PRINCÍPIOS DE ENUMERAÇÃO

SÓSTENES LINS

INSTITUTO DE MATEMÁTICA PURA E APLICADA
Rua Luiz de Camões, 68
20.060 - Rio de Janeiro - RJ

A Laurinho

PREFÁCIO

Enumeração é o ramo da Matemática Finita, ou Combinatória, que se ocupa da contagem de estruturas (ou configurações) discretas. Questões enumerativas aparecem com freqüência em Estatística, Física, Química, Biologia, etc, e também sob vários disfarces, internamente, nas entrelinhas da maioria das áreas de Matemática.

Neste texto visamos apresentar algumas das técnicas importantes usadas em Enumeração. Procuramos ser o mais tutorial possível sacrificando, onde uma escolha é cabível, concisão e brevidade por um tratamento suave do assunto visando tornar a exposição psicologicamente mais "digestível".

Queremos agradecer à Comissão Organizadora do 13º Colóquio Brasileiro de Matemática pela oportunidade que nos deu de ministrar o curso baseado neste texto, a Neide Maria pelo paciente e esmerado trabalho de datilografia e a Bernardete pelas revisões que fez e em reconhecimento pelo ambiente tranqüilo que nos proporcionou a despeito das inúmeras horas de lazer sacrificadas.

Recife, 23 de maio de 1981

Sostenes Lins

ÍNDICE

CAPÍTULO I

TÉCNICAS CONTÍNUAS PARA CONTAR

I.1 - NÚMEROS DE FIBONACCI

Com freqüência, em questões de contagem é possível encontrarmos uma expressão para o número de configurações de uma certa ordem em termos do número de configurações de ordem inferior. Isto é, podemos encontrar uma "fórmula de recorrência". Nesta seção mostramos como podemos usar as funções geradoras (ordinárias) para obter uma fórmula fechada para o termo geral de uma recorrência linear homogênea. Tratamos extensivamente um exemplo concreto: A seqüência de Fibonacci e a seguir, com os termos bem motivados e bem definidos tratamos o caso geral.

O problema seguinte aparece em "liber Abaci" (O Livro do Ábaco) escrito por Leonardo de Pisa, mais conhecido como Fibonacci em 1202. (Fibonacci é considerado um dos maiores matemáticos da pré-renascença.)

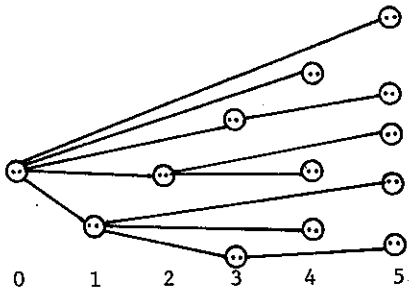
"Quantos casais de coelhos, gerados a partir de um único casal, nascem ao fim de n meses se as seguintes condições são verificadas:

(a) cada casal de coelhos produz um casal novo a cada mês;

(b) cada coelho fica fértil a partir de um mês de idade;

(c) não há mortes".

A figura seguinte dá uma idéia do que acontece.



Observe que as condições do problema conduzem à seqüência

$$0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ \ldots$$

onde os termos de ordem zero e um são 0 e 1 e a partir do segundo cada termo é obtido somando-se seus dois predecessores imediatos. Esta seqüência é a importante *seqüência de Fibonacci*. O nosso problema é calcular com uma fórmula "fechada" o termo de ordem n, F_n, da seqüência acima. Escolhemos este problema como o protótipo para o estudo das recorrências lineares homogêneas porque, historicamente, sua solução foi uma das primeiras aparições da idéia de funções geradoras, num trabalho de A. de Moivre em 1730. Nas notas ao final desta seção tentamos justificar o uso do adjetivo "importante" qualificando a seqüência de Fibonacci.

Antes de resolver o problema vamos dar a resposta: ao fim de n meses nascem precisamente $(n \geq 0)$

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right]$$

casais de coelhos!

Esta é, sem sombra de dúvidas, uma resposta bem estranha à primeira vista. Em particular, não é nem claro que a expressão para F_n seja um inteiro. Uma vez "adivinhada" contudo, ela pode ser provada por indução, o que deixamos a cargo do leitor diligente como um exercício. O difícil, diríamos quase impossível, é adivinhar tal resposta. E é aqui que entram em cena as funções geradoras.

A *função geradora ordinária* da seqüência

$$(a_0,\ a_1,\ a_2, \ldots, a_n,\ \ldots)$$

é a função

$$a(z) = \sum_{n \geq 0} a_n\, z^n\ ,$$

onde z pode ser pensado como uma variável complexa de norma bem pequena, para que a convergência se verifique. A rigor, nunca estamos interessados em somar tais séries e sim em extrair coeficientes da expansão em série de potências de $a(z)$, que em grande parte dos casos é uma função simples. Como vemos a seguir com nossos exemplos, a representação da seqüência completa $(a_n)_{n\geq 0}$ como uma (única) função abre o caminho para a utilização de técnicas contínuas do cálculo para a efetiva determinação da função $a(z)$ e subsequente extração do coeficientes de sua série de Taylor.

Seja

$$F(z) = \sum_{n\geq 0} F_n \, z^n$$

a função geradora (ordinária) da seqüência de Fibonacci. (De agora por diante omitimos o adjetivo "ordinária".) Sabemos que

$$F_0 = 0 \quad , \quad F_1 = 1$$

e que

$$F_n = F_{n-1} + F_{n-2} \quad , \quad n\geq 2.$$

Esta recorrência nos sugere escrever

$$z\,F(z) = F_0\, z + F_1\, z^2 + F_2\, z^3 + F_3\, z^4 + \ldots$$

$$z^2 F(z) = \qquad F_0\, z^2 + F_1\, z^3 + F_2\, z^4 + \ldots$$

Subtraindo de $F(z)$ a soma das duas funções acima obtemos:

$$(1-z-z^2)\, F_{(z)} = F_0 + (F_1 - F_0)\, z + \sum_{n\geq 2} (F_n - F_{n-1} - F_{n-2})\, z^n.$$

Observe que cada coeficiente de z^n para $n\geq 2$ é nulo, pela recorrência que define a seqüência $(F_n)_{n\geq 0}$. Como $F_0 = 0$ e $F_1 = 1$ o lado direito da equação acima vale simplesmente z e obtemos

$$F(z) = \frac{-z}{z^2+z-1}.$$

A solução do nosso problema para n meses é expressível como o coeficiente de z^n na expansão de F(z) em série de potências na vizinhança da origem (Série de Taylor). Isto é tão freqüente em enumeração que é conveniente usar um operador apropriado: $[z^n]$.

Se

$$a(z) = \sum_{n\geq 0} a_n z^n ,$$

definimos para cada $n\geq 0$ o operador *extrator*, $[z^n]$, como

$$[z^n]\{a(z)\} = a_n .$$

A nossa resposta é

$$[z^n]\left\{\frac{-z}{z^2+z-1}\right\}$$

e para dar uma fórmula mais explícita à mesma expressamos F(z) como frações parciais. Seja $q(z) = 1-z-z^2$. É conveniente encontrar as raízes de $z^2\, q(\frac{1}{z})$ ou seja z^2-z-1. Estas raízes são $\phi = \frac{1}{2}(1+\sqrt{5})$ e $\phi' = \frac{1}{2}(1-\sqrt{5})$. Vemos que F(z) pode ser expresso como

$$F(z) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-z\phi} - \frac{1}{1-z\phi'}\right) .$$

(Tomamos as raízes de $z^2\, q(\frac{1}{z})$ porque isto acarreta expressões adequadas nos denominadores; expressões que, em geral como mostramos na próxima seção, permitem encontrar rapidamente as séries de Taylor que precisamos.) Note que as duas frações na equação acima têm expansão de Taylor simples numa vizinhança da origem. Especi-

ficamente

$$F(z) = \frac{1}{\sqrt{5}} \left[(1 + \phi z + \phi^2 z^2 + \ldots) - (1 + \phi' z + \phi'^2 z^2 + \ldots) \right] .$$

Assim obtemos

(I.1.a) PROPOSIÇÃO: O n-ésimo número de Fibonacci é

$$\left[z^n \right] \{ F(z) \} = \frac{1}{\sqrt{5}} (\phi^n - \phi'^n)$$

$$= \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right] .$$

Observe que esta é a resposta anunciada a priori.

CONTANDO SUBCONJUNTOS SEM ADJACÊNCIAS

Vamos agora encontrar uma outra interpretação enumerativa para os números de Fibonacci. Em seguida tratamos uma versão "circular" do mesmo problema que é usada posteriormente no capítulo IV. Considere a seguinte questão: quantos subconjuntos de $N = \{1,2,\ldots,n\}$ com k elementos existem nos quais não há dois números consecutivos? Seja $g(n,k)$ este número.

Representemos cada subconjunto S de N por seu vetor característico, isto é, por uma n-upla onde a i-ésima coordenada vale 1 se $i \in S$ e vale 0 se $i \notin S$. Assim $g(n,k)$ é o número de n-uplas de 0 e 1's onde existem k 1's não adjacentes. Considere n-k 0's ordenados. Para precisarmos a inserção de k 1's é suficiente dizer quantos zeros precedem cada 1. Dessa forma, é fácil concluir que o conjunto das n-uplas sem adjacências de 1's está em bijeção com os conjuntos de k elementos do conjunto $\{0,1,2,\ldots,n-k\}$. Logo $g(n,k)$ pode ser expresso como o coeficiente binominal

$$g(n,k) = \binom{n-k+1}{k} = \frac{(n-k+1)!}{k!\,(n-2k+1)!} ,$$

onde o fatorial de um número negativo é definido como zero.

O número total de subconjuntos de N sem elementos consecutivos é portanto

$$G_n = \sum_{n\geq 0} \binom{n-k+1}{k} .$$

Note que $\binom{r}{s} = 0$ se $s>r$. Existe uma conexao estreita entre os G_n's e os números de Fibonacci. A seqüência $(G_0, G_1, G_2, \ldots)$ é

$$(1,\ 2,\ 3,\ 5,\ 8,\ \ldots)$$

e a seqüência de Fibonacci (a do problema dos coelhos) é

$$(0,\ 1,\ 1,\ 2,\ 3,\ 5,\ 8,\ \ldots) .$$

Aparentemente temos, para $n\geq 0$, $F_{n+2} = G_n$. Vamos provar por indução que isto é um fato. Suponhamos que $F_{j+2} = G_j$, para $j \leq n$. Pela definição dos F_n's temos

$$F_{n+3} = F_{n+2} + F_{n+1} .$$

O que temos de provar, uma vez que a base da indução já está verificada, é que

$$G_{n+1} = G_n + G_{n-1} .$$

Pela expressão para os G_n's obtemos

$$G_n + G_{n-1} = \sum_{k\geq 0} \binom{n-k+1}{k} + \sum_{k\geq 0} \binom{n-k}{k}$$

$$= \sum_{k\geq 0} \binom{n-k+1}{k} + \sum_{k\geq 1} \binom{n-k+1}{k-1}$$

$$= \binom{n-k+1}{0} + \sum_{k>1} \left[\binom{n-k+1}{k} + \binom{n-k+1}{k-1} \right]$$

$$= \binom{n-k+2}{0} + \sum_{k\geq 1} \binom{n-k+2}{k}$$

$$= \sum_{k\geq 0} \binom{n-k+2}{k} = G_{n+1} .$$

Logo, para todo n, $F_{n+2} = G_n$. Na realidade não é muito importante de onde a seqüência de Fibonacci começa. Assim é muito comum chamar G_n do n-ésimo número de Fibonacci. Adotando-se esta convenção, podemos definir o n-ésimo número de Fibonacci como o número de subconjuntos de

$$N = \{1,2,\ldots,n\}$$

em que não aparecem números consecutivos.

A QUESTÃO CIRCULAR

Consideramos agora a mesma questão, acerca do número de subconjuntos de N sem elementos consecutivos, com a diferença de que agora n e 1 são considerados consecutivos. A solução deste problema é usada no "Problema do Jantar", considerado no capítulo IV.

Seja $f(n,k)$ o número de k-subconjuntos de N sem elementos consecutivos mod n. Os subconjuntos deste tipo que contêm n não contêm 1 nem $n-1$. Assim o seu número, $f_1(n,k)$, é igual ao número de $(k-1)$-subconjuntos de $\{2,3,\ldots,n-2\}$ sem adja

cências linear tratado anteriormente

$$f_1(n,k) = g(n-3,k-1) .$$

O número, $f_2(n,k)$, de k-subconjuntos permitidos que não contêm n é claramente

$$f_2(n,k) = g(n-1,k) .$$

Assim temos

$$\begin{aligned} f(n,k) &= f_1(n,k) + f_2(n,k) \\ &= g(n-3,k-1) + g(n-1,k) \\ &= \binom{(n-3) - (k-1) + 1}{k-1} + \binom{n - (k-1) + 1}{k} \\ &= \binom{n-k-1}{k-1} + \binom{n-k}{k} \\ &= \frac{n}{n-k}\binom{n-k}{k} . \end{aligned}$$

Somando para k obtemos

(I.1.b) PROPOSIÇÃO: O número F_n^o de subconjuntos de $N = \{1,2,\ldots,n\}$ sem elementos consecutivos mod n é

$$F_n^o = \sum_{k\geq 0} \frac{n}{n-k}\binom{n-k}{k} .$$

NOTAS

Os números de Fibonacci aparecem em grande número de situações. Na análise de casos extremos em vários algorítmos, por exemplo. No algorítmo de Euclides para se encontrar o mdc (m,n) onde $m,n \leq F_k$, k-ésimo número de Fibonacci, são necessárias no máximo k+1 divisões. Isto foi provado em 1844 por G. Lamé e foi a primeira aplicação desses números ao estudo de Algorítmos. Durante a segunda metade do século passado E. Lucas obteve resultados, generalizações e aplicações interessantes envolvendo estes números usando-os por exemplo, para provar que o número $2^{127} - 1$ (que tem 39 dígitos) é primo.

Desenvolvimentos recentes em Ciência da Computação mostraram que os números de Fibonacci têm aplicações úteis em ordenação de dados, recuperação de informações, geração de números aleatórios, etc. Para dar vazão a estas descobertas recentes foi até criado em 1963 um Jornal que publica generalizações teóricas e aplicações do conceito: "The Fibonacci Quaterly".

É no entanto em Biologia que os números de Fibonacci aparecem de maneira mais inesperada. Citamos dois exemplos: As sementes do girassol são dispostas na flor de tal maneira que formam 2 conjuntos de espirais, um conjunto horário e o outro anti-horário. Invariavelmente os números de espirais nestes dois conjuntos são números de Fibonacci consecutivos: $F_9=34$ e $F_{10}=55$ para girassóis de tamanho médio $F_{11}=89$ e $F_{12}=144$ para girassóis gigantes e há menção na literatura de girassóis super- gigantes tendo $F_{12}=144$ e $F_{13}=233$ espirais!

Outro exemplo são as faixas de losangos no abacaxi. A parte externa do abacaxi é formada por pequenos losangos verticais dispostos lado a lado. O número de faixas destes losangos são para todos os abacaxis em que as contamos $F_6=8$ num sentido e $F_7=13$ no outro. Há também menção de abacaxis gigantes que têm $F_7=13$ e $F_8=21$ faixas de losangos. Cada uma destas faixas forma uma espécie de hélice. Podemos definir, então abacaxi "horário" como aquele em que as hélices em maior número são em sentido horário;

de maneira análoga abacaxi "anti-horário". Perguntas (não matemáticas) que gostaríamos de saber a resposta são:

Qual o tipo mais comum de abacaxi?

Existe uma explicação biológica simples para a aparição dos números de Fibonacci no girassol e no abacaxi?

Algumas propriedades aritméticas interessantes dos números de Fibonacci são encontradas nos exercícios deste capítulo.

I.2 - RECORRÊNCIAS LINEARES

Seja f uma função dos naturais em si mesmo. Dizemos que f satisfaz uma *recorrência linear homogênea com coeficientes constantes* se existem constantes complexas $a_1, a_2, \ldots, a_k$ tal que para todo $n \geq k$

$$f(n) + a_1 f(n-1) + a_2 f(n-2) + \ldots + a_k f(n-k) = 0.$$

O natural k é chamado a *ordem* da recorrência. A recorrência é linear porque f e as constantes aparecem apenas com o expoente 1. É homogênea porque não há termo independente de f.

Note que a recorrência para os números de Fibonacci é uma recorrência linear homogênea com coeficientes constantes de ordem 2. Já a recorrência

$$f(n) = \sum_{i=1}^{n} f(n-i)\, f(i)$$

que tratamos na próxima seção não é linear e sim quadrática em f.

Nesta seção assumimos que o leitor esteja familiarizado com a técnica de decomposição em frações parciais e com o teorema binomial, estudados nos primeiros cursos de cálculo. Usando estas ferramentas vamos praticamente repetir o que fizemos para encontrar o termo geral da seqüência de Fibonacci e "resolver" a recorrência linear homogênea com coeficientes constantes de ordem k, isto é, encontrar a fórmula para $f(n)$. Isto mostra que a técnica utilizada, à primeira vista bastante particular, se generaliza consideravelmente.

RESOLUÇÃO DE $f(n) = -\sum_{i=1}^{k} a_i f(n-i)$.

Denotemos $f(n)$ por f_n e seja $f(z)$ a função geradora para $(f_n)_{n \geq 0}$. Temos

$$f(z) = \sum_{n\geq 0} f_n z^n$$

$$a_1 z\, f(z) = \sum_{n\geq 1} a_1 f_{n-1} z^n$$

$$a_2 z^2 f(z) = \sum_{n\geq 2} a_2 f_{n-2} z^n$$

.....

$$a_k z^n f(z) = \sum_{n\geq k} a_k f_{n-k} z^n.$$

Somando estas igualdades obtemos, fazendo $a_0 = 1$,

$$(a_0 + a_1 z + a_2 z^2 + \ldots + a_k z^k) f(z) = a_0 f_0 + (a_0 f_1 + a_1 f_0) z +$$

$$+ (a_0 f_2 + a_1 f_1 + a_2 f_0) z^2 + \ldots + \sum_{i=0}^{k-1} a_i f_{k-1-i} z^{k-1}$$

uma vez que os coeficientes de z^n se anulam para $n \geq k$.

Assim

$$f(z) = p(z)/q(z),$$

onde

$$p(z) = \sum_{i=0}^{k-1} \left(\sum_{j=0}^{i} a_j f_{i-j} \right) z^i$$

e

$$q(z) = \sum_{i=0}^{k} a_i z^i.$$

Como a recorrência é de ordem k, $a_k \neq 0$ e $q(z)$ é um polinômio de grau k; $p(z)$ tem grau no máximo $k-1$.

O que nos interessa é uma fórmula para

$$[z^n]\left\{\frac{p(z)}{q(z)}\right\}$$

e portanto temos de desenvolver a fração entre chaves em série de Taylor. Para isto é conveniente encontrarmos a expressão da mesma como soma de frações parciais.

Seja r o polinômio de grau k definido a partir de q como

$$r(z) = z^k\, q(\tfrac{1}{z}).$$

Pelo teorema fundamental da Álgebra $r(z)$ se decompõe em fatores lineares sobre o corpo dos números complexos C. Sejam $r_1, r_2, \ldots, r_d$ as raízes distintas de $r(z)$. Como $r(z)$ é um polinômio mônico (coeficiente do termo de maior grau é 1) obtemos

$$r(z) = \prod_{i=1}^{d} (z-r_i)^{m_i}$$

onde m_i é a multiplicidade da raiz r_i. O polinômio q se decompõe como

$$q(z) = z^k\, r(\tfrac{1}{z}) = \prod_{i=1}^{d} (1-zr_i)^{m_i},$$

uma vez que o número total de fatores é k.

Usamos agora o teorema básico sobre decomposição em frações parciais, que é muito usado em cálculo para integrar formas racionais. Para uma prova veja [GO 1 - seção 32.4]. Como o grau de p é menor que grau de q, podemos encontrar um conjunto único de k números complexos $\{c_{ij_i}\}$ onde $1 \leq i \leq d$, $1 \leq j_i \leq m_i$ tal que

$$\frac{p(z)}{q(z)} = \frac{p(z)}{\prod_{i=1}^{j} (1-r_i)^{m_i}} = \sum_{i=1}^{d} \left(\sum_{j_i=1}^{m_i} \frac{c_{ij_i}}{(1-r_i z)^{j_i}} \right).$$

Na realidade os números c_{ij_i}'s são determinados a partir de um sistema linear com solução única definido pela equação acima. Depois de concluir esta análise damos um exemplo onde isto é esclarecido.

Para terminar, precisamos apenas desenvolver cada parcela do tipo

$$c_{ij_i} \frac{1}{(1-r_i z)^{j_i}}$$

em sua expansão de Taylor. Isto pode ser feito com o auxílio do teorema binomial de Newton, que enunciamos sem prova.

TEOREMA BINOMIAL: Seja α um número complexo qualquer. Se $|z|<1$, então

$$(1+z)^{\alpha} = \sum_{n\geq 0} \binom{\alpha}{n} z^n,$$

onde

$$\binom{\alpha}{n} = \frac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-n+1)}{n!}. \qquad \square$$

Para uma prova deste teorema veja, por exemplo, [MO 1 - seção 10.8].

Usando este teorema para $\alpha = -j_i$ e $z = r_i z$ obtemos para $|z| < \frac{1}{|r_i|}$

$$(1+r_i z)^{-j_i} = \sum_{n\geq 0} \binom{-j_i}{n} (-r_i z)^n .$$

Note que

$$\binom{-j_i}{n} = (-1)^n \binom{j_i+n-1}{n}$$

e assim

$$(1+r_i z)^{-j_i} = \sum_{n\geq 0} \binom{j+n-1}{n} r_i^n \, z^n .$$

Somando os coeficientes de mesmo grau obtemos

(I.2.a) TEOREMA (Solução de Recorrência):

$$\left[z^n\right] \{ f(z)\} = \left[z^n\right] \left\{\frac{p(z)}{q(z)}\right\} = \sum_{i=1}^{d} \left(\sum_{j_i=1}^{m_i} c_{ij_i} \binom{j_i+n-1}{n} r_i^n \right)$$

é a solução geral da recorrência linear homogênea com coeficientes constantes de ordem k apresentada no ínicio desta seção. □

Para recordar os conceitos envolvidos na equação acima repetimos: o índice superior da primeira soma, d, é o número de raízes distintas que o polinômio de grau k

$$r(z) = z^k \, q(\tfrac{1}{z})$$

tem. O segundo índice superior, m_i, é a multiplicidade da i-ésima raiz, r_i, de r. Finalmente, as constantes complexas

$$\{ c_{ij_i} \} \quad 1\leq i\leq d, \quad 1\leq j_i\leq m_i$$

são obtidas como solução única para a equação

$$\frac{p(z)}{q(z)} = \frac{p(z)}{\prod_{i=1}^{j}(1-r_i)^{m_i}} = \sum_{i=1}^{d} \sum_{j_i=1}^{m_i} \frac{c_{ij_i}}{(1-r_i z)^{j_i}} .$$

Vamos agora dar dois exemplos para ilustrar o uso do teorema acima. No primeiro deles há raízes múltiplas, porém a expressão de raízes e constantes é bastante simples

(I.2.b) EXEMPLO: Considere a recorrência

$$f_n - 4f_{n-1} + 5f_{n-2} - 2f_{n-3} = 0, \quad n \geq 3,$$

sujeita às condições iniciais

$$f_0 = 2, \quad f_1 = -1, \quad f_2 = 7.$$

Os polinômios $p(z)$ e $q(z)$ são

$$\begin{aligned} p(z) &= a_0 f_0 + (a_0 f_1 + a_1 f_0) z + (a_0 f_2 + a_1 f_1 + a_2 f_0) z^2 \\ &= 1.2 + [(1.-1) + (-4.2)] z + [(1.7) + (-4.1) + (5.2)] z^2 \\ &= 2 - 9z + 21 z^2 \end{aligned}$$

$$\begin{aligned} q(z) &= a_0 + a_1 z + a_2 z^2 + a_3 z^3 \\ &= 1 - 4z + 5z^2 - 2z^3 \end{aligned}$$

e $r(z)$ vale

$$r(z) = z^3 q(\tfrac{1}{z}) = z^3 - 4z^2 + 5z - 2.$$

As raízes de r são 1,1 e 2. Para encontrar as constantes c_{ij_i}'s fazemos portanto

$$\frac{2-9z+21z^2}{1-4z+5z^2-2z^3} = \frac{c_{11}}{1-z} + \frac{c_{12}}{(1-z)^2} + \frac{c_{21}}{1-2z}.$$

Ou equivalentemente para todo z,

$$\begin{aligned} 2 - 9z + 7z^2 &= (1-z)(1-2z)\, c_{11} + (1-2z)\, c_{12} + (1-z)^2\, c_{21} \\ &= (1-3z+2z^2)\, c_{11} + (1-2z)\, c_{12} + (1-2z+z^2)\, c_{21} \\ &= (c_{11} + c_{12} + c_{21}) + (-3c_{11} - 2c_{12} - 2c_{21})z \\ &\quad + (2c_{11} + c_{21})\, z^2. \end{aligned}$$

Igualando os coeficientes obtemos o seguinte sistema linear

$$\begin{aligned} c_{11} + c_{12} + c_{21} &= 2 \\ 3c_{11} + 2c_{12} + 2c_{21} &= 9 \\ 2c_{11} + c_{21} &= 21, \end{aligned}$$

cuja solução única é $c_{11} = 5$, $c_{12} = -14$, $c_{21} = 11$. (Na realidade o teorema básico sobre decomposição em frações parciais afirma que o sistema linear obtido como acima tem sempre uma única solução.)

A fórmula que deduzimos nos dá

$$\left[z^n\right]\{f(z)\} = f_n = 5\binom{n}{n} 1^n - 14\binom{n+1}{n} 1^n + 11\binom{n}{n} 2^n$$

$$= 5 - 14(n+1) + 11.2^n$$

para solução do exemplo.

Os 13 primeiros f_n's dados por esta fórmula são

n	f_n	n	f_n
0	2		
1	-1	7	1301
2	7	8	2695
3	37	9	5497
4	111	10	11115
5	273	11	22365
6	611	12	44879

Estes valores podem ser comprovados comparando-os com os obtidos diretamente da recorrência.

No segundo exemplo vamos ilustrar o ponto de que, mesmo num problema simples, a solução pode envolver expressões complexas sem forma racional concisa. Ilustra também de como podemos, baseando-nos em aproximações reais, obter uma fórmula exata.

(I.2.c) EXEMPLO: Suponha que palavras de comprimento n nos símbolos $\{x,y,z\}$ sejam transmitidas por um canal de comunicações. A restrição imposta nas palavras é a de que 3 símbolos x não apareçam juntos. Determine o número p_n de palavras permitidas de comprimento n.

Por enumeração direta encontramos

$$p_1 = |\{x,y,z\}| = 3$$

$$p_2 = |\{x,y,z\} \times \{x,y,z\}| = 9$$

$$p_3 = |\{x,y,z\}^3 \setminus \{x,x,x\} = 27 - 1 = 26.$$

Assuma que $n \geq 4$. Abaixo listamos o começo de uma palavra e o número de palavras que assim começam

z.....	p_{n-1}	palavras
y.....	p_{n-1}	palavras
xy.....	p_{n-2}	palavras
xz.....	p_{n-2}	palavras
xxy...	p_{n-3}	palavras
xxz...	p_{n-3}	palavras.

Assim a expressão procurada satisfaz à seguinte recorrência para $n \geq 4$

$$p_n = {}^2p_{n-1} + {}^2p_{n-2} + {}^2p_{n-3}.$$

Para coincidir com a notação usada na prova do teorema (I.2.a) seja $f_n = p_{n+1}$ para $n \geq 0$. Temos para $n \geq 3$

$$f_n - 2f_{n-1} - 2f_{n-2} - 2f_{n-3} = 0$$

$$f_0 = 3 \ , \ f_1 = 9 \ , \ f_2 = 26.$$

Encontramos para $p(z)$, $q(z)$, $r(z)$ (veja prova do teorema (I.2.a),

$$p(z) = a_0 f_0 + (a_0 f_1 + a_1 f_0)z + (a_0 f_2 + a_1 f_1 + a_2 f_1)z^2$$

$$= 3 + (9-6)z + (26-18-6)z^2$$

$$= 3 + 3z + 2z^2.$$

$$q(z) = 1 - 2z - 2z^2 - 2z^3$$

$$r(z) = z^3 - 2z^2 - 2z - 2.$$

Esta última equação tem uma raíz real e duas raízes complexas conjugadas que vamos chamar de r e de $a \pm b_i$. Podemos, usando por exemplo o método descrito na introdução de [GO 2] explicitar estas raízes obtendo para r, a, b:

$$r = \frac{1}{9s} (9s^2+6s+10)$$

$$a = \frac{1}{18s} (-9s^2+12s-10)$$

$$b = \frac{1}{18s} (9s^2-10) \sqrt{3} \ i$$

onde s vale (estranhamente para quem não está acostumado com cúbicas irredutíveis)

$$s = \sqrt[3]{\frac{106 + \sqrt{7236}}{54}}.$$

A equação

$$\frac{p(z)}{q(z)} = \frac{c_{11}}{1-rz} + \frac{c_{21}}{1-(a+bi)z} + \frac{c_{31}}{1-(a-bi)z},$$

conduz ao sistema linear complexo em c_{11}, c_{21}, c_{31}:

$$c_{11} + c_{21} + c_{31} = 3$$

$$2ac_{11} + \left[(a+r) - bi\right] c_{21} + \left[(a+r) + bi\right] c_{31} = -3$$

$$(a^2+b^2)\, c_{11} + (ar-bri)\, c_{21} + (ar+bri)\, c_{31} = 2$$

cuja solução única, obtida com a regra de Cramer, vale

$$c_{11} = \frac{\Delta_1}{\Delta}\ ,\quad c_{21} = \frac{\Delta_2}{\Delta}\ ,\quad c_{31} = \frac{\Delta_3}{\Delta}\ ,$$

onde

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ 2a & a+r-bi & a+r+bi \\ a^2b^2 & ar-bri & ar+bri \end{vmatrix} = \left[(r-a)^2 + b^2\right] 2bi$$

$$\Delta_1 = \begin{vmatrix} 3 & 1 & 1 \\ -3 & a+r-bi & a+r+bi \\ 2 & ar-bri & ar+bi \end{vmatrix} = (3r^2+3r+2)2bi$$

$$\Delta_2 = \begin{vmatrix} 1 & 3 & 1 \\ 2a & -3 & a+r+bi \\ a^2+b^2 & 2 & ar+bri \end{vmatrix}$$

$$\Delta_3 = \begin{vmatrix} 1 & 1 & 3 \\ 2a & a+r-bi & -3 \\ a^2+b^2 & ar-bri & 2 \end{vmatrix}.$$

Note que a matriz associada a Δ_3 se consegue trocando a $2^{\underline{a}}$ e $3^{\underline{a}}$ colunas de Δ_2 e em seguida tomando os conjugados dos elementos da $3^{\underline{a}}$ coluna. Assim concluimos que

$$\Delta_3 = -\bar{\Delta}_2$$

e como Δ é um imaginário puro, obtemos

$$c_{31} = \bar{c}_{21}.$$

Utilizando esta igualdade bem como o fato de $c=c_{11}$ ser um número real podemos derivar do sistema acima um sistema real. Seja $c_{21} = y + zi$. Obtemos das primeiras 2 equações do sistema original

$$c + 2y = 3$$

$$2ac + 2(a+r)y + 2bz = -3.$$

Como já sabemos que

$$c = \frac{3r^2+3r+2}{(r-a)^2+b^2},$$

estas duas equações são suficientes para obter y e z:

$$y = \frac{1}{2}(3-c)$$

$$z = \frac{1}{2b}(-3-2(a+r)y - 2ac).$$

Pelo teorema (I.2.a) a solução é

$$p_{n+1} = cr^n + (y+zi)(a+bi)^n + (y-zi)(a-bi)^n.$$

Como a função conjugado comuta com soma e produto, as duas últimas parcelas são conjugadas e assim podemos escrever

$$p_{n+1} = cr^n + 2\mathrm{Re}\left[(y+zi)(a+bi)^n\right],$$

onde $\mathrm{Re}(\omega)$ é a parte real do número complexo ω.

Sejam (ρ_1,θ_1) e (ρ_2,θ_2) as coordenadas polares de $a+bi$ e de $y+zi$ respectivamente, isto é,

$$\rho_1 = (a^2+b^2)^{1/2} \qquad \theta_1 = \text{arctg}(\frac{b}{a})$$

$$\rho_2 = (y^2+z^2)^{1/2} \qquad \theta_2 = \text{arctg}(\frac{z}{y})$$

onde a função arctg assume valores em $[-\pi,\pi] \setminus \{-\pi/2, \pi/2\}$.

Usando a forma polar para as multiplicações complexas na fórmula para p_{n+1} acima obtemos

$$p_{n+1} = cr^n + 2\rho_1^n\rho_2 \cos(n\theta_1+\theta_2).$$

Vamos agora estimar os parâmetros envolvidos e com isto mostrar que para todo $n>0$ a segunda parcela é menor que 1/2 em valor absoluto. Observe que isto implica, uma vez que p_{n+1} é um inteiro, que

$$p_{n+1} = \left\lfloor cr^n + \frac{1}{2} \right\rfloor,$$

onde $\lfloor x \rfloor$ significa o maior inteiro menor ou igual a x.

VALORES APROXIMADOS

$$s = \sqrt[3]{\frac{106 + \sqrt{7236}}{54}} = 1,52380321...$$

$$a = \frac{1}{18s}(-9s^2+12s+10) = -0,45981978...$$

$$b = \frac{1}{18s}(9s^2-10)\sqrt{3} = 0,68817282...$$

E daqui obtemos,

$$\rho_1 = (a^2+b^2)^{1/2} = 0,82765697...$$

$$\theta_1 = \text{arctg}(\frac{b}{a}) = 2,15984234...$$

Temos também

$$r = \frac{1}{9s}(9s^2+6s+10) = 2,91963956...$$

$$c = \frac{3r^2+3r+2}{(r-a)^2+b^2} = 3,05454888...$$

$$y = \frac{1}{2}(3-c) = -0,02727444...$$

$$z = \frac{-1}{2b}\left[3+2(a+r)y + 2ac\right] = -0,04122187...$$

$$\rho_2 = (y^2+z^2)^{1/2} = 0,04942811...$$

$$\theta_2 = \text{arctg}\left(\frac{z}{y}\right) = -2,15531761...$$

Com estes valores podemos concluir

$$2\rho_1^n\rho_2 \leq 2\rho_2 < \frac{1}{2}$$

e assim

$$|2\rho_1^n\rho_2 \cos(n\theta_1+\theta_2)| < \frac{1}{2}.$$

Desse modo podemos escrever

$$p_{n+1} = \left\lfloor cr^n + \frac{1}{2} \right\rfloor.$$

Assim, a resposta exata para o nosso problema pode ser expressa em termos de

$$s = \sqrt[3]{\frac{106 + \sqrt{7236}}{54}}.$$

Substituindo c e r por seus valores em termos de s obtemos que existem

$$p_{n+1} = \left\lfloor \frac{81s^4+189s^3+324s^2+210s+100}{81s^4+90s^2+100} \left(\frac{9s^2+6s+10}{9s}\right)^n + \frac{1}{2} \right\rfloor$$

palavras de comprimento n+1 em três símbolos com a restrição de que um dos símbolos não aparece três vezes juntos.

A tabela abaixo dá os 13 primeiros valores obtidos com a fórmula acima:

n	$c r^{n-1}$	$\left\lfloor c r^{n-1} + \frac{1}{2} \right\rfloor = p_n$
1	3,054...	3
2	8,918...	9
3	26,037...	26
4	76,021...	76
5	221,954...	222
6	648,027...	648
7	1892,006...	1892
8	5523,975...	5524
9	16128,018...	16128
10	47087,999...	47088
11	137479,987...	137480
12	401392,009...	401392
13	1171919,981...	1171920.

Podemos comprovar estes valores observando que qualquer um deles, a partir do quarto, é o duplo de seus 3 predecessores imediatos.

I.3 - MULTIPLICANDO N FATORES: RECORRÊNCIA QUADRÁTICA

Vamos nesta seção tratar um tipo especial de recorrência quadrática e ilustrar o uso do teorema binomial com expoente fracionário (o que torna a soma infinita). O nosso tratamento é feito através de um exemplo simples que agora enunciamos.

Suponhamos que $*$ seja uma operação binária definida em algum conjunto. Podemos avaliar o produto $a * b * c$ de duas maneiras distintas, a saber,

$$(a * b) * c$$

$$a * (b * c).$$

Se temos quatro fatores, $a * b * c * d$ pode ser calculado de cinco maneiras

$$(a * b) * (c * d)$$

$$((a * b) * c) * d$$

$$(a * (b * c)) * d$$

$$a * ((b * c) * d)$$

$$a * (b * (c * d)).$$

A nossa pergunta é: de quantas maneiras distintas podemos multiplicar n fatores mantendo a ordem dos mesmos?

Se a operação $*$ é associativa o produto final será o mesmo em qualquer das sequências em que se efetuem as operações. Mesmo assim mostramos, nas notas desta seção, que no caso de matrizes a ordem em que os fatores parciais são efetuados pode ser extremamente importante do ponto de vista computacional.

UMA RECORRÊNCIA QUADRÁTICA ESPECIAL

Quando estamos efetuando o produto de n fatores na última multiplicação calculamos o produto de um fator, que corresponde originalmente ao produto dos $k \geq 1$ primeiros fatores por um fator que corresponde ao produto dos últimos $n-k$ fatores. Deno-

temos por c_n o número de maneiras distintas de se multiplicar n fatores. A observação acima implica a seguinte relação de recorrência:

$$c_n = c_1 c_{n-1} + c_2 c_{n-2} + \ldots + c_{n-1} c_1,$$

onde c_1 é definido como 1. Observe que não faz sentido multiplicarmos 1 fator, porém note que a definição de c_1 como 1 é consistente com a situação combinatorial e facilita a notação, evitando exceções.

Seja f a função geradora dos c_n's, isto é,

$$f(x) = \sum_{n\geq 1} c_n x^n.$$

A recorrência quadrática acima nos sugere computarmos o quadrado de f, que é

$$f^2(x) = \sum_{n\geq 2} \left(\sum_{i=1}^{n-1} c_i \, c_{n-i} \right) x^n.$$

Observe, no entanto, que o termo entre parênteses é precisamente o valor de c_n pela recorrência acima. Desse modo obtemos

$$f^2(x) = \sum_{n\geq 2} c_n \, x^n,$$

o que conduz à seguinte equação funcional

$$f^2(x) - f(x) + x = 0.$$

Desta equação quadrática em f obtemos

$$f(x) = \frac{1 \pm (1-4x)^{1/2}}{2},$$

onde apenas um dos sinais deve ser considerado. Qual? Vamos determinar combinatorialmente.

Pelo Teorema binomial (para complexos x com $|x| < \frac{1}{4}$) temos

$$(1-4x)^{1/2} = \sum_{n>0} \binom{1/2}{n} (-4x)^n.$$

Note que

$$\binom{1/2}{n} = \frac{1/2(1/2-1)(1/2-2)\ldots(1/2-n+1)}{n!}$$

$$= (-1)^{n+1} \frac{1.3.5\ldots 2n-3}{2^n\, n!}$$

$$= (-1)^{n+1} \frac{(2n-2)!}{2.4.6\ldots(2n-2)\; 2^n\, n!}$$

$$= (-1)^{n+1} \frac{(2n-2)!}{(n-1)!\; 2^{2n-1} n!}$$

Utilizando este valor de $\binom{1/2}{n}$ na soma acima obtemos

$$(1-4x)^{1/2} = 1-2x + \sum_{n\geq 2} (-1)^{n+1} \frac{(2n-2)!}{(n-1)!\; 2^{2n-1} n!} (-1)^n\, 2^{2n}\, x^n$$

$$= 1-2x - \sum_{n\geq 2} \frac{2(2n-2)!}{(n-1)!n!}\, x^n .$$

Estamos agora em condições de desprezar um dos sinais na expressão de $f(x)$ acima. Como os coeficientes de $f(x)$ devem ser positivos, pois correspondem à solução de um problema de contagem, o sinal positivo não deve ser levado em conta pois conduz a coeficientes negativos. Obtemos assim

$$f(x) = \frac{1-(1-4x)^{1/2}}{2} =$$

$$= \frac{1}{2}\left\{1 - \left[1-2x - \sum_{n\geq 2} \frac{2(2n-2)!}{(n-1)!n!}\, x^n\right]\right\}$$

$$= \sum_{n\geq 1} \frac{(2n-2)}{(n-1)!n!}\, x^n .$$

A equação acima nos dá a resposta da nossa questão.

(I.3a) PROPOSIÇÃO: Existem

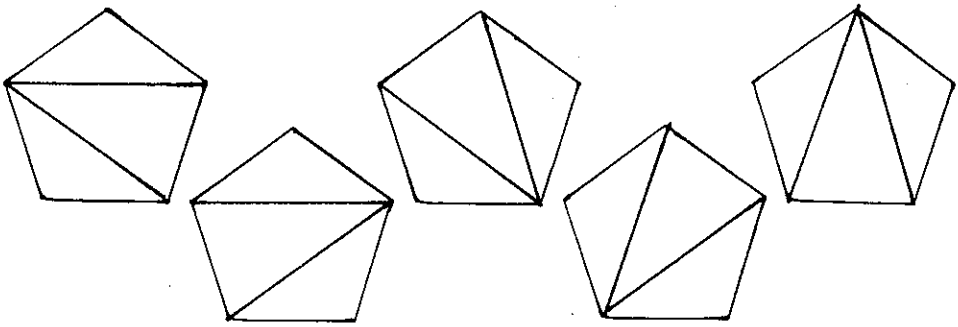
$$c_n = \frac{(2n-2)!}{(n-1)!\ n!} = \frac{1}{n}\binom{2n-2}{n-1}$$

maneiras distintas de se avaliar um produto de n fatores. □

Os números c_n , $n\geq 1$ são conhecidos como *números de Catalão* e aparecem como resposta para vários problemas de contagem. Isto é um reflexo do fato de que a decomposição básica da qual construimos a recorrência se aplica a vários problemas. Damos apenas mais dois exemplos, o primeiro deles tirado de uma situação geométrica.

TRIANGULAÇÕES DE UM POLÍGONO

Existem duas maneiras de se triangular um quadrilátero convexo traçando-se uma diagonal e cinco de se triangular um pentágono convexo traçando-se 3 diagonais que não se cruzam Estas são mostradas abaixo.



Uma vez que a forma do polígono não é necessariamente regular, equivalência sob rotações e reflexoes não são consideradas. É como se tivéssemos "rótulos" para os lados do polígono.

Seja t_n o número de maneiras de se triangular um polígono com n lados.

(I.3.b) PROPOSIÇÃO: O valor de t_n é o $(n-1)$-ésimo número de Catalão. Isto é

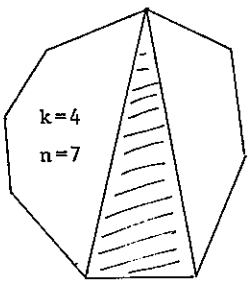
$$t_{n+1} = c_n = \frac{1}{n}\binom{2n-2}{n-1}, \quad n \geq 1.$$

PROVA: Embora nao fazendo sentido a priori, definimos $t_2 = c_1 = 1$. É suficiente mostrar que a recorrência para $n \geq 2$

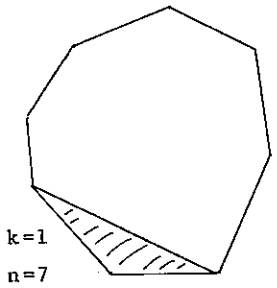
$$t_{n+1} = t_2 t_n + t_3 t_{n-1} + \ldots + t_n t_2,$$

com valor inicial $t_2 = 1$ é satisfeita pelos t_n's.

Vamos distinguir um lado do polígono e chamá-lo de base. Numa triangulação arbitrária de um $(n+1)$-polígono removendo-se o triângulo que contém a base, "quebramos" o polígono em dois polígonos, um à esquerda com $k+1$ lados e o outro à direita com $n-k+1$, para $k \geq 1$.



base



base

Para k=1 e k=n-1 temos os casos em que um polígono é degenerado com 2 lados, ou seja, um segmento de reta. Um destes casos é ilustrado à direita da figura acima. Para englobar estes casos na análise seguinte é que definimos t_2 como sendo 1.

Vamos chamar uma triangulação de *tipo k*, se o triângulo da base subdivide o polígono original em polígonos com k+1 e n-k+1 lados. Evidentemente o número de triangulações de tipo k de um (n-1)-polígono é

$$t_{k+1} \cdot t_{n-k+1}$$

como k varia de 1 a n-1 obtemos para o número total de triangulações

$$t_{n+1} = \sum_{k=1}^{n-1} t_{k+1}\, t_{n-k+1}.$$

Esta é precisamente a recorrência, inclusive com a mesma condição inicial, que define os números de Catalão, desde que façamos a translação de uma unidade nos índices: $t_{n+1} = c_n$.

