$  sendo encaixada, se todos  $F_N \neq \emptyset$ , existe  $x \in B_\infty \cap \bigcap_N F_N$ . Tal  $x$  deve satisfazer  $\|x\| = +\infty$ , o que é impossível.

(4)  $\subseteq$  (5): Seja  $\|\cdot\|$  uma norma qualquer sobre  $\mathbb{R}^n$ . Definamos o operador linear e bijetor  $T: \ell^1(n) \rightarrow \mathbb{R}^n$  por

$$T(e_i) = \|e_i\|^{-1} e_i.$$

Em virtude do exercício G.0.1,  $\|T\| = \max \|e_i\|^{-1} = 1$ , logo  $T$  é limitado e contínuo, e segue-se que a topologia gerada pelas bolas abertas na norma  $\ell^1(n)$  é mais fina do que a topologia gerada pela norma  $\|\cdot\|$ .

(5)  $\subseteq$  (1) Sejam  $(x_m)$  uma sequência de elementos de  $\mathbb{R}^n$  e  $x \in \mathbb{R}^n$  tais que para cada  $i = 1, 2, \dots, n$ ,  $\pi_i(x_m) \rightarrow \pi_i(x)$ . Temos:

$$\begin{aligned} \|x_i - x\|_1 &= \sum_{i=1}^n |x_i - x| \\ &\rightarrow 0, \end{aligned}$$

o que significa que a topologia gerada pela norma  $\ell^1$  é mais fraca do que a topologia produto sobre  $\mathbb{R}^n$ .  $\square$

**Definição G.0.4.** Relembremos que um *grupo* é um conjunto  $G$  munido de uma operação binária, chamado o produto, e um elemento fixo,  $e$ , o *elemento neutro*, tais que o produto é associativo, para todo  $x$ ,  $xe = ex = x$ , e todo elemento  $x$  admite um inverso,  $x^{-1}$ , de modo que  $xx^{-1} = x^{-1}x = e$ .

Um grupo cuja operação é comutativa,  $xy = yx$ , é chamado *abeliano*, e o produto será frequentemente (mas não sempre) denotado  $+$  (notação aditiva).

**Exemplo G.0.5.** Cada espaço linear é um grupo abeliano, onde adição é a operação binária, zero é o elemento neutro, e  $-x$  é o inverso de  $x$ . Em particular,  $\mathbb{R}^n$  é um grupo, e  $\mathbb{Z}^n$  é um subgrupo.

**Exemplo G.0.6.** O grupo  $\mathbb{T} = U(1) = \{z \in \mathbb{C} : |z| = 1\}$  é um subgrupo multiplicativo do grupo  $\mathbb{C}^\times$  de elementos não zero de  $\mathbb{C}$ , munido da multiplicação dos números complexos.

**Exemplo G.0.7.** O grupo simétrico  $S_n$ , que consiste de permutações do conjunto  $[n]$  munidos da operação de composição de funções, não é abeliano.

Dado um grupo  $G$  e um subconjunto  $X \subseteq G$ , existe o menor subgrupo de  $G$  que contém  $X$ .

**Exemplo G.0.8.** O subgrupo de  $\mathbb{R}^n$  gerado pelos vetores básicos,  $e_1, e_2, \dots, e_n$ , é exatamente o grupo  $\mathbb{Z}^n$ .

**Exemplo G.0.9.** Seja  $x \in \mathbb{R}$ ,  $x \neq 0$ . O subgrupo gerado por  $x$  é igual a

$$x\mathbb{Z} = \{xn : n \in \mathbb{Z}\}.$$

**Definição G.0.10.** Um grupo  $G$  munido de uma topologia é dito *grupo topológico* se as operações são contínuas:

$$m: G \times G \ni (g, h) \mapsto gh \in G,$$

$$i: G \ni g \mapsto g^{-1} \in G.$$

**Exercício G.0.11.** Mostre que  $\mathbb{R}^n$  e  $\mathbb{T}^n$  (com a topologia usual) são grupos topológicos.

**Exercício G.0.12.** Seja  $G$  um grupo topológico e  $H$  um sub-grupo. Mostre que a aderência  $\bar{H}^G$  é um subgrupo.

[ *Sugestão:* suponha que  $G$  é metrizável, e deste modo basta trabalhar com as sequências. Mostre que se  $g_n \rightarrow g$  e  $h_n \rightarrow h$ , então  $g_n h_n \rightarrow gh$  e  $g_n^{-1} \rightarrow g^{-1}$ . ]

**Teorema G.0.13.** Cada subgrupo fechado e próprio de  $\mathbb{R}$  é da forma  $x\mathbb{Z}$ ,  $x \neq 0$ .

*Demonstração.* Seja  $G$  um subgrupo fechado de  $\mathbb{R}$ . Se  $G$  contém uma sequência não trivial convergente para zero,  $x_n \rightarrow 0$ , então  $G$  contém todos subgrupos  $x_n\mathbb{Z}$ , cuja união

é densa em  $\mathbb{R}$ , e como  $G$  é fechado,  $G = \mathbb{R}$ . Suponha agora que  $G \neq \{0\}$  e  $G$  não contém seqüências convergentes para zero. Neste caso, o elemento seguinte é bem definido:

$$x = \inf\{g \in G : g > 0\},$$

e como  $G$  é fechado,  $x \in G$ , é um mínimo. Afirmamos que  $x\mathbb{Z} = G$ . É claro que  $x\mathbb{Z} \subseteq G$ . Se existisse  $y \in G \setminus x\mathbb{Z}$ , o elemento  $z = x \lfloor y/x \rfloor$  satisfaria  $z \in x\mathbb{Z}$ ,  $y - z \in G$ , e  $0 < y - z < x$  ( $G$  é um grupo ordenado), o que é impossível.  $\square$

**Lema G.0.14.** *Seja  $x \in \mathbb{R}^n$ . O subgrupo de  $\mathbb{R}^n$  gerado por  $\mathbb{Z}^n \cup \{x\}$  é discreto se e somente se  $x \in \mathbb{Q}^n$ .*

*Demonstração.* Suponha que o grupo  $G$  gerado por  $\mathbb{Z}^n \cup \{x\}$  é discreto, ou seja, não contém seqüências convergentes não triviais. Seja  $g \in G$  qualquer,  $g = (g_1, g_2, \dots, g_n)$ . Para todo  $m \in \mathbb{Z}$ , consideremos o vetor

$$\tilde{g}_m = mg - \sum_{i=1}^n \lfloor mg_i \rfloor e_i = (mg_1 - \lfloor mg_1 \rfloor, mg_2 - \lfloor mg_2 \rfloor, \dots, mg_n - \lfloor mg_n \rfloor).$$

Ele pertence a  $G$ , sendo a diferença de dois elementos de  $G$ , e também pertence à bola  $B_\infty$ . Como a interseção  $G \cap B_\infty$  é finita por causa da compacidade da bola, existem dois inteiros distintos,  $m$  e  $k$ , tais que  $\tilde{g}_m = \tilde{g}_k$ . Por conseguinte,

$$(m - k)g_i = \lfloor mg_i \rfloor - \lfloor kg_i \rfloor, \quad i = 1, 2, \dots, n,$$

o que significa que  $g_i \in \mathbb{Q}$ .

Suponha agora que  $x \in \mathbb{Q}^n$ . Se  $q$  é um denominador comum de  $x_i$ , então o grupo gerado por  $\mathbb{Z}^n \cup \{x\}$  é um subgrupo do grupo discreto  $\frac{1}{q}\mathbb{Z}^n$ .  $\square$

**Lema G.0.15.** *Seja  $G$  um sub-grupo fechado e não discreto de  $\mathbb{R}^n$ . Então,  $G$  contém uma reta passando por 0, ou seja, um sub-grupo fechado da forma  $\mathbb{R}x$ ,  $x \in \mathbb{R}^n$ ,  $x \neq 0$ .*

*Demonstração.* Existe uma seqüência convergente e não trivial,  $x_n \rightarrow x$ ,  $x_n, x \in G$ ,  $x_n \neq x$ . Substituindo  $x_n = x_n - x \in G$ , supomos que  $x_n \rightarrow 0$ . Como  $\|x_n\|_\infty \rightarrow 0$ , temos  $\|x_n\|_\infty^{-1} \rightarrow \infty$ . A seqüência  $\|x_n\|_\infty^{-1} x_n$  pertence à esfera unitária  $S_\infty$  em relação à norma  $\ell^\infty(n)$ , logo converge para um elemento  $x$  da esfera. O mesmo se aplica à seqüência  $\lfloor \|x_n\|_\infty^{-1} \rfloor x_n$ , pois a diferença entre as duas seqüências converge para zero. Como os elementos da última seqüência pertencem a  $G$ , concluímos que  $x \in G$  também. Para todo  $\lambda \in \mathbb{R}$ , os elementos da seqüência

$$\left\lfloor \frac{\lambda}{\|x_n\|_\infty} \right\rfloor \cdot x_n$$

pertencem a  $G$ , e é fácil a ver que a seqüência acima converge para  $\lambda x$ .  $\square$

A reta,  $\mathbb{R}$ , pode ser vista como um espaço vetorial sobre o corpo  $\mathbb{Q}$ .

**Exercício G.0.16.** Mostre que  $\mathbb{R}$ , visto como um espaço vetorial sobre o corpo  $\mathbb{Q}$ , tem dimensão do contínuo,  $c$ .

**Definição G.0.17.** Um conjunto de reais é dito *racionalmente independente* se ele é um conjunto linearmente independente em  $\mathbb{R}$  como um espaço linear sobre  $\mathbb{Q}$ .

**Lema G.0.18.** *Sejam  $1 \leq m \leq n$ , e  $x = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$  um vetor tal que os reais*

$$x_1, x_2, \dots, x_n, 1$$

*são racionalmente independentes. Seja  $A$  uma matriz  $m \times n$  com coeficientes racionais, de posto  $m$ . Então o vetor  $y = Ax$ ,  $y = (y_1, y_2, \dots, y_m)$ , tem a propriedade que os reais*

$$y_1, y_2, \dots, y_m, 1$$

*são racionalmente independentes.*

*Demonstração.* Os reais  $y_1, y_2, \dots, y_m, 1$  são racionalmente independentes se e apenas se, quaisquer que sejam coeficientes racionais  $\lambda_1, \dots, \lambda_m$ , não todos iguais a zero,

$$\sum_{i=1}^m \lambda_i y_i \notin \mathbb{Q}.$$

Temos

$$\begin{aligned} \sum_{i=1}^m \lambda_i y_i &= \sum_{i=1}^m \lambda_i \sum_{j=1}^n a_{ij} x_j \\ &= \sum_{j=1}^n \left( \sum_{i=1}^m \lambda_i a_{ij} \right) x_j, \end{aligned}$$

e como a matriz  $A$  tem posto  $m$  sobre o corpo  $\mathbb{Q}$ , as  $m$  linhas da matriz são linearmente independentes sobre  $\mathbb{Q}$ , ou seja,  $\sum_{i=1}^m \lambda_i a_{ij}$  não se anulam simultaneamente. Graças à hipótese sobre  $x$ , concluímos.  $\square$

**Lema G.0.19.** *Seja  $x = (x_1, x_2, \dots, x_n)$  um vetor em  $\mathbb{R}^n$ , tal que os reais*

$$x_1, x_2, \dots, x_n, 1$$

*são racionalmente independentes, ou seja, linearmente independentes como vetores sobre o corpo  $\mathbb{Q}$ . Então o único subgrupo fechado de  $\mathbb{R}^n$  que contém  $x$  e  $\mathbb{Z}^n$  é  $\mathbb{R}^n$  próprio.*

*Demonstração.* Denotemos  $V$  a união de todas as retas contidas em  $G$  e passando por zero. É claro que  $V$  é um subespaço vetorial de  $\mathbb{R}^n$ . Escolhamos algum subespaço linear  $V'$  complementar a  $V$ , ou seja,  $V' + V = \mathbb{R}^n$ . Denotemos  $G' = G \cap V'$ . Segue-se que  $G = V + G'$ . Segundo o lema G.0.15, o grupo  $G'$  é discreto.

Denotemos  $\pi$  a aplicação linear quociente de  $\mathbb{R}^n$  sobre o espaço linear quociente,  $\mathbb{R}^n/V$ . Entre os vetores  $\pi(e_i)$ ,  $i = 1, 2, \dots, n$ , escolhemos uma base do espaço quociente. Identificamos  $\mathbb{R}^{n+1}/V$  com o espaço  $\mathbb{R}^m$ , onde  $m = n - \dim V$ . O operador  $\pi$ , restrito sobre  $V'$ , é um isomorfismo de  $V'$  com  $\mathbb{R}^m$ , e existem  $m$  vetores de base em  $\mathbb{R}^n$  cujas imagens são vetores de base padrão em  $\mathbb{R}^m$ . Ademais, a imagem de  $G$  por  $T \circ \pi$  é igual a imagem de  $G'$ , logo é um subgrupo discreto. Em virtude do lema G.0.14, a imagens de todos elementos de  $\mathbb{Z}^n$  tem coordenadas racionais, logo a matriz do operador quociente tem coeficientes racionais. Lema G.0.18 diz que as coordenadas de  $\pi(x)$  em  $\mathbb{R}^m$ , mais 1, formam uma família de reais racionalmente independente. Lema G.0.14 implica que isso é apenas possível se  $m = 0$ .  $\square$

**Definição G.0.20.** Um *homomorfismo* entre dois grupos,  $f: G \rightarrow H$ , é uma aplicação que conserva as operações:  $f(gh) = f(g)f(h)$  e  $f(e_G) = e_H$ . O *núcleo* de um homomorfismo é a imagem recíproca de identidade:

$$N = f^{-1}(e).$$

É um *subgrupo normal*, ou seja, um subgrupo  $N$  tendo a propriedade  $x^{-1}Nx = N$  qualquer que seja  $x \in G$ .

**Exemplo G.0.21.** Um homomorfismo contínuo  $f: \mathbb{R} \rightarrow \mathbb{T}$  é dado por

$$f(t) = \exp(2\pi it).$$

Este homomorfismo estende-se até um homomorfismo contínuo entre  $\mathbb{R}^n$  e o toro  $\mathbb{R}^n$ :

$$f(t_1, \dots, t_n) = (\exp(2\pi it_1), \dots, \exp(2\pi it_n)). \quad (\text{G.1})$$

O núcleo deste homomorfismo é o subgrupo  $\mathbb{Z}^n$ . A toro pode ser visto como o *grupo quociente*  $\mathbb{R}^n/\mathbb{Z}^n$ , que consiste de todas as classes de equivalência  $x + \mathbb{Z}^n$  módulo o subgrupo  $\mathbb{Z}^n$ , munidas da adição de conjuntos: a fórmula

$$(x + \mathbb{Z}^n) + (y + \mathbb{Z}^n) = (x + y) + \mathbb{Z}^n$$

é bem definida. Deste ponto de vista, identificamos

$$x + \mathbb{Z}^n \leftrightarrow f(x).$$

**Teorema G.0.22** (Lema de Kronecker). *Seja  $x \in \mathbb{R}^n$  um vetor tal que*

$$x_1, x_2, \dots, x_n, 1$$

*são racionalmente independentes. Então o subgrupo gerado pela imagem de  $x$  sob o homomorfismo (G.1) é denso no toro  $\mathbb{T}^n$ .*

*Demonstração.* Denotemos  $G$  o subgrupo do toro gerado pelo elemento  $f(x)$ . A imagem inversa  $f^{-1}G$  é um subgrupo fechado de  $\mathbb{R}^n$  que contém  $x$  e  $\mathbb{Z}^n$ . Agora apliquemos o lema G.0.19, junto com o fato que  $f[f^{-1}(G)] = G$  pois  $f$  é surjetor.  $\square$

A prova neste apêndice é baseada sobre a de Bourbaki [Bourbaki 1974], Chap. VII, §1. Quero agradecer Vladimir V. Uspenskij por ter trazido a prova de Bourbaki à minha atenção. Todos os erros que eu possivelmente tenho introduzidos tentando encurtar a prova ainda mais são meus próprios.

# H

## Integração e desintegração

---

### H.1 Integral de Lebesgue, espaço $L^1(\mu)$ , esperança

#### H.1.1 Integral de Lebesgue

Sejam  $\mu$  uma medida de probabilidade sobre um espaço boreliano padrão  $\Omega$ , e  $f : \Omega \rightarrow \mathbb{R}$  uma função boreliana e não negativa. A integral de  $f$  no sentido de Lebesgue é o valor

$$\int_{\Omega} f(x) d\mu(x) = \int_0^{+\infty} \mu\{x \in \Omega : f(x) \geq y\} dy, \quad (\text{H.1})$$

onde a integral à direita é a integral definida de uma função real (no sentido de Riemann). Isto corresponde ao dividir a área sob o gráfico de  $f$  em faixas horizontais, ao invés de verticais, como na definição da integral de Riemann.

*Observação H.1.1.* Uma função mensurável é dita *função*  $L^1(\mu)$  se a integral acima da função positiva  $|f|$  é finita.

**Exercício H.1.2.** Observe que a função

$$\mathbb{R} \ni y \mapsto \mu\{x \in \Omega : f(x) \geq y\} \in \mathbb{R}$$

é monótona, logo a integral no sentido de Riemann é bem-definida, com um valor em  $\mathbb{R}_+ \cup \{+\infty\}$ .

**Exercício H.1.3.** Deduza que o conjunto

$$S_f = \{(x, y) \in \Omega \times \mathbb{R} : f(x) \leq y\}$$

(a área sob o gráfico de  $f$ ) é boreliano, e verifique que

$$\int_{\Omega} f(x) d\mu(x) = (\mu \otimes \lambda)(S_f),$$

onde  $\lambda$  é a medida de Lebesgue unidimensional.

**Lema H.1.4.** *Seja  $(\Omega, \mu)$  um espaço probabilístico padrão, e seja  $f : \Omega \rightarrow \mathbb{R}$  uma função boreliana. Então a transformação*

$$\text{id}_{\Omega} \times T_f : \Omega \times \mathbb{R} \ni (x, y) \mapsto (x, y + f(x)) \in \Omega \times \mathbb{R}$$

é um automorfismo boreliano do produto  $\Omega \times \mathbb{R}$  que conserva a medida  $\mu \otimes \lambda$  (um “automorfismo vertical”).

*Demonstração.* É claro que a transformação acima é bijetora, com a inversa que corresponde à função  $-f$ . Portanto, para verificar a primeira afirmação, basta mostrar que a imagem de um subconjunto retangular aberto qualquer,  $U \times O$ , seja boreliano. Usemos o teorema de Luzin E.2.14 para escolher, para cada  $\varepsilon > 0$ , um compacto  $K_{\varepsilon} \subseteq \Omega$  tal que  $\mu(K_{\varepsilon}) > 1 - \varepsilon$  e  $f|_{K_{\varepsilon}}$  é contínua. Temos

$$(\text{id}_{\Omega} \times T_f)(U \times O) \cap (K_{\varepsilon} \times \mathbb{R}) = (\text{id}_{\Omega} \times T_{f|_{K_{\varepsilon}}})(U \cap K_{\varepsilon}) \times O,$$

um subconjunto aberto de  $K_{\varepsilon} \times \mathbb{R}$ , logo boreliano em  $\Omega \times \mathbb{R}$ , e quando  $\varepsilon_n \downarrow 0$ ,

$$(\text{id}_{\Omega} \times T_f)(U \times O) = \bigcup_{n=0}^{\infty} (\text{id}_{\Omega} \times T_f)(U \times O) \cap (K_{\varepsilon_n} \times \mathbb{R}),$$

de onde concluímos.

Para mostrar a segunda afirmação, notemos que o resultado para a parte atômica de  $\Omega$  é evidente, e suponhamos que  $\mu$  seja não atômica. Identifiquemos  $\Omega$  através de um isomorfismo de espaços probabilísticos com o intervalo  $[0, 1]$  (teorema E.2.7). Estendamos  $f|_{K_{\varepsilon}}$  até uma função contínua  $\tilde{f}$  sobre  $[0, 1]$  (veja o argumento na página 170). Agora é bastante simples fazer a conclusão desejada, aproximando a imagem de  $U \times O$  com uniões de subconjuntos retangulares cuja base converge para zero.  $\square$

**Exercício H.1.5.** Conclua que a função distância  $L^1(\mu)$ ,

$$d(f, g)_1 = \int_{\Omega} |f(x) - g(x)| d\mu(x),$$

é uma pseudométrica sobre o conjunto de todas as funções  $L^1(\mu)$  positivas.

[*Sugestão:* use um automorfismo vertical do lema H.1.4 para concluir que a distância entre duas funções,  $f$  e  $g$ , é igual ao valor da medida  $\mu \otimes \lambda$  da diferença simétrica  $S_f \Delta S_g$ .]



**Exercício H.1.6.** Mostre que a integral de Lebesgue é aditivo para funções positivas:

$$\int_{\Omega} (f + g) d\mu = \int_{\Omega} f d\mu + \int_{\Omega} g d\mu.$$

[ *Sugestão:* mais uma vez, use um automorfismo vertical para mostrar que a área sob o gráfico de  $f + g$  é igual a soma das áreas sob os gráficos de  $f$  e de  $g$ . ]

Se agora a função mensurável  $f : \Omega \rightarrow \mathbb{R}$  é qualquer, representemos

$$f = f_+ - f_-,$$

onde

$$f_+ = \max\{f, 0\}, \quad f_- = \max\{-f, 0\}$$

são positivas, e escrevamos

$$\int_{\Omega} f(x) d\mu(x) = \int_{\Omega} f_+(x) d\mu(x) - \int_{\Omega} f_-(x) d\mu(x).$$

A função é  $L^1$  se e somente se ambas integrais são finitas. Neste caso, o valor da integral de  $f$  é bem definido e finito.

*Observação H.1.7.* As definições acima têm sentido para todas as funções  $\mu$ -mensuráveis. No entanto, como toda função  $\mu$ -mensurável apenas difere de uma função boreliana  $f'$  sobre um conjunto negligenciável (exercício E.1.33), basta observar que

$$\int_{\Omega} f d\mu = \int_{\Omega} f' d\mu,$$

e sempre trabalhar só com as funções borelianas.

**Exercício H.1.8.** Estenda a afirmação do exercício H.1.5 para todas as funções  $L^1(\mu)$ .

## H.1.2 $L^1(\mu)$

**Exercício H.1.9.** Mostre que as funções  $L^1(\mu)$  formam um espaço linear (denotado  $L^1(\mu)$ ), e que a integral  $\int_{\Omega} d\mu$  é um funcional linear sobre o espaço  $L^1(\mu)$ .

**Exercício H.1.10.** Mostre que a função

$$\|f\|_1 = \int_{\Omega} |f(x)| d\mu(x)$$

é uma prenorma sobre o espaço  $L^1(\mu)$ , ou seja, satisfaz os axiomas 2 e 3 de uma norma (definição F.1.1).

**Exercício H.1.11.** Mostre que o núcleo da prenorma  $L^1(\mu)$ ,

$$N = \{x \in L^1(\mu) : \|x\|_1 = 0\},$$

é um sub-espaço linear, e que a fórmula

$$\|x + N\|_1 = \|x\|_1$$

defina uma norma sobre o espaço vetorial quociente  $L^1(\mu)/N$ .

Este espaço é também denotado pelo mesmo símbolo  $L^1(\mu)$ . Seus elementos são classes de equivalência de funções. Cada classe contém pelo menos um representante que é uma função boreliana.

**Exercício H.1.12.** Mostre que as condições seguintes são equivalentes.

1.  $f$  e  $g$  pertencem à mesma classe da equivalência modulo  $N$ .
2.  $f$  e  $g$  só diferem sobre um conjunto negligenciável.

**Exercício H.1.13.** Mostre que, se  $\mu$  não é puramente atômica, o núcleo  $N$  é não trivial.

**Exercício H.1.14.** Sejam  $f$  e  $g$  duas funções mensuráveis sobre um espaço probabilístico padrão  $\Omega$ . Suponha que  $\|f - g\|_1 < \varepsilon$ . Observe que o conjunto de pontos  $x$  onde  $|f(x) - g(x)| \geq \varepsilon$  tem medida  $\leq \varepsilon$ . Agora escolha sobre  $\Omega$  uma métrica completa e separável gerando a estrutura boreliana, e deduza a seguinte: se  $(f_n)$  é uma sequência de Cauchy no espaço  $L^1(\mu)$ , então para cada  $\varepsilon > 0$  existe um aberto  $U \subseteq \Omega$  com  $\varepsilon(U) < \varepsilon$  e uma subsequência  $(f_{n_i})$  que é Cauchy em relação à métrica uniforme sobre  $\Omega \setminus U$ . Conclua que o espaço normado  $L^1(\mu)$  é um espaço de Banach.

[ *Sugestão:* a escolha de  $U$  e de uma subsequência são recursivas, usando uma sequência somável dos reais positivos  $(\varepsilon_n)$  e a definição equivalente de uma sequência de Cauchy do lema C.3.4. ]

### H.1.3 Esperança

Agora, dada uma variável aleatória real  $X$ , tomando valores positivos, podemos definir a esperança de  $X$  no mesmo espírito que a integral na eq. (H.1):

$$\mathbb{E}X = \int_0^\infty (1 - \Phi_X(t)) dt,$$

onde

$$\Phi(t) = P[X < t]$$

é a função de distribuição de  $X$ . A definição se estende sobre v.a. reais quaisquer pela fórmula:

$$\mathbb{E}X = \mathbb{E}X_+ - \mathbb{E}X_-,$$

onde a notação é clara. Na prática, a caracterização seguinte será mais útil.

**Exercício H.1.15.** Seja  $X$  uma variável aleatória real qualquer. Mostre que, qualquer que seja uma realização  $f: (\mathfrak{X}, \nu) \rightarrow \mathbb{R}$  de  $X$ , temos

$$\mathbb{E}X = \int_{\mathfrak{X}} f(x) d\nu(x).$$

*Observação H.1.16.* Em particular,

$$\mathbb{E}X = \int_{\mathbb{R}} x d\mu(x),$$

onde  $\mu$  é a lei de  $X$ .

