CÓDIGOS CORRETORES DE ERROS

JOSÉ FELIPE VOLOCH

COPYRIGHT © by JOSÉ FELIPE VOLOCH

Nenhuma parte deste livro pode ser reproduzida,
por qualquer processo, sem a permissão do autor.

MINISTÉRIO DA CIÊNCIA E TECNOLOGIA
CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO
INSTITUTO DE MATEMÁTICA PURA E APLICADA
Estrada Dona Castorina, 110
22.460 — Rio de Janeiro — RJ

INTRODUÇÃO

Desde a sua introdução por Claude Shannon (um matemático que trabalhava no Bell Lab.) a teoria de códigos corretores de erros tem tido inúmeras aplicações. Ela intervem todas as vezes que queremos transmitir ou estocar mensagens ou dados que estão sujeitos a interferência que causem erros na mensagem a ser lida posteriormente. Exemplos usuais são as transmissões por satélite e a estocagem de dados em fitas magnéticas de computadores.

O problema que se põe é: dada uma mensagem recebida que contem um número de erros, como corrigir estes erros e recuperar a mensagem enviada? Se a mensagem enviada contem redundâncias então, se a quantidade de erros é pequena, podemos esperar recuperar a mensagem. Essa é a filosofia dos códigos corretores de erros. No aspecto prático da coisa a percentagem de erros na mensagem é conhecida (por experiência, por exemplo) pois o canal de comunicação é dado. Por outro lado a quantidade de redundância que podemos colocar é limitada pelos gastos que queremos fazer.

Vamos dar um exemplo específico. Suponhamos que queremos enviar mensagens (a,b,c) com $a,b,c \in \{0,1\}$ e digamos que o nosso canal de comunicações causa um erro em cada seis

digitos consecutivos. Então se enviarmos a mensagem pura e simples o receptor vai receber uma mensagem errada a cada duas enviadas. Isso é ruim. Outra tentativa é repetir cada mensagem, introduzindo redundância. Isso também é ruim pois se o receptor recebe por exemplo $(a,b,c)(a',b,c)$ $a \neq a'$, como ele vai saber se o primeiro digito da mensagem é a ou a'? (Que os outros dois são b,c, ele já sabe, pois vieram repetidos). Se repetirmos a mensagem três vezes então certamente o receptor saberá qual é a mensagem (verifique). Para isso tivemos que introduzir seis digitos redundantes em cada mensagem. Daremos agora um exemplo de como podemos mandar nossa mensagem corretamente enviando apenas três digitos redundantes.

Dada a mensagem (a,b,c) enviamos a mensagem $(a,b,c,a+b,a+c,b+c)$. Aqui a soma é a soma "módulo 2", isto é, $0+0 = 0$, $0+1 = 1$, $1+0 = 1$, $1+1 = 0$. Vamos então mostrar que podemos recuperar a mensagem.

Suponha que o receptor recebe $(r_1,r_2,r_3,r_4,r_5,r_6)$ e ele já sabe que há um único erro. Ele procede do seguinte modo. Calcula r_1+r_2. Se $r_1+r_2 = r_4$ então r_1,r_2,r_4 estão corretos, logo $a=r_1$, $b=r_2$ e c é o digito que ocorrer duas vezes em r_3, r_5+a, r_6+b. Se $r_1+r_2 \neq r_4$ um dos três está errado, logo r_3,r_5,r_6 estão certos. Logo $c=r_3$, $a=r_3+r_5$, $b=r_3+r_6$. Em ambos os casos o receptor recuperou a,b,c.

A aritmética modulo 2 nos ajudou muito no exemplo acima. Isso é um fenomeno usual, os melhores códigos proveem de objetos com estrutura, por isso é bastante conveniente usar os

corpos finitos (para uma referência completa aos corpos finitos ver [11]), o que faremos consistentemente no que segue. O nosso objetivo será mostrar como construir sistematicamente bons códigos corretores de erros e analisar sua "performance".

Os Capítulos I e II são básicos, neles introduzimos os conceitos e resultados que serão utilizados consistentemente no que segue. Os capítulos seguintes descrevem construções diversas de códigos e podem ser lidos independentemente uns dos outros.

Com a exceção do Capítulo VI, essas notas serão acessíveis a quem tiver conhecimento dos conceitos básicos de álgebra e álgebra linear normalmente vistos na graduação. Mais especificamente usaremos os conceitos de corpos, aneis e espaços vetoriais e suas propriedades básicas. O Capítulo VI, por outro lado, necessita de conhecimentos de geometria algébrica (como, por exemplo, [5]) para sua compreensão. Meu gosto pessoal me "forçou" a inclui-lo e espero que os leitores que tenham lido o resto dessas notas se sinta motivado a aprender o necessário para lê-lo.

O que me atrai na teoria dos códigos corretores de erros é como um problema, a princípio tão "aplicado", se relaciona intimamente com vários tópicos de matemática "pura" motivando novos problemas e novos resultados em ambos os lados. É essa interrelação que procurei ilustrar nestas notas. Essas notas não se propõem a ser nem um livro texto ([12] é ótimo) nem uma obra de referência ([15] é a "bíblia" do assunto). Meu objetivo

é apenas transmitir minha fascinação pelo assunto aos leitores e, quem sabe, motivá-los a serem usuários ou pesquisadores da teoria dos códigos.

Certamente, dado o tamanho do texto, muita coisa foi omitida. O leitor interessado deve então referir-se a bibliografia e, se não estiver satisfeito, consultar a bibliografia de [15]. Devemos mencionar a omissão total do importante aspecto probabilístico da teoria dos códigos o qual pode ser visto em [14]. Àqueles leitores que, por engano, acharam que íamos falar de criptografia, recomenda-se a consulta de [17].

Finalmente gostaria de agradecer a Elon Lima e Paulo Sad por insistirem que eu desse esse curso no Colóquio, a Lincoln de Souza por várias sugestões e a Rogério Trindade pela datilografia.

CAPÍTULO I

GENERALIDADES

Denotaremos por $\mathbb{F}_q$ o corpo finito com q elementos. Um <u>código</u> linear C sobre o alfabeto $\mathbb{F}_q$ é um subespaço vetorial de $\mathbb{F}_q^n$. Se d é a dimensão de C sobre $\mathbb{F}_q$ dizemos que C é um $[n,d]$-código.

Há varias maneiras de se descrever um código, podemos por exemplo, dar uma base $v_1,\ldots,v_d$ de C. Neste caso, se $v_i = (v_{i1},\ldots,v_{in})$ então a aplicação $V\colon \mathbb{F}_q^d \to \mathbb{F}_q^n$ dada por

$$V(a_1,\ldots,a_d) = \sum_{i=1}^{d} a_i v_i = \left(\sum_{i=1}^{d} a_i v_{i1},\ldots,\sum_{i=1}^{d} a_i v_{in}\right)$$

é um "codificador", isto é, pensando $\mathbb{F}_q^d$ como o conjunto das palavras numa linguagem "natural" a função V nos diz como codificar as palavras.

A matriz $V = (v_{ij})$ que descreve a aplicação linear V é chamada a <u>matriz geradora</u> do código. Diremos que V está na forma standard se $V = (I_d P)$ para uma matriz P, isto é, $v_{ij} = \delta_{ij}$ para $i,j = 1,\ldots,d$ (onde $\delta_{ij} = 0$, $i \neq j$, $\delta_{ii}=1$). Neste caso diremos que os primeiros d simbolos ou coordenadas de $c \in C$ são os simbolos de informação e os restantes os simbolos de controle.

Porque simbolos de controle? Dado um vetor $x=(x_1,\ldots,x_n) \in \mathbb{F}_q^n$ para checar se $x \in C$ basta verificar se $x = V(a)$ para algum a e neste caso (estamos supondo C standard) $x_j = a_j$, $j \leq d$ e $x_j = \sum_{i=1}^{d} a_i v_{ij} = \sum_{i=1}^{d} x_i v_{ij}$ para $j > d$. Logo, para checar se $x \in C$ basta verificar se $x_j = \sum_{i=1}^{d} x_i v_{ij}$, para $j = d+1,\ldots,n$.

Diremos que dois códigos C_1, C_2 são equivalentes se pudermos obter C_2 a partir de C_1 por permutação das coordenadas. Pode-se provar que todo código é equivalente a um código que pode ser gerado por uma matriz na forma standard (ver ex. 9).

Pelo que vimos acima a informação contida numa palavra $c \in C$ depende de d de suas coordenadas e o resto é redundância que é usada para controle. Definimos então a <u>razão de informação</u> de C, denotada por $i(C)$, como sendo $i(C) = d/n$ isso medirá então a razão entre o número de coordenadas "informativas" e o número total de coordenadas.

Outra maneira de descrever um código é dar uma aplicação linear sobrejetiva $H: \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$ tal que o núcleo de H é C. Neste caso temos $(x_1,\ldots,x_n) \in C$ se e só se $H(x_1,\ldots,x_n) = 0$. Se $H = (h_{ij})$ então a ultima equação se escreve

$$\sum_{j=1}^{n} h_{ij} x_j = 0, \qquad i = 1,\ldots,n-d.$$

A matriz H é então chamada de <u>matriz de controle de paridade</u> de C.