Assim

$$t_{n+1} = \frac{1}{n}\binom{2n-2}{n-1},$$

provando a proposição. □

ÁRVORES BINÁRIAS

As árvores binárias são as estruturas não lineares mais usadas em computação. Uma árvore binária é uma 3-upla ordenada

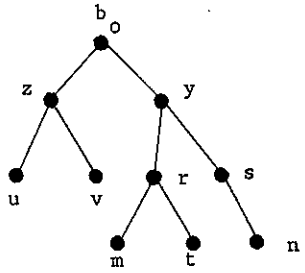
$$(B\ ,\ esq\ ,\ dir)$$

onde B, o *conjunto base*, é um conjunto finito com um elemento b_0 distinguido chamado *raiz* e esq, dir são duas funções

$$esq, dir : B \longrightarrow B \setminus \{b_0\} \cup \{\bigcirc\},$$

em que $\bigcirc$ é um símbolo especial (chamado símbolo *terminal*) que não está em B. As duas funções esq e dir são injetivas a menos de $\bigcirc$. Isto é, se $f \in \{esq, dir\}$ e $f(x) = f(y)$ então $r=y$ ou $f(x) = f(y) = \bigcirc$.

Uma maneira pictorial conveniente de se apresentar uma árvore binária é mostrada abaixo.



Esta figura é uma maneira auto-explicativa de representar a seguinte árvore binária:

$$B = \{b_0, z, y, u, v, r, s, v, t, n\}$$

x	esq(x)	dir(x)
b_0	z	y
z	u	v
y	r	s
u	$\bigcirc$	$\bigcirc$
v	$\bigcirc$	$\bigcirc$
r	m	t
s	$\bigcirc$	n
m	$\bigcirc$	$\bigcirc$
t	$\bigcirc$	$\bigcirc$
n	$\bigcirc$	$\bigcirc$

A representação pictorial acima é a maneira mais natural de se pensar numa árvore binária.

Duas árvores binárias são consideradas equivalentes se existe uma bijeção β entre os conjuntos bases que comute com as funções dir e esq, ou seja,

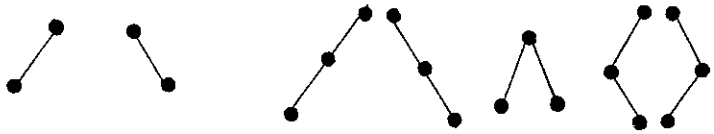
$$\beta(esq(x)) = esq(\beta(x))$$

$$\beta(dir(x)) = dir(\beta(x))$$

para todo elemento x de uma das árvores. O nosso problema é calcular o número b_n de árvores binárias não equivalentes com n elementos em seu conjunto base.

É fácil verificarmos por exemplo que

$$b_1 = 1,\ b_2 = 2,\ b_3 = 5 :$$

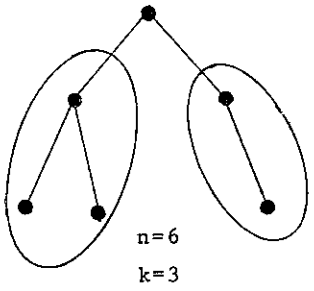


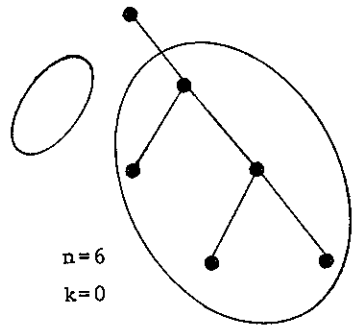
Estes primeiros valores sugerem que os números b_n's satisfazem $b_{n-1} = c_n$. E isto, na realidade, é verdade.

(I.3.c) PROPOSIÇÃO: O número de árvores binárias com n elementos, b_n, é o (n+1)-ésimo número de Catalão, isto é

$$b_{n-1} = c_n = \frac{1}{n}\binom{2n-2}{n-1},\ n\geq 1.$$

PROVA: Uma vez mais a definição $b_0=c_1=1$ é conveniente. Quando deletamos a raiz de uma n-árvore binária, obtemos duas sub-árvores, uma à esquerda com k, $0\leq k\leq n-1$, elementos e outra à direita com n-k-1 elementos. Veja figura abaixo.





Observe que para $k=0$ e $k=n-1$ temos o caso degenerado de sub-árvores sem elementos, e simplifica a nossa análise convencionarmos $b_0=1$.

Dizemos que uma n-árvore binária é de *tipo k* se k é o número de elementos da sub-árvore à esquerda quando a sua raiz é deletada. Evidentemente o número de n-árvores binárias de tipo k é

$$b_k \cdot b_{n-k-1}$$

e como k pode variar entre 0 e n-1 obtemos,

$$b_n = \sum_{k=0}^{n-1} b_k \cdot b_{n-k-1}.$$

Seja $c'_n = b_{n-1}$ para $n \geq 1$. Reescrevendo a equação acima obtemos

$$c'_{n+1} = c'_1 \cdot c'_n + c'_2 c_{n-2} + \ldots + c'_n \cdot c'_1.$$

Como $c'_1 = c_1$ e os números de Catalão verificam a mesma recorrência, obtemos $c'_n = c_n$ para todo n.

Assim,

$$b_{n-1} = c_n = \frac{1}{n} \binom{2n-2}{n-1},$$

concluindo a prova da proposição. □

Note o fato curioso que a translação de uma unidade nos índices é negativa (em relação aos t_n's): $b_{n-1} = c_n = t_{n+1}$.

NOTAS

Equações funcionais do tipo encontrado nesta seção,

$$f^2(x) - f(x) + x = 0,$$

são muito comuns em enumeração. A técnica mais empregada para se extrair coeficientes destas equações é baseada no teorema de Lagrange para funções implícitas. Uma forma conveniente deste teorema, onde as condições de derivabilidade e analiticidade são implícitamente assumidas é

(I.3.d) TEOREMA: Sejam x e y variáveis relacionadas por

$$y = x\, g(y) + a,$$

onde g é uma função dada e a é uma constante. Seja $f(y)$ uma outra função. Então temos

$$f(y) = f(a) + \sum_{n>1} \frac{x^n}{n!} \left[\frac{d^{n-1}}{dz^{n-1}} \{ f'(z)\, g^n(z) \} \right]_{z=a} . \quad \square$$

Note que em

$$y = x.g(y) + a$$

y é uma função implícita de x, e em particular, tomando f=identidade, o teorema acima nos permite explicitar y em série de potências de x.

Neste texto quase não fazemos uso deste teorema, porém queremos frisar o fato de que ocupa posição de destaque como técnica enumerativa. Damos apenas um exemplo de aplicação do mesmo.

(I.3.e) EXEMPLO: Seja $y = x\, e^y$. Encontre y como série de potên

cias de x. Isto é uma aplicação rotineira do teorema acima. Fazendo

$$\begin{aligned} a &= 0 \\ y &= y \\ x &= x \\ g(y) &= e^{y} \\ f(x) &= x \end{aligned}$$

obtemos

$$y = \sum_{n\geq 1} \frac{x^n}{n!} \left[\frac{d^{n-1}}{dz^{n-1}} \{ 1 . e^{nz} \} \right]_{z=0}$$

$$= \sum_{n\geq 1} \frac{x^n}{n!} n^{n-1} .$$

Na realidade, a equação $y = x\, e^{y}$ aparece do problema de enumerar um tipo especial de estrutura, chamada de árvore enraizada com rótulos, de que tratamos na subseção de (II.4) sobre árvores rotuladas. Para uma prova inteiramente combinatorial da fórmula de Lagrange referimos o leitor a [TU 2].

Um aspecto tangencial que queremos mencionar agora relaciona-se com a escolha da ordem em que os produtos parciais devem ser efetuados num produto de n fatores. Vamos mostrar que no caso de matrizes, por exemplo, uma escolha conveniente dessa ordem pode poupar uma tremenda quantidade de trabalho.

Para se multiplicar uma matriz de ordem $p \times q$ por uma matriz de ordem $q \times r$ são requeridos, pelo algorítmo usual, da ordem de pqr operações básicas (somas e multiplicações de números). O exemplo seguinte aparece em [AH 1]. Considere o produto de quatro matrizes

$$M = \underset{(10\times 20)}{M_1} \times \underset{(20\times 50)}{M_2} \times \underset{(50\times 1)}{M_3} \times \underset{(1\times 100)}{M_4} .$$

Calcular M na ordem $M_1 \times (M_2 \times (M_3 \times M_4))$ requer cerca de 125000.k operações básicas, para alguma constante k. No entanto, avaliando M na ordem $(M_1 \times (M_2 \times M_3)) \times M_4$ apenas cerca de 2200 k operações básicas são requeridas, para a mesma constante k.

Com 4 matrizes existem apenas 5 possibilidades para o cálculo do produto e podemos facilmente escolher a melhor. O que fazer no caso de, por exemplo, 12 matrizes quando existem

$$c_{12} = 58786$$

possibilidades? Felizmente uma técnica que evita de maneira inteligente a resolução do mesmo subproblema mais de uma vez, conhecida como programação dinâmica, permite uma avaliação "rápida" (da ordem de O(n)) da maneira ótima de se efetuar o produto. Veja [AH 1, pgs 67-69].

I.4 - SEQÜÊNCIAS "SOBE-DESCE": FUNÇÃO GERADORA EXPONENCIAL

A *função geradora exponencial* da seqüência

$$(a_0, a_1, a_2, \ldots)$$

é a função

$$a(z) = \sum_{n \geq 0} a_n \frac{z^n}{n!} ,$$

onde z é uma variável complexa, ou uma variável formal de algum anel comutativo com elemento 1. A princípio $\sum_{n \geq 0} a_n z^n$ "codifica" $a(z)$ tão bem quanto $\sum_{n \geq 0} a_n \frac{z^n}{n!}$ com a vantagem de ser mais simples. Porém, a introdução de fatoriais no denominador interage muito bem com a operação de "tomar subconjuntos" Isto fica claro no exemplo que tratamos em seguida. Em conseqüência, para problemas "rotulados" a função geradora exponencial é a adequada. Vejamos agora como estas funções geradoras podem ser utilizadas na solução de um problema.

Dentre as 24 sequências com símbolos distintos de (1,2,3,4) existem 5 em que os números se alternam crescendo e decrescendo:

(1,3,2,4) (1,4,2,3) (2,3,1,4) (2,4,1,3) e (3,4,1,2).

Para n=5 existem 16 seqüências deste tipo, que chamamos seqüências *sobe-desce*:

(1,3,2,5,4) (1,4,2,5,3) (1,4,3,5,2) (1,5,2,4,3)

(1,5,3,4,2) (2,3,1,5,4) (2,4,1,5,3) (2,4,3,5,1)

(2,5,1,4,3) (2,5,3,4,1) (3,4,1,5,2) (3,4,2,5,1)

(3,5,1,4,2) (3,5,2,4,1) (4,5,1,3,2) (4,5,2,3,1)

O problema que resolvemos nesta seção, para ilustrar o

uso das funções geradoras exponenciais, é o de determinar o número a_n de seqüências sobe-desce com base no conjunto

$$N = \{1,2,\ldots,n\}.$$

Este problema foi resolvido por um francês no século passado: D. André [Jour. de Math. (3) 7 (1881), 167-184]. A forma de sua resposta exemplifica uma destas conexões supreendentes que constituem marca registrada de beleza em matemática.

É conveniente separar o problema em 2 casos, conforme n seja par ou ímpar. Chamemos de $f(x)$ a função geradora exponencial para o número de seqüências sobe-desce com n ímpar, e $g(x)$ o mesmo com n par. Assim,

$$f(x) = \sum_{n\geq 0} a_{2n+1} \frac{x^{2n+1}}{(2n+1)!}$$

$$g(x) = \sum_{n\geq 0} a_{2n} \frac{x^{2n}}{(2n)!}.$$

Para encaixar as expressões acima na definição que demos de funções geradoras, assumimos implicitamente que os coeficientes de potências pares de f e de potências ímpares de g valem zero.

CASO ÍMPAR

Vamos primeiro encontrar $f(x)$. Começamos definindo a_1 como sendo 1, pois isto simplifica a notação na análise que se segue. (Além disso é razoável dizermos que a única permutação de $\{1\}$ é do tipo sobe-desce.) Considere uma seqüência sobe-desce com base em

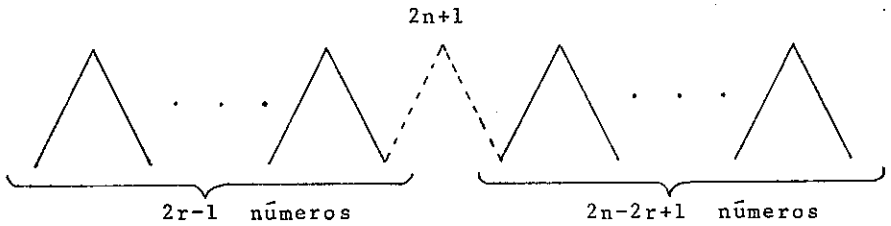
$$N_{imp} = \{1,2,\ldots,n,\ldots,2n+1\},$$

onde $n>1$ e suponha que $2n+1$ ocorre na $(2r)$-ésima posição. Note que $2n+1$ tem de aparecer numa posição de índice par. Se consi-

derarmos os $2r-1$ primeiros números e os $2n-2r+1$ últimos notamos que ambas as subseqüências consecutivas são permutações do tipo sobe-desce de dois subconjuntos complementares de

$$N_{imp} \setminus \{2n+1\}.$$

A figura abaixo ilustra a situação



Observe que os números a_{2r-1}'s que buscamos são independentes do fato de usarmos os "rótulos" $\{1,2,\ldots,2r+1\}$ para denotar os elementos. Assim, se $R \subseteq N_{imp} \setminus \{2n+1\}$ e $|R| = 2r-1$, podemos formar a_{2r-1} seqüências sobe-desce com base em R. Logo para cada bipartição de $N_{imp} \setminus \{2n+1\}$ onde as classes têm $2r-1$ e $2n-2r+1$ elementos podemos formar

$$a_{2r-1} \cdot a_{2n-2r-1}$$

seqüências sobe-desce de N_{imp} com $2n+1$ ocorrendo na $(2r)$-ésima posição. Claro que todas estas permutações são distintas, porque se a bipartição muda, os rótulos são diferentes para se formar as subseqüências componentes. Observe aqui que a definição $a_1=1$ é necessária para o produto acima englobar os casos $r=1$ e $r=n$.

O número total de seqüências sobe-desce com base em N_{imp} nas quais $2n+1$ ocorre na $(2r)$-ésima posição é portanto

$$\binom{2n}{2r-1} a_{2r-1} \cdot a_{2n-2r+1},$$

onde o coeficiente binomial dá conta do número de bipartições de $N_{imp} \setminus \{2n+1\}$ onde as classes têm $2r-1$ e $2n-2r+1$ elementos.

Somando as diversas possibilidades para r obtemos a recorrência

$$a_{2n+1} = \sum_{r=1}^{n} \binom{2n}{2r-1} a_{2r-1} \cdot a_{2n-2r+1}.$$

Note agora a importância de usarmos a função geradora de tipo exponencial para este problema: ao computarmos o quadrado de f re-obtemos a recorrência acima. Isto graças à interação entre os fatoriais "impostos" e o coeficiente binomial que conta sub-conjuntos.

$$f^2(x) = \sum_{n\geq 1} \left[\sum_{r=1}^{n} \left(a_{2r-1} \frac{x^{2r-1}}{(2r-1)!} \right) a_{2n-2r+1} \left(\frac{x^{2n-2r+1}}{(2n-2r+1)!} \right) \right]$$

$$= \sum_{n\geq 1} \left[\sum_{r=1}^{n} \binom{2n}{2r-1} a_{2r-1}\, a_{2n-2r+1} \right] \frac{x^{2n}}{(2n)!}.$$

E como a soma interna é precisamente o valor de a_{2n+1}, pela recorrência obtida, podemos escrever

$$f^2(x) = \sum_{n\geq 1} a_{2n+1} \frac{x^{2n}}{(2n)!}.$$

Esta expressão lembra em tudo a derivada de f que é

$$f'(x) = \sum_{n\geq 0} a_{2n+1} \frac{x^{2n}}{(2n)!}.$$

Como $a_1 = 1$, obtemos a seguinte equação diferencial:

$$f'(x) = 1 + f^2(x).$$

Podemos integrar esta equação diferencial e obter

$$\text{arctg}(f(x) = x + C,$$

onde a constante C vale um múltiplo de π, uma vez que da nossa definição $f(0) = 0$, do que segue $\text{arctg}(0) = C$, isto é, $C = k\pi$ para algum $k \in Z$. Invertendo as funções obtemos

$$f(x) = \text{tg}(x+k\pi) = \text{tg}(x).$$

E assim podemos enunciar

(I.4.a) PROPOSIÇÃO: O número a_{2n+1} de seqüências sobe-desce com base em $N_{imp} = \{1,2,\ldots,2n+1\}$ é

$$a_{2n+1} = \left[x^{2n+1}\right] \{(2n+1)!\ \text{tg}(x)\}. \quad \square$$

Este resultado é, para dizer pouco, inesperado. Vamos agora rumo à uma segunda surpresa com a determinação de $g(x)$, função geradora exponencial para os números de seqüências sobe-desce em $N_{par} = \{1,2,\ldots,2n\}$. Nas notas desta seção explicamos rapidamente como se pode extrair coeficientes de $f(x) = \text{tg}(x)$.

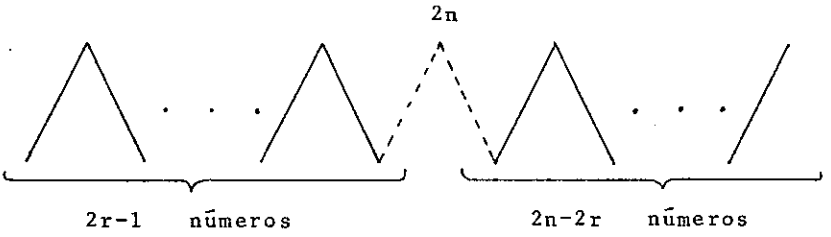
CASO PAR

Recorde que $g(x)$ foi definida como

$$g(x) = \sum_{n\geq 0} a_{2n} \frac{x^{2n}}{(2n)!},$$

onde os coeficientes de potências ímpares de x valem zero. Desta vez é conveniente, para simplificar as notações, definirmos a_0 como sendo 1, embora seja desprovido de sentido falarmos no número de seqüências sobe-desce com base num conjunto com 0 elementos.

O procedimento de análise é análogo ao do caso ímpar. Veja figura abaixo



Assuma que $2n$ ocorre na $(2r)$-ésima posição de uma seqüência sobe-desce com base em N_{par}. Então os primeiros $2r-1$ elementos formam uma seqüência sobe-desce com base em algum subconjunto de cardinalidade $2r-1$ de $N_{par} \setminus \{2n\}$ e os últimos $2n-2r$ elementos formam uma seqüência sobe-desce com base no complemento em relação a $N_{par} \setminus \{2n\}$ do primeiro subconjunto.

Pelo mesmo argumento do caso anterior quando determinamos $f(x)$, temos que o número de seqüências sobe-desce com base em N_{par} onde $2n$ aparece na posição de índice $2r$ é

$$\binom{2n-1}{2r-1} a_{2r-1} \cdot a_{2n-2r}.$$

Note aqui que a definição $a_0=1$ é necessária para a expressão acima englobar o caso $r=n$.

Notando que $2n$ pode aparecer nas posições: $2,4,\ldots,2n$, encontramos a recorrência

$$a_{2n} = \sum_{r=1}^{n} \binom{2n-1}{2r-1} a_{2r-1} \cdot a_{2n-2r}.$$

Consideremos agora o produto de f e g.

$$f(x) \cdot g(x) = \left(\sum_{n \geq 1} a_{2n-1} \frac{x^{2n-1}}{(2n-1)!} \right) \left(\sum_{n \geq 0} a_{2n} \frac{x^{2n}}{(2n)!} \right)$$

$$= \sum_{n\geq 1} \left[\sum_{r=1}^{n} \left(a_{2r-1} \frac{x^{2r-1}}{(2r-1)!} \right) \left(a_{2n-2r} \frac{x^{2n-2r}}{(2n)!} \right) \right]$$

$$= \sum_{n\geq 1} \left[\sum_{r=1} \binom{2n-1}{2r-1} a_{2r-1} \, a_{2n-2r} \right] \frac{x^{2n-1}}{(2n-1)!}.$$

Note, uma vez mais, que a terceira igualdade só foi possível pela interação entre os fatoriais impostos nas funções geradoras exponenciais e o coeficiente binomial. Pela recorrência obtida acima podemos escrever

$$f(x) \cdot g(x) = \sum_{n\geq 1} a_{2n} \frac{x^{2n-1}}{(2n-1)!}.$$

A expressão à direita lembra a derivada de g e, na realidade, é exatamente igual a esta. Assim,

$$g'(x) = f(x) \cdot g(x).$$

Como já sabemos que $f(x) = tg(x)$,

$$\frac{g'(x)}{g(x)} = tg(x),$$

o que integrando nos dá

$$\ell n(g(x)) = \int tg(x)dx = \ell n(\sec(x)) + C.$$

Para determinar o valor da constante C considere $x=0$. Temos $g(0) = a_0 = 1$; portanto,

$$\ell n(1) = \ell n(\sec(0)) + C$$

$$0 = \ell n(1) + C$$

implicando $C=0$.

Desse modo $\ell n(g(x)) = \ell n(\sec(x))$, e exponenciando obtemos

$$g(x) = \sec(x).$$

Podemos assim enunciar

(I.4.b) PROPOSIÇÃO: O número a_{2n} de seqüências sobe-desce com base em $N_{par} = \{1,2,\ldots,2n\}$ é

$$a_{2n} = \left[x^{2n}\right] \{(2n)!\ \sec(x)\}. \qquad \square$$

A proposição acima é também, sem dúvidas, bem inesperada. Relembre que, por definição, os coeficientes de potências pares de x na expansão de $f(x)$ se anulam. Assim temos que a expansão de $tg(x)$ não tem potências pares. Considerando $g(x)$ temos também que a expansão de $\sec(x)$ não tem potências ímpares. Esses fatos são bem conhecidos. Dessa forma, há uma disjunção completa entre os casos ímpar e par e podemos unificá-los simplesmente somando as suas funções geradoras exponenciais.

(I.4c) PROPOSIÇÃO: O número a_n de seqüências sobe-desce com base em $N = \{1,2,\ldots,n\}$ é

$$a_n = \left[x^n\right] \{n!\ (tg(x) + \sec(x))\}. \qquad \square$$

Para concluir esta seção vamos falar rapidamente sobre a extração dos coeficientes acima.

NOTAS

A expansão explícita da função tangente em série de Taylor é uma expressão bastante complicada envolvendo os chamados números de Bernoulli, B_{2n}:

$$tg(x) = \sum_{n\geq 1} \left[\frac{(1)^{n-1}\ 2^{2n}\ (2^{2n}-1)\ B_{2n}}{2n}\right] \frac{x^{2n-1}}{(2n-1)!}.$$

A expansão similar da secante é um pouco mais simples, e é expressa em termos dos números de Euler, E_{2n}.

$$\sec x = \sum_{n\geq 0} \left[(-1)^n E_{2n}\right] \frac{x^{2n}}{(2n)!} .$$

Os números de Bernoulli e de Euler podem ser calculados a partir de certos polinômios com os mesmos nomes. Para cada natural $n\geq 0$ existem polinômios de grau n $B_n(x)$ e $E_n(x)$ chamados respectivamente de n-ésimo polinômio de Bernoulli e n-ésimo polinômio de Euler. O n-ésimo número de Bernoulli é definido como

$$B_n = B_n(0).$$

O n-ésimo número de Euler é definido como

$$E_n = 2^n E_n(1/2).$$

Finalmente, os polinômios $B_n(x)$ e $E_n(x)$ são definidos pelas seguintes funções geradoras (exponenciais em t):

$$\frac{te^{xt}}{e^t-1} = \sum_{n\geq 0} B_n(x) \frac{t^n}{n!}$$

$$\frac{2e^{xt}}{e^t-1} = \sum_{n\geq 0} E_n(x) \frac{t^n}{n!} .$$

Pode-se observar portanto que, apesar da fórmula elegante obtida, é uma tarefa laboriosa se explicitar os números a_n's de seqüências sobe-desce com base em N. Nos exercícios 15 e 16 deste capítulo recorrências diretas para os números de Bernoulli e de Euler, sem necessidade de computar os polinômios respectivos, sao consideradas.

Os primeiros termos da expansão de $tg(x) + sec(x)$ são

$$1 + x + \frac{x^2}{2!} + 2\,\frac{x^3}{3!} + 5\,\frac{x^4}{4!} + \frac{16x^5}{5!} + \frac{61x^6}{6!} + \frac{272x^7}{7!} + \ldots$$

EXERCÍCIOS

1. Qual é a função geradora para a seqüência dos quadrados

$$(0,1,4,9,16 \ \ldots\ ) \ ?$$

2. Qual é a função geradora para a seqüência $(2,9,53,351,\ldots)$ onde $a_n = 2^n + 7^n$?

3. Os *números de Lucas*, L_n's, são definidos a partir da recorrência

$$L_n = L_{n-1} + L_{n-2} \ , \ n \geq 3$$

onde $L_1 = 1$ e $L_2 = 3$. Prove que

$$L_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n \ .$$

4. Mostre que os números de Lucas e Fibonacci satisfazem:

$$L_n = F_{n-1} + F_n$$
$$F_{2n} = L_n \cdot F_n$$

e tente encontrar um significado combinatorial para estas identidades.

5. Mostre que o n-ésimo número de Fibonacci satisfaz

$$2^n F_n = 2 \sum_{k \text{ ímpar}} \binom{n}{k} 5^{\frac{k-1}{2}} \ .$$

6. Prove que a equação diofantina

$$5x^2 \pm 4 = y^2$$

tem soluções em inteiros apenas quando x é um número de Fibonacci e y é o número de Lucas de índice correspondente.

7. *O Sistema Numérico de Fibonacci*: Mostre que todo inteiro positivo m tem uma única representação

$$m = F_{k_1} + F_{k_2} + \ldots + F_{k_r},$$

onde $k_i \geq k_{i+1}+2$ para $r=1,2,\ldots,r-1$ e $k_r \geq 2$.

8. Considere o seguinte jogo de fichas para 2 pessoas. Começa-se com n fichas. O primeiro jogador em sua primeira jogada pode retirar qualquer número de fichas exceto o número total n. Daí por diante cada jogador deve retirar um número entre 1 e o dobro do número de fichas retiradas pelo adversário na jogada anterior. O jogador que não deixa fichas ao oponente é o vencedor.

   (a) Prove que o primeiro jogador tem sempre uma estratégia vitoriosa, exceto no caso em que n é um número de Fibonacci, caso em que o segundo jogador tem a vitória assegurada, se jogar certo.

   (b) Qual é o único lance ganhador para n=800?
   (Sugestão: Considere o sistema numérico de Fibonacci, mencionado no problema acima.

9. Prove que o número de palavras em três letras {a,b,c} de comprimento n e sem a's consecutivos é

$$p_n = \left(\frac{2+\sqrt{3}}{2\sqrt{3}}\right)(1+\sqrt{3})^n + \left(\frac{-2+\sqrt{3}}{2\sqrt{3}}\right)(1-\sqrt{3})^n, \quad n \geq 1.$$

(Sugestão: mostre que p_n satisfaz a recorrência

$$p_n = 2p_{n-1} + 2p_{n-2}.$$

10. Resolva a seguinte recorrência não homogênea

$$a_n + 2a_{n-1} + a_{n-2} = 2^n.$$

(Sugestão: A solução geral destas recorrências é a soma da solução da homogênea associada com uma solução particular encontrada por tentativa. Tente uma solução da forma $k.2^n$.)

11. Considere a seqüência $(a_0, a_1, \ldots)$ que começa com $(1,0,\ldots)$ e satisfaz a partir do termo de ordem 2,

$$a_n = a_{n-1} - a_n.$$

Verifique que

$$a_n = \cos \frac{n\pi}{3} + \frac{1}{\sqrt{3}} \operatorname{sen} \frac{n\pi}{3}.$$

Como podemos chegar a esta expressão do Teorema (I.2.a)?
(Sugestão: Use coordenadas polares.)

12. Encontre o número de seqüências binárias com n dígitos que contêm precisamente um par de 1's consecutivos.
(Sugestão: considere primeiro o número de seqüências sem pares de 1's consecutivos; a seguir encontre uma recorrência e resolva-a dando a fórmula para o n-ésimo termo.)

13. Uma moeda é jogada $2n$ vezes. Em quantas das 2^{2n} seqüências de possibilidades o número de caras e de coroas será igual pela primeira vez depois das $2n$ jogadas?

(Resposta: $2c_n$)

14. Obtenha os números de Catalão com a aplicação da Fórmula de Lagrange dada em (I.3.d) à equação funcional

$$f^2 - f + x = 0.$$

(Sugestão: faça $f=xy$.)

15. Os números de Bernoulli $B_0, B_1, B_2, \ldots$ podem ser diretamente definidos pela relação de recorrência

$$B_n = \sum_{k=0}^{n} \binom{n}{k} B_{n-k} \quad , \quad n \geq 1$$

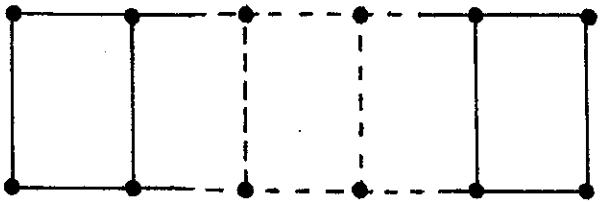
onde $B_0=1$.

(a) Calcule $B_0, B_1, B_2, \ldots, B_{10}$

(b) Mostre que a função geradora exponencial para esta seqüência é t/e^t-1.

16. Encontre uma recorrência para os números de Euler definidos nas notas da sec(I.4).
(Sugestão: observe que a função geradora do exercício anterior é obtida fazendo $x=0$ na expressão para a função geradora exponencial dos polinômios de Bernoulli $B_n(x)$. Encontre de maneira análoga a função geradora exponencial para os números de Euler e extraia uma recorrência desta função geradora.)

17. De quantas maneiras distintas podemos emparelhar vértices adjacentes no grafo "escada" abaixo de maneira que não sobrem vértices desemparelhados?



n degraus

18. Qual é o número de permutações π de $\{1,2,\ldots,n\}$ tendo a propriedade de que

$$|\pi(i) - i| \leq 1 \quad (i=1,2,\ldots n)?$$

Em que sentido este problema é o mesmo anterior?

19. Seja B_n o número de partições de um conjunto finito N onde $|N| = n$. Tente mostrar que a função geradora exponencial para

P_n é (onde $P_0=1$)

$$B(x) = e^{(e^x-1)}.$$

(NOTA: os números B_n's são conhecidos por *números de Bell*. Com o conceito de "prefabs exponenciais" que estudamos adiante no capítulo III esta expressão para $B(x)$ é fácilmente obtida.)

20. Generalize a base do método apresentado para calcular o número de seqüências sobe-desce provando o seguinte resultado: Suponha que $f(x)$ e $g(x)$ são funções geradoras exponenciais para o número de certas "estruturas com rótulos" $E_1(A)$ e $E_2(B)$ nos conjuntos disjuntos de rótulos A e B respectivamente. Se $v \notin A \cup B$ e se existe uma bijeção entre $E_1(A) \times E_2(B)$ e $E_0(A \cup B \cup \{v\})$ (onde E_0 é uma terceira estrutura) então a derivada da função geradora exponencial para $E_0(A \cup B \cup \{v\})$ é o produto $f(x).\ g(x)$.

CAPÍTULO II

COMPOSIÇÃO COMBINATORIAL : PREFABS

II.1 - PREFABS SIMPLES E TEOREMA MULTIPLICATIVO

No capítulo I nossa estratégia geral para resolver um problema de enumeração pode ser sintetizada como

Problema ⟹ Recorrência ⟹ Função Geradora ⟹ Coeficientes.

Neste capítulo mostramos que em grande número de problemas a abordagem mais conveniente inverte os dois ítens intermediários acima:

Problema ⟹ Função Geradora ⟹ Recorrência ⟹ Coeficientes.

A maneira adequada de conduzir tal estratégia é através de uma estrutura abstrata chamada "prefab" pelos seus formalizadores; veja [BG 1 - 1971]. A seguir definimos esta estrutura (num caso particular) e provamos um teorema multiplicativo do qual funções geradoras de inúmeros problemas de contagem emergem cristalinas.

Encontrar uma recorrência a partir das funções geradoras pode ser difícil, porém encontrá-la diretamente a partir do problema, é em muitos casos, literalmente impossível. Ilustramos este ponto com os exemplos de partições numéricas e árvores com raiz.

PREFABS SIMPLES (DE COMPOSIÇÃO ÚNICA)

Sejam C um conjunto (no máximo enumerável), A um anel contendo os racionais e

$$\pi: C \longrightarrow A$$

uma função chamada *peso*. Se $X \subseteq C$ o *inventário* de X com respeito ao peso π é definido por

$$\mathrm{Inv}_{\pi}(X) = \sum_{x \in X} \pi(x).$$

Por exemplo, seja C a coleção dos subconjuntos de um

subconjunto finito dado. Seja A o anel $Q[x]$. Se atribuirmos a um membro de C um peso igual a x^k onde k é a sua cardinalidade, o coeficiente de x^k em $Inv_\pi(X)$ nos diz quantos subconjuntos de cardinalidade k estão presentes em X. O inventário de um subconjunto com respeito a uma funçao peso tem sua motivação original na idéia de função geradora, mas, como vemos a seguir, é bem mais geral. A informação, via coeficientes, que o inventário de um subconjunto nos dá é, para cada peso p_α, quantos elementos com peso p_α existem em A.

Vamos sempre supor que existe em C uma operação binária "o", chamada *composição*:

$$o: C \times C \longrightarrow C.$$

Definimos um primo em C como um elemento $p \in C$, $p \neq e$, tal que

$$p = a \circ b \quad \text{implica} \quad p=a \quad \text{ou} \quad p=b.$$

A terna ordenada (C, o, π) é chamado um *prefab simples* se os seguintes axiomas são verificados:

(i) a composição o é associativa e comutativa;

(ii) existe em C um elemento neutro e para o, isto é, $a \circ e = e \circ a = a$ para todo a em C;

(iii) cada x em C tem uma única (a menos de ordem) fatorização finita em primos

$$x = p_1^{n_1} \circ p_2^{n_2} \circ \ldots \circ p_k^{n_k}.$$

(iv) Se x e y são *coprimos*, isto é, a interseção do conjunto de primos da fatorização de x com o da fatorização de y é vazia, então

$$\pi(x \circ y) = \pi(x).\ \pi(y).$$

O teorema seguinte é, embora de prova direta, muito importante.

(II.1.a) TEOREMA MULTIPLICATIVO. Seja (C,o,π) um prefab simples e X e Y subconjuntos de C tais que se $x \in X$ e $y \in Y$ então x e y são coprimos. Então

$$Inv_{\pi}(X \circ Y) = Inv_{\pi}(X).\ Inv_{\pi}(y).$$

PROVA: Note que na equação acima $X \circ Y \subseteq C$, pois

$$X \circ Y = \{x \circ y : x \in X \text{ e } y \in Y\};$$

além disso o produto à direita é simplesmente o produto de elementos, $Inv_{\pi}(X)$ e $Inv_{\pi}(Y)$, do anel A, contradomínio de π.

Inicialmente mostramos que cada $z \in X \circ Y$ é escrito de maneira única como um produto $z=x \circ y$, onde $x \in X$ e $y \in Y$. Pela definição de $X \circ Y$ existem $x \in X$ e $y \in Y$ tais que $z=x \circ y$. Suponhamos que $x' \in X$ e $y' \in Y$ satisfaçam $x \circ y = x' \circ y'$. Sejam

$$x = \overset{\circ}{\prod} p_i^{k_i} \qquad y = \overset{\circ}{\prod} q_i^{\ell_i}$$

$$x' = \overset{\circ}{\prod} r_i^{m_i} \qquad y' = \overset{\circ}{\prod} s_i^{n_i}$$

as fatorizações de x,y,x',y'. Pela hipótese assumida sabemos que

$$\left(\overset{\circ}{\prod} p_i^{k_i}\right) \circ \left(\overset{\circ}{\prod} q_i^{\ell_i}\right) = \left(\overset{\circ}{\prod} r_i^{m_i}\right) \circ \left(\overset{\circ}{\prod} s_i^{n_i}\right).$$

Como tanto x e y quanto x' e y' são primos entre si deduzimos que nenhum p_i é igual a algum q_j e que nenhum r_i é igual a algum s_j. Logo pela unicidade da fatorização de $x \circ y$, a menos de ordem, os p_i's são iguais aos r_i's e os q_i's são iguais aos s_i's. Assim $x=x'$ e $y=y'$. A conclusão da prova é agora imediata.

$$Inv_{\pi}(X \circ Y) = \sum_{z \in X \circ Y} \pi(z)$$

$$= \sum_{x \in X} \sum_{y \in Y} \pi(x \circ y).$$

Pelo terceiro axioma, uma vez que x e y são coprimos, obtemos

$$\mathrm{Inv}_\pi(X \circ Y) = \sum_{x \in X} \sum_{y \in Y} \pi(x) \cdot \pi(y)$$

$$= \sum_{x \in X} \pi(x) \sum_{y \in Y} \pi(y)$$

$$= \mathrm{Inv}_\pi(X) \cdot \mathrm{Inv}_\pi(Y),$$

o que conclui a prova. □

O próximo teorema é, na realidade um corolário do anterior, e é bastante útil nas aplicações.

(II.1.b) TEOREMA BÁSICO. Seja $(C,\circ,\pi)$ um prefab simples e P o conjunto dos primos de C. Então

$$\mathrm{Inv}_\pi(C) = \prod_{p \in P} \frac{1}{1-\pi(p)}.$$

PROVA: Considere para cada primo p_k o conjunto

$$P_k = \{ e, p_k, p_k^2, p_k^3, \ldots \}.$$

Note que $C = \overset{\circ}{\prod_k} P_k$ onde k indexa os primos de C. Além disso $P_j \neq P_k$ implica obviamente que P_j e P_k estão nas condições do teorema multiplicativo anterior. Observe que cada parcela da expansão do produto acima contém apenas uma quantidade finita de fatores distintos de e. Assim obtemos, com a aplicação, de no máximo uma quantidade enumerável de vezes, do teorema multiplicativo (II.1.a),

$$\mathrm{Inv}_{\pi}(C) = \prod_{k} \mathrm{Inv}_{\pi}(P_k)$$

$$= \prod_{p \in P} (1 + \pi(p) + \pi(p^2) + \ldots)$$

$$= \prod_{p \in P} \frac{1}{1-\pi(p)},$$

o que conclui a prova. □

(II.1.c) EXEMPLO : PARTIÇÕES NUMÉRICAS. Uma partição de um inteiro positivo n é uma representação de n como a soma de inteiros positivos e onde a ordem não é levada em conta. Por exemplo, existem 7 partições do número 5: 5,4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1 e 1+1+1+1+1. Determine o número p_n de partições de n.

Vamos definir um prefab simples no conjunto S das seqüências finitas não crescentes de inteiros positivos. Note que estas seqüências estão em bijeção natural com o conjunto das partições numéricas. Por exemplo

$$(5,3,3,2,1,1)$$

corresponde à partição

$$5+3+3+2+1+1$$

do número 15.

O peso π de um elemento em S é definido como x^n, onde n é a soma das coordenadas da seqüência. A composição a o b com a,b∈ S é a justaposição das seqüências a e b seguida da classificação em ordem não crescente da seqüência resultante. Assim

$$(5,3,2,2,1) \text{ o } (7,4,2,2,2)$$

dá como resultado

$$(7,5,4,3,2,2,2,2,2,1).$$

Como pode ser trivialmente verificado pelo leitor, (S,o,π) é um prefab simples onde o conjunto P de primos é formado pelas seqüências de comprimento 1. O elemento neutro é a seqüência vazia. Além disso segue das definições que o inventário de S é a função geradora (ordinária) para as partições numéricas. Aplicando o teorema (II.1.b) obtemos

$$\mathrm{Inv}_{\pi}(S) = \prod_{p \in P} \frac{1}{1-\pi(p)}$$

$$= \prod_{k \geq 1} \frac{1}{1-x^k},$$

e assim

$$p_n = \left[x^n\right] \prod_{k \geq 1} \frac{1}{1-x^k} =$$

$$= \left[x^n\right] \prod_{k=1}^{n} \frac{1}{1-x^k} .$$

Da função geradora $\prod_{k \geq 1} \frac{1}{1-x^k}$ podemos encontrar uma recorrência que permite o cálculo dos p_n's. Esta tarefa requer uma certa preparação e por isto a adiamos para a próxima seção. Damos a seguir uma outra aplicação dos prefabs simples.

(II.1.d) EXEMPLO: (IDENTIDADE PARA A FUNÇÃO ZETA DE RIEMMAN). Usamos agora a teoria de prefabs para dar uma prova simples da seguinte identidade clássica. Se $s \in \mathbb{C}$ e $\mathrm{Re}(s) > 1$,

$$\xi(s) = \sum_{n \geq 1} n^{-s} = \prod_{\text{primo}} \frac{1}{1-p^s} .$$

(ξ é uma função conhecida como função zeta de Riemman.) Este exemplo ilustra um novo tipo de função geradora, chamada de função geradora de Dirichilet. Para a seqüência $(a_1, a_2, \ldots)$ esta última vale

$$a(s) = \sum_{n \geq 1} a_n \, n^{-s}.$$

Como mostramos a seguir a escolha dessas funções nos é dada de maneira natural pela estrutura do problema e a manipulação das mesmas é justificada pela base abstrata oferecida pelos prefabs.

Para demonstrarmos a identidade construimos um prefab simples (θ, o, π) da seguinte maneira: θ é a classe de todos os submulticonjuntos finitos de primos. (Um multiconjunto é um conjunto onde elementos aparecem com multiplicidades.) Por exemplo

$$\{2,2,3,5,5,5\} \quad \text{ou} \quad \{2^2, 3^1, 5^3\},$$

é um elemento de θ.

A composição $F \circ G$ onde F e G são elementos de θ é a união de F e G, somando as multiplicidades. Assim,

$$\{2^1, 3^1, 5^3\} \circ \{2^5, 5^1, 7^3\} = \{2^7, 3^1, 5^4, 7^3\}.$$

O elemento neutro e é o multiconjunto vazio ϕ.

Espelhado no que queremos, definimos o peso π de um elemento F de θ como

$$\pi(F) = 1 \qquad \text{se } \theta = \phi$$

$$= \left(\prod_{x \in F} x \right)^{-s} \qquad \text{se } \theta \neq \phi.$$

(Note que o mesmo elemento $x \in F$ pode aparecer muitas vezes no produto acima, pois F é um multiconjunto.)

Dadas estas definições deixamos para o leitor o encargo de verificar que

$$(\theta, o, \pi)$$

é um prefab simples, onde os primos são os multiconjuntos da forma $\{p^1\}$, com p primo. Aplicando o teorema (II.1.b) obtemos para inventário de θ

$$Inv_{\pi}(\theta) = \prod_{p \text{ primo}} \frac{1}{1-p^{-s}}.$$

Se agora interpretamos o inventário de θ a partir da definição, obtemos que

$$Inv_{\pi}(\theta) = \sum_{n \geq 1} F_n \, n^{-s}$$

onde F_n é o número de elementos de θ com peso n^{-s}. O teorema fundamental da aritmética implica agora que cada um dos F_n's vale 1. Isto porque os elementos de θ estão em bijeção com as fatorizações dos números naturais em primos e assim, o número de elementos de θ com peso n^{-s} é o mesmo número de fatorizações de n em primos ou seja, vale 1. Desse modo concluímos

$$\sum_{n \geq 1} n^{-s} = \prod_{p \text{ primo}} \frac{1}{1-p^{s}},$$

para qualquer s para o qual a soma convirja.

II.2 - RECORRÊNCIA PARA PARTIÇÕES NUMÉRICAS

Nesta seção vamos extender ligeiramente o teorema (II.1.b) de forma a permitir a avaliaçao do inventário de certos subconjuntos especiais do conjunto base C de um prefab simples (C,o,π). Esta extensão é bastante útil pois esses subconjuntos especiais aparecem freqüentemente em aplicações. Ilustrando este ponto usamos, em seguida a extensão para encontrar uma recorrência para partições numéricas, tarefa que titula esta seção.

Considere um prefab simples (C,o,π) e, como temos feito, denotemos por P o conjunto dos seus primos. Seja também dada uma função

$$\alpha: P \longrightarrow 2^{\mathbb{N}}$$

que associa a cada primo um subconjunto de $\mathbb{N} = \{0,1,2,\ldots\}$ Seja C^{α} o subconjunto de C constituído pelos elementos $x \in C$ cuja fatorização

$$x = p_1^{k_1} \circ p_2^{k_2} \circ \ldots \circ p_n^{k_n}$$

satisfaça $k_i \in \alpha(p_i)$ para $i=1,2,\ldots,n$.