### H.1.4 Convergência dominada

**Teorema H.1.17** (Teorema de Lebesgue de convergência dominada). *Seja  $(f_n)$  uma sequência de funções mensuráveis sobre um espaço boreliano padrão  $\Omega$  munido de uma medida de probabilidade,  $\mu$ . Suponhamos que  $f_n$  convergem quase em toda parte para uma função  $f$ :*

$$\mu\{x \in \Omega: f_n(x) \rightarrow f(x)\} = 1,$$

e que existe uma função  $L^1(\mu)$ ,  $g$ ,

$$\int_{\Omega} |g| d\mu < +\infty,$$

que majoriza as funções da sequência:

$$\forall n, |f_n| \leq |g|.$$

Então  $f$  é mensurável, e

$$\int_{\Omega} |f_n - f| d\mu \rightarrow 0 \text{ quando } n \rightarrow \infty,$$

ou seja,  $f_n \rightarrow f$  na pseudométrica  $L^1(\mu)$ .

**Exercício H.1.18.** Seja  $(f_n)$  uma sequência de funções borelianas que converge simplesmente para uma função  $f$  sobre um domínio boreliano padrão:

$$\forall x \in \Omega, f_n(x) \rightarrow f(x) \text{ quando } n \rightarrow \infty.$$

Mostrar que  $f$  é boreliana.

*Observação H.1.19.* Todo subconjunto de um conjunto negligenciável é negligenciável, logo mensurável. Por conseguinte, se uma função  $f$  é boreliana sobre um subconjunto de um espaço probabilístico  $\Omega$  que tem medida um, segue-se que  $f$  é mensurável sobre  $\Omega$ .

*Prova do teorema H.1.17.* Denotemos  $Y$  um conjunto mensurável da medida  $\mu$  sobre qual  $f_n \rightarrow f$  simplesmente. Graças ao exercício E.1.33, podemos supor sem perda de generalidade que as funções  $f_n|_Y$  são borelianas sobre  $Y$ . (O conjunto  $Y$  tem uma estrutura boreliana — não necessariamente padrão — induzida de  $\Omega$ ). Segundo o exercício H.1.18, a função limite  $f$  é boreliana sobre  $Y$ , logo mensurável sobre  $\Omega$  (observação H.1.19). Seja  $\varepsilon > 0$  qualquer fixo. Para cada  $n$ , o conjunto

$$B_n = \{x \in Y : \forall n' \geq n, |f_{n'}(x) - f(x)| < \varepsilon\}$$

é boreliano (exercício),  $B_n \subseteq B_{n+1}$ , e  $\cup_n B_n$  tem medida 1. Segue-se que, quando  $n \rightarrow \infty$ ,

$$\mu(B_n) \rightarrow 1.$$

Temos

$$\begin{aligned} \int_{\Omega} |f_n - f| d\mu &= \int_{B_n} |f_n - f| d\mu + \int_{\Omega \setminus B_n} |f_n - f| d\mu \\ &< \varepsilon + \int_{\Omega \setminus B_n} 2|g| d\mu \\ &\rightarrow \varepsilon \text{ quando } n \rightarrow \infty, \end{aligned}$$

pois  $\mu(\Omega \setminus B_n) \rightarrow 0$  quando  $n \rightarrow \infty$ , e  $g$  é integrável.  $\square$

## H.1.5 Função caraterística de uma medida de probabilidade

A *função caraterística*,  $\phi_\mu$ , de uma medida de probabilidade,  $\mu$ , sobre  $\mathbb{R}^d$  é uma função de  $\mathbb{R}^d$  para  $\mathbb{C}$ , dada por

$$\begin{aligned} \mathbb{R}^d \ni t \mapsto \phi_\mu(t) &= \mathbb{E}_\mu(\exp i \langle t, X \rangle) \\ &= \int_{\mathbb{R}^d} \exp i \langle t, x \rangle d\mu(x) \in \mathbb{C}, \end{aligned}$$

onde  $X \in \mathbb{R}^d$  segue a lei  $\mu$ . É claro que  $\phi_\mu$  é sempre bem definida.

**Exercício H.1.20.** Mostrar as propriedades seguintes da função caraterística  $\phi_\mu$ .

1.  $\phi_\mu$  é uniformemente contínua.
2.  $\phi_\mu(0) = 1$  and  $|\phi_\mu| \leq 1$ .

A função caraterística permite de reconstruir a medida  $\mu$  unicamente.

**Exercício H.1.21.** Sejam  $\mu_1, \mu_2$  duas medidas de probabilidade sobre  $\mathbb{R}^d$ . Mostrar que existe uma função contínua  $f: \mathbb{R}^d \rightarrow \mathbb{R}$ , que se anula fora de um compacto, e tal que  $\int f d\mu_1 \neq \int f d\mu_2$ . (As funções de suporte compacto separam as medidas).

[*Sugestão:* existe um compacto  $K \subseteq \mathbb{R}^d$  tal que  $\mu_1(K) \neq \mu_2(K)$ . Agora pode-se escolher um  $\varepsilon > 0$  tal que  $\mu_1(K_\varepsilon) \neq \mu_2(K_\varepsilon)$ , onde  $K_\varepsilon$  denota a  $\varepsilon$ -vizinhança de  $K$ ....etc.] Compare o exercício H.2.3.

**Teorema H.1.22.** *Sejam  $\mu_1$  e  $\mu_2$  duas medidas de probabilidade borelianas distintas sobre  $\mathbb{R}^d$ . Então,  $\phi_{\mu_1} \neq \phi_{\mu_2}$ .*

Suponha que  $\phi_{\mu_1} = \phi_{\mu_2}$ . Segundo exercício H.1.21, basta mostrar que para todas funções  $f: \mathbb{R}^d \rightarrow \mathbb{R}$  de suporte compacto temos  $\int f d\mu_1 = \int f d\mu_2$ . Fixemos uma tal função  $f$  e um  $\varepsilon > 0$  qualquer. Existe um real  $L > 0$  tão grande que  $\text{supp } f \subseteq [-L/2, L/2]^d$  e  $\mu_i[-L/2, L/2]^d > 1 - \varepsilon, i = 1, 2$ . Formemos o toro (exemplo G.0.21)

$$\mathbb{T}^d = \mathbb{R}^d / L\mathbb{Z}^d$$

e definamos a função  $\tilde{f}: T \rightarrow \mathbb{R}$  por

$$\tilde{f}(x + LZ^d) = f(x),$$

para todos  $x \in [-L/2, L/2]^d$ . É claro que  $\tilde{f}$  é bem definida e contínua (exercício).

Para cada  $m \in \mathbb{Z}^d$ , defina

$$g_m: \mathbb{R}^d \rightarrow \mathbb{C}, \\ x \mapsto \exp(i \langle \pi m / L, x \rangle)$$

Seja  $\mathcal{F}$  o espaço linear gerado pelas funções  $g_m, m \in \mathbb{Z}^d$ . Este espaço é fechado pela multiplicação (exercício), logo, forma uma álgebra. Tudo como as funções geradoras,  $g_m$ , todos os elementos  $g \in \mathcal{F}$  são periódicos:

$$g(x + 2Ln) = g(x), \quad n \in \mathbb{Z}^d, \quad x \in \mathbb{R}^d.$$

Por isso, a função

$$\tilde{g}: \mathbb{T}^d \rightarrow \mathbb{C}, \\ \tilde{g}(x + 2LZ^d) = g(x)$$

é bem-definida, contínua, e limitada.

**Exercício H.1.23.** Verificar que o conjunto de funções com valores complexos

$$\tilde{\mathcal{F}} = \{\tilde{g}: g \in \mathcal{F}\}$$

forma uma álgebra, fechada pelas conjugações.

Como o toro  $\mathbb{T}^d$  é compacto, o teorema de Stone–Weierstrass F.3.1 implica que  $\tilde{\mathcal{F}}$  é densa em álgebra  $C(\mathbb{T}^d)$ . Em particular, existe  $\tilde{g} \in \tilde{\mathcal{F}}$  tal que  $\|\tilde{g} - \tilde{f}\|_\infty < \varepsilon$  (a norma uniforme). Isso implica, segundo a definição das duas funções,

$$\|(f - g)\chi_{[-L, L]^d}\|_\infty < \varepsilon,$$

assim como

$$\begin{aligned} \|(f - g)\chi_{\mathbb{R}^d \setminus [-L, L]^d}\|_\infty &\leq \|g\|_\infty \\ &= \|\tilde{g}\|_\infty \\ &\leq \|\tilde{f}\|_\infty + \varepsilon \\ &= \|f\|_\infty + \varepsilon. \end{aligned}$$

Para todo  $m \in \mathbb{Z}^d$ ,

$$\begin{aligned} \int g_m d\mu_1 &= \phi_{\mu_1}(\pi m/L) \\ &= \phi_{\mu_2}(\pi m/L) \\ &= \int g_m d\mu_2, \end{aligned}$$

logo, para cada  $g \in \mathcal{F}$ ,

$$\int g d\mu_1 = \int g d\mu_2.$$

Usando a última igualdade, concluímos:

$$\begin{aligned} \left| \int f d\mu_1 - \int f d\mu_2 \right| &= \left| \int (f - g) d\mu_1 - \int (f - g) d\mu_2 \right| \\ &\leq \left| \int |f - g| d\mu_1 + \int |f - g| d\mu_2 \right| \\ &\leq \varepsilon \left( 2\|f\|_\infty + 2\varepsilon + \mu_1(\mathbb{R}^d) + \mu_2(\mathbb{R}^d) \right). \end{aligned}$$

Como  $\varepsilon > 0$  foi qualquer, isto termina a demonstração do teorema [H.1.22](#). (A demonstração foi emprestada do livro [\[Klenke 2014\]](#), teorema 15.8).

## H.2 Teoremas de Riesz e de Banach–Alaoglu

### H.2.1 Teorema de representação de Riesz

Relembramos que, para um espaço compacto  $X$ , o espaço de Banach  $C(X)$  consiste de todas as funções contínuas sobre  $X$ , munidas da norma uniforme. Um funcional linear  $\phi$  sobre um espaço linear que consiste de funções reais é dito *positivo* se  $\phi(f) \geq 0$  cada vez que  $f \geq 0$ . É claro que, dada uma medida boreliana de probabilidade,  $\mu$ , sobre um espaço compacto métrico  $X$ , o funcional

$$C(X) \ni f \mapsto \int_X f(x) d\mu(x) \in \mathbb{R}$$

é linear, positivo, e envia a função 1 para 1. Verifica-se que cada funcional linear sobre  $C(X)$  com estas propriedades é desta forma.

**Teorema H.2.1** (Teorema de Representação de Riesz). *Seja  $X$  um espaço métrico compacto. Então a fórmula*

$$\mu \mapsto [C(X) \ni f \mapsto \int_X f(x) d\mu(x) \in \mathbb{R}]$$

*estabelece uma correspondência bijetora entre as medidas de probabilidade borelianas sobre  $X$  e os funcionais lineares positivos sobre o espaço de Banach  $C(X)$  enviando 1 para 1.*

**Exercício H.2.2.** Mostre que cada funcional linear e positivo  $\phi: C(X) \rightarrow \mathbb{R}$  enviando 1 para 1 é limitado, de norma 1.

[Sugestão: dado uma  $f \in C(X)$  com  $\|f\|_\infty \leq 1$ , estudar as imagens por  $\phi$  das funções  $f_+$ ,  $1 - f_+$ , etc.]

**Exercício H.2.3.** Seja  $X$  um espaço compacto, e  $F \subseteq K$  um subconjunto fechado. Mostre que para cada  $\varepsilon > 0$ , existe uma função contínua  $f_\varepsilon: X \rightarrow [0, 1]$  tal que  $f_\varepsilon|_F \equiv 1$  e  $f_\varepsilon$  se anula fora da  $\varepsilon$ -vizinhança de  $F$ . Conclua que

$$\int_X f_\varepsilon(x) d\mu(x) \rightarrow \mu(F) \text{ quando } \varepsilon \rightarrow 0.$$

**Exercício H.2.4.** Deduza que se  $\mu_1 \neq \mu_2$ , então existe uma função contínua  $f \in C(X)$  tal que

$$\int_X f(x) d\mu_1(x) \neq \int_X f(x) d\mu_2(x).$$

Deste modo, apenas resta a mostrar que cada funcional linear positivo  $\phi$ , com  $\phi(1) = 1$ , seja da forma

$$\phi(f) = \int_X f(x) d\mu(x)$$

para uma medida de probabilidade apropriada sobre  $X$ . Com esta finalidade, precisamos mais dois resultados (teoremas H.2.10 e H.2.13) que são importantes em si mesmos.

**Definição H.2.5.** Seja  $V$  um espaço linear real. Um *cone* (ou: *cone positivo*) em  $V$  é um subconjunto  $P$  tendo as propriedades seguintes:

- Se  $x, y \in P$ , então  $x + y \in P$ .
- Se  $x \in P$  e  $\lambda \geq \mathbb{R}$ , então  $\lambda x \in P$ .
- Se  $x \in P$  e  $-x \in P$ , então  $x = 0$ .

**Exemplo H.2.6.** O nosso exemplo motivador é o espaço  $V = C(X)$  de funções contínuas reais sobre um espaço compacto  $X$ , munido do cone  $P = \{f : f \geq 0\}$ .

**Exercício H.2.7.** Dado um cone  $P \subseteq V$ , verifique que a relação

$$x \leq y \iff y - x \in P$$

é uma ordem parcial sobre  $V$ . (Portanto, o par  $(V, P)$  se chama um *espaço linear parcialmente ordenado*). Deste modo, o cone  $P$  consiste exatamente de todos os elementos (não estritamente) positivos:

$$P = \{x \in V : x \geq 0\}.$$

**Definição H.2.8.** Um funcional linear  $\phi : V \rightarrow \mathbb{R}$  sobre um espaço linear parcialmente ordenado  $(V, P)$  é *positivo* se  $\phi(x) \geq 0$  quando  $x \in P$  (ou seja,  $x \geq 0$ ).

*Observação H.2.9.* Se  $X$  é um espaço linear parcialmente ordenado tendo o cone  $P$ , e  $Y$  é um subespaço linear de  $X$ , então  $Y$  é parcialmente ordenado também, com o cone  $P \cap Y$ .

**Teorema H.2.10** (Teorema de Hahn–Banach para funcionais positivos). *Seja  $V$  um espaço linear parcialmente ordenado, e seja  $E$  um subespaço linear de  $V$ . Então cada funcional linear positivo  $\phi$  sobre  $E$  se estende até um funcional linear positivo sobre  $V$ .*

A prova segue as mesmas linhas que a prova do teorema de Hahn–Banach para funcionais limitados (F.2.1). Sentimos que não há alguma necessidade de replicar o argumento completo. Apenas um análogo positivo do lema F.2.3 pode colocar ligeiras dificuldades, e por esta razão, discutamos a prova aqui.

**Exercício H.2.11.** Mostrar que  $\sup \emptyset = -\infty$  e  $\inf \emptyset = +\infty$ .

**Lema H.2.12.** *Sejam  $G$  um sub-espaço vetorial de um espaço parcialmente ordenado  $E = (E, P)$ ,  $g$  um funcional linear positivo sobre  $F$ , e  $x \in E$ . Então existe um funcional linear positivo  $g_1$  sobre o espaço vetorial*

$$G + \mathbb{R}x = \{y + tx : y \in G, t \in \mathbb{R}\},$$

*gerado pela união  $G \cup \{x\}$ , cuja restrição sobre  $G$  é igual a  $g$ .*

*Demonstração.* A ideia da escolha é também parecida à no lema F.2.3, só que ao invés da norma temos que usar a positividade para escolhermos corretamente a imagem,  $a \in \mathbb{R}$ , de  $x$  por  $g_1$ . Seja  $t \geq 0$  qualquer,  $y \in G$ . A condição

$$y + tx \geq 0$$

é equivalente a  $x \geq t^{-1}y$ , e deve implicar

$$g_1(y + tx) = g(y) + ta \geq 0,$$



ou seja  $a \geq g(t^{-1}y)$ . Da mesma maneira, a condição  $y - tx \geq 0$  é equivalente a  $x \leq t^{-1}y$ , e deve implicar  $a \leq g(t^{-1}y)$ . Concluímos: a extensão desejada existe se e somente se existe  $a \in \mathbb{R}$  tal que, quaisquer que sejam  $y', y'' \in G$  tais que  $y' \leq x \leq y''$ , temos

$$g(y') \leq a \leq g(y'').$$

Como  $y' \leq y''$ , temos que

$$g(y') \leq g(y'').$$

a por conseguinte,

$$\sup_{y' \leq x} g(y') \leq \inf_{y'' \geq x} g(y''),$$

se permitirmos que o supremo e o ínfimo assumam seus valores na reta estendida  $\mathbb{R} \cup \{\pm\infty\}$ , como no exercício H.2.11. Basta escolher  $a$  de modo que

$$\sup_{y' \leq x} g(y') \leq a \leq \inf_{y'' \geq x} g(y'').$$

□

Agora, um resultado bastante importante da topologia geral.

**Teorema H.2.13.** *Seja  $X$  um espaço métrico compacto. Existe uma aplicação contínua e sobrejetora  $g: \{0, 1\}^{\mathbb{N}} \rightarrow X$  do espaço de Cantor sobre  $X$ .*

*Demonstração.* Usando a precompactidade de  $X$ , para cada  $n$  construímos uma  $2^{-n}$ -rede finita  $F_n$  para  $X$ . Escolhamos uma sequência  $d_n \geq 1$  tendo a propriedade  $2^{d_n} \geq \#F_n$ . Agora construímos recursivamente uma sequência de aplicações sobrejetoras

$$g_n: \{0, 1\}^{\sum_{i \leq n} d_i} \rightarrow F_n,$$

$n \geq 1$ , satisfazendo a propriedade: se  $\sigma \in \{0, 1\}^{\sum_{i \leq n} d_i}$ , onde  $n \geq 2$ , então

$$d_X(g_n(\sigma), g_{n-1}(\sigma \upharpoonright [\sum_{i \leq n-1} d_i])) < 2^{-n+1}.$$

Dado um  $\sigma \in \{0, 1\}^{\mathbb{N}}$ , a sequência de pontos

$$g_n(\sigma \upharpoonright [\sum_{i \leq n} d_i]) \in X$$

é Cauchy, e portanto possui um e apenas um limite em  $X$ , que denotemos por  $g(\sigma)$ . Verifica-se facilmente que a aplicação  $g: \{0, 1\}^{\mathbb{N}} \rightarrow X$  é sobrejetora, usando o fato que cada ponto  $x \in X$  é o limite de uma sequência da forma  $(x_n)$ , onde  $x_n \in F_n$  e  $d(x, x_n) < 2^{-n}$ . A imagem por  $g$  de um conjunto aberto cilíndrico da forma

$$\pi_{[\sum_{i \leq n} d_i]}^{-1}(\tau)$$

tem diâmetro  $\leq \sum_{i=n-1}^{\infty} 2^{-i} = 2^{-n+2}$ , o que estabelece a continuidade de  $g$ . □

**Exercício H.2.14.** Seja  $g: X \rightarrow Y$  uma aplicação contínua entre dois espaços compactos. Então, a fórmula

$$g^*(f)(x) = f(g(x))$$

estabelece um operador linear limitado e positivo  $g^*: C(Y) \rightarrow C(X)$ , enviando 1 para 1. É o *operador dual* a  $g$ .

Agora seja  $\phi$  um funcional linear positivo qualquer sobre  $C(X)$ , enviando 1 para 1. Escolhemos uma aplicação sobrejetora  $g: \{0, 1\}^{\mathbb{N}} \rightarrow X$ . Formemos o operador dual  $g^*: C(X) \rightarrow C(\{0, 1\}^{\mathbb{N}})$ . Como  $g$  é sobrejetora, o operador  $g^*$  é uma imersão isométrica (exercício). O funcional  $\phi$ , definido sobre um sub-espaço fechado do espaço de Banach  $C(\{0, 1\}^{\mathbb{N}})$ , se estende até um funcional linear positivo  $\tilde{\phi}$  sobre  $C(\{0, 1\}^{\mathbb{N}})$ , graças ao teorema de Hahn–Banach na versão parcialmente ordenada [H.2.10](#). É claro que  $\tilde{\phi}(1) = \phi(1) = 1$ , logo  $\tilde{\phi}$  é limitado, da norma 1 (exercício [H.2.2](#)).

Os conjuntos cilíndricos de  $\{0, 1\}^{\mathbb{N}}$  são exatamente os conjuntos abertos e fechados (exercício). Para cada aberto e fechado,  $V$ , a função  $\chi_V$  é contínua. Definemos

$$\nu(V) = \tilde{\phi}(\chi_V).$$

**Exercício H.2.15.** Verifique que a medida  $\nu$  sobre o campo de abertos e fechados do espaço  $\{0, 1\}^{\mathbb{N}}$  é finitamente aditiva, logo sigma-aditiva pelo mesmo argumento que no exemplo [E.1.11](#).

Agora  $\nu$  estende-se até uma medida de probabilidade boreliana sobre  $\{0, 1\}^{\mathbb{N}}$  (teorema de Carathéodory [E.1.15](#)). As combinações lineares finitas de funções indicadoras de conjuntos abertos e fechados satisfazem as hipóteses do teorema de Stone–Weierstrass [F.3.1](#) (exercício), logo são densas em  $C(\{0, 1\}^{\mathbb{N}})$ .

**Exercício H.2.16.** Mostrar este fato diretamente, sem usar o teorema de Stone–Weierstrass.

Segue-se que para cada  $f \in C(\{0, 1\}^{\mathbb{N}})$ ,

$$\tilde{\phi}(f) = \int_{\{0, 1\}^{\mathbb{N}}} f(x) d\nu(x).$$

Denotemos

$$\mu = g_*(\nu)$$

a imagem direta da medida  $\nu$  pela aplicação contínua  $g: \{0, 1\}^{\mathbb{N}} \rightarrow X$ . Qualquer que seja  $f \in C(X)$ , temos

$$\begin{aligned} \phi(f) &= \tilde{\phi}(g^*(f)) \\ &= \int_{\{0, 1\}^{\mathbb{N}}} f(g(x)) d\nu(x) \\ &= \int_X f(x) d\mu, \end{aligned}$$

estabelecendo o teorema de Riesz [H.2.1](#).

## H.2.2 Teorema de Banach–Alaoglu

**Definição H.2.17.** Seja  $E$  um espaço normado qualquer. O espaço dual  $E^*$  consiste de todos os funcionais lineares contínuos sobre  $E$ , munido das operações naturais da adição e da multiplicação escalar, assim que da norma operadora (definição F.1.19).

**Exercício H.2.18.** Mostrar que  $E^*$  é um espaço de Banach (ou mostre o exercício F.1.20, mais geral).

Graças ao teorema de Hahn–Banach, o espaço dual não é trivial. Suas elementos *separam pontos* de  $E$ : se  $x, y \in E$ ,  $x \neq y$ , então existe  $\phi \in E^*$  tal que  $\phi(x) \neq \phi(y)$  (corolário F.2.2).

Denotemos por  $B_{E^*} = \{\phi \in E^* : \|\phi\| \leq 1\}$  a bola unitária *fechada* do espaço dual de  $E$ .

**Teorema H.2.19** (Teorema de Banach–Alaoglu, caso separável). *Seja  $E$  um espaço normado separável. Existe uma métrica sobre a bola unitária  $B_{E^*}$  do espaço dual  $E^*$  tal que a bola é compacta, e a restrição de cada funcional  $\phi \in E^*$  sobre  $B_{E^*}$  é contínua.*

Esta topologia se chama a *topologia fraca\**.

*Observação H.2.20.* A topologia fraca\* é bem definida e o teorema de Banach–Alaoglu vale para um espaço normado qualquer, só que para espaços não separáveis a prova já exige o Axioma de Escolha (o teorema de Tychonoff sobre a compacidade do produto de uma família qualquer dos espaços topológicos compactos). Como nós apenas precisamos uma versão separável, dêmos uma versão restrita do resultado.

Transformamos  $[0, 1]^{\mathbb{N}}$  num espaço métrico como segue:

$$d(x, y) = \sum_{k \in \mathbb{N}_+} 2^{-k} |x_k - y_k|. \quad (\text{H.2})$$

**Exercício H.2.21.** Mostrar que  $[-1, 1]^{\mathbb{N}}$ , munido da métrica acima, é um espaço compacto.

[*Sugestão:* mostre que a métrica acima gera a topologia produto no sentido da definição C.2.93, e use o exercício C.3.29.]

Seja  $\bar{x} = (x_k)$  uma seqüência de elementos da bola unitária  $B$  de  $E$  cujos elementos são densos na bola. Definamos uma aplicação  $i_{\bar{x}}$  da bola  $B_{E^*}$  para o cubo  $[-1, 1]^{\mathbb{N}}$  como segue:

$$B_{E^*} \ni \phi \mapsto i_{\bar{x}}(\phi), \text{ onde } \forall k, i(\phi)_k = \phi(x_k) \in [-1, 1].$$

**Exercício H.2.22.** Mostre que a aplicação  $i_{\bar{x}}$  é injetora e contínua.

**Lema H.2.23.** *A imagem da bola  $B_{E^*}$  por  $i_{\bar{x}}$  é fechada no cubo  $[-1, 1]^{\mathbb{N}}$ , logo compacta.*

Seja  $(\phi_n)$  uma sequência de elementos da bola cujas imagens  $i_{\bar{x}}(\phi_n)$  formam uma sequência de Cauchy em relação à métrica (H.2). A propriedade de Cauchy é equivalente à condição seguinte: para cada  $\varepsilon > 0$  e  $M$ , existe  $N$  e  $\delta > 0$  tais que, se  $n \geq N$ , então

$$|\phi_n(x_k) - \phi_N(x_k)| < \varepsilon \text{ quando } k = 1, 2, \dots, M.$$

Em particular, para cada  $k \in \mathbb{N}$ , a sequência  $(\phi_n(x_k))$  é Cauchy em  $\mathbb{R}$ , logo possui um limite, que denotemos por  $\phi(x_k)$ .

**Exercício H.2.24.** Verifique que a aplicação com o domínio  $\{x_k\}_{k \in \mathbb{N}}$

$$x_k \mapsto \phi(x_k) \in \mathbb{R}$$

é Lipschitz contínua de constante 1.