Se C é dado pela matriz geradora $(I_d P)$ como acima, isto é, C é standard, é fácil calcular a matriz de controle de C. De fato temos $x \in C$ se e só se $x_j = \sum_{i=1}^{d} x_i v_{ij}$, $j > d$ como vimos acima logo a matriz de controle é dada por $(-{}^t P\ I_{n-d})$ onde ${}^t P$ é a transposta de P.

Um exemplo ilustrativo, que origina o nome "controle de paridade" é o código de controle de paridade sobre $\mathbb{F}_2$ definido pela matriz geradora $(I_n 1)$ onde $1 = {}^t(1,\ldots,1)$, isto é, $C \subseteq \mathbb{F}_q^{n+1}$ dado por $\{(x_1,\ldots,x_n, x_1+\ldots+x_n) \mid (x_1,\ldots,x_n \in \mathbb{F}_q^n\}$. A matriz de controle de paridade de C é $(1,\ldots,1)$. É fácil ver então que $x \in C$ se e só se $\Sigma x_i = 0$ isto é, x tem um número par de coordenadas não nulas, daí o nome controle de paridade.

Falando em erros, mencionamos na introdução que os códigos seriam escolhidos de tal modo que duas palavras do código fossem sempre bem diferentes, para que quando recebesemos uma mensagem com possiveis erros pudessemos decodificá-la como a palavra no código mais parecida com a mensagem recebida. Para formalizar os conceitos de "diferente" e "parecido" definimos a <u>norma de Hamming</u> em $\mathbb{F}_q^n$ pondo para $x \in \mathbb{F}_q^n$, $|x|$ = número de coordenadas não nulas de x. Valem então as seguintes propriedades:

1) $|x| = 0$ se e só se $x = 0$

2) $|\lambda x| = |x|$ se $\lambda \in \mathbb{F}_q$, $\lambda \neq 0$

3) $|x+y| \leq |x|+|y|$

Definimos também a distância de Hamming pondo $d(x,y) = |x-y|$, que safisfaz

1') $d(x,y) = 0$ se e só se $x = y$

2') $d(x,y) = d(y,x)$

3') $d(x,z) \leq d(x,y)+d(y,z)$

Note que $d(x,y)$ é o número de coordenadas onde x e y diferem, logo $d(x,y)$ mede quão diferentes são x e y. d é uma métrica em $\mathbb{F}_q^n$.

Note que 1') segue de 1), 2') de 2) (com $\lambda=-1$) e 3') de 3). As propriedades 1) e 2) são imediatas. Provaremos agora a propriedade 3).

Seja $I = \{i \in \{1,\ldots,n\} \mid x_i = 0\}$ e $J = \{i \in \{1,\ldots,n\} \mid y_i = 0\}$ então, por definição $|x| = n-\#I$, $|y| = n-\#J$. Logo

$$|x|+|y| = 2n-(\#I+\#J).$$

Por outro lado, temos que $\#I+\#J = \#(I\cup J)+\#(I\cap J)$ e $\#(I\cup J) \leq n$, logo

$$|x|+|y| \geq n-\#(I\cap J).$$

Porém se $i \in I\cap J$, $x_i = y_i = 0$, logo $x_i+y_i = 0$. Então $x+y$ tem i-ésima coordenada nula para todo $i \in I\cap J$, consequentemente $|x+y| \leq n-\#(I\cap J)$. Isso conclui a demonstração.

Já podemos então medir quanto as palavras de um código diferem uma das outras. Definimos então o <u>peso de um código</u> C, denotado w(C) pondo $w(C) = \min\{d(x,y) \mid x,y \in C,\ x \neq y\}$. Como o código é um subespaço temos que $x-y \in C$ toda vez que $x,y \in C$, logo $w(C) = \min\{|x| \mid x \in C,\ x \neq 0\}$.

Podemos então passar a correção e detecção de erros. Dizemos que um código C <u>corrige e erros</u> se para todo $y \in \mathbb{F}_q^n$ existe no máximo um único $x \in C$ com $d(x,y) \leq e$. Isso significa que ao recebermos uma mensagem y com no máximo e erros, isto é, y difere de algum elemento de $x \in C$ no máximo em e coordenadas, esse elemento x sendo a mensagem enviada, então x é o único elemento de C tão próximo de y logo podemos recuperar x a partir de y. Mais adiante veremos como implementar esse procedimento. Agora vamos ver quantos erros um código pode corrigir.

(1.1) <u>Teorema</u>: Seja C um código de peso w(C) então C corrige $\left[\frac{w(C)-1}{2}\right]$ erros.

<u>Prova</u>: Seja $e = \left[\frac{w(C)-1}{2}\right]$ então $2e+1 \leq w(C)$. Suponha que C não corrija e erros e seja $y \in \mathbb{F}_q^n$ tal que existam $x_1, x_2 \in C$, $x_1 \neq x_2$ com $d(x_i,y) \leq e$, $i=1,2$. Por 3') temos $d(x_1,x_2) \leq d(x_1,y)+d(y,x_2) \leq 2e$. Por outro lado como $x_1 \neq x_2$, pela definição de w(C) temos $d(x_1,x_2) \geq w(C) \geq 2e+1$, contradição.

Um resultado util para se determinar $w(C)$ é o seguinte:

(1.2) Proposição: Seja C um código com matriz de controle H e peso $w(C)$. Então quaisquer $w(C)-1$ colunas de H são linearmente independentes e existem $w(C)$ colunas de H linearmente dependentes.

Prova: Seja s o inteiro tal que quaisquer s colunas de H são linearmente independentes e existem $s+1$ colunas de H linearmente dependentes.

Sejam $h_1,\ldots,h_n$ as colunas de H. Se $h_{i_1},\ldots,h_{i_{s+1}}$ são linearmente dependentes existem $c_{i_1},\ldots,c_{i_{s+1}} \in \mathbb{F}_q$ com $\Sigma c_{i_j} h_{i_j} = 0$. Seja $c = (c_1,\ldots,c_n)$ definido por $c_i = c_{i_j}$ se $i \in \{i_1,\ldots,i_{s+1}\}$, $c_i = 0$ caso contrário. Então $\Sigma c_i h_i$ 0 e $c \in C$, porém c tem no máximo $s+1$ coordenadas não nulas, logo $w(C) \leq s+1$.

Se $w(C) < s+1$ existe $c \in C$, $c \neq 0$, com no máximo s coordenadas não nulas, digamos $c_i = 0$ se $i \neq i_1,\ldots,i_s$. Como $c \in C$, $\sum_{i=1}^{n} c_i h_i = 0$, logo $\sum_{i=1}^{s} c_{i_j} h_{i_j} = 0$ logo $h_{i_1},\ldots,h_{i_s}$ são linearmente dependentes, isso contradiz a definição de s logo $w(C) = s+1$, como queriamos demonstrar.

(1.3) Corolário (Singleton): Se C é um $[n,d]$ código então $w(C) \leq n-d+1$.

Prova: Seja H matriz de controle de C. Como as colunas de

H estão em $\mathbb{F}_q^{n-d}$, quaisquer n-d+1 colunas de H são linearmente dependentes. O resultado agora segue da proposição.

Códigos com $w(C) = n-d+1$ são chamados códigos separáveis pela distância máxima ou MDS (maximum distance separable). Eles tem uma descrição interessante como conjuntos satisfazendo certas propriedades geométricas em espaços projetivos sobre corpos finitos que discutiremos no capítulo IV.

Passamos agora a dar um procedimento simples de decodificação.

Se C um $[n,d]$ código dado como núcleo de $H: \mathbb{F}_q^n \to \mathbb{F}_q^{n-d}$. Se $x \in \mathbb{F}_q^n$ chamaremos $H(x)$ de <u>sindrome</u> de x. Para cada $v \in \mathbb{F}_q^{n-d}$ escolha e_v tal que $H(e_v) = v$ e tal que $|e_v|$ é mínima. e_v é chamado um lider da classe lateral $H^{-1}(v)$. e_v pode não ser único, mas fixemos um em cada classe. Se recebermos uma mensagem y calculamos $H(y) = v$ e tomamos $c = y-e_v$ como a decodificação de y.

Note primeiro que $H(c) = H(y)-H(e_v) = v-v = 0$ logo $c \in C$. Note também que $d(c,y) = |e_v|$. Como e_v foi escolhido minimizando a norma em $H^{-1}(v)$ temos que c é o elemento de C mais próximo de y. Consequentemente se C corrige e erros a decodificação nos dará a mensagem enviada toda a vez que a mensagem recebida tem sindrome v satisfazendo $|e_v| \leq e$. Esse processo é chamado decodificação por semelhança máxima.

Em geral esse procedimento é muito custoso pois nos obriga a calcular os e_v. Código com propriedades particulares

podem ter algoritmos de decodificação mais eficientes. Encontraremos alguns exemplos disso mais adiante.

EXERCÍCIOS:

1. Considere o [7,4]-código sobre $\mathbb{F}_2$ que tem matriz de controle

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Este código é chamado o [7,4] código de Hamming

a) Calcule o peso de C;

b) Calcule uma matriz geradora de C;

c) Calcule lideres para as classes laterais de C;

d) Escreva alguns elementos de $\mathbb{F}_2^7$ aleatóriamente e decodifique-os.