(II.2.a) EXTENSÃO DO TEOREMA BÁSICO. Sejam (C,o,π) um prefab simples, P o conjunto de seus primos e $\alpha: P \longrightarrow 2^{\mathbb{N}}$ uma função dada. Temos

$$Inv_{\pi}(C^{\alpha}) = \prod_{p \in P} \left(\sum_{j \in \alpha(p)} \pi(p^j) \right) .$$

PROVA: Note que se tomamos $\alpha(p) = \mathbb{N}$ para todo $p \in P$ então obtemos o teorema (II.a.b). Para cada $p_k \in P$ definamos

$$P_k^{\alpha} = \{ p_k^i : i \in \alpha(p_k) \}.$$

Observe que

$$C^{\alpha} = \prod_{k}^{o} p_k^{\alpha}.$$

Aplicando o teorema (II.1.a) obtemos

$$\mathrm{Inv}_{\pi}(C^{\alpha}) = \prod_{k} \mathrm{Inv}_{\pi}(p_k^{\alpha})$$

$$= \prod_{p \in P} \left(\sum_{j \in \alpha(p)} \pi(p^j) \right),$$

estabelecendo o teorema.□

LEMAS COMBINATORIAIS

Vamos agora usar a função geradora obtida para o exemplo (II.1.c) e a extensão provida pelo teorema anterior para obter uma recorrência que permita o cálculo efetivo dos p_n's. Como vemos a seguir isto depende de dois lemas. O primeiro deles é provado usando o teorema anterior.

(II.2.b) LEMA: A função geradora para a seqüência $(d_0, d_1, d_2, \ldots)$ onde $d_0 = 1$ e d_i, $i \geq 1$, é a diferença entre a quantidade de partições de n com um número par de partes distintas e a quantidade de partições de n com um número ímpar de partes distintas é

$$\prod_{n \geq 1} (1 - x^n).$$

PROVA: Note, antes de tudo que o produto acima é o inverso da função geradora das partições numéricas obtida no exemplo (II.1.c), donde a sua relevância para o cálculo dos p_n's.

Considere o prefab simples (S, o, π') onde S e o são os mesmos do exemplo (II.1.c) e π' é definido para $\alpha \in S$ com

$$\pi'(\sigma) = (-1)^k x^n,$$

onde k é o comprimento da seqüência σ e n é a soma de suas

coordenadas. Seja agora a função $\alpha: P \longrightarrow 2^{\mathbb{N}}$, onde P é o conjunto de primos de (S,o,π'), a função constante

$$\alpha(\{i\}) = \{0,1\}.$$

Aplicando o teorema (II.2a) obtemos

$$\begin{aligned} Inv_{\pi'}(S^{\alpha}) &= \prod_{p \in P} (\pi'(p^0) + \pi'(p^i)) \\ &= \prod_{i \geq 1} (1-x^i). \end{aligned}$$

A interpretação de $Inv_{\pi'}(S^{\alpha})$, que deve ser comprovada pelo leitor, é a seguinte. O conjunto S^{α} são as seqüências decrescentes correspondentes às partições numéricas com partes distintas. O peso de um elemento σ de S^{α} que tem soma n nas suas coordenadas é $\pm x^n$, e o sinal é positivo ou não dependendo da paridade do comprimento de σ. Assim $Inv_{\pi'}(S^{\alpha})$ é a função geradora da seqüência mencionada no enunciado do lema. Isto conclui a prova. □

A prova do lema seguinte requer um argumento combinatorial delicado

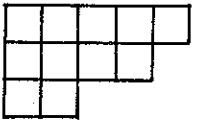
(II.2.c) LEMA: Seja e_n o número de partições de n em partes desiguais e com um número par de partes; seja i_n o número de partições de n em partes desiguais e com número ímpar de partes. Então

$$\begin{aligned} e_n &= i_n + (-1)^k, \text{ se existe } k \in Z : n = \frac{k}{2}(3k \pm 1) \\ &= i_n, \text{ se não existe } k \text{ como acima.} \end{aligned}$$

PROVA: A maneira mais simples de provar o lema é fazer uso dos chamados *diagramas de Ferrer* para representar partições numéricas. Por exemplo, a partição

$$(5,4,2)$$

de 11 tem para diagrama de Ferrer



Sejam para $n \geq 1$,

E_n o conjunto das partições de n em partes distintas e com uma quantidade par de partes.

I_n o conjunto das partições de n em partes distintas e com uma quantidade ímpar de partes.

Dada $\sigma \in E_n \cup I_n$ seja $k(\sigma)$ o número de partes de σ; seja também $s(\sigma)$ o tamanho da menor parte de σ; finalmente, seja $\ell(\sigma)$ o número máximo de elementos subsequentes a partir do primeiro da seqüência identificável com σ que estão em progressão aritmética de razão -1. Por exemplo, $s((5,4,2)) = 2$, $\ell((5,4,2)) = 2$. Outros exemplos, $\ell((6,5,4,2)) = 3$, $\ell((6,3,2,1)) = 1$.

Se for o caso de $\ell(\sigma) < k(\sigma)$ e $\sigma \in I_n$ temos possibilidade de associar a σ um elemento bem definido de E_n. Se

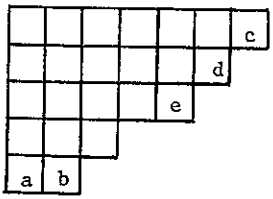
$$\ell(\sigma) < k(\sigma)$$

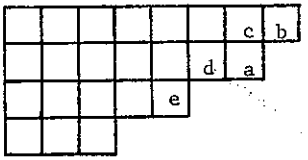
e $\sigma \in E_n$ podemos associar a σ um elemento bem definido de I_n. Isto se consegue com a seguinte regra:

se $s(\sigma) \leq \ell(\sigma)$ mova os quadrados do "sul" do diagrama de Ferrer de σ para o "leste" do diagrama.

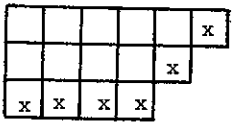
se $s(\sigma) > \ell(\sigma)$ mova os quadrados do leste do diagrama para o "sul" do mesmo.

Por exemplo:

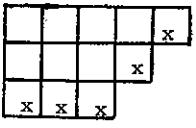




Claramente esta *função* que estamos definindo entre E_n e I_n é uma bijeção, desde que para nenhuma partição σ de $E_n \cup I_n$ tenhamos $\ell(\sigma) = k(\sigma)$. Quando existe tal σ em $E_n \cup I_n$ a nossa regra não pode ser aplicada. Por exemplo considere o seguinte diagrama, onde $\ell(\sigma) = k(\sigma) = s(\sigma) - 1$,



Se fossemos aplicar a regra deveríamos mover o "leste" do diagrama para o "sul"; mas aí obteríamos duas partes iguais. A outra dificuldade ocorre nos diagramas do tipo $\ell(\sigma) = k(\sigma) = s(\sigma)$,



pois o "sul" não pode ser movido para o leste.

Nestes casos excepcionais n pode ser expresso em termos de $k = k(\sigma)$ e vale, onde $j=0$ ou 1,

$$n = (k+j) + (k+j+1)+\ldots+(2k+j-1)$$

$$= \frac{k}{2}\,(3k+2j-1)$$

ou seja

$$n = \frac{k}{2}\,(3k\pm1).$$

Concluindo, observe que se $n \neq \frac{k}{2}\,(3k\pm1)$ para todo $k \in Z$, então

$$e_n = |E_n| = |I_n| = i_n.$$

Se k for ímpar e $n = \frac{k}{2}\,(3k\pm1)$, então existe precisamente um elemento em I_n a mais do que em E_n:

$$e_n = |E_n| = |I_n| - 1 = i_n - 1.$$

Se k for par e $n = \frac{k}{2}\,(3k\pm1)$, então existe precisamente um elemento em E_n a mais do que em I_n:

$$e_n = |E_n| = |I_n| + 1 = i_n + 1.$$

Unificando os dois últimos casos obtemos em geral,

$$e_n = i_n + (-1)^k \quad \text{se} \quad n = \frac{k}{2}\,(3k\pm1)$$

$$= i_n \quad \text{se} \quad n \neq \frac{k}{2}\,(3k\pm1),$$

estabelecendo o lema. □

Usando os dois últimos lemas podemos deduzir diretamente o seguinte corolário descoberto por Euler.

(II.2.d) COROLÁRIO. (IDENTIDADE DE EULER):

$$\prod_{n\geq 1}(1-x^n) = 1 + \sum_{k\geq 1}(-1)^k \left[x^{\frac{3k^2-k}{2}} + x^{\frac{3k^2+k}{2}}\right].$$

PROVA: Pelo Lema (II.2.b) o coeficiente de x^n na expansão do pro

duto à esquerda é $e_n - i_n$, com a notação do lema (II.2.c). Por este lema, o coeficiente de x^n na soma à direita é também $e_n - i_n$. □

Uma consequência da identidade acima e do fato de que a expressão do seu lado esquerdo é a inversa da função geradora das partições implica

$$\left[1 + \sum_{k\geq 1} (-1)^k \left(x^{\frac{3k^2-k}{2}} + x^{\frac{3k^2+k}{2}}\right)\right] \cdot \left[\sum_{n\geq 0} p_n x^n\right] = 1,$$

onde $p_0 = 1$ por convenção (adequada e permitida).

(II.2.e) TEOREMA. RECORRÊNCIA PARA PARTIÇÕES: Os números p_n, de partições do inteiro $n \geq 1$, satisfaz à recorrência seguinte, onde $r = \frac{3k^2-k}{2}$ e $s = \frac{3k^2+k}{2}$:

$$p_n = \sum_{k=1}^{\left\lfloor \frac{\sqrt{1+24n}-1}{6} \right\rfloor} (-1)^{k-1} (p_{n-r} + p_{n-s}).$$

PROVA: Para $n \geq 1$ o coeficiente de x^n no produto acima é zero. Este coeficiente é

$$p_n + \sum_k (-1)^k (p_{n-r} + p_{n-s}).$$

A soma acima varia entre 1 e um valor de k tal que $n-s \geq 0$ ou seja

$$3k^2 + k - 2n \leq 0,$$

ou ainda, uma vez que k é inteiro positivo

$$k \leq \left\lfloor \frac{\sqrt{1+24n}-1}{6} \right\rfloor$$

Transpondo a soma em k para o segundo membro obtemos a expressão para p_n apresentada no teorema. □

Aplicando a recorrência apresentada acima podemos facilmente encontrar os valores de p_n. Os primeiros 30 valores são

n	p_n	n	p_n
1	1	16	231
2	2	17	297
3	3	18	385
4	5	19	490
5	7	20	627
6	11	21	792
7	15	22	1002
8	22	23	1255
9	30	24	1575
10	42	25	1958
11	56	26	2436
12	77	27	3010
13	101	28	3718
14	135	29	4565
15	176	30	5604

Exemplificando o cálculo para n=8 : o limite superior do somatório é 2 e utilizando a fórmula de recorrência encontramos

$$p_8 = p_7 + p_6 - p_3 - p_1$$

$$= 15 + 11 - 3 - 1 = 22.$$

II.3 - PROVANDO EXISTÊNCIA E UNICIDADE POR CONTAGEM

No que segue, exemplificamos como é possível contando, provar existência e unicidade de uma certa representação dos inteiros positivos. Como mostramos nas notas desta seção, esta representação permite a construção de uma bijeção "efetiva" entre $\{0,1,2,\ldots,n!-1\}$ e as permutações de n símbolos. Na prova do teorema de representação construímos um prefab simples tal que o inventário do conjunto que interessa enumerar é a função geradora do número de representações dos inteiros. Acontece que a seqüência do coeficientes é do tipo $(1,1,1,\ldots,1,0,0,\ldots)$. Isto prova existência e unicidade num segmento inicial dos números inteiros e ilustra a flexibilidade dos prefabs.

A termologia *base de arranjos* no teorema seguinte diz respeito às constantes multiplicativas da forma

$$\frac{(n-k+j)!}{(n-k)!}$$

que enumeram os arranjos de subconjuntos com cardinalidade $n-k$ de um conjunto com $n-k+j$ elementos.

(II.3.a) TEOREMA. (BASE DE ARRANJOS): Sejam k e n inteiros com $0 < k \leq n$. Dado um inteiro m tal que

$$0 \leq m < \frac{n!}{(n-k)!}$$

existe uma única seqüência de inteiros

$$(s_0, s_1, s_2, \ldots, s_{k-1})$$

tal que $0 \leq s_j \leq n-k+j$, para $j=0,1,\ldots,k-1$ e satisfazendo

$$m = \sum_{j=0}^{k-1} s_j \frac{(n-k+j)!}{(n-k)!}$$

Uma forma mais simples é obtida fazendo $k=n$ no teorema acima.

(II.3.b) COROLÁRIO. (BASE FATORIAL): Dados m,n inteiros com $0 \leq m < n$, existe uma única seqüência de inteiros

$$(s_1, s_2, \ldots, s_{n-1})$$

tal que $0 \leq s_j \leq j$, para $j=1,2,\ldots,n-1$ e satisfazendo

$$m = \sum_{j=1}^{n-1} s_j (j!).$$

Note que retiramos s_0 do enunciado do corolário porque a restrição na gama de valores que s_j pode assumir no caso de $k=n$ implica $s_0=0$.

PROVA DO TEOREMA:

Seja Ω a classe dos submulticonjuntos de

$$\{0,1,2,\ldots,k-1\},$$

isto é, a classe dos subconjuntos com multiplicidades. Definimos a composição o de dois elementos de Ω como a sua união, exatamente como no exemplo (II.1.d). O elemento neutro para o é o multiconjunto vazio ϕ. O conjunto de primos P é formado pelos multiconjuntos do tipo

$$\{n^1\}.$$

O peso de ϕ é $\pi(\phi) = 1$ e o peso de a Ω,

$$a = \left\{0^{s_0}, 1^{s_1}, 2^{s_2}, \ldots, (k-1)^{s_{k-1}}\right\}$$

é

$$\pi(a) = x^{\left[\sum_{j=0}^{k-1} s_j \frac{(n-k+j)!}{(n-k)!}\right]}$$

Observe que (Ω,o,π) é um prefab simples.

Consideremos agora a função $\alpha: P \longrightarrow 2^{\mathbb{N}}$ dada por

$$\alpha(\{p^j\}) = \{0,1,2,\ldots,n-k+j\}.$$

Recorde que, pela notação explicada para a extensão do teorema básico (II.2.a), Ω^α representa o subconjunto de Ω formado pelos elementos cuja fatorização em primos tem os expoentes dos primos na imagem sob α dos mesmos.

Para concluir a prova é portanto suficiente estabelecermos que

$$\mathrm{Inv}_\pi(\Omega^\alpha) = \sum_{j=0}^{\frac{n!}{(n-k)!}} 1.x^j,$$

uma vez que o coeficiente de x^m no inventário de Ω^α nos diz quantas representações do inteiro m do tipo permitido existem.

Para estabelecer a igualdade acima usamos o teorema (II.2.a) para obter

$$\mathrm{Inv}_\pi(\Omega^\alpha) = \prod_{p\in P}\left(\sum_{j\in\alpha(P)} \pi(p^j)\right)$$

$$= \prod_{j=0}^{k-1} \sum_{0\le s_j\le n-k+j} x^{s_j\frac{(n-k+j)!}{(n-k)!}}.$$

Para tornar clara a simplificação que segue vamos denotar por x_j o termo

$$x^{s_j\frac{(n-k+j)!}{(n-k)!}}$$

Para cada $j\in\{0,1,\ldots,k-1\}$ a soma acima vale

$$1 + x_j + x_j^2 + \ldots + x_j^{n-k+j} = \frac{1-x_j^{n-k+j+1}}{1-x_j} .$$

Observe porém que $x_j^{n-k+j+1}$ é simplesmente x_{j+1}. Assim

$$\mathrm{Inv}_\pi(\Omega^\alpha) = \prod_{j=0}^{k-1} \left(\frac{1-x_j+1}{1-x_j} \right)$$

$$= \frac{1-x_k}{1-x_o} = \frac{1-x^{\frac{n!}{(n-k)!}}}{1-x}$$

$$= \sum_{j=0}^{\frac{n!}{(n-k)!}} x^j ,$$

demonstrando o teorema. □

NOTAS

O corolário da base fatorial (II.3.6) afirma que se $0 \leq m < n$ então

$$m = \sum_{j=1}^{n-1} s_j (j!),$$

onde a seqüência $(s_j)_{j=1,2,\ldots,n-1}$ é única satisfazendo $0 \leq s_j \leq j$. Isto define uma bijeção

$$\beta: V_n \longrightarrow \{0,1,\ldots,n! -1\},$$

onde V_n é o conjunto das seqüências do tipo descrito. Observe se $v \in V_n$, então $\beta(v)$ é facilmente encontrado com o somatório acima. Além disso, se m é um número entre 0 e $n! -1$, o processo pa

ra encontrar a única seqüência v em V_n tal que $\beta^{-1}(m) = v$ é simples e deixamo-lo a cargo do leitor, ver exercício 2.8.

Vamos agora apresentar uma bijeção natural

$$\gamma: S_n \longrightarrow V_n$$

onde S_n é o conjunto de permutações de $\{1,2,\ldots,n\}$. Vamos, como de costume, representar os elementos de S_n como seqüências de comprimento n sem repetições nos símbolos $1,2,\ldots,n$. Se $s = (s_1,s_2,\ldots,s_n)$ é uma seqüência em S_n, definimos $\gamma(s)$ como a seqüência $(v_1,v_2,\ldots,v_{n-1})$ em que v_i é a quantidade de números precedendo s_{i+1} que são maiores que este. Por exemplo, se $s = (5,3,2,4,1)$ então $\gamma(s) = (1,2,1,4)$. Observamos diretamente que $\gamma(s) \in V_n$. O algoritmo que define γ é invertível, isto é, γ é uma bijeção entre S_n e V_n, ver exercício 2.8.

Note que a função composta $\delta = \beta \circ \gamma$ é uma bijeção "efetiva" entre S_n e $\{0,1,\ldots,n! -1\}$. Se o leitor convenceu-se que β e γ são invertíveis, pode ignorar as aspas do "efetiva" acima, pois está de posse de um algoritmo rápido para calcular construtivamente, não só $\delta(m)$ para qualquer $m \in \{0,1,\ldots,n!-1\}$, como também $\delta^{-1}(s)$ para qualquer seqüência s em S_n.

A função δ pode ser usada em situações onde é conveniente se "individualizar a ordem dos ítens". Um caso concreto é o exame Vestibular. Para se dificultar a "fila" costuma-se (ou pelo menos costumava-se) elaborar dois a quatro tipos de provas. Uma implementação adequada da função δ em computador aliada a alguns refinamentos permite

(a) a elaboração de uma única prova;

(b) ordem de quesitos individuais;

(c) alunos próximos com interseção nas ordens dos quesitos quase que vazia.

Uma variante do método foi levada a efeito em 1975 no ciclo básico da área II da UFPE. Os resultados foram satisfatórios

no que tange a diminuição do esforço de fiscalizar quase 300 alunos.

II.4 - CONTANDO ÁRVORES ENRAIZADAS

Iniciamos esta seção apresentando, sob uma hipótese adicional uma outra forma do teorema básico para prefab simples estabelecido em (II.1.b). Em seguida usamos esta forma do teorema para conseguir uma equação funcional envolvendo a função geradora do número de "árvores enraizadas com n vértices". (Estes termos são definidos posteriormente.) Finalmente, da equação funcional obtemos uma recorrência para os coeficientes.

(II.4.a) TEOREMA BÁSICO (OUTRA FORMA): Seja (C,o,π) um prefab simples e P o conjunto de seus primos. Seja também, para $n\geq 1$, P^n o conjunto $\{p^n: p\in P\}$. Suponha que para todo par $a, b \in C$ $\pi(a\ o\ b) = \pi(a).\ \pi(b)$. Então

$$Inv_\pi(C) = \exp\left(\sum_{n\geq 1} \frac{Inv_\pi(P^n)}{n}\right).$$

PROVA: Pelo teorema básico (II.1.b) sabemos que

$$Inv_\pi(C) = \prod_{p\in P} \frac{1}{1-\pi(p)}.$$

Tomando o logaritmo natural de ambos os membros obtemos

$$\ell n(Inv_\pi(C)) = \sum_{p\in P} -\ell n(1-\pi(p))$$

$$= \sum_{p\in P}\left[\pi(p) + \frac{\pi(p^2)}{2}+\ldots\frac{\pi(p^n)}{n}+\ldots\right]$$

A segunda igualdade acima vem da conhecida expansão de Taylor para $-\ell n(1-x)$ que é

$$-\ell n(1-x) = \sum_{n\geq 1} \frac{x^n}{n}$$

e da hipótese adicional, isto é, que $\pi(a\ o\ b) = \pi(a).\ \pi(b)$ não

só para coprimos a e b mas para todo par a,b de elementos de C. De fato, esta hipótese implica que $(\pi(p))^n = \pi(p^n)$.

Para concluir observe que

$$\sum_{p\in P} (\pi(p) + \frac{\pi(p^2)}{2} + \ldots) = \sum_{p\in P} \sum_{n\geq 1} \frac{\pi(p^n)}{n}$$

$$= \sum_{n\geq 1} \frac{1}{n} \sum_{p\in P} \pi(p^n)$$

$$= \sum_{n\geq 1} \frac{Inv_\pi(P^n)}{n}.$$

Tomando agora a exponencial obtemos

$$Inv_\pi(C) = \exp\left(\sum_{n\geq 1} \frac{Inv_\pi(P^n)}{n} \right),$$

estabelecendo o teorema. □

Queremos alertar o leitor de que, quando na dedução acima trocamos a ordem das somas infinitas, estamos assumindo implicitamente hipóteses delicadas de convergência uniforme e outros detalhes analíticos. É possível evitá-los completamente usando o ponto de vista adotado em [TU 2], porém preferimos que o leitor aceite sem provas que estas manipulações são corretas. Do contrário nos afastaríamos demais do nosso propósito. O leitor interessado deve consultar o paper acima mencionado.

GRAFOS E ÁRVORES

Um *grafo* G é constituído por 2 conjuntos disjuntos V(G), A(G) chamados respectivamente de conjunto dos *vértices* de G e conjunto das *arestas* de G tal que cada aresta esteja associada a exatamente 2 vértices (suas *extremidades*) não necessariamente distintos.

Dois grafos G_1 e G_2 são *isomorfos* se existem bijeções

$$b_1 : V(G_1) \longrightarrow V(G_2)$$

$$b_2 : A(G_1) \longrightarrow A(G_2)$$

tais que se v_1, v_2 são as extremidades da aresta a então $b_1(v_1)$ e $b_2(v_2)$ são as extremidades da aresta $b_2(a)$.

Um grafo H é chamado de *subgrafo* de G se

$$V(H) \subseteq V(G) \quad \text{e} \quad A(H) \subseteq A(G).$$

Um *polígono* é um grafo que tem seus vértices e arestas disposto numa seqüência cíclica

$$v_0, a_1, v_1, a_2, v_2, \ldots, a_n, v_n = v_0$$

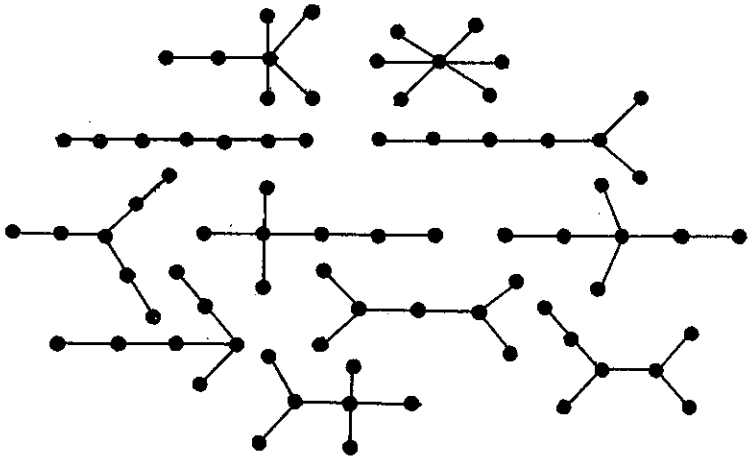
onde os v_i's são vértices distintos com exceção de v_0 que aparece duas vezes, os a_i's são arestas distintas e as extremidades da aresta a_i são v_{i-1} e v_i.

Uma *árvore* é um grafo "conexo" sem polígonos como subgrafos.

Conexidade é uma noção topológica e embora possamos defini-la combinatorialmente damos, ao invés a definição topológica de grafos. Isto se justifica pois usamos diagramas topológicos para representar as árvores e grafos em geral. Topologicamente um grafo é um espaço obtido da seguinte maneira: iniciamos com uma coleção de intervalos fechados disjuntos chamados de arestas. Consideremos agora uma partição arbitrária do conjunto das extremidades dos intervalos. Façamos a identificação topológica dos extremos que estiverem na mesma classe da partição. O espaço quociente assim obtido é chamado um *grafo* e cada classe de equivalência de extremos é chamada de um *vértice*.

Um grafo é conexo se é conexo como espaço topológico e assim as aspas do "conexo" na definição de árvore podem ser removidas. Deixamos como exercício para o leitor convencer-se de que dois grafos (combinatoriais) são isomorfos se e somente se os grafos (topológicos) são homeomorfos e têm o mesmo número de vértices.

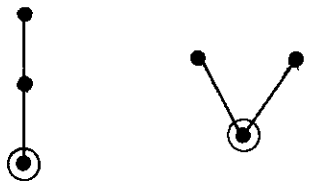
Na seção seguinte vamos contar árvores a menos de isomorfismos. Vamos, por exemplo, provar que com 7 vértices só existem as 11 árvores seguintes:



Este problema é difícil e instrutivo pois embora tenha ocupado Cayley no século passado só foi resolvido satisfatoriamente em 1948 por Otter [OT 1]. O esforço para contar vários tipos de árvores, historicamente motivado por aplicações a circuitos elétricos, foi causador de importantes avanços na teoria de enumeração.

ÁRVORES ENRAIZADAS

Antes de podermos enumerar árvores, temos de fazê-lo para com as árvores enraizadas. Uma árvore *enraizada* é uma árvore em que um dos vértices é distinguido e chamado de *raiz*. Assim por exemplo, embora só exista uma árvore com 3 vértices, existem 2 árvores enraizadas distintas com 3 vértices:



Como o isomorfismo deve preservar a raiz, as duas árvores enraizadas acima são claramente distintas.

Uma *floresta* é um grafo sem polígonos. Uma outra maneira de definir é dizer que uma floresta é uma coleção de árvores duas a duas disjuntas. Uma floresta *enraizada* é uma floresta onde cada componente conexa é uma árvore enraizada. O lema seguinte dá uma conexão bastante simples para as funções geradoras por número de vértices das árvores enraizadas e das florestas enraizadas.

(II.4.b) LEMA: Se $f(x)$ e $r(x)$ são respectivamente as funções geradoras por número de vértices das florestas enraizadas e das árvores enraizadas, então

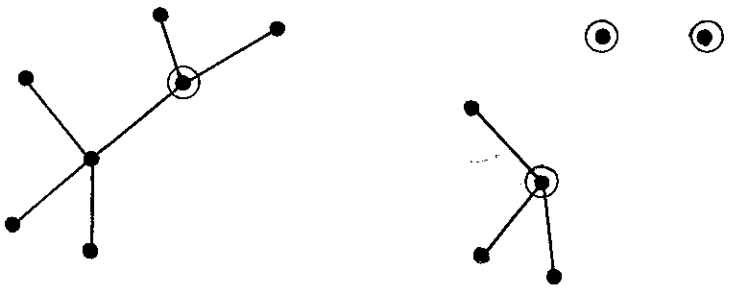
$$xf(x) = r(x).$$

PROVA: Sejam f_n e r_n os coeficientes de x^n em $f(x)$ e $r(x)$ respectivamente. A igualdade que queremos estabelecer é equivalente a termos para todo n

$$f_{n-1} = r_n.$$

Isto é, devemos provar que o número de florestas enraizadas tendo $n-1$ vértices é igual ao número de árvores enraizadas tendo n vértices.

Dada uma árvore enraizada tendo n vértices deletemos a raiz e declaremos seus vértices vizinhos como raízes da floresta enraizada com $n-1$ vértices assim obtida. Veja figura abaixo:



Este procedimento nos dá uma bijeção entre o conjunto das árvores enraizadas tendo n vértices e o conjunto das florestas enraizadas tendo n-1 vértices. O fato da função ser bijetiva decorre do fato dela ter uma inversa: dada uma floresta enraizada há uma única possibilidade (qual?) de compor uma árvore enraizada com um vértice (a raiz) a mais de maneira compatível com a composição. Assim, o lema está estabelecido. □

Agora só resta construir um prefab simples e estabelecer a seguinte equação funcional para as árvores enraizadas originalmente obtida por Polya em 1937.

(II.4.c) TEOREMA (POLYA - 1937): Se $r(x)$ é a função geradora por número de vértices das árvores enraizadas, então

$$r(x) = x \exp\left(\sum_{n\geq 1} \frac{r(x^n)}{n}\right).$$

PROVA: O conjunto Γ das florestas enraizadas forma um prefab simples onde as árvores enraizadas são os primos desde que a composição o e o peso π sejam assim definidos:

Se F_1 e F_2 são florestas enraizadas, $F_1 \circ F_2$ é a floresta enraizada cujas componentes são as árvores enraizadas componentes de F_1, juntamente com as árvores enraizadas componentes de F_2. O peso π de uma floresta enraizada F com n vértices é $\pi(F) = x^n$.

Note que (Γ, o, π) é um prefab simples onde o conjunto de primos A é o conjunto de árvores enraizadas. Além disso o elemento neutro para o é a floresta vazia ϕ que não tem vértices. Finalmente note que quaisquer que sejam as florestas F_1 e F_2,

$$\pi(F_1 \circ F_2) = \pi(F_1) \cdot \pi(F_2).$$

Podemos assim aplicar o Teorema (II.4.a) e obter, onde para $n\geq 1$ $A^n = \{a^n : a \in A\}$,

$$\mathrm{Inv}_{\pi}(\Gamma) = \exp\left(\sum_{n\geq 1} \frac{\mathrm{Inv}_{\pi}(A^n)}{n} \right) .$$

Observe agora que $\mathrm{Inv}_{\pi}(\Gamma) = f(x)$, função geradora das florestas enraizadas. Além disso

$$\mathrm{Inv}_{\pi}(A^n) = \mathrm{Inv}_{\pi}(\{ a^n : a \in A\})$$

$$= r(x^n),$$

uma vez que os elementos de A^n estão em bijeção natural com os elementos de A e têm peso n vezes maior.

Podemos então escrever

$$f(x) = \exp\left(\sum_{n\geq 1} \frac{r(x^n)}{n} \right),$$

e pelo lema (II.4.b) anterior, ao multiplicarmos por x obtemos

$$r(x) = x \exp\left(\sum_{n\geq 1} \frac{r(x^n)}{n} \right),$$

que é o teorema de Polya. □

Como vemos a seguir é ainda uma tarefa não trivial se explicitar os coeficientes de $r(x)$.

UMA RECORRÊNCIA PARA ÁRVORES ENRAIZADAS

Vamos usar a equação funcional deduzida acima para obter uma recorrência que permita o cálculo mecânico dos r_n's. Começamos com o seguinte lema que dá uma conexão entre os coeficientes de funções geradoras relacionadas pela exponencial.

(II.4.d) LEMA: Seja $a(x) = \exp(b(x))$, onde $a(x) = \sum_{n\geq 0} a_n x^n$ e

$b(x) = \sum_{n\geq 1} b_n x^n$. Então para $n \geq 1$

$$a_n = \frac{1}{n} \sum_{k=1}^{n} k.b_k.a_{n-k}$$

ou equivalentemente,

$$b_n = a_n - \frac{1}{n} \sum_{k=1}^{n-1} k.b_k.a_{n-k}.$$

PROVA: Note em primeiro lugar que $a_0=1$, pela primeira igualdade do lema, e asim as expressões para a_n e b_n são equivalentes e portanto, provamos apenas a primeira delas. Tomando logaritmos naturais da equação dada obtemos

$$\ell n(a(x)) = b(x).$$

(Observe que $a(x) = 1 + f(x)$ e portanto

$$\ell n(a(x)) = \ell n(1 + f(x)) = \sum_{n\geq 1} (-1)^{n+1} \frac{(f(x))^n}{n}.)$$

Derivando a equação acima podemos escrever

$$\frac{a'(x)}{a(x)} = b'(x)$$

ou

$$a'(x) = a(x) \cdot b'(x).$$

Usando as definições e multiplicando ambos os termos por x a última equação se torna

$$\sum_{n\geq 1} n\, a_n\, x^n = \left(\sum_{n\geq 0} a_n\, x^n \right) \left(\sum_{n\geq 1} n\, b_n\, x^n \right).$$

Igualando os coeficientes de x^n obtemos

$$n\, a_n = \sum_{k=1}^{n} k\, b_k\, a_{n-k}.$$

Dividindo esta equação por n concluímos a prova do lema. □

Vamos usar o lema acima numa equação que é conseqüência da equação obtida na prova do teorema (II.4.c) que nos dá f, função geradora das florestas enraizadas, em função de r, especificamente,

$$f(x) = \exp\left(\sum_{n\geq 1} \frac{r(x^n)}{n}\right).$$

Seja

$$b(x) = \sum_{n\geq 1} b_n\, x^n$$

tal que

$$\sum_{n\geq 1} b_n\, x^n = \sum_{n\geq 1} \frac{r(x^n)}{n}.$$

Derivando e multiplicando por x ambos os termos desta equação encontramos

$$\sum n\, b_n\, x^n = \sum_{n\geq 1} x\, r'(x^n)$$

$$= \sum_{j\geq 1} \left(\sum_{k\geq 1} k\, r_k\, x^{jk}\right).$$

Igualando os coeficientes de x^n temos

$$n\, b_n = \sum_{k|n} k\, r_k,$$

uma vez que cada divisor k de n contribui com a parcela kr_k ao coeficiente de $x^{jk} = x^n$.

Uma vez expresso nb_n em função dos r_k's a obtenção da recorrência é simples. Temos

$$f(x) = \exp\left(\sum_{n\geq 1} b_n x^n\right)$$

e aplicando o lema anterior, com $f(x)$ no lugar de $a(x)$,

$$f_n = \frac{1}{n} \sum_{k=1}^{n} k\, b_k\, f_{n-k}.$$

Recorde agora que pela lema (II.4.b), $f_n = r_{n+1}$ para todo $n\geq 0$. Utilizando esta relação conjuntamente com a expressão obtida para $n\cdot b_n$ (ou $k\cdot b_k$), concluimos a prova do seguinte resultado:

(II.4.e) TEOREMA: Os números r_n's que contam as árvores enraizadas com n vértices satisfazem à seguinte recorrência

$$r_1 = 1$$

$$r_{n+1} = \frac{1}{n} \sum_{k=1}^{n} \left(\sum_{j\,|\,k} j r_j\right) r_{n-k+1}$$

para $n\geq 1$. □

Dessa recorrência é uma tarefa simples se explicitar os r_n's. Os vinte primeiros são

n	r_n	n	r_n	n	r_n	n	r_n
1	1	6	20	11	1842	16	235381
2	1	7	48	12	4766	17	634847
3	2	8	115	13	12486	18	1721159
4	4	9	286	14	32973	19	4688676
5	9	10	719	15	87811	20	12826228

Como exemplo de cálculo, vamos obter r_{12} em função de seus predecessores

$$
\begin{aligned}
11.r_{12} = {} & (1r_1)\, r_{11} + \\
& (1r_1 + 2r_2)\, r_{10} + \\
& (1r_1 + 3r_3)\, r_9 + \\
& (1r_1 + 2r_2 + 4r_4)\, r_8 + \\
& (1r_1 + 5r_5)\, r_7 + \\
& (1r_1 + 2r_2 + 3r_3 + 6r_6)\, r_6 + \\
& (1r_1 + 7r_7)\, r_5 + \\
& (1r_1 + 2r_2 + 4r_4 + 8r_8)\, r_4 + \\
& (1r_1 + 3r_3 + 9r_9)\, r_3 + \\
& (1r_1 + 2r_2 + 5r_5 + 10r_{10})\, r_2 + \\
& (1r_1 + 11r_{11})\, r_1
\end{aligned}
$$

Substituindo pelos valores numéricos obtemos

$$
\begin{aligned}
11r_{12} = {} & 1.1842 + (1.1+2.1).719 + (1.1+3.2).286 + \\
& + (1.1+2.1+4.4)115 + (1.1+5.9).48 \\
& + (1.1+2.1+3.2+6.20).20 \\
& + (1.1+7.48).9 \\
& + (1.1+2.1+4.4+8.115).4 \\
& + (1.1+3.2+9.286).2 \\
& + (1.1+2.1+5.9+10.719).1 \\
& + (1.1+11.1842).1 = 52426.
\end{aligned}
$$

E dividindo por 11, r_{12}=4766.

II.5 - CONTANDO ÁRVORES

Depois de termos desenvolvido uma técnica de enumeração para as árvores enraizadas, podemos agora contar as árvores em função das últimas. Mesmo conhecendo-se $r(x)$, explicitar $a(x)$, função geradora (por número de vértices) das árvores em termos de $r(x)$ é ainda um problema difícil cuja solução depende, como vamos ver, de propriedades estruturais intrínsecas das árvores.

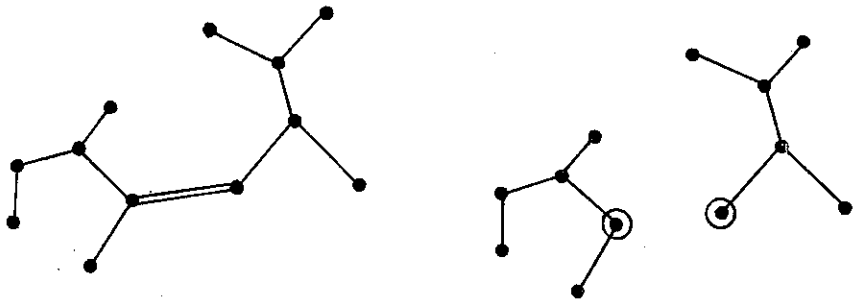
ÁRVORES COM ARESTA DISTINGUIDA

Vamos começar por encontrar uma expressão, em termos de $r(x)$, para a função geradora (por número de vértices) das árvores com aresta distinguida. Chamemos de s a função geradora para tais árvores

$$s(x) = \sum_{n \geq 2} s_n x^n.$$

Isto é, s_n representa o número de árvores com aresta distinguida tendo n vértices.

Dada uma árvore com aresta distinguida, ao deletarmos esta última e declararmos que as suas extremidades são as raízes das duas árvores obtidas, temos definida uma bijeção entre as árvores com aresta distinguida tendo n vértices e os pares desordenados de árvores enraizadas cuja soma do número de vértices é n. Veja figura abaixo.



Vamos chamar a inversa desta bijeção de *justaposição* de árvores enraizadas.

II.5.a) LEMA: Sejam s_n o número de árvores com aresta distinguida tendo n vértices e r_n o número de árvores enraizadas também com n vértices. Então para $n \geq 2$

$$s_n = \frac{1}{2}\left(\sum_{i=1}^{n-1} r_i \, r_{n-i} \right), \text{ se } n \text{ é ímpar}$$

$$= \frac{1}{2}\left(\sum_{i=1}^{n-1} r_i \, r_{n-i} \right) + \frac{1}{2} r_{n/2}, \text{ se } n \text{ é par.}$$

PROVA: Como mostramos esta expressão para s_n é uma conseqüência direta da bijeção acima mencionada. No caso de n ímpar as duas árvores enraizadas que quando ligadas pelas raízes forma a árvore com aresta distinguida, são diferentes, pois têm número de vértices diferentes. O fator de $\frac{1}{2}$ é para destruir a ordem, porque o somatório conta pares ordenados. Já quando n é par a metade do somatório leva em conta apenas a metade do número de árvores com aresta distinguida formadas por duas árvores enraizadas iguais. Assim somos obrigados a somar a outra metade, isto é, a parcela $\frac{1}{2} r_{n/2}$. □

(II.5.b) COROLÁRIO: Sejam $s(x)$ a função geradora para as árvores com aresta distinguida e $r(x)$ a função geradora das árvores enraizadas. Então

$$s(x) = \frac{1}{2}\left[r^2(x) + r(x^2) \right].$$

PROVA: Pelo lema anterior podemos escrever

$$s(x) = \frac{1}{2} \sum_{n \geq 1} \left(\sum_{i=1}^{2n} r_i \; r_{2n+1-i} \right) x^{2n+1} \; +$$

$$+ \frac{1}{2} \sum_{n\geq 1} \left[\left(\sum_{i=1}^{2n-1} r_i \, r_{2n-i} \right) + r_n \right] x^{2n}.$$

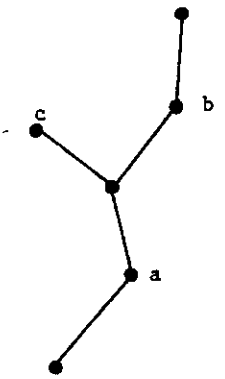
E rearrumando obtemos

$$s(x) = \frac{1}{2} \sum_{n\geq 2} \left(\sum_{i=1}^{n-1} r_i \, r_{n-i} \right) x^n + \frac{1}{2} \sum_{n\geq 1} r_n (x^2)^n$$

$$= \frac{1}{2} \left[r^2(x) + r(x^2) \right],$$

o que demonstra o corolário. □

Dois vértices de uma árvore são equivalentes se as árvores com raízes nestes vértices são topologicamente indistinguíveis. Por exemplo, os vértices a e b na árvore desenhada abaixo são equivalentes; já a e c não o são. O conceito de arestas



equivalentes é inteiramente análogo.

Se A é uma árvore vamos denotar por v(A) o número de classes de vértices equivalentes e por a(A) o número de classes de arestas equivalentes que existem em A. Seja também u(A)

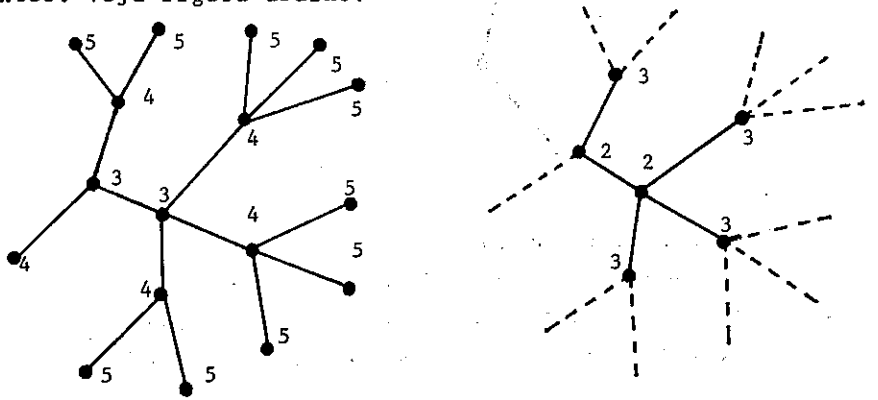
o número de arestas em A que ligam vértices equivalentes. Nossa próxima tarefa é provar a seguinte propriedade de árvores:

(II.5.c) LEMA: Seja A uma árvore qualquer. O valor de u(A) é 0 ou 1. No segundo caso, a árvore cuja aresta distinguida é a (única) aresta que liga vértices equivalentes é formada pela justaposição de duas árvores enraizadas iguais.

PROVA: Seja x um vértice em A. A *distância* de x a um outro vértice qualquer y de A é o número de aresta diferentes percorridas no único caminho que liga x a y. A *excentricidade* de um vértice x de A é definida como

$$exc(x) = \max_{y \in V(A)} \{dist(x,y)\}.$$

Os *centros* de A são os vértices com menor excentricidade. Antes de prosseguirmos para a prova do lema, vamos precisar mostrar que qualquer árvore A tem um ou dois centros. Nenhum vértice *pendente* de A (um vértice que é extremidade de uma única aresta) é um centro de A, a menos que A seja constituída por uma única aresta. Se A tem alguma aresta, A tem pelo menos dois vértices pendentes, um fato que é simples de ser demonstrado. A operação de deletar todos os vértices pendentes de A simultaneamente tem o efeito de reduzir de um a excentricidade de todos os vértices restantes. Veja figura abaixo.



Assim os centros são preservados após a supressão de todos os vértices pendentes de uma árvore com mais de uma aresta. Iterando esta operação de supressão simultânea, chegamos a uma árvore constituída por um único vértice ou por dois vértices ligados por uma aresta. Isto mostra que a árvore original tem um ou dois centros.

Podemos agora concluir a prova do lema. A diferença em valor absoluto das excentricidades das extremidades de uma aresta arbitrária de uma árvore é 1 ou 0. Esta diferença assume valor 0 se e somente se os dois vértices em questão são os dois centros da árvore. Excentricidade é uma propriedade que é certamente mantida por isomorfismos de grafos. Assim vértices equivalentes têm necessariamente a mesma excentricidade. Logo para qualquer árvore A o número u(A) de arestas ligando vértices equivalentes é no máximo 1. Além disso, no caso de valer 1 a árvore é formada pela justaposição de árvores enraizadas iguais. Isto conclui a prova. □

Necessitamos agora de apenas mais um lema antes de podermos expressar a função geradora das árvores em termos das árvores enraizadas. Recorde que dada uma árvore A, v(A) é o número de classes de equivalência de vértices e a(A) é o número de classes de equivlência de arestas. Em geral não podemos dizer quanto valem estes números isoladamente. Mas como prova o lema seguinte eles são "quase" iguais, o que é suficiente para nosso objetivo.