**Exercício H.2.25.** Seja  $f: X \rightarrow Y$  uma aplicação uniformemente contínua entre dois espaços métricos. Mostre que  $f$  admite uma e uma só prorrogação uniformemente contínua sobre os completamentos:  $\hat{f}: \hat{X} \rightarrow \hat{Y}$ . Se  $f$  for Lipschitz contínua, então  $\hat{f}$  é Lipschitz contínua, com a mesma constante.

Estendamos  $\phi$  até uma função (que denotemos pela mesma letra) de  $B_{E^*}$  para  $\mathbb{R}$ .

**Exercício H.2.26.** Sejam  $x, y \in B_{E^*}$  and  $\lambda \in \mathbb{R}$  tais que  $x + y \in B_{E^*}$  e  $\lambda x \in B_{E^*}$ . Mostre que  $\phi(x + y) = \phi(x) + \phi(y)$  e  $\phi(\lambda x) = \lambda \phi(x)$ .

**Exercício H.2.27.** Mostre que  $\phi$  admite uma extensão única até um funcional linear da norma  $\leq 1$ , definido sobre  $E$ .

Isto conclui a prova do lema H.2.23.

Agora coloquemos sobre  $B_{E^*}$  a topologia induzida do cubo  $[-1, 1]^{\mathbb{N}}$  pela imersão da bola como um sub-espaço compacto com ajuda da aplicação  $i_{\bar{x}}$ . Em outras palavras,  $B_{E^*}$  é munido da métrica

$$d_{\bar{x}}(\phi, \psi) = d(i_{\bar{x}}(\phi), i_{\bar{x}}(\psi)),$$

onde  $d$  é como na eq. (H.2).

**Exercício H.2.28.** Deduza dos exercícios C.3.29 e C.2.94 que a topologia induzida pela métrica  $d_{\bar{x}}$  sobre a bola  $B_{E^*}$  (através da imersão  $i_{\bar{x}}$ ) é a menor topologia tal que todas as aplicações  $\phi(x_n) = \pi_n(i_{\bar{x}}(\phi))$ ,  $n \in \mathbb{N}$  são contínuas.

**Lema H.2.29.** Em relação à métrica  $d_{\bar{x}}$ , para cada  $x \in B_E$ , a aplicação

$$B_{E^*} \ni \phi \mapsto \phi(x) \in \mathbb{R} \tag{H.3}$$

é contínua.

*Demonstração.* Seja  $x \in B_E$  qualquer. Formemos uma nova sequência, incluindo  $x$  como o primeiro elemento:  $\tilde{x} = (x, x_1, x_2, \dots)$ . A topologia induzida sobre a bola pela métrica  $d_{\tilde{x}}$  é também compacta, e mais fina do que a topologia induzida pela métrica  $d_{\tilde{x}}$  (exercício H.2.28). Corolário C.3.39 aplicada à aplicação identidade  $\text{id}_{B_{E^*}}$  implica que as duas topologias são iguais, logo a aplicação  $\phi \mapsto \phi(x)$  é contínua em relação às ambas.  $\square$

**Exercício H.2.30.** Conclua do exercício H.2.28 e do lema H.2.29, que, qualquer que seja sequência  $\bar{x}$  densa na bola  $B_E$ , a topologia gerada pela métrica  $d_{\bar{x}}$  sobre a bola dual  $B_{E^*}$  é a menor topologia tal que para cada  $x \in B$  a aplicação  $\phi \mapsto \phi(x)$  é contínua.

Segue-se que  $\bar{x}$  e  $\bar{y}$  são duas sequências densas na bola  $B_E$  quaisquer, então as métricas  $d_{\bar{x}}$  e  $d_{\bar{y}}$  são equivalentes sobre a bola  $B_{E^*}$ , o que conclue a prova do teorema H.2.19.

**Exercício H.2.31.** Mostrar que a topologia normada sobre  $B_{E^*}$  é mais forte do que a topologia fraca\*, e que as duas coincidem se e somente se  $\dim E < \infty$ .

## H.2.3 Topologia sobre o espaço de medidas de probabilidade

Denotemos  $P(X)$  o conjunto de todas as medidas de probabilidade sobre um espaço compacto  $X$ . Segundo o teorema de Riesz,  $P(X)$  pode se identificar com o conjunto de funcionais lineares e positivos sobre  $C(X)$ , enviando 1 para 1. Deste modo,  $P(X)$  é um subconjunto da bola dual  $B_{C(X)^*}$ .

**Proposição H.2.32.** *Seja  $X$  um espaço métrico compacto. Então o espaço de Banach  $C(X)$  é separável.*

Isso segue imediatamente da combinação de dois resultados estabelecidos na prova do teorema de Riesz: o espaço  $C(X)$  é um subespaço normado do espaço  $C(\{0, 1\}^{\mathbb{N}})$ , e o último espaço é separável. No mesmo tempo, o resultado é muito mais simples, e não exige algumas ferramentas avançadas. Eis uma prova direta deste fato, que vamos fazer só para  $X = [0, 1]$ .

**Exercício H.2.33.** Denotemos por  $A$  o subconjunto do espaço  $\ell^\infty[0, 1]$  que consiste de todas as funções  $f: [0, 1] \rightarrow \mathbb{Q}$  tais que existe  $n \in \mathbb{N}_+$  com a propriedade que  $f$  é constante sobre cada intervalo demi-aberto

$$\left[ \frac{i}{n}, \frac{i+1}{n} \right), \quad i = 0, 1, 2, \dots, n-1.$$

Mostrar que  $A$  é enumerável.

**Exercício H.2.34.** Sejam  $f \in C[0, 1]$  e  $\epsilon > 0$  quaisquer. Escolhamos  $\delta > 0$  tal que

$$\forall x, y \in [0, 1], \quad |x - y| < \delta \Rightarrow |f(x) - f(y)| < \epsilon.$$

Existe  $n$  tal que

$$\frac{1}{n} < \delta$$

(a propriedade de Arquimede). Definiremos a função  $g \in A$  pelos condições seguintes:  $g$  é constante sobre cada intervalo  $[i/n, (i+1)/n]$ ,  $i = 0, 1, \dots, n-1$ , e

$$\forall i = 1, 2, 3, \dots, n, \quad g\left(\frac{i}{n}\right) \in \mathbb{Q} \text{ e } \left|g\left(\frac{i}{n}\right) - f\left(\frac{i}{n}\right)\right| < \epsilon.$$

Mostrar que  $d_\infty(d, f) < 2\epsilon$ .

Segue-se que o subespaço  $\bar{A}$  (a aderência em  $\ell^\infty[0, 1]$ ) é separável e contém  $C[0, 1]$ , logo  $C[0, 1]$  é separável (teorema C.2.74).

**Exercício H.2.35.** Generalizar o argumento no caso do espaço métrico  $C(X)$ , onde  $X$  é um espaço métrico compacto qualquer.

**Lema H.2.36.** *O espaço  $P(X)$  é fechado na bola dual  $B_{C(X)^*}$  em relação à topologia fraca\*, logo compacto.*

*Demonstração.* Seja  $\phi \in B_{C(X)^*} \setminus P(X)$ . Indiquemos uma vizinhança  $V$  de  $\phi$  na topologia fraca\* disjunta de  $P(X)$ . Se  $\phi(1) = a \neq 1$ , então definemos  $\epsilon = |a - 1|$  e

$$V = \{\psi \in B_{C(X)^*} : \psi(1) \in (a - \epsilon, a + \epsilon)\}.$$

Se  $\phi$  não é positivo, existe  $f \in B_E$  tal que  $f \geq 0$  e  $\phi(f) = b < 0$ . Definemos

$$V = \{\psi \in B_{C(X)^*} : \psi(f) \in (2b, 0)\}.$$

□

Chegamos ao resultado seguinte.

**Teorema H.2.37.** *O espaço  $P(X)$  de medidas borelianas de probabilidade sobre um espaço compacto metrizável  $X$  é munido de uma topologia compacta metrizável, que é a menor topologia tal que todas as aplicações*

$$\mu \mapsto \int_X f(x) d\mu(x) \in \mathbb{R}$$

são contínuas, quando  $f \in C(X)$ .

Esta topologia tem o mesmo nome: topologia fraca\* sobre  $P(X)$ .

## H.3 Convergência de martingales e derivada de Radon–Nikodým

### H.3.1 Teorema de convergência de martingales

Nós já vimos martingales sobre espaços probabilísticos finitos na sub-seção 1.3.3. Agora consideremos martingales um pouco mais complicados: ainda definidas pelas partições finitas, embora formando uma sequência infinita, sobre um espaço probabilístico padrão.

**Definição H.3.1.** Seja  $(X, \mu)$  um espaço probabilístico padrão, e seja

$$\Omega_0 \succ \Omega_1 \succ \cdots \succ \Omega_n \succ \Omega_{n+1} \succ \cdots$$

uma sequência refinadora de partições finitas mensuráveis de  $\Omega$ , onde  $\Omega_0 = \{\Omega\}$  é uma partição trivial. Um martingale (formado em relação à sequência acima) é uma coleção de funções mensuráveis reais  $(f_0, f_1, \dots)$  sobre  $X$ , que pertencem a  $L^1(\mu)$  e satisfazem, para todo  $i = 1, 2, \dots$ ,

$$E_\mu(f_i \mid \Omega_{i-1}) = f_{i-1}.$$

A esperança condicional é entendida no sentido da definição 1.3.31.

**Definição H.3.2.** Digamos que uma função mensurável real  $f$  sobre um espaço probabilístico padrão  $(\Omega, \mu)$  é *essencialmente limitada* se existe uma função limitada,  $g$ , que difere de  $f$  sobre um conjunto negligenciável. O *supremo essencial* de  $f$  é o valor

$$\text{ess sup } f = \inf\{\sup f \mid A: \mu(A) = 1\}.$$

**Exercício H.3.3.** Verifique que as funções mensuráveis e essencialmente limitadas formam um sub-espaço linear de  $\mathbb{R}^\Omega$ , e a fórmula

$$\|f\|_\infty = \text{ess sup}|f|$$

defina uma pre-norma sobre este espaço.

O espaço acima é notado  $L^\infty(\Omega, \mu)$ , ou simplesmente  $L^\infty(\mu)$ . O espaço normado associado ao espaço acima é denotado pelo mesmo símbolo.

**Exercício H.3.4.** Mostre que o espaço normado  $L^\infty(\mu)$  é um espaço de Banach.

[ *Sugestão:* use o teorema C.3.23. ]

O resultado seguinte forma uma ferramenta técnica maior.

**Teorema H.3.5** (Primeiro teorema de Doob de convergência de martingale). *Seja  $(f_n)$  um martingale, tal que  $\|f_n\|_1 < \infty$  uniformemente em  $n$ . Então  $f_n$  converge em quase todo ponto para um limite que pertence a  $L^1(\mu)$ .*

Vamos “quase” mostrar o resultado, e a única coisa que nos faltará, será o lema de Fatou, que garante que o limite simples da sequência  $(f_n)$  pertença a  $L^1(\mu)$ . Como queremos evitar uma prova extra bastante técnica, formulemos uma versão do teorema de Doob mais fraca possível do que atende às nossas necessidades.

**Teorema H.3.6.** *Seja  $(f_n)$  um martingale, tal que  $\|f_n\|_\infty < \infty$  uniformemente em  $n$ . Então  $f_n$  converge em  $L^1(\mu)$  para um limite.*

**Exercício H.3.7.** Mostre que sem a hipótese sobre as normas  $L^\infty$  de  $f_n$ , a conclusão do teorema H.3.6 não é verdadeira.

**Exercício H.3.8.** Mostre que, se apenas exigirem que as normas  $L^1(\mu)$  de  $f_n$  sejam uniformemente limitadas, pode ocorrer que  $\mathbb{E}_\mu f_n = 1$  para todos  $n$ , portanto  $f_n \rightarrow 0$  q.c.

*Observação H.3.9.* O segundo teorema de Doob dá condições necessárias e suficientes para  $(f_n)$  convergirem em  $L^1(\mu)$ . No entanto, só vamos precisar do resultado mais fraco H.3.6.

**Definição H.3.10.** Sejam  $(x_n)$  uma sequência de reais, finita ou infinita, e  $a < b$ . Uma *travessia para cima* (*upcrossing*) do intervalo  $(a, b)$  pela sequência  $(x_n)$  é qualquer par de elementos  $x_m, x_n$ , onde  $m < n$ ,  $x_m \leq a$ ,  $x_n \geq b$ , e para qualquer  $k$  com  $m < k < n$ , temos  $x_k \in (a, b)$ .

**Definição H.3.11.** O número total de travessias para cima do intervalo  $(a, b)$  pela sequência  $(x_n)$  é denotado  $U[(x_n), (a, b)]$ .

De mesmo modo, as *travessias para baixo* (*downcrossings*) são definidas, e o seu número é denotado  $D[(x_n), (a, b)]$ . É claro que a diferença entre os números  $U[(x_n), (a, b)]$  e  $D[(x_n), (a, b)]$  pode ser  $\pm 1$  ao máximo.

**Exercício H.3.12.** Mostre que uma sequência limitada  $(x_n)$  de reais converge para um limite se e somente se, para todos  $a < b$  (equivalente: para todos  $a < b$  racionais), o número de travessias para cima do intervalo  $(a, b)$  pela sequência é finito.

Agora o teorema H.3.6 segue do resultado seguinte, aplicado ao conjunto de intervalos com pontos extremos racionais, e depois combinado com o teorema de convergência dominada H.1.17. Relembramos que  $f_-$  denota a parte negativa de uma função:

$$f_- = \max\{-f, 0\}.$$

**Lema H.3.13** (Lema de Doob de travessias para cima). *Suponha que  $L^1(f_n) < \infty$  uniformemente em  $n$ . Então, para todos  $a < b$  e  $N \in \mathbb{N}$ ,*

$$(b - a)\mathbb{E}_{x \sim \mu} U[(f_i(x))_{i=1}^N, (a, b)] \leq \mathbb{E}_\mu (f_N - a)_-.$$



Definamos recursivamente as funções  $t_k, k \in \mathbb{N}$ , e  $s_k, k \in \mathbb{N}_+$ , sobre  $X$  com valores em  $\mathbb{N}$  (ou: realizações de variáveis aleatórias) como segue:

$$\begin{aligned} t_0 &= 0, \\ s_k &= \min\{n > t_{k-1} : f_n \leq a\}, \\ t_k &= \min\{n > s_k : f_n \geq b\}. \end{aligned}$$

Deste modo,

$$0 = t_0 < s_1 < t_1 < s_2 < \dots$$

**Exercício H.3.14.** Verifique que

$$U[(f_i(x))_{i=1}^N, (a, b)] = \max\{k : t_k(x) \leq N\}.$$

**Definição H.3.15.** Uma função  $N : X \rightarrow \mathbb{N}$  é chamada *tempo de parada* se para todo  $n$ , o evento

$$\{x \in X : N(x) = n\}$$

pertence à álgebra de conjuntos gerada pela partição  $\Omega_n$ .

**Exercício H.3.16.** Mostre que  $t_k$  e  $s_k$  são tempos de parada.

Para dois funções  $f$  e  $g$ , usemos a notação

$$(f \wedge g)(x) = \min\{f(x), g(x)\}.$$

**Exercício H.3.17.** Mostre que, se  $(f_n)$  é um martingale e  $N$  é um tempo de parada, então a sequência  $(f_{n \wedge N})$  é um martingale. A função  $f_{n \wedge N}$  deve ser entendida como

$$f_{n \wedge N}(x) = f_{\min\{n, N(x)\}}.$$

[ *Sugestão:* para um elemento  $A \in \Omega_{n-1}$  e os elementos  $A_i \in \Omega_n, \cup A_i = A$ , considere várias possibilidades para o valor de  $n \wedge N$  sobre  $A$  e  $A_i$ . ]

**Teorema H.3.18.** *Seja  $(f_n)$  um martingale e  $N$  um tempo de parada. Então,*

$$\mathbb{E} f_{N \wedge n} = \mathbb{E} f_0.$$

Para mostrar o resultado, precisamos da noção seguinte.

**Definição H.3.19.** Uma sequência  $h = (h_n)$  de funções sobre  $X$  chama-se *previsível* se cada  $h_n$  é mensurável em relação à álgebra gerada por  $\Omega_{n-1}$ , ou seja, é constante sobre os elementos de  $\Omega_{n-1}$ .

Dado um martingale  $f = (f_n)$  e uma sequência previsível  $(h_n)$ , definamos a *transformação martingale*,

$$(h \cdot f)_n = f_0 + \sum_{i=1}^n h_i d_i,$$

onde  $d_j = f_j - f_{j-1}$  são diferenças de martingale (definição 1.3.44). Por exemplo, se  $h_n = 1$ , obtemos o martingale original.

**Exercício H.3.20.** Mostre que a transformação martingale  $((h \cdot f)_n)_{n=0}^\infty$  é um martingale. [Sugestão: use proposições 1.3.46 e 1.3.34.(2).]

**Exercício H.3.21.** Mostre que para cada  $n$ ,

$$\mathbb{E}(h \cdot f)_n = \mathbb{E}f_0.$$

Modulo o exercício H.3.21, a prova do teorema H.3.18 será terminada pela observação seguinte.

**Lema H.3.22.** *Seja  $(f_n)$  um martingale e  $N$  um tempo de parada. Então,*

$$(f_{n \wedge N}) = (z \cdot f)_n,$$

onde  $(z_n)$  é uma sequência previsível, dada por

$$z(x) = \begin{cases} 1, & \text{se } N \geq n, \\ 0, & \text{se } N < n \end{cases}$$

*Demonstração.* O evento  $z_n = 1$  é igual ao evento  $N \geq n$ , e ele é  $\Omega_{n-1}$ -mensurável porque o evento complementar  $N \leq n-1$  é (definição de tempo de parada). Logo,  $(z_n)$  é uma sequência previsível. Agora,

$$\begin{aligned} (z \cdot f)_n &= f_0 + \sum_{i=1}^n z_n (f_n - f_{n-1}) \\ &= f_0 + \sum_{i=1}^{n \wedge N} (f_n - f_{n-1}) \\ &= f_{n \wedge N}, \end{aligned}$$

pois a soma é telescópica. □

*Prova do lema H.3.13.* Denotemos  $K(x) = U[(f_i(x))_{i=1}^N, (a, b)]$ . Qualquer que seja  $n$ , temos:

$$\begin{aligned}
 0 &= \sum_{j=1}^{\infty} (\mathbb{E} f_0 - \mathbb{E} f_0) \\
 &= \mathbb{E} \sum_{j=1}^{\infty} (f_{t_j \wedge n} - f_{s_j \wedge n}) \\
 &= \mathbb{E} \sum_{j=1}^{K(x)} (f_{t_j} - f_{s_j}) + \mathbb{E} (f_n - f_{s_{K(x)}}) \\
 &\geq \mathbb{E} K(x)(b - a) - \mathbb{E} (f_n - a)_-,
 \end{aligned}$$

e o resultado segue. □

**Exercício H.3.23.** Deduza o teorema H.3.6 do lema H.3.13 e o exercício H.3.12.

### H.3.2 Derivada de Radon–Nikodým

**Definição H.3.24.** Sejam  $\mu$  e  $\nu$  duas medidas sobre um espaço boreliano padrão,  $\Omega$ . Diz-se que  $\mu$  é absolutamente contínua em relação a  $\nu$ , notação

$$\mu \ll \nu,$$

se cada conjunto  $\nu$ -negligenciável é  $\mu$ -negligenciável:

$$\forall B \in \mathcal{B}_\Omega, \nu(B) = 0 \Rightarrow \mu(B) = 0.$$

**Exercício H.3.25.** Sejam  $\mu$  uma medida finita boreliana sobre um espaço boreliano padrão,  $\Omega$ , e  $f \in L^1(\mu)$ . Mostre que a fórmula

$$(f\mu)(B) = \int_{\Omega} \chi_B d\mu$$

defina uma medida finita boreliana,  $f\mu$ , sobre  $\Omega$ .

**Exemplo H.3.26.**  $f\mu \ll \mu$ .

O teorema de Radon–Nikodým diz que isto é o único exemplo possível.

**Teorema H.3.27** (Teorema de Radon–Nikodým). *Sejam  $\mu$  e  $\nu$  duas medidas finitas sobre um espaço boreliano padrão,  $\Omega$ , tais que*

$$\mu \ll \nu.$$

*Então, existe uma função  $f \in L^1(\nu)$  tal que*

$$\mu = f\nu.$$

**Definição H.3.28.** A função  $f$  no teorema H.3.27 chama-se a *derivada de Radon–Nikodým*.  
Notação:

$$f = \frac{d\mu}{d\nu}.$$

**Exercício H.3.29.** Mostre o teorema de Radon–Nikodým no caso onde  $\nu$  é puramente atômica. Deduza que basta mostrar o teorema sob a hipótese que  $\nu$  seja uma medida não atômica.

Na parte principal, somente usamos o teorema de Radon–Nikodým para mostrar a existência da função de regressão (p. 161), e neste caso, a medida  $\mu$  satisfaz uma forte restrição adicional: para cada conjunto  $A$  mensurável,  $\mu(A) \leq \nu(A)$ . A prova torna se consideravelmente mais simples. Vamos apenas mostrar este resultado:

**Teorema H.3.30** (Teorema de Radon–Nikodým, caso especial). *Sejam  $\mu$  e  $\nu$  duas medidas finitas sobre um espaço boreliano padrão,  $\Omega$ , tais que para cada  $A \in \mathcal{B}_\Omega$ ,*

$$\mu(A) \leq \nu(A).$$

*Então, existe uma função boreliana  $f$  com valores em  $[0, 1]$  tal que*

$$\mu = f\nu.$$

Graças ao exercício H.3.29, podemos supor que  $\nu$  é uma medida não atômica. Aplicando o teorema E.2.7, suponhamos sem perda de generalidade que  $\Omega = \{0, 1\}^{\mathbb{N}}$  é o cubo de Cantor, e  $\nu$  é a medida de Haar.

Para cada  $n$ , seja  $\Omega_n$  a partição de  $\{0, 1\}^{\mathbb{N}}$  em  $2^n$  subconjuntos cilíndricos da forma  $\pi_n^{-1}(\sigma)$ ,  $\sigma \in \{0, 1\}^n$ . Definamos  $f_n: \{0, 1\}^{\mathbb{N}} \rightarrow \mathbb{R}$  por

$$f_n(x) = \frac{\mu(\pi_n^{-1}(\pi_n(x)))}{\nu(\pi_n^{-1}(\pi_n(x)))} = 2^n \mu(\pi_n^{-1}(\pi_n(x))).$$

**Exercício H.3.31.** Verifique que  $(f_n)$  é um martingale em relação à sequência de partições  $(\Omega_n)$ .

A hipótese adicional sobre  $\mu$  implica que  $\|f_n\|_\infty \leq 1$ , e segundo o teorema de convergência de martingale H.3.6,  $f_n \rightarrow f$  no espaço  $L^1(\mu)$ .

**Exercício H.3.32.** Mostre que para todo conjunto cilíndrico  $C = \pi_n^{-1}(\sigma)$  temos

$$f(C) = f_n(C) = 2^n \mu(\pi_n^{-1}(\pi_n(x))).$$

Com ajuda do teorema de extensão de medidas, deduza que

$$\mu = f\nu.$$

### H.3.3 Espaço dual de $L^1(\mu)$

Todo elemento  $f \in L^\infty(\mu)$  define um funcional linear sobre  $L^1(\mu)$ , como segue:

$$L^1(\mu) \ni g \mapsto \hat{f}(g) = \int_{\Omega} f(x)g(x) d\mu(x) \in \mathbb{R}.$$

**Exercício H.3.33.** Verifique que a funcional acima é limitado, e a sua norma satisfaz

$$\|\hat{f}\| = \|f\|_\infty.$$

Deste modo, a correspondência

$$L^\infty(\mu) \ni f \mapsto \hat{f} \in L^1(\mu)^* \tag{H.4}$$

é uma imersão isométrica linear.

De fato, verifica-se que todos os funcionais limitados sobre  $L^1(\mu)$  são daquela forma.

**Teorema H.3.34.** *O espaço de Banach  $L^1(\mu)^*$  dual ao espaço  $L^1(\mu)$  é isometricamente isomorfo ao espaço  $L^\infty(\mu)$ . O isomorfismo é estabelecido pela eq. (H.4).*

Apenas resta mostrar que para cada funcional linear limitado  $\phi: L^1(\mu) \rightarrow \mathbb{R}$  existe uma função  $f \in L^\infty(\mu)$  tal que  $\phi = \hat{f}$ . No caso de um espaço probabilístico finito, isso segue das considerações de dimensão.

**Exercício H.3.35.** Mostre o teorema H.3.34 no caso onde  $\Omega$  é finito.

A prova do caso geral é muito semelhante à prova do teorema H.3.30. Sem perda de generalidade, pode-se supor que  $\Omega$  é o cubo de Cantor,  $\{0, 1\}^{\mathbb{N}}$ , munido de uma medida de probabilidade,  $\mu$ . Seja  $\phi \in L^1(\mu)^*$ . Mais uma vez, denotemos por  $\Omega_n$  a partição de  $\{0, 1\}^{\mathbb{N}}$  em  $2^n$  subconjuntos cilíndricos  $\pi_n^{-1}(\sigma)$ ,  $\sigma \in \{0, 1\}^n$ . Para cada  $n$ , definamos  $f_n: \{0, 1\}^{\mathbb{N}} \rightarrow \mathbb{R}$  por

$$f_n(x) = \frac{\phi(\chi_{\pi_n^{-1}(\pi_n(x))})}{\mu(\pi_n^{-1}(\pi_n(x)))} = \phi \left( \frac{\chi_{\pi_n^{-1}(\pi_n(x))}}{\|\chi_{\pi_n^{-1}(\pi_n(x))}\|_1} \right).$$

**Exercício H.3.36.** Verifique que  $(f_n)$  é um martingale, e  $f_n$  são uniformemente limitados em  $L^\infty(\mu)$  por  $\|\phi\|$ .

O teorema de convergência de martingale H.3.6 garante que  $f_n \rightarrow f$  no espaço  $L^1(\mu)$ .