2. Considere o [4,2]-código sobre $\mathbb{F}_3$ que tem matriz geradora

$$\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

a) Calcule o peso de C;

b) Calcule uma matriz de controle de C;

c) Decodifique $(0,1,1,1)$, $(1,1,1,0)$ e $(0,0,2,2)$.

3. Sejam C,C' respectivamente $[n,d]$ e $[n',d']$ códigos. Considere o código $C \oplus C'$ que é um $[n+n',d+d']$ código. Prove que $w(C\oplus C') = w(C)+w(C')$ e calcule matrizes geradoras e de controle de $C \oplus C'$ em função das de C e C'.

4. Seja C um $[n,d]$-código. Se $\ell \leq d$ e $i_1,\ldots,i_\ell \in \{1,\ldots,n\}$ Seja C' o código consistindo dos $c \in C$ tais que $c_{i_1} = \ldots = c_{i_\ell} = 0$. Considere, da maneira natural, C' como um código em $\mathbb{F}_q^{n-\ell}$. Mostre que $i_1,\ldots,i_\ell$ podem ser escolhidos tais que $\dim C' = d-\ell$ e $w(C') = w(C)$.

5. Seja C um $[n,d]$-código. Se $i_1,\ldots,i_r \in \{1,\ldots,n\}$ considere $A: \mathbb{F}_q^n \to \mathbb{F}_q^r$, $A(x_1,\ldots,x_n) = (x_{i_1},\ldots,x_{i_r})$. Seja C' a imagem de C por A. Prove que se $r \leq n-d$ pode se escolher $i_1,\ldots,i_r$ tais que C' seja um $[r,d]$-código e que $w(C') = w(C)-n+r$.

6. Defina para $x,y \in \mathbb{F}_q^n$ o produto interno $(x,y) = \sum_{i=1}^{n} x_i y_i$. Cuidado, o produto interno nada tem a ver com a norma. Dê um exemplo de $x \in \mathbb{F}_3^2$ com $x \neq 0$ e $(x,x) = 0$. Se C é um código em $\mathbb{F}_q^n$ defina o código dual $C^\perp = \{y \in \mathbb{F}_q^n \mid (x,y) = 0 \ \forall\, x \in C\}$. Qual é a relação entre as matrizes geradora e de controle de C e $C^\perp$?

Dê um exemplo de um código C onde $C = C^{\perp}$. Calcule $C^{\perp}$ para C como nos exercícios 1 e 2.

Nota: A relação entre os pesos de C e $C^{\perp}$ em geral não é simples, mas temos o seguinte resultado devido a MacWilliams (ver por exemplo [12]).

Sejam para $C \subseteq \mathbb{F}_q^n$ um $[n,d]$-código, $A_i = \#\{x \in C, |x| = i\}$ e $P_C(r) = \sum_{i=0}^{n} A_i r^i$. Então $P_{C^{\perp}}(t) =$

$= q^{-d}(1+(q-1)t)^n P_C(\frac{1-t}{1-(q-1)t})$.

7. Seja C um código com $w(C) = 2m$. Já sabemos que C corrige $m-1$ erros. Prove que C detecta m erros, isto é, se recebermos uma mensagem, podemos saber se ela contém no máximo m erros e se ela contiver no máximo m erros podemos dizer quantos erros ela contém.

8. As fitas magnéticas de armazenagem de dados em computadores são usualmente gravadas com nove cabeçotes, um em cima do outro. Isto é, os dados são armazenados numa matriz (b_{ij}), $i=1,\ldots,9$, $j=1,\ldots,n$, $b_{ij} \in \mathbb{F}_2$, para um certo $n > 1$. Para facilitar a leitura mecanica exige-se que haja pelo menos um bit aceso em cada coluna. Isso se garante exigindo $\sum_{i=1}^{9} b_{ij} = 1$ para todo j (justifique). Mostre também que isso permite corrigir erros decorrentes de defeito em um dos cabeçotes (o que é um defeito comum). Para garantir correção de outros tipos de erros exige-se também que $\sum_{j=1}^{n} b_{ij} = n \pmod 2$, para todo i. Para a análise

matemática deste código não perdemos nada trocando os zeros por uns e uns por zero (i.e. $b_{ij} \mapsto b_{ij}+1$). Com isso as equações de controle ficam $\sum_i b_{ij} = \sum_j b_{ij} = 0$. Descreva esse código em termos de uma matriz de controle num espaço apropriado e calcule sua dimensão e seu peso.

9. Dois códigos $C, C' \subseteq \mathbb{F}_q^n$ são ditos equivalentes se eles coincidem a menos de permutação das coordenadas. Prove que todo código é equivalente a um código que pode ser gerado por uma matriz na forma standard.

CAPÍTULO II

C O T A S

Quais são os melhores códigos que podemos construir? Nessa generalidade essa pergunta não está resolvida. O que podemos dizer, por outro lado, é que não podemos ser otimistas demais, há limitações no que podemos conseguir. O objetivo deste capítulo é demonstrar alguns resultados que limitam a possivel performance de códigos.

Já provamos um tal resultado, a cota de Singleton (Corolário (1.3)) que afirma que um $[n,d]$-código C satisfaz $w(C) \leq n-d+1$. Passaremos agora a discutir outros resultados deste tipo.

Introduzamos algumas notações:

Se $r \leq n$ é um inteiro e $a \in \mathbb{F}_q^n$, definimos a bola de centro a e raio r, como o conjunto

$$B(a,r) = \{x \in \mathbb{F}_q^n \mid d(x,a) \leq r\}.$$

Se n,w são inteiros $w \leq n$, definimos

$$A_q(n,w) = \max\{\dim C \mid C \subseteq \mathbb{F}_q^n, \text{ código com } w(C) = w\}.$$

Então, $A_q(n,w)$ é a maior dimensão possivel entre os códigos de peso e comprimento w,n dados sobre $\mathbb{F}_q$ e os resultados que estamos procurando são cotas superiores para $A_q(n,w)$. Por exemplo a cota de Singleton diz que $A_q(n,w) \leq n-w+1$.

Seja $V_q(n,r) = \#B(a,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$.

Essa última definição merece um comentário. Primeiro ela afirma que $\#B(a,r)$ não depende de a. De fato a função $x \to x-a$ estabelece uma bijeção entre $B(a,r)$ e $B(0,r)$. Segundo, a igualdade $\#B(0,r) = \sum_{i=0}^{r} \binom{n}{i}(q-1)^i$. Bom, $B(0,r)$ é o conjunto dos $x \in \mathbb{F}_q^n$, com $|x| \leq r$. Mostraremos que o conjunto dos $x \in \mathbb{F}_q^n$ com $|x| = i$ tem cardinalidade $\binom{n}{i}(q-1)^i$ e isso provará o que queremos.

Como escolher x tal que $|x| = i$? Primeiro, x tem i coordenadas não nulas, temos que escolher quais as coordenadas, temos então $\binom{n}{i}$ escolhas. Agora temos que escolher o valor de cada coordenada em $\mathbb{F}_q \setminus \{0\}$, temos $q-1$ escolhas para cada coordenada logo $(q-1)^i$ escolhas para todas as coordenadas não nulas.. O resultado segue.

A nossa primeira cota é conhecida como cota do empacotamento de esferas

(2.1) Teorema (Hamming): $A_q(n,w) \leq \log_q(q^n/V_q(n,[\frac{w-1}{2}]))$

Prova: Seja C um $[n,d]$-código de peso w e $e = [\frac{w-1}{2}]$. Vimos no Capítulo I que C corrige e erros e isso significa

que as bolas $B(c,e)$, $c \in C$ são disjuntas, então

$$\sum_{c \in C} \#B(c,e) \leq \#\mathbb{F}_q^n = q^n$$

logo

$$\#C.V_q(n,e) \leq q^n$$

mas $\#C = q^d$ e o resultado segue.

Essa cota tem relações com o problema clássico de empacotamento de esferas. Esse problema pode ser descrito da seguinte maneira: quantas bolas de pingue pongue cabem numa caixa dada? Evidentemente podemos formular o problema em um número qualquer de dimensões. O caso de dimensão dois foi resolvido por uma abelha a alguns milhões de anos atrás! Mas em dimensões maiores o problema é bem mais difícil.

Mas as relações não param aí e o problema se conecta com redes em $\mathbb{R}^n$, cristais, grupos finitos e outras coisas mais. Infelizmente não trataremos dessas coisas aqui, mas o leitor interessado pode (e deve) consultar [21].

A técnica de empacotar esferas leva ao seguinte resultado na direção inversa do Teorema 2.1

(2.2) Teorema (Varshamov-Gilbert): Se $w \leq n$

$$A_q(n,w) \geq \log_q(q^n/V_q(n,w-1))$$

Prova: Suponha que d é um inteiro satisfazendo $d < \log_q(q^n/V_q(n,w-1))$ e que C é um $[n,d]$-código com $w(C) = w$. Vamos mostrar que podemos construir um código C' com dimensão $d+1$ em $\mathbb{F}_q^n$ e com $w(C) = w$. Temos que

$$\sum_{c\in C} \#B(c,w-1) = q^d V_q(n,w-1) < q^n = \#\mathbb{F}_q^n.$$

Logo, existe $x \in \mathbb{F}_q^n$, $x \notin \bigcup_{c\in C} B(c,w-1)$. Em particular $x \notin C$ e $d(x,c) \geq w$ para todo $c \in C$. Considere o código C' gerado como espaço vetorial por C e x. Mostraremos que C' é o código desejado. Claramente a dimensão de C' é $d+1$. Calculemos $w(C')$.