(II.5.d) LEMA: Para qualquer árvore A

$$1 = v(A) - a(A) + u(A).$$

PROVA: Pelo lema anterior u(A) vale 0 ou 1. Vamos chamar uma árvore de *simétrica* se u(A) = 1. (A razão para esta terminologia é a caracterização de tais árvores dada no lema anterior.) Sejam arest(A), vert(A) os conjuntos de vértices e arestas de A. Sejam também cnt(A) o conjunto dos centros de A e esp(A) o conjunto

de arestas ligando os centros de A. Observe que $|esp(A)| = u(A) \leq 1$ e que $1 \leq |cnt(A)| \leq 2$. Vamos definir uma bijeção

$$\beta: arest(A) \setminus esp(A) \longrightarrow vert(A) \setminus cnt(A)$$

da seguinte maneira: a imagem de uma aresta por β é o seu extremo de maior excentricidade. A função β está bem definida pois em toda árvore uma aresta que não liga dois centros tem as excentricidades de seus extremos diferindo de 1. A função inversa β^{-1} também está bem definida pois em toda árvore, dado um vértice x que não é um centro, existe um único vértice y ligado a x com excentricidade menor que a de x. Tome então como $\beta^{-1}(x)$ a aresta com extremidades x e y. Note também que β é compatível com as classes de vértices e arestas equivalentes, isto é, arestas a_1 e a_2 no domínio de β são equivalentes se e somente se $\beta(a_1)$ e $\beta(a_2)$ são vértices equivalentes. Assim β induz uma bijeção entre as classes de arestas que não contêm a aresta em esp(A) (se esta existir) e as classes de vértices equivalentes cujos membros não contêm vértices em cnt(A).

Se a árvore A contêm um único centro, então $esp(A) = \phi$ e $u(A) = 0$, e computando a classe de vértices equivalentes constituída unicamente pelo centro de A obtemos

$$1 = v(A) - a(A) + u(A).$$

Se A tem dois centros mais não é simétrica, então os dois centros formam cada um uma classe de vértices distinta. Além disso, esp(A) tem uma aresta não equivalente às do domínio de β. Como $u(A) = 0$, obtemos novamente

$$1 = v(A) - a(A) + u(A).$$

Finalmente, se A é simétrica, então seus dois centros formam uma classe de vértices equivalentes. Considerando a classe formada pela aresta em esp(A) chegamos a $v(A) = a(A)$. Porém agora $u(A) = 1$, o que implica uma vez mais

$$1 = v(A) - a(A) + u(A),$$

concluindo a prova do lema. □

Estamos agora em condições de provar o teorema do Otter [OT 1].

(II.5.e) TEOREMA (OTTER - 1948): Sejam $a(x) = \sum_{n\geq 1} a_n x^n$ a função geradora das árvores e $r(x) = \sum_{n\geq 1} r_n x^n$ a função geradora das árvores enraízadas. Então

$$a(x) = r(x) - \frac{1}{2}\left[r^2(x) - r(x^2)\right].$$

PROVA: Pelo lema anterior, para cada árvore A temos

$$1 = v(A) - a(A) + u(A).$$

Somando esta equação para todas as árvores com n vértices obtemos

$$a_n = r_n - s_n + \sum_{\substack{A: \\ |V(A)|=n}} u(A),$$

onde, como definido no lema (II.5.a), s_n é o número de árvores com arestas distinguidas com n vértices.

Pelo lema (II.5.c) o somatório acima é o número de árvores simétricas com n vértices. Se n for ímpar este número é zero. Se n for par ele vale $r_{\frac{n}{2}}$, pois as árvores simétricas com n vértices estão em bijeção natural com as árvores enraízadas tendo $\frac{n}{2}$ vértices. Estas são "metade" daquelas. Assim podemos escrever

$$\sum_{n\geq 1}\left(\sum_{\substack{A: \\ |V(A)|=n}} u(A)\right) x^n = \sum_{n\geq 1}\left(\sum_{\substack{A: \\ |V(A)|=2n}} u(A)\right) x^{2n}$$

$$= \sum_{n\geq 1} r_n (x^2)^n$$

$$= r(x^2).$$

Desse modo ao multiplicarmos a equação anterior por x^n e somarmos para $n\geq$ encontramos

$$a(x) = r(x) - s(x) + r(x^2).$$

Usando agora a expressão para $s(x)$ deduzida no lema (II.5.b) obtemos finalmente

$$a(x) = r(x) - \frac{1}{2}\,(r^2(x) - r(x^2))$$

o que prova o teorema. □

Usando a equação acima e o teorema (II.4.e) que nos permite calcular os r_n's podemos encontrar efetivamente os a_n's. Os primeiros vinte valores são

1	1	11	235
2	1	12	551
3	1	13	1301
4	2	14	3159
5	3	15	7741
6	6	16	19320
7	11	17	48629
8	23	18	123867
9	47	19	317955
10	106	20	823065.

EXERCÍCIOS

1. Qual é a função geradora para as partições numéricas onde cada parcela é ímpar?

2. Prove que o número de partições do número n em parcelas desiguais é igual ao número de partições do número n em parcelas ímpares.

3. Encontre o número de soluções inteiras não negativas nos x_i's para

$$x_1 + x_2 + \ldots + x_k = n.$$

4. Mostre que o número de soluções inteiras nos n_i's para

$$x_1 + x_2 + \ldots + x_k = n$$

onde para cada $i=1,2,\ldots,k$, $a_i \leq x_i < b_i$ é

$$\left[x^n\right]\left\{x_1^{a_1+a_2+\ldots+a_k}(1-x)^{-k}\prod_{i=1}^{\ }1-x^{b_i-a_i}\right\}.$$

5. Use o exercício anterior para computar o número de soluções inteiras de $x_1+x_2+x_3+x_4 = 21$ onde $1\leq x_1\leq 6$, $0\leq x_2\leq 5$, $4\leq x_3\leq 7$, $2\leq x_4\leq 10$.

6. Demonstre, construindo um prefab simples, que todo inteiro não negativo tem uma única representação na base k para $k\geq 2$.

7. Prove que todo inteiro não negativo menor que $\prod_{i=1}^{k} a_i$ tem uma única representação na forma

$$x_1 + \sum_{j=2}^{k} x_j\left(\prod_{i=1}^{j-1} a_i\right)$$

onde

$$0 \leq x_j \leq a_{j-1},$$

onde $k \geq 1$ e $a_1, a_2, \ldots, a_k$ são inteiros arbitrários maiores que 1.

8. Considere a função

$$\beta: V_n \longrightarrow \{0,1,\ldots,(n!)-1\}$$

definida nas notas da seção II.3. Enuncie um algoritmo para calcular β^{-1} e prove que seu algoritmo funciona. Faça o mesmo para a função $\gamma: S_n \longrightarrow V_n$ também ali definida.

9. Seja

$$S_{n,k} = \sum_{n>x_k>\ldots>x_1\geq 0} z^{\binom{x_1}{1} + \binom{x_2}{2} + \ldots + \binom{x_k}{k}}.$$

Prove que

$$S_{n,k} = \frac{1-z^{\binom{n}{k}}}{1-z}$$

e use este fato para mostrar que cada inteiro r não negativo tem uma única representação na forma

$$r = \binom{x_1}{1} + \binom{x_2}{2} + \ldots + \binom{x_k}{k},$$

onde $0 \leq x_1 < x_2 < \ldots < x_k$ e k é um inteiro positivo arbitrário.

10. Prove que o número de partições do número n em k parcelas é igual ao número de partições de n nas quais a maior parcela é k.

11. Se $\alpha = (\alpha_1, \alpha_2, \ldots)$ é uma partição do número n, então

$$\alpha^* = (\alpha_1^*, \alpha_2^*, \ldots)$$

onde α_i^* é o número de parcelas de α de cardinalidade maior ou igual a i é chamada de partição conjugada de α. Observe que α^* é também uma partição de n. Prove que o número de partições de n que são iguais às suas conjugadas é igual ao número de partições de n em parcelas ímpares e desiguais.

12. Mostre que o número de maneiras ordenadas de se obter um total de n jogando-se um dado k vezes é

$$\sum_{i \geq 0} (-1)^i \binom{k}{i} \binom{n-5k-6i-1}{k-1}.$$

13. Use o teorema de Otter (II.5.e) e a recorrência para árvores enraízadas dada no teorema (II.4.e) para provar que existem exatamente 47 árvores com 9 vértices. Tente desenhar todas elas.

CAPÍTULO III

PREFABS MULTIVALUADOS

III.1 - AXIOMAS E TEOREMA BÁSICO

A noção de prefab simples (C,o,π) pode ser extendida proveitosamente ao permitirmos que a composição $x \circ y$ seja não mais um elemento de C, porém um subconjunto do mesmo. Evidentemente algumas restrições precisam ser impostas para obtermos uma estrutura útil. A formalização seguinte incorpora estas restrições em forma de axiomas e aparece com ligeiras modificações em [BG 1 - 1971].

Um *prefab* $(C,*,k)$ é um conjunto C juntamente com uma operação binária multivaluada $*$, $(a,b \in C$ implica $a * b \subseteq C)$ e uma função $k: C \longrightarrow \mathbb{N} \setminus \{0\}$, chamada função corretiva. Extendemos $*$ a subconjuntos de C definindo $A * B = \{c: c \in a * b$ para algum $a \in A$ e $b \in B\}$. Esta estrutura satisfaz os seguintes axiomas:

(a) A composição $*$

- (a_1) é comutativa
- (a_2) é associativa
- (a_3) tem uma identidade e; $a * e = e * a = \{a\} \equiv a$, para todo $a \in C$. (Identificamos um conjunto com um único elemento com este elemento, para simplificar a notação.)

Chamamos $p \in C$ primo se $p \in a * b$ implica que $p=a$ ou $p=b$.

(b) Temos as seguintes decomposições:

- (b_1) fatorização única - cada $a \in C$ se fatoriza univocamente em primos no sentido que

$$a \in p_1^{r_1} * p_2^{r_2} * \ldots * p_n^{r_n},$$

onde os p_i's são primos distintos e os p_i's e os r_i's são únicos a menos de ordem.

(b_2) fatorização estritamente única - se

$$c \in \left(\overset{*}{\prod} p_i^{r_i}\right) * \left(\overset{*}{\prod} q_j^{s_j}\right)$$

onde os p_i's e os q_j's são primos distintos, então existem um único (a,b) com $a \in \overset{*}{\prod} p_i^{r_i}$, $b \in \overset{*}{\prod} q_i^{s_i}$ tal que $c \in a * b$.

(c) A função corretiva κ satisfaz

(c_1) se $c_1, c_2 \in a * b$ então $\kappa(c_1) = \kappa(c_2)$; assim podemos definir $\kappa(a * b)$ como $\kappa(c)$ para qualquer $c \in a * b$; temos também

(c_2) $$|a * b| = \frac{\kappa(a * b)}{\kappa(a).\kappa(b)},$$

sempre que a e b forem coprimos, isto é, a interseção dos primos de suas decomposições é vazia.

As propriedades impostas pelos axiomas (c_1) e (c_2) são a chave para aplicações dos prefabs à enumeração.

Uma função peso

$$\pi: C \longrightarrow A$$

onde A é um anel contendo os racionais é chamada *multiplicativa para* $*$ se

$$\pi(c) = \pi(a).\ \pi(b)$$

sempre que $c \in a * b$ e a,b coprimos.

Seja $(C,*,\kappa)$ um prefab e π uma função peso multiplicativa para $*$. O *inventário* de $B \subseteq C$ relativo a κ e π é definido como

$$\mathrm{Inv}_{\kappa,\pi}(B) = \sum_{b \in B} \frac{\pi(b)}{\kappa(b)}.$$

(III.1.a) TEOREMA MULTIPLICATIVO: Suponha que $(C,*,\kappa)$ é um prefab e que π é um peso multiplicativo relativo a $*$. Se $X,Y \subseteq C$ são tais que para $x \in X$, $y \in Y$ x e y não têm fatores primos em comum, então

$$\mathrm{Inv}_{\kappa,\pi}(X * Y) = \mathrm{Inv}_{\kappa,\pi}(X)\ \mathrm{Inv}_{\kappa,\pi}(Y).$$

PROVA: Seja $z \in X * Y$. Pelo axioma (b_1) e pela hipótese de que X e Y são coprimos, podemos fatorar z univocamente como

$$z \in \left(\overset{*}{\prod_i} p_i^{r_i}\right) * \left(\overset{*}{\prod_j} q_j^{s_j}\right)$$

onde $\overset{*}{\prod_i} p_i^{r_i} \in A$ e $\overset{*}{\prod_j} q_j^{s_j} \in B$. Pelo axioma (b_2) existe um único par (x,y) com

$$x \in \overset{*}{\prod_i} p_i^{r_i}, \quad y \in \overset{*}{\prod_j} q_j^{s_j}$$

tal que $z \in x * y$. Assim obtemos

$$\mathrm{Inv}_{\kappa,\pi}(X * Y) = \sum_{z \in X * Y} \frac{\pi(z)}{\kappa(z)}$$

$$= \sum_{x \in X} \sum_{y \in Y} \sum_{z \in x * y} \frac{\pi(z)}{\kappa(z)}.$$

Pelos axiomas (c_1) e (c_2) e pelo fato de π ser multiplicativo, obtemos

$$\sum_{z \in x * y} \frac{\pi(z)}{\kappa(z)} = |x * y| \frac{\pi(x * y)}{\kappa(x * y)} = \frac{\pi(x)}{\kappa(x)} \frac{\pi(y)}{\kappa(y)}.$$

Assim,

$$\begin{aligned} \mathrm{Inv}_{\kappa,\pi}(X * Y) &= \sum_{x \in X} \sum_{y \in Y} \frac{\pi(x)}{\kappa(x)} \frac{\pi(y)}{\kappa(y)} \\ &= \left(\sum_{x \in X} \frac{\pi(x)}{\kappa(x)} \right) \left(\sum_{y \in Y} \frac{\pi(y)}{\kappa(y)} \right) \\ &= \mathrm{Inv}_{\kappa,\pi}(X) \cdot \mathrm{Inv}_{\kappa,\pi}(Y), \end{aligned}$$

o que prova o teorema. □

O teorema seguinte que na realidade é um corolário do que acabamos de mostrar, é o mais usado nas aplicações. Ele expressa o inventário do conjunto C como um produto de parâmetros que envolve apenas os primos do prefab, que em muitos casos são fáceis de serem obtidos.

(III.1.b) TEOREMA BÁSICO: Suponha que $(C,*,\kappa)$ é um prefab com conjunto P de primos e que π é um peso multiplicativo para $*$ satisfazendo a implicação para todo $p \in P$ e todo $n \geq 0$,

$$a,b \in p^n \Longrightarrow \pi(a) = \pi(b) = \pi(p^n),$$

onde a última igualdade é a *definição* de $\pi(p^n)$. Então

$$\mathrm{Inv}_{\kappa,\pi}(C) = \prod_{p \in P} \left(\sum_{n \geq 0} \frac{\pi(p^n)}{\kappa(p^n)} |p^n| \right).$$

PROVA: Se $p_1, p_2, \ldots, p_n, \ldots$ são os primos de C e P_j é a união de todas as potências de p_j, então

$$\mathrm{Inv}_{\kappa,\pi}(P_j) = \sum_{n \geq 0} \left(\sum_{c \in p_j^n} \frac{\pi(c)}{\kappa(c)} \right)$$

$$= \sum_{n \geq 0} \frac{\pi(p_j^n)}{\kappa(p_j^n)} \; |p_j^n| .$$

Observando que

$$\prod_j^* P_j = C$$

e aplicando o teorema multiplicativo obtemos a expressão

$$\mathrm{Inv}_{\kappa,\pi}(C) = \prod_{p \in P} \left(\sum_{n \geq 0} \frac{\pi(p^n)}{\kappa(p^n)} \; |p^n| \right),$$

que estabelece o teorema. □

Na próxima seção usamos o teorema básico acima para resolver um problema interessante sobre seqüências.

III.2 - QUE FRAÇÃO DO QUE PODE ACONTECER DEVEMOS ESPERAR QUE ACONTEÇA?

Considere a seguinte questão: um experimento onde n resultados são igualmente prováveis é repetido k vezes. Qual o valor esperado para o número de resultados diferentes?

Posto em linguagem de seqüências o problema é o seguinte: seja $S(n,k)$ o conjunto das n^k seqüências em n símbolos (com repetições) de comprimento k. Se $s \in S(n,k)$ seja $u(s)$ o número de símbolos diferentes que aparecem em s. O que se pede é o valor

$$E(n,k) = \left(\sum_{s \in S(n,k)} u(s) \right) / n^k .$$

Vamos também ter oportunidade de calcular assintoticamente o valor

$$\lim_{n \to \infty} \frac{E(n,n)}{n},$$

isto é, o limite do número esperado do que acontece pelo menos uma vez sobre o número total de possibilidades, n.

Para resolver este problema iniciamos construindo um prefab e uma função peso multiplicativa nas hipóteses do teorema básico (III.1.b).

Seja $S^{(n)}$ o conjunto das seqüências finitas em n símbolos tirados de $\{1,2,\ldots,n\}$. Isto é

$$S^{(n)} = \bigcup_{k \geq 0} S(n,k).$$

O conjunto $S(n,0)$ é constituído pela seqüência vazia que faz o papel de identidade para a composição $*$ que agora definimos.

Para $a,b \in S^{(n)}$, com comprimentos $comp(a)=r$ e $comp(b)=s$, definimos $a * b$ como o conjunto de todas as seqüências de comprimento $r+s$

$$(c_1, c_2, \ldots, c_{r+s})$$

de onde possamos extrair duas subseqüências complementares

$$(c_{v_1}, c_{v_2}, \ldots, c_{v_r}) = a$$

e

$$(c_{u_1}, c_{u_2}, \ldots, c_{u_s}) = b.$$

Para dar um exemplo desta composição, sejam $(1,2)$ e $(1,1,2) \in S^{(2)}$.

$$(1,2) * (1,1,2) = \{ (1,2,1,1,2), (1,1,1,2,2), (1,1,2,1,2)\}.$$

Neste exemplo, das $\binom{5}{2} = 10$ possibilidades, correspondentes à bipartição do conjunto de coordenadas $\{1,2,3,4,5\}$ em duas partes ordenadas uma com 2 e a outra com 3 elementos, para compormos as duas seqüências, apenas 3 são distintas.

Os primos em $S^{(n)}$ são obviamente as seqüências de comprimento 1. É fácil observar que se a e b são coprimos, isto é, não têm símbolos comuns, então $|a * b|$ é o número binomial

$$|a * b| = \binom{\text{comp}(a) + \text{comp}(b)}{\text{comp}(a)}$$

$$= \frac{(\text{comp}(a) + \text{comp}(b))!}{(\text{comp}(a))!\ (\text{comp}(b))!}.$$

Esta expressão sugere definirmos $\kappa(s)$ para $s \in S^{(n)}$ como $(\text{comp}(s))!$ Desse modo, para a e b seqüências coprimas

$$|a * b| = \frac{\kappa(a * b)}{\kappa(a)\ \kappa(b)}.$$

Deixamos para o leitor a verificação de que $(S^{(n)}, *, \kappa)$ é um prefab. Exceto a associatividade de $*$, os outros axiomas são

de simples verificação. Para provar a associatividade, é conveniente em primeiro lugar dar um sentido ao produto múltiplo

$$a * b * c \ldots * z,$$

da maneira natural que generalize o que foi definido para dois fatores. É importante que o leitor pense um pouco sobre como provar a associatividade de $*$, pois isto o ajuda a fixar os conceitos.

Para $a \in S^{(n)}$ definamos o peso de a como

$$\pi(a) = x^{comp(a)}\, y^{dist(a)},$$

onde $dist(a)$ é o número de símbolos distintos aparecendo em a. Note que se a e b são coprimos então para todo $c \in a * b$,

$$\pi(c) = \pi(a).\ \pi(b).$$

Assim π é multiplicativo para $*$. Além disso, como $|p^m| = 1$ para todo primo e todo $m \geq 0$, a hipótese adicional do teorema básico (III.1.b) é trivialmente satisfeita. Assim podemos aplicar este teorema e denotando por $P^{(n)}$ o conjunto de primos de $S^{(n)}$ obtemos

$$Inv_{\kappa,\pi}(S^{(n)}) = \prod_{p \in P^{(n)}} \sum_{m \geq 0} \frac{\pi(p^m)}{\kappa(p^m)} |p^n|$$

$$= \prod_{p \in P^{(n)}} \left(1 + \frac{xy}{1} + \frac{x^2 y}{2!} + \frac{x^3 y}{3!} + \ldots\right)$$

$$= \prod_{p \in P^n} \left[ye^x - (y-1)\right].$$

Como a expressão entre colchetes não depende de p e existem n elementos em $P^{(n)}$, obtemos

$$Inv_{\kappa,\pi}(S^{(n)}) = \left[ye^x - (y-1)\right]^n.$$

Queremos agora abrir um parênteses para fazer notar ao leitor que o peso π não é totalmente multiplicativo, isto é, existem elementos $a,b \in S^{(n)}$ com $c \in a * b$, onde $\pi(c) \neq \pi(a) \cdot \pi(b)$. Por exemplo,

$$(1,2,1,1,2) \in (1,2) * (1,1,2),$$

mas

$$\pi((1,2,1,1,2)) = x^5y^2$$

e

$$\pi((1,2)) \cdot \pi((1,1,2)) = x^5y^4.$$

Um enfraquecimento na hipótese de π ser totalmente multiplicativa é importante nos prefabs exponenciais estudados na próxima seção. Na realidade, multiplicatividade total é requerida em [BG 1]. Se mantivéssemos esta restrição, não poderíamos aplicar o teorema básico ao problema de seqüências em pauta.

Da igualdade para o inventário de $S^{(n)}$ obtida acima, obtemos os seguintes corolários que, em princípio, resolvem o problema proposto no começo da seção:

(III.2.a) COROLÁRIO: A função geradora em y

$$\sum_{d \geq 1} f(n,k,d)\, y^d$$

onde $f(n,k,d)$ é o número de seqüências em $S(n,k)$ contendo precisamente d símbolos distintos é o coeficiente de x^k no produto da expansão de

$$\left[ye^x - (y-1)\right]^n$$

por $k!$

PROVA: Este corolário é um conseqüência direta da expressão de

$\mathrm{Inv}_{\kappa,\pi}(S^{(n)})$ e da interpretação das funções peso π e corretiva κ. □

(III.2.b) COROLÁRIO: Seja $f(n,\kappa,d)$ definida como no corolário anterior. Temos

$$f(n,k,d) = \left\{ \left[y^d\right] \quad \left[x^k\right] \quad \left\{ k! \quad \left[ye^x-(y-1)\right]^n \right\} \right\} .$$

PROVA: Imediata conseqüência de (III.2.a).

Antes de prosseguirmos, vamos exemplificar os corolários acima para $n=k=3$. O conjunto $S(3,3)$ é

$$S(3,3) = \{1,2,3\} \times \{1,2,3\} \times \{1,2,3\}.$$

Pelo Corolário (III.2.a) a função geradora para $S(3,3)$ com respeito a número de símbolos distintos é

$$\left[x^3\right] \left\{ 3! \quad \left[ye^x-(y-1)\right]^3 \right\} = 6y^3 + 18y^2 + 3y^1.$$

Este polinômio em y nos diz pelo corolário (III.2.b) que existem 6 membros de $S(3,3)$ com 3 símbolos distintos, 18 membros de $S(3,3)$ com 2 símbolos distintos e 3 membros de $S(3,3)$ com apenas 1 símbolo. Estes valores podem (e devem) ser diretamente comprovados com uma lista explícita dos elementos de $S(3,3)$.

Vamos agora trabalhar para obter uma fórmula simples em termos de n e k do valor esperado para o número de símbolos distintos nas seqüências em n símbolos de comprimento k. Isto é, queremos calcular

$$\frac{1}{n^k} \sum_{d \geq 1} d.f(n,k,d).$$

Observe que deduzimos uma expressão para cada $f(n,k,d)$ individualmente no último corolário. Vamos, no entanto, obter uma expressão bem simples para o somatório acima, ilustrando o uso de derivadas (parciais) para contar!

Temos a igualdade

$$\sum_{d\geq 1} d.f(n,k,d) = \frac{d}{dy}\left\{\sum_{d\geq 1} f(n,k,d)y^d\right\}_{y=1}.$$

Pelo corolário (III.2.a) a expressão da direita vale

$$\frac{d}{dy}\left\{\left[x^k\right]\left\{k!\ \left[ye^x-(y-1)^n\right]\right\}\right\}_{y=1}.$$

É simples verificar que os operadores diferencial e extrator comutam. Assim obtemos

$$\left[x^k\right]\left\{k!\ \frac{\partial}{\partial y}\left\{\left[ye^x-(y-1)\right]^n\right\}_{y=1}\right\}$$

$$= \left[x^k\right]\left\{k!\left\{n\left[ye^x-(y-1)\right]^{n-1}\ (e^x-1)\right\}_{y=1}\right\}.$$

Fazendo $y=1$

$$= \left[x^k\right]\left\{k!\ \left[ne^{nx-x}\ (e^x-1)\right]\right\}$$

$$= n\ k!\ \left[x^k\right]\left\{e^{nx}\ -\ e^{(n-1)x}\right\}$$

$$= n\left[n^k\ -\ (n-1)^k\right].$$

Desse modo concluímos que

$$\sum_{d\geq 1} d\ f(n,k,d) = n\left[n^k\ -\ (n-1)^k\right].$$

Vamos comparar o valor desta fórmula com a contagem direta no caso, $k=n=3$. Temos pela fórmula

$$3(3^3-2^3) = 57.$$

Já calculamos antes que existem 6, 18 e 3 seqüências em $S(3,3)$ com 3,2, e 1 símbolos distintos respectivamente. Note que

$$3 \times 6 + 2 \times 18 + 1 \times 3 = 57,$$

como previsto pela fórmula.

Dividindo a soma ponderada dos $f(n,k,d)$ obtida acima por n^k, que é o número total de elementos em $S(n,k)$ obtemos

(III.2.c) PROPOSIÇÃO: O valor esperado para o número de símbolos distintos nas seqüências de $S(n,k)$ é

$$n\left[1 - (\frac{n-1}{n})^k\right]. \quad \square$$

É interessante calcular o limite desta expressão dividida por n no caso em que $k=n \longrightarrow \infty$:

$$\lim_{n\to\infty}\left[1 - (1 - \frac{1}{n})^n\right] = 1 - \frac{1}{e} = \frac{e-1}{e}.$$

A fração $\frac{e-1}{e}$ representa aproximadamente $\frac{E(n,n)}{n}$ para n grande, onde $E(n,k)$ é o valor esperado do número de símbolos distintos nas seqüências em $S(n,k)$. Foi a curiosa resposta $\frac{e-1}{e}$ que tínhamos em mente para a pergunta título desta seção.

NOTAS

Derivar uma função geradora e calculá-la no ponto 1 é uma técnica geral para se obter valores esperados de experimentos aleatórios discretos. Assim, o método de solução apresentado nesta seção nada tem de particular. Observe que em tais casos, o problema fundamental é o de enumeração de subconjuntos especiais: "quantos de tal tipo?". Isto porque o número total de possibilidades usualmente é fácil de ser computado permitindo calcular as probabilidades. Reflita também no poder desta técnica que permite, no exemplo que apresentamos e em muitos outros, expressar o valor de uma soma "maluca" de maneira tão concisa. Além disso a característica curiosa de tais problemas é que as parcelas da soma são trabalhosas de computar, veja o corolário (III.2.b). No entanto, para encontrar a soma simples precisamos primeiro descobrir as parcelas complicadas!

Podemos também encontrar a variância [ME 1] de um experimento aleatório discreto a partir de uma função geradora g que nos diz: "tantos casos de tal tipo". É suficiente calcular [KN 3, pg 37] o valor

$$g''(1) + g'(1) - (g'(1))^2$$

e dividir pelo quadrado do número de casos. Em nosso exemplo temos para n e k fixos

$$g(y) = \sum_{d \geq 1} f(n,k,d)y^d$$

Efetuando os cálculos encontramos para a variância o valor

$$\frac{1}{n^{2k}} \left[n(n-1)^k \, n^k - (n-1)^{2k} + n(n-1)(n-2)^k \, n^k \right].$$

III.3 - TEOREMA EXPONENCIAL E GRAFOS ROTULADOS

Suponha que $(C,*,\kappa)$ é um prefab, P o conjunto de primo e π é um peso multiplicativo para $*$. Se as condições seguintes forem verificadas, $(C,*,\kappa,\pi)$ é chamada um *prefab exponencial*:

(d) Para todo $p \in P$ e $n \geq 0$

(d_1) $a,b \in p^n$ implica $\pi(a) = \pi(b) = (\pi(p))^n$

(d_2) $|p^n| = \dfrac{\kappa(p^n)}{(\kappa(p))^n\, n!}$

A restrição (d_1) é automaticamente satisfeita se o peso é totalmente multiplicativo, isto é, se $c \in a * b$ implica $\pi(c)=\pi(a)\,\pi(b)$, para todo a,b independentes de serem primos ou não. A restrição (d_2), ao ser comparada com o axioma (c_2) para prefabs, diz intuitivamente que multiplicar primos iguais é como multiplicar primos desiguais, exceto pela confusão que faz aparecer n! vezes o mesmo produto em p^n, e daí a divisão por n!.

O teorema seguinte dá uma expressão elegante para o inventário de C em função do inventário dos primos para prefabs exponenciais. Este teorema explica, em parte, a freqüência com que a função exponencial aparece em problemas de enumeração.

(III.3.a) TEOREMA EXPONENCIAL: Se $(C,*,\kappa,\pi)$ é um prefab exponencial com conjunto de primos P, então

$$\mathrm{Inv}_{\kappa,\pi}(C) = \exp\left[\mathrm{Inv}_{\kappa,\pi}(P)\right].$$

PROVA: Observe que um prefab exponencial satisfaz às condições do teorema básico (III.1.6). (A recíproca não é verdadeira, veja o exemplo tratado na seção III.2.)

Pelo Teorema (III.1.6)

$$\mathrm{Inv}_{\kappa,\pi}(C) = \prod_{p \in P}\left(\sum_{n\geq 0} \frac{\pi(p^n)}{\kappa(p^n)}\,|p^n|\right).$$

Como temos um prefab exponencial

$$\pi(p^n) = (\pi(p))^n$$

$$|p^n| = \frac{\kappa(p^n)}{(\kappa(p))^n\, n!}\,,$$

e introduzindo estas relações obtemos

$$\mathrm{Inv}_{\kappa,\pi}(C) = \prod_{p\in P}\left(\sum_{n\geq 0}\frac{(\pi(p))^n}{(\kappa(p))^n\, n!}\right)$$

$$= \prod_{p\in P}\exp\frac{\pi(p)}{\kappa(p)}$$

$$= \exp\sum_{p\in P}\frac{\pi(p)}{\kappa(p)}$$

$$= \exp\left[\mathrm{Inv}_{\kappa,\pi}(P)\right],$$

demonstrando o teorema. □

Vamos, no resto desta seção, construir um prefab (fácilmente extensível a um prefab exponencial por escolhas óbvias de funções pesos) bastante geral. Este prefab é usado para resolver problemas de enumeração aparentemente distintos como por exemplo: Quantas partições tem um conjunto de n elementos? Quantas das permutações do grupo simétrico S_n têm exatamente k ciclos? Quantas permutações em S_n não têm ponto fixo?

(III.3.b) EXEMPLO: GRAFOS ROTULADOS

G é um grafo bem *rotulado* se os $|V(G)| = n$ vértices de G são identificados pelos números $1,2,\ldots,n$. A priori, não há nada especial acerca dos símbolos $1,2,\ldots,n$. Certamente os grafos ro

tulados com a,b,c estão em bijeção natural com os grafos rotulados com 1,2,3. No entanto, por questões de referências e para aproveitar a "ordem natural dos naturais" introduzimos o conceito de grafo bem rotulado. Dois grafos bem rotulados são iguais se e somente se a bijeção natural entre seus vértices que, para todo i, manda o vértice i no vértice i, pode ser complementada por uma bijeção conveniente das arestas de forma a constituir um isomorfismo de grafos.

Seja ψ o conjunto de grafos bem rotulados (com número finito de vértices). Vamos construir um prefab com base em ψ que para muitos pesos úteis é um prefab exponencial. Os primos do prefab são os grafos bem rotulados conexos. O elemento neutro para $*$ é o grafo rotulado vazio que tem sua existência postulada exatamente para este fim.

Para definir a composição multivada $*$ de dois grafos bem rotulados, precisamos introduzir alguma terminologia. Para um inteiro positivo k seja N_k o conjunto $\{1,2,\ldots,k\}$. Para cada A, subconjunto finito não vazio de $\mathbb{N}\setminus\{0\}$, considere a função bijetiva

$$\rho_A : N_{|A|} \longrightarrow A$$

definida para $i \in N_{|A|}$ por

$$\rho_A(i) \text{ é o } i\text{-ésimo elemento de } A.$$

Se G é um grafo bem rotulado e A é um subconjunto dos inteiros positivos com $|A| = |V(G)|$, então G(A) é o grafo rotulado obtido a partir de G trocando o rótulo do vértice i por $\rho_A(i)$.

A definição de $*$ é a seguinte. Para $G, G_2 \in \psi$,

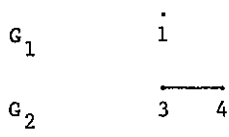
$$G_1 * G_2 = \{G_1(A) \cup G_2(\bar{A}) : A \subseteq N_{|V(G_1)|+|V(G_2)|}$$

$$\text{e } |A| = |V(G_1)|\},$$

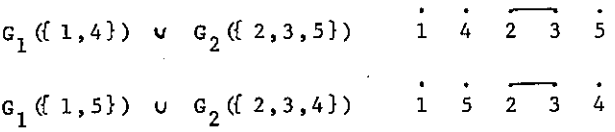
onde a união (disjunta) dos dois grafos $G_1(A)$ e $G_2(\bar{A})$ significa o grafo cujas componentes são as componentes de $G_1(A)$ juntamente com as componentes de $G_2(\bar{A})$. Evidentemente, o complemento $\bar{A}$ de A é tomado com relação a

$$^{N}|V(G_1)|+|V(G_2)|.$$

Note que na definição acima podemos ter subconjuntos A e A' diferentes, dando origem ao mesmo grafo. Por exemplo, sejam



Temos



e embora $A = \{1,4\}$, $A' = \{1,5\}$ sejam diferentes, os grafos bem rotulados resultantes são evidentemente iguais.

Como $G_1 * G_2$ é um subconjunto (não um multiconjunto) de grafos bem rotulados, estas diplicatas devem desaparecer e só devemos consevar um grafo de cada tipo. No exemplo de G_1 e G_2 dado acima embora hajam em princípio $\binom{2+3}{2} = 10$ candidatos para elementos de $G_1 * G_2$ só 6 são diferentes depois de eliminadas as duplicatas. Um exercício simples, porém útil para ajudar a compreensão da definição de $G_1 * G_2$ em geral é encontrar os 6 grafos bem rotulados que aparecem no caso particular mencionado.

Um fato importante é o seguinte: duplicatas em $G_1 * G_2$ só são possíveis no caso em que G_1 e G_2 não forem coprimos. Se as componentes bem rotuladas são diferentes, então duplicata é impossível, pois não podemos "confundir," para $A \neq A'$ uma componente de $G_1(A) \cup G_2(\bar{A})$ com uma componente de $G_1(A') \cup G_2(\bar{A}')$. Veja no exemplo acima que trocamos as componentes constituídas, cada uma, por um único vértice rotulado 4 numa delas e 5 na outra. Se a

ordem das componentes fosse levada em consideração, não haveria duplicatas.

A observação acima nos induz a definir a função corretiva κ como

$$\kappa(G) = |V(G)| \; !$$

Com esta definição o axioma (c_1) é (trivialmente) satisfeito e para G_1 e G_2 coprimos

$$|G_1 * G_2| = \binom{|V(G_1)|+|V(G_2)|}{|V(G_1)|}$$

$$= \frac{(|V(G_1)| + |V(G_2)|)!}{|V(G_1)| \; ! \; |V(G_2)|!}$$

$$= \frac{\kappa(G_1 * G_2)}{\kappa(G_1)\kappa(G_2)},$$

verificando o axioma (c_2).

Para verificar a comutatividade de $*$ sejam G_1 e G_2 grafos bem rotulados. Se $G \in G_1 * G_2$, então existe

$$A \subseteq N_{|V(G_1)|+|V(G_2)|} \; , \; |A| = |V(G_1)|$$

tal que

$$G = G_1(A) \cup G_2(B)$$

onde B é o complemento de A em $N_{|V(G_1)|+|V(G_1)|}$. Como a união de grafos é comutativa,

$$G = G_2(B) \cup G_1(A)$$

e portanto $G \in G_2 * G_1$, concluindo que $G_1 * G_2 \subseteq G_2 * G_1$. Do mesmo modo se prova a inclusão inversa. Logo $G_1 * G_2 = G_2 * G_1$, provando a comutatividade de $*$. A prova da associatividade é um pouco técnica e por isto a enuncamos sob forma de proposição para futura re-

ferências.

(III.3.c) PROPOSIÇÃO: A composição $*$ de grafos bem rotulados é associativa.

PROVA: Sejam G_1, G_2 e G_3 grafos bem rotulados com v_1, v_2 e v_3 vértices respectivamente. Por definição,

$$G \in (G_1 * G_2) * G_3$$

significa que existem partições (A_1,A_2) de $N_{v_1+v_2+v_3}$ e (A_3,A_4) de $N_{v_1+v_2}$ tais que

$$G = (G_1(A_3) \cup G_2(A_4))\ (A_1) \cup G_3(A_2)$$

$$= G_1(\rho_{A_1}(A_3)) \cup G_2(\rho_{A_1}(A_4)) \cup G_3(A_2).$$

Observe que $(\rho_{A_1}(A_4), A_2)$ é uma partição de $N_{v_2+v_3}$. Seja A_5 o complemento de $\rho_1(A_3)$ em $N_{v_1+v_2+v_3}$. Podemos então escrever

$$G = G_1(\rho_{A_1}(A_3)) \cup (G_2(\rho_{A_5}^{-1}\ \rho_{A_1}(A_4)) \cup G_3(\rho_{A_5}^{-1}\ (A_2)))(A_5).$$

Desse modo, existem partições $(B_1,B_2) = (\rho_{A_1}(A_3), A_5)$ de $N_{v_1+v_2+v_3}$ e $(B_3,B_4) = (\rho_{A_5}^{-1}\ \rho_{A_1}(A_4), \rho_{A_5}^{-1}(A_2))$ de $N_{v_2+v_3}$ tais que

$$G = G_1(B_1) \cup (G_2(B_3) \cup G_2(B_4))\ (B_2),$$

e isto significa, por definição, que $G \in G_1 * (G_2 * G_3)$. Assim concluimos

$$(G_1 * G_2) * G_3 \subseteq G_1 * (G_2 * G_3).$$

A prova da inclusão inversa é inteiramente análoga. □

Uma vez que o elemento neutro para $*$ é o grafo bem rotulado vazio, temos comprovado para $(\psi,*,K]$ os axiomas tipo (a) e (c) de prefabs.

O axioma (b_1) que diz respeito à fatorização única é verificado da seguinte maneira. Seja G um grafo bem rotulado e $G_1, G_2, \ldots, G_k$ as suas componentes cujos conjuntos de rótulos são respectivamente, $R_1, R_2, \ldots, R_k$. Para $i=1,2,\ldots,k$, seja H_i o grafo bem rotulado obtido a partir de G_i trocando o rótulo r por $\rho_{R_i}^{-1}(r)$. Desse modo

$$G \in H_1 * H_2 * \cdots * H_k$$

e é uma verificação fácil, que deixamos para o leitor, comprovar que o produto acima é único a menos de ordem.

Para verificar axioma (b_2) que diz respeito à fatorização estritamente única seja

$$G \in \left(\prod_{i=1}^{r} P_i^{k_i} \right) * \left(\prod_{j=1}^{s} Q_j^{k_j} \right),$$

onde os grafos bem rotulados P_i's e Q_j's são todos distintos. Isto significa que existe uma partição única $(A_1, A_2, \ldots, A_r)$ de $\{1,2,\ldots,\sum_{i=1}^{r} |V(P_i)|\}$ e uma partição única $(B_1, B_2, \ldots, B_s)$ de $\{1,2,\ldots,\sum_{j=1}^{s} |V(Q_j)|\}$ tais que

$$G \in \left(\bigcup_{i=1}^{r} P_i(A_i) \right) * \left(\bigcup_{j=1}^{s} Q_j(A_j) \right).$$

Note que o primeiro desses grafos pertence ao produto dos P_i's e que o segundo pertence ao produto dos Q_j's. Assim o axioma (b_2) é satisfeito e podemos concluir quase que integralmente o seguinte lema:

(III.3.d) LEMA: O conjunto ψ de grafos bem rotulados, juntamente

com a composição $*$ e a função corretiva $\kappa(G) = |V(G)|!$ é um prefab que satisfaz

$$|G^n| = \frac{\kappa(G^n)}{(\kappa(G))^n\, n!}$$

para todo primo G.

PROVA: Desde que já vimos que $(\psi,*,\kappa)$ é um prefab, o que nos resta mostrar é que a igualdade acima (que é o axioma (d_2) para prefabs exponenciais) é satisfeita. Se G é um primo, isto é, G é um grafo conexo bem rotulado, então o produto de n cópias iguais a G tem cardinalidade.

$$|G * G *\ldots *G| = \frac{(n.|V(G)|)!}{|V(G)|^n\, n!}.$$

A melhor maneira de verificar esta igualdade é convercer-se de que com a ordem dos fatores considerada cada elemento do produto está em bijeção natural com uma partição de $\{1,2,\ldots,(n|V(G)|)\}$ em n partes de $|V(G)|$ elementos cada uma. Existem

$$\frac{(n.|V(G)|)!}{|V(G)|^n}$$

tais partições. Ao eliminarmos a ordem, dividindo por $n!$, obtemos a expressão à direita de $G * G *\ldots *G$.

Assim qualquer grafo conexo bem rotulado G satisfaz

$$|G^n| = \frac{(n|V(G)|)!}{|V(G)|^n\, n!}$$

$$= \frac{\kappa(G^n)}{(\kappa(G))^n\, n!},$$

e o axioma (d_2) está comprovado. □

Podemos escolher a função peso π de diversas maneiras, de forma a tornar $(\psi,*,\kappa)$ um prefab exponencial:

(III.3.e) EXEMPLOS: Seja $\pi(G)$, onde $G \in \psi$, igual a $x^{|V(G)|}$. Então π é totalmente multiplicativa para a composição de grafos bem rotulados e $(\psi,*,\kappa,\pi)$ é um prefab exponencial. O mesmo é verdade tomando $\pi(G) = x^{|V(G)|}\, y^{|A(G)|}$ ou $\pi(G) = x^{|V(G)|}\, y^{k(G)}$ onde $k(G)$ é o número de componentes de G.

(III.3.f) EXEMPLOS: Seja ψ_F o subconjunto de ψ formado pelas florestas bem rotuladas . Então com qualquer dos pesos π do exemplo acima, $(\psi_F,*,\kappa,\pi)$ é um prefab exponencial. Seja ψ_c o subconjunto de ψ cujas componentes são polígonos bem rotulados . Então $(\psi_c,*,\kappa,\pi)$ é um prefab exponencial. Seja ψ_k o subconjunto de ψ cujas componentes são grafos *completos* bem rotulados . Grafos *simples* são grafos onde cada aresta tem duas extremidades distintas e dados dois vértices distintos eles são extremidades de no máximo uma aresta. Um grafo é *completo* se é simples e cada par de vértices distintos são as extremidades de uma aresta. Aqui novamente, $(\psi_k,*,\kappa,\pi)$ é um prefab exponencial.

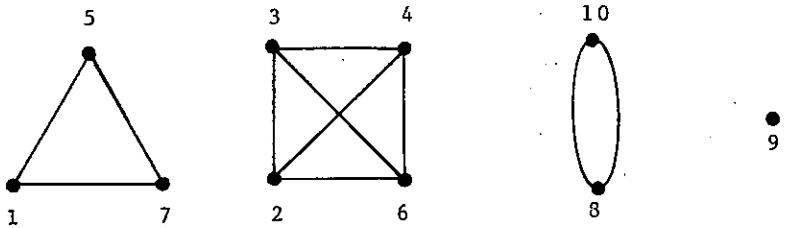
Os exemplos dados acima com ligeiras variações são utilizados na próxima seção e por isto eles devem ser bem entendidos. Verifique que cada um deles satisfaz o axioma (d_1) para prefabs exponenciais.

III.4 - APLICAÇÕES DO TEOREMA EXPONENCIAL

Queremos nesta seção mostrar o papel unificador que o teorema exponencial juntamente com os prefabs baseados em grafos rotulados desempenham em enumeração.