**Exercício H.3.37.** Verifique que para todo conjunto cilíndrico da forma  $C = \pi_n^{-1}(\sigma)$ ,

$$\int_C f(x) d\mu(x) = \phi(C).$$

Deduza que para toda combinação linear finita,

$$g = \sum_{i=1}^k \lambda_k \chi_{C_k}, \quad (\text{H.5})$$

onde  $C_k$  são conjuntos cilíndricos como acima, temos

$$\int_{\{0,1\}^{\mathbb{N}}} g(x) f(x) d\mu(x) = \phi(g).$$

**Exercício H.3.38.** Mostre que as funções como na eq. (H.5) (*funções simples*) são densas em  $L^1(\mu)$ .

[ *Sugestão:* use a regularidade de  $\mu$  para aproximar cada conjunto da forma  $\{x \in \Omega : t_i < f(x) < t_{i+1}\}$  com um conjunto aberto e fechado, e depois use o fato que abertos e fechados em  $\{0, 1\}^{\mathbb{N}}$  são exatamente conjuntos cilíndricos. ]

Em particular, o espaço  $L^1(\mu)$ , onde  $\mu$  é uma medida de probabilidade sobre um espaço boreliano padrão, é separável.

**Exercício H.3.39.** Complete a prova do teorema H.3.34.

## H.4 Teorema da desintegração de Rokhlin

### H.4.1

Nós precisamos a versão seguinte do teorema de Rokhlin.

**Teorema H.4.1** (Teorema da desintegração de Rokhlin). *Sejam  $f : \Omega \rightarrow \Upsilon$  uma função boreliana entre dois espaços borelianos padrão, e  $\mu$  uma medida de probabilidade boreliana sobre  $\Omega$ . Para quase todo  $x \in \Upsilon$ , existe uma medida de probabilidade  $\mu_x$  sobre a fibra  $f^{-1}(x) \subseteq \Omega$ , tal que, qualquer que seja função  $g \in L^1(\mu)$ ,*

$$\int_{\Omega} g(x) d\mu(x) = \int_{\Upsilon} df_*(\mu) \int_{f^{-1}(x)} g(y) d\mu_x(y). \quad (\text{H.6})$$

Em particular, para cada conjunto mensurável  $A \subseteq \Omega$ ,

$$\mu(A) = \int_{\Upsilon} \mu_x(A \cap f^{-1}(x)) df_*(\mu).$$

*Observação H.4.2.* Na fala probabilística, as medidas  $\mu_x$  são *probabilidades condicionais* dado  $f(X) = x$ , onde  $X$  é um elemento aleatório de  $\Omega$  seguindo a lei  $\mu$ . Notação:

$$P[\cdot \mid f(X) = x].$$

Analogamente, a integral  $\int d\mu_x$  é a *esperança condicional* dado  $f(X) = x$ . A igualdade (H.6) serve da base do *jeito de condicionamento*.

**Exercício H.4.3.** Mostre o teorema de Rokhlin no caso onde a medida  $f_*(\mu)$  é puramente atômica em  $\mathcal{Y}$ .

[ *Sugestão:* se  $x$  é um átomo, a medida  $\mu_x$  é simplesmente a normalização da restrição de  $\mu$  sobre  $f^{-1}(x)$ ,

$$\mu_x = \frac{\mu|_{f^{-1}(x)}}{\mu(f^{-1}(x))}. ]$$

Deduzo que basta mostrar o teorema de Rokhlin apenas para medidas  $\mu$  cuja imagem direta  $f_*(\mu)$  é não-atômica.

## H.4.2

Para começar, mostremos o teorema de Rokhlin no caso especial onde  $\Omega$  e  $\mathcal{Y}$  são espaços compactos métricos,  $f: \Omega \rightarrow \mathcal{Y}$  é uma função contínua, e  $\mathcal{Y} = \{0, 1\}^{\mathbb{N}}$  é homeomorfo ao cubo de Cantor. Com o exercício H.4.3 em mente, suponhamos que  $f_*(\mu)$  é uma medida não-atômica.

Diz-se que um espaço métrico tem *dimensão zero* se para cada ponto  $x$  e cada vizinhança  $V$  de  $x$ , existe um conjunto aberto e fechado,  $U$ , tal que  $x \in U \subseteq V$ .

**Exercício H.4.4.** Mostre que o cubo de Cantor  $\{0, 1\}^{\mathbb{N}}$  é um espaço de dimensão zero.

**Exercício H.4.5.** Seja  $K$  um espaço métrico compacto, de dimensão zero, e sem pontos isolados. Mostre que  $K$  é homeomorfo ao cubo de Cantor  $\{0, 1\}^{\mathbb{N}}$ .

[ *Sugestão:* construa uma sequência de partições de  $K$  com abertos e fechados, onça a cada passo todo elemento da partição é dividido em dois.... ]

**Exercício H.4.6.** Mostre que o suporte,  $\text{supp } \mu$ , de uma medida boreliana não-atômica  $\mu$  sobre um espaço métrico qualquer não tem pontos isolados. (Como diz-se,  $\text{supp } \mu$  é um conjunto *perfeito*).

Os exercícios acima permitem assumir, sem perda de generalidade, que a medida  $f(\mu)$  tem  $\mathcal{Y} = \{0, 1\}^{\mathbb{N}}$  como o suporte. Como nas seções precedentes, formemos uma sequência refinadora de partições finitas do cubo de Cantor,  $(\Omega_n)$ , onde  $\Omega_n$  consiste de conjuntos abertos e fechados cilíndricos da forma  $\pi_n^{-1}(\sigma)$ ,  $\sigma \in \{0, 1\}^n$ . Dado um elemento  $C \in \Omega_n$ , definemos uma medida de probabilidade  $\mu_C$  sobre  $\Omega$  como a restrição normalizada de  $\mu$  sobre o conjunto aberto e fechado  $f^{-1}(C)$ :

$$\mu_C = \frac{\mu|_{f^{-1}(C)}}{\mu(f^{-1}(C))}.$$

Como  $\mu(f^{-1}(C)) = f_*(\mu)(C) \neq 0$ , a definição é correta.

Definemos, para cada  $n$ , uma aplicação  $\mu_n: \mathcal{Y} \rightarrow P(\Omega)$  como segue:

$$\mu_n(x) = \mu_C, \text{ para o único } C \in \Omega_n \text{ que contém } x.$$

A sequência  $(\mu_n)$  forma um martingale com valores no espaço  $P(\Omega)$  (relativo a sua estrutura afim), que converge para uma aplicação  $\nu: \mathcal{Y} \rightarrow P(\Omega)$ , cujos valores,  $\nu(x)$ , serão exatamente as nossas medidas  $\mu_x$ . Ao invés de desenvolvermos uma teoria de martingales com valores nos espaços localmente convexos, reduzamos tudo ao caso de martingais reais.

Seja  $g \in C(\Omega)$  uma função contínua qualquer sobre o espaço compacto  $\Omega$ . Para cada  $n$ , definemos a função

$$g_n: \mathcal{Y} \rightarrow \mathbb{R},$$

igual a esperança condicional de  $g$  em relação à partição  $f^{-1}(\Omega_n)$ , pela condição

$$\tilde{g}_n(x) = \int_C g(x) d\mu_C, \text{ onde } x \in C \in \Omega_n.$$

**Exercício H.4.7.** Verificar que a sequência  $[(\tilde{g}_n)]$  é um martingale sobre  $\mathcal{Y}$  em relação à sequência de partições  $(\Omega_n)$ .

Como  $(g_n)$  são uniformemente limitados por  $\|g\|_\infty$ , o martingale tem limite em  $L^1(f_*(\mu))$ , que denotemos por  $\tilde{g}$ . Também temos a convergência em  $f_*(\mu)$ -quase todo  $x$ ,  $\tilde{g}_n(x) \rightarrow \tilde{g}(x)$ .

Fixemos uma sequência  $(g_k)_{k=1}^\infty$  densa na bola unitária de  $C(\Omega)$ . Segue-se que, para  $f_*(\mu)$ -quase todo  $x \in \mathcal{Y}$  e todos  $k$ ,  $(\tilde{g}_k)_n(x) \rightarrow \tilde{g}_k(x)$ , e  $\|(\tilde{g}_k)_n - \tilde{g}_k\|_1 \rightarrow 0$ . Denotemos por  $\mathcal{X}$  o conjunto de  $x \in \mathcal{Y}$  onde a convergência pontual tem lugar para todos  $k$ .

**Exercício H.4.8.** Mostre que, para  $x \in \mathcal{X}$ , a aplicação

$$g_k \mapsto \tilde{g}_k(x)$$

estende-se até um funcional linear positivo sobre  $C(\Omega)$  enviando 1 para 1. Logo, quase certamente existe a única medida de probabilidade  $\mu_x$  sobre  $\Omega$  tal que

$$\tilde{g}_k(x) = \int_\Omega g_k d\mu_x.$$

**Exercício H.4.9.** Verifique que, para  $x \in \mathcal{X}$ , se  $g, h \in C(\Omega)$ ,  $V \ni x$  e uma vizinhança de  $x$  em  $\mathcal{Y}$  são tais que  $g|_{f^{-1}(V)} = h|_{f^{-1}(V)}$ , então

$$\tilde{g}(x) = \tilde{h}(x).$$

Deduzo que, para quase todo  $x$ ,

$$\text{supp } \mu_x \subseteq f^{-1}(x).$$

[ *Sugestão:*  $f$  é contínua. ]



**Exercício H.4.10.** Seja  $x \in \mathcal{Y}$  e  $(C_n)$  uma sequência de abertos e fechados cilíndricos da forma  $C_n = \pi_n^{-1}(\pi_n(x))$ . Mostre que, para quase todo  $x$ ,

$$\mu_{C_n} \rightarrow \mu_x \text{ quando } n \rightarrow \infty$$

na topologia fraca\* em  $P(\Omega)$ .

**Exercício H.4.11.** Combine o exercício precedente com a observação que para cada  $g \in C(\Omega)$  e todo  $k$ ,

$$\int_{\mathcal{Y}} \tilde{g}_k df_*(\mu) = \int_{\Omega} g d\mu$$

para deduzir a afirmação do teorema de Rokhlin (eq. H.6) sob as nossas hipóteses adicionais. (Primeiramente, para funções contínuas, e no conseguinte, para funções  $L^1(\mu)$ ).

### H.4.3

Agora, o caso geral. Começemos com uma variação do teorema de Luzin E.2.14.

**Exercício H.4.12.** Mostre o seguinte. Seja  $f$  uma função mensurável sobre um espaço métrico completo e separável,  $\Omega$ , munido de uma medida de probabilidade boreliana,  $\mu$ , com valores no cubo de Cantor  $\{0, 1\}^{\mathbb{N}}$ . Dado  $\varepsilon > 0$ , existe um subconjunto compacto  $K \subseteq \Omega$  com  $\mu(\Omega \setminus K) < \varepsilon$  tal que a restrição  $f|_K$  é contínua.

Agora identifiquemos  $\mathcal{Y}$ , como espaço boreliano, com  $\{0, 1\}^{\mathbb{N}}$ , e  $\Omega$ , com um espaço compacto métrico qualquer. Para cada  $\varepsilon > 0$ , escolhemos um compacto  $K \subseteq \Omega$  com  $\mu(K) > 1 - \varepsilon$  e  $f|_K$  contínua. Definemos a medida de probabilidade normalizada

$$\mu^\varepsilon = \frac{\mu|_{K_\varepsilon}}{\mu(K_\varepsilon)}.$$

Escolhemos uma família de medidas de probabilidade condicionais,  $(\mu_x^\varepsilon)$ ,  $x \in \mathcal{Y}$ , desintegrando a medida  $\mu^\varepsilon$ . Deixemos como um exercício, de verificar que, se  $\varepsilon_n \downarrow 0$  bastante rápido, então o lema de Borel–Cantelli E.2.27 garante que, para quase todo  $x \in \mathcal{Y}$ , a sequência de medidas  $(\mu_x^{\varepsilon_n})_{n=1}^\infty$  converge na topologia fraca\* para uma medida de probabilidade  $\mu_x$ , e a família  $(\mu_x)$  satisfaz todas as conclusões do teorema de Rokhlin.

### H.4.4 Teorema de Fubini

Um exemplo clássico da desintegração de medidas é o teorema de Fubini.

**Teorema H.4.13.** *Sejam  $(\mathcal{Y}, \mu)$  e  $(\Omega, \nu)$  dois espaços probabilísticos padrão. Então, a desintegração da medida de produto  $\mu \otimes \nu$  sobre  $\mathcal{Y} \times \Omega$  tem forma  $\mu_x = \nu$  para quase todos  $x \in \mathcal{Y}$ . Em outras palavras, para toda função  $f \in L^1(\mu \otimes \nu)$ ,*

$$\int_{\mathcal{Y} \times \Omega} f d(\mu \otimes \nu) = \int_{\mathcal{Y}} d\mu(x) \int_{\Omega} f(x, y) d\nu(y).$$

**Exercício H.4.14.** Mostre o teorema, primeiramente para  $f$  contínua (na topologia de produto, onde  $\Omega$  e  $\mathcal{Y}$  são munidas de estruturas de espaços métricos apropriados), usando as funções  $\tilde{f}_n$  na prova do teorema de Rokhlin, e depois para  $f \in L^1(\mu)$ .

# I

# *Desigualdade de concentração de Paul Lévy*

---

## I.1 Fenômeno de concentração

Consideremos um domínio,  $\Omega$ , potencialmente de “alta dimensão”, como a esfera euclidiana:

$$\mathbb{S}^d = \{x \in \mathbb{R}^{d+1} \mid |x| = 1\}.$$

Suponhamos que o único meio de estudar o objecto em questão seja por uma série dos experimentos aleatórios, do seguinte modo. Cada experimento produz um ponto  $x \in \Omega$  tirado de maneira aleatória (cuja distribuição é conforme a medida natural de  $\Omega$ , como o volume), e cada vez podemos registrar os valores  $f(x)$  de funções (quantidades observáveis)

$$f : X \rightarrow \mathbb{R}$$

para  $x$ . Quanta informação sobre a geometria de  $\Omega$  podemos obter desta maneira?

Por exemplo, o que podemos deduzir sobre o *diâmetro* de  $\Omega$ ? O diâmetro de  $\Omega$  é a quantidade

$$\text{diam } \Omega := \sup\{d(x, y) \mid x, y \in \Omega\},$$

onde  $d(x, y)$  denota a distância entre  $x$  e  $y$ . Nesta situação, como as observáveis  $f : \Omega \rightarrow \mathbb{R}$ , é lógico considerar as funções *Lipschitz contínuas* com a constante de Lipschitz 1, isso é, as funções que não aumentam a distância:

$$\forall x, y \in \Omega \quad |f(x) - f(y)| \leq d(x, y).$$

Eis uma fonte das tais funções.

**Exercício I.1.1.** Seja  $x_0 \in \Omega$  um ponto de  $X$  qualquer. Mostrar que a função distância definida por

$$x \mapsto \text{dist}(x_0, x)$$

é Lipschitz contínua com a constante 1.

Por conseguinte, obtemos o resultado seguinte.

**Exercício I.1.2.** Mostre que

$$\begin{aligned} \text{diam } \Omega &= \sup \{|f(x) - f(y)| : x, y \in \Omega, \\ & f : \Omega \rightarrow \mathbb{R} \text{ é 1-Lipschitz contínua com } L = 1\}. \end{aligned}$$

**Exercício I.1.3.** Verifique que, se  $\Omega$  é compacto, então o valor do diâmetro é realizado pela uma função 1-Lipschitz contínua  $f$  apropriada:

$$\text{diam } \Omega = \max\{d(f(x), f(y)) : x, y \in \Omega\}.$$

Se nós pudéssemos medir os valores de *todos as observáveis* para *todos os pares de pontos de  $X$*  e então escolher o supremo, saberíamos o diâmetro  $\text{diam } X$ . Mas isto é impossível. Podemos escolher *uma* observável  $f$ , e gerar então a seqüência mais ou menos longa, mas *finita*, de pontos aleatórios,

$$x_1, x_2, \dots, x_N,$$

registrando cada vez o valor  $f(x_i)$ ,  $i = 1, 2, 3, \dots$

Depois que produzimos uma série de números reais

$$f(x_1), f(x_2), \dots, f(x_N),$$

calcularemos a diferença máxima

$$D_N = \max_{i,j=1}^N |f(x_i) - f(x_j)|.$$

É imediato que

$$D_N \leq D_{N+1} \leq D,$$

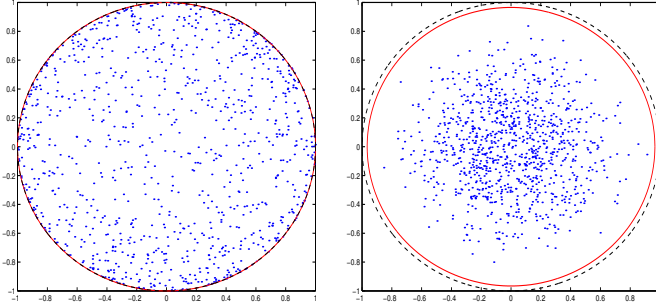


Figura I.1:  $\mathbb{S}^2$  e  $\mathbb{S}^{10}$

de modo que os valores  $D_N$  “melhoram” cada vez.

Pararemos o experimento quando a probabilidade de melhorar o valor precedente,  $D_N$ , se torna demasiado pequena. Mais precisamente, seja  $\kappa > 0$  (um valor limiar) um número fixo muito pequeno, tal como  $\kappa = 10^{-10}$  (sugerido por Gromov).

Nós pararemos depois que o número  $D = D_N$  satisfaz

$$\mu\{x \mid |f(x) - M| < D\} > 1 - \kappa\},$$

onde  $\mu$  é a medida “natural” sobre  $X$ . O valor  $D = D_N$  obtido desta maneira chama-se o *diâmetro observável* de  $X$ . Mais precisamente, o diâmetro observável  $\text{obs-diam}_\kappa X$  é definido por

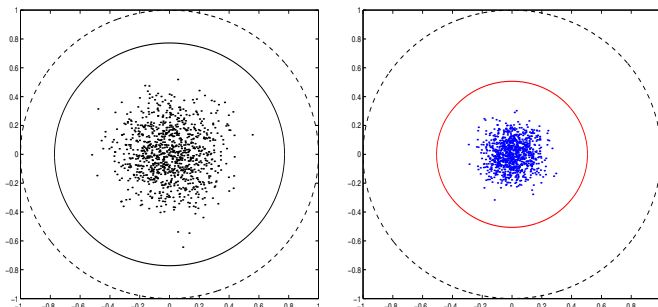
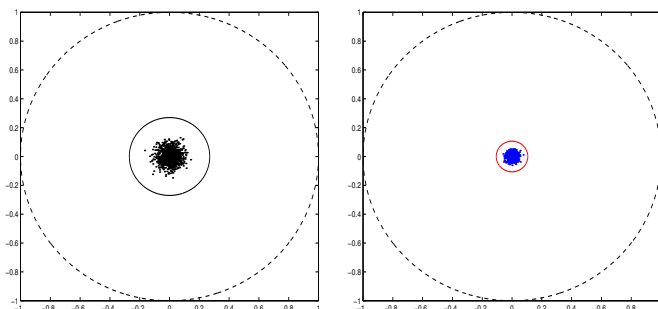
$$\text{obs-diam}_\kappa X = \inf\{D > 0: \text{para cada observável } f \text{ sobre } X, \\ \mu\{x \in X \mid |f(x) - M| \geq D\} \leq \kappa\}.$$

Ilustremos o conceito para as esferas euclidianas  $\mathbb{S}^n$ . Neste experimento, substituímos a reta  $\mathbb{R}$  com uma “tela”  $\mathbb{R}^2$ , e usamos como a observável a projeção coordenada  $\mathbb{R}^{d+1} \rightarrow \mathbb{R}^2$ ,

$$(x_1, x_2, \dots, x_{d+1}) \rightarrow (x_1, x_2).$$

O número dos pontos tirados será fixo a  $N = 1000$ .

As Figuras I.1, I.2 e I.3 mostram os resultados de experimentos. A linha pontilhada representa a projeção da esfera de raio um (a saber, o círculo de raio um), enquanto a linha sólida mostra um círculo de tal raio que a probabilidade de um evento de que a projeção de um ponto aleatório na esfera esteja fora deste círculo é menos que  $\kappa = 10^{-10}$ . Em outras palavras, o diâmetro do círculo solido é o diâmetro observável da esfera  $\mathbb{S}^d$ .

Figura I.2:  $\mathbb{S}^{30}$  e  $\mathbb{S}^{100}$ Figura I.3:  $\mathbb{S}^{500}$  e  $\mathbb{S}^{2500}$

É possível provar que o diâmetro observável da esfera satisfaz

$$\text{obs-diam}_\kappa(\mathbb{S}^d) = \Theta\left(\frac{1}{\sqrt{d}}\right)$$

para cada valor limiar  $\kappa > 0$ . Em outras palavras, assintoticamente, o diâmetro observável da esfera  $\mathbb{S}^n$  é de ordem  $1/\sqrt{d}$ .

Como o diâmetro atual da esfera  $\mathbb{S}^d$  é 2, uma esfera da alta dimensão aparece como um “cometa” formado de um “núcleo” muito pequeno e um “envoltório gasoso” de grande tamanho e de densidade baixa. (Figura I.4).

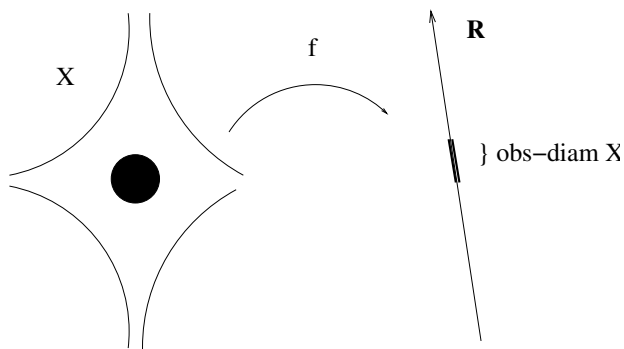


Figura I.4: O diâmetro observável de um espaço da alta dimensão.

Esta observação é típica de outros objetos geométricos da alta dimensão. Por exemplo, é possível mostrar que o diâmetro observável do cubo unitário,

$$\mathbb{I}^d = \{x \in \mathbb{R}^d \mid \forall i = 1, \dots, d, 0 \leq |x_i| \leq 1\},$$

satisfaz

$$\text{obs-diam}_\kappa(\mathbb{I}^d) = \Theta(1).$$

Ou seja, assintoticamente  $\text{obs-diam}_\kappa(\mathbb{I}^d)$  é constante. Ao mesmo tempo,

$$\text{diam}(\mathbb{I}^d) = \sqrt{d}.$$

Com efeito, nas altas dimensões a projeção ortogonal do cubo  $\mathbb{I}^d$  com  $N = 1000$  pontos aleatórios sobre um plano aleatório assemelha-se fortemente à projeção da esfera. Veja as Figuras I.5, I.6, e I.8.

A dependência do diâmetro observável no valor limiar  $\kappa$  não é muito sensível (somente logarítmica).

O fenômeno de concentração de medida sobre as estruturas de alta dimensão pode ser exprimido da seguinte maneira informal:

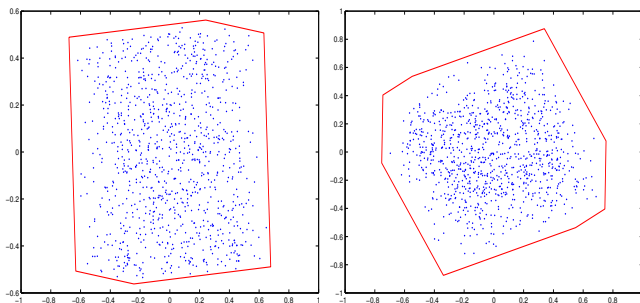


Figura I.5: Projeções do cubo  $\mathbb{I}^d$  e dos 1,000 pontos aleatórios no cubo sobre um plano aleatório,  $d = 3, 4$ .

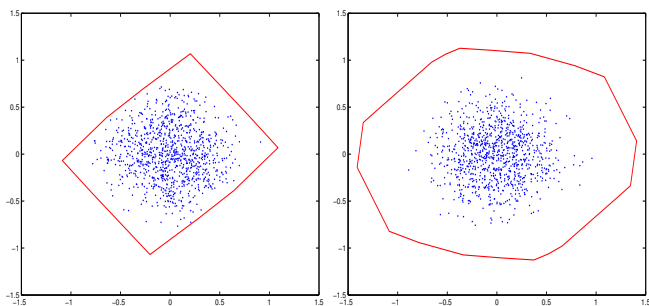


Figura I.6: O mesmo,  $d = 5, 10$ .

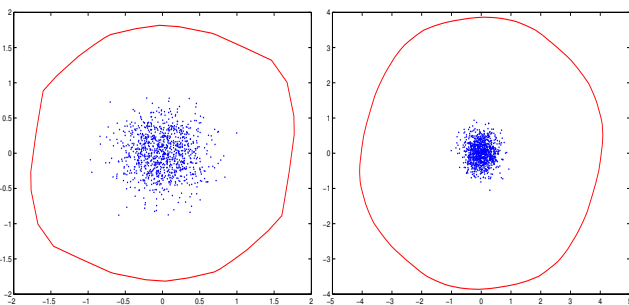


Figura I.7: O mesmo,  $d = 20, 100$ .



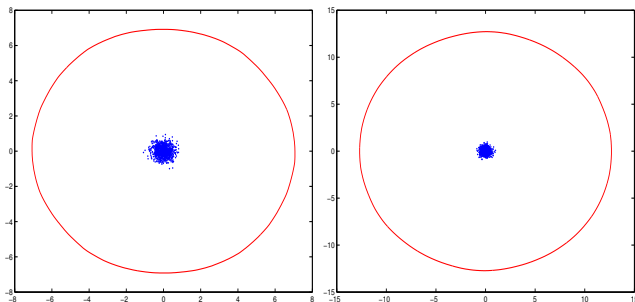


Figura I.8: O mesmo,  $d = 300, 1000$ .