Se $c' \in C'$, $c' \neq 0$, então $c' = c+\lambda x$, $c \in C$, $\lambda \in \mathbb{F}_q$. Se $\lambda = 0$ então $c \neq 0$ e $|c'| = |c| \geq w$. Se $\lambda \neq 0$ $|c'| = |\frac{1}{\lambda}c'| = |x+\frac{c}{\lambda}| = d(x,-\frac{c}{\lambda})$. Como $-c/\lambda \in C$, pois C é subespaço linear de $\mathbb{F}_q^n$, devemos ter $d(x,-c/\lambda) \geq w$ pela construção de x, logo $|c'| \geq w$. Mostramos então que $w(C') \geq w$, porém existe $c \in C$ com $|c| = w$, como $C \subseteq C'$ concluimos que $w(C') = w$.

Para provar o teorema começamos com um elemento $a \in \mathbb{F}_n^q$ $|a| = w$ e consideremos $C_1 = \{\lambda a \mid \lambda \in \mathbb{F}_q\}$ que é um código de dimensão 1 e $w(C_1) = w$. O procedimento dado acima nos permite, se $1 < \log_q q^n/V_q(n,w-1)$, construir um código C_2 de peso w e dimensão 2. Sucessivamente, então construimos, se $d < \log_q q^n/V_q(n,w-1)$ códigos $C_1, C_2, \ldots, C_{d+1}$ tais que $w(C_i) = w$ e $\dim C_i = i$ e isso prova o teorema.

Notemos que a prova do teorema nos dá um algoritmo para construir bons códigos. Porém, na prática esse algoritmo é impraticável, pois consome muito tempo. Goppa e outros autores construiram códigos por algoritmos praticáveis a partir de uma construção devida a Goppa que produz códigos satisfazendo

$$\dim C \geq \log_q(q^n/V_q(n,w-1)).$$

Mais ainda esses códigos fazem parte de uma família infinita de bons códigos. Veremos essa construção no capítulo V

Voltando ao problema das cotas superiores para $A_q(n,w)$, temos ainda

(2.3) Teorema (Plotkin): Ponha $\theta = 1-1/q$. Se $w > \theta n$ então

$$A_q(n,w) \leq \log_q(w/w-\theta n)$$

Prova: Seja C um $[n,d]$-código de peso $w > n\theta$. Considere os conjuntos $\{c \in C \mid c_i \neq 0\}$, $i=1,\ldots,n$. Dado um elemento $c \in C$ este elemento aparece em $|c|$ destes conjuntos, logo temos

$$\sum_{c\in C} |c| = \sum_{i=1}^{n} \#\{c \in C, \quad c_i \neq 0\}.$$

Seja i um inteiro $1 \leq i \leq n$ e considere $D = \{c \in C, \quad c_i = 0\}$. D é um subespaço linear de C e a codimensão de D em C é no máximo 1, logo $\dim D = d$ ou $d-1$,

logo $\#D = q^d$ ou q^{d-1}. Por outro lado $\#\{c \in C,\ c_i \neq 0\} =$ $= \#C - \#D$. Logo, em qualquer hipótese, $\#\{c \in C,\ c_i \neq 0\} \leq$ $\leq q^d - q^{d-1} = \theta q^d$. Concluimos que

$$\sum_{c \in C} |c| \leq n\theta q^d$$

Por outro lado, se $c \in C$, $c \neq 0$ temos $|c| \geq w$, logo

$$\sum_{c \in C} |c| \geq w(q^d - 1).$$

Segue-se então que

$$q^d \leq \frac{w}{w - \theta n}$$

e o teorema está provado.

Vamos agora comparar as cotas obtidas. Para isso é conveniente olhar as coisas assintóticamente. Para isso definimos $\alpha_q(\delta) = \limsup_{n \to \infty} \frac{A_q(n, \lfloor \delta n \rfloor)}{n}$, $0 \leq \delta \leq 1$.

Isto é, $\alpha_q(\delta)$ é o supremo dos números α tal que exista uma sequência de códigos C_i, $i=1,2,\ldots$, $C_i \subset \mathbb{F}_q^{n_i}$ tais que $\frac{w(C_i)}{n_i} \to \delta$ e $\frac{\dim C_i}{n_i} \to \alpha$. Isso nos permite considerar as cotas para n grande sem se ater a peculiaridades de um número finito de valores de n.

O primeiro resultado interessante sobre $\alpha_q(\delta)$ é devido a Manin ([13]): $\alpha_q(\delta)$ é uma função continua e decrescente. Não provaremos isso aqui.

A cota de Singleton nos dá

$$\alpha_q(\delta) \leq 1-\delta$$

A cota de Plotkin nos dá, $(\theta=1-1/q)$

$$\alpha_q(\delta) \leq 0 \qquad \text{se} \qquad \theta \leq \delta \leq 1$$

logo

$$\alpha_q(\delta) = 0 \qquad \text{se} \qquad \theta \leq \delta \leq 1.$$

Usando a cota de Plotkin podemos deduzir o seguinte

$$\alpha_q(\delta) \leq 1-\delta/\theta \qquad 0 \leq \delta \leq \theta.$$

O raciocínio é o seguinte. Suponha C é um $[n,d]$-código de peso w com $w \leq \theta n$. Ponha $n' = [\frac{w-1}{\theta}]$ e tome um subcódigo C' de C obtido anulando $n-n'$ coordenadas. Então podemos considerar C' como um $[n',d']$ código (ver ex.) e $d' \geq d+n'-n$ e $w(C') = w$. Podemos aplicar o Teorema 2.3 a C' e obtemos

$$d' \leq \log_q(w(C')/w(C')-\theta n') = \log_q(w/w-n'\theta)$$

Se tomarmos C numa sequência com $\frac{w}{n} \to \delta$ e $\frac{d}{n} \to \alpha$ então $\frac{n'}{n} \to \frac{\delta}{\theta}$ e

$$\frac{d}{n} \leq \frac{d'+n-n'}{n} \leq \frac{1}{n} \log_q(\frac{w}{w-n'\theta}) + 1 - \frac{n'}{n}$$

e temos que

$$\frac{1}{n} \log_q(\frac{w}{w-n'\theta}) \to 0 \qquad \text{logo}$$

$$\alpha \leq 1-\delta/\theta$$

e o resultado segue.

A cota de Hamming nos dá

$$\alpha_q(\delta) \leq 1-H_q(\delta/2) \qquad 0 \leq \delta \leq \theta$$

onde $H_q(x) = \begin{cases} 0, & x = 0 \\ x \log_q \theta - x \log_q x - (1-x)\log_q(1-x), & 0 < x \leq \theta \end{cases}$

Isso segue do seguinte fato que se prova facilmente através da fórmula de Stirling (ver [12] Lemma 5.1.6)

$$\lim_{n\to\infty} \frac{\log_q V_q(n,[\lambda n])}{n} = H_q(\lambda)$$

Das três cotas mencionadas, a pior é a de Singleton. A cota de Hamming é melhor que a de Plotkin para $0 \leq \delta \leq \delta_o$ para um certo $\delta_o \in (0,\theta)$ para $\delta_o \leq \delta \leq \theta$ a de Plotkin é melhor. A melhor cota conhecida, devida a Elias, é a seguinte

$$(*) \qquad \alpha_q(\delta) \leq 1-H_q(\theta-\sqrt{\theta(\theta-\delta)}) \qquad 0 \leq \delta \leq \theta$$

Uma prova desta cota pode ser vista em [12]. Quando $q = 2$ há uma cota melhor ainda ([15]).

Para constar, o Teorema 2.2 nos dá:

$$(**) \qquad \alpha_q(\delta) \geq 1-H_q(\delta) \qquad 0 \leq \delta \leq \theta$$

Há um espaço entre (*) e (**) e no presente momento não se sabe o que ocorre aí nesse espaço

EXERCÍCIOS:

1. Seja C um $[n,d]$-código sobre $\mathbb{F}_q$ com $d \geq 2$ que contém o vetor $1=(1,1,1,\ldots,1)$. Prove que $w(C) \leq \frac{(q-1)n}{q}$.