PARTIÇÕES DE CONJUNTOS

Seja $N_m = \{1,2,\ldots,m\}$. De quantas maneiras distintas podemos particionar N_m? Seja ψ_k, como definido num exemplo de (III.3.f), o conjunto dos grafos bem rotulados cujas componentes são grafos completos. Obviamente existe uma bijeção natural entre os membros de ψ_k com m vértices e as partições de N_m. Por exemplo,



está associado à partição $\{\{1,5,7\}, \{3,4,6,2\}, \{8,10\}, \{9\}\}$ de N_{10}.

Definimos, para $G \in \psi_k$, $\pi(G) = x^{|V(G)|}$. Como mencionado em (III,3,f), $(\psi_k,*,\kappa,\pi)$ é um prefab exponencial. Por definição de π, sabemos que

$$[x^m]\{m!\ [Inv_{\kappa,\pi}(\psi_k)]\}$$

é o número procurado. Pelo teorema exponencial,

$$Inv_{\kappa,\pi}(\psi_k) = \exp[Inv_{\kappa,\pi}(P_k)],$$

onde P_k é o conjunto de primos de ψ_k, isto é, o conjunto dos grafos completos conexos e bem rotulados. Ora, o inventário de P_k é trivial de se calcular, porque, para cada $m \geq 1$ só existe 1 elemento de P_k com m vértices. Assim,

$$\mathrm{Inv}_{\kappa,\pi}(P_k) = \sum_{G \in P_k} \frac{\pi(G)}{\kappa(G)}$$

$$= \sum_{m \geq 1} \frac{x^m}{m!}$$

$$= e^x - 1.$$

Usando agora o teorema exponencial, obtemos

(III.4.a) TEOREMA: O número B_m de partições de um conjunto com m elementos é

$$B_m = \left[x^m\right] \left\{ m! \left[e^{e^x - 1} \right] \right\}. \quad \square$$

Note que B_0, o coeficiente de x^0, é 1 que corresponde à única partição do conjunto vazio.

Vamos obter agora uma recorrência para calcular os B_m's, que são chamados *números de Bell*. Seja $f(x) = e^{e^x - 1}$. Derivando f obtemos

$$f'(x) = f(x).e^x.$$

Multiplicando por x e introduzindo os somatórios correspondentes às funções geradoras exponenciais,

$$\sum_{m \geq 1} m\, B_m \frac{x^m}{m!} = \left(\sum_{m \geq 0} B_m \frac{x^{m+1}}{m!} \right) \left(\sum_{m \geq 0} \frac{x^m}{m!} \right)$$

$$= \left(\sum_{m \geq 1} B_{m-1} \frac{x^m}{(m-1)!} \right) \left(\sum_{m \geq 0} \frac{x^m}{m!} \right)$$

$$= \sum_{m \geq 1} \left(\sum_{j=0}^{m-1} \frac{1}{j!\,(m-1-j)!}\, B_{m-1-j} \right) \frac{x^m}{m!}.$$

Para $m \geq 1$ fixo, se multiplicarmos por $(m-1)!$ e igualarmos os coeficientes de x^m obtemos,

$$B_m = \sum_{j=0}^{m-1} \binom{m-1}{m-1-j} B_{m-1-j}.$$

Fazendo $n=m-1$ e $k=m-1-j$, obtemos,

(III.4.b) COROLÁRIO: Os números de Bell satisfazem à seguinte recorrência

$$B_0 = 1$$

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_n \ , \ n \geq 0. \ \square$$

Utilizando esta recorrência encontramos,

n	B_n
0	1
1	1
2	2
3	5
4	15
5	52
6	203
.	.
.	.
.	.

DESARRANJAMENTOS

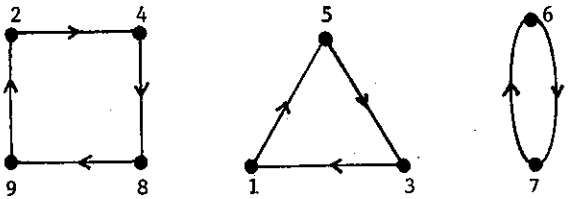
Uma permutação ρ de $N_m = \{1,2,\ldots,m\}$ tal que $\rho(i) \neq i$ para todo i em N_m é chamada um *desarranjamento*. Qual é o número de desarranjamentos em N_m?

O prefab que utilizamos aqui tem como base uma ligeira

variação de ψ_c, mencionado no exemplo (III.3.f). Seja ψ_c^1 o conjunto dos digrafos (grafos com setas dirigindo as arestas) bem rotulados, cujas componentes são polígonos consistentemente dirigidos com pelo menos dois vértices. Existe uma bijeção natural entre os elementos de ψ_c^1 com m vértices e os desarranjamentos de N_m. Por exemplo a permutação cujos ciclos são

$$(1,5,3)\ (7,6)\ (2,4,8,9)$$

corresponde ao seguinte membro de ψ_c^1:



Seja $\pi(G) = x^{|V(G)|}$ para $G \in \psi_c^1$. Agora o leitor já não deve ter dificuldades de concluir que

$$(\psi_c^1, *, \kappa, \pi)$$

é um prefab exponencial. Os primos deste prefab são os polígonos dirigidos bem rotulados e existem $(k-1)!$ deles com k vértices. A resposta da nossa questão é

$$\left[x^m\right]\ \{m!\ \left[\mathrm{Inv}_{\kappa,\pi}(\psi_c^1)\right]\},$$

e pelo teorema exponencial, onde P_c^1 é o conjunto dos primos de ψ_c^1,

$$\mathrm{Inv}_{\kappa,\pi}(\psi_c^1) = \exp\left[\mathrm{Inv}_{\kappa,\pi}(P_c^1)\right]$$

$$\exp\left(\sum_{k\geq 2} (k-1)!\ \frac{x^k}{k!}\right) =$$

$$= \exp\left(\frac{x^2}{2} + \frac{x^3}{3} + \frac{x^4}{4} + \ldots\right)$$

Mas,

$$x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots = -\ell n(1-x) = \left[\ell n(1-x)\right]^{-1}.$$

Assim,

$$\mathrm{Inv}_{K,\pi}(\psi_c^1) = \exp\left\{\left[\ell n(1-x)\right]^{-1} - x\right\}$$
$$= \frac{e^{-x}}{1-x}.$$

Se denotarmos por d_m o número de desarranjamentos de N_m temos então

$$d_m = \left[x^m\right]\left\{m!\left[\frac{e^{-x}}{1-x}\right]\right\}$$
$$= m!\left[x^m\right]\left\{\left[\sum_{n\geq 0}(-1)^n\frac{x^n}{n!}\right]\left[\sum_{n\geq 1}x^n\right]\right\}$$
$$= m!\sum_{n=0}^{m}\frac{(-1)^n}{n!}.$$

Note que o somatório acima é formado pelos primeiros $m+1$ termos no desenvolvimento de e^{-1}. Portanto não é difícil de provar

(III.4.c) TEOREMA: O número d_m de desarranjamentos de

$$N_m = \{1,2,\ldots,m\}$$

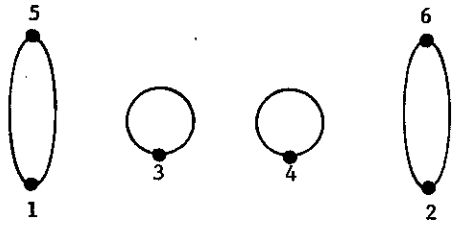
é o inteiro mais próximo de $m!/e$. □

NÚMERO DE INVOLUÇÕES

Uma permutação é chamada de *involução* se é igual à sua inversa. Queremos agora encontrar o número i_m de involuções de S_m, grupo de todas as permutações de $\{1,2,\ldots,m\}$. Uma permutação em

S_m é uma involução se e somente se a sua decomposição em ciclos tem sõmente ciclos de comprimento 1 ou 2.

Seja ψ_c^2 o conjunto de grafos bem rotulados cujas componentes são polígonos contendo 1 ou 2 vértices. Existe uma bijeção natural entre os elementos de ψ_c^2 tendo m vértices e as involuções de S_m. Por exemplo,



está associado à involução (15) (3) (4) (26). Seja $\pi(G) = x^{|V(G)|}$. Desse modo temos um prefab exponencial

$$(\psi_c^2, *, \kappa, \pi),$$

e o número i_m que queremos é

$$i_m = \left[x^m\right] \left\{ m! \left[\mathrm{Inv}_{\kappa,\pi}(\psi_c^2) \right] \right\}.$$

Seja P_c^2 o conjunto dos primos de ψ_c^2. Note que $\mathrm{Inv}_{\kappa,\pi}(P_c^2) = x + \frac{x^2}{2}$ (existem apenas dois primos).

Usando o teorema exponencial concluímos

$$\mathrm{Inv}_{\kappa,\pi}(\psi_c^2) = \exp(x + \tfrac{x^2}{2}).$$

Assim,

(III.4.d) TEOREMA: O número de involuções em S_m é

$$i_m = \left[x^m\right] \left\{ m! \left[\exp(x + \tfrac{x^2}{2}) \right] \right\}. \square$$

Agora vamos obter uma recorrência que permite o cálculo

simples dos i_n's. Seja

$$i(x) = \exp(x + \frac{x^2}{2}) = \sum_{n\geq 0} \frac{i_n x^n}{n!} .$$

Note que $i(x)$ satisfaz $i'(x) = i(x)\,(1+n)$ e que $i_o=1$. Logo,

$$\sum_{n\geq 1} n\, i_n \frac{x^{n-1}}{n!} = (1+x)\left(\sum_{n\geq 0} i_n \frac{x^n}{n!}\right)$$

$$= 1 + \sum_{n\geq 1}\left(\frac{i_n}{n!} + \frac{i_{n-1}}{(n-1)!}\right) x^n .$$

Fixando $n=m\geq 1$, multiplicando por $m!$ e igualando os coeficientes de x^m obtemos

(III.4.e) COROLÁRIO: Os números i_m's de involução em S_m satisfazem à seguinte recorrência

$$i_o = 1$$

$$i_{m+1} = i_m + m\, i_{m-1} \ , \ m\geq 0. \square$$

Os primeiros 15 valores de i_m são

m	i_m
1	1
2	2
3	4
4	10
5	26
6	76
7	232
8	764
9	2620
10	9496
11	35696
12	140152
13	568504
14	2390480
15	10349536

ÁRVORES ROTULADAS

Um grafo bem rotulado conexo e sem polígonos é chamado, naturalmente, uma árvore bem rotulada. Quantas árvores bem rotuladas existem?

Seja ψ_F como definido no exemplo (III.3.f) e

$$\pi(G) = x^{|V(G)|}$$

para $G \in \psi_F$. Usando que $(\psi_F, *, \kappa, \pi)$ é um prefab exponencial podemos escrever

$$\mathrm{Inv}_{\kappa,\pi}(\psi) = \exp\left[\mathrm{Inv}_{\kappa,\pi}(A_F)\right],$$

onde A_F é o conjunto de primos de ψ_F, isto é, o conjunto das árvores bem rotuladas. No entanto usando esta idéia chegamos a um impasse, pois não há maneira simples de expressar o número de florestas bem rotuladas a partir do de árvores bem rotuladas. Isto nos induz a considerar florestas bem rotuladas *com raízes*, isto é, um dos vértices de cada componente da floresta bem rotulada, é distinguido, digamos, pintando-o com uma cor diferente das dos demais. Seja ψ_F^r o conjunto das florestas bem rotuladas com raízes e P_F^r o das árvores bem rotuladas com raíz. Se mantivermos os vértices raízes fixos na re-rotulação que define a composição, observamos facilmente que

$$(\psi_F^r, *, \kappa, \pi)$$

é também um prefab exponencial e que P_F^r é o seu conjunto de primos.

Denotemos por

$$F^r(x) = \sum_{n\geq 0} F_n \frac{x^n}{n!} = \mathrm{Inv}_{\kappa,\pi}(\psi_F^r)$$

$$A^r(x) = \sum_{n\geq 1} A_n \frac{x^n}{n!} = \mathrm{Inv}_{\kappa,\pi}(P_F^r)$$

as funções geradoras exponenciais (por número de vértices) para as florestas bem rotuladas com raízes e as árvores bem rotuladas com raíz.

Pelo teorema exponencial,

$$F^r(x) = \exp(A^r(x))$$

e agora podemos expressar F^r em função de A^r. Uma floresta bem rotulada com raízes tendo n vértices dá origem a n+1 árvores bem rotuladas com raíz, ao adicionarmos um novo vértice rotulado n+1, ligando-o às raízes de cada componente da floresta e escolhendo cada ponto da árvore resultante como uma possível raíz. Este processo é invertível. Assim, $(n+1)\, F_n = A_{n+1}$. Para utilizar esta relação, multipliquemos a identidade das florestas, acima, por x,

$$xF^r(x) = \sum_{n\geq 0} F_n \frac{x^{n+1}}{n!}$$

$$= \sum_{n\geq 0} (n+1)\, F_n \frac{x^{n+1}}{(n+1)!}$$

$$= \sum_{n\geq 0} A_{n+1} \frac{x^{n+1}}{(n+1)!}$$

$$= \sum_{n\geq 1} A_n \frac{x^n}{n!} = A(x).$$

Desse modo obtemos a seguinte equação funcional para A^r:

$$A^r(x) = x \exp(A^r(x)).$$

Esta equação funcional foi originalmente obtida por Polya [PO 1] e é exatamente a que resolvemos no exemplo (I.3.e), para ilustrar o uso da fórmula de Lagrange (enunciada sem prova como teorema (I.3.d)). A solução é

$$A^r(x) = \sum_{n\geq 1} n^{n-1} \frac{x^n}{n!}$$

e assim podemos enunciar

(III.4.f) TEOREMA: O número de árvores enraizadas com n vértices e com rótulos nos vértices é n^{n-1}. □

(III.4.g) COROLÁRIO; O número de árvores bem rotuladas com n vértices é n^{n-2}.

PROVA: Cada árvore com n vértices, bem rotulada corresponde, fazendo a raíz variar entre os n vértices, a n árvores bem rotuladas com raíz. Assim para obter o número daquelas, dividimos o número destas por n. □

A descoberta que expressão do número de árvores bem rotuladas com n vértices é n^{n-2} foi feita por Cayley ainda no século passado. Existem muitas maneiras de se chegar a este resultado. No exercício 10 propomos uma maneira algorítmica bastante interessante, conhecida como *código de Prüfer*.

PERMUTAÇÕES COM K CICLOS

Nesta subseção vamos encontrar o número $c_{n,k}$ das permutações em S_n com exatamente k ciclos.

Seja ψ_c o conjunto dos digrafos bem rotulados cujas componentes são polígonos consistentemente dirigidos. (A diferença para ψ_c^1 (considerado quando tratamos desarranjamentos) é a de que agora permitimos polígonos de 1 só lado. Seja

$$\pi(G) = x^{|V(G)|}\, y^{k(G)}$$

como definido em (III.3.e). Obtemos um prefab exponencial

$$(\psi_c, *, \kappa, \pi).$$

Usando a mesma idéia dos desarranjamentos, ψ_c está em bijeção natural agora com todas as permutações em

$$\bigcup_{n\geq 0} S_n .$$

O que queremos saber é

$$c_{n,k} = \left[y^k\right]\left\{\left[x^n\right]\left\{n!\ \left[\mathrm{Inv}_{\kappa,\pi}(\psi_c^2)\right]\right\}\right\}.$$

Seja P_c o conjunto dos primos de ψ_c. Temos

$$\mathrm{Inv}_{\kappa,\pi}(P_c) = \sum_{G\in P_c} \frac{\pi(G)}{\kappa(G)}$$

$$= \sum_{n\geq 1} (n-1)!\ \frac{x^n y}{n!},$$

uma vez que existem $(n-1)!$ primos com peso $\frac{x^n y}{n!}$. Simplificando podemos escrever

$$\mathrm{Inv}_{\kappa,\pi}(P_c) = \sum_{n\geq 1} \frac{x^n y}{n}$$

$$= -y\ \ell n(1-x).$$

Usando o teorema exponencial obtemos

$$\mathrm{Inv}_{\kappa,\pi}(\psi_c) = \exp\left[-y\ \ell n(1-x)\right]$$

$$= (1-x)^{-y}.$$

Expandindo $(1-x)^{-y}$ pelo teorema binomial (enunciado antes de (I.2.a)) obtemos

$$(1-x)^{-y} = \sum_{n\geq 0} (-1)^n \binom{-y}{n} x^n$$

$$= \sum_{n\geq 0} (-1)^n \left[(-1)^n \binom{y+n-1}{n} \right] x^n$$

$$= \sum_{n\geq 0} \binom{y+n-1}{n} x^n$$

$$= \sum_{n\geq 0} \left[(y+n-1)(y+n-2)\ldots(y+1)(y) \right] \frac{x^n}{n!}.$$

Assim obtemos

(III.4.h) TEOREMA: O número de permutações em S_n com exatamente k ciclos é

$$c_{n,k} = \left[y^k \right] \left\{ y(y+1)\ldots(y+n-1) \right\}. \quad \square$$

A partir desta expressão, podemos calcular os coeficientes $c_{n,k}$ recursivamente. Para isto, seja $f_n(y)$ a expressão entre chaves acima. Claramente, para $n\geq 1$,

$$f_{n+1}(y) = f_n(y)(y+n),$$

logo, para k, $2\leq k\leq n$,

$$\left[y^k \right] \{ f_{n+1}(y) \} = \left[y^k \right] \{ f_n(y).(y+n) \}$$

ou

$$c_{n+1,k} = c_{n,k-1} + n\, c_{n,k}.$$

Os valores de fronteira desta recorrência são obtidos diretamente do que os $c_{n,k}$'s contam. Como o número de membros de S_n tendo n ciclos é 1, (correspondendo à permutação identidade) temos para $n\geq 1$, $c_{n,n} = 1$. O número de permutações em S_n tendo 1 ciclo (permutações circulares) é $(n-1)!$. Assim, para $n\geq 1$, $c_{n,1}=(n-1)!$ Estas observações nos dão o seguinte esquema de recorrência, de

onde os números $c_{n,k}$'s podem ser facilmente obtidos:

(III.4.i) COROLÁRIO: Os números $c_{n,k}$'s de permutações em S_n com k ciclos satisfazem à seguinte recorrência:

$$c_{n,1} = (n-1)! \quad , n \geq 1$$

$$c_{n,n} = 1 \quad , n \geq 1$$

$$c_{n+1,k} = c_{n,k-1} + n\, c_{n,k}, \quad 1 < k \leq n.$$

Usando estas relações construimos a seguinte tabela dos primeiros $c_{n,k}$'s:

n \ k	1	2	3	4	5	6
1	1	0	0	0	0	0
2	1	1	0	0	0	0
3	2	3	1	0	0	0
4	6	11	6	1	0	0
5	24	50	35	10	1	0
6	120	274	225	85	15	1

Como era de se esperar, a soma das entradas da n-ésima linha desta tabela é n!.

ÍNDICE DE CICLOS DE S_n

Vamos agora usar o teorema exponencial para obter certos polinômios que são muito úteis no capítulo V.

A cada permutação $\alpha \in S_n$ associemos o monômio em n variáveis

$$\omega(\alpha) = x_1^{b_1(\alpha)}\, x_2^{b_2(\alpha)} \cdots x_n^{b_n(\alpha)},$$

onde $b_i(\alpha)$ é o número de ciclos de comprimento i na decomposição de α em ciclos disjuntos. Queremos calcular o polinômio

$$\gamma_n = \frac{1}{n!} \sum_{\alpha \in S_n} \omega(\alpha)\, z^n$$

que é chamado de *índice de ciclos* de S_n. Índices de ciclos de grupos de permutações são fundamentais na teoria de Polya, tratada no capítulo V. Para encontrar γ_n, se $\alpha \in S_n$ definamos

$$\pi'(\alpha) = \omega(\alpha) z^n,$$

e identificando α com um conjunto de polígonos obtemos um prefab exponencial $(\psi_c, *, \kappa, \pi')$, onde ψ_c, $*$ e κ são os mesmos do exemplo anteiror. Desse modo

$$\gamma_n = \left[z^n\right]\left\{n!\left[\frac{1}{n!}\,\mathrm{Inv}_{\kappa,\pi'}(\psi_c)\right]\right\}$$
$$= \left[z^n\right]\left\{\mathrm{Inv}_{\kappa,\pi'}(\psi_c)\right\}.$$

Com o peso π' temos para o inventário de P_c

$$\mathrm{Inv}_{\kappa,\pi'}(P_c) = \sum_{n\geq 1} \frac{x_n y}{n}.$$

(Note o fato curioso de que a única diferença do inventário do mesmo conjunto com o peso π do exemplo anterior é que x^n é aqui substituído por x_n.)

Usando o Teorema exponencial e o valor acima para γ_n:

(III.4.j) TEOREMA: O índice de ciclos de S_n é

$$\gamma_n = \left[z^n\right]\left\{\exp\left[\sum_{m\geq 1} \frac{z^m x_m}{m}\right]\right\}. \quad \square$$

Como feito nos exemplos anteriores deduzimos agora como um corolário uma recorrência para os γ_n's. Seja

$$f(z) = \exp\left(\sum_{m\geq 1} \frac{z^m x_m}{m}\right).$$

Derivando e multiplicando por z obtemos

$$zf'(z) = f(z) \sum_{m\geq 1} z^m x_m .$$

Igualando os coeficientes de z^m concluímos

(III.4.k) COROLÁRIO: Os índices de ciclos γ_m's, dos grupos simétricos, satisfazem à seguinte recorrência:

$$\gamma_o = 1$$

$$\gamma_m = \frac{1}{m} \sum_{i=1}^{m-1} \gamma_i \, x_{m-i} . \quad \square$$

Utilizando esta recorrência, obtemos sem difilcudades

$$\gamma_1 = x_1$$

$$\gamma_2 = \frac{1}{2} (x_1^2+x_2)$$

$$\gamma_3 = \frac{1}{6} = (x_1^3+3x_2x_1+2x_3)$$

$$\gamma_4 = \frac{1}{24} (x_1^4+6x_1^2x_2+3x_2^2+8x_1x_3+6x^4)$$

$$\gamma_5 = \frac{1}{120} (x_1^5+10x_1^3x_2+15x_1x_2^2+20x_1^2x_3+30x_1x_4+20x_2x_3+24x_5).$$

Estes polinômios desempenham papel relevante na enumeração de grafos e digrafos, como mostramos no capítulo V.

EXERCÍCIOS

1. Quantas involuções sem ponto fixo existem em S_n? Dê a resposta sob a forma de recorrência.

2. Mostre que o número de permutações em S_n que não têm ciclo ímpar é

$$\left[x^n\right] \left\{ n! \ (1-x^2)^{\frac{1}{2}} \right\}$$

3. Generalize o exercício anterior mostrando que o número de permutações em S_n cujos ciclos têm comprimento múltiplo de um certo k é

$$\left[x^n\right]\left\{n!\,(1-x^k)^{1/k}\right\}.$$

4. Encontre a função geradora exponencial para o número de permutações em S_n com k ciclos nenhum dos quais tem um ponto fixo.

5. Deduza uma recorrência para responder ao exercício anterior e encontre o número de permutações desejadas para k=3, n=7.

6. Quantas partições de um conjunto com n elementos existem com a restrição de que as classes das partições têm 2 ou 3 elementos.

7. Quantas permutações em S_{10} satisfazem a propriedade de que o seu cubo é a identidade? Dê uma resposta numérica à esta pergunta.

8. Baseando-se na dedução da fórmula para B_n dada no teorema (III.4.a) convença-se de que o número S_n^k de maneiras distintas de se colocar n objetos em k caixas ordenadas sem que nenhuma fique vazia é

$$S_n^k = \left[y^k\right]\left\{\left[x^n\right]\left\{n!\; e^{y(e^x-1)}\right\}\right\}.$$

(Nota: os números S_n^k's são chamados de números de Stirling de segunda espécie.)

9. Aceitando a fórmula para S_n^k dada no exercício anterior mostre que

$$S_{n+1}^k = S_n^{k-1} + k\, S_n^k$$

e que

$$S_n^1 = S_n^n = 1.$$

Tente provar estas identidades diretamente da interpretação combinatorial de S_n^k.

10. Seja A uma árvore cujos rótulos dos vértices são $\{1,2,\ldots,n\}$. Remova o vértice pendente tendo o menor rótulo e escreva o rótulo do seu único vizinho. Repita este processo com a árvore resultante, até que reste uma árvore com só um vértice. Isto associa à árvore original A uma sequência de n-1 números chamado o *código de Prüfer* de A. Prove que

    (a) O código de Prüfer de A caracteriza A univocamente.

    (b) Dada qualquer sequência $(a_1,a_2,\ldots,a_{n-1})$ tal que $1 \leq a_i \leq n$ e $a_{n-1} = n$, existe uma única árvore com este código de Prüfer.

    (c) Prove a fórmula de Cayley: existem n^{n-2} árvores rotuladas com n vértices.

11. Prove que os números de desarranjamentos satisfazem às seguintes recorrências

$$d_n = n\, d_{n-1} + (-1)^n \quad , \quad n \geq 2$$

$$d_n = (n-1)(d_{n-2} + d_{n-1}) \quad n \geq 3$$

Prove que $d_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor$ é ímpar se e somente se n é par.

12. De quantas maneiras distintas podem n casais dançarem simultaneamente numa festa com a restrição de que nenhum homem dança com sua esposa?

13. Construa um prefab análogo ao da seção (III.2) e use o teorema multiplicativo (III.1.b) para dizer quantas palavras de comprimento n nas letras a,b existem onde cada uma delas ocorre um número ímpar de vezes.

CAPÍTULO IV

INVERTER PARA CONTAR

IV. - A FUNÇÃO DE MÖBIUS

Neste capítulo vamos explorar uma idéia das mais antigas em enumeração: a de que em muitos casos é possível através do conhecimento de somas se obter as parcelas. O exemplo trivial disto é que conhecendo a soma dos i primeiros termos de uma série $1 \leq i \leq n$, é possível encontrar a sequência dos termos. Extensões desta idéia, no contexto de conjuntos parcialmente ordenados em geral, formam a base para técnicas importantes em enumeração. Introduzimos a seguir alguns conceitos que conduzem à definição da função de Möbius, que é, conceitualmente, a idéia central do capítulo.

Seja P um conjunto parcialmente ordenado, ou *poset* (do inglês "partial ordered set"). Isto é, existe uma relação binária "$\leq$" em P, que é reflexiva, antisimétrica e transitiva. Uma relação R é *antisimétrica* se xRy e yRx implicam $x=y$.

Sejam x,y elementos de um poset $(P, \leq)$ tais que $x \leq y$. O *intervalo* $[x,y]$ é definido como

$$[x,y] = \{ z \in P : x \leq z \leq y \}.$$

P é *localmente finito* se todo intervalo de P tem cardinalidade finita. Vamos sempre assumir que $(P, \leq)$ é localmente finito. Além disso supomos que existe em P um menor elemento denotado por 0 (zero) tal que $0 \leq x$ para todo x em P.

Dada uma função

$$f: P \longrightarrow \mathbb{R},$$

podemos definir uma outra função

$$f^s: P \longrightarrow \mathbb{R}$$

fazendo

$$f^s(x) = \sum_{0 \leq y \leq x} f(y).$$

A matriz *zeta* ξ^P de um poset $(P, \leq)$ é uma matriz cujas linhas e colunas são indexadas por P e onde, para $x,y \in P$, a entrada correspondente a (x,y) é .

$$\xi^P_{x,y} \begin{cases} 1 & \text{se } x \leq y \\ 0 & \text{em caso contrário .} \end{cases}$$

Em função de ξ^P a definição de $f^s(x)$ é

$$f^s(x) = \sum_{y \in P} \xi^P_{x,y} f(y).$$

Como P é localmente finito e tem um menor elemento, a soma acima tem apenas uma quantidade finita de parcelas diferentes de zero. Se considerarmos agora f e f^s sob a forma de vetores colunas (de números reais) com as entradas $f(x)$ e $f^s(x)$ para cada $x \in P$ obtemos a equação matricial:

$$f^s = \xi^P f.$$

É possível calcular f conhecendo-se f^s? Isto é, se conhecemos $f^s(x)$, $x \in P$, podemos determinar $f(x)$, $x \in P$? Na resposta positiva desta pergunta se apoia, como mostramos, técnicas muito úteis de enumeração.

É claro que se ξ^P é invertível, então $f = (\xi^P)^{-1} f^s$. No processo de calcular f estamos interessados em seus valores nos elementos de intervalos do tipo $[0,x]$. Desse modo, é suficiente provar que para $x \in P$ e $P_x = \{y \in P : y \leq x\} = [0,x]$, ξ^{P_x} é invertível.

(IV.1.a) TEOREMA: Seja $(P, \leq)$ um poset com zero, localmente fini

to e $x \in P$. Então a matriz ξ^{P_x} é inversível.

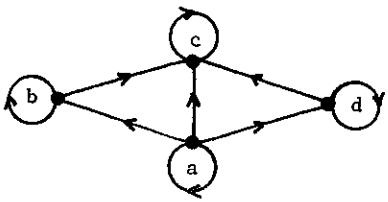
PROVA: Seja $|P_x| = n$. O passo principal desta prova é o de que podemos usar os símbolos $\{e_1, e_2, \ldots, e_n\}$ para rotular os elementos de P_x de tal forma que

$$e_i \leq e_j \Longrightarrow i \leq j.$$

Assumindo que isto é possível, a conclusão da prova é a seguinte. Considere a matriz ξ^{P_x} com as linhas e colunas indexadas por $\{1,2,\ldots,n\}$ onde linha (coluna) i corresponde a e_i. Observe que a diagonal principal de ξ^{P_x} é constituída por 1's pela reflexividade de $\leq$. Note também que pela rotulação apropriada, todo elemento abaixo da diagonal principal é zero: se 1 aparece na posição (i,j), como $e_i \leq e_j$ então $i \leq j$, ou seja (i,j) está acima da ou na diagonal principal. Assim ξ^{P_x} é uma matriz triangular superior com 1's na diagonal principal. Portanto seu determinante vale 1 e ela é invertível. A prova está concluída a menos de mostrarmos que uma rotulação dos elementos de P_x satisfazendo a implicação mostrada acima é possível.

Para isto é conveniente representarmos o poset $(P_x, \leq)$ por um digrafo. Os vértices do digrafo são os elementos de P_x e colocamos uma aresta dirigida (ou *seta*) de y para z no caso de $y \leq z$. A característica fundamental de tais digrafos, que representam posets, é que os únicos polígonos dirigidos (um polígono com todas as arestas apontando no mesmo sentido) têm apenas uma aresta. Isto é uma conseqüência simples da reflexividade e antisimetria do poset. Na figura abaixo representamos por um digrafo o poset

$(\{a,b,c,d\}, \{(a,a), (a,b), (a,c), (a,d), (b,b), (b,d), (c,c), (c,d), (d,d)\})$



Nossa tarefa é rotular os vértices do digrafo com os símbolos $\{e_1, e_2, \ldots, e_n\}$ de forma a que se existe uma seta de e_i para e_j, então $i \leq j$. Para isto começamos removendo todos os laços do digrafo. Um *laço* é uma aresta com ambas as extremidades num mesmo vértice. Feito isto obtemos um digrafo G_0 sem polígonos dirigidos, ou um digrafo *acíclico*. Uma *fonte* num digrafo é um vértice em que não há setas apontando para ele; isto é, as arestas incidentes a ele apontam para fora. Na figura acima, a torna-se uma fonte quando o laço incidente a este vértice é removido.

Todo digrafo acíclico tem pelo menos uma fonte. Se assim não fosse, poderíamos retroagir nas setas indefinidamente sem repetir vértices, o que contraria o fato do número de vértices ser finito.

Damos agora o algoritmo que nos dá uma rotulação adequada: rotule com e_1 alguma fonte de G_0 e em seguida remova esta fonte deste digrafo (bem como as arestas incidentes à e_1). Seja G_1 o subdigrafo de G_0 assim obtido. Repita n-1 vezes este procedimento, rotulando com e_i para i=2,3,...,n alguma fonte de G_{i-1}, deletando em seguida este vértice para conseguir digrafo G_i. Considere agora os rótulos $e_1, e_2, \ldots, e_n$ no grafo original G_0. É fácil provar que se existe uma seta de e_i para e_j, então $i \leq j$. Se $i>j$, então existiria uma seta de e_i para e_j no digrafo G_{j-1} e portanto e_j não seria uma fonte neste digrafo contradizendo a nossa construção. Isto conclui a prova do teorema. □

Para simplificar as notações no resto deste capítulo vamos considerar que $P=Q_x$ onde Q é um poset com zero e localmente finito. Seja também $\xi = \xi^P = \xi^{Q_x}$. Observe que, em geral, a ordem em $[0,x]$ não é total.

A *função de Möbius* de P, $\mu: P \times P \longrightarrow R$ é definida pela matriz inversa de ξ, isto é,

$$\mu(x,y)$$

é o valor da entrada (x,y) de ξ^{-1}. O teorema seguinte ensina a calcular recursivamente esta função. Se $(P, \leq)$ é um poset escre-

vemos $x < y$ se $x \leq y$ e $x \neq y$, onde $x, y \in P$.

(IV.1.b) TEOREMA: A função de Möbius μ de P é dada por

$$\mu(y,z) = \begin{cases} 1 & \text{se } y = z \\ -\sum_{y \leq r < z} \mu(y,r) & \text{se } y < z \\ 0 & \text{nos outros casos} \end{cases}$$

PROVA: Seja ξ a matriz zeta de P, isto é,

$$\xi_{x,y} = \begin{cases} 1 & \text{se } x \leq y \\ 0 & \text{em outro caso,} \end{cases}$$

e θ a matriz definida pela função μ obtida do enunciado do teorema, isto é,

$$\theta_{y,z} = \mu(y,z).$$

O que vamos mostrar é que $\Omega = \theta \circ \xi$ é a matriz identidade. Como θ é uma matriz quadrada, o fato de ξ ser uma inversa à direita implica que é de fato a inversa de θ. Veja [HK 1, pg 24].

Assim, devemos provar que $\Omega_{y,y} = 1$ para todo $y \in P$ e $\Omega_{y,z} = 0$ se $z \neq y$.

Temos

$$\Omega_{y,y} = \sum_{z} \theta_{y,z} \cdot \xi_{z,y}$$

$$= \sum_{z \leq y} \mu(y,z).$$

Pela definição de μ, o único valor distinto de zero na soma acima é para $z=y$. Assim obtemos $\Omega_{y,y} = 1$.

Consideremos agora $\Omega_{y,z}$ com $y \neq z$:

$$\Omega_{y,z} = \sum_{r} \theta_{y,r}\ \xi_{r,z}$$

$$= \sum_{r \leq z} \mu(y,r).$$

Se não é o caso de $y \leq r$, obtemos por definição $\mu(y,r) = 0$. Logo é suficiente provar que se $y < z$

$$\Omega_{y,z} = \sum_{y \leq r \leq z} \mu(y,r) = 0.$$

Provar a segunda igualdade é bem simples a partir da definição recursiva de μ. Temos

$$\Omega_{y,z} = \sum_{y \leq r \leq z} \mu(y,r)$$

$$= \sum_{y \leq r < z} \mu(y,r) + \mu(y,z).$$

Esta soma vale 0 pela definição de $\mu(y,z)$. Isto demonstra o teorema. □

Observe que, na realidade, o teorema que acabamos de estabelecer é uma outra prova de que a inversa da matriz zeta de um poset localmente finito com zero existe. Temos portanto,

(IV.1.c) COROLÁRIO: Inversão de Möbius. Seja $f: P \longrightarrow \mathbb{R}$, onde $(P, \leq)$ é um poset localmente finito com 0. Se $f^s(x) = \sum_{y \leq x} f(y)$, então

$$f(x) = \sum_{y \leq x} \mu(y,x)\ g(y)$$

onde μ é a função de Möbius para P. □

(IV.1.d) EXEMPLO: Sobrejeções. Para dar um primeiro exemplo do uso da inversão de Möbius, vamos calcular uma fórmula explícita para o número de funções sobrejetivas de N em M, onde $|N| = n$ e $|M| = m$.

Denotemos por $\left\{ {n \atop m} \right\}$ o número de partições de N (ou qualquer subconjunto com n elementos) em m partes ou classes. Qualquer sobrejeção α de N em M induz uma partição de N em m classes, cada classe definida pelos elementos que têm a mesma imagem sob α. Além disso, para cada partição de N em m classes, podemos, permutando estas classes, obter m! sobrejeções de N em M. Logo, o número de sobrejeções de N em M é

$$\left\{ {n \atop m} \right\} \cdot m!$$

e resta-nos calcular $\left\{ {n \atop m} \right\}$. (Os números $\left\{ {n \atop m} \right\}$ são conhecidos como números de Stirling de 2ª espécie.)

Podemos classificar o conjunto de todas as funções de N em M (cuja cardinalidade é m^n) pelas suas imagens. Como toda função é uma sobrejeção na sua imagem, obtemos a seguinte fórmula a ser invertida,

$$m^n = \sum_{X \subseteq M} \left\{ {n \atop |X|} \right\} |X|!$$

Considerando agora o poset dos subconjuntos de M ordenados por inclusão, podemos usar a fórmula de inversão de Möbius. Sejam, para $X \subseteq M$,

$$f^s(X) = |X|^n$$

$$f(X) = \left\{ {n \atop |X|} \right\} |X|!.$$

Usando a fórmula (dada em (IV.1.c)) obtemos

$$\left\{ \begin{matrix} n \\ m \end{matrix} \right\} m! = \sum_{X \subseteq M} \mu(X,M) \ |X|^n .$$

Existem $\binom{m}{i}$ subconjuntos de M com cardinalidade i e a cardinalidade das imagens varia de 1 a $n = |N|$. Além disso, antecipando um resultado provado na seção (IV.3), quando $X \subsetneq M$,

$$\mu(X,M) = (-1)^{|M \setminus X|} .$$

Estas observações implicam a seguinte fórmula para $\left\{ \begin{matrix} n \\ m \end{matrix} \right\}$:

$$\left\{ \begin{matrix} n \\ m \end{matrix} \right\} = \frac{1}{m!} \sum_{i=1}^{n} (-1)^{m-i} \binom{m}{i} i^n .$$

Esta equação é chamada fórmula de Stirling.

IV.2 - INVERSÃO NO RETICULADO DOS DIVISORES

Historicamente a primeira e uma das mais úteis, do ponto de vista enumerativo, expressões particulares para a função de Möbius, foi obtida pelo próprio em 1832. Trata-se do caso em que o poset $(P, \leq)$ é o reticulado dos divisores de um número natural. (Um *reticulado* é um poset em que cada par de elementos tem um supremo e um ínfimo. Como em análise, um *supremo* é um menor majorante e um *ínfimo* é um maior minorante.)

A função μ de Möbius assume, no caso em que $(P, \leq)$ é D_n, o reticulado dos divisores de n, uma forma simples e elegante.

(IV.2.a) TEOREMA: Sejam $k, m \leq n$ naturais. A função μ de Möbius em D_n é dada por

$$\mu(k,m) = \begin{cases} (-1)^r & \text{se } k|m \text{ e se } \frac{m}{k} \text{ é o produto de } r \text{ primos distintos} \\ 0 & \text{nos outros casos.} \end{cases}$$

Para provar este resultado estabelecemos primeiro os dois lemas seguintes.

(IV.2.b) LEMA: Se $a, b \leq n$ são coprimos então a função μ de Möbius em D_n satisfaz

$$\mu(1,ab) = \mu(1,a) \cdot \mu(1,b).$$

PROVA: Consideremos inicialmente o caso em que a e b são primos distintos. Pelo teorema (IV.1.b)

$$-\mu(1,ab) = \sum_{\substack{c|ab \\ c \neq ab}} \mu(1,c)$$

$$= \mu(1,1) + \mu(1,a) + \mu(1,b) +$$

$$= 1 - 1 - 1.$$

Assim,

$$\mu(1,ab) = 1$$

$$= (-1) \cdot (-1)$$

$$= \mu(1,a) \cdot \mu(1,b).$$

Vamos agora assumir, por hipótese de indução que o lema é verdade para o produto $a'b'$ onde $a|a'$, $b|b'$ e $a'b' < ab$. Pelo teorema (IV.1.b) temos

$$-\mu(1,ab) = \sum_{\substack{c|ab \\ c<ab}} \mu(1,c).$$

Como a e b são coprimos a soma acima vale

$$\sum_{\substack{a'|a \\ b'|b \\ a'b'<ab}} \mu(1,a'b')$$

Utilizando a hipótese de indução obtemos

$$-\mu(1,ab) = \sum_{\substack{a'|a \\ b'|b \\ a'b'\neq ab}} \mu(1,a') \cdot \mu(1,b')$$

Partindo convenientemente a soma,

$$-\mu(1,ab) = \sum_{\substack{a'|a \\ a'<a}} \mu(1,a')\ \mu(1,b) + \sum_{\substack{b'|b \\ b'<b}} \mu(1,a)\ \mu(1,b')$$

$$+ \sum_{\substack{a'|a \\ b'|b \\ a'<a \\ b'<b}} \mu(1,a')\,\mu(1,b')$$

As três somas acima, podem ser reescritas como

$$-\mu(1,a)\,\mu(1,b) - \mu(1,a)\,\mu(1,b) + \\ + \left(\sum_{\substack{a'|a \\ a'<a}} \mu(1,a) \right) \left(\sum_{\substack{b'|b \\ b'<b}} \mu(1,b) \right)$$

Usando uma vez mais o teorema (IV.1.b) a terceira parcela acima vale $\mu(1,a)\,\mu(1,b)$. Assim obtemos, depois de trocarmos os sinais,

$$\mu(1,ab) = \mu(1,a)\,\mu(1,b)$$

o que conclui a prova. □

(IV.2.c) LEMA: Se $p \leq n$ é um primo, então a função de Möbius em D_n satisfaz

$$\mu(1,p) = -1$$

$$\mu(1,p^n) = 0 \text{ , para } n>1.$$

PROVA: Pelo teorema (IV.1.b),

$$\mu(1,p) = - \sum_{\substack{a|p \\ a<p}} \mu(1,a)$$

$$= - \mu(1,1) = -1.$$

Para $m=2$ o mesmo teorema nos dá,

$$\mu(1,p^2) = -\mu(1,1) - \mu(1,p)$$

$$= -1 + 1 = 0.$$

Assumindo agora, por hipótese de indução que $\mu(1,p^m) = 0$ para $2 \leq m < n$, considere $\mu(1,p^n)$. Pelo teorema (IV.1.b),

$$-\mu(1,p^n) = \mu(1,1) + \mu(1,p) + \ldots + \mu(1,p^{n-1}).$$

Note que o primeiro termo à direita é 1, o segundo é -1 e a partir do terceiro todos valem zero por hipótese de indução. Assim

$$\mu(1,p^n) = 0,$$

estabelecendo o lema. □

Estamos agora em condições de oferecer uma prova simples para o teorema (IV.2.a).

PROVA DO TEOREMA (IV.2.a). Inicialmente, pela expressão geral para μ da no teorema (IV.1.b) podemos concluir facilmente que em D_n,

$$\mu(k,m) = \mu(1, \tfrac{m}{k}),$$

uma vez que os intervalos $[k,m]$ e $[1, \frac{m}{k}]$ são isomorfos como posets. Pelo lema (IV.2.b), se

$$\frac{m}{k} = p_1^{e_1} p_2^{e_2} \ldots p^{e_r}$$

é a fatorização de $\frac{m}{k}$, então

$$\mu(1, \tfrac{m}{k}) = \mu(1,p_1^{e_1})\, \mu(1,p_2^{e_2}) \ldots \mu(1,p_r^{e_r}).$$

Pelo lema (IV.2.c), temos então,

$$\mu(k,m) = \mu(1, \tfrac{m}{k}) = \begin{cases} (-1)^r & \text{se cada } e_i = 1 \\ 0 & \text{se existe } e_i > 1. \end{cases}$$

Assim, o teorema está demonstrado. □

Damos agora duas aplicações da inversão de Möbius em D_n.

(IV.2.d) EXEMPLO: *O problema das palavras circulares.* Considere um conjunto

$$A = \{a_1, a_2, \ldots, a_m\}$$

chamado *alfabeto*, com m elementos ou *letras*. Uma *palavra* de comprimento n é uma função

$$\alpha: \{1,2,\ldots,n\} \longrightarrow A.$$

Duas palavras são consideradas *equivalentes*, ou são a mesmo *palavra circular*, se existe um inteiro p, chamado *período*, tal que

$$\alpha(i) = \beta(i+p)$$

onde $i=1,2,\ldots,n$ e a soma é mod n. O que queremos saber é o número de palavras circulares em m letras de comprimento n.

O período *primitivo* de uma palavra α é o menor inteiro p tal que

$$\alpha(i) = \alpha(i+p)$$

para todo $i \in \{1,2,\ldots,n\}$. Certamente se p é um período de uma palavra α de comprimento n, então p/n.