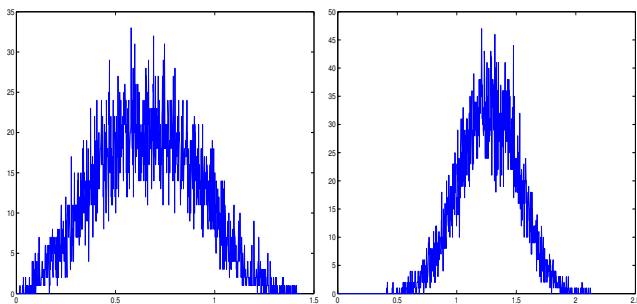


Figura I.9: Distribuição das distâncias entre 10,000 pontos aleatórios do cubo  $\mathbb{I}^d$ ,  $d = 3, 10$ .

*O diâmetro observável de um objeto geométrico de alta dimensão é tipicamente demasiado pequeno comparado ao diâmetro atual:*

$$\text{obs-diam}(X) \ll \text{diam}(X).$$

A formulação mais precisa usa a noção do *tamanho característico* de  $X$  em vez do diâmetro. Sobre um espaço de grande dimensão, os valores da distância  $d(x, y)$  tipicamente concentram em torno da esperança da distância, ou do *tamanho característico* de  $X$ ,

$$\text{charSize}(X) = \mathbb{E}_{\mu \otimes \mu}(d(x, y)).$$

Veja as Figuras I.9 e I.10 para o cubo  $\mathbb{I}^d$ .

Por exemplo, o tamanho característico da esfera é, assintoticamente,  $\Theta(1)$ :

$$\text{charSize}(S^n) \rightarrow \sqrt{2} \text{ quando } n \rightarrow \infty.$$

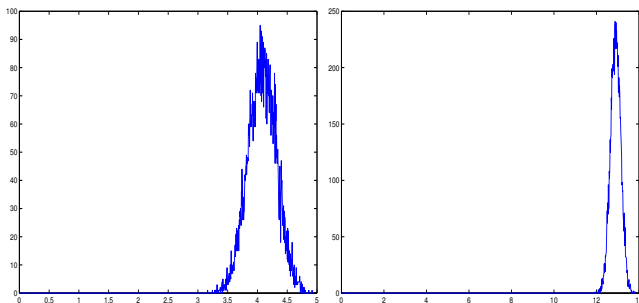


Figura I.10: O mesmo,  $d = 100, 1000$ .

O fenômeno de concentração de medida na forma mais exata diz o que

Diâmetro observável  $\ll$  tamanho característico.

O fenômeno é o assunto de estudo de uma disciplina matemática relativamente nova: a *análise geométrica assintótica*. Esta introspeção na geometria dos objectos de dimensão alta é a mais importante, e tem muitas aplicações e conseqüências amplas em ciências matemáticas.

Eis uma reformulação heurística equivalente (embora não evidente) do fenômeno:

*Tipicamente, num espaço  $\Omega$  de grande dimensão, para cada subconjunto  $A \subseteq \Omega$  que contém pelo menos a metade dos pontos, a maior parte dos pontos de  $\Omega$  estão próximos ao  $A$ .*

Nós já formalizamos a noção de uma “estrutura” no texto principal, como um espaço métrico  $\Omega = (\Omega, \rho, \mu)$  munido de uma medida de probabilidade boreliana. Concentração no cubo de Hamming  $\{0, 1\}^n$  forma o assunto do capítulo 1. Neste apêndice vamos estabelecer a concentração de medida na esfera euclideana unitária  $\mathbb{S}^d$ .

Denotemos

$$A_\epsilon = \{x \in \Omega : \exists a \in A \ \rho(x, a) < \epsilon\}$$

a  $\epsilon$ -vizinhança do sub-conjunto  $A$  de  $\Omega$ .

**Definição I.1.4.** Seja  $(\Omega_d, \rho_d, \mu_d)$ ,  $d = 1, 2, 3, \dots$  uma família de espaços métricos munidos de uma medida de probabilidade boreliana (espaços métricos com medida). Esta família é uma família de Lévy se, para cada família  $A_d$ ,  $d = 1, 2, \dots$ , de sub-conjuntos boreleanos de  $\Omega_d$ , tais que

$$\liminf \mu_d(A_d) > 0,$$

e por cada  $\epsilon > 0$ , temos

$$\mu_d((A_d)_\epsilon) \rightarrow 1.$$

As famílias “naturais” dos espaços métricos com medida são tipicamente as famílias de Lévy, depois de normalizarmos o tamanho característico. Um instrumento conveniente para quantificar o fenômeno da concentração é a *função de concentração*.

**Definição I.1.5.** Seja  $(\Omega, d, \mu)$  um espaço métrico com medida. A *função de concentração* de  $\Omega$ , notada  $\alpha_\Omega(\epsilon)$ , é definida pelas condições seguintes:

$$\alpha(\epsilon) = \begin{cases} \frac{1}{2}, & \text{se } \epsilon = 0, \\ 1 - \min \{ \mu_\#(A_\epsilon) : A \subseteq \Sigma^n, \mu_\#(A) \geq \frac{1}{2} \}, & \text{se } \epsilon > 0. \end{cases}$$

**Teorema I.1.6.** Uma família  $(\Omega_d, \rho_d, \mu_d)$  é uma família de Lévy se e apenas se as funções de concentração tendem a zero:

$$\alpha(\Omega_d, \epsilon) \rightarrow 0 \text{ para cada } \epsilon > 0.$$

□

**Definição I.1.7.** Uma família de Lévy  $(\Omega_d, d_d, \mu_d)$  é chamada uma *família de Lévy normal* se existem  $C_1, C_2 > 0$  tais que

$$\alpha(\Omega_d, \epsilon) \leq C_1 e^{-C_2 \epsilon^2 d}.$$

Aqui está a ligação com o diâmetro observável: sobre uma estrutura de grande dimensão, toda função Lipschitz contínua é quase constante em toda parte exceto sobre um conjunto da medida muito pequena.

Relembramos que um número real  $M = M_f$  é dito um *valor mediano* de uma função boreliana  $f$ , sobre um espaço com medida de probabilidade  $(\Omega, \mu)$  se

$$\mu\{x \in \Omega : f(x) \geq M\} \geq \frac{1}{2} \text{ e } \mu\{x \in \Omega : f(x) \leq M\} \geq \frac{1}{2}.$$

Um valor mediano  $M = M_f$  existe sempre, mas geralmente, não é único.

**Exercício I.1.8.** Seja  $f$  uma função Lipschitz contínua com a constante de Lipschitz  $L \geq 0$  sobre um espaço métrico com medida,  $(\Omega, \rho, \mu)$ . Provar que

$$\mu\{|f(x) - M| > \epsilon\} \leq 2\alpha_\Omega\left(\frac{\epsilon}{L}\right).$$

Mais geralmente, se  $f$  é uniformemente contínua de tal modo que

$$\forall x, y \in X, d(x, y) < \delta \Rightarrow |f(x) - f(y)| < \epsilon,$$

então

$$\mu\{|f(x) - M| > \epsilon\} \leq 2\alpha_X(\delta).$$

▲

A função distância  $d(-, p)$  de um ponto  $p$  fixo qualquer é Lipschitz contínua (com a constante 1), e nos domínios de alta dimensão uma tal função concentra-se em torno do valor mediano.

Entre os livros tratando do fenômeno de concentração de medida, [Milman e Schechtman 1986] é o mais acessível, [Ledoux 2001] o mais abrangente e [Gromov 1999] contém uma riqueza de idéias. Eu não tive a chance de obter uma cópia do livro recente [Artstein-Avidan, Giannopoulos e Milman 2015], que parece ser excelente e pode tornar-se a fonte principal de referência. Também, eu ainda não estudei o livro [Vershynin 2018] dedicado às aplicações do fenômeno de concentração na ciência de dados, inclusive tópicos na aprendizagem estatística.

## I.2 Medida de Haar sobre a esfera euclidiana

### I.2.1 Duas métricas

A esfera euclidiana de raio um

$$\mathbb{S}^n = \{x \in \ell^2(n+1) \mid |x| = 1\}$$

admite duas métricas padrão. Elas são: a distância euclidiana induzida do espaço  $\ell^2(n+1)$ ,

$$d_{eucl}(x, y) = \|x - y\|_2,$$

assim como a distância geodésica, ou seja, o comprimento do menor arco do círculo máximo entre  $x$  e  $y$ , ou, de modo equivalente, o valor do ângulo entre dois vetores (em radianos):

$$d_{geo}(x, y) = \angle(x, y).$$

As duas distâncias são equivalentes: para todos  $x, y \in \mathbb{S}^n$ , temos

$$d_{eucl}(x, y) \leq d_{geo}(x, y) \leq \frac{\pi}{2} d_{eucl}(x, y),$$

e no caso onde  $d_{geo}(x, y) \leq \pi/2$ , temos

$$d_{eucl}(x, y) \leq d_{geo}(x, y) \leq \frac{\pi}{2\sqrt{2}} d_{eucl}(x, y). \quad (\text{I.1})$$

Até melhor, as duas distâncias são ligadas por uma transformação métrica:

$$d_{eucl}(x, y) = 2 \sin\left(\frac{d_{geo}(x, y)}{2}\right). \quad (\text{I.2})$$

O grupo ortogonal

$$O(n+1) = \{u \in M_{n+1}(\mathbb{R}) : u^t u = u u^t = 1\}$$

age sobre a esfera por isometrias:

$$\mathbb{S}^n \ni x \mapsto ux \in \mathbb{S}^n, \quad u \in O(n+1).$$

Aqui  $ux$  é o produto usual de uma matriz ortogonal  $u$  do comprimento  $(n+1) \times (n+1)$  e um vetor-coluna  $x$  do comprimento  $(n+1) \times 1$ . De fato, isometrias com relação a uma distância são isometrias com relação a outra.

## 1.2.2 Medidas de probabilidade sobre a esfera

Como antes, denotemos por  $P(X)$  a família de todas as medidas de probabilidade borelianas sobre um espaço boreliano padrão  $X$ . O teorema de representação de Riesz [H.2.1](#) diz que as medidas de probabilidade borelianas sobre um espaço compacto  $X$  admitem uma correspondência bijetora com os funcionais lineares e positivos sobre  $C(X)$  enviando 1 para 1.

No teorema de Riesz, em vez de funções contínuas, basta considerar as funções Lipschitz contínuas. Por exemplo, teorema de Stone–Weierstrass [F.3.1](#) implica que as funções Lipschitz contínuas são densas em  $C(X)$ .

Para  $X$  compacto metrizável,  $P(X)$  torna-se em um espaço compacto metrizável (teorema [H.2.37](#)). A topologia sobre  $P(X)$  é completamente determinada pelas seqüências convergentes, e uma seqüência  $(\mu_n)$  de medidas de probabilidade converge para uma medida de probabilidade  $\mu$  se e somente se, para toda função  $f: X \rightarrow \mathbb{R}$ , temos

$$\int f d\mu_n \rightarrow \int f d\mu. \tag{I.3}$$

Uma medida de probabilidade,  $\mu$ , sobre  $\mathbb{S}^n$  é *invariante por rotações* se para todo subconjunto boreliano  $A \subseteq \mathbb{S}^n$  e toda  $u \in O(n+1)$ , temos

$$\mu(uA) = \mu(A).$$

De modo equivalente, isso é o caso se para todas funções contínuas (ou Lipschitz contínuas, ou mesmo 1-Lipschitz contínuas)  $f: \mathbb{S}^n \rightarrow \mathbb{R}$  e todas  $u \in O(n+1)$ , temos

$$\int u f d\mu = \int f d\mu,$$

onde

$$u f(x) = f(u^{-1}x)$$

é a translação a esquerda de  $f$  por  $u$ .

Finalmente, pode-se definir uma translação a esquerda da medida  $\mu$  por  $u$ , como segue:

$$u * \mu(A) = \mu(u^{-1}A).$$

A invariância de  $\mu$  significa que para cada  $u$ ,

$$u * \mu = \mu.$$

O nosso resultado principal é o seguinte.

**Teorema I.2.1.** *Existe uma e uma só medida de probabilidade boreliana  $\nu = \nu_n$  sobre  $\mathbb{S}^n$  que é invariante por isometrias:*

$$\nu_n(A) = \nu_n(uA) \text{ para toda } u \in O(n+1).$$

Esta medida é chamada a *medida de Haar*. A prova que vamos fazer estende-se facilmente sobre todos grupos compactos e seus espaços homogêneos. Ela pode ser estendido sobre todos os grupos localmente compactos, mas a extensão exige a Axioma de Escolha.

### 1.2.3 Teorema de Hall–Rado

Seja  $C$  um subconjunto finito de vértices de um grafo. Denotemos por  $\partial C$  a coleção de todos os vértices adjacentes a um ou mais vértices de  $C$ .

**Teorema I.2.2** (Teorema de emparelhamento de Hall–Rado). *Seja  $\Gamma = (V, E) = (A, B, E)$  um grafo finito bipartido, onde  $V$  denota vértices,  $E$  denota arestas,  $V = A \sqcup B$ . As condições seguintes são equivalentes.*

1. *Existe uma aplicação injetora  $i: A \rightarrow B$  com  $(a, i(a)) \in E$  para todo  $a \in A$  (um emparelhamento para  $A$ ).*
2. *Para todo  $C \subseteq A$ , temos*

$$|\partial C| \geq |C|.$$

*Demonstração.* A implicação (1)  $\Rightarrow$  (2) é óbvia porque  $i(C) \subseteq \partial C$ . A implicação contrária (2)  $\Rightarrow$  (1) tem pelo menos 7 diferentes provas conhecidas. Vamos apresentar uma delas, usando indução matemática sobre o tamanho  $n$  de  $A$ .

Para  $n = 1$  a afirmação é evidente. Suponha que ela foi mostrada para todos valores  $1 \leq k \leq n$ , e seja  $|A| = n + 1$ . Vamos estudar dois casos separadamente.

(a) Tem muita redundância no grafo, nomeadamente, para todo subconjunto próprio  $C \subsetneq A$  temos  $|\partial C| > |C|$ . Se for o caso, escolha um vértice  $a_0 \in A$  assim como um vértice adjacente  $b_0 \in B$ . Denote  $\tilde{\Gamma} = (\tilde{V}, \tilde{E})$  o grafo obtido de  $\Gamma$  apagando os vértices  $a_0, b_0$  assim como todas as arestas provenientes de  $a_0$  ou chegando em  $b_0$ . Se  $C \subseteq \tilde{V}$ , então  $C \subseteq A$  e por que no máximo um elemento da fronteira de  $C$  foi perdido (nomeadamente,  $b_0$ ), temos  $|\partial_{\tilde{\Gamma}} C| \geq |\partial_{\Gamma} C - 1 \geq |C|$ . Logo, o grafo  $\tilde{\Gamma}$  satisfaz a hipótese e como  $\tilde{A} = A \setminus \{a_0\}$  só tem  $n$  vértices, existe um emparelhamento  $i$  para  $\tilde{A}$  cuja imagem exclui  $b_0$ . Extendendo  $i$  sobre  $A$  por  $i(a_0) = b_0$ , obtemos o emparelhamento desejado para  $A$ .

(b) Não tem redundância como acima, logo existe um conjunto  $C \subsetneq A$ ,  $C \neq \emptyset$  tal que  $|\partial C| = |C|$ . Neste caso, todo vértice  $c \in C$  à adjacente à um vértice de  $B$  só, logo pode-se definir um emparelhamento parcial  $i_C$  de  $C$  de modo único possível. Definamos  $D = A \setminus C$ , e seja  $\tilde{\Gamma}$  um grafo bipartido obtido de  $\Gamma$  apagando  $C$  e  $i_C(C)$ ,

assim como todas as arestas entre estes dois conjuntos. O grafo  $\Gamma$  satisfaz a hipótese: de fato, supondo que para  $E \subsetneq D$  tem  $|\partial E| < |E|$ , obtemos uma contradição, porque  $\partial(D \cup C) = \partial D \cup \partial C$ , onde a união é disjunta, de modo que a cardinalidade dela é  $< |D| + |C|$ . Como  $|D| \leq n$ , existe um emparelhamento parcial  $i_D$  segundo a hipótese indutiva. Coalescendo  $i_C$  e  $i_D$ , obtemos o emparelhamento desejado  $i$  para  $A$ .  $\square$

### 1.2.4 Construção da medida de Haar

Seja  $\epsilon > 0$  qualquer. A esfera  $\mathbb{S}^n$ , sendo compacta, admite uma  $\epsilon$ -rede finita. Seja  $\mathcal{N} = \mathcal{N}(\epsilon)$  uma tal  $\epsilon$ -rede do menor tamanho possível, com  $N(\epsilon) = N(\epsilon, \mathbb{S}^n)$  elementos. (A distância sobre a esfera pode ser euclídeana ou geodésica). Denotemos por  $\mu_{\mathcal{N}(\epsilon)}$  a medida empírica suportada sobre os elementos da rede  $\mathcal{N}(\epsilon)$ , e seja

$$\int f d\mu_{\mathcal{N}(\epsilon)} = \frac{1}{N(\epsilon, \mathbb{S}^n)} \sum_{x \in \mathcal{N}(\epsilon)} f(x)$$

a integral correspondente (o valor médio de  $f$  sobre elementos de  $\mathcal{N}(\epsilon)$ ).

A sequência de medidas  $(\mu_{\mathcal{N}(1/k)})$ ,  $k \in \mathbb{N}_+$  admite uma subsequência convergente, pois o espaço  $P(\mathbb{S}^n)$  é compacto e metrizável. Escolha uma sequência de valores de  $\epsilon$ ,  $(\epsilon_k)$ , e uma medida  $\mu$ , tais que

$$\mu_{\mathcal{N}(\epsilon_k)} \rightarrow \mu.$$

É a nossa medida de Haar, faltando só verificar a sua invariância e a unicidade.

### 1.2.5 Invariância de $\mu$ pelas isometrias

**Lema 1.2.3.** *Seja  $\mathcal{N}, \mathcal{N}'$  duas  $\epsilon$ -redes quaisquer do tamanho mínimo  $N(\epsilon)$ , e seja  $f : \mathbb{S}^n \rightarrow \mathbb{R}$  uma função 1-Lipschitz contínua. Então,*

$$\left| \int f d\mu_{\mathcal{N}} - \int f d\mu_{\mathcal{N}'} \right| < 2\epsilon.$$

*Demonstração.* Formemos um grafo bipartido com o conjunto de vértices  $\mathcal{N} \sqcup \mathcal{N}'$ , onde  $x \in \mathcal{N}$  e  $y \in \mathcal{N}'$  são adjacentes se e somente se as bolas abertas de raio  $\epsilon$  em torno de  $x$  e de  $y$  se encontram. Vamos verificar a condição (ii) do teorema de Hall–Rado. Seja  $C \subseteq \mathcal{N}$  qualquer.

Segundo a definição de uma  $\epsilon$ -rede, todo elemento de uma bola  $B_\epsilon(x)$ ,  $x \in C$ , e contido numa bola  $B_\epsilon(y)$ , onde  $y \in \mathcal{N}'$ . Isso implica que  $y$  é adjacente a  $x$ , logo pertence a  $\partial C$ . Concluimos:

$$\bigcup_{x \in C} B_\epsilon(x) \subseteq \bigcup_{y \in \partial C} B_\epsilon(y).$$

Por conseguinte, se eliminarmos da rede  $\mathcal{N}$  o conjunto  $C$  e substituirmos  $\partial C$ , obtemos uma  $\epsilon$ -rede de novo. Como o tamanho de uma  $\epsilon$ -rede não pode ser menor do tamanho de  $\mathcal{N}$ , concluímos:  $|\partial C| \geq |C|$ .

Segundo o teorema de Hall–Rado, existe uma injeção  $i: \mathcal{N} \rightarrow \mathcal{N}'$  (logo, uma bijeção) tal que

$$d(x, i(x)) < 2\epsilon$$

para todo  $x \in \mathcal{N}$ . Porque  $f$  é 1-Lipschitz contínua, temos

$$|f(x) - f(i(x))| < 2\epsilon,$$

o que traduz-se na propriedade parecida para os valores médios. □

Sejam agora  $u \in O(n+1)$  qualquer, e  $f$  uma função 1-Lipschitz contínua sobre a esfera. Seja  $\delta > 0$ . Escolha  $N$  tão grande que para todo  $k \geq N$ ,

$$\left| \int f d\mu - \int f d\mu_{\epsilon_k} \right| < \delta \text{ and } \left| \int u f d\mu - \int u f d\mu_{\epsilon_k} \right| < \delta.$$

A medida  $u * \mu_{\epsilon_k}$  é uma medida uniforme suportada sobre os elementos de  $u^{-1}\mathcal{N}(\epsilon_k)$ , uma  $\epsilon_k$ -rede do tamanho mínimo. Segundo lema 1.2.3,

$$\left| \int f d\mu_{\epsilon_k} - \int u f d\mu_{\epsilon_k} \right| < 2\epsilon_k.$$

Concluimos:

$$\left| \int f d\mu - \int u f d\mu \right| < 2(\delta + \epsilon_k) \rightarrow 0,$$

e o resultado segue-se. □

*Observação 1.2.4.* O mesmo argumento estabelece a existência de uma medida de probabilidade boreliana sobre cada grupo compacto metrizável, munido de uma métrica é invariante pelas translações a esquerda e a direita. Particularmente, isto se aplica ao grupo ortogonal  $O(n+1)$ . Como uma métrica bi-invariante gerando a topologia, pode-se usar, por exemplo, a distância de Hilbert-Schmidt, ou seja, a distância entre as matrizes vistas como vetores num espaço euclidiano:

$$\|u - v\|_2 = \text{tr}((u - v)^t(u - v)).$$

Mais uma vez, esta medida chama-se a medida de Haar sobre  $O(n+1)$ .

**Exercício 1.2.5.** Verifique que a distância de Hilbert-Schmidt é bi-invariante sobre o grupo  $O(n+1)$ .



### I.2.6 Unicidade de $\mu$

Com a finalidade de estabelecer a unicidade da medida  $\mu$ , vamos utilizar uma medida de Haar sobre  $O(n+1)$ , denotada  $\nu$ . Dado uma  $f \in C(\mathbb{S}^n)$ , temos, usando o teorema de Fubini H.4.13 e a invariância das medidas,

$$\begin{aligned}\mu(f) &= \int_{\mathbb{S}^n} f(x) d\mu(x) \\ &= \int_{O(n+1)} \underbrace{\int_{\mathbb{S}^n} f(ux) d\mu(x)}_{\text{constante em } u} d\nu(u) \\ &= \int_{\mathbb{S}^n} \int_{O(n+1)} f(ux) d\nu(u) d\mu(x).\end{aligned}$$

Agora vamos mostrar que, de fato, a integral interior

$$\int_{O(n+1)} f(ux) d\nu(u)$$

não depende de  $x$ . Para todo  $y \in \mathbb{S}^n$ , tem  $v \in O(n+1)$  tal que  $v^{-1}x = y$ , o que implica

$$\begin{aligned}\int_{O(n+1)} f(ux) d\nu(u) &= \int_{O(n+1)} v f(ux) d\nu(u) \\ &= \int_{O(n+1)} f(v^{-1}uv y) d\nu(u) \\ &= \int_{O(n+1)} f(wy) d\nu(w)\end{aligned}$$

(depois a mudança de variável  $w = v^{-1}uv$ , compare exercício H.1.15).

Denotemos o valor dessa integral por  $\bar{\nu}(f)$ . Deste modo,

$$\mu(f) = \bar{\nu}(f).$$

Se agora  $\mu'$  é uma outra medida de probabilidade invariante sobre a esfera, temos pelo mesmo argumento

$$\mu'(f) = \bar{\nu}(f) = \mu(f).$$

□

*Observação I.2.6.* O argumento idêntico estabelece a unicidade de uma medida de Haar sobre um espaço homogêneo qualquer de um grupo compacto, inclusive sobre o grupo  $O(n)$  próprio.

## I.3 Concentração de medida na esfera

### I.3.1 Medida de calotas esféricas

Denotemos por

$$C_r(x) = \{y \in \mathbb{S}^n : d_{geo}(x, y) \leq r\}$$

a calota fechada esférica de raio geodésico  $r$ . Por exemplo, as calotas de raio  $\pi/2$  são hemisférios.