2. Seja n impar e $C = \{(0,\ldots,0),(1,\ldots,1)\} \subseteq \mathbb{F}_2^n$. Prove que C atinge a cota de Hamming.

3. Calcule $A_q(n,w)$ para $(q,n,w) \in \{(2,6,1),(2,7,1),(2,7,2),(3,5,1),(3,5,2)\}$.

4. Seja $n = q^m$ e (a_{ij}), $i=1,\ldots,m$, $j=1,\ldots,n$ tal que $(a_{1j},\ldots,a_{mj})$ percorre $\mathbb{F}_q^m$. Seja C o $[n,m+1]$-código gerado por

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ a_{11} & \ldots\ldots & & a_n \\ \vdots & & & \\ a_{m1} & \ldots\ldots & & a_{mn} \end{pmatrix}$$

Prove que o peso de qualquer $x \in C$, $x \neq 0,1$ (ver

ex. 1) é da forma $q^m - q^i$, $0 \leq i < m$. Conclua que $w(C) = \frac{(q-1)n}{q}$, logo a cota do ex. 1 pode ser atingida. (Sugestão: as equações que descrevem o anulamento de coordenadas de x definem um subconjunto de $\mathbb{F}_q^n$, qual?). Esses códigos são um caso especial dos códigos de Reed-Muller. O código de Reed-Muller como acima com $m = 5$ e $q = 2$ foi usado na transmissão para a Terra das fotografias de Marte tiradas pelo Mariner 9.

5. Nesse exercício provaremos a cota de Griesmer: Se C é um $[n,d]$-código com peso w então $n \geq \sum_{i=0}^{d-1} \lceil w/q^i \rceil$. $\lceil x \rceil$ é o menor inteiro $\geq x$.

Seja $c \in C$ um vetor não nulo de norma $r = |c|$. Suponha que $c = (c_1,\ldots,c_r,0,\ldots,0)$. Considere a aplicação linear $f: (x_1,\ldots,x_n) \mapsto (\frac{x_1}{c_1},\ldots,\frac{x_r}{c_r}, x_{r+1},\ldots,x_n)$. Prove que $f(C)$ é um $[n,d]$-código de peso w.

Seja agora C um código com matriz geradora $G = (g_{ij})$ tal que $g_{1j} = 1$, $j \leq w$, $g_{1j} = 0$, $j > w$. Prove que o código C' de matriz geradora

$$G' = (g_{ij})_{\substack{i=2,\ldots,d \\ j=w+1,\ldots,n}}$$

é um $[n-w,d-1]$-código de peso $w(C') \geq \lceil w/q \rceil$. (Ver ex. 1)

Defina agora $N(d,w)$ como o menor n tal que exista um $[n,d]$-código de peso w. Conclua do raciocínio acima que

$N(d-1, \lceil w/q \rceil) \leq N(d,w)-d$. Complete a prova da cota de Griesmer.

Sugestão: Se $v \in C'$, $\exists\, u$, $(u,v) \in C$. Então $(u-\lambda(1,\ldots,1),v) \in C$. Escolha λ tal que $|u-\lambda(1,\ldots,1)|$ é o menor possível.

CAPÍTULO III

CÓDIGOS CÍCLICOS

Um <u>código cíclico</u> $C \subset \mathbb{F}_q^n$ é um código tal que $(c_{n-1},c_o,\ldots,c_{n-2}) \in C$ sempre que $(c_o,\ldots,c_{n-1}) \in C$. Isto é, C é invariante com respeito a permutações cíclicas de coordenadas.

O interesse fundamental dos códigos cíclicos é que eles admitem uma representação interessante em termos de polinomios sobre $\mathbb{F}_q$ que permite a descrição de um algoritmo de decodificação muito simples.

Consideramos o anel $A = \mathbb{F}_q[x]/(x^n-1)$, quociente de $\mathbb{F}_q[x]$ pelo ideal gerado por x^n-1. Todo elemento de A pode ser representado unicamente por um polinomio $a_o+\ldots+a_{n-1}x^{n-1}$ de grau no máximo n-1 (pelo algoritmo da divisão de polinomios.) Vamos identificar $\mathbb{F}_q$ com A identificando $a = (a_o,\ldots,a_{n-1})$ com $a_o+\ldots+a_{n-1}\,x^{n-1} = a(x)$. Note que se $b = (a_{n-1},a_o,\ldots,a_{n-2})$ então $b(x) \equiv xa(x) \bmod (x^n-1)$. De fato $xa(x) = a_ox+\ldots+a_{n-1}x^n \equiv$ $\equiv a_{n-1}+a_ox+\ldots+a_{n-2}x^{n-1} \pmod{x^n-1}$. Então os códigos cíclicos podem ser caracterizados como os subespaços C de A tais que

$C(x) \in C \Rightarrow xC(x) \in C$.

Notemos agora que se C é um código cíclico e $C(x) \in C$ então $xC(x) \in C$, $x^2C(x) \in C$, etc... logo $b(x)a(x) \in C$ para todo $b(x) \in A$. Bem, isto quer dizer que C é um ideal de A. Reciprocamente se C é um ideal de A então C é um subespaço de A e $xC(x) \in C$ sempre que $c(x) \in C$, logo C é um código cíclico. Resumindo os códigos cíclicos são os ideais de A. Os ideais de A tem a seguinte caracterização:

(3.1) Proposição: Todo ideal de A é da forma (g) onde g é um divisor monico de x^n-1. Além disso tal g é unicamente determinado pelo ideal.

Prova: Seja $\varphi: \mathbb{F}_q[x] \to A$ a aplicação natural. Se C é um ideal de A então obviamente $\varphi^{-1}(C)$ um ideal de $\mathbb{F}_q[x]$. Como $\mathbb{F}_q[x]$ é euclidiano $\varphi^{-1}(C)$ é principal, $\varphi^{-1}(C) = (h)$. Logo C é gerado por h em A. Escrevamos $h = f.g$ onde g é um divisor monico de x^n-1 e $(f, x^n-1) = 1$, isto é, g é o MDC de h e x^n-1. Mostraremos que $C = (g)$. Como f e x^n-1 são coprimos existe $\bar{f}$ tal que $f.\bar{f} \equiv 1 \pmod{x^n-1}$. Seja $c \in C$, sabemos então que $c = ah = afg$ logo $c \in (g)$, isto é, $c \subseteq (g)$. Se mostrarmos que $g \in (h)$ então teremos $C = (h) \supseteq (g)$ e consequentemente $C = (g)$. De fato $g \in (h)$ pois $\bar{f}h = \bar{f}.fg \equiv g \pmod{x^n-1}$ logo $g = \bar{f}h$ em A.

Para a unicidade suponha que $(g) = (g')$ então $g' = f.g$ e $g = f'g'$ logo $ff' = 1$ e f é invertível em A.

Isso implica que f é coprimo com x^n-1. Como g' divide x^n-1 devemos então ter que $f \in \mathbb{F}_q$ e como g e g' são monicos, f = 1 logo g = g'.

Se C = (g) é um código cíclico então o polinomio g é chamado o <u>gerador</u> de C e o polinomio $h = (x^n-1)/g$ é chamado o <u>polinomio de controle</u> de C. Notemos que $c(x) \in C$ se e só se $h(x)c(x) \equiv 0 \pmod{x^n-1}$, dai o nome de controle.

Lembramos agora que se $a(x) \in A$, $a(x)=a_o+\ldots+a_{n-1}x^{n-1}$ então existem polinomios b(x),r(x) tais que $a(x)= b(x).g(x)+r(x)$, grau r(x) ≤ grau g(x). Mais ainda grau b(x) < n-grau g(x). Seja d o grau de g. Então para todo elemento $a(x) \in C$, devemos ter r(x) = 0, logo $a(x) = b(x).g(x)$ onde grau b(x) < < n-d. Dai segue-se imediatamente que dim C = n-d.

Vemos também que $g(x),xg(x),\ldots,x^{n-d-1}g(x)$ é uma base de C sobre $\mathbb{F}_q$, logo, se $g = g_o+g_1x+\ldots+g_dx^d$, então

$$G = \begin{pmatrix} g_o & g_1 & \cdots & g_d & 0 & \cdots & 0 \\ 0 & g_o & \cdots & g_d & \cdots & & 0 \\ 0 & 0 & g_o & \cdots & g_d & \cdots & 0 \\ \cdots & & & & & & \\ 0 & \cdots & 0 & g_o & \cdots & & g_d \end{pmatrix}$$

é uma matriz geradora de C.

Vimos acima também que $c(x) \in C$ se e só se $h(x).c(x) = 0$. Dai conclui-se facilmente que

$$H = \begin{pmatrix} 0 & \cdots & 0 & h_{n-d} & \cdots & h_1 & h_o \\ 0 & \cdots & h_{n-d} & \cdots & h_o & 0 & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ h_{n-d} & \cdots & h_o & 0 & \cdots & 0 & \end{pmatrix}$$

é uma matriz de controle de C, onde $h(x) = \frac{x^n-1}{g(x)} = \sum_{i=0}^{n-d} h_i x^i$.

De agora em diante suporemos que $(n,q) = 1$.

Estudaremos agora o peso de um código cíclico para isso introduziremos o chamado polinômio de Mattson Solomon (ou transformada de Fourier discreta).