Seja $B_n^m(p)$ o número de palavras circulares de comprimento n com no máximo m letras e com período primitivo p. Para cada uma destas palavras existem exatamente p palavras lineares distintas. Logo o número total de palavras lineares, m^n, vale

$$m^n = \sum_{p|n} p\, B_n^m(p).$$

Para inverter esta fórmula, usamos a função de Möbius μ dada no teorema (IV.2.a). Efetuando a inversão obtemos

$$p\, B_n^m(p) = \sum_{r|p} \mu(r,p)\, m^r,$$

e podemos expressar o número total das palavras circulares como

$$\sum_{p|n} B_n^m(p) = \sum_{p|n} \frac{1}{p} \sum_{r|p} \mu(r,p)\, m^r,$$

uma soma explícita que pode ser facilmente obtida. Por exemplo, para $n=6$ e $m=2$ obtemos

$$B_6^2(1) + B_6^2(2) + B_6^2(3) + B_6^2(6) =$$

$$\frac{1}{1} 2^1 + \frac{1}{2} (2^2-2^1) + \frac{1}{3} (2^3-2^1)$$

$$+ \frac{1}{6} (2^6-2^3-2^2+2^1)$$

$$= 2 + 1 + 2 + 9 = 14.$$

A seguir constatamos este valor, com uma enumeração direta. Claramente, apenas duas palavras circulares de comprimento 6 nas letras a e b têm período primitivo 1:

a a a a a a (1)

b b b b b b (1)

Apenas uma palavra circular têm período primitivo 2:

a b a b a b (2)

Duas palavras têm período primitivo 3,

a a b a a b (3)

b b a b b a (3)

Finalmente, nove palavras têm período primitivo 6:

a a a a a b	(6)	a a a b a b	(6)
b b b b b a	(6)	b b b a b a	(6)
a a a a b b	(6)	a a b a b a	(6)
b b b b a a	(6)	b b a b a a	(6)
a a a b b b	(6).		

Os números entre parênteses indicam quantas palavras lineares podem ser formadas a partir da palavra circular à esquerda. Somando estes números obtemos 64, que é o número de palavras circulares de comprimento 6 em 2 letras, o que prova que a enumeração está completa.

(IV.2.e) EXEMPLO: *Elementos primitivos e polinômios irredutíveis sobre corpos finitos*. Para desenvolver este exemplo, usamos sem provas algumas propriedades básicas de corpos finitos. Por exemplo, todo corpo finito tem cardinalidade igual à potência de algum primo. Dado um primo p e um inteiro $n \geq 1$, existe um único corpo, chamado corpo de Galois de ordem p^n e denotado por $GF(p^n)$. Este é a menos de isomorfismo o corpo das raízes do polinômio

$$x^{p^n} - x = 0.$$

Sabe-se também que o grupo multiplicativo de corpos finitos é cíclico. Para provas elegantes destas propriedades veja a seção 15.3 de [BM 1]. Um elemento *primitivo* em $GF(p^n)$ é um gerador do grupo multiplicativo deste corpo. Assim, se α é primitivo,

$$\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{p^n-1}\} = GF(p^n) \setminus \{0\}.$$

O nosso problema inicial é calcular o número de elementos primitivos em $K = GF(p^n)$, $n>1$. Se $n=1$, certamente existem $p-1$ elementos primitivos em $GF(p)$: todos menos o zero.

Seja P o corpo *primo* de K, isto é, $P = GF(p)$. Seja $\alpha \in K$. Se α é primitivo, $P(\alpha)$, isto é, o menor corpo que contém α e P, é igual a K. Reciprocamente, se α não é primitivo, existe

algum elemento $\beta \in K \setminus P(\alpha)$: qualquer $\beta \in K$ que não é potência de α satisfaz esta pertinência. Assim $P(\alpha) = K$ se e somente se α é primitivo. Ora $P(\alpha) = K$ é equivalente ao fato do polinômio mínimo de α sobre P ter grau n.

O lema básico, do qual a enumeração dos elementos primitivos em K depende, é a seguinte identidade polinomial:

$$x^{p^n} - x = \prod_{f \in A} f(x),$$

onde A é o conjunto de todos os polinômios mônicos irredutíveis sobre P cujo grau é um divisor de n. Para provar este lema, seja f um polinômio irredutível sobre P que divide $x^{p^n}-x$. Queremos mostrar que o grau de f divide n. Seja α uma raíz de f. Como $\alpha \in K$, $P(\alpha)$ é um subcorpo de K. Usando agora o teorema de multiplicidade dos graus para extensões finitas de corpos (Veja seção 14.5 de [BM 1]), temos

$$[K : P] = [K : P(\alpha)] \cdot [P(\alpha) : P].$$

O primeiro membro vale n e $\text{grau}(f) = [P(\alpha) : P]$. Assim concluímos que $\text{grau}(f)$ é um divisor de n.

Reciprocamente, seja f um polinômio mônico irredutível sobre P e suponha que $\text{grau}(f)$ divide n. Seja $d = [P(\alpha):P] = \text{grau}(f)$. O inteiro d é um divisor de n. Considere a extensão de grau $\frac{n}{d}$ de $P(\alpha)$. Pela unicidade dos corpos finitos e o teorema de multiplicidade dos graus, tal extensão existe e é isomorfa a K. Assim $P(\alpha)$ é isomorfo a um subcorpo de K. Fazendo a identificação de $P(\alpha)$ com este subcorpo, α pode ser pensado como um elemento de K. Isto é verdade para toda raíz α de f. Logo

$$f(x) \mid x^{p^n}-x,$$

pois como vimos, todas as raízes de f "estão" em K que é, em particular, o conjunto das raízes de $x^{p^n}-x$. Como este polinômio

se decompõe em K em fatores lineares distintos, deduzimos que cada elemento de A, isto é, cada polinômio mônico irredutível sobre P cujo grau divide n, aparece precisamente uma vez como fator de $x^{p^n}-x$. Isto conclui a prova da identidade polinomial.

Para um inteiro d que divide n, vamos denotar por I_p^n o número de polinômios mônicos irredutíveis sobre P com grau d. Como cada um destes polinômios tem d raízes distintas das dos outros e entre si, o número de elementos primitivos em K é precisamente $n\, I_p^n$. Isto porque, como frisamos, α é primitivo, se e somente se o polinômio mínimo de α sobre P tem grau n.

Comparando os graus da identidade polinomial acima obtemos

$$p^n = \sum_{d|n} d\, I_p^d.$$

Esta equação pode ser invertida usando a função de Möbius em D_n. Assim obtemos,

(IV.2.f) TEOREMA: O número de elementos primitivos em $GF(p^n)$ é

$$n\, I_p^d = \sum_{d|n} \mu(d,n)\, p^d,$$

onde $\mu(d,n)$ é dada explicitamente pelo teorema (IV.2.a) □

Para exemplificar numericamente este teorema, considere o corpo de 8 elementos $GF(2^3)$. Existem

$$3\, I_3 = \mu(1,3)\, 2^1 + \mu(3,3)\, 2^3$$

$$= -2^1 + 2^3$$

$$= 6$$

elementos primitivos neste corpo. Podemos dizer também que existem 2 polinômios mônicos irredutíveis de grau 3 sobre $GF(2)$. Note que obtivemos também,

(IV.2.g) COROLÁRIO: O número I_p^n de polinômios mônicos irredutíveis de grau n sobre GF(p) é

$$I_p^n = \frac{1}{n} \sum_{d|n} \mu(d,n)\ p^d. \ \square$$

Continuamos com nosso exemplo numérico $GF(2^3)$, para encontrar os dois polinômios mônicos irredutíveis de grau 3 sobre GF(2). Um polinômio de grau 3 é irredutível se e somente se não tem raízes. Na tabela abaixo listamos os 8 polinômios mônicos de grau 3 sobre GF(2) e damos uma raíz para cada redutível. Como "previsto" pelo corolário acima exatamente 2 não têm raízes.

POLINÔMIOS

$$a_o + a_1x + a_2x^2 + x_3 \in (GF(2)\ [x]$$

a_o	a_1	a_2	a_3	raiz
0	0	0	1	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	1	1
1	0	1	1	?
1	1	0	1	?
1	1	1	1	1

Assim os dois polinômios mônicos irredutíveis de grau 3 sobre Gf(2) são

$$1 + x + x^3$$

$$1 + x^2 + x^3.$$

IV.3 - O PRINCÍPIO DE INCLUSÃO E EXCLUSÃO

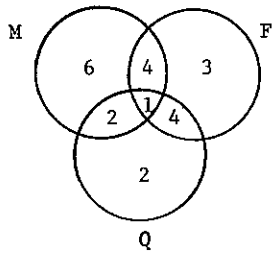
Vamos, nesta seção, deduzir a função de Möbius para o reticulado dos subconjuntos de um conjunto finito e aplicá-la para estabelecer uma das mais usadas técnicas de enumeração: o princípio de inclusão e exclusão.

Exemplificamos intuitivamente o que é este Princípio. Considere um conjunto finito C e sejam $P_1, P_2, \ldots, P_n$ certas "propriedades" que os elementos de C podem ou não possuir. A questão básica é a seguinte: dado, todo subconjunto $M \subseteq \{1,2,\ldots,n\}$, o número de elementos que satisfazem P_i para todo $i \in M$, pede-se o número de elementos que não possuem nenhuma das propriedades. Ilustrando concretamente, seja C um conjunto de 50 alunos que fizeram provas de matemática (M), física (F) e química (Q). Suponha que $R_{X\ldots Y}$ é o número de reprovados em $X,\ldots,Y$. Sabendo que

$$\begin{aligned} R_{MFQ} &= 1 \\ R_{MF} &= 5 \\ R_{MQ} &= 3 \\ R_{FQ} &= 5 \\ R_{M} &= 13 \\ R_{F} &= 12 \\ R_{Q} &= 9, \end{aligned}$$

perguntamos: quantos alunos passaram nas três disciplinas?

Para dar ums solução heurística a este problema, consideramos todos os alunos em C, subtraímos os alunos que não passaram em pelo menos uma matéria, somamos os alunos que não passaram em pelo menos duas matérias e subtraimos os alunos que não passaram em pelo menso 3 matérias. (Se houvessem mais matérias, esta alternância de somas e subtrações continuaria,) Veja figura abaixo



A resposta do nosso problema é

$$50 - (13+12+9) + (5+3+5) - 1$$

ou seja, 28 alunos foram aprovados nas três matérias. Este valor está correto, pois do diagrama de Vann acima, constatamos que exatamente 22 alunos não passararam em alguma matéria.

FORMALIZAÇÃO DO PRINCÍPIO

Damos agora uma formalização adequada ao princípio de inclusão e exclusão. Considere uma função

$$\# : C \longrightarrow \mathbb{R}^+$$

que é extendida a subconjuntos de C por

$$\#(A) = \sum_{a \in A} \#(a) \ , \ A \subseteq C.$$

Usualmente, como em todos os nossos exemplos, $\#$ é a função constante igual a 1, o que acarreta, para subconjuntos, que é a função cardinalidade

$$\#(A) = |A|.$$

As propriedades que desenvolvemos, no entanto, funcionam para $\#$ arbitrária.

Para cada $i \in \{1,2,\ldots,n\} = N$ seja A_i o subconjunto de C cujos elementos satisfazem a propriedade P_i. Para cada subcon

junto J de N seja E_J o subconjunto de C cujos elementos satisfazem exatamente as propriedades P_i para $i \in J$, isto é,

$$E_J = \left(\bigcap_{j \in J} A_j \right) \setminus \left(\bigcup_{j \notin J} A_j \right).$$

Note que por uma convenção da teoria dos conjuntos, adequada no presente caso, se $J=\phi$, $\bigcap_{j \in J} A_j = C$. Finalmente, para $k \in N \cup \{0\}$ sejam

$$E^{(k)} = \bigcup_{\substack{J \subseteq N \\ |J|=k}} E_J,$$

$$e_k = \#(E^{(k)}).$$

Com esta terminologia, podemos agora enunciar a forma geral do princípio de inclusão e exclusão, também chamado de *fórmula do crivo*.

(IV.3.a) TEOREMA: *Fórmula geral do crivo*. Sejam C um conjunto finito, $A_1, A_2, \ldots, A_n$ subconjuntos de C, $N = \{1,2,\ldots,n\}$ e $\omega, E^{(k)}$, e_k como definidos acima. Então

$$e_k = \sum_{i=k}^{} (-1)^{i-k} \binom{i}{k} \sum_{\substack{I \subseteq N \\ |I|=i}} \left(\bigcap_{j \in I} A_j \right).$$

OBSERVAÇÕES: Note que para usar a fórmula acima no problema dos 50 alunos, fazemos $\#(X) = |X|$, n=3, k=0. Quando $\#(X) = |X|$ e k=0 a solução heurística apresentada lembra o crivo de Eratóstenes para eliminar não primos e daí a denominação "fórmula do crivo". Neste caso particular, a fórmula foi descoberta por Sylvester no século passado e, por isto, é também conhecida como fórmula de Sylvester. A razão principal para a utilidade da fórmula do crivo em numerosas situações, é a relativa facilidade de computar

$$\#\left(\bigcap_{j\in I} A_j\right).$$

Isto fica claro nos exemplos que consideramos.

INVERSÃO DE MÖBIUS NO RETICULADO DE SUBCONJUNTOS

Nesta subseção mostramos que a fórmula geral do crivo é uma conseqüência direta da inversão de Möbius no reticulado dos subconjuntos de $N = \{1,2,\ldots,n\}$. Para isto explicitamos a função μ de Möbius neste poset.

(IV.3.b) TEOREMA: Seja B_n o reticulado dos subconjuntos de

$$N = \{1,2,\ldots,n\}$$

ordenados parcialmente por inclusão inversa $\supseteq$. A função μ de Möbius neste poset é dada por

$$\mu(B,A) = (-1)^{|B\setminus A|}, \quad \text{para} \quad B \supseteq A$$

$$= 0 \ , \text{ caso contrário.}$$

OBSERVAÇÃO: A fórmula para μ em B_n com a inclusão direta $\subseteq$ é

$$\mu(B,A) = (-1)^{|A\setminus B|}, \quad \text{para} \quad B \subseteq A.$$

$$= 0 \ , \text{ caso contrário.}$$

A prova é essencialmente a mesma que apresentamos a seguir. Escolhemos $\supseteq$ porque é a que se aplica diretamente para provar a fórmula geral do crivo.

PORVA DE (IV.3.b): Se B não é "menor ou igual" a A, isto é, se B não é um superconjunto de A, então pelo teorema (IV.1.b)

$$\mu(B,A) = 0.$$

Se B é um superconjunto de A, usando este mesmo teorema podemos escrever

$$\mu(B,A) = \begin{cases} 1, \text{ se } B = A \\ -\sum_{B \supseteq X \supset A} \mu(b,X), \text{ se } B \supset A. \end{cases}$$

Vamos usar indução sobre $|B \setminus A|$ para estabelecer o teorema. Se $|B \setminus A| = \phi$ então $B=A$ e claramente obtemos a base da indução. Assumamos, agora, como hipótese de indução que a expressão para $\mu(B \setminus A)$ dada no enunciado do teorema se verifica sempre que $|B \setminus A| \leq m$. Suponhamos que $|B \setminus A| = m+1$. Pela expressão obtida do teorema (IV.1.b)

$$-\mu(B,A) = \sum_{B \supseteq X \supset A} \mu(B,X).$$

Podemos usar a hipótese de indução para todas as parcelas da soma acima, obtendo

$$-\mu(B,A) = \sum_{B \supseteq X \supset A} (-1)^{|B \setminus X|}.$$

Observando que existem $\binom{m+1}{k}$ conjuntos X tais que $|B \setminus X| = k$ podemos escrever

$$-\mu(B,A) = \sum_{k=0}^{m} \binom{m+1}{k} (-1)^k$$

$$= (-1)^m + \sum_{k=0}^{m+1} \binom{m+1}{k} (-1)^{m+1}.$$

Note que a soma acima vale $(1 -1)^{m+1}$, ou seja 0. Assim,

$$-\mu(B,A) = (-1)^m$$

ou seja

$$\mu(B,A) = (-1)^{m+1} = (-1)^{|B \setminus A|}.$$

Isto conclui o passo de indução e a prova do teorema. □

Podemos agora estabelecer a fórmula geral do crivo.

PROVA DE (IV.3.a). Além dos conjuntos

$$E_J = \left(\bigcap_{j\in J} A_j\right) \setminus \left(\bigcup_{j\notin J} A_j\right),$$

$J = \{1,2,\ldots,n\} = N$, consideremos também os conjuntos F_J's formados pelos elementos que pertencem pelo menos aos A_i's com $i\in J$,

$$F_J = \bigcap_{j\in J} A_j.$$

Da relação entre os E_J's e os F_j's obtemos facilmente a fórmula a ser invertida:

$$\#(F_J) = \sum_{N\supseteq I\supseteq J} \#(E_I),$$

uma vez que os E_I's são dois a dois disjuntos. Para tornar clara a inversão definamos as funções

$$f, f^s : 2^N \longrightarrow \mathbb{R}^+$$

dadas por $f(J) = \#(E_J)$ e $f^s(J) = \#(F_J)$. Reescrevendo a equação acima temos

$$f^s(J) = \sum_{N\supseteq I\supseteq J} f(I).$$

Aplicando agora a inversão de Möbius, onde μ é dada pelo teorema (IV.3.b),

$$f(J) = \sum_{N\supseteq I\supseteq J} (-1)^{|I\setminus J|} f^s(I).$$

Somando para todos os subconjuntos J com $|J| = k$,

$$\sum_{\substack{N \supseteq J \\ |J|=k}} f(J) = \sum_{\substack{N \supseteq J \\ |J|=k}} \sum_{N \supseteq I \supseteq J} (-1)^{|I \setminus J|} f^s(I)$$

$$= \sum_{|I|=k}^{n} \sum_{N \supseteq I \supseteq J} (-1)^{|I \setminus J|} f^s(I).$$

$$= \sum_{i=k}^{n} (-1)^{i-k} \binom{i}{k} \sum_{I \subseteq N} f^s(I).$$

Note que, por nossas definições,

$$\sum_{\substack{J \subseteq N \\ |J|=k}} f(J) = \sum_{\substack{J \subseteq N \\ |J|=k}} \#(E_J) = \#(E^{(k)}) = e_k$$

e

$$f^s(I) = \#(F_I) = \left(\bigcap_{j \in I} A_j \right).$$

Assim, reescrevendo o que deduzimos acima obtemos

$$e_k = \sum_{i=k} (-1)^{i-k} \binom{i}{k} \sum_{\substack{I \subseteq N \\ |I|=i}} \# \left(\bigcap_{j \in I} A_j \right)$$

que é precisamente a fórmula geral do crivo. □

Damos a seguir dois exemplos de aplicação da fórmula acima.

IV.3.c) EXEMPLO: *função totiente de Euler*. Dado um número natural m, seja $\phi(m)$ a quantidade de números menores que m e coprimos com ele. Quanto vale $\phi(m)$? A função ϕ é chamada de função to-

tiente de Euler e aparece freqüentemente em situações diversas.

Para calcular $\phi(m)$ suponha que $p_1, p_2, \ldots, p_n$ são os divisores primos distintos de m. Seja, para $i \in \{1,2,\ldots n\} = N$,

$$A_i = \{r \leq m : p_i \mid r\}$$

e tomemos

$$\# (X) = |X|, \text{ para } X \subseteq \{1,2,\ldots,m\}.$$

Note que

$$\# (A_i) = |A_i| = \frac{m}{p_i}$$

e que, em geral,

$$\# \left(\bigcap_{i \in I \subseteq N} A_i \right) = \left| \bigcap_{i \in I \subseteq N} A_i \right| = \frac{m}{\prod\limits_{i \in I} p_i} .$$

Pela fórmula do crivo obtemos para e_0, que é certamente o que procuramos,

$$\phi(m) = e_0 = \sum_{i=0}^{n} (-1)^i \sum_{I \subseteq N} \left(\frac{m}{\prod\limits_{i \in I} p_i} \right).$$

Assim,

$$\phi(m) = m - \sum_i \frac{m}{p_i} + \sum_{i<j} \frac{m}{p_i p_j} - \sum_{i<j<k} \frac{m}{p_i p_j p_k} \ldots$$

Esta expressão pode ser reescrita na forma mais elegante

$$\phi(m) = m(1 - \frac{1}{p_1}) \ (1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_n}).$$

(IV.3.d) EXEMPLO: problema do jantar. Este problema pergunta pelo número J(n) de configurações de num jantar sentarem-se a uma mesa circular n maridos e suas esposas de forma a que homem e mulher se alternem e que nenhum marido fique adjacente a sua esposa.

Parece ser uma regra de etiqueta se evitar tais adjacências. Pelo menos o é para os ingleses... De forma mais "sêria" esta questão aparece também em conexão com a enumeração de projeções de nós alternantes. Leitores interessados devem consultar a parte final de [BE 1]. O problema do jantar (problème des ménages) foi resolvido originalmente por Touchard [TO 1] e Kaplanski [KA 1] independentemente. Ambas as soluções aparecem em 1943. Para uma breve história deste problema veja [RI 1], pg 195. O método de solução ilustra uma aplicação não trivial do princípio de inclusão e exclusão.

SOLUÇÃO DO PROBLEMA DO JANTAR

Suponhamos que as n mulheres sentem-se primeiro de tal forma que de ambos os lados de cada uma delas fique um lugar desocupado. Supomos que as cadeiras são rotuladas de 1 a 2n e assim existem n! maneiras diferentes de elas sentarem nos lugares pares e outras tantas de sentarem nos lugares ímpares. Vamos fixar uma destas maneiras, digamos, a mulher i senta no lugar i,

$$i \in N = \{1,2,\ldots,n\}.$$

Em seguida calculamos o número H(n) de extender a configuração, sentando todos os n homens de forma a obter uma disposição permitida. O número procurado, J(n), certamente é expresso por

$$J(n) = 2\, n!\, H(n)$$

e toda dificuldade está em calcular H(n).

Fixa, como consideramos, a ordem das mulheres, cada maneira arbitrária de sentar os n homens pode ser univocamente re-

presentada por uma permutação α de N. Isto é, construímos uma bijeção entre a ordem em que os homens aparecem e o conjunto das n! permutações de N. Para definir tal bijeção, consideramos os homens também rotulados de 1 a n com homem e mulher i sendo casados, $i \in N$. Dada uma disposição alternante em que as mulheres aparecem $1,2,\ldots,n$ em sentido antihorário, definamos como $\alpha(i)$ o rótulo do homem sentado à direita da mulher com rótulo i. Isto implica, em particular que mulher com rótulo i+1 (mod. n) senta à direita do homem com rótulo $\alpha(i)$. Evidentemente dada α podemos recuperar a disposição alternante (com as mulheres fixas na ordem $1,2,\ldots,n$) que origina α.

A condição de marido e mulher não sentarem adjacente numa disposição alternante é equivalente no contexto de permutações a termos, para $i \in N$,

$$\alpha(i) \neq i$$
$$\alpha(i-1) \neq i \qquad \text{mod. n.}$$

A primeira desigualdade proibe o fato do homem rotulado i sentar à direita de sua esposa e a segunda proibe o fato desse homem sentar à esquerda de sua esposa.

Desse modo, o número H(n) procurado é o número de permutações α's de N em S_n tais que $\alpha(i) \neq i$, $i+1 \bmod n$, $i \in N$. Sejam, para $i \in N$,

$$A_{2i-1} = \{\alpha \in S_n : \alpha(i) = i\}$$
$$A_{2i} = \{\alpha \in S_n : \alpha(i) = i+1\}.$$

Uma vez mais consideramos, para $X \subseteq S_n$,

$$\# (X) = |X|.$$

O que procuramos é, com a notação da fórmula do crivo, simplesmente e_0. Desta fórmula obtemos

$$H_n = e_o = \sum_{i=0} (-1)^i \sum_{\substack{I \subseteq 2N \\ |I|=i}} \left| \bigcap_{j \in I} A_j \right|,$$

onde $2N = \{1,2,\ldots,n,n+1,\ldots,2n\}$. Se $I \subseteq 2N$ contém dois elementos consecutivos da seqüência $(1,2,\ldots,2n,1)$ então

$$\left| \bigcap_{j \in I} A_j \right| = 0$$

porque se $2r-1$ e $2r$ estão em I, para α estar na interseção acima deveria satisfazer simultaneamente

$$\alpha(r) = r$$

$$\alpha(r) = r+1,$$

por definição de A_{2r-1} e de A_{2r}. Como isto é impossível, temos que a cardinalidade da interseção é zero como mencionado.

Uma conseqüência deste fato é que se $[I] > n$, então

$$\left| \bigcap_{j \in I} A_j \right| = 0$$

uma vez que elementos consecutivos são forçados quando $[I]>n$. Assim, o limite superior do somatório que define e_o pode ser reduzido de $2n$ para n.

Se I não contém elementos consecutivos de

$$(1,2,\ldots,2n,1),$$

então temos certamente

$$\left| \bigcap_{j \in I} A_j \right| = (n - |I|)!.$$

Na seção (I.a) sobre números de Fibonacci mostramos que o número de subconjuntos de $\{1,2,\ldots,n\}$ com k elementos e sem elemen-

tos consecutivos mod. n é

$$f(n,k) = \frac{n}{n-k}\binom{n-k}{k}.$$

Para aplicar esta fórmula no caso presente, substituímos n por 2n e k por $i = |I|$. Obtemos assim a seguinte expressão para H(n)

$$H(n) = e_0 = \sum_{i=0}^{n} (-1)^i \frac{2n}{2n-i}\binom{2n-i}{i}(n-i)!.$$

Para calcular J(n) é suficiente multiplicar a expressão acima por 2n! De maneira inteiramente análoga podemos mostrar que existem 2n! e_k maneiras distintas de sentar os casais de forma a que exatamente k deles fiquem adjacentes, onde e_k vale

$$e_k = \sum_{i=k} (-1)^{i-k}\binom{i}{k}\frac{2n}{2n-i}\binom{2n-i}{i}(n-i)!.$$

O problema do jantar é um exemplo particular do tópico: permutações com posições proibídas, veja [LI 1]. Outro exemplo, é o problema dos desarranjamentos cujo número é dado no teorema (III.4.c). O número de desarranjamentos pode também ser facilmente obtido por inclusão e exclusão.

EXERCÍCIOS

1. Em quantos zeros termina a expansão decimal de 1000!? Use o princípio de inclusão e exclusão para justificar a sua resposta.

2. Determine o número de permutações de $\{1,2,\ldots,7\}$ em que nenhum ímpar esteja em sua posição natural.

3. Dentre os números de 1 a 1000 quantos não são divisíveis por 11 mas são divisíveis por 3,5, e 7?

4. Dois professores em diferentes matérias devem examinar oralmente 6 estudantes na mesma hora. Cada estudante deve ser examinado individualmente por 10 minutos. De quantas maneiras distintas pode ser feito um horário compatível?

5. Os n inteiros $1,2,\ldots,n$ são dispostos ao redor de um círculo. Use o princípio de inclusão e exclusão para calcular o número g_n de maneiras distintas de colocá-los de forma a que i e i+1 mod n não apareçam juntos, $i=1,2,\ldots,n$. Em seguida prove que

$$g_n + g_{n+1} = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor = d_n.$$

6. Prove que o valor I_p^n dado no corolário (IV.2.g) nunca é nulo. Isto resolve com uma enumeração explícita um exercício do tipo existencial muito comum em cursos de álgebra: o de provar que existem polinômios irredutíveis de qualquer grau sobre GF(p).

7. Quantos elementos primitivos têm os seguintes corpos

(a) $GF(7^2)$

(b) $GF(7^3)$

(c) $GF(11^4)$

(d) $GF(11^{30})$?

8. Quantos polinômios mônicos irredutíveis de grau n sobre GF(p) existem para

(a) $n = 2$ $\quad p = 5$

(b) $n = 4$ $\quad p = 7$

(c) $n = 8$ $\quad p = 11$

(d) $n = 30$ $\quad p = 17$?

9. Em quantas das n! permutações em S_n exatamente $k \leq n$ inteiros estão em sua posição original?

10. Um número par, $2n$, de pessoas dam-se as mãos para formar um círculo. De quantas maneiras o círculo pode ser desfeito e refeito novamente de forma a que a oposta a cada pessoa seja diferente do círculo original?

11. Considere a matriz $n \times n$ M onde a entrada (i,j) é dada por

$$m_{ij} = mdc(i,j).$$

Prove que $\det(M) = \prod_{i=1}^{m} \phi(i)$, onde ϕ é a função totiente de Euler.

12. Sejam $u_0, u_1, \ldots, u_n$; $v_0, v_1, \ldots, v_n$ números reais. Prove que

$$v_n = \sum_{k=0}^{n} \binom{n}{k} u_k \quad \text{se e somente se}$$

$$u_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} v_k$$

13. O *permanente* de uma matriz $A = (a_{ij})$, $m \times n$ com $m \leq n$ é definido por

$$P(A) = \sum_{f \in inj(L,C)} \prod_{i=1}^{m} a_{i f(i)},$$

onde $L = \{1,2,\ldots,m\}$, $C = \{1,2,\ldots,n\}$. Se $I \subseteq C$ denotamos por $P(A|I)$ o permanente da matriz obtida removendo de A as colunas complementares de I. Se $f \in inj(L,C)$ seja

$$\#(f) = \prod_{i=1}^{m} a_{i f(i)}.$$

Mostre que, com a notação da fórmula do crivo,

$$P(A) = e_{n-m} = \sum_{k=1}^{m} (-1)^{m-i} \binom{n-i}{n-m} \sum_{\substack{I \subseteq C \\ |I|=i}} P(A|I).$$

Se A é uma matriz quadrada,

$$P(A) = e_o = \sum_{i=1} (-1)^{n-i} \sum_{\substack{I \subseteq C \\ |I|=i}} P(A|I).$$

14. Use o exercício anterior para provar que

$$n! = \sum_{i=1}^{n} (-1)^{n-i} \, i^n$$

$$\left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor = \sum_{i=1}^{n} (-1)^{n-i} \binom{n}{i} (i-1)^k.$$

15. Sejam $N = \{1,2,\ldots,n\}$, $A = \{A_1, A_2, \ldots A_k\}$, $B = \{B_1, B_2, \ldots, B_r\}$ partições de N. Dizemos que B é uma *subpartição* de A se cada A_i é a união de alguns B_j's. A relação de subpartição induz uma ordem parcial no conjunto de partições de N. Prove que a função de Möbius neste poset é dada por, onde n_i é o número de B_j's que formam A_i,

$$\mu(B,A) = 0, \text{ se } B \text{ não é subpartição de } A$$

$$= (-1)^{k+n_1+n_2+\ldots+n_k} (n_1-1)! \, (n_2-1)! \ldots (n_k-1),$$

se é o caso.

CAPÍTULO V

ENUMERANDO SIMETRIAS : A TEORIA DE POLYA

V.1 - LEMA ALGÉBRICO BÁSICO

Iniciamos este capítulo formulando duas questões típicas das que podem ser resolvidas com a teoria de enumeração de Polya:

(V.1.a) QUESTÃO: Encontre o número de maneiras distintas de se pintar as faces de um cubo com no máximo n cores, onde duas colorações são consideradas iguais se uma pode ser transformada na outra por rotações do cubo.

RESPOSTA: $\frac{1}{24}\,(n^6 + 3n^4 + 12n^3 + 8n^2)$.

(V.1.b) QUESTÃO: Calcule o número de isômeros espaciais de um determinado composto químico cuja molécula é formada por um átomo de tipo A, 5 átomos de tipo B, 2 átomos de tipo C. Sabe-se que estes 8 átomos formam os vértices de um cubo, e assim, equivalência é novamente dada por congruência módulo rotação do cubo.

RESPOSTA: $\frac{1}{24}\left[a^1b^5c^2\right]\,\{(a+b+c)^8 + 9(a^2+b^2+c^2)^4 + 6(a^4+b^4+c^4)^2$

$$+ 8(a+b+c)^2\,(a^3+b^3+c^3)^2\} = 7.$$

Nesta segunda questão, ao invés de apenas o grupo de rotações do cubo, poderíamos considerar o grupo das simetrias deste, isto é, poderíamos incluir as reflexões. Isto nos permitiria calcular o número de isômeros auto-enantiomorfos, ou seja, o número de isômeros que são congruentes com suas imagens especulares.

O teorema fundamental que permite tratar problemas do tipo acima for obtido por Polya em 1937. Este teorema é extremamente poderoso. Ele combina de maneira simples e elegante as idéias de equivalências de funções módulo um grupo, funções geradoras (inventários) e índice de ciclos de um grupo de permutações. O teorema ilustra de maneira contundente o uso de métodos algébricos para captar simetrias geométricas, topológicas, combinatoriais, etc.

Vamos agora desenvolver a terminologia necessária para enunciar e provar o teorema fundamental de Polya. A parte algébrica deste depende tão somente de uma ligeira extensão do lema (V.1.c) abaixo, provado por Burnside [BU 1] em 1911.

Seja X um conjunto finito e Q um grupo finito de permutações de X. Dois elementos a e b de X são chamados Q-associados, se existe $q \in Q$ tal que $q(a) = b$. Claramente a relação "ser Q-associado a" é uma relação de equivalência. As classes desta relação de equivalência são chamadas de Q-órbitas.

(V.1.c) LEMA DE BURNSIDE: O número de Q-órbitas induzidas sobre um conjunto finito X por um grupo de permutações de X é dado por

$$|\mathrm{orb}(A,Q)| = \frac{1}{|Q|} \sum_{q \in Q} \mu(q),$$

onde $\mu(q)$ é o número de elementos de X que são fixados por q.

O lema de Burnside é um corolário do próximo resultado, o qual se ajusta melhor aos nossos propósitos. Para enunciá-lo precisamos definir alguns conceitos. Sejam $(G,*)$ um grupo e X um conjunto ambos finitos. Suponhamos que exista um homomorfismo

$$\alpha: G \longrightarrow S_X,$$

onde S_X é o grupo das permutações de X. Se $g \in G$ seja $\alpha(g)$ denotada por α_g. Desde que α é um homomorfismo temos para $g,h \in G$

$$\alpha_{g * h} = \alpha_g \circ \alpha_h.$$

Note que não exigimos a injetividade nem a sobrejetividade de α, e assim, elementos distintos de G podem ter como imagens a mesma permutação de S_X; também permutações de S_X podem não estar na imagem de α.

Dizemos que $a,b \in X$ são *G-associados* e denotamos isto por $a \; G \; b$ se existe $g \in G$ tal que $\alpha_g(a) = b$. Esta relação é, como mostramos, uma relação de equivalência:

(i) a G a pois $\alpha_e(a) = e$, onde e é a identidade em G.

(ii) a G b implica que existe $g \in G$ tal que $\alpha_g(a) = b$. A condição de homomorfismo nos dá $\alpha_g^{-1} = \alpha_{g-1}$ e como $a = \alpha_g^{-1}(b)$, temos $\alpha_{g-1}(b) = a$, ou seja, b G a.

(iii) a G b e b G c significa que existem $g,h \in G$ tais que $\alpha_g(a) = b$, $\alpha_g(b) = c$. Temos $\alpha_{g*h}(a) = \alpha_g\,\alpha_h(a) = \alpha_h(b) = c$. Logo a G c.

Desse modo, a relação binária "ser G-associado a" é um relação de equivalência. Aqui também, as classes desta relação de equivalência são chamadas G-órbitas. Estabelecemos agora a generalização do lema de Burnside.

(V.1.d) LEMA ALGÉBRICO BÁSICO: Sejam (G,*) um grupo e X um conjunto ambos finitos. Suponha que

$$\alpha: G \longrightarrow S_X$$

é um homomorfismo de G no grupo S_X de permutações de X. O número de G-órbitas em que X é particionado é

$$|orb(X,G)| = \frac{1}{|G|} \sum_{g \in G} \mu(\alpha_g),$$

onde $\mu(\alpha_g)$ é o número de elementos de X fixados por α_g.

PROVA: Inicialmente observe que o lema de Burnside é um caso particular do presente. Para isso faça G igual ao próprio grupo de permutações Q e o homomorfismo α igual à identidade.

Para $x \in X$, denotemos por $\phi(x)$ o número de elementos $g \in G$ tal que $\alpha_g(x) = x$. Temos então que

$$\sum_{g \in G} \mu(\alpha_g) = \sum_{x \in X} \phi(x),$$

uma vez que ambas as somas contam o número total de elementos fixados pelas permutações induzidas pelos elementos de G. Sejam x e y elementos de X na mesma G-órbita. Mostramos agora que existem $\phi(x)$ elementos $g \in G$ tais que $\alpha_g(x) = y$. Para isto, seja

$$\{g_1, g_2, \ldots, g_{\phi(x)}\}$$

o subconjunto de G tal que $\alpha_{g_i}(x) = x$, $i=1,2,\ldots,\phi(x)$. Seja também $g \in G$ tal que $\alpha_g(x) = y$. Tal g existe porque x e y estão na mesma G-órbita. As permutações que são imagens por α dos membros do conjunto

$$\Omega = \{g * g_1,\ g * g_2, \ldots, g * g_{\phi(x)}\}$$

têm y como imagem de x. Certamente, se $i \neq j$, $g * g_i \neq g * g_j$ e assim Ω tem $\phi(x)$ elementos. Seja $h \in G$ e $\alpha_h(x) = y$. Note que

$$\alpha_{g^{-1} * h}(x) = \alpha_{g^{-1}}\,\alpha_h(x) = \alpha_{g^{-1}}(y) = x.$$

Dessa igualdade podemos concluir que existe i, $1 \leq i \leq \phi(x)$ tal que $g^{-1} * h = g_i$, isto é, $h = g * g_i \in \Omega$. Assim Ω é precisamente o conjunto dos elementos de G cujas imagens por α são permutações que têm y como imagem de X. Por simetria, em x e y existem $\phi(y)$ elementos em G cujas imagens por α são permutações que têm x como imagem de y. Note que estes elementos são precisamente os inversos dos elementos de Ω. Logo $\phi(x) = \phi(y)$.

Seja agora $Y = \{x_1, x_2, \ldots, x_t\} \subseteq X$ uma G-órbita qualquer com t elementos. Note que G pode ser particiondo em t classes

$$\{G_1, G_2, \ldots, G_t\}$$

onde

$$G_i = \{g \in G : \alpha_g(x_1) = x_i\}.$$

Pelo que provamos acima

$$|G_i| = \phi(x_1) = \phi(x_i) = \frac{1}{t}\,|G|.$$

Assim, se x está numa G-órbita com t elementos, podemos concluir que

$$\phi(x) = \frac{1}{t}\,|G|.$$

Logo, para qualquer G-órbita Y,

$$\sum_{y \in Y} \phi(y) = |G|.$$

Somando esta equação para todas as G-órbitas,

$$\sum_{x \in X} \phi(x) = |\mathrm{orb}(X,G)| \cdot |G|.$$

Dividindo por $|G|$ e recordando que $\displaystyle\sum_{x \in X} \phi(x) = \sum_{g \in G} \mu(g)$ conclui-mos

$$|\mathrm{orb}(X,G)| = \frac{1}{|G|} \sum_{g \in G} \mu(\alpha_g),$$

estabelecendo o lema. □

V.2 - CLASSES DE EQUIVALÊNCIA DE FUNÇÕES

Tendo estabelecido o lema álgebrico básico vamos agora prosseguir definindo conceitos adicionais necessários para o entendimento da Teoria de Polya.

Sejam D um conjunto finito e C um conjunto no máximo enumerável. Seja também G um grupo de permutações de D. Definimos uma relação binária em C^D (o conjunto de todas as funções de D em C) da seguinte maneira: se $f,g \in C^D$, dizemos que f é G-associada a g se existe $\alpha \in G$ tal que $f(d) = g(\alpha(d))$ para todo $d \in D$. É fácil verificar que ser "G-associada a" é uma relação de equivalência:

(i) como a permutação identidade está em G, reflexividade é satisfeita;

(ii) se $f(d) = g(\alpha(d))$ para $d \in D$, então $g(d)=f(\alpha^{-1}(d))$ para $d \in D$, verificando a simetria.

(iii) se para $d \in D$ $f(d) = g(\alpha(d))$ e $g(d) = h(\beta(d))$ onde $\alpha,\beta \in G$, então $f(d) = h(\beta.\alpha(d))$, comprovando a transitividade.

Dessa forma a relação binária acima é de fato uma relação de equivalência e portanto particiona C^D em classes de equivalência. Cada uma dessas classes é chamada um *G-padrão*. Duas funções no mesmo G-padrão são, como é natural, chamadas G-equivalentes. Intuitivamente os G-padrões são as maneiras distintas de se "pintar" os elementos de D com as "cores" de C levando em conta a equivalência induzida pelo grupo G de permutações de D. Como exemplo concreto para fixar as idéias veja a questão (V.2.a) posta no começo do capítulo. Neste problema, D é o conjunto das 6 faces de um cubo, C é um conjunto de n cores e G é o grupo de rotações do cubo, efetivamente representado por permutações de faces. O valor do polinômio resposta dado é o número de G-padrões em função do número de cores n. A contagem dos G-padrões sai como um corolário de uma técnica mais refinada, onde são in-

troduzidos "pesos" e a enumeração é referente a G-padrões de mesmo peso.

PESOS E INVENTÁRIOS DE FUNÇÕES

É possível (e conveniente) se generalizar consideravelmente a enumeração dos G-padrões com a introdução de "pesos" para os elementos de C. Suponhamos que a cada $c \in C$ seja atribuído um *peso* $\pi(c)$ que em geral é um elemento de algum anel comutativo A que contém os racionais.

O inventário de C é definido como

$$Inv_{\pi}(C) = \sum_{c \in C} \pi(c).$$

O inventário de um conjunto supostamente nos dá uma idéia do que o conjunto contém. Isto é, no entanto, bastante flexível dependendo do que se quer. Seja como ilustração um conjunto C contendo 3 relógios (chamados r_1, r_2, r_3), 2 canetas (c_1 e c_2) e 1 minicalculadora (m_1). Podemos conservar estes símbolos como pesos dos respectivos objetos. Neste caso o inventário de C é

$$r_1 + r_2 + r_3 + c_1 + c_2 + m_1.$$

Podemos estar interessados em classificar os objetos por tipos dando pesos r,c,m a relógios, canetas e minicalculadora respectivamente obtendo como inventário o valor 3r+2c+m. Se estimarmos cada relógio em CR$ 5000,00, cada caneta em CR$ 1000,00 e a minicalculadora em CR$ 7000,00, o inventário de C torna-se uma quantia: CR$ 24000,00. Finalmente, se estamos interessados em contar os objetos, atribuímos o peso 1 a cada um deles e o inventário de C se torna $|C| = 6$.

Para uma função $f \in C^D$ definimos seu *peso* como

$$\pi(f) = \prod_{d \in D} \pi(f(d)).$$

Se $\Omega \subseteq C^D$, o *inventário* de Ω é a soma

$$Inv_\pi(\Omega) = \sum_{f \in \Omega} \pi(f).$$

É possível se expressar o inventário de C^D em função do inventário de C e da cardinalidade de D. Embora não utilizemos este fato nós o provamos em seguida. O argumento utilizado na prova é um exercício para o leitor, preparando-o para argumentos mais complicados de tipo semelhante.

(V.2.a) PROPOSIÇÃO:

$$Inv_\pi(C^D) = \left[Inv_\pi(C)\right]^{|D|}.$$

PROVA: Considere a expansão da expressão à direita como um produto de $|D|$ fatores iguais a $Inv_\pi(C)$. Fixe uma correspondência bijetiva entre cada um desses fatores e os elementos de D. A cada seleção de uma parcela de $Inv_\pi(C)$ para cada um dos $|D|$ fatores, corresponde de maneira natural uma função f de D em C. O produto dessas parcelas selecionadas é por definição o peso de f, que é uma parcela do produto expandido. Assim existe uma correspondência bijetiva entre as parcelas da expansão do produto e as funções em C^D. Como cada parcela é o peso da função correspondente, temos que

$$\left[Inv_\pi(C)\right]^{|D|} = \sum_{f \in C^D} \pi(f) = Inv_\pi(C^D)$$

o que prova a proposição. □

A proposição que acabamos de estabelecer não leva em conta a equivalência induzida por G. Na realidade, o que queremos é levar em conta uma vez apenas o peso das funções G-equivalentes. Isto faz sentido porque temos

(V.2.b) PROPOSIÇÃO: Se f e g estão no mesmo G-padrão, então

$$\pi(f) = \pi(g)$$

PROVA: Como f e g estão no mesmo G-padrão existe $\alpha \in G$ tal que

$$f(d) = g(\alpha(d))$$

para todo $d \in D$. Temos

$$\pi(f) = \prod_{d \in D} \pi(f(d))$$

$$= \prod_{d \in D} \pi(g(\alpha(d)))$$

$$= \prod_{d \in D} \pi(g(d)) = \pi(g). \quad \square$$

O peso comum a todas as funções num G-padrão é definido como o *peso do G-padrão*. Claramente a recíproca da proposição acima não é verdadeira. Duas funções podem ter o mesmo peso sem estar no mesmo G-padrão.

V.3 - INVENTÁRIOS DE G-PADRÕES E ÍNDICES DE CICLOS

Depois de definido o conceito de peso π de um G-padrão, a definição da importante noção de inventário de G-padrões é bastante simples. Seja $\Omega \subseteq C^D$. O *inventário de G-padrões* de Ω é definido como a soma dos pesos dos G-padrões em Ω, e é denotado por $Inv_\pi(\Omega \text{ mod. } G)$.

O teorema fundamental de Polya, provado na próxima seção nos dá o inventário de G-padrões de C^D em termos do inventário de C e de um polinômio obtido do grupo G de permutações de D. Este polinômio é chamado índice de ciclos de G e é, em geral, definido abaixo. Para o caso dos grupos simétrico de permutações já tivemos oportunidade de introduzir os índices de ciclos e até mesmo de obter uma recorrência para os mesmos, corolário (III.4.k). De maneira mais explícita o que o teorema de Polya nos dá é, para cada valor π_0 assumido pela função peso π, quantos G-padrões com peso π_0 existem.