**Exercício I.3.1.** Verificar que

$$\cos t \leq e^{-t^2/2}$$

quando  $0 \leq t \leq \pi/2$ . ▲

**Lema I.3.2.** A medida de Haar normalizada,  $\mu_{n+1}$ , da calota esférica da esfera  $\mathbb{S}^{n+1}$  de raio geodésico  $\frac{\pi}{2} - \epsilon$ , onde  $\epsilon > 0$ , satisfaz

$$\mu_{n+1}(C_\epsilon) \leq \sqrt{\frac{\pi}{8}} e^{-n\epsilon^2/2}. \quad (\text{I.4})$$

*Demonstração.* Denotemos, para simplificar,  $C = C_{\pi/2-\epsilon}(x_0)$ . Para todo  $\theta > 0$ , o conjunto de pontos à distância  $\pi/2 - \theta$  de  $x_0$  forma uma esfera de dimensão  $n$  de raio  $\cos \theta$ , cujo volume é proporcional a  $\cos^n \theta$ . Por conseguinte,

$$\mu(C) = \frac{\int_\epsilon^{\pi/2} \cos^n \theta d\theta}{\int_{-\pi/2}^{\pi/2} \cos^n \theta d\theta}.$$

Denotemos

$$I_n = \int_0^{\pi/2} \cos^n \theta d\theta.$$

Integrando por partes,

$$\begin{aligned} I_k &= \int_0^{\pi/2} \cos^k \theta d\theta \\ &= \int_0^{\pi/2} \cos^{k-1} \theta d(\sin \theta) \\ &= \cos^{k-1} \theta \sin \theta \Big|_0^{\pi/2} - \int_0^{\pi/2} (k-1) \cos^{k-2} \theta (-\sin \theta) \sin \theta d\theta \\ &= (k-1) \int_0^{\pi/2} \cos^{k-2} \theta \sin^2 \theta d\theta \\ &= (k-1) \int_0^{\pi/2} \cos^{k-2} \theta d\theta - (k-1) \int_0^{\pi/2} \cos^k \theta d\theta \\ &= (k-1) I_{k-2} - (k-1) I_k, \end{aligned}$$

obtemos a relação recursiva

$$I_k = \frac{k-1}{k} I_{k-2},$$

qual, depois a multiplicação por  $\sqrt{k}$  e usando o fato óbvio  $k-1 \geq \sqrt{k(k-2)}$ , leva a

$$\sqrt{k} I_k \geq \sqrt{k-2} I_{k-2}.$$

Concluimos:

$$\sqrt{n} I_n \geq \min\{I_1, \sqrt{2} I_2\} = \min\{1, \sqrt{2\pi}/4\} = 1.$$

Segue-se que

$$\frac{1}{2I_n} \leq \frac{\sqrt{n}}{2}. \quad (1.5)$$

Usando a mudança de variáveis  $\theta = \tau/\sqrt{n}$ , seguida por mais uma mudança de variáveis,  $t = \tau - \epsilon\sqrt{n}$ , conseguimos

$$\begin{aligned} 2I_n \mu(C) &= \int_{\epsilon}^{\pi/2} \cos^n \theta d\theta \\ &= \frac{1}{\sqrt{n}} \int_{\epsilon\sqrt{n}}^{(\pi/2)\sqrt{n}} \cos^n \left( \frac{\tau}{\sqrt{n}} \right) d\tau \\ &\leq \frac{1}{\sqrt{n}} \int_{\epsilon\sqrt{n}}^{(\pi/2)\sqrt{n}} e^{-\tau^2/2} d\tau \\ &\leq \frac{1}{\sqrt{n}} e^{-\epsilon^2 n/2} \int_0^{(\pi/2-\epsilon)\sqrt{n}} e^{-t^2/2} dt \\ &\leq \frac{1}{\sqrt{n}} e^{-\epsilon^2 n/2} \int_0^{\infty} e^{-t^2/2} dt \\ &= \frac{e^{-\epsilon^2 n/2} \sqrt{\pi/2}}{\sqrt{n}}, \end{aligned}$$

e a eq. (1.5) leva a

$$\begin{aligned} \mu(C) &\leq \frac{e^{-\epsilon^2 n/2} \sqrt{\pi/2}}{\sqrt{n}} \times \frac{\sqrt{n}}{2} \\ &= \sqrt{\frac{\pi}{8}} e^{-n\epsilon^2/2}. \end{aligned}$$

### 1.3.2 Distância de Hausdorff

Seja  $X = (X, d)$  um espaço métrico de diâmetro finito. Para todos subconjuntos  $A, B \subseteq X$ , defina-se a *distância de Hausdorff* entre eles, como segue:

$$d_H(A, B) = \inf\{\epsilon > 0: A \subseteq B_\epsilon \wedge B \subseteq A_\epsilon\}.$$

**Exercício 1.3.3.** Verificar que a distância de Hausdorff sobre o espaço de todos os subconjuntos de  $X$  é não negativa, simétrica, e satisfaz a desigualdade triangular. (Ou seja,  $d_H$  é uma *pseudométrica*). ▲

**Exercício 1.3.4.** Mostre que, se  $F, G$  são subconjuntos fechados num espaço métrico  $X$  tais que  $d_H(F, G) = 0$ , então  $F = G$ .

Por conseguinte, a família  $\mathfrak{F}(X)$  de todos os subconjuntos não vazios e fechados de  $X$ , munida da distância de Hausdorff, é um espaço métrico.

Relembremos que um espaço métrico  $X$  é *totalmente limitado*, ou *precompacto*, se para todo  $\epsilon > 0$  existe uma  $\epsilon$ -rede finita para  $X$ . Um espaço métrico  $X$  é compacto se e somente se ele é precompacto e completo.

**Lema 1.3.5.** *Se  $X$  é um espaço métrico totalmente limitado, então  $\mathfrak{F}(X)$  é totalmente limitado.*

*Demonstração.* Seja  $\epsilon > 0$  qualquer. Escolha uma  $\epsilon$ -rede para  $X$ ,  $\mathcal{N}$ . É fácil de verificar que a família finita  $2^{\mathcal{N}}$  de todos os subconjuntos não vazios de  $\mathcal{N}$  forma uma  $\epsilon$ -rede para o espaço  $\mathfrak{F}(X)$ . □

**Lema 1.3.6.** *Se  $X$  é um espaço métrico compacto, então  $\mathfrak{F}(X)$  é compacto.*

*Demonstração.* Só temos que mostrar que o espaço métrico  $\mathfrak{F}(X)$  é completo. Seja  $(F_n)$  uma sequência de Cauchy em  $\mathfrak{F}(X)$ . Sem perda de generalidade e passando a uma sub-sequência se for necessário, pode-se supor que para todos  $n \leq m$ ,

$$F_m \subseteq (F_n)_{2^{-n}}.$$

Seja  $\overline{(F_n)_{2^{-n-1}}}$  a aderência da  $2^{-n-1}$ -vizinhança de  $F_n$ , para todo  $n$ . É claro que a sequência seguinte de conjuntos fechados é encaixada:

$$\overline{(F_1)_{1/4}} \supseteq \overline{(F_2)_{1/8}} \supseteq \dots \supseteq \overline{(F_n)_{2^{-n-1}}} \supseteq \dots$$

A interseção

$$F = \bigcap_{n=1}^{\infty} \overline{(F_n)_{2^{-n-1}}}$$

não é vazia em virtude da compacidade de  $X$ , e agora verifica-se facilmente que a sequência  $(F_n)$  converge para  $F$ . □

**Definição 1.3.7.** Uma função  $f : X \rightarrow \mathbb{R}$  sobre um espaço métrico (ou topológico)  $X$  é dita *semicontínua superiormente* em um ponto  $x_0 \in X$  se para todo  $\epsilon > 0$  tem uma vizinhança  $V$  de  $x_0$  tal que

$$\forall y \in V, f(y) \leq f(x_0) + \epsilon.$$

A função  $f$  é semicontínua superiormente se ela é semicontínua superiormente em todo ponto.

De modo equivalente,  $f$  é semicontínua superiormente se a imagem inversa de todo intervalo aberto e semi-infinito  $(-\infty, b)$  é aberto em  $X$ . Mais uma definição equivalente: a imagem inversa de todo intervalo fechado e semi-infinito  $[a, +\infty)$  é fechado em  $X$ . ▲

Os dois resultados seguintes são verdadeiros se a esfera  $\mathbb{S}^n$  for substituída por um espaço métrico qualquer do diâmetro limitado, munido de uma medida boreliana de probabilidade.

**Exercício 1.3.8.** Mostre que a função

$$A \mapsto \mu(A)$$

sobre o espaço  $\mathfrak{F}(\mathbb{S}^n)$  munido da distância de Hausdorff e a medida de Haar é semicontínua superiormente, mas não é contínua. ▲

**Exercício 1.3.9.** Seja  $A$  um subconjunto fechado de  $\mathbb{S}^n$ . Definamos a família  $\mathcal{G} \subseteq \mathfrak{F}(\mathbb{S}^n)$  como a coleção de todos subconjuntos fechados  $B$  da esfera  $\mathbb{S}^n$  tendo duas propriedades:

1.  $\nu(B) = \nu(A)$ ,
2. para todo  $\epsilon > 0$ ,  $\nu(B_\epsilon) \leq \nu(A_\epsilon)$ .

Mostre que o conjunto  $\mathcal{G}$  é fechado em  $\mathfrak{F}(\mathbb{S}^n)$  com relação à métrica de Hausdorff. ▲

O seguinte é a “metade superior” do teorema de Weierstrass sobre as funções contínuas sobre os conjuntos compactos.

**Exercício 1.3.10.** Mostre que toda função semicontínua superiormente sobre um espaço compacto tem o máximo.

[ *Sugestão:* use a contrapositiva. ]

### 1.3.3 Simetrização por dois pontos

Seja  $\vec{x} \in \mathbb{S}^n \subseteq \ell^2(n+1)$  um vetor de comprimento um. Denotemos

$$H = H(\vec{x}) = \{y \in \ell^2(n+1) : \langle y, \vec{x} \rangle = 0\}$$

o hiperplano ortogonal à direção  $\vec{x}$ ,

$$S_0 = S_0(\vec{x}) = \{y \in \mathbb{S}^n : \langle y, \vec{x} \rangle = 0\} = \mathbb{S}^n \cap H,$$

a esfera equatorial correspondente,

$$\mathbb{S}_+ = \mathbb{S}_+(\vec{x}) = \{y \in \mathbb{S}^n : \langle y, \vec{x} \rangle > 0\},$$

o hemisfério aberto superior, e

$$\mathbb{S}_- = \mathbb{S}_-(\vec{x}) = \{y \in \mathbb{S}^n : \langle y, \vec{x} \rangle < 0\},$$

o hemisfério aberto inferior (com relação ao vetor de direção  $\vec{x}$ ).

Denotemos por  $\sigma = \sigma(\vec{x})$  a involução (reflexão) com relação a  $H$ :

$$\sigma(y) = y - 2\langle y, \vec{x} \rangle \vec{x}.$$

Temos claramente

$$\sigma^2 = \text{Id}.$$

Sendo uma transformação ortogonal,  $\sigma$  conserva a distância (euclídeana assim como geodésica), assim como a medida de Haar sobre a esfera  $\mathbb{S}^n$ . Em particular,  $\sigma$  estabelece um isomorfismo entre os hemisférios  $\mathbb{S}_+$  e  $\mathbb{S}_-$  vistos como espaços métricos com medida.

**Exercício I.3.11.** Mostre que, dado  $y, z \in \mathbb{S}_+$ , temos

$$d_{geo}(y, z) \leq d_{geo}(y, \sigma(z)).$$

[ *Sugestão:* graças à Eq. (I.2), a desigualdade é verdadeira para a distância euclídeana se e somente se ele vale para a distância geodésica, e no último caso basta mostrar o resultado para  $y = e_1$ , o primeiro vetor da base de coordenadas padrão. ]

Para um subconjunto  $A \subseteq \mathbb{S}^n$ , denotemos

$$A_{\pm/0} = A \cap \mathbb{S}_{\pm/0}.$$

A *simetrização de  $A$  com dois pontos* é o conjunto

$$\begin{aligned} A^\dagger &= A_+ \cup A_0 \cup \sigma(A_- \setminus \sigma(A_+)) \cup (A_- \setminus \sigma(A_+)) \\ &= A_+ \cup A_0 \cup \sigma(A_-) \cup (A_- \setminus \sigma(A_+)). \end{aligned}$$

Em outras palavras, os pontos de  $A_+$  sempre ficam onde estão, mas os pontos de  $A_-$  são “empurrados” na direção de  $A_+$ . Um ponto  $y \in A_-$  é permitido ficar onde ele está só no caso onde o ponto  $\sigma(y)$  já está ocupado por um elemento de  $A_+$ . Se  $\sigma(y) \notin A_+$ , então  $y$  é retirado de  $A_-$  e  $\sigma(y)$  é adicionado a  $A_+$ . A expressão “simetrização por dois pontos” não foi muito bem escolhida. É um “deslocamento” na direção  $\vec{x}$ .

É imediato que a simetrização de um conjunto boreliano é boreliano, e que

$$\mu(A^\dagger) = \mu(A).$$

Ademais, temos, usando exercício I.3.11:

**Exercício I.3.12.** Seja  $A$  um subconjunto boreliano da esfera, e seja  $\epsilon > 0$ . Então

$$(A^\dagger)_\epsilon \subseteq (A_\epsilon)^\dagger.$$

(A inclusão não é necessariamente estrita). ▲

Eis um corolário importante:

$$\mu\left((A^\dagger)_\epsilon\right) \leq \mu\left((A_\epsilon)^\dagger\right) = \mu(A_\epsilon). \quad (\text{I.6})$$

### I.3.4 A desigualdade isoperimétrica de Lévy

**Teorema I.3.13** (Paul Lévy, 1922). *Seja  $A$  um sub-conjunto boreliano da esfera  $\mathbb{S}^n$  e seja  $C$  uma calota esférica em  $\mathbb{S}^n$  que tem a mesma medida de Haar:*

$$\nu(C) = \nu(A).$$

Então temos para todo  $\epsilon > 0$

$$\nu(C_\epsilon) \leq \nu(A_\epsilon). \quad (\text{I.7})$$

*Demonstração.* Primeiramente, vamos mostrar que em vez de um conjunto boreliano  $A$ , basta mostrar o resultado para um conjunto fechado, nomeadamente, para a aderência  $\bar{A}$ .

**Exercício I.3.14.** Seja  $A$  um subconjunto de um espaço métrico  $X$ . Mostre que para todo  $\epsilon > 0$ ,

$$A_\epsilon = (\bar{A})_\epsilon.$$

Por conseguinte, para toda medida de probabilidade boreliana  $\mu$  sobre  $X$ , temos

$$\mu(A_\epsilon) = \mu((\bar{A})_\epsilon).$$

▲

Como  $\mu(\bar{A}) \geq \mu(A)$ , assumindo a conclusão do teorema é verdadeira para uma calota  $C'$  da medida  $\mu(\bar{A})$ , concluímos

$$\mu(C_\epsilon) \leq \mu(C'_\epsilon) \leq \mu((\bar{A})_\epsilon) = \mu(A_\epsilon),$$

como desejado.

Denotemos por  $\mathcal{G}$ , como no exercício I.3.9, a família de todos subconjuntos fechados de  $\mathbb{S}^n$  tendo as propriedades

1.  $\mu(B) = \mu(A)$ ,
2. para todo  $\epsilon > 0$ ,  $\mu(B_\epsilon) \leq \mu(A_\epsilon)$ .

Este  $\mathcal{G}$  é um subconjunto fechado e não vazio de  $\mathfrak{F}(\mathbb{S}^n)$ . Escolha uma calota esférica  $C$  em torno de um elemento  $x_0 \in \mathbb{S}^n$  tal que

$$\mu(C) = \mu(A).$$

A nossa tarefa é de mostrar que  $C \in \mathcal{G}$ . Com ajuda do exercício 1.3.10 assim como uma modificação óbvia do exercício 1.3.8, a função  $B \mapsto \mu(B \cap C)$  tem o máximo sobre  $\mathcal{G}$ , digamos atingido no ponto  $B' \in \mathcal{G}$ . Como  $B'$  é fechado, basta mostrar que

$$\overset{\circ}{C} \subseteq B',$$

onde  $\overset{\circ}{C}$  denota o interior de  $C$  na esfera  $\mathbb{S}^n$ .

Suponha o contrário:  $\overset{\circ}{C} \not\subseteq B'$ . Então,  $\mu(\overset{\circ}{C} \setminus B') = \mu(B' \setminus \overset{\circ}{C}) > 0$ . O primeiro conjunto sendo aberto, existem  $z \in \overset{\circ}{C} \setminus B'$  e  $r > 0$  tais que  $U_r(z) \subseteq \overset{\circ}{C} \setminus B'$ . Aqui  $U_r(z)$  denota uma calota esférica aberta de raio  $r$  em torno de  $z$ . Como o conjunto  $B' \setminus \overset{\circ}{C}$  é compacto, ele pode ser coberto com um número finito de bolas abertas  $U_r(y)$ ,  $y \in B' \setminus \overset{\circ}{C}$ . Pelo menos uma delas satisfaz  $\mu(U_r(y) \cap B') > 0$ . Escolha um tal elemento  $y$ .

Definamos

$$\vec{x} = \frac{z - y}{\|z - y\|}.$$

Como  $\|x_0 - z\| < r_C < \|x_0 - y\|$ , um cálculo simples mostra que

$$\langle x_0, z - y \rangle = \langle x_0, z \rangle - \langle x_0, y \rangle > 0,$$

e por conseguinte  $x_0 \in S_+(\vec{x})$ .

Como  $\sigma_{\vec{x}}(y) = z$  e a involução  $\sigma_{\vec{x}}$  é isométrica, a imagem de  $U_r(y)$  por  $\sigma_{\vec{x}}$  é igual a  $U_r(z)$ . Este último conjunto não contém pontos de  $B'$ , logo a simetriação  $B \mapsto B^\dagger$  na direção  $\vec{x}$  vai transferir todos os pontos do conjunto  $U_r(y) \cap B'$  dentro a calota  $U_r(z)$ .

Se  $a \in C_-$ , então  $\sigma(a) \in S_+$  e por conseguinte  $d(x_0, \sigma(a)) \leq d(x_0, a) \leq r(C)$  (exercício 1.3.11), logo  $\sigma(a) \in C_+$ . Concluimos:  $\sigma(C_-) \subseteq C_+$ . Isso significa que para todo  $x \in B \cap \overset{\circ}{C}$ , a imagem de  $x$  pela simetriação ou muda para  $B^\dagger \cap \overset{\circ}{C}$ , ou fica onde ele está. Concluimos:  $\mu(B^\dagger \cap C) \geq \mu(B \cap C) + \mu(U_r(z) \cap B) > \mu(B \cap C)$ , e no mesmo tempo  $B^\dagger \in \mathcal{G}$ , contradizendo a escolha de  $B$ .  $\square$

### 1.3.5 Concentração de medida na esfera euclidiana

**Teorema 1.3.15.** *Seja  $\mathbb{S}^{n+1}$  a esfera euclidiana munida da distância geodésica e a medida de Haar. A função de concentração dessa esfera satisfaz*

$$\alpha(\mathbb{S}^{n+1}, \epsilon) \leq \sqrt{\frac{\pi}{8}} e^{-n\epsilon^2/2}. \quad (1.8)$$



*Demonstração.* É uma consequência imediata da desigualdade isoperimétrica de Lévy (teorema I.3.13), combinada com o lema I.3.2.  $\square$

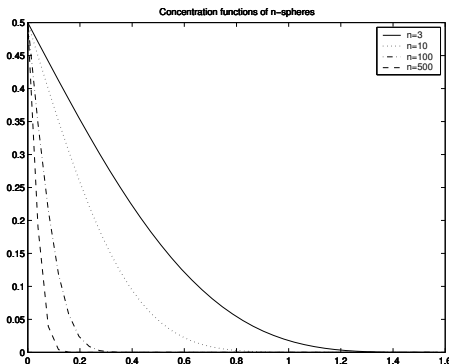


Figura I.11: Funções de concentração de esferas de dimensões  $n = 3, 10, 100, 500$ .

**Corolário I.3.16.** *Seja*

$$f : \mathbb{S}^{n+1} \rightarrow \mathbb{R}$$

*uma função 1-Lipschitz contínua (relativo à distância geodésica). Para todo  $\epsilon > 0$ , temos*

$$\mu\{x \in \mathbb{S}^{n+1} : |f(x) - M_f| > \epsilon\} < \sqrt{\frac{\pi}{2}} e^{-n\epsilon^2/2}.$$

$\square$

*Observação I.3.17.* Como  $d_{eucl} \leq d_{geo}$ , a função de concentração da esfera  $\mathbb{S}^{n+1}$  munida da distância euclídeana admite a mesma cota superior (I.8).  $\blacktriangle$

Na seção 6.2 vamos trabalhar com a esfera  $\mathbb{S}^{n-1}$  do espaço euclídeano  $\ell^2(n)$ , e por isso é mais cómodo extrair do teorema I.3.15 o seguinte.

**Corolário I.3.18.** *Relativo à distância euclídeana,*

$$\alpha(\mathbb{S}^{n-1}, \epsilon) \leq 5 \exp(-\epsilon^2 n/2),$$

*e na região  $\epsilon \leq 1$ , temos uma estimativa melhor:*

$$\alpha(\mathbb{S}^{n-1}, \epsilon) \leq 2 \exp(-\epsilon^2 n/2).$$

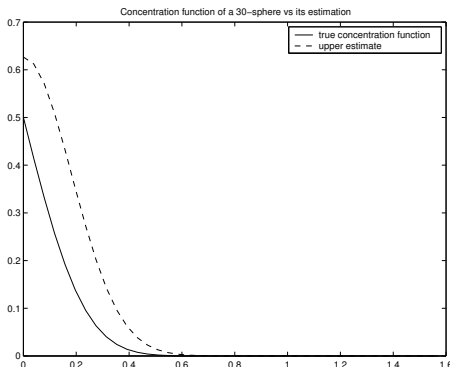


Figura I.12: A função de concentração da esfera de dimensão 30 contra a sua cota superior gaussiana.

*Demonstração.*

$$\begin{aligned} \alpha_{n-1}(\epsilon) &\leq \sqrt{\frac{\pi}{8}} \exp(-\epsilon^2(n-2)/2) \\ &= \sqrt{\frac{\pi}{8}} \cdot \exp(\epsilon^2) \exp(-\epsilon^2 n/2) \\ &< 5 \exp(-\epsilon^2 n/2), \end{aligned}$$

porque se  $\epsilon \leq \sqrt{2}$ , então

$$\sqrt{\frac{\pi}{8}} \cdot \exp(\epsilon^2) \leq \sqrt{\frac{\pi}{8}} \cdot e^2 \approx 4.630404 < 5,$$

e se  $\epsilon \geq \sqrt{2}$ , então a desigualdade é verdadeira pelas razões triviais:  $\alpha_{n-1}(\epsilon) = 0$ . (A distância é euclidiana!) O caso  $\epsilon \leq 1$  é parecido.  $\square$

### I.3.6 Estabilidade por oscilações

**Lema I.3.19.** Para todo subconjunto boreliano,  $A$ , da esfera  $\mathbb{S}^{n-1}$  e  $\xi \in \mathbb{S}^{n-1}$  qualquer, temos

$$\mu(A) = \nu\{u \in O(n) : u\xi \in A\}, \quad (\text{I.9})$$

onde  $\nu$  é a medida de Haar sobre o grupo ortogonal  $O(n)$ .

*Demonstração.* A expressão no lado direito da fórmula (I.9) define uma medida de probabilidade sobre  $\mathbb{S}^{n-1}$ , digamos  $\tilde{\mu}$ , nomeadamente, a imagem direita de  $\nu$  pela aplicação

de órbita. Essa medida é invariante por isometrias:

$$\begin{aligned}
 \tilde{\mu}(vA) &= \nu\{u \in O(n): u\xi \in vA\} \\
 &= \nu\{u \in O(n): v^{-1}u\xi \in A\} \\
 &= \nu(v^{-1} \cdot \{u \in O(n): u\xi \in vA\}) \\
 &= \nu\{u \in O(n): u\xi \in vA\} \\
 &= \tilde{\mu}(A).
 \end{aligned}$$

Por causa da unicidade da medida de Haar sobre a esfera,  $\tilde{\mu}$  deve ser igual a  $\mu$ .  $\square$

O resultado seguinte é uma ferramenta importante da análise funcional geométrica.

**Lema I.3.20.** *Seja  $f: \mathbb{S}^{n-1} \rightarrow \mathbb{R}$  uma função real 1-Lipschitz contínua sobre a esfera  $\mathbb{S}^{n-1}$ , e seja  $0 < \epsilon \leq 1$ . Qual quer seja um subconjunto finito  $F \subseteq \mathbb{S}^{n-1}$  da cardinalidade*

$$|F| < \frac{1}{4} \exp(\epsilon^2 n/2),$$

*existe uma transformação ortogonal  $u \in O(n)$  tal que a função  $f$  tem pequena oscilação sobre a translação  $uF$  de  $F$ :*

$$\forall y \in uF, |f(y) - M_f| < \epsilon.$$

*Demonstração.* Para todo  $x \in F$ , definamos

$$U_x = \{u \in O(n): |f(ux) - M_f| < \epsilon\}.$$

Como

$$\mu\{x \in \mathbb{S}^{n-1}: |f(x) - M_f| < \epsilon\} \geq 1 - 2\alpha_{\mathbb{S}^{n-1}}(\epsilon) > 1 - 4 \exp(-\epsilon^2 n/2),$$

o lema I.3.19 implica que

$$\nu(U_x) \geq 1 - 4 \exp(-\epsilon^2 n/2).$$

Logo, a interseção de todos os conjuntos  $U_x$ ,  $x \in F$  não é vazia por causa da nossa hipótese sobre a cardinalidade de  $F$ . Escolha

$$u \in \bigcap_{x \in F} U_x.$$

Esse  $u$  tem a propriedade desejada.  $\square$

Reformulamos o lema. Para uma função  $f : \mathbb{S}^{n-1} \rightarrow \mathbb{R}$  e uma transformação ortogonal  $u \in O(n)$  defina a função  ${}^u f$ , como antes, por

$${}^u f(x) = f(u^{-1}x).$$

É óbvio que se  $f$  for 1-Lipschitz contínua, então  ${}^u f$  é tal, e além disso,

$$M_{{}^u f} = M_f.$$

Eis uma forma equivalente do lema [I.3.20](#).

**Lema I.3.21.** *Seja  $f : \mathbb{S}^{n-1} \rightarrow \mathbb{R}$  uma função real 1-Lipschitz contínua sobre a esfera  $\mathbb{S}^{n-1}$ , e seja  $\epsilon > 0$ . Qual quer seja um subconjunto finito  $F \subseteq \mathbb{S}^{n-1}$  com*

$$|F| < \frac{1}{4} \exp(\epsilon^2 n/2), \tag{I.10}$$

*existe uma transformação ortogonal  $u \in O(n)$  tendo a propriedade que para todo  $x \in F$ ,*

$$|{}^u f(x) - M_{{}^u f}| < \epsilon.$$

□

### I.3.7 Comentários históricos e sugestões de leitura

Tem provavelmente uma dúzia de várias provas do teorema [I.3.15](#) sobre a concentração de medida sobre as esferas. Historicamente, a primeira prova foi dévida a de Paul Lévy [[Lévy 1922](#)], mesmo se ela só tornou-se matematicamente exata no trabalho de Gromov [[Gromov 1986](#)]. Em particular, o lema [I.3.2](#) foi diretamente emprestado do livro de Lévy (*loc. cit.*), veja também [[Milman e Schechtman 1986](#)], pp. 5-6.

A prova com simetrização, provavelmente a mais simples de todas, foi descoberto por Figiel, Lindenstrauss, e Milman [[Figiel, Lindenstrauss e Milman 1977](#)]. Ela foi simplificada por Benyamini [[Benyamini 1984](#)]. A nossa apresentação segue a de Schechtman [[Schechtman 2003](#)], mas é simplificada mesmo mais, tendo eliminado a necessidade de usar o teorema de densidade de Lebesgue. Desta forma, o argumento torna-se elementar.