Seja $\bar{\mathbb{F}}_q$ o fecho algébrico de $\mathbb{F}_q$ e $\beta \in \bar{\mathbb{F}}_q$ uma raiz primitiva n-ésima da unidade e T o conjunto de polinômios de grau menor que n com coeficientes em $\bar{\mathbb{F}}_q$. Define-se $\mathfrak{F}: T \to T$ pondo

$$\mathfrak{F}(a) = \sum_{j=0}^{n} a(\beta^j)x^{n-j}$$

(3.2) Lema: $\mathfrak{F}(a)(\beta^k) = na_k$

Prova: Calculemos $\mathfrak{F}(a)(\beta^k)$

$$\mathfrak{F}(a)(\beta^k) = \sum_{j=0}^{n} \left(\sum_{i=0}^{n-1} a_i \beta^{ij} \right)(\beta^k)^{n-j} = (\beta^n = 1)$$

$$= \sum_{j=0}^{n} \sum_{i=0}^{n-1} a_i \beta^{ij} \beta^{-kj} = \sum_{j=0}^{n} \sum_{i=0}^{n-1} a_i \beta^{j(i-k)} =$$

$$= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{n} \beta^{j(i-k)} \right) a_i$$

Afirmo que $\sum_{j=0}^{n} \beta^{jr} = \begin{cases} n & \text{se } r = 0 \\ 0 & \text{se } -n < r < n \end{cases}$

Desta afirmação seguirá que $A(\beta^k) = na_k$. A afirmação é trivial se $r = 0$. Nos outros casos temos

$$\sum_{j=0}^{n} \beta^{jr} = \frac{\beta^{rn}-1}{\beta^r-1} = \frac{(\beta^n)^r-1}{\beta^r-1} = 0.$$

(3.3) Teorema: Seja r o grau de $(x^n-1, \mathfrak{F}(a))$ então $|a|=n-r$.

Prova: $n-|a|$ é o número de coeficientes de $a(x)$ que são nulos. Temos que $a_k = 0$ se e só se $\mathfrak{F}(a)(\beta^k) = 0$, pelo Lema (3.2). Então $n-|a|$ é o número de raizes n-ésimas da unidade que são zeros de $\mathfrak{F}(a)$, isto é, o número de raizes comuns de $\mathfrak{F}(a)$ e x^n-1 que é o grau de $(x^n-1, \mathfrak{F}(a))$, provando o teorema.

Vamos agora estudar mais detalhadamente uma classe especial de códigos, conhecidos como códigos BCH (i.e., Bose, (Ray) Chaudhuri, Hocquenghem). Seja $\beta \in \bar{\mathbb{F}}_q$ uma raiz primitiva n-ésima da unidade e denotemos por $g^{(i)}(x)$ o polinomio mínimo de β^i sobre $\mathbb{F}_q$, isto é, o polinomio monico não nulo de menor grau com coeficientes em $\mathbb{F}_q$ que tem β^i como raiz.

O código BCH de distância designada δ e o código cíclico C com polinomio gerador $g(x) = \text{MMC}(g^{(1)}, \ldots, g^{(\delta-1)})$.

Seja m o menor inteiro positivo tal que $q^m \equiv 1 \pmod{n}$ então (ver ex. 3) $\mathbb{F}_{q^m}$ é a menor extensão de $\mathbb{F}_q$ que contém todas as raizes de $x^n-1 = 0$. Consequentemente grau $g^{(i)} \leq m$ para $i=1,\ldots,n$, logo grau $g \leq m(\delta-1)$. Dai se conclui que $\dim C \geq n-m(\delta-1)$. O resultado seguinte nos dá uma estimativa para o peso de C e justifica o nome de distância designada

(3.4) Teorema: $w(C) \geq \delta$.

Prova: Seja $c(x) \in C$, $c(x) \neq 0$. Como $g(x)|c(x)$ e $g(\beta^i) = 0$, $i=1,\ldots,\delta-1$, temos $c(\beta^i) = 0$, $i=1,\ldots,\delta$. Consequentemente, o grau de $\mathfrak{I}(c)$ é no máximo $n-\delta$. Segue-se que o grau de $(\mathfrak{I}(c),x^n-1)$ é no máximo $n-\delta$, logo $|c| \geq \delta$ pelo Teorema (3.3).

Suponha que escolhemos um código BCH de distância designada $\delta = 2t+1$, sabemos então que esse código corrige t erros. O que torna os códigos BCH muito interessantes é que há um algoritmo de decodificação eficiente, devido a Berlekamp, que passamos a expor.

Seja $C \in A$ então um código BCH de distância designada $\delta = 2t+1$ e β a raiz primitiva n-ésima da unidade usada para definir C.

Seja $a(x) \in A$ é uma palavra recebida com no máximo t erros. Suponhamos inicialmente que conhecemos a palavra en-

viada $c(x)$ e seja $e(x) = a(x)-c(x)$ o erro. Definimos então, se $e(x) = e_o+\ldots+e_{n-1}x^{n-1}$

$M = \{i \mid e_i \neq 0\}$

$r = \#M$

$$\ell(x) = \prod_{i\in M} (1-\beta^i x)$$

$$s(x) = \sum_{i\in M} e_i\beta^i x \sum_{j\in M\setminus\{i\}} (1-\beta^j x).$$

M é o conjunto das posições onde os erros ocorrem e r é o número de erros, que estamos supondo ser no máximo t. $\ell(x)$ é chamado o polinomio localizador dos erros. De fato, $i \in M$ se e só se $\ell(\beta^{-i}) = 0$, logo conhecendo $\ell(x)$ saberemos onde os erros estão. O polinomio $s(x)$ servirá para nos dizer qual foi o erro. De fato se $i \in M$ temos

$$s(\beta^{-i}) = e_i \sum_{j\in M\setminus\{i\}} (1-\beta^j\beta^{-i}) = -e_i\ell'(\beta^{-i})$$

onde ℓ' é a derivada de ℓ. Desta equação podemos calcular e_i a partir de ℓ e s. Resumindo se conhecermos ℓ e s saberemos onde os erros ocorreram e quais foram os erros. O algoritmo consistirá então de se obter $\ell(x)$ e $s(x)$ somente a partir de $a(x)$. Se pudermos fazer isso então obtemos o processo de correção como foi feito acima.

A observação crucial é a seguinte (onde trabalhamos com séries formais, ver apendice):

$$\frac{s(x)}{\ell(x)} = \sum_{i\in M} \frac{e_i\beta^i x}{1-\beta^i x} = \sum_{i\in M} e_i \sum_{j=1}^{\infty} (\beta^i x)^j =$$

(*)

$$= \sum_{j=1}^{\infty} \Big(\sum_{i\in M} e_i \beta^{ij} \Big) x^j = \sum_{j=1}^{\infty} e(\beta^j) x^j .$$

Por outro lado, $e(\beta^j) = a(\beta^j) - c(\beta^j) = a(\beta^j)$ para $j=1,\ldots,\delta-1$. Logo conhecemos os valores $e(\beta^j)$ para $1 \le j \le 2t$ a partir de $a(x)$ somente.

O ponto crucial agora é que, por hipótese, $r \le t$ e como grau ℓ, grau $s \le r$ temos grau ℓ, grau $s \le t$.

Seja $$f(x) = \sum_{j=1}^{2t} a(\beta^j) x^j$$

a equação (*) se reescreve como

(*) $$\frac{s(x)}{\ell(x)} \equiv f(x) \pmod{x^{2t+1}}.$$

Como $f(x)$ é conhecido, isso nos permite determinar ℓ e s. De fato

$$s(x) - \ell(x) f(x) \equiv 0 \pmod{x^{2t+1}}$$

como $(\ell, s) = 1$ e $\ell(0) = 1$, isso segue dos resultados do apendice.

Poderiamos falar eternamente sobre códigos cíclicos e códigos BCH mas vamos parar por aqui. O leitor interessado pode consultar [15].

APENDICE

Seja F um corpo. O corpo de séries formais $F((x))$ é o conjunto das expressões $\sum_{i=n}^{\infty} a_i x^i$, $a_i \in F$, $n \in \mathbb{Z}$. (Note que essas expressões são apenas formais, não discutiremos nenhuma noção de convergência).

Em $F((x))$ definimos a soma e o produto de dois elementos pondo

$$\Sigma a_i x^i + \Sigma b_i x^i = \Sigma (a_i + b_i) x^i$$

$$(\Sigma a_i x^i)(\Sigma b_i x^i) = \Sigma c_i x^i$$

onde $c_k = \sum_{i+j=k} a_i b_j$

Com essas operações $F((x))$ é um corpo (ver ex. 1). Se $\varphi = \sum_{i=n}^{\infty} a_i x^i \in F((x))$ e $a_n \neq 0$, dizemos que n é a ordem de φ, denotado ord φ. Se ord $\varphi \geq 0$ dizemos que φ é inteiro. Temos que $\text{ord}(\varphi\psi) = \text{ord}(\varphi) + \text{ord}(\psi)$ (ex. 2).

Claramente $F[x] \subset F((x))$. Como $F((x))$ é um corpo, temos então $F(x) \subset F((x))$. Vamos mostrar que $\frac{1}{1-ax} = \sum_{i=0}^{\infty} a^i x^i$, pois utilizamos isso no texto. De fato $(\sum_{i=0}^{\infty} a^i x^i)(1-ax) =$

$= \sum_{i=0}^{\infty} a^i x^i - \sum_{i=1}^{\infty} a^i x^i = 1.$

Se $\varphi \in F((x))$ e $\operatorname{ord}\varphi \geq n > 0$ escrevamos $\varphi \equiv 0 \pmod{x^n}$

(A.1) Teorema (Padé): Seja $\varphi \in F((x))$, $\operatorname{ord}\varphi \geq 0$ e N um inteiro positivo. Então existem $a,b \in F[x]$, $b \neq 0$ de grau no máximo N satisfazendo $\operatorname{ord}(a-b\varphi) \geq 2N+1$. Se a,b forem tais polinomios que além disso satisfaçam $(a,b) = 1$, $b(0) = 1$ então eles são únicos com esta propriedade.