Para exemplificar concretamente, considere a questão (V.1.b) formulada no começo do capítulo. O domínio D é o conjunto de vértices do cubo e C é o conjunto {A,B,C} de tipos de átomos. Os pesos são $\pi(A) = a$, $\pi(B) = b$, $\pi(C) = c$. O grupo G é o grupo de rotações do cubo representado por permutações dos vértices do mesmo. O inventário dos G-padrões de C^D é (veja a resposta da questão (V.1.b) sem se preocupar com a razão da mesma, por enquanto),

$$\frac{1}{24}\left[(a+b+c)^8 + 9(a^2+b^2+c^2)^4 + 6(a^4+b^4+c^4)^2 + 8(a+b+c)(a^3+b^3+c^3)^2\right]$$

Para obter a resposta do número de isômeros procuramos pelo número de G-padrões com peso $a^1b^5c^2$ e isto é dado pelo coeficiente de $a^1b^5c^2$ na expansão do polinômio acima. O valor deste coeficiente é 7. Se existissem 2 átomos de tipo A, 4 de tipo B e 2 de tipo C, obteríamos para resposta 22. Isto nos é dado pelo coeficiente de $a^2b^4c^2$ na expansão do mesmo polinômio.

Definimos agora o conceito geral de índice de ciclos

de um grupo de permutações. Seja G um grupo finito de permutações de um conjunto D com m elementos. A cada permutação $g \in G$ associamos o monômio

$$x_1^{b_1(g)} \quad x_2^{b_2(g)} \quad \cdots \quad x_m^{b_m(g)},$$

onde $b_i(g)$ é o número de ciclos de comprimento i que aparece na decomposição de g em ciclos disjuntos. O *índice de ciclos* de G é definido como

$$\gamma_G(x_1,\ldots,x_m) = \frac{1}{|G|} \sum_{g \in G} x_1^{b_1(g)} \quad x_2^{b_2(g)} \quad \ldots x_m^{b_m(g)}.$$

(V.3.a) EXEMPLO: *Índice de ciclos do grupo de rotações do cubo como permutações de faces.* As 24 rotações do cubo podem ser classificadas da seguinte maneira:

(a) a identidade;

(b) 8 rotações de 120° (4 horárias e 4 antihorárias) ao redor das 4 diagonais ligando vértices opostos;

(c) 6 rotações de 180° ao redor das linhas ligando o meio dos 6 pares de arestas opostas;

(d) 6 rotações de 90° (3 horárias e 3 antihorárias) ao redor das linhas ligando os centros dos 3 pares de faces opostas;

(e) 3 rotações de 180° ao redor das linhas ligando os centros dos 3 pares de faces opostas.

A identidade contribui com x_1^6 para o índice de ciclos; cada rotação do tipo (b) contribui com x_3^2; cada uma do tipo (c) contribui com x_2^3; cada uma do tipo (d) contribui com $x_1^2 x_4^1$; finalmente, cada uma do tipo (e) contribui com $x_1^2 x_2^2$. Assim, o índice de ciclos do grupo de rotações do cubo, como per-

mutações de faces é

$$\frac{1}{24}\,(x_1^6 + 8x_3^2 + 6x_2^3 + 6x_1^2x_4^1 + 3x_1^2x_2^2).$$

Se substituirmos cada x_i, na expressão acima, por n obtemos precisamente a resposta da questão (V.1.a). Como dá para desconfiar, a resposta é obtida desta maneira e o teorema de Polya explica porque.

(V.3.b) EXEMPLO: *Índice de ciclos do grupo de rotações do cubo como permutações de vértices*. A classificação das rotações do cubo dada no exemplo anterior é também adequada para o presente exemplo.

A contribuição da identidade é agora x_1^8; rotações do tipo (b) contribuem cada uma com $x_1^2x_3^2$; do tipo (c) com x_2^4; do tipo (d) com x_4^2; do tipo (e) com x_2^4. Daqui se conclui que o índice de ciclos do grupo de rotações do cubo como permutações de vértices é

$$\frac{1}{24}\,(x_1^8 + 8x_1^2x_3^2 + 9x_2^4 + 6x_4^2).$$

Note que ao substituirmos cada x_i na expressão acima por $a^i + b^i + c^i$, obtemos precisamente o inventário dos G-padrões utilizado na resposta para a questão (V.1.b), formulada no começo do capítulo. A justificativa que assim obtemos a resposta correta é, em essência, o teorema fundamental de Polya, de que tratamos a seguir.

V.4 - TEOREMA FUNDAMENTAL DE POLYA

Depois da extensa preparação desenvolvida nas seções anteriores estamos agora em condições de enunciar e estabelecer o teorema central do capítulo.

(V.4.a) TEOREMA FUNDAMENTAL (Polya 1937): O inventário dos G-padrões das funções em C^D é

$$\mathrm{Inv}_{\pi}(C^D \bmod G) = Y_G\left(\sum_{c \in C} \pi(c), \sum_{c \in C} (\pi(c))^2, \ldots, \sum_{c \in C} (\pi(c))^{|D|}\right)$$

PROVA: Suponhamos que os diferentes pesos das funções em C^D formem o subconjunto de A

$$\{\pi_\beta : \beta \in J\},$$

para algum conjunto de índices J. (Como $|C|$ é no máximo enumerável e $|D|$ finito podemos supor que J é enumerável.) Para $\beta \in J$ seja Φ_β o conjunto das funções com peso π_β.

Para cada $g \in G$ e cada $\beta \in J$ fixados vamos definir uma função $\alpha^\beta(g) = \alpha_g^\beta$ que, como provamos em seguida é uma permutação de Φ_β. Se $f \in \Phi_\beta$, definimos

$$\alpha_g^\beta(f) = fg^{-1},$$

onde fg^{-1} é a função $d \longrightarrow f(g^{-1}(d))$ para todo $d \in D$. Observe que

$$\pi(\alpha_g^\beta(f)) = \pi(fg^{-1}) = \pi(f)$$

para qualquer $f \in \Phi_\beta$. Logo

$$\alpha_g^\beta(\Phi_\beta) \subseteq \Phi_\beta.$$

Para provar que α_g^β **é uma permutação de** Φ_β, **mostramos primeiro que esta função é injetiva. Seja** $\alpha_g^\beta(f_1) = \alpha_g^\beta(f_2)$. Isto é,

$f_1 g^{-1} = f_2 g^{-1}$ e daqui obtemos $f_1 = f_2$, provando a injetividade de α_g^β. Suponhamos que $h \in \Phi_\beta$. Queremos encontrar $f \in \Phi_\beta$ tal que $\alpha_g^\beta(f) = h$, isto é, f satisfazendo $fg^{-1} = h$. Para isto é suficiente considerar $f=hg$. Logo, α_g^β é sobrejetiva e portanto uma permutação de Φ_β.

É nossa intenção aplicar o lema algébrico básico (V.1.d) com Φ_β fazendo o papel do X do enunciado deste lema. Para isto precisamos comprovar a condição de homomorfismo. Isto é, para $\beta \in J$ e $g,g' \in G$ devemos ter

$$\alpha^\beta_{g \circ g'} = \alpha^\beta_g \circ \alpha^\beta_{g'}.$$

Para provar a igualdade acima, dado $f \in \Phi_\beta$ precisamos mostrar que

$$\alpha^\beta_{g \circ g'}(f) = \alpha_g(\alpha^\beta_{g'}(f)).$$

Temos, pelas definições

$$\alpha^\beta_{g \circ g'}(f) = f(g \circ g')^{-1} = f\, g'^{-1}\, g^{-1}$$

e

$$\alpha^\beta_g \alpha^\beta_{g'}(f) = \alpha^\beta_g(fg'^{-1}) = f\, g'^{-1}\, g^{-1},$$

comprovando assim que α^β é um homomorfismo de G em S_{Φ_β}, grupo simétrico de permutações de Φ_β.

Entramos agora na fase conclusiva da prova. Seja m_β o número de G-padrões em Φ_β. Como não restringimos $|C|$ a valores finitos, precisamos aqui impor a condição de que cada m_β é finito. Isto é uma hipótese razoável porque se ela é falsa, o problema de enumerar os G-padrões por peso π_β, deixa de ter sentido. A quantidade que procuramos vale simplesmente

$$\mathrm{Inv}_\pi(C^D \mathrm{mod.}\ G) = \sum_{\beta \in J} m_\beta\, \pi_\beta.$$

Para cada $\beta \in J$ vimos que α^β é um homomorfismo de G em S_Φ. O valor de m_β é exatamente o número de G-órbitas induzidas$^\beta$ sobre Φ_β. Podemos aplicar o lema (V.1.d) obtendo

$$m_\beta = |orb(\Phi_\beta, G)| = \frac{1}{|G|} \sum_{g \in G} \mu(\alpha_g^\beta).$$

Assim

$$\begin{aligned} Inv_\pi(C^D \text{ mod. } G) &= \sum_{\beta \in J} m_\beta \pi_\beta \\ &= \sum_{\beta \in J} \left(\frac{1}{|G|} \sum_{g \in G} \mu(\alpha^\beta) \right) \pi_\beta \\ &= \frac{1}{|G|} \sum_{g \in G} \left(\sum_{\beta \in J} \mu(\alpha_g^\beta)\ \pi_\beta \right) \end{aligned}$$

Esta troca nos somatórios se justifica porque estamos interessados em calcular os coeficientes dos π_β's, que são finitos. (Não há problemas de convergência, como usual.) O valor de

$$\sum_{\beta \in J} \mu(\alpha_g^\beta)\ \pi^\beta$$

é o inventário de todas as funções f de C^D que satisfazem $f(d) = f(g(d))$, para $d \in D$. Uma função f satisfaz $f(d)=f(g(d))$ para todo $d \in D$ se e somente se o valor de f é constante nos ciclos de g. Assim, para cada $g \in G$

$$\sum_{\beta \in J} \mu(\alpha_g^\beta)\pi_\beta = \left(\sum_{c \in C} \pi(c) \right)^{b_1(g)} \left(\sum_{c \in C} (\pi(c))^2 \right)^{b_2(g)} \cdots \left(\sum_{c \in C} (\pi(c))^{|D|} \right)^{b_{|D|}(g)}$$

onde $b_i(g)$ é o número de ciclos de g de comprimento i. Para se convencer da igualdade acima, note que cada parcela na expansão do produto à direita corresponde de maneira natural e

biunívoca a uma função de C^D que é constante em cada ciclo de g. Como cada uma de tais parcelas é o peso da função a ela associada. Obtemos assim,

$$\mathrm{Inv}_\pi(C^D \bmod G) =$$

$$\frac{1}{|G|}\sum_{g\in G}\left(\sum_{c\in C}\pi(c)\right)^{b_1(g)}\left(\sum_{c\in C}(\pi(c))^2\right)^{b_2(g)}\cdots\left(\sum_{c\in C}(\pi(c))^{|D|}\right)^{b_{|D|}(g)}$$

$$= Y_G\left(\sum_{c\in C}\pi(c), \sum_{c\in C}(\pi(c))^2, \ldots, \sum_{c\in C}(\pi(c))^{|D|}\right)$$

o que estabelece o teorema. □

Uma expressão para o número de G-padrões é uma consequência direta do teorema que acabamos de provar.

(V.4.b) COROLÁRIO: O número de G-padrões em C^D é

$$Y_G(|C|, |C|, \ldots, |C|).$$

PROVA: Se fizermos $\pi \equiv 1$, o valor de $\mathrm{Inv}_\pi(C^D \bmod D)$ é o número de G-padrões. Se $\pi \equiv 1$,

$$\mathrm{Inv}_\pi(C^D \bmod G) = Y_G(|C|, |C|, \ldots, |C|),$$

provando o corolário. □

O leitor está agora em condições de obter por si mesmo as resposta das duas questões iniciais (V.1.a) e (V.1.b). A resposta da primeira questão é uma aplicação direta do corolário acima. A resposta da segunda questão é uma aplicação simples do teorema (V.4.a). Note que os índices de ciclos já foram obtidos anteriormente, nos requeridos exemplos (V.3.a) e (V.3.b). Aconselhamos o leitor a gastar algum tempo nestes problemas, pois eles são protótipos das aplicações que fazemos a seguir bem como dos exercícios.

(V.4.c) EXEMPLO: *Problema dos colares coloridos*. Considere colares com n contas coloridas com no máximo m cores. Se G é o grupo C_n de rotações das contas, quantos C_n-padrões existem?

Observe que este problema é o mesmo das palavras circulares resolvido no exemplo (IV.2.d) com o auxílio de inversão de Möbius no reticulado dos divisores. É interessante resolvê-lo novamente usando um método diferente e comparar as respostas.

Pelo corolário (V.4.b) o número procurado é

$$\gamma_{C_n}(m,m,\ldots,m).$$

Deixamos, como exercício e deste capítulo, para o leitor provar que

$$\gamma_{C_n}(x_1,x_2,\ldots,x_n) = \frac{1}{n}\sum_{d|n}\phi(d)\,x_d^{n/d},$$

onde ϕ é a função totiente de Euler obtida no exemplo (IV.3.c). Portanto, obtemos para número dos C_n-padrões

$$\frac{1}{n}\sum_{d|n}\phi(d)\,m^{n/d}.$$

No caso de $n=6$ e $m=2$ obtemos para a expressão acima o valor

$$\frac{1}{6}\,(\phi(1)\,2^6 + \phi(2)\,2^3 + \phi(3)\,2^2 + \phi(6)\,2^1)$$

$$= \frac{1}{6}\,(64 + 8 + 8 + 4) = 14.$$

Note que os 14 C_n-padrões foram explicitamente listados na resolução do problema em (IV.2.d). A resolução do mesmo problema usando métodos diferentes nos dá uma conexão interessante entre a função μ de Möbius para o reticulado dos divisores e a função totiente ϕ de Euler:

$$\frac{1}{n}\sum_{d|n}\phi(d)\,m^{n/d} = \sum_{d|n}\frac{1}{d}\sum_{r|d}\mu(r,d)\,m^r.$$

Esta identidade não é óbvia à primeira vista.

(V.4.d) EXEMPLO: *Colares coloridos com reflexão.* Considere a mesma questão do exemplo anterior com a diferença de que agora podemos "virar" os colares além de rodá-los. Isto é, o grupo de simetrias é agora D_n, o grupo diedral em n elementos.

No exercício 5 do presente capítulo, o leitor é solicitado a fornecer uma prova de que

$$Y_{D_n}(x_1,x_2,\ldots,x_n) = \frac{1}{2} Y_{C_n}(x_1,x_2,\ldots,x_n) + \begin{cases} \frac{1}{2} x_1 x_2^{\frac{n-1}{2}}, & n \text{ ímpar} \\ \frac{1}{4}\left(x_2^{n/2} + x_1^2 x_2^{\frac{n-2}{2}}\right), & n \text{ par} \end{cases}$$

Aplicando o corolário (V.4.b) a esta expressão de Y_{D_n} obtemos para o número de D_n-padrões

$$\frac{1}{2n} \sum_{d|n} \phi(d)\, m^{n/d} + \begin{cases} \frac{1}{2} m^{\frac{n+1}{2}}, & n \text{ ímpar} \\ \frac{1}{4}\left(m^{n/2} + m^{\frac{n+2}{2}}\right), & n \text{ par.} \end{cases}$$

Para $n=6$ e $m=2$ obtemos

$$7 + \frac{1}{4}(2^3 + 2^4) = 13$$

D_n-padrões. Comparando com a resposta obtida para o exemplo anterior, concluimos que existe apenas 1 C_n-padrão de contas que quando refletido dá um C_n-padrão diferente. Isto pode ser comprovado pela inspeção direta nas 14 palavras circulares listadas no exemplo (IV.2.d): explicitamente, as palavras circulares.

a a b a b b

b b a b a a

são os únicos C_n-padrões diferentes que quando refletidos (invertidas as palavras) coincidem. As outras palavras circulares são todas iguais às suas inversas.

Na próxima seção consideramos a enumeração de grafos, historicamente a maior fonte de desafios em enumeração. Estes desafios ao serem ultrapassados vão deixando como legado as técnicas enumerativas. A teoria que emerge do teorema fundamental de Polya é um exemplo típico deste fato.

V.5 - CONTANDO GRAFOS

Nesta seção enumeramos grafos simples. Um grafo *simples* é um grafo onde entre cada par de vértices há no máximo 1 aresta e onde não há laços, ou seja, arestas ligando um vértice a si mesmo. Desenvolvemos a seguir uma técnica, utilizando o teorema (V.4.a), para encontrar o número de grafos simples com n vértices e m arestas.

Note que o problema de contar grafos simples rotulados é trivial: existem

$$\left(\binom{n}{2} \right)_m$$

grafos rotulados simples distintos com n vértices e m arestas, pois existem $\binom{n}{2}$ pares (desordenados) de vértices e entre eles pode haver uma aresta ou não. Para o nosso problema dois grafos simples rotulados são considerados o mesmo, se é possível encontrar uma bijeção entre os vértices que preserve as incidências, em outras palavras, os rótulos são irrelevantes. (Decidir se existe tal bijeção usando um algoritmo cujo número de passos básicos seja limitado pelo valor em n, número de vértices do grafo, de um polinômio fixo (de qualquer grau), é um dos problemas abertos mais importantes de nosso tempo em computação teórica. Felizmente não precisamos efetuar esta decisão.)

Identificamos agora os objetos para aplicar o teorema (V.4.a). O domínio D é o conjunto de pares desordenados de vértices, cada um destes últimos representados por um número de 1 a n. O contradomínio C, por motivo que fica claro logo a seguir, é formado por dois adjetivos:

$$C = \{\text{presente, ausente}\}.$$

Um grafo rotulado simples pode ser visto como uma função

$$f: D \longrightarrow C$$

onde

$$f(\{i,j\}) = \begin{cases} \text{presente, se há aresta entre } i \text{ e } j \\ \text{ausente, em caso contrário.} \end{cases}$$

O grupo de simetrias, G, no caso, é o chamado grupo *par-desordenado* $S_n^{\{2\}}$. Este grupo abstratamente é S_n, porém como grupo de permutações (que é o que nos interessa sempre) é o grupo de permutações de pares ordenados induzidos por S_n. Por exemplo, à permutação

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

de S_n corresponde a permutação

$$\begin{pmatrix} \{1,2\} & \{1,3\} & \{1,4\} & \{2,3\} & \{2,4\} & \{3,4\} \\ \{1,3\} & \{3,4\} & \{2,3\} & \{1,4\} & \{1,2\} & \{2,4\} \end{pmatrix}.$$

Para completar os nossos preparativos para usar o teorema de Polya, seja o peso π definido como

$$\pi(\text{ausente}) = x^0 = 1$$
$$\pi(\text{presente}) = x^1 = x.$$

Com esta definição, o peso de cada grafo simples rotulado, visto como função de D em C, pela definição de peso de função em C^D, é simplesmente x^m onde m é o número de arestas do grafo. Com este peso, o inventário dos G-padrões em C^D nos dá como coeficiente de x^m o número g(n,m) de grafos simples com n vértices e m arestas. Pelo teorema (V.4.a) concluímos,

(V.5.a) TEOREMA: O número de grafos simples com n vértices e m arestas é

$$g(n,m) = \left[x^m\right]\left\{ Y_{S_n^{\{2\}}}\left(1 + x,\ 1 + x^2, \ldots, 1 + x^{\binom{n}{2}}\right)\right\}. \ \square$$

Vamos agora explicar, com um exemplo, como o índice de ciclos de $S_n^{\{2\}}$ pode ser calculado a partir do índice de ciclos de S_n. Como mostramos no corolário (III.4.k) estes últimos podem ser recursivamente calculados. Ilustramos como $Y_{S_n^{\{2\}}}$ pode ser obtido a partir de Y_{S_n} tratando o caso n=5. Usando a recorrência do corolário (III.4.k) já obtivemos

$$Y_{S_5} = Y_5 = \frac{1}{120}\,(x_1^5 + 10x_1^3x_2 + 15x_1x_2^2 + 20x_1^2x_3 + 30x_1x_4 + 20x_2x_3 + 24x_5).$$

Ao termo x_1^5 que vem da identidade, corresponde em $Y_{S_5^{\{2\}}}$ o termo x_1^{10}. A cada uma das 10 permutações responsáveis por $10\,x_1^3\,x_2$ corresponde a parcela $x_1^4\,x_2^3$ de $Y_{S_5^{\{2\}}}$. Para constatar isto note que à permutação de S_5 expressa como ciclos disjuntos como

$$(1)\ (2)\ (3)\ (4,5)$$

que tem tipo $x_1^3\,x_2$ corresponde a permutação

$$(\{1,2\})(\{1,3\})(\{2,3\})(\{4,5\},\{4,5\})(\{2,4\},\{2,5\})(\{3,4\},\{3,5\})$$

que tem tipo $x_1^4\,x_2^3$. Por simetria, cada uma das outras 9 permutações de tipo $x_1^3\,x_2$ em S_5 induz uma permutação de tipo $x_1^4\,x_2^3$. Logo à parcela $10\,x_1^3\,x_2$ de Y_{S_5} corresponde a parcela $10\,x_1^4\,x_2^3$ de $Y_{S_5^{\{2\}}}$.

À parcela $15\,x_1\,x_2^2$ de Y_{S_6} corresponde a parcela $15\,x_1^2\,x_2^4$, pois

(1) (2 3) (4 5)

induz

$$(\{2,3\})(\{4,5\})(\{1,2\},\{1,3\})(\{1,4\},\{1,5\})(\{2,4\},\{3,5\})(\{3,4\},\{2,5\}).$$

À parcela $20\, x_1^2\, x_3$ de γ_{S_5} corresponde a parcela $20\, x_1\, x_3^3$ de $\gamma_{S_5^{\{2\}}}$ pois

(1) (2) (3,4,5)

induz

$$(\{1,2\})(\{1,3\},\{1,4\},\{1,5\})(\{2,3\},\{2,4\},\{2,5\})(\{3,4\}\,\{4,5\}\,\{5,3\}).$$

De maneira análoga obtemos as correspondências restantes

$$\begin{aligned} 30\, x_1\, x_4 &\longrightarrow 30\, x_2\, x_4^2 \\ 20\, x_2\, x_3 &\longrightarrow 20\, x_1\, x_3\, x_6 \\ 24\, x_5 &\longrightarrow 24\, x_5^2 \,. \end{aligned}$$

Agrupando o que foi obtido concluímos que

$$\gamma_{S_5^{\{2\}}}(x_1,x_2,x_{10}) =$$

$$= \frac{1}{120}\,(x_1^{10} + 10x_1^4x_2^3 + 15x_1^2x_2^4 + 20x_1x_3^3 + 30x_2x_4^2 + 20x_1x_3x_6 + 24x_5^2).$$

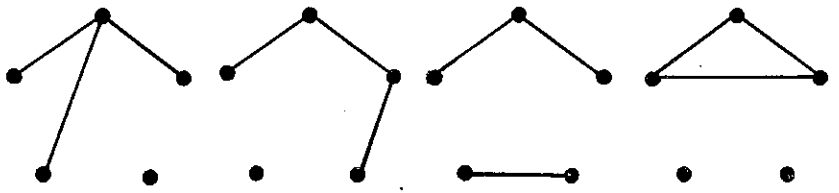
Pelo teorema (V.5.a) o número $g(5,m)$ é

$$\frac{1}{120}\,[x^m]\left\{(1+x)^{10} + 10(1+x)^4\,(1+x^2)^3 + 15(1+x)^2\,(1+x^2)^4 + 20(1+x)\,(1+x^3)^3 + 30(1+x^2)\,(1+x^4)^2 + 20(1+x)\,(1+x^3)\,(1+x^6) + 24(1+x^5)^2\right\},$$

ou seja

$$[x^m]\left\{1 + x + 2x^2 + 4x^3 + 6x^4 + 6x^5 + 6x^6 + 4x^7 + 2x^8 + x^9 + x^{10}\right\}.$$

Assim, por exemplo, existem 4 grafos distintos com 5 vértices e 3 arestas, que são mostrados abaixo:



Se somarmos os coeficientes do polinômio acima, obtemos o total de grafos simples com 5 vértices. Explicitamente, existem

$$1 + 1 + 2 + 4 + 6 + 6 + 6 + 4 + 2 + 1 + 1 = 34$$

grafos simples com 5 vértices. Este valor pode ser diretamente obtido do corolário (V.4.b). Segundo este corolário, o número total de grafos simples com 5 vértices é

$$Y_{S_5^{\{2\}}}(2,2,2,2,2,2,2,2,2,2),$$

ou seja

$$\frac{1}{120}(2^{10} + 10.2^7 + 15.2^6 + 20.2^4 + 30.2^3 + 20.2^3 + 24.2^2)$$

$$= \frac{1}{120}(1024 + 1280 + 960 + 320 + 240 + 160 + 96) = 34 .$$

Outros tipos de grafos além dos simples, como grafos com múltiplas arestas, grafos dirigidos, etc, são enumerados usando a mesmas idéias básicas aqui apresentadas e o leitor não deve encontrar dificuldades em aplicá-las. Nos exercícios 13 - 15 e 20 - 22 deste capítulo extensões deste tipo com sugestões são considerados.

V.6 - G×H - PADRÕES

Nesta seção vamos extender a situação básica tratada no teorema fundamental (V.4.a). Além do grupo G de permutações dos elementos do domínio D consideramos também um grupo H de permutações dos elementos do contradomínio C. Este conjunto é doravante considerado finito. Se H for o grupo trivial, temos a situação anterior.

Duas funções f_1 e f_2 são G×H-associadas se existem $g \in G$, $h \in H$ tais que

$$f_1(g(d)) = h(f_2(d)),$$

para todo $d \in D$. É fácil verificar que G×H-associação é uma relação de equivalência, o que deixamos a cargo do leitor. Cada classe desta relação de equivalência é chamada de *GXH-padrão*. Suponhamos que cada $f \in C^D$ tem associada um peso

$$\pi(f),$$

isto é, é dada uma função

$$\pi: C^D \longrightarrow A,$$

onde A é um anel comutativo contendo os racionais. Exigimos também que se f_1 e f_2 estão no mesmo G×H - padrão, então

$$\pi(f_1) = \pi(f_2).$$

Esta restrição é chamada de *condição de compatibilidade*. Observe que esta condição no caso de G-padrões é uma conseqüência da definição de $\pi(f)$, naquele caso como produto dos pesos das imagens de f.

Ilustramos agora o fato de que a condição de compatibilidade não é mantida no caso de repetirmos esta estratégia de atribuição dos pesos. Sejam $D = \{1,2\}$, $C = \{x,y\}$, G o grupo simétrico agindo em D e H o grupo simétrico agindo em C. Con-

sidere f_1, $f_2 \in C^D$ definidas por

$$f_1(1) = x \ , \ f_2(2) = x$$

$$f_2(1) = y \ , \ f_2(2) = y.$$

Estas funções estão no mesmo G×H-padrão, pois denotando a identidade de G por g e o elemento diferente da identidade de H por h temos

$$f_1(g(1)) = f_1(1) = x = h(y) = h(f_2(1))$$

$$f_1(g(2)) = f_2(2) = x = h(y) = h(f_2(2)).$$

Se associarmos os pesos $\pi(x) = a$, $\pi(y) = b$ e encontrarmos $\pi(f_1)$ e $\pi(f_2)$ como no caso dos G-padrões obtemos,

$$\pi(f_1) = \pi(f_1(1))\ \pi(f_1(2)) = a^2$$

$$\pi(f_2) = \pi(f_2(1))\ \pi(f_2(2)) = b^2.$$

Dessa maneira, funções no mesmo G × H-padrão poderiam ter pesos diferentes. Como a condição de compatibilidade é vital para nossos propósitos temos de impô-la explicitamente. Esta imposição restringe bastante a aplicabilidade do teorema principal desta seção que provamos abaixo. Este teorema é obtido por De Brujin em [DB 1] e neste trabalho ele nos dá estratégias bastante gerais de atribuir pesos de forma a satisfazer à condição de compatibilidade. Como as estratégias são complicadas, mesmo de serem enunciadas, nos restringimos neste texto a particularizar o teorema de De Brujin para tratar o caso do número total de G × H-padrões. O peso π neste caso associa 1 a toda função de C^D, e a condição de compatibilidade é trivialmente satisfeita. Nos exercícios 24 e 25 deste capítulo o leitor é solicitado a estabelecer a expressão para o número de G×H-padrões de funções em C^D que são injetivas. Neste caso o peso π associa a f o valor 1 se f é injetiva ou 0 em caso contrário. A condição de compatibilidade, novamente, é trivialmente satisfeita.

De maneira análoga à dos G-padrões, o *inventário* dos G×H-padrões é a soma dos pesos dos G×H-padrões. Certamente, como impomos a condição de compatibilidade, definimos o peso de um G×H-padrão como o peso comum a todas as funções a ele pertencentes. Tratamos agora o resultado básico sobre G × H-padrões.

(V.6.a) TEOREMA (De Brujin - 1956): O inventário dos G H-padrões de funções em C^D é

$$\mathrm{Inv}_{\pi}(C^D \text{ mod.}(G\times H)) = \frac{1}{|G|.|H|} \sum_{g \in G} \sum_{h \in H} \sum_{f}^{(g,h)} \pi(f).$$

O peso π satisfaz à condição de compatibilidade e a soma interna é extendida a todas as funções de C^D que satisfazem $fg=hf$, isto é, $f(g(d)) = h(f(d))$ para todo $d \in D$.

PROVA: A prova é uma aplicação do lema algébrico básico (V.1.d) a cada conjunto de funções com o mesmo peso, exatamente como na prova do teorema fundamental (V.4.a). Seja portanto

$$\{\pi_\beta : \beta \in J\}$$

o subconjunto de A formado pela imagem de π. Para $\beta \in J$ seja também Φ_β o conjunto das funções em C^D com peso π_β. Considere o grupo (produto direto) G × H definido pelos pares (g,h) com $g \in G$, $h \in H$, com a operação) $*$ dada por

$$(g,h) * (g',h') = (gg', hh').$$

Para cada β fixado definimos uma função

$$\alpha^\beta : G \times H \longrightarrow S_{\Phi_\beta},$$

onde S_{Φ_β} é o grupo simétrico das permutações de Φ_β. A imagem de (g,h) por f é denotada por

$$\alpha^\beta(g,h) = \alpha^\beta_{g,h}$$

e é definida como sendo a função de $\Phi_\beta \longrightarrow C^D$ que leva f em

$$\alpha^\beta_{g,h}(f) = h\ f\ g^{-1}.$$

Pela condição de compatibilidade, $\alpha^\beta_{g,h}$ mantêm o peso das funções. Assim $\alpha^\beta_{g,h}(\Phi_\beta) \subseteq \Phi_\beta$. Para provar a injetividade, suponha que

$$\alpha^\beta_{g,h}(f_1) = \alpha^\beta_{g,h}(f_2).$$

Isto é equivalente a $h\ f_1\ g^{-1} = h\ f_2\ g^{-1}$, ou seja, a $f_1 = f_2$. A função $\alpha^\beta_{g,h}$ é também sobrejetiva: se $f_2 \in \Phi_\beta$, procuramos por $f \leq \Phi_\beta$ tal que $\alpha^\beta_{g,h}(f) = f_2$, ou seja, $f_2 = h\ f\ g^{-1}$. Se definirmos $f_1 = h^{-1}\ f_2\ g$ e tomarmos f_1 para o nosso f, comprovamos a sobrejetividade de $\alpha^\beta_{g,h}$. Assim esta função é uma permutação do conjunto Φ_β.

Mostramos agora que para todo $\beta \in J$, α^β é um homomorfismo. Para cada $f \in \Phi_\beta$,

$$\alpha^\beta_{(g,h)\ *\ (g',h)}(f) = \alpha^\beta_{gg',\ hh'}(f) = hh'\ f(g'^{-1}\ g^{-1})$$

e

$$\alpha^\beta_{g,h}(\alpha^\beta_{g',h'}(f)) = \alpha^\beta_{g,h}(h'\ f\ g'^{-1}) = h(h'\ f\ g'^{-1})\ g^{-1},$$

de onde obtemos

$$\alpha^\beta_{(g,h)\ *\ (g',h')} = \alpha^\beta_{g,h}\ o\ \alpha^\beta_{g',h'},$$

estabelecendo que α^β é um homomorfismo.

Podemos agora aplicar, desde que estamos sob suas hipóteses, o lema algébrico básico (V.1.d) para calcular o número de $G \times H$ órbitas nas quais Φ_β se decompõe. Fazendo isto obtemos

$$\left|\mathrm{orb}(\Phi_\beta,\ G \times H)\right| = \frac{1}{|G \times H|} \sum_{(g,h) \in G \times H} \mu(\alpha^\beta_{g,h})$$

onde, interpretado na presente situação, $\mu(\alpha^{\beta}_{g,h})$ é o número de funções em Φ_β satisfazendo

$$\alpha^{\beta}_{g,h}(f) = f.$$

Para obter o inventário que queremos, precisamos apenas multiplicar o número de $G \times H$ - órbitas de funções com peso π_β por π_β e somar para $\beta \in J$. Isto é, o que procuramos pode ser escrito como

$$\sum_{\beta \in J} \frac{1}{|G \times H|} \left(\sum_{g,h \in G \times H} \mu(\alpha^{\beta}_{g,h}) \right) \pi_\beta$$

ou como,

$$\frac{1}{|G|.|H|} \sum_{g \in G} \sum_{h \in H} \left(\sum_{\beta \in J} \mu(\alpha^{\beta}_{g,h}) \, \pi_\beta \right).$$

Note que,

$$\sum_{\beta \in J} \mu(\alpha^{\beta}_{g,h}) \, \pi_\beta = \sum_{f}^{(g,h)} \pi(f).$$

Assim, o inventário procurado é

$$\mathrm{Inv}_\pi(C^D \text{ mod. } (G \times H)) = \frac{1}{|G|.|H|} \sum_{g \in G} \sum_{h \in H} \sum_{f}^{(g,h)} \pi(f),$$

Como queríamos provar.

V.7 - NÚMERO TOTAL DE G × H-PADRÕES

Nesta seção particularizamos o teorema de De Brujin provado na seção anterior para o caso em que $\pi \equiv 1$. Neste caso o inventário de G × H-padrões é simplesmente o seu número.

(v.7.a) TEOREMA (De Brujin - 1956): O número total de G × H - padrões em C^D é dado por

$$Y_G\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \ldots, \frac{\partial}{\partial x_{|D|}}\right)\left\{ Y_H\left[\exp\left(\sum_{j=1}^{|D|} x_j\right), \exp\left(\sum_{j=2}^{\left\lfloor \frac{|D|}{2} \right\rfloor} 2x_{2j}\right), \ldots, \exp\left(\sum_{j=1}^{\left\lfloor \frac{|D|}{|C|} \right\rfloor} |C|\, x_{|C|j}\right)\right]\right\}$$

avaliado em $x_1 = x_2 = \ldots = x_{|D|} = 0$.

(V.7.b) EXEMPLO: Antes de estabelecermos o teorema acima, vamos exemplificar sua aplicação numa situação simples. Com isto visamos ajudar o leitor a entender a complicada expressão acima envolvendo operadores diferenciais.

Recorde, em primeiro lugar, que $\left\lfloor \frac{n}{m} \right\rfloor$ é o maior inteiro menor ou igual a $\frac{n}{m}$. Sejam $D = \{a,b,c\}$, $C = \{x,y\}$, G o grupo simétrico S_D e H o grupo simétrico S_C. Vamos aplicar o teorema acima para obter o número de $S_D \times S_C$ - padrões. Temos, por inspeção direta ou obtido recursivamente, como o fizemos após o corolário (III.4.k),

$$Y_{S_C}(x_1,x_2) = Y_2 = \frac{1}{2}(x_1^2 + x_1^3)$$

$$Y_{S_D}(x_1,x_2,x_3) = Y_3 = \frac{1}{6}(x_1^3 + 3x_2x_1 + 2x_3)$$

O que o teorema nos diz é que, primeiro, devemos obter um operador diferencial substituindo cada x_i por $\frac{\partial}{\partial x_i}$ na expressão do índice de ciclos de $G = S_D$. Fazendo isto conseguimos

$$\frac{1}{6}\left(\frac{\partial^3}{\partial x_1^3} + 3\,\frac{\partial}{\partial x_1}\,\frac{\partial}{\partial x_2} + 2\,\frac{\partial}{\partial x_3}\right).$$

Em seguida devemos aplicar este operador à expressão obtida do índice de ciclos de $H = S_C$ com a substituição de cada x_i por

$$\exp\left(\sum_{j=1}^{\left\lfloor \frac{D}{i} \right\rfloor} i\, x_{ij}\right).$$

No nosso caso esta expressão é

$$\frac{1}{2}\left\{\left[\exp(x_1+x_2+x_3)\right]^2 + \exp(2x_2)\right\} =$$

$$= \frac{1}{2}\left(e^{x_1+x_2+x_3} + e^{2x_2}\right).$$

Aplicando o operador diferencial à expressão acima e calculando no ponto $x_1=x_2=x_3=0$ obtemos

$$\frac{1}{12}\,(2^3 + 3 \times 2 \times 2 + 2 \times 2) = \frac{24}{12} = 2.$$

Note que este exemplo é suficientemente simples para conferirmos a resposta. O número de maneira distintas de colocarmos 3 objetos indistinguíveis em duas caixas também indistinguíveis é 2: 3 numa caixa e 0 na outra ou 2 numa caixa e 1 na outra. Em termos de funções de D em C temos 2 $S_D \times S_C$ - padrões:

a ⟶ x	a ⟶ x
b ⟶ x	b ⟶ x
c ⟶ x	c ⟶ y

PROVA DO TEOREMA (V.7.a). A base da prova é o teorema anterior,

que trata o caso de pesos arbitrários que satisfazem à condição de compatibilidade. No caso presente, vamos ter condições de avaliar a expressão chave

$$\sum_{f}^{(g,h)} \pi(f).$$

No nosso caso, como $\pi \equiv 1$, esta expressão conta o número de funções $f \in C^D$ que satisfazem $fg=hf$ para g e h fixados.

Suponha que f satisfaz $fg=hf$. Então se $d \in D$ é um elemento que está num ciclo de comprimento i de g e $f(d)= c$ temos

$$fg(d) = hf(d) = h(c)$$

$$f(g^2(d)) = hf(g(d)) = h^2 f(d) = h^2(c)$$

$$\cdots$$

$$f(g^{i-1}(d)) = hf\, g^{i-1}(d) = \ldots = h^{i-1} f(d) = h^{i-1}(c)$$

e isto nos diz em particular que o comprimento j do ciclo de h que contém c divide i. Claramente a recíproca é também verdadeira: se cada ciclo de g de comprimento i é levado i/j vezes num ciclo de h de comprimento j com $j|i$ da maneira cíclica especificada acima, então $fg=hf$.

Com esta caracterização é fácil computar o número de f's satisfazendo $fg=hf$. Para cada ciclo de g escolhamos um elemento distinguido chamado de *cabeça de ciclo*. O número de possibilidades para a imagem por f de uma cabeça de ciclos é

$$\sum_{j|i} j\, c_j,$$

onde $(c_1, c_2, \ldots, c_{|C|})$ é o tipo de h, isto é, existem c_j ciclos em h com comprimento j.

Como as escolhas das imagens das cabeças de ciclos são

independentes e elas especificam completamente uma função f satisfazendo fg=hf, temos que o número de tais funções é

$$\sum_{f}^{g,h} \pi(f) = \prod_{i=1}^{|D|} \left(\sum_{j|i} j c_j \right)^{b_i} ,$$

onde $(b_1, b_2, \ldots, b_{|D|})$ é o tipo de G. Usando este fato e o teorema (V.6.a), podemos escrever o número total de G × H- padrões como

$$\frac{1}{|G| \cdot |H|} \sum_{g \in G} \sum_{h \in H} \prod_{i=1}^{|D|} \left(\sum_{j|i} j c_j \right)^{b_i} .$$

Neste ponto os operadores diferenciais entram em cena para associar a expressão acima com os índices de ciclos de G e de H. Note que uma potência r^n pode ser expressa como a n-ésima derivada de e^{rx} calculada no ponto x=0. Uma generalização direta para muitas variáveis independentes deste fato permite escrever o produto

$$\prod_{i=1}^{|D|} \left(\sum_{j|i} j c_j \right)^{b_i} .$$

como

$$\frac{\partial}{\partial x_1} \frac{\partial}{\partial x_2} \cdots \frac{\partial}{\partial x_{|D|}} \left\{ \exp \left[\sum_{i=j}^{|D|} x_i \left(\sum_{j|i} j c_j \right) \right] \right\}$$

avaliado em $x_1 = x_2 = \ldots = x_{|D|} = 0$.

Observe em seguida que

$$\sum_{i=1}^{|D|} x_i \left(\sum_{j|i} j c_j \right) = \sum_{j=1}^{|D|} j c_j \left(x_j + x_{2j} + \ldots + x_{\left\lfloor \frac{|D|}{j} \right\rfloor j} \right)$$

$$= \sum_{i=1}^{|C|} i c_i \left(\sum_{j=1}^{\left\lfloor \frac{|D|}{i} \right\rfloor} x_{ij} \right).$$

Note que para obter a última expressão, trocamos os papéis de i e j com o intuito de obter uma notação consistente com o enunciado do teorema. Além disso, trocamos o limite superior da soma externa de $|D|$ para $|C|$. Isto não causa alterações pelo seguinte: se $|D| > |C|$, todo c_i com $i > |C|$ vale 0. Se $|D| < |C|$ e $h \in H$ tem algum ciclo de comprimento i maior que $|D|$, então a soma interna não faz sentido a priori, pois o índice varia entre 1 e 0. No entanto, analisando a situação combinatorial vê-se claramente que no caso esta soma interna deve ser definida como 0.

Podemos então escrever para o número de $G \times H$-padrões,

$$\frac{1}{|G| \times |H|} \sum_{g \in G} \sum_{h \in H} \left(\frac{\partial}{\partial x_1} \right)^{b_1} \left(\frac{\partial}{\partial x_2} \right)^{b_2} \cdots \left(\frac{\partial}{\partial x_{|D|}} \right)^{b_{|D|}}$$

$$\left\{ \exp \left[\sum_{i=1}^{|C|} i c_i \left(\sum_{j=1}^{\left\lfloor \frac{|D|}{i} \right\rfloor} x_{ij} \right) \right] \right\}_{x_1 = x_2 = \ldots = x_{|D|} = 0}.$$

Como os b_i's são fixos para cada $g \in G$, usado a linearidade dos operadores diferenciais e outras modificações simples obtemos para a expressão acima:

$$\frac{1}{|G|}\sum_{g\in G}\left(\frac{\partial}{\partial x_1}\right)^{b_1}\left(\frac{\partial}{\partial x_2}\right)^{b_2}\cdots\left(\frac{\partial}{\partial x_{|D|}}\right)^{b_{|D|}}$$

$$\left\{\frac{1}{|H|}\sum_{h\in H}\prod_{i=1}^{|C|}\exp\left(\sum_{j=1}^{\left\lfloor\frac{|D|}{i}\right\rfloor} i x_{ij}\right)^{c_i}\right\}_{x_1=x_2=\ldots=x_{|D|}=0}.$$

Finalmente observe que o operador diferencial pode ser obtido a partir da substituição

$$x_i \longrightarrow \frac{\partial}{\partial x_i}\ ,\ i=1,2,\ldots,|D|,$$

da expressão para o índice de ciclos de G. Analogamente, o operando pode ser obtido a partir da expressão para o índice de ciclos de H efetuando a substituição

$$x_i \longrightarrow \exp\left(\sum^{\left\lfloor\frac{|D|}{i}\right\rfloor} i\, x_{ij}\right)\ ,\ i=1,2,\ldots,|C|.$$

Desse modo obtemos que o número de $G \times H$ - padrões é

$$Y_G\left(\frac{\partial}{\partial x_1},\frac{\partial}{\partial x_2},\ldots,\frac{\partial}{\partial x_{|D|}}\right)\left\{Y_H\left[\exp\left(\sum_{j=1}^{|D|} x_j\right),\ \exp\left(\sum_{j=1}^{\left\lfloor\frac{|D|}{2}\right\rfloor} 2x_{2j}\right),\ \ldots\right.\right.$$

$$\left.\left.\ldots\ \exp\left(\sum_{j=1}^{\left\lfloor\frac{|D|}{|C|}\right\rfloor} |C|\, x_{|C|j}\right)\right]\right\}$$

avaliado em $x_1=x_2=\ldots=x_{|D|}=0$. Isto conclui a prova do teorema. □

(V.7.b) EXEMPLO: *Colorações cíclicas das faces de um tetraedro.*

Vamos calcular o número de maneiras distintas de pintarmos as faces de um tetraedro com no máximo 4 cores rotuladas 1, 2, 3, 4. Duas colorações são consideradas idênticas, se uma é obtida da outra por uma rotação do tetraedro, seguida por uma rotação cíclica das cores. O grupo G é no caso o grupo de rotações do tetraedro como permutações de faces. O índice de ciclos de G é pedido no exercício 1 desta seção e vale

$$\frac{1}{12}\,(x_1^4 + 8x_1x_3 + 3x_2^2).$$

O grupo H, no caso presente, é o grupo cíclico de 4 elementos, representados por permutações da maneira usual. O seu índice de ciclos pode ser diretamente calculado e vale

$$\frac{1}{4}\,(x_1^4 + x_2^2 + 2x_4).$$

Aplicando o teorema (V.7.a) obtemos para o número de colorações cíclicas distintas, ou G × H - padrões,

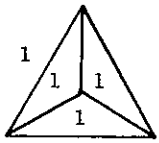
$$\frac{1}{12}\left(\frac{\partial}{\partial x_1^4} + 8\,\frac{\partial}{\partial x_1}\,\frac{\partial}{\partial x_3} + 3\,\frac{\partial^2}{\partial x_2^2}\right)\left\{\frac{1}{4}\left(e^{4(x_1+x_2+x_3+x_4} + e^{2(2x_2+2x_4)} + 2e^{x_4}\right)\right\}_{x_1=x_2=x_3=x_4=0}.$$

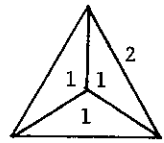
Computando este valor obtemos

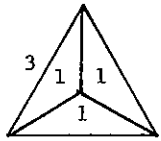
$$\frac{1}{48}\,(4^4 + 8 \times 4 \times 4 + 3 \times 4^2 + 3 \times 4^2) =$$

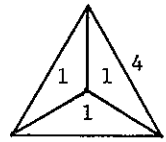
$$\frac{1}{48}\,(256 + 128 + 48 + 48) = 10$$

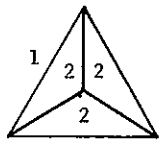
G × H - padrões ou colorações cíclicas distintas. Como uma verificação listamos abaixo as 10 colorações cíclicas distintas.