Para outras provas da desigualdade de Lévy (ou seja, a cota superior gaussiana no teorema [I.3.15](#)), usando os vários métodos da análise e geometria, veja por exemplo [[Gromov 1986](#)], [[Ledoux 2001](#)], [[Matoušek 2002](#)], [[Pisier 1989](#)], [[Benyamini e Lindenstrauss 2000](#)].

O lema [I.3.20](#), descoberto e explorado por Vitali Milman nos anos 1960 [[Milman 1967](#)], está ligando a análise funcional geométrica, teoria combinatória, e teoria de grupos de transformações. Esta ligação é o assunto principal do livro [[Pestov 2006](#)].

# J

## Teorema Minimax de von Neumann

---

Pensemos de uma medida de probabilidade sobre o espaço boreliano finito  $[n]$  como um  $n$ -vetor,  $p$ , com coordenadas (pesos) não negativas,  $p_i$ , cuja soma é igual a 1.

**Teorema J.0.1** (Teorema Minimax “concreto” de von Neumann (1928)). *Seja  $M$  uma matriz com coeficientes reais, de formato  $m \times n$ . Então,*

$$\max_{p \in P[m]} \min_{q \in P[n]} p^t M q = \min_{q \in P[n]} \max_{p \in P[m]} p^t M q.$$

Primeiramente, notemos que a desigualdade  $\leq$  não é específica ao teorema e seque do resultado geral seguinte.

**Teorema J.0.2** (Desigualdade min-max). *Seja  $f: X \times Y \rightarrow \mathbb{R}$  uma função qualquer. Então*

$$\sup_{x \in X} \inf_{y \in Y} f(x, y) \leq \inf_{y \in Y} \sup_{x \in X} f(x, y).$$

*Demonstração.* A desigualdade simplesmente afirma que cada número real (ou símbolo  $\pm\infty$ ) da forma  $\inf_{y \in Y} f(x, y)$ ,  $x \in X$ , é menor ou igual a cada elemento de  $\mathbb{R} \cup \{\pm\infty\}$  da forma  $\sup_{x \in X} f(x, y)$ ,  $y \in Y$ . Sejam  $x \in X$ ,  $y \in Y$  quaisquer. Temos:

$$\inf_{y' \in Y} f(x, y') \leq f(x, y) \leq \sup_{x' \in X} f(x', y),$$

estabelecendo a afirmação. □

Resta-nos apenas verificar a desigualdade  $\geq$ . Note que o conjunto  $P[n]$  pode se identificar com a envoltória convexa do conjunto dos vetores de base,  $e_1, e_2, \dots, e_n$  (o *simplex* padrão), denotado  $\Delta^n$ .

**Exercício J.0.3.** Seja  $f$  uma função contínua e *convexa* sobre  $\Delta^n$ , ou seja, quaisquer que sejam  $x, y \in \Delta^n$  e  $t, s \in [0, 1]$ ,

$$f(tx + sy) \leq tf(x) + sf(y).$$

Mostre que o máximo de  $f$  sobre  $\Delta^n$  é necessariamente atingido em um vértice  $e_i$ ,  $i = 1, 2, \dots, n$ . Do mesmo jeito, o mínimo de uma função *côncava* é atingido em um vértice.

Segue-se do exercício que o mínimo  $\min_{q \in P[n]} p^t M q$  da função linear  $q \mapsto p^t M q$  sobre  $P(m)$  seja atingido sobre um vetor de base:

$$\begin{aligned} \min_{q \in P[n]} p^t M q &= \min_{j \in [m]} p^t M e_j \\ &= \min_{j \in [m]} p^t M_{*,j}, \end{aligned}$$

onde  $M_{*,j}$  significa o  $j$ -ésima coluna de  $M$ .

Similarmente, o *máximo*  $\max_{p \in P[m]} p^t M q$  da função linear (logo *côncava*)  $p \mapsto p^t M q$  é atingido sobre um vetor de base também:

$$\begin{aligned} \max_{p \in P[m]} p^t M q &= \max_{i \in [m]} e_i^t M q \\ &= \max_{i \in [m]} M_{i,*} q, \end{aligned}$$

onde  $M_{i,*}$  é a  $i$ -ésima linha de  $M$ .

Agora o teorema de Minimax “concreto” pode ser reformulado assim:

$$\max_{p \in P[m]} \min_{j \in [n]} p^t M_{*,j} = \min_{q \in P[n]} \max_{i \in [m]} M_{i,*} q. \quad (\text{J.1})$$

(Note que é exatamente esta forma que usamos na prova do teorema de Moran–Yehudayoff 8.3.21).

**Exercício J.0.4.** Sejam  $C$  um subconjunto compacto e convexo do espaço euclidiano  $\ell^2(n)$ ,  $x \notin C$ . Mostre que  $C$  possui o ponto  $c \in C$  mais próximo de  $x$ :

$$\forall y \in C, y \neq c \Rightarrow \|x - c\| < \|x - y\|.$$

**Lema J.0.5** (Alternativa para matrizes). *Seja  $M$  uma matriz com coeficientes reais, de formato  $m \times n$ . Então, vale uma e apenas uma das duas condições seguintes:*

1. O vetor  $0 \in \mathbb{R}^m$  pertence à envoltória convexa de  $n$  colunas de  $M$  e  $m$  vetores de base de  $\mathbb{R}^m$ .

2. Existe uma medida de probabilidade  $p \in P[m]$  com todos pesos estritamente positivos tal que  $\langle p, A_{*,j} \rangle > 0$  para todos  $j = 1, 2, \dots, n$ .

*Demonstração.* Denote

$$C = \text{conv}(M_{*,1}, \dots, M_{*,n}, e_1, \dots, e_m)$$

e suponha que  $0 \notin C$ . Seja  $c \in C$  o ponto mais próximo de  $x$  em  $C$ . O funcional linear  $\langle -, c \rangle$  toma o valor  $c^2 > 0$  em  $c$ , e para cada  $y \in C$ ,  $y \neq c$ , temos  $\langle c, y \rangle > c^2$ . (Caso contrário, um sub-intervalo não trivial do intervalo  $[c, y] = \{tc + (1-t)y : t \in [0, 1]\} \subseteq C$  pertence à esfera  $S_{c^2}(0)$  pelas razões puremante planimétricas, o que seria uma contradição com a escolha de  $c$ ). Em particular, para todo  $y \in C$ ,  $\langle y, c \rangle > 0$ . Substituindo  $y = e_i \in C$ , concluímos que  $c_i > 0$  para todos  $i$ . Agora basta normalizar  $c$ , definindo a medida de probabilidade  $p = c / \sum_i c_i$ .  $\square$

*Observação J.0.6.* O funcional  $\langle c, - \rangle$  que aparece na prova acima fazendo uma separação entre  $0$  e  $C$  é um caso particular da versão seguinte (não imediatamente óbvia) do teorema de Hahn–Banach F.2.1: seja  $C$  um subconjunto fechado e convexo de um espaço de Banach  $E$ , e seja  $x \notin C$ . Então existe um funcional linear limitado  $\phi \in E^*$  tal que

$$\phi(x) > \sup_{c \in C} \phi(c).$$

Suponha que a possibilidade (1) ocorre no lema J.0.5: existem coeficientes  $\lambda_j \geq 0$ ,  $j = 1, \dots, m+n$ , tais que  $\sum_{j=1}^{m+n} \lambda_j = 1$  e

$$0 = \sum_{j=1}^n \lambda_j A_{*,j} + \sum_{k=1}^m \lambda_{n+k} e_k.$$

É claro que  $\sum_{j=1}^n \lambda_j > 0$ . Por conseguinte,

$$q_j = \left( \sum_{k=1}^n \lambda_k \right)^{-1} \lambda_j, \quad j \in [n]$$

define uma medida de probabilidade,  $q$ , sobre  $[n]$ . Qualquer que seja  $i \in [m]$ , temos

$$\begin{aligned} \langle A_{i,*}, q \rangle &= - \left( \sum_{k=1}^n \lambda_k \right)^{-1} \sum_{k=1}^m \lambda_{n+k} e_k \\ &\leq 0. \end{aligned}$$

Concluímos:

$$\min_{q \in P[n]} \max_{i \in [m]} M_{i,*} q \leq 0.$$

Agora suponha que a possibilidade (2) ocorre. Neste caso, existe  $p \in P[m]$  tal que temos para todos  $j \in [n]$

$$\langle p, A_{*,j} \rangle > 0.$$

Por conseguinte,

$$\max_{p \in P[m]} \min_{j \in [n]} p^t M_{*,j} > 0.$$

Denotemos para simplicidade

$$\begin{aligned} v_{(I)} &= \max_{p \in P[m]} \min_{j \in [n]} p^t M_{*,j} = \max_{p \in P[m]} \min_{q \in P[n]} p^t M q, \\ v_{(II)} &= \min_{q \in P[n]} \max_{i \in [m]} M_{i,*} q = \min_{q \in P[n]} \max_{p \in P[m]} p^t M q. \end{aligned}$$

O nosso argumento acima exclui a possibilidade do que

$$v_{(I)} \leq 0 < v_{(II)}.$$

Denotemos  $J = J_{m \times n}$  uma matriz com todos coeficientes iguais a 1, e seja  $t$  um real qualquer. Formemos uma matriz do mesmo tamanho  $m \times n$ ,

$$B = M + tJ.$$

**Exercício J.0.7.** Verifique que, quaisquer que sejam  $p \in P[m]$ ,  $q \in P[n]$ ,

$$p^t J q = 1.$$

Por conseguinte,

$$p^t B q = p^t M q + t.$$

Nós impossibilizamos o caso onde  $v_{(I)} + t \leq 0 < v_{(II)} + t$ , ou seja,

$$v_{(I)} \leq -t < v_{(II)},$$

qualquer que seja um número real  $t$ . Concluimos:  $v_{(I)} \geq v_{(II)}$ .

A apresentação foi inspirada pela nota [Scarvalone 2008].



# Bibliografia

---

- N. Alon, S. Ben-David, N. Cesa-Bianchi e D. Haussler (1997). “Scale-sensitive dimensions, uniform convergence, and learnability.” *J. ACM* 44.4, pp. 615–631. MR: [1481318](#) (ver p. [75](#)).
- N. Alon e J. H. Spencer (1992). *The probabilistic method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley & Sons, Inc., New York, pp. xvi+254. MR: [1140703](#) (ver p. [45](#)).
- M. Anthony e P. L. Bartlett (1999). *Neural network learning: theoretical foundations*. Cambridge University Press, Cambridge, pp. xiv+389. MR: [1741038](#) (ver pp. [viii](#), [12](#), [55](#), [64](#)).
- S. Artstein-Avidan, A. Giannopoulos e V. D. Milman (2015). *Asymptotic geometric analysis. Part I*. Vol. 202. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, pp. xx+451. MR: [3331351](#) (ver pp. [45](#), [442](#)).
- P. Assouad e T. Quentin de Gromard (2006). “Recouvrements, dérivation des mesures et dimensions”. *Rev. Mat. Iberoamericana* 22.3, pp. 893–953. MR: [2320406](#) (ver p. [184](#)).
- S. Banach e K. Kuratowski (1929). “Sur une généralisation du probleme de la mesure”. *Fundamenta Mathematicae* 14, pp. 127–131 (ver p. [278](#)).
- O. Barkol e Y. Rabani (2002). “Tighter Lower Bounds for Nearest Neighbor Search and Related Problems in the Cell Probe Model.” *J. Comput. Syst. Sci.* 64.4, pp. 873–896. MR: [1912306](#) (ver p. [94](#)).
- P. L. Bartlett e S. Mendelson (2002). “Rademacher and Gaussian Complexities: Risk Bounds and Structural Results.” *Journal of Machine Learning Research* 3, pp. 463–482. MR: [1984026](#) (ver p. [129](#)).
- S. Ben-David e A. Litman (1998). “Combinatorial Variability of Vapnik-Chervonenkis Classes with Applications to Sample Compression Schemes”. *Discrete Applied Mathematics* 86.1, pp. 3–25. MR: [1634863](#) (ver p. [247](#)).
- G. M. Benedek e A. Itai (1991). “Learnability with Respect to Fixed Distributions.” *Theor. Comput. Sci.* 86.2, pp. 377–390. MR: [1122796](#) (ver p. [97](#)).

- Y. Benyamini (1984). “Two-point symmetrization, the isoperimetric inequality on the sphere and some applications”. Em: *Texas functional analysis seminar 1983–1984 (Austin, Tex.)* Longhorn Notes. Univ. Texas Press, Austin, TX, pp. 53–76. MR: [0832231](#) (ver p. [458](#)).
- Y. Benyamini e J. Lindenstrauss (2000). *Geometric nonlinear functional analysis. Vol. 1*. Vol. 48. American Mathematical Society Colloquium Publications. American Mathematical Society, Providence, RI, pp. xii+488. MR: [1727673](#) (ver p. [458](#)).
- K. S. Beyer, J. Goldstein, R. Ramakrishnan e U. Shaft (1999). “When Is ”Nearest Neighbor” Meaningful?” Em: *Database Theory - ICDT '99, 7th International Conference, Jerusalem, Israel, January 10-12, 1999, Proceedings*. Pp. 217–235 (ver p. [192](#)).
- G. Biau, L. Devroye e G. Lugosi (2008). “Consistency of Random Forests and Other Averaging Classifiers.” *Journal of Machine Learning Research* 9, pp. 2015–2033. MR: [2447310](#) (ver p. [8](#)).
- A. Blum, J. Hopcroft e R. Kannan (2016). “[Foundations of Data Science](#)”. Book in preparation (ver p. [12](#)).
- A. Blumer, A. Ehrenfeucht, D. Haussler e M. K. Warmuth (1989). “[Learnability and the Vapnik-Chervonenkis dimension.](#)” *J. ACM* 36.4, pp. 929–965. MR: [1072253](#) (ver pp. [140](#), [142](#)).
- B. Bollobás e A. J. Radcliffe (1995). “[Defect Sauer Results.](#)” *J. Comb. Theory, Ser. A* 72.2, pp. 189–208. MR: [1357769](#) (ver pp. [252](#), [255](#)).
- N. Bourbaki (1974). *Éléments de mathématique. Topologie générale, Chapitres 5 à 10, Deuxième édition*. Hermann, Paris. MR: [0149429](#) (ver p. [404](#)).
- J. Braun e M. Griebel (2009). “[On a constructive proof of Kolmogorov’s superposition theorem](#)”. *Constr. Approx.* 30.3, pp. 653–675. MR: [2558696](#) (ver p. [222](#)).
- P. Bro Miltersen (abr. de 2000). “Cell probe complexity - a survey”. Em: *Proceedings of the 19th Conference on the Foundations of Software Technology and Theoretical Computer Science, 1999. Advances in Data Structures Workshop* (ver p. [94](#)).
- B. Brosowski e F. Deutsch (1981). “[An elementary proof of the Stone-Weierstrass theorem](#)”. *Proc. Amer. Math. Soc.* 81.1, pp. 89–92. MR: [0589143](#) (ver p. [393](#)).
- F. Cérou e A. Guyader (2006). “[Nearest neighbor classification in infinite dimension](#)”. *ESAIM Probab. Stat.* 10, pp. 340–355. MR: [2247925](#) (ver pp. [184](#), [185](#)).
- E. Chavez, G. Navarro, R. A. Baeza-Yates e J. L. Marroquin (2001). “[Searching in metric spaces](#)”. *ACM Computing Surveys* 33.3, pp. 273–321 (ver p. [202](#)).
- T. M. Cover e P. E. Hart (1967). “[Nearest Neighbor Pattern Classification](#)”. *IEEE Transactions on Information Theory* 13.1, pp. 21–27 (ver pp. [149](#), [165](#)).
- M. J. Crawley (dez. de 2012). *The R Book*. Wiley (ver p. [6](#)).
- F. Cucker e S. Smale (2002). “[On the mathematical foundations of learning](#)”. *Bull. Amer. Math. Soc. (N.S.)* 39.1, pp. 1–49. MR: [1864085](#) (ver p. [12](#)).
- F. Cucker e D.-X. Zhou (2007). *Learning theory: an approximation theory viewpoint*. Vol. 24. Cambridge Monographs on Applied and Computational Mathematics. Cambridge University Press, Cambridge, pp. xii+224. MR: [2354721](#) (ver p. [12](#)).

- G. Cybenko (1989). “Approximation by superpositions of a sigmoidal function”. *Mathematics of Control, Signals, and Systems* 2.4, pp. 303–314. MR: [1015670](#) (ver pp. [233](#), [234](#)).
- R. O. Davies (dez. de 1971). “Measures not approximable or not specifiable by means of balls”. *Mathematika* 18.02, p. 157. MR: [0310162](#) (ver p. [173](#)).
- C. J. J. Despres (2014). *The Vapnik-Chervonenkis dimension of cubes in  $\mathbb{R}^d$* . Fall 2014 Honours research project, University of Ottawa, 4 pp. arXiv: [1412.6612](#) (ver p. [55](#)).
- L. Devroye (1981). “On the Almost Everywhere Convergence of Nonparametric Regression Function Estimates”. *Ann. Statist.* 9.6, pp. 1310–1319. MR: [0630113](#) (ver p. [184](#)).
- L. Devroye e L. Györfi (1985). *Nonparametric density estimation. The  $L_1$  view*. Wiley Series in Probability and Mathematical Statistics: Tracts on Probability and Statistics. John Wiley & Sons, Inc., New York, pp. xi+356. MR: [0780746](#) (ver p. [185](#)).
- L. Devroye, L. Györfi, A. Krzyżak e G. Lugosi (1994). “On the strong universal consistency of nearest neighbor regression function estimates”. *Ann. Statist.* 22.3, pp. 1371–1385. MR: [1311980](#) (ver p. [185](#)).
- L. Devroye, L. Györfi e G. Lugosi (1996). *A probabilistic theory of pattern recognition*. Vol. 31. Applications of Mathematics (New York). Springer-Verlag, New York, pp. xvi+636. MR: [1383093](#) (ver pp. [12](#), [172](#)).
- H. H. Duan (2014). *Applying Supervised Learning Algorithms and a New Feature Selection Method to Predict Coronary Artery Disease*. M.Sc. thesis, University of Ottawa, 2014, 102 pp. arXiv: [1402.0459](#) (ver p. [172](#)).
- H. H. Duan, G. Giordano, S. Hatko e V. Pestov (s.d.). *2013 Cybersecurity Data Mining Competition Methods overview*. 8 pp. (ver p. [218](#)).
- R. M. Dudley (2014). *Uniform central limit theorems*. Second. Vol. 142. Cambridge Studies in Advanced Mathematics. Cambridge University Press, New York, pp. xii+472. MR: [3445285](#) (ver p. [12](#)).
- M. Durst e R. M. Dudley (1980). “Empirical processes, Vapnik-Chervonenkis classes and Poisson processes”. *Probab. Math. Statist.* 1.2, 109–115 (1981). MR: [0626305](#) (ver p. [141](#)).
- R. Engelking (1989). *General topology*. Second. Vol. 6. Sigma Series in Pure Mathematics. Heldermann Verlag, Berlin, pp. viii+529. MR: [1039321](#) (ver p. [151](#)).
- T. Figiel, J. Lindenstrauss e V. D. Milman (1977). “The dimension of almost spherical sections of convex bodies”. *Acta Math.* 139.1-2, pp. 53–94. MR: [0445274](#) (ver p. [458](#)).
- S. Floyd e M. K. Warmuth (1995). “Sample Compression, Learnability, and the Vapnik-Chervonenkis Dimension.” *Machine Learning* 21.3, pp. 269–304 (ver pp. [247](#), [249](#)).
- R. Fraiman, A. Justel e M. Svarc (2010). “Pattern recognition via projection-based  $k$ NN rules”. *Comput. Statist. Data Anal.* 54.5, pp. 1390–1403. MR: [2600840](#) (ver p. [213](#)).
- P. Frankl e Z. Füredi (1981). “A short proof for a theorem of Harper about Hamming-spheres”. *Discrete Math.* 34.3, pp. 311–313. MR: [0613409](#) (ver p. [24](#)).
- C. Freiling (1986). “Axioms of symmetry: throwing darts at the real number line”. *J. Symbolic Logic* 51.1, pp. 190–200. MR: [0830085](#) (ver p. [142](#)).
- F. Giroso e T. A. Poggio (1989). “Representation Properties of Networks: Kolmogorov’s Theorem Is Irrelevant.” *Neural Computation* 1.4, pp. 465–469 (ver p. [222](#)).

- P. Goldberg e M. Jerrum (1995). “Bounding the Vapnik–Chervonenkis dimension of concept classes parametrized by real numbers”. *Machine Learning* 18, pp. 131–148 (ver p. 205).
- M. Gromov (1986). *Isoperimetric inequalities in Riemannian manifolds. Appendix I in Milman e Schechtman 1986* (ver p. 458).
- M. Gromov (1998). “Possible trends in mathematics in the coming decades”. *Notices Amer. Math. Soc.* 45.7, pp. 846–847. MR: [1850687](#) (ver p. xi).
- M. Gromov (1999). *Metric structures for Riemannian and non-Riemannian spaces*. Vol. 152. Progress in Mathematics. Based on the 1981 French original [MR0682063 (85e:53051)], With appendices by M. Katz, P. Pansu and S. Semmes, Translated from the French by Sean Michael Bates. Birkhäuser Boston, Inc., Boston, MA, pp. xx+585. MR: [1699320](#) (ver pp. 197, 442).
- I. Guyon, M. Nikravesh, S. Gunn e L. A. Zadeh, ed. (2006). *Feature Extraction, Foundations and Applications*. Springer Berlin Heidelberg (ver p. 187).
- T. Hanika, F. M. Schneider e G. Stumme (2018). *Intrinsic Dimension of Geometric Data Sets*. 28 pp. arXiv: [1801.07985](#) (ver p. 201).
- S. Hatko (2013). *Borel Isomorphic Dimensionality Reduction of Data and Supervised Learning*. Honours research project, University of Ottawa. arXiv: [1307.8333](#) (ver p. 218).
- (2015). *k-Nearest Neighbour Classification of Datasets with a Family of Distances*. M.Sc. thesis, University of Ottawa. arXiv: [1512.00001](#) (ver p. 185).
- A. Hefeç e M. L. T. Villela (2017). *Códigos Corretores de Erros*. 2a edição, 206 páginas. IMPA, Rio de Janeiro (ver p. 15).
- K. H. Hofmann e S. A. Morris (2013). *The structure of compact groups*. Vol. 25. De Gruyter Studies in Mathematics. Third edition. De Gruyter, Berlin, pp. xxii+924. MR: [3114697](#) (ver p. 71).
- K. Hornik (1991). “Approximation capabilities of multilayer feedforward networks”. *Neural Networks* 4.2, pp. 251–257 (ver p. 235).
- R. Hecht-Nielsen (1987). “Kolmogorov’s Mapping Neural Network Existence Theorem”. Em: *Proceedings of the IEEE First International Conference on Neural Networks* (San Diego, CA). Vol. III. Piscataway, NJ: IEEE, pp. 11–13 (ver p. 221).
- B. Igel'nik (2003). “Use of the Kolmogorov’s Superposition Theorem and Cubic Splines for Efficient Neural-Network Modeling”. Em: *Knowledge-Based Intelligent Information and Engineering Systems, 7th International Conference, KES 2003, Oxford, UK, September 3-5, 2003, Proceedings, Part I*, pp. 184–190 (ver p. 222).
- P. Indyk (2004). “Nearest Neighbors in High-Dimensional Spaces”. Em: *Handbook of Discrete and Computational Geometry, Second Edition*. Pp. 877–892 (ver pp. 94, 195).
- W. B. Johnson e J. Lindenstrauss (1984). “Extensions of Lipschitz mappings into a Hilbert space”. Em: *Conference in modern analysis and probability (New Haven, Conn., 1982)*. Vol. 26. Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 189–206. MR: [0737400](#) (ver p. 212).

- J.-P. Kahane (1975). “[Sur le théorème de superposition de Kolmogorov](#)”. *J. Approximation Theory* 13. Collection of articles dedicated to G. G. Lorentz on the occasion of his sixty-fifth birthday, III, pp. 229–234. MR: [0372134](#) (ver p. [222](#)).
- D. Kalajdziewski (2012). *[Measurability Aspects of the Compactness Theorem for Sample Compression Schemes](#)*. M.Sc. thesis, University of Ottawa, 64 pp., 2012. arXiv: [1205.5819](#) (ver pp. [243](#), [248](#)).
- M. J. Kearns e U. Vazirani (1994). *An Introduction to Computational Learning Theory*. The MIT Press. MR: [1331838](#) (ver p. [59](#)).
- A. S. Kechris (1995). *Classical descriptive set theory*. Vol. 156. Graduate Texts in Mathematics. Springer-Verlag, New York, pp. xviii+402. MR: [1321597](#) (ver p. [355](#)).
- A. Klenke (2014). *Probability theory. A comprehensive course*. German. Universitext. Springer, London, pp. xii+638. MR: [3112259](#) (ver p. [412](#)).
- A. N. Kolmogorov (1963). “On the representation of continuous functions of many variables by superposition of continuous functions of one variable and addition”. *Amer. Math. Soc. Transl. (2)* 28, pp. 55–59. MR: [0153799](#) (ver p. [221](#)).
- V. Koltchinskii e D. Panchenko (2000). “Rademacher processes and bounding the risk of function learning”. Em: *High dimensional probability, II (Seattle, WA, 1999)*. Vol. 47. Progr. Probab. Birkhäuser Boston, Boston, MA, pp. 443–457. MR: [1857339](#) (ver p. [129](#)).
- S. Kumari (2018). “[Topics in Random Matrices and Statistical Machine Learning](#)”. 125 pages. Tese de dout. Kyoto University. arXiv: [1807.09419](#) (ver pp. [184](#), [185](#)).
- V. Kurková (1991). “[Kolmogorov’s Theorem Is Relevant](#)”. *Neural Computation* 3.4, pp. 617–622 (ver p. [222](#)).
- E. Kushilevitz, R. Ostrovsky e Y. Rabani (2000). “[Efficient Search for Approximate Nearest Neighbor in High Dimensional Spaces](#)”. *SIAM J. Comput.* 30.2, pp. 457–474. MR: [1769366](#) (ver p. [94](#)).
- D. Kuzmin e M. K. Warmuth (2007). “Unlabeled Compression Schemes for Maximum Classes”. *Journal of Machine Learning Research* 8, pp. 2047–2081. MR: [2353827](#) (ver pp. [248](#), [250](#)).
- M. Ledoux (2001). *The concentration of measure phenomenon*. Vol. 89. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, pp. x+181. MR: [1849347](#) (ver pp. [45](#), [442](#), [458](#)).
- P. Lévy (1922). *Leçons d’analyse fonctionnelle*. Gauthier-Villars, Paris (ver p. [458](#)).
- N. Littlestone e M. K. Warmuth (jun. de 1986). “[Relating Data Compression and Learnability](#)”. Unpublished manuscript (ver pp. [243](#), [266](#), [267](#)).
- P. A. Loeb (1975). “[Conversion from nonstandard to standard measure spaces and applications in probability theory](#)”. *Trans. Amer. Math. Soc.* 211, pp. 113–122. MR: [0390154](#) (ver p. [152](#)).
- G. G. Lorentz (1976). “The 13th problem of Hilbert”. Em: *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Vol. XXVIII, Northern Illinois Univ., De Kalb, Ill., 1974)*. Amer. Math. Soc., Providence, R.I., pp. 419–430. MR: [0507425](#) (ver pp. [221](#), [222](#)).