Prova: Escrevamos $\varphi = \sum_{i=0}^{\infty} \varphi_i x^i$, $a = \sum_{i=0}^{N} a_i x^i$, $b = \sum_{i=0}^{N} b_i x^i$, onde os coeficientes a_i, b_i ainda estão para ser determinados. Considere o sistema de equações, equivalente a $\operatorname{ord}(a-b\varphi) \geq 2N+1$.

$$(i) \qquad \sum_{i+j=k} b_i \varphi_i = a_k \qquad k = 0,\ldots,N$$

$$(ii) \qquad \sum_{i+j=k} b_i \varphi_i = 0 \qquad k = N+1,\ldots,2N$$

O sistema (ii) é um sistema de N equações nas $N+1$ incognitas b_i, logo tem uma solução não nula $(b_0,\ldots,b_N)$ e $a_0,\ldots,a_N$ estão determinados por (i). Isso prova a primeira parte do Teorema. Quanto a unicidade sejam a,b, $\bar{a},\bar{b}$ soluções satisfazendo todas as propriedades. Temos então que

$$\operatorname{ord}(a\bar{b}-b\bar{a}) = \operatorname{ord}(\bar{b}(a-b\varphi)-b(\bar{a}-\bar{b}\varphi)) \geq 2N+1$$

como o grau de $a\bar{b}-b\bar{a}$ é no máximo $2N$ isso implica $a\bar{b}-b\bar{a} = 0$ ou $a/b = \bar{a}/\bar{b}$. Como $(a,b) = (\bar{a},\bar{b}) = 1$ isso implica $a = \lambda\bar{a}$, $b = \lambda\bar{b}$, $\lambda \in F$. Como $b(0) = \bar{b}(0) = 1$, temos $\lambda = 1$ logo $a = \bar{a}$, $b = \bar{b}$ o que prova o teorema.

Daremos agora um algoritmo para se obter os polinomios a e b do teorema que é mais rápido que resolver o sistema linear (ii). Primeiramente, façamos a observação importante que a,b dependem somente de $\varphi_o,\ldots,\varphi_{2N}$. Podemos então supor que $\varphi = \varphi_o+\varphi_1 x +\ldots+ \varphi_{2N}x^{2N}$.

Definiremos polinomios $r_{-1},r_o,\ldots,q_1,q_2,\ldots$, pelo algoritmo de Euclides, pondo

$r_{-1} = x^{2N+1}, \quad r_o = \varphi$

$r_{i-2} = q_i r_{i-1} + r_i, \quad \deg r_i < \deg r_{i-1}$.

Isto é, r_i é o resto da divisão de r_{i-2} por r_{i-1}.

Definimos também polinomios t_i, $i = -1,0,\ldots$ por

$t_{-1} = 0, \quad t_o = 1$

$t_i = t_{i-2} - q_i t_{i-1}, \quad i \geq 1$

(A.2) Lema: $t_i\varphi \equiv r_i \pmod{x^{2N+1}}, \quad i = -1,0,1,\ldots$

Prova: A afirmação é óbvia para i=-1,0. Supondo por indução que vale para i-1, i-2, temos

$$t_i\varphi - r_i = (t_{i-2}-q_i t_{i-1})\varphi-(r_{i-2}-q_i r_{i-1}) =$$

$$= (t_{i-2}\varphi-r_{i-2})-q_i(t_{i-1}\varphi-r_{i-1}) \equiv 0 \pmod{x^{2N+1}}$$

logo a afirmação é verdadeira.

Notemos agora que como os graus dos r_i decrescem e r_{-1} tem grau 2N+1, temos que $r_i = 0$, $i > 2N$. Seja n o maior inteiro tal que $r_n \neq 0$.

(A.3) Lema: Existe um único j, $0 \leq j \leq n$, tal que grau t_j, grau $r_j \leq N$.

Prova: Pode-se provar facilmente (ver ex. 3) que grau r_{i-1}+grau t_i = 2N+1, $0 \leq i \leq n+1$.

Como grau r_i decresce de 2N a 0 para $0 \leq i \leq n$ existe um único j, $0 \leq j \leq n$ tal que

$$\text{grau } r_{j-1} > N$$

$$\text{grau } r_j \leq N$$

então grau t_j = 2N+1-grau $r_{j-1} \leq N$. Isso mostra a existência do j como anunciado no lema. Para provar a unicidade, notemos que se grau r_i, grau $t_i \leq N$ então grau r_{i-1} = 2N+1-grau $t_i > N$, logo i=j. Com isso, o lema está provado.

O algoritmo para achar a e b no Teorema A.1 então é o seguinte, calculamos os q_i, r_i sucessivamente pelo algoritmo da divisão até que achamos j como na prova do lema então calculamos os t_i pela sua definição recursiva e temos $a = r_j$, $b = t_j$. O Lema (A.3) garante que grau a, grau $b \leq N$ e o Lema (A.2) garante que ord$(a-b\varphi) \geq 2N+1$.

O polinomios a,b do Teorema (A.1) são chamados de aproximantes de Padé de ordem N de φ. Quando $b(0) \neq 0$

a/b é chamado um quociente parcial (da fração contínua) de φ.

EXERCÍCIOS:

1. Um código C é dito constaciclico (sic) de constante λ se $(c_0,\ldots,c_{n-1}) \in C \Rightarrow (\lambda c_{n-1},c_0,\ldots,c_{n-2}) \in C$. Generalize alguns dos resultados deste capítulo para códigos constaciclicos.

2. Prove que se $a,b \in \mathbb{F}_q[x]$, $a = \Sigma a_i x^i$, $b = \Sigma b_i x^i$ então $\mathfrak{F}(ab) = \Sigma a_i b_i x^i$. (Análogo da fórmula de convolução).

3. Seja β uma raiz primitiva n-ésima da unidade em $\bar{\mathbb{F}}_q$. Seja m o menor inteiro com $q^m \equiv 1 \pmod n$. Prove que $\mathbb{F}_{q^m}$ é o menor corpo contendo $\mathbb{F}_q$ e β (sugestão, $\beta \in \mathbb{F}_{q^r} \Rightarrow \beta^{q^r-1} = 1$).

4. Seja n um número primo e p um primo que gera o grupo multiplicativo $\mathbb{F}_n^*$. Ache o polinomio gerador do código BCH de comprimento n sobre $\mathbb{F}_p$ e distância designada δ para cada $\delta = 1,\ldots,n$. Calcule sua dimensão e seu peso.

5. Prove que um código BCH sobre $\mathbb{F}_q$ de comprimento $n=q-1$ é MDS.

6. Considere o código BCH sobre $\mathbb{F}_q$ de comprimento 7 e distância designada 3. Decodifique, se possível, (1110001), (1000100) e (1111100).

7. Mostre que o dual de um código cíclico (no sentido do exercício 6 do Capítulo I) é equivalente a um código cíclico. Descreva seu gerador em termos do gerador do código.

8. O código [23,12] de Golay é o código cíclico com $n = 23$, sobre $\mathbb{F}_2$ gerado por $x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$. Prove que seu peso é 7.

9. Seja $n = 31$ e α um gerador do grupo multiplicativo $\mathbb{F}_{32}^*$. Seja g um divisor de $x^{31}-1$ tal que $g(\alpha) = g(\alpha^5) = 0$. Prove que o código cíclico de comprimento 31 sobre $\mathbb{F}_2$ com gerador g tem peso pelo menos 4.

10. Seja C um código cíclico sobre $\mathbb{F}_q$. Mostre que se $c(x) \in C$ então $c(x^q) \in C$.

11. Um polinomio $g(x)$ é dito reversivel se para todo α com $g(\alpha) = 0$ temos $\alpha \neq 0$ e $g(\alpha^{-1}) = 0$. Um código cíclico C é reversivel se $(c_0,\ldots,c_{n-1}) \in C \Rightarrow (c_{n-1},c_{n-2},\ldots,c_0) \in C$. Prove que C é reversivel se e só se seu polinomio gerador é reversivel.

EXERCÍCIOS DO APENDICE:

1. Seja $\sum_{n=0}^{\infty} a_n x^n \in F((x))$, com $a_o = 1$. Mostre que o sistema de equações $\sum_{i+j=k} a_i b_j = 0$, $k \geq 2$, $b_o = 1$ define $b_1, b_2, \ldots$ univocamente tais que $\Sigma a_n x^n \, \Sigma b_n x^n = 1$. Conclua que $F((x))$ é um corpo.

2. Mostre que se $\varphi, \psi \in F((x))$, $\text{ord}(\varphi\psi) = \text{ord}\,\varphi + \text{ord}\,\psi$ e $\text{ord}(\varphi+\psi) \geq \min\{\text{ord}\,\varphi, \text{ord}\,\psi\}$.