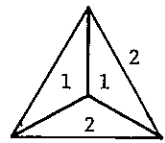

1
1
1
1

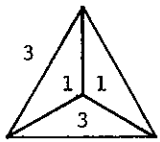

2
1
1
1

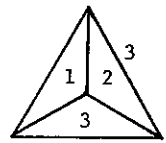

3
1
1
1

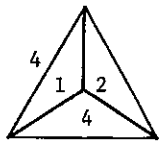

4
1
1
1

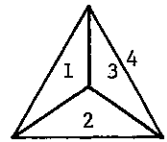

1
2
2
2


2
1
1
2


3
1
1
3


3
1
2
3


4
1
2
4


1
3
4
2

V.8 - G-PADRÕES AUTO-COMPLEMENTARES

Nesta seção, inicialmente encontramos uma forma mais simples do teorema (V.7.a) no caso $|C| = 2$ e $H = S_2$. A seguir, mostramos que esta especialização tem como aplicação a enumeração de G-padrões auto-complementares, conceito que definimos abaixo. Um exemplo típico desta aplicação é a enumeração dos grafos simples que são isomorfos aos seus complementos. (O *complemento* $\overline{G}$ de um grafo simples G é o grafo simples obtido de G trocando aresta por não aresta.)

O índice de ciclos de S_2 é

$$Y_{S_2}(x_1, x_2) = \frac{1}{2}(x_1^2 + x_2).$$

Portanto, para $H = S_2$ o teorema (V.7.a) nos dá para número total de G × H - padrões

$$\frac{1}{2} Y_G\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2}, \ldots, \frac{\partial}{\partial x_{|D|}}\right)\left\{ e^{2(x_1+x_2+\ldots+x_{|D|})} + e^{2(x_2+x_4+\ldots+x_{2\left\lfloor\frac{|D|}{2}\right\rfloor})}\right\}$$

calculado em $x_1=x_2=\ldots=x_{|D|}$. Esta expressão, como pode ser facilmente verificada, é igual à expressão dada no corolário seguinte.

(V.8.a) COROLÁRIO: O número total de G × S_2 - padrões em 2^D é

$$\frac{1}{2} Y_G(2,2,\ldots,2) + \frac{1}{2} Y_G(0,2,0,2,\ldots),$$

onde o número de variáveis é $|D|$, as variáveis da segunda parcela de índice ímpar valem 0 e as de índice par valem 2. □

Se compararmos a soma acima com a expressão que se obtém no caso em que $H = \{id\}$, ou seja, o número de G-padrões com $|C| = 2$, que pelo corolário (V.4.b) vale

$$Y_G(2,2,\ldots,2),$$

não é difícil chegarmos à conclusão enunciada no próximo teorema. Antes porém, precisamos definir o conceito central desta seção.

Suponhamos que $C = \{x,y\}$ e que $H = \{id\}$. Um G-padrão Ω é dito *autocomplementar* se a função $\bar{f}$ obtida de uma função $f \in \Omega$ por

$$\bar{f}(d) = x \quad \text{se} \quad f(d) = y$$
$$= y \quad \text{se} \quad f(d) = x,$$

para todo $d \in D$ está em Ω. Note que no caso presente com $|C|=2$, um elemento de C pode ser pensado como "presença" e o outro como "ausência", daí a razão da terminologia auto-complementar.

(V.8.b) **TEOREMA:** Se $|C| = 2$ o número de G-padrões auto-complementares de funções em C^D é

$$|\text{Autcomp}(2^D \bmod G)| = \gamma_G(0,2,0,2,\ldots).$$

PROVA: O número total de $G \times S_2$-padrões é grosseiramente a metade do número de G-padrões: se não houvessem G-padrões auto-complementares este cálculo estaria correto. Em geral é claro que 2 vezes o número de $G \times S_2$-padrões é igual ao número de G-padrões mais o número de G-padrões auto-complementares. Isto porque pares iguais de $G \times S_2$-padrões correspondem naturalmente a pares de G-padrões complementares e cada G-padrão auto-complementar aparece duas vezes nestes pares. Pelo corolário anterior, duas vezes o número de $G \times S_2$-padrões é

$$\gamma_G(2,2,\ldots,2) + \gamma_G(0,2,0,2,\ldots).$$

Pelo argumento acima e pelo corolário (V.4.b) esta expressão é igual a

$$\gamma_G(2,2,\ldots,2) + |\text{Autcomp}(2^D \bmod G)|.$$

Logo

$$|\mathrm{Autcomp}(2^D \bmod G)| = Y_G(0,2,0,2,\ldots),$$

provando o teorema. □

(V.8.c) EXEMPLO: *Grafos simples auto-complementares* . Quantos grafos simples auto-complementares com n vértices existem?

O grupo G neste caso é o grupo par - desordenado $S_n^{\{2\}}$, introduzido na seção V.5. Pelo teorema anterior, o número procurado é

$$Y_{S_n^{\{2\}}}(0,2,0,2,\ldots).$$

Para ilustrar concretamente tratamos o caso n=5. Na seção V.5 calculamos o valor de $Y_{S_5^{\{2\}}}$:

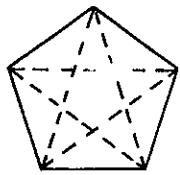
$$Y_{S_5^{\{2\}}}(x_1,x_2,\ldots,x_{10}) =$$

$$= \frac{1}{120}(x_5^{10} + 10x_1^4x_2^3 + 15x_1^2x_2^4 + 20x_1x_3^3 + 30x_2x_4^2 + 20x_1x_3x_6 + 24x_5^2)$$

Logo, pelo teorema acima, existem

$$\frac{1}{120}(0 + 0 + 0 + 0 + 30 \times 2 \times 2^2 + 0 + 0) = 2$$

grafos simples com 5 vértices que são auto-complementares. Um destes grafos, onde o complementar é indicado por linhas partidas é mostrado abaixo.



Desafiamos o leitor a encontrar o outro. Observe, depois de ter encontrado o segundo grafo simples auto-complementar por tentativa e erro, a "força" da teoria provando que não existem outros.

Uma tabela dos números a_n de grafos auto-complementares com n vértices pode ser facilmente obtida dos índices de ciclos de $S_n^{\{2\}}$. Seus primeiros valores são

n	a_n
4	1
5	2
8	10
9	36
12	720
13	5600
16	703760
17	11.220.000

Para os valores intermediários de n não listados a_n vale zero. No exercício 27 deste capítulo o leitor é solicitado a explicar este fato.

(V.8.d) EXEMPLO : *Digrafos simples auto-complementares* . Quantos digrafos simples auto-complementares com n vértices existem?

Seja $S_n^{(2)}$ o grupo de permutações dos $n(n-1)$ pares ordenados distintos nos símbolos $1,2,\ldots,n$ induzidos pelo grupo simétrico S_n. Um digrafo simples é um grafo com as arestas dirigidas (setas) sem laços e com no máximo uma seta ligando cada par ordenado de vértices. O complemento de um digrafo simples é conseguido colocando-se setas onde não existem e retirando-as de onde existem. Uma aplicação direta do corolário (V.4.b) nos diz que existem

$$Y_{S_n^{(2)}}(2,2,\ldots,2)$$

digrafos simples. Pelo teorema (V.8.b) o número de digrafos simples auto-complementares vale

$$Y_{S_n^{(2)}}(0,2,0,2,\ldots).$$

Ilustramos agora a situação considerando n=4. No exercício 21 deste capítulo, pedimos uma comprovação de que

$$Y_{S_4^{(2)}}(x_1,x_2,\ldots,x_{12}) =$$

$$\frac{1}{24}(x_1^{12} + 6x_1^2x_2^5 + 8x_3^4 + 3x_2^6 + 6x_4^3).$$

Assim, o número de digrafos simples auto-complementares com 4 vértices é

$$\frac{1}{24}(0 + 0 + 0 + 3 \times 2^6 + 6 \times 2^3) = 10.$$

Uma tabela dos números a_n' de digrafos simples auto-complementares com n vértices começa com

n	a_n'
2	1
3	4
4	10
5	136
6	720
7	44224
8	703760

Observe, comparando com os a_n's da tabela análoga para grafos, que $a_n' = a_{2n}$ para n=2 e 4. Na realidade em [RE 1] Read provou o fato curioso que para $n \geq 1$,

$$a_{2n}' = a_{4n},$$

isto é, o número de digrafos simples com 2n vértices que são

auto-complementares é igual ao número de grafos simples auto-complementares com 4n vértices. É interessante notar que uma bijeção explícita entre as duas classes de objetos não é conhecida.

Outra aplicação do teorema (V.8.b) é feita na próxima seção para enumerar funções booleanas auto-complementares.

V.9 - CONTANDO FUNÇÕES BOOLEANAS

Uma função booleana em n variáveis é definida como uma função de todas as seqüências nos símbolos 0 e 1 de comprimento n em $\{0,1\}$. Em alguns problemas concernentes a circuitos lógicos é conveniente se considerar duas funções booleanas como equivalentes se uma é obtida a partir da outra por uma permutação das variáveis seguida da negação de um subconjunto das mesmas. Por exemplo, com os símbolos usuais $\vee$ (para "ou"), $\wedge$ (para "e") e $\sim$ (para negação) temos que as funções

$$(x_1,x_2,x_3,x_4) \longrightarrow x_1 \vee (x_2 \wedge \sim x_3) \vee (x_4 \wedge \sim x_1)$$

$$(x_1,x_2,x_3,x_4) \longrightarrow \sim x_2 \vee (x_1 \wedge \sim x_4) \vee (\sim x_3 \wedge x_2)$$

são, com a definição acima, equivalentes pois a segunda é obtida da primeira pela permutação

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_4 & x_3 \end{pmatrix}$$

seguida da negação de x_2 e de x_3.

O nosso problema nesta seção é o de enumerar as funções booleanas módulo a equivalência acima. Este problema foi tratado originalmente por Slepian em [SL 1].

Uma função booleana em n-variáveis pode ser pensada como uma coloração dos vértices do n-cubo com duas cores. Pode ser mostrado que a equivalência de funções booleanas acima definida equivale à congruência das duas 2-colorações via rotação e reflexão do n-cubo. Este fato básico é intuitivo e pode ser verificado diretamente em dimensões 2 e 3 e se generaliza para dimensões maiores. Assumimos o mesmo sem nos determos numa prova formal.

Desse modo o número de funções booleanas em n variáveis procurado, é o número de 2-colorações dos vértices do n-cubo módulo o grupo de simetrias deste. Podemos aplicar a teoria de Polya desde que conheçamos o índice de ciclos do grupo de si-

metrias do n-cubo como permutação de vértices. É fácil, construindo um prefab exponencial, obter uma recorrência simples para os índices de ciclos dos grupos de simetrias do n-cubo, porém como permutações de faces. Na realidade é possível obter polinômios que contêm mais informação que os índices de ciclos (das faces). Informação adicional esta que nos permite obter dos mesmos os índices de ciclos do grupo de simetrias do n-cubo como permutações de vértices.

PREFAB NAS PERMUTAÇÕES DE FACES DO N-CUBO

Considere um n-cubo com as faces rotuladas pelos elementos do conjunto

$$R_n = \{1,\bar{1},2,\bar{2},\ldots,n,\bar{n}\},$$

onde i e $\bar{i}$ rotulam (hiper-) faces opostas ($\bar{\bar{i}} = i$). É fácil se observar que uma permutação ρ de R_n é induzida por uma simetria do n-cubo se e somente se $\rho(\bar{i}) = \overline{\rho(i)}$, para $i \in R_n$, isto é, a imagem da face oposta é a face oposta da imagem. Claramente existem $2^n n!$ tais permutações.

Construimos um prefab $(\Omega,\star,\kappa,\pi)$ da seguinte maneira.

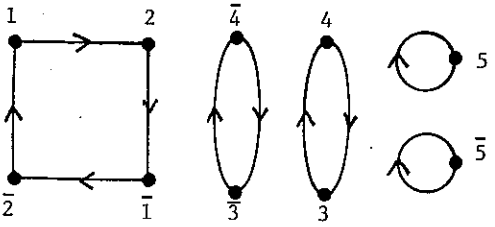
(i) $\Omega = \bigcup_{n\geq 0} \Omega_n$, onde Ω_0 é o elemento neutro que pode ser pensado como o polígono vazio. Para $n\geq 1$ Ω_n é o conjunto das permutações ρ de R_n satisfazendo

$$\rho(\bar{i}) = \overline{\rho(i)}.$$

As permutações em Ω_n são representadas pelos polígonos rotulados dirigidos associados à sua decomposição em ciclos disjuntos. Por exemplo, se $\alpha \in \Omega_5$ vale

$$(1,2,\bar{1},\bar{2})\ (3,\bar{4})\ (\bar{3},4)\ (5)\ (\bar{5}),$$

α é representada por



(ii) A composição $*$ é essencialmente a composição de dígrafos rotulados: se $\alpha \in \Omega_m$, $\beta \in \Omega_n$ então, $\alpha * \beta$ é o subconjunto de Ω_{m+n} definido como segue. Um elemento γ de Ω_{m+n} está em $\alpha * \beta$, se é possível encontrar uma partição (A,B) de $N = \{1,2,\ldots,n\}$ tal que γ é obtido a partir da união das componentes de α e de β trocando-se os rótulos i e $\bar{i}$ de α por i'_A e $\bar{i}'_A$ respectivamente, onde i'_A é o i-ésimo menor elemento de A, seguida por troca análoga para o rótulo dos polígonos em β com B no lugar de A.

(iii) A função corretiva κ é definida para $\alpha \in \Omega_n$ como $\kappa(\alpha) = 2^n\, n!$

(iv) Definimos a função peso π no conjunto de primos P e extendenmo-la para torná-la totalmente multiplicativa, isto é se $\alpha \in p_1^{k_1} * p_2^{k_2} * \ldots * p_n^{k_n}$ (p_i's distintos) então

$$\pi(\alpha) = \prod_{i=1}^{n} (\pi(p_i))^{k_i}.$$

Para identificar os primos de Ω, precisamos considerar os polígonos desse conjunto. Podemos distinguir dois tipos de polígonos: *polígonos de tipo 1* são aqueles em que para algum $i \in N$, i e $\bar{i}$ aparecem rotulando dois de seus vértices. Pela restrição de que a imagem da face oposta é a face oposta da imagem é fácil de concluir que em polígonos do tipo 1, se j aparece, então $\bar{j}$ tam-

bém aparece rotulando o vértice oposto. *Polígonos de tipo 2* são aqueles em que i e $\bar{i}$ não aparecem simultaneamente como rótulos. Pela restrição acima, se os vértices de um polígono de tipo 2 aparecem em ordem cíclica rotulados por $(i_1,i_2,\ldots,i_n)$, então a mesma permutação que induz tal polígono induz também o polígono disjunto rotulado em ordem cíclica por $(\bar{i}_1,\bar{i}_2,\ldots,\bar{i}_n)$.

É agora uma observação simples que os primos em Ω correspondem aos polígonos do tipo 1, chamados *primos de tipo 1*, e aos pares de polígono de tipo 2, que são os *primos de tipo 2*. Definimos os pesos respectivos como

$$\pi(\alpha) = z^n y_{2n} \quad \text{se} \quad \alpha \in \Omega_n \quad \text{e é primo de tipo 1}$$

$$\pi(\alpha) = z^n x_n^2 \quad \text{se} \quad \alpha \in \Omega_n \quad \text{e é primo de tipo 2.}$$

Tendo definido a estrutura $(\Omega,*,\kappa,\omega)$ deixamos para o leitor a verificação (que é direta porém tediosa) de que trata-se de um prefab exponencial. O inventário do conjunto P de primos é

$$\mathrm{Inv}_{\kappa,\pi}(P) = \sum_{p \in P} \frac{\pi(p)}{\kappa(p)}$$

$$= \sum_{m \geq 1} 2^{m-1}(m-1)! \left(\frac{x_m^2}{2^m m!} + \frac{y_{2m}}{2^m m!} \right) z^m,$$

uma vez que existem $2^{m-1}(m-1)!$ primos em Ω_m de tipo 1 e outros tantos de tipo 2. Usando agora o teorema exponencial obtemos

$$\mathrm{Inv}_{\kappa,\pi}(\Omega) = \exp\left(\frac{1}{2m} \sum_{m \geq 1} (x_m^2 + y_{2m}) \right) z^m .$$

O uso de duas variáveis x e y foi motivado pelo propósito de guardar informação sobre os tipos de permutações de faces. Esta informação é imprescindível para o cálculo do índice de ciclos do grupo de simetrias do n-cubo como permutações de vértices. Se es-

tivermos interessados no índice de ciclos das faces, podemos obtê-lo fazendo $y_{2i} = x_{2i}$ para todo $i \in N$. Temos o seguinte teorema cuja prova a partir da expressão para o inventário acima é uma simples verificação de definições, que deixamos a cargo do leitor.

(V.9.a) TEOREMA: O índice de ciclos do grupo de permutações das faces de um n-cubo induzidas pelo seu grupo de simetrias é

$$Y_{Q_n^f} = \left[z^n\right]\left\{ \exp\left[\frac{1}{2m}\sum_{m\geq 1}(x_m^2 + x_{2m})\, z^m\right]\right\}. \square$$

A fórmula para o inventário de Ω permite a construção de uma recorrência simples para o cálculo dos coeficientes de z^n. Seja $f(z) = \mathrm{Inv}_{K,\pi}(\Omega)$. Usando a expressão obtida acima obtemos depois de derivar, a seguinte equação funcional

$$zf'(z) = \frac{1}{2m} f(z) \sum_{m\geq} (x_m^2 + y_{2m})\, {}^{-m}.$$

Se denotarmos por c_n o valor de

$$\left[z^n\right]\{f(z)\}$$

obtemos após comparação de coeficientes a seguinte recorrência.

$$c_0 = 1$$

$$c_m = \frac{1}{2m}\sum_{i=0}^{m-1} c_i (x_{m-1}^2 + y_{2m-2i}).$$

Dessa recorrência obtemos facilmente

$$c_0 = 1$$

$$c_1 = \frac{1}{2}(x^2 + y_2)$$

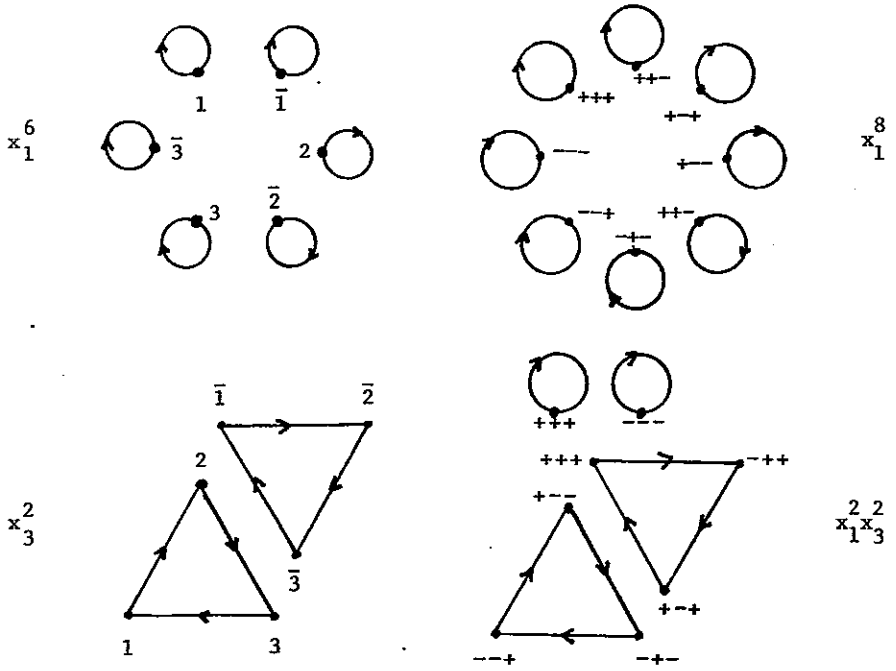
$$c_2 = \frac{1}{8}\,(2x_2^2 + 2y_4 + x_1^4 + 2x_1^2y_2 + y_2^2)$$

$$c_3 = \frac{1}{48}\,(x_1^6 + 8x_3^2 + 8y_6 + 6x_1^2x_2^2 + 6x_1^2y_4 +$$

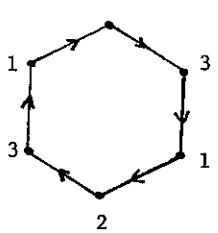
$$6x_2^2y_2 + 6y_2y_4 + 3x_1^4y_2 + 3x_1^2y_2^2 + y_2^3).$$

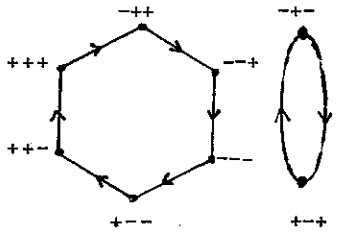
Como mencionamos, para enumerar as funções booleanas, precisamos do índice de ciclo do grupo de permutações de vértices do n-cubo induzidos pelas simetrias do mesmo. Vamos agora exemplificar para n=3 como obter este índice de ciclos a partir de c_n, coeficiente de z^n em $\mathrm{Inv}_{K,\omega}(\Omega)$. A idéia é fazer a correspondência entre as permutações de faces e as permutações de vértices, de maneira análoga à que foi feita no caso do grupo simétrico atuando em símbolos e em pares de símbolos, para a enumeração de grafos.

As seguintes correspondências são facilmente encontradas:



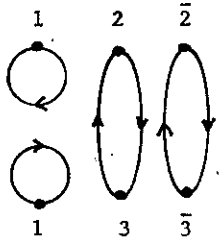
y^6

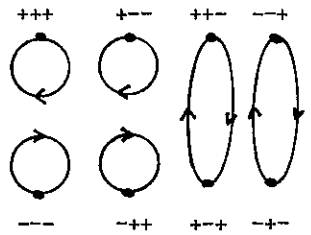




x_2x_6

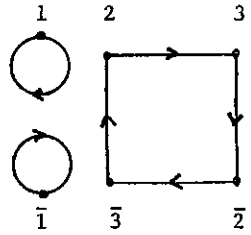
$x_1^2y^4$

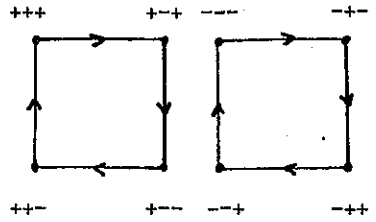




x_4^2

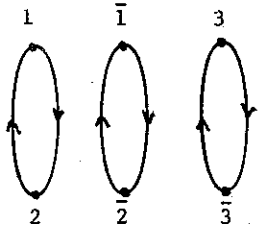
$x_1^2y_4$

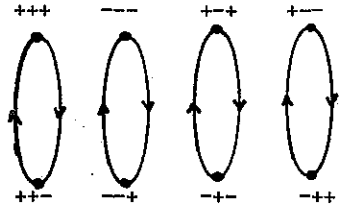




x_4^2

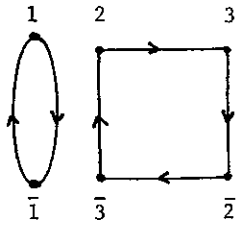
$x_2^2y_2$

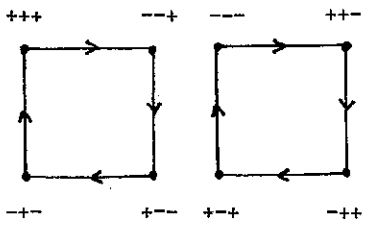




x_2^4

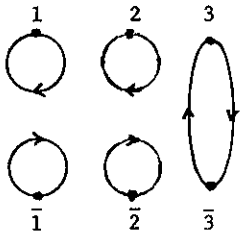
$y_2 y^4$

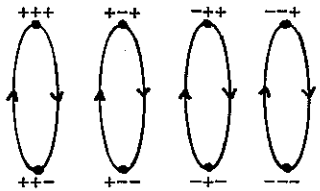




x_4^2

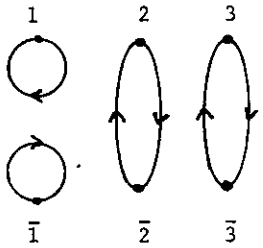
$x_1^4 y_2$

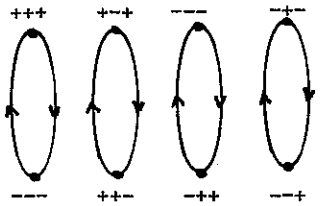




x_2^4

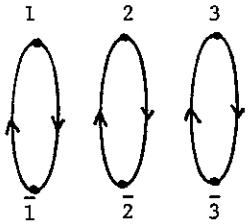
$x_1^2 y_2^2$

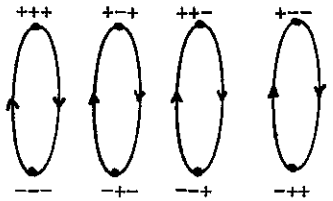




x_2^4

y_2^3





x_2^4

Levando em conta os coeficientes vemos assim que o índice de ciclos procurado $Y^{V}_{Q_3}$ vale

$$Y_{Q^{V}_{3}} = \frac{1}{48}\,(x_1^8 + 13x_2^4 + 8x_1^2x_3^2 + 8x_2x_6 + 6x_1^4x_2^2 + 12x_4^2).$$

De maneira análoga, poderíamos mostrar que

$$Y_{Q^{V}_{4}} = \frac{1}{384}\,(x_1^{16} + 51x_2^8 + 48x_1^2x_2x_4^3 + 48x_8^2 +$$

$$+ 12x_1^8x_2^4 + 84x_4^4 + 12x_1^4x_2^6 + 32x_1^4x_3^4 + 96x_2^2x_6^2).$$

(V.9.b) EXEMPLO: Quantas Q^{V}_{3} - classes de funções booleanas em 3 variáveis existem tendo na imagem 4 valores iguais a 1?

Associemos ao 0 da imagem das funções booleanas o peso $x^0=1$ e ao 1 o peso $x^1=x$. Pelo teorema de Polya (V.4.a) o número procurado é

$$\frac{1}{48}\left[x^4\right]\{(1+x)^8 + 13(1+x^2)^4 + 8(1+x)^2\,(1+x^3)^2$$

$$+ 8(1+x^2)\,(1+x^6) + 6(1+x)^4\,(1+x^2)^2 + 12(1+x^4)^2\}$$

$$= \frac{1}{48}\left[\binom{8}{4} + 13.\,\binom{4}{2} + 8.2.2\right.$$

$$\left. + 6\left[1 + \binom{4}{2}\,.\,2 + 1\right] + 12.2\right]$$

$$= \frac{1}{48}\,(70 + 78 + 32 + 84 + 24)$$

$$= \frac{288}{48} = 6$$

Q^{V}_{3} - classes de funções booleanas.

(V.9.c) EXEMPLO: Quantas Q^{V}_{3} - classes auto-complementares de funções booleanas em 3 variáveis existem? Uma função booleana f em n variáveis é *auto-complementar* se a função g obtida de f

trocando os valores da imagem desta última está na mesma Q_n^v - classe uma Q_n^v - classe é *auto-complementar* se suas funções constituintes são auto-complementares. Pelo teorema (V.8.b) para se obter o número requerido basta substituir em $\gamma_{Q_3^v}$ as variáveis de índice ímpar por 0 e as variáveis de índice par por 2. Assim existem

$$\frac{1}{48}\,(0 + 13.2^4 + 12.2^2 + 0 + 8.2.2) =$$

$$= \frac{528}{48}$$

$$= 11$$

Q_3^v - classes auto-complementares de funções booleanas em 3 variáveis.

EXERCÍCIOS

1. Mostre que o índice de ciclos do grupo de rotações do tetraedro regular como permutações de faces é

$$\frac{1}{12}\,(x_1^4 + 8x_1x_3 + 3x_1^2).$$

   E como permutações de vértices?

2. Calcule o índice de ciclos do grupo de simetrias total (rotações e reflexões) do tetraedro regular como permutações de faces. Compare sua resposta com o valor de γ_4 dado após o corolário (III.4.k). A relação obtida é natural?

3. Comprove que os índices de ciclos do grupo de rotações do icosaedro regular são

   (i) como permutações de faces

$$\frac{1}{60}\,(x_1^{20} + 20x_1^2x_3^6 + 24x_5^4 + 15x_2^{10})$$

   (ii) como permutações de vértices

$$\frac{1}{60}\,(x_1^{12} + 20x_3^4 + 24x_1^2x_5^2 + 15x_2^6)$$

Em seguida calcule os índices de ciclos incluindo além das rotações as reflexões, obtendo assim o grupo de simetrias total.

4. Seja c_n o grupo cíclico em n elementos representados por permutações da maneira usual. Prove que

$$Y_{c_n}(x_1,x_2,\ldots,x_n) = \frac{1}{n}\sum_{d|n}\phi(n)\,x_d^{n/d},$$

onde ϕ é a função totiente de Euler.

5. Seja D_n o grupo diedral em n elementos representados por permutações de maneira usual. Prove que

$$Y_{D_n}(x_1,x_2,\ldots,x_n) = \frac{1}{2}\,Y_{C_n}(x_1,x_2,\ldots,x_n) + \begin{cases} \frac{1}{2}\,x_1\,x_2^{\frac{n-1}{2}}, & n \text{ ímpar} \\ \frac{1}{4}\left(x_2^{\frac{n}{2}} + x_1^2\,x_2^{\frac{n-2}{2}}\right), & n \text{ par} \end{cases}$$

6. As 6 faces de um cubo devem ser pintadas com no máximo 5 cores. De quantas maneiras a menos de rotação isto pode ser feito? Suponha que uma das cores é azul. Em quantas das colorações possíveis existem 3 faces azuis?
(Sugestão: para resolver à segunda questão dê à cor azul o peso $\pi(\text{azul})=x$ e às outras o peso y. O inventário do contradomínio é então $x + 4y$. Procure pelo coeficiente de x^3y^3 em $\text{Inv}_\pi(C^D \bmod G)$.)

7. Quantas colorações em duas cores das faces e dos vértices de um icosaedro regular existem nas quais cada uma das duas cores aparece o mesmo número de vezes?

(Sugestão: os índices de ciclos apropriados são dados no exercício 3 acima).

8. Prove que existem exatamente 3 colorações dos vértices de um octaedro regular nas quais 3 vértices são pintados com verde, 2 são pintados com azul e 1 é pintado com vermelho.

9. Prove que existem exatamente 5 colorações das faces de um dodecaedro regular nas quais 9 faces são pintadas com verde, 2 são pintadas com azul e 1 é pintada com vermelho.

10. Encontre um polinômio p tal que p(n) é igual ao número de maneiras distintas, a menos de rotação e reflexão, de pintarmos as arestas de um tetraedro regular com no máximo n cores uma das quais é verde. Em quantas destas colorações existem precisamente 4 arestas pintadas de verde?

11. Seja $f_5(x) = Y_{S_5\{2\}}(1+x, 1+x^2+,\ldots,1+x^{10})$. Desenhe os 6 grafos com 5 vértices e 5 arestas "previstos" por $f_5(x)$. (Este polinômio é dado explícitamente no texto.)

12. Existem alguma explicação simples para o fato de $f_5(x)$, acima, ser simétrico, isto é, ter os coeficientes de x^i e de x^{10-i} iguais para $0 \leq i \leq 10$? Mostre que se $f_n(x)$ é a função geradora, por arestas, para os grafos simples com n vértices então $[x^i]$ $f_n(x)$ e $\left[x^{\binom{n}{2}-i}\right]$ $f_n(x)$ são iguais para $0 \leq i \leq \binom{n}{2}$.

13. Prove que o número $g_k(n,m)$ de grafos com n vértices, m arestas com no máximo k arestas ligando 2 vértices é

$$g_k(n,m) = \left[x^m\right]\left\{Y_{S_n\{2\}}\left(\sum_{i=0}^{k} x^i\ ,\ \sum_{i=0}^{k} x^{2i},\ldots,\sum_{i=0}^{k} x^{\binom{n}{2}i}\right)\right\}$$

e também que

$$\sum_{m=0}^{k\binom{n}{2}} g_k(n,m) = Y_{S_n\{2\}}(k+1,\ k+1,\ldots,k+1).$$

14. Com a notação do exercício anterior calcule explicitamente $g_2(4,m)$ para m entre 0 e 12. Tente desenhar para m=7 os grafos correspondentes.

15. Mostre que o número $g_*(n,m)$ com n vértices, m arestas e sem limite para o número de arestas ligando 2 vértices é

$$g_*(n,m) = \left[x^m\right]\left\{Y_{S_n^{\{2\}}}\left(\frac{1}{1-x}, \frac{1}{1-x^2}, \ldots, \frac{1}{1-x^{\binom{n}{2}}}\right)\right\}$$

(Observe que o contradomínio C neste problema não é finito e isto justifica porque não fazemos esta restrição.)

16. Calcule, usando o índice de ciclos de $S_5^{\{2\}}$ fornecido no texto, o valor de $g_*(5,5)$. Verifique sua resposta desenhando os grafos.

17. Encontre o grupo de permutações adequado para responder à seguinte pergunta: Quantos grafos com n vértices, m arestas e no máximo k arestas ligando 2 vértices existem, se laços são permitidos.

18. Prove que $Y_{S_6^{\{2\}}}(x_1,x_2,\ldots,x_{15}) =$

$$\frac{1}{6!}(x_1^{15} + 15x_1^7x_4^2 + 40x_1^3x_3^4 + 45x_1^3x_2^6 + 90x_1x_2x_4^3 + 120x_1x_2x_3^2x_6 +$$

$$+ 144x_5^3 + 15x_1^3x_2^6 + 90x_1x_2x_4^3 + 40x_3^5 + 120x_3x_6^2).$$

19. Damos a seguir o começo de uma tabela dos número g(n,m) de grafos simples com n vértices e m arestas. A tarefa do leitor é se convencer de que seria capaz de gerar esta tabela a partir da teoria desenvolvida no texto

n/m	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1												
2	1	1											
3	1	1	1	1									
4	1	1	2	3	2	1	1						
5	1	1	2	4	6	6	6	4	2	1	1		
6	1	1	2	5	9	15	21	24	24	21	15	9	5
7	1	1	2	5	10	21	41	65	97	131	148	148	131
8	1	1	2	5	11	24	56	115	221	402	663	980	1312
9	1	1	2	5	11	25	63	148	345	771	1637	3252	5992

20. Seja $S_n^{(2)}$ o grupo de permutações dos $n(n-1)$ pares ordenados distintos nos símbolos $1,2,\ldots,n$ induzidos por S_n. Mostre que

$$Y_{S_4^{(2)}}(x_1,x_2,\ldots,x_{12}) = \frac{1}{24}\,(x_1^{12} + 6x_1^2x_2^5 + 8x_3^4 + 3x_2^6 + 6x_4^3).$$

21. Prove que o número $d(n,m)$ de digrafos simples (grafos dirigidos, sem laços e com no máximo uma seta ligando cada par ordenado de vértices) com n vértices e m setas é

$$d(n,m) = \left[x^m\right]\left\{Y_{S_n^{(2)}}\left((1+x,\ 1+x^2,\ldots,1+x^{n(n-1)}\right)\right\}.$$

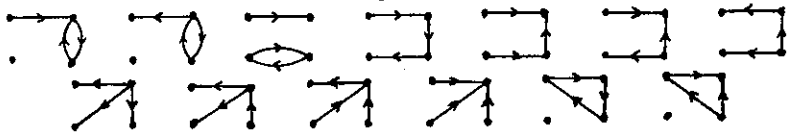
22. Usando o resultado do exercício 14 verifique que

$$Y_{S_4^{(2)}}(x_1,\ldots,x_{12})$$

é

$$1+x+5x^2+13x^3+27x^4+38x^5+48x^6+38x^7+27x^8+13x^9+5x^{10}+x^{11}+x^{12}$$

Como "previstos" neste polinômio existem 13 digrafos simples com 4 vértices e 3 setas, apresentados abaixo:



Prove que você tem "fé" nesta teoria exibindo os 27 digrafos simples com 4 vértices e 8 setas previstos pelo mesmo polinômio.

23. Para leitores hábeis em programação de computadores: escreva um programa que calcule

$$Y_{S_n}(x_1,x_2,\ldots,x_n)$$

$$Y_{S_n^{\{2\}}}(x_1,x_2,\ldots,x_{\binom{n}{2}})$$

$$Y_{S_n^{(2)}}(x_1,x_2,\ldots,x_{n(n-1)})$$

para $n=2,2,\ldots,15$.

24. Utilizando idéias análogas às da prova do teorema (V.7.a) prove que o número de G×H-padrões injetivos em C^D é

$$\mathrm{Inj}(C^D \bmod (G\times H)) = Y_G\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2},\ldots,\frac{\partial}{\partial x_{|D|}}\right) \left\{ Y_H\left(1+x_1,\ 1+2x_2+\ldots,1+|C|x_{|C|}\right)\right\}$$

avaliado em $x_1=x_2=\ldots=x_{|C|}=0$.

25. Particularize o exercício anterior mostrando que se $|D|=|C|=n$ então o número de G×H-padrões bijetivos é

$$\mathrm{Bij}(C^D \bmod (G\times H)) = Y_G\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2},\ldots,\frac{\partial}{\partial x_n}\right) \left\{ Y_H(x_1,\ 2x_2,\ldots,nx_n)\right\}.$$

Note em particular que esta expressão é um polinômio constante. Prove também pela simetria do caso que

$$Y_H\left(\frac{\partial}{\partial x_1}, \frac{\partial}{\partial x_2},\ldots,\frac{\partial}{\partial x_n}\right) \left\{ Y_G(x_1,\ 2x_2,\ldots,nx_n)\right\}$$

é também igual a $Bij(C^D \bmod (G \times H))$.

26. Mostre que o número de maneiras distintas de se rotular ciclicamente as faces de um dado com $\{1,2,3,4,5,6\}$, onde duas rotulações são iguais se uma pode ser transformada na outra por rotação do cubo e permutação cíclica dos rótulos, é 9. Faça uma figura mostrando estas 9 rotulações cíclicas.

27. Dê uma explicação simples para o fato de a_2, a_3, a_6, a_7, a_{10}, a_{11}, a_{14}, a_{15} na tabela que segue o exemplo (V.8.c) serem todos iguais a zero.

28. No exemplo (V.7.8) mostramos que existem 10 digrafos simples auto-complementares. Desenhe estes 10 digrafos.

29. Calcule quantas classes auto-complementares de funções booleanas em 4 variáveis existem. Use o índice de ciclos dado no texto.

30. De quantas maneiras podemos pintar as faces de um 3-cubo com no máximo 3 cores

    a) a menos de rotação?

    b) a menos de rotação e reflexão?

A resposta para (a) é 57 e a resposta para (b) é 56. Isto significa que existe exatamente uma 3-coloração das faces do cubo usual que não é superponível com sua imagem especular por rotação. Encontre tal 3-coloração.

REFERÊNCIAS

[AB1] Abramowitz, M. (ed), *Handbook of Mathematical Functions*, Dover (1972).

[AH1] Ahu, Hopcroft Ullman, *The Design and Analysis of Computer Algorithms*, Addinson - Wesley (1975).

[AI1] Aigner, Martin, *Combinatorial Theory*, Springer Verlag (1979).

[BG1] Bender E.A, Goldman, J.R., *Enumerative Uses of Generating Functions*, Indiana Univ. Math. J. 20(1971) 753-765.

[BE1] Berge, C., *Principles of Combinatorics*, Academic Press (1971).

[BM1] Birkhoff, G., Maclane S., *A Survey of Modern Algebra*, Macmillan (1977) - (4ª edição).

[BR1] Brualdi, R., *Introductory Combinatorics*, North Holland (1977).

[BU1] Burnside, W., *Theory of Groups of Finite Order*, Cambridge Univ. Press (1911).

[CA1] Cayley, A., *A Theorem on Trees*, Quart. J. Math. 23, (1889) 376-378.

[CO1] Cori R., *Graphes Planaires et Systèmes de Parenthèses*, Thèse de 3 ème cycle, Paris, (1969).

[DB1] De Brujin, N.G., *Generalization of Polya's Fundamental Theorem in Enumerative Combinatorial Analysis*, Indag. Math. 21 (1956) 59-79.

[DB2] De Brujin, N.G., *Polya's Theory of Counting*, Applied Combinatorial Mathematics (E.F. Beckenbach, ed) 144-184 Wiley (1964).

[DE1] Deo, Narsingh, *Graph Theory with Applications to Engineering and Computer Science*, Prentice Hall (1974).

[GO1] Godement, Roger, *Algebra*, Hermann - (1968).

[GO2] Gonçalves, Adilson, *Introdução à Algebra*, Projeto Euclides (1979).

[HA1] Hall, M., *Combinatorial Theory*, Blaisdell (1967).

[HA1] Harary, F., *Graph Theory Addinson*, Wesley (1969).

[HK1] Hoffman K., Kunze, R., *Linear Algebra*, Prentice Hall (1971).

[HO1] Honsberger, R., *Mimeographed Notes*, University of Waterloo (1979).

[HP1] Harary, F., Palmer, E.M., *Graphical Enumeration*, Academic Press. (1973).

[JA1] Jackson, D.M., *Mimeographed Lecture Notes*, University of Watertoo (1978).

[JG1] Jackson, Goulden, I.R., *The Combinatorics of the Ordinary Generating Function*, a ser publicado pela Academic Press (1981).

[KA1] Kaplanski, I., *Solution of the "Problème de Ménages"*, Bull. Amer. Math. Soc. 49 784-785 (1943).

[KN1] Knuth, D., *The Art of Computer Programming, vol 1 Fundamental Algorithms*, Addinson-Wesley (1975).

[KN2] Knuth, D., *The Art of Computer Programming vol 2 Seminumerical Algorithms*, Addinson-Wesley (1975).

[KN3] Knuth D., *The Art of Computer Programming vol 3 Sorting and Searching*, Addinson-Wesley (1975).

[KR1] Kruskal, J.B., *On the Shortest Spanning Subtree of a Graph.* Proc. Amer. Math. Soc. 7, (1956), pg 48.

[LI1] Liu, C.L., *Introduction to Combinatorial Mathematics,* McGraw-Hill (1968).

[LO1] Lovãsz, L., *Combinatorial Problems and* Exercises, North Holland (1979).

[ME1] Meyer, P.L., *Probabilidade e Aplicações à Estatística,* Ao Livro Técnico (1970).

[MO1] Moise, E., *Elements of Calculus,* Addinson Wesley (1972).

[NW1] Nijenhuis, A., Wilf, H.S., *Combinatorial Algorithms,* Academic Press (1978).

[OT1] Otter, R., *The Number of Trees,* Ann. of Math. 49(1948) 583-599.

[PO1] Polya, G., *Kombinatorische Anzahlbestimmungen für Gruppen, Graphen, und Chemische Verbindungen,* Acta. Math. 68 (1937) 145-254.

[RE1] Read, R., *On the number of Self-Complementar Graphs and Digraphs,* J. London Math. Soc. 38 99-104 (1963).

[RI1] Riordan, J., *An Introduction to Combinatorial Analysis,* John Wyley (1958).

[SL1] Slepian, D., *On the Number of Symmetry Types of Boolean Functions,* Canad. Jour. Math. 5, 185-193 (1953).

[TO1] Touchard, J., *Sur un Problème de Permutations,* C.R Acad. Sci. 198, 631-633 (1943).

[TU1] Tutte, W.T., *The Enumerative Theory of Planar Maps. J. N. Srivastava et al. (eds) A Survey of Combinatorial Theory,* North Holland (1973).

[TU2] Tutte, W.T., *On the Elementary Calculus and the Good Formula*, Journ. Comb. Theory, vol 18, (1975).