- U. von Luxburg, O. Bousquet e B. Schölkopf (2003/04). “A compression approach to support vector model selection”. *J. Mach. Learn. Res.* 5, pp. 293–323. MR: [2247982](#) (ver p. [251](#)).
- J. Maindonald (2008). *Using R for Data Analysis and Graphics. Introduction, Code and Commentary* (ver p. [6](#)).
- R. Mansuy (jun. de 2009). “The Origins of the Word “Martingale””. *Journal Électronique d’Histoire des Probabilités e de la Statistique* 5.1. 10 pp. MR: [2520661](#) (ver p. [34](#)).
- J. Matoušek (2002). *Lectures on discrete geometry*. Vol. 212. Graduate Texts in Mathematics. Springer-Verlag, New York, pp. xvi+481. MR: [1899299](#) (ver pp. [45](#), [458](#)).
- (2008). “On variants of the Johnson-Lindenstrauss lemma”. *Random Structures Algorithms* 33.2, pp. 142–156. MR: [2436844](#) (ver p. [212](#)).
- S. Mendelson (2002). “A Few Notes on Statistical Learning Theory.” Em: *Machine Learning Summer School*. Ed. por S. Mendelson e A. J. Smola. Vol. 2600. Lecture Notes in Computer Science. Springer, pp. 1–40 (ver pp. [viii](#), [129](#)).
- V. D. Milman (1967). “The infinite dimensional geometry of the unit sphere of a Banach space”. *Dokl. Akad. Nauk SSSR* 177, pp. 514–517. MR: [0241953](#) (ver p. [458](#)).
- V. D. Milman e G. Schechtman (1986). *Asymptotic theory of finite-dimensional normed spaces*. Vol. 1200. Lecture Notes in Mathematics. With an appendix by M. Gromov. Springer-Verlag, Berlin, pp. viii+156. MR: [0856576](#) (ver pp. [45](#), [442](#), [458](#), [466](#)).
- S. Moran e M. K. Warmuth (2016). “Labeled Compression Schemes for Extremal Classes”. Em: *Algorithmic Learning Theory - 27th International Conference, ALT 2016, Bari, Italy, October 19-21, 2016, Proceedings*, pp. 34–49 (ver pp. [249](#), [258](#)).
- S. Moran e A. Yehudayoff (2016). “Sample Compression Schemes for VC Classes”. *J. ACM* 63.3, 21:1–21:10. MR: [3549531](#) (ver pp. [244](#), [258](#), [267](#)).
- D. Mumford (2000). “The dawning of the age of stochasticity”. Em: *Mathematics: frontiers and perspectives*. Amer. Math. Soc., Providence, RI, pp. 197–218. MR: [1754778](#) (ver pp. [145](#), [275](#)).
- A. Naor (2018). *Metric dimension reduction: A snapshot of the Ribe program*. Also Naor’s 2018 plenary ICM [lecture](#). arXiv: [1809.02376](#) (ver pp. [212](#), [213](#)).
- P. A. Ostrand (1965). “A conjecture of J. Nagata on dimension and metrization”. *Bull. Amer. Math. Soc.* 71, pp. 623–625. MR: [0177392](#) (ver p. [178](#)).
- W. Owen (2010). *The R Guide* (ver p. [6](#)).
- A. Pajor (1985). *Sous-espaces  $l_1^n$  des espaces de Banach*. Vol. 16. Travaux en Cours. Hermann, Paris, pp. xii+112. MR: [0903247](#) (ver p. [56](#)).
- M. Patrascu e M. Thorup (2009). “Higher Lower Bounds for Near-Neighbor and Further Rich Problems”. *SIAM J. Comput.* 39.2, pp. 730–741. MR: [2529777](#) (ver p. [94](#)).
- V. Pestov (2006). *Dynamics of infinite-dimensional groups*. Vol. 40. University Lecture Series. The Ramsey-Dvoretzky-Milman phenomenon, Revised edition of *Dynamics of infinite-dimensional groups and Ramsey-type phenomena* [IMPA, Rio de Janeiro, 2005]. American Mathematical Society, Providence, RI, pp. viii+192. MR: [2277969](#) (ver p. [458](#)).
- (2007). “Intrinsic dimension of a dataset: what properties does one expect?” Em: *Proceedings of the International Joint Conference on Neural Networks, IJCNN 2007, Ce-*

- celebrating 20 years of neural networks, Orlando, Florida, USA, August 12-17, 2007, pp. 2959–2964 (ver p. 201).
- (2008). “An axiomatic approach to intrinsic dimension of a dataset”. *Neural Networks* 21.2-3, pp. 204–213 (ver p. 201).
  - (2010). “A Note on Sample Complexity of Learning Binary Output Neural Networks under Fixed Input Distributions.” Em: *SBRN*. Ed. por T. B. Ludermir, K. Figueiredo e C. E. Thomaz. IEEE Computer Society, pp. 7–12 (ver p. 101).
  - (2011). “PAC learnability versus VC dimension: A footnote to a basic result of statistical learning”. Em: *The 2011 International Joint Conference on Neural Networks, IJCNN 2011, San Jose, California, USA, July 31 - August 5, 2011*, pp. 1141–1145 (ver p. 147).
  - (2012). “Indexability, concentration, and VC theory”. *J. Discrete Algorithms* 13, pp. 2–18. MR: 2916047 (ver pp. 94, 203).
  - (2013a). “Is the  $k$ -NN classifier in high dimensions affected by the curse of dimensionality?” *Comput. Math. Appl.* 65.10, pp. 1427–1437. MR: 3061714 (ver p. 217).
  - (2013b). “Lower bounds on performance of metric tree indexing schemes for exact similarity search in high dimensions”. *Algorithmica* 66.2, pp. 310–328. MR: 3028642 (ver pp. 94, 203).
  - (2013c). “PAC learnability under non-atomic measures: a problem by Vidyasagar”. *Theoret. Comput. Sci.* 473, pp. 29–45. MR: 3015337 (ver p. 141).
- V. Pestov e A. Stojmirović (2006). “Indexing schemes for similarity search: an illustrated paradigm”. *Fund. Inform.* 70.4, pp. 367–385. MR: 2246980 (ver pp. 186, 202).
- G. Pisier (1989). *The volume of convex bodies and Banach space geometry*. Vol. 94. Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, pp. xvi+250. MR: 1036275 (ver p. 458).
- D. Preiss (1979). “Invalid Vitali theorems”. Em: *Proc. Seventh Winter School in Abstract Analysis (Prague, 1979)*. Institute of Mathematics of the Academy of Sciences of the Czech Republic, pp. 58–60 (ver p. 176).
- (1981). “Gaussian measures and the density theorem”. *Comment. Math. Univ. Carolin.* 22.1, pp. 181–193. MR: 0609946 (ver p. 177).
  - (1983). “Dimension of metrics and differentiation of measures”. Em: *General topology and its relations to modern analysis and algebra, V (Prague, 1981)*. Vol. 3. Sigma Ser. Pure Math. Heldermann, Berlin, pp. 565–568. MR: 0698459 (ver pp. 184, 185).
- H. Samet (ago. de 2006). *Foundations of Multidimensional and Metric Data Structures (The Morgan Kaufmann Series in Computer Graphics)*. Morgan Kaufmann (ver p. 202).
- S. Santini (set. de 2001). *Exploratory Image Databases: Content-Based Retrieval (Communications, Networking and Multimedia)*. Academic Press (ver p. 202).
- N. Sauer (1972). “On the density of families of sets”. *J. Combinatorial Theory Ser. A* 13, pp. 145–147. MR: 0307902 (ver pp. 55, 252).
- M. Scarvalone (2008). *Game theory and the Minimax theorem*. University of Chicago VIGRE undergraduate project, 5 pp. (Ver p. 462).

- G. Schechtman (2003). “Concentration results and applications”. Em: *Handbook of the geometry of Banach spaces, Vol. 2*. North-Holland, Amsterdam, pp. 1603–1634. MR: [1999604](#) (ver pp. [45](#), [458](#)).
- S. Shalev-Shwartz e S. Ben-David (2014). *Understanding Machine Learning: From Theory to Algorithms*. Cambridge University Press (ver p. [12](#)).
- C. E. Shannon (1948). “A mathematical theory of communication”. *Bell System Tech. J.* 27, pp. 379–423, 623–656. MR: [0026286](#) (ver p. [66](#)).
- S. Shelah (1972). “A combinatorial problem; stability and order for models and theories in infinitary languages”. *Pacific J. Math.* 41, pp. 247–261. MR: [0307903](#) (ver p. [55](#)).
- T. Shioya (2016). *Metric measure geometry*. Vol. 25. IRMA Lectures in Mathematics and Theoretical Physics. Gromov’s theory of convergence and concentration of metrics and measures. EMS Publishing House, Zürich, pp. xi+182. MR: [3445278](#) (ver p. [198](#)).
- J. Song, H. Takakura e Y. Kwon (jul. de 2008). “A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts”. Em: *2008 International Symposium on Applications and the Internet*. IEEE (ver p. [3](#)).
- E. D. Sontag (1992). “Feedforward Nets for Interpolation and Classification.” *J. Comput. Syst. Sci.* 45.1, pp. 20–48. MR: [1170916](#) (ver p. [70](#)).
- Y. Sternfeld (1985). “Dimension, superposition of functions and separation of points, in compact metric spaces”. *Israel J. Math.* 50.1-2, pp. 13–53. MR: [0788068](#) (ver p. [227](#)).
- C. J. Stone (1977). “Consistent nonparametric regression”. *Ann. Statist.* 5.4, pp. 595–645. MR: [0443204](#) (ver p. [8](#)).
- M. Talagrand (1984). “Solution du problème de Glivenko-Cantelli”. *C. R. Acad. Sci. Paris Sér. I Math.* 298.9, pp. 213–216. MR: [0741098](#) (ver p. [129](#)).
- (1996). “The Glivenko-Cantelli problem, ten years later”. *J. Theoret. Probab.* 9.2, pp. 371–384. MR: [1385403](#) (ver p. [129](#)).
- L. Torgo (2010). *Data Mining with R: Learning with Case Studies (Chapman & Hall/CRC Data Mining and Knowledge Discovery Series)*. Chapman e Hall/CRC. MR: [2779331](#) (ver p. [12](#)).
- L. Valiant (1984). “A Theory of the Learnable”. *Communications of the ACM* 27.11, pp. 1134–1142 (ver p. [86](#)).
- V. N. Vapnik e A. J. Červonenkis (1971). “The uniform convergence of frequencies of the appearance of events to their probabilities”. *Teor. Veroyatnost. i Primenen.* 16, pp. 264–279. MR: [0288823](#) (ver pp. [55](#), [129](#), [140](#)).
- V. N. Vapnik (1998). *Statistical learning theory*. Adaptive and Learning Systems for Signal Processing, Communications, and Control. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, pp. xxvi+736. MR: [1641250](#) (ver p. [235](#)).
- (2000). *The nature of statistical learning theory*. Second. Statistics for Engineering and Information Science. Springer-Verlag, New York, pp. xx+314. MR: [1719582](#) (ver pp. [x](#), [12](#)).
- S. S. Vempala (2004). *The random projection method*. Vol. 65. DIMACS Series in Discrete Mathematics and Theoretical Computer Science. American Mathematical Society, Providence, RI, pp. x+105. MR: [2073630](#) (ver p. [212](#)).



- R. Vershynin (2018). *High-dimensional probability*. Vol. 47. Cambridge Series in Statistical and Probabilistic Mathematics. An introduction with applications in data science, With a foreword by Sara van de Geer. Cambridge University Press, Cambridge, pp. xiv+284. MR: [3837109](#) (ver p. [442](#)).
- M. Vidyasagar (2003). *Learning and generalization. With applications to neural networks*. Second. Communications and Control Engineering Series. Springer-Verlag London, Ltd., London, pp. xxii+488. MR: [1938842](#) (ver pp. [12](#), [141](#)).
- D. V. Voiculescu, K. J. Dykema e A. Nica (1992). *Free random variables*. Vol. 1. CRM Monograph Series. American Mathematical Society, Providence, RI, pp. vi+70. MR: [1217253](#) (ver p. [375](#)).
- K. Q. Weinberger e L. K. Saul (2009). “Distance Metric Learning for Large Margin Nearest Neighbor Classification”. *Journal of Machine Learning Research* 10, pp. 207–244 (ver p. [185](#)).
- J. D. Weston (1957). “A short proof of Zorn’s lemma”. *Arch. Math. (Basel)* 8, p. 279. MR: [0092743](#) (ver p. [296](#)).
- B. H. Yandell (2002). *The honors class. Hilbert’s problems and their solvers*. A K Peters, Ltd., Natick, MA, pp. x+486. MR: [1880187](#) (ver p. [220](#)).
- P. N. Yianilos (1993). “Data structures and algorithms for nearest neighbor search in general metric spaces”. Em: *Proceedings of the Fourth Annual ACM-SIAM Symposium on Discrete Algorithms (Austin, TX, 1993)*. ACM, New York, pp. 311–321. MR: [1213243](#) (ver p. [202](#)).
- P. Zezula, G. Amato, V. Dohnal e M. Batko (2006). *Similarity Search: The Metric Space Approach*. Springer Science + Business Media, New York, p. 220 (ver p. [202](#)).
- L. C. Zhao (1987). “Exponential bounds of mean error for the nearest neighbor estimates of regression functions”. *J. Multivariate Anal.* 21.1, pp. 168–178. MR: [0877849](#) (ver p. [185](#)).
- Z.-H. Zhou (2012). *Ensemble Methods: Foundations and Algorithms*. Chapman & Hall/Crc Machine Learning & Pattern Recognition. Chapman e Hall/CRC. MR: [3184068](#) (ver p. [61](#)).

# Índice Remissivo

---

- $\aleph_0$ , 285
- aplicação
  - de compressão amostral, 242
  - de descompressão amostral, 241
- aprendiz, 82
- aprendizagem ensemble, 61
- Axioma da Escolha (AC), 294
- bola
  - aberta, 14
  - de Hamming, 24
  - fechada, 15
- bondade de ajuste empírica, 113
- c, 285
- caminho
  - amostral, 150
- campo de conjuntos, 357
- cardinal
  - mensurável, 151
- cardinalidade, 285
- carga de trabalho de semelhança, 189
- $\mathcal{C}^D$ , 256
- $\mathcal{C}_H$ , 242
- classe
  - consistentemente aprendizável, 100
  - de Glivenko–Cantelli, 91, 106
  - dual, 259
  - extremal, 252
  - filtrada, 238
  - maximal, 249
  - máxima, 249
  - PAC aprendizável, 86
  - universalmente
    - densa, 145
    - separável, 145
- classificador
  - de Bayes, 162
  - $k$ -NN, 166
    - exemplo de Davis, 173
    - exemplo de Preiss, 176
- cobertura, 30
- coeficiente
  - de fragmentação, 56
  - médio, 132
- completude de Dedekind, 306
- complexidade
  - amostral, 83, 266
  - de Rademacher, 114
    - empírica, 114
- compressão

- para baixo, 252
- conceito, 84
- confiança, 79
- conjunto
  - cilíndrico, 357
  - de Cantor, 153
  - fortemente fragmentado, 251
  - indutivo, 296
  - $\mu$ -mensurável, 362
  - negligenciável, 368
- constante
  - de Lipschitz, 18
- consulta de intervalo, 189
- convergência
  - em probabilidade, 379
  - quase certa, 152, 379
  - uniforme de medidas empíricas, 106
- cubo
  - de conceitos, 251
  - de Hamming, 13
  - de Rademacher, 108
- desempate, 165
- desigualdade
  - de Azuma, 36
  - de contração de Ledoux–Talagrand, 123
  - de Euler, 22
  - de Jensen, 119
  - de Markov, 29
  - isoperimétrica
    - de Harper, 24
    - de Lévy, 453
  - min-max, 459
- diferenças de martingale, 35
- diferença simétrica, 82
- dimensão
  - de Nagata, 177, 181
  - sigma-finita, 181
  - de Vapnik–Chervonenkis, 48
  - de intervalos, 49
  - de paralelepípedos, 51
  - de retângulos, 50
  - de semi-espacos, 54
  - de semi-planos, 49
  - dual, 259
- $\dim_{Nag}^S$ , 177
- distância
  - de caminho, 257
  - de Gromov, 197
  - de Hamming, 14
    - normalizada, 14
  - de Hausdorff, 450
  - geodésica, 157
- diâmetro
  - de espaço métrico, 14
  - observável, 435
- empates, 180
- entropia, 65
  - métrica, 131
  - empírica, 131
- envoltória convexa, 121
- erro
  - de Bayes, 162
  - de classificação, 161
  - de generalização, 82
  - empírico, 92
- erro de generalização, 84
- espaço
  - boreliano, 279
  - padrão, 281, 350
- $c_0$ , 174
- de Banach, 385
- de Cantor, 174, 176
- de estados
  - da unidade computacional, 58
  - de uma rede, 62
- metricamente homogêneo, 15
- métrico, 312
  - compacto, 337
  - precompacto, 87
  - separável, 322
  - totalmente limitado, 87
- normado, 383
- probabilístico, 279

- finito, 65
  - padrão, 282
  - pseudométrico, 95
- espaço métrico
  - completo, 332
  - precompacto, 340
- esperança, 409
  - condicional, 32
  - empírica, 91
- esquema
  - de compressão amostral, 242
  - com informação adicional, 267
  - rotulado, 250
  - de indexação, 189, 202
- estabilidade por oscilações, 457
- estado
  - de perceptron, 58
- $\mathbb{E}X$ , 409
- família
  - centrada, 300
  - de Lévy, 41, 440
  - normal, 41, 441
  - de Rademacher, 88
  - uniformemente equicontínua, 155
- $f_*(\mu)$ , 280
- fat shattering dimension, 75
- $\text{fat}_\epsilon(\mathcal{F})$ , 75
- fenômeno de concentração de medida, 40, 439
- fronteira de um conjunto, 152
- função
  - boreliana, 280
  - caraterística, 231, 410
  - convexa, 36
  - de concentração, 41, 441
  - de dimensão intrínseca, 199
  - de regressão, 160
  - Lipschitz contínua, 18, 327
  - semicontínua superiormente, 451
  - uniformemente contínua, 343
- grafo
  - conexo, 257
- de 1-inclusão, 256
  - dirigido, 61
- grau
  - de entrada, 61
  - de saída, 61
- grupo, 400
  - ortogonal, 443
  - simétrico, 27
- hipótese, 84
- Hipótese do Contínuo (CH), 295
- imagem direta de medida, 280
- independência de variáveis aleatórias, 374
- instabilidade da busca, 192
- integral de Lebesgue, 405
- isometria, 15
- isomorfismo
  - boreliano, 282
- jeito
  - de condicionamento, 428
- $L^1(\mu)$ , 408
- lei dos grandes números
  - forte, 381
  - fraca, 39
  - geométrica, 39, 89
- lema
  - de Borel–Cantelli, primeira, 382
  - de Borel–Cantelli, segunda, 381
  - de Cover–Hart, 149, 165
  - de Doob, 422
  - de Dudley de separação, 260
  - de Fekete, 130
  - de Fremlin, 136
  - de Johnson–Lindenstrauss, 205
  - de Kronecker, 71, 403
  - de Sauer–Shelah, 55
  - de Zorn, 296
  - geométrico de Stone, 157, 170, 178
- maldição de dimensionalidade, 187
- martingale, 34

- medida
  - de contagem, 21
  - normalizada, 27
  - de Haar, 367, 444
  - de Lebesgue, 367
  - de probabilidade
    - boreliana, 279
  - de semelhança, 152
  - empírica, 89
  - gaussiana, 283
  - puramente atômica, 280
- métrica, 14
  - não arquimediana, 178
- $[n]$ , 27
- nó
  - de entrada, 62
  - de saída, 62
- número
  - de cobertura, 96
  - de empacotamento, 97
- $\Omega(n)$ , 193
- $\omega(n)$ , 193
- $O(n)$ , 193
- ordem
  - boa, 289
  - parcial, 288
  - total, 288
- P-dimensão, 74
- paradoxo
  - de Freiling, 144
  - do espaço vazio, 191
- partição, 31
- perceptron, 58, 63
- permutações, 289
- pesos
  - de perceptron, 63
- ponto de consulta, 189
- princípio
  - da boa ordem, 300
  - de minimização
    - de erro empírico, 128
    - de risco estrutural, 239
- professor, 82
- pré-ordem, 289
- pseudodimensão, 74
- pseudofragmentação, 74
- pseudométrica, 86, 95
- $P(X)$ , 419
- $\mathbb{R}$ , 307
- reais racionalmente independentes, 70, 402
- realização de uma variável aleatória, 281, 374
- rede
  - de Sontag, 73
  - de unidades de computação, 62
  - sem realimentação, 62
    - com valor limiar linear, 63
- redução
  - de dimensionalidade, 187
    - boreliana, 217
  - de uma classe, 256
- regra
  - consistente, 163
  - consistente com uma classe, 83, 100
  - de aprendizagem, 83, 84
    - inteligente, 172
  - de histograma, 60
  - de minimização de erro empírico, 98
  - provavelmente aproximadamente correta (PAC), 86
  - universalmente consistente, 163
- risco, 79
- $r_{k-\text{NN}}^{\Sigma^n}$ , 164
- sequência
  - subaditiva, 130
  - submultiplicativa, 130
- $\Sigma^n$ , 13
- sigma-álgebra, 357
- simetrização
  - por dois pontos, 452
  - por transposições, 158
- $S_n$ , 289, 400
- sobreajustamento, 117

- subconjunto
  - fragmentado, 47
  - precompacto, 96
  - relativamente compacto, 96
  - totalmente limitado, 96
- subgráfico, 74
- suporte
  - da medida, 150
- tamanho característico, 195, 439
- taxa
  - de aprendizagem, 101
- teorema
  - da categoria de Baire, 346–348
  - da superposição
    - de Kolmogorov, 221
    - de Kolmogorov–Lorentz, 221
    - versão de Kahane, 225
  - de Banach–Alaoglu, 417
  - de Benedek–Itai, 97
  - de Bollobás–Radcliffe, 255
  - de Cantor–Bernstein, 285
  - de Carathéodory, 360, 367
  - de Charles Stone, 170
  - de compacidade, 247
  - de convergência de martingales, 421, 422
  - de convergência dominada, 409
  - de Cramér–Wold, 230
  - de Cybenko, 230, 233
  - de desintegração de medidas, 428
  - de Dudley, 264
  - de Fubini, 431
  - de Hahn–Banach, 388, 414
  - de Hall–Rado, 444
  - de Helly, 55
  - de interserção de Cantor, 311
  - de isomorfismo boreliano, 350
  - de Littlestone–Warmuth, 244, 267
  - de Luzin, 378
  - de Moran–Warmuth, 258
  - de Moran–Yehudayoff, 267
  - de Pajor, 56
  - de Radon–Nikodým, 425
  - de Riesz, 413
  - de Stone–Weierstrass, 392
  - Minimax, 459
- testemunha
  - de fragmentação, 75
  - de irregularidade, 133
- teto, 30
- $\lceil x \rceil$ , 30
- $\Theta(n)$ , 193
- topologia
  - fraca\*, 417
  - produto, 328
- ultrafiltro, 301
- unidade computacional, 58
- valor
  - limiar de perceptron, 58
  - mediano, 29, 441
- variância, 207
- VC-dim( $\mathcal{C}$ ), 48
- VC-dim\*, 260
- árvore de decisão, 60

## **Títulos Publicados — 32º Colóquio Brasileiro de Matemática**

**Emergence of Chaotic Dynamics from Singularities** – *Pablo G. Barrientos, Santiago Ibáñez, Alexandre A. Rodrigues e J. Ángel Rodríguez*

**Nonlinear Dispersive Equations on Star Graphs** – *Jaime Angulo Pava e Márcio Cavalcante de Melo*

**Scale Calculus and M-Polyfolds An Introduction** – *Joa Weber*

**Real and Complex Gaussian Multiplicative Chaos** – *Hubert Lacoin*

**Rigidez em Grafos de Proteínas** – *Carlile Lavor*

**Gauge Theory in Higher Dimensions** – *Daniel G. Fadel e Henrique N. Sá Earp*

**Elementos da Teoria de Aprendizagem de Máquina Supervisionada** – *Vladimir Pestov*

**Función Gamma: Propriedades Clásicas e Introducción a su Dinâmica** – *Pablo Diaz e Rafael Labarca*

**Introdução à Criptografia com Curvas Elípticas** – *Sally Andria, Rodrigo Gondim e Rodrigo Salomão*

**O Teorema dos Quatro Vértices e sua Recíproca** – *Mário Jorge Dias Carneiro e Ronaldo Alves Garcia*

**Uma Introdução Matemática a Blockchains** – *Augusto Teixeira*