3. Prove que $t_i r_{i-1} - t_{i-1} r_i = (-1)^i x^{2N+1}$, $0 \leq i \leq n+1$ (sugestão: indução). Prove que grau $t_i >$ grau t_{i-1} para $0 \leq i \leq n+1$. Conclua que grau t_i + grau $r_{i-1} = 2N+1$.

4. Calcule o aproximante de Padé de ordem 5 de $x^{10} + x^5 + 1$.

CAPÍTULO IV

CÓDIGOS MDS E GEOMETRIA FINITA

O objetivo deste capítulo é relacionar os códigos MDS (C é MDS se C é um $[n,d]$-código com $w(C) = n-d+1$) com certos conjuntos definidos por propriedades geométricas em espaços projetivos sobre corpos finitos. Isso nos permite relacionar o estudo destes códigos com outros problemas interessantes de Geometria finita e combinatória. Mais detalhes sobre os assuntos abordados aqui podem ser vistos em [8].

O espaço projetivo n-dimensional $\mathbb{P}^n$ sobre $\mathbb{F}_q$ é definido como o conjunto das retas que passam pela origem em $\mathbb{F}_q^{n+1}$. Uma reta em $\mathbb{F}_q^{n+1}$ passando pela origem é dada por λa, $\lambda \in \mathbb{F}_q$ onde $a = (a_0,\ldots,a_n) \neq 0$. Então $\mathbb{P}^n$ pode ser descrito como $\mathbb{F}_q^{n+1} - \{0\}/\sim$ onde $\sim$ é a relação de equivalência $a \sim b$ se e só se $a = \lambda b$, $\lambda \in \mathbb{F}_q \setminus \{0\}$.

Se $(a_0,\ldots,a_n) \in \mathbb{F}_q^{n+1} \setminus \{0\}$ denotaremos o ponto de $\mathbb{P}^n$ definido por ele por $(a_0:\ldots:a_n)$. Note então que $(a_0:\ldots:a_n) = (b_0:\ldots:b_n)$ se e só se $a_i = \lambda b_i$, $i=0,\ldots,n$ para $\lambda \in \mathbb{F}_q - \{0\}$.

Um subespaço i-dimensional de $\mathbb{P}^n$ é o conjunto de retas contidos em um subespaço $(i+1)$-dimensional de $\mathbb{F}_q^{n+1}$. Um subespaço 1-dimensional de $\mathbb{P}^n$ é chamado uma reta e um subespaço $(n-1)$-dimensional é chamado um hiperplano. Notemos que um subespaço i-dimensional intersecta um subespaço j-dimensional num subespaço que terá dimensão no mínimo $n-(i+j)$. Um hiperplano é sempre dado como conjunto de soluções de uma equação $\sum_{i=0}^{n} a_i x_i = 0$ onde os a_i não são todos nulos.

Uma <u>transformação projetiva</u> $f: \mathbb{P}^n \to \mathbb{P}^n$ é por definição a transformação induzida a partir de uma transformação linear $A: \mathbb{F}_q^{n+1} \to \mathbb{F}_q^{n+1}$ invertivel, isto é, $\det A \neq 0$. Isto é $f((x_o:\ldots:x_n)) = (\sum_{j=0}^{n} a_{oj}x_j:\ldots: \sum_{j=0}^{n} a_{nj}x_j)$, $\det(a_{ij}) \neq 0$.

Um conjunto $K \subset \mathbb{P}^n$, $n \geq 2$ é chamado um <u>arco</u> se $\#K > n$ e K não contiver $n+1$ pontos contidos num mesmo hiperplano. Um exemplo de arco é o conjunto, em $\mathbb{P}^n$, $n \leq q$, dado por:

$$K_n = \{(1:\lambda:\ldots:\lambda^{n-1}),\ \lambda \in \mathbb{F}_q\} \cup \{(0:\ldots:0:1)\}$$

K_n é chamada a curva normal racional. Note que $\#K_n = q+1$.

Para ver que K_n é um arco, vamos explicitar a condição de $n+1$ pontos de $\mathbb{P}^n$ estarem num mesmo hiperplano. Se os pontos terem $(a_{io}:\ldots:a_{in})$, $i = 0,\ldots,n$ isso significa que $(a_{io},\ldots,a_{in}) \in \mathbb{F}_q^{n+1}$ estão num mesmo hiperplano, o que é equivalente a $\det(a_{ij}) \neq 0$. No caso de K_n essa última condição se checa usando o teorema de Vandermonde.

Pela Proposição (1.2) se $H = (h_{ij})$ $i=1,\ldots,n-d$ $j=1,\ldots,n$ é a matriz de controle de um $[n,d]$-código MDS então qualquer menor $(n-d) \times (n-d)$ de H tem determinante não nulo, isso significa que podemos obter um arco $K=\{(h_{1j};\ldots;h_{n-d,j}),$ $j=1,\ldots,n\}$ em $\mathbb{P}^{n-d-1}$. Reciprocamente dado um arco K em $\mathbb{P}^m$ com $\#K = n$, podemos construir um código MDS em $\mathbb{F}_q^n$ de dimensão $n-m-1$. Dai, a relação entre arcos e códigos MDS.

Vamos agora estudar mais cuidadosamente os arcos de $\mathbb{P}^n$. Diremos que um arco é <u>completo</u> se ele não for subconjunto próprio de outro arco. Diremos que um arco $K \subseteq \mathbb{P}^\infty$ é <u>máximo</u> se não houver nenhum arco em $\mathbb{P}^n$ com cardinalidade maior que $\#K$. A cardinalidade de um arco máximo será denotada por $m(n,q)$

Começaremos tratando o caso do plano, isto é, $n=2$.

(4.1) <u>Teorema</u> (Bose): $m(2,q) = \begin{cases} q+1 & q \text{ impar} \\ q+2 & q \text{ par} \end{cases}$

<u>Prova</u>: Seja K um arco e $k = \#K$. As retas ℓ de $\mathbb{P}^2$ cortam K em 0,1 ou 2 pontos. Se $\#(\ell \cap K) = 1$ dizemos que ℓ é uma unisecante a K e se $\#(\ell \cap K) = 2$ dizemos que ℓ é uma bisecante a K.

Seja $P \in K$ e $t(P)$ o número de unisecantes a K que contém P. As bisecantes a K contendo P são em número de $k-1$, uma para cada $Q \in K-\{P\}$. Como há $q+1$ retas por P (ex. 2) concluimos que $t(P) = t = q+2-k$.

Como $t(P)$ foi definido como a cardinalidade de um

conjunto, temos $t(P) \geq 0$, logo $k \leq q+2$. Vamos mostrar que $k \leq q+1$ se q é impar.

Suponha q impar e $k = q+2$ então $t = 0$ e logo $t(P) = 0$, para todo $P \in K$, o que significa que não há nenhuma unisecante a K. Seja $Q \in \mathbb{P}^2 \setminus K$ e m o número de retas passando por Q que intersectam K. Cada uma dessas m retas então contem exatamente dois pontos de K e esses pontos são distintos para retas distintas. Logo $k = 2m$ logo $q = 2(m-1)$ é par, absurdo.

Provamos então que $m(2,q) \leq \begin{cases} q+1 & q \text{ impar} \\ q+2 & q \text{ par} \end{cases}$

Se q é impar $\#K_2 = q+1$, logo $m(2,q) = q+1$.
Se q é par $K_2 \cup \{(0:1:0)\}$ é um arco, como se verifica facilmente e logo $m(2,q) = q+2$.

Notemos que K_2 é dado pelo conjunto dos pontos $(x_o:x_1:x_2)$ satisfazendo $x_2x_o = x_1^2$. Um conjunto de pontos C satisfazendo uma equação $f(x_o,x_1,x_2) = 0$ onde $f \in \mathbb{F}_q[x_o,x_1,x_2]$ é um polinomio homogeneo de grau 2, irredutível sobre $\mathbb{F}_q$ é chamado uma <u>conica</u>. Como f tem grau 2 podemos ver que uma reta corta C no máximo em 2 pontos (ver Capítulo V) logo toda conica é um arco. Pode-se mostrar também que toda conica tem $q+1$ pontos e temos

(4.2) <u>Teorema</u> (Segre): Se q é impar todo arco maximal é uma conica.

Não provaremos este teorema, ver [8].

Se q é par e C é uma conica existe um único ponto P de $\mathbb{P}^2 \setminus C$ tal que $C \cup \{P\}$ é um arco, este ponto é dito o núcleo de C. Porém o analogo ao teorema de Segre não vale em geral, para $q \geq 8$ existem arcos maximais em $\mathbb{P}^2$ que não são da forma $C \cup \{P\}$ com C uma conica e P seu núcleo. (Ver [8]).

Para classificar os arcos de $\mathbb{P}^2$ podemos nos restringir aos arcos completos. Esse problema ainda está em aberto mas temos alguns resultados parciais concernentes as possiveis cardinalidades de arcos completos.

(4.3) Proposição: Se K é um arco completo de cardinalidade k então $\frac{k(k-1)}{2} \geq \frac{q^2+q+1}{q+1}$.

Prova: Considere o conjunto das bisecantes a k, como uma bisecante está determinada pelos dois pontos de K que ela cortar, K tem $\frac{k(k-1)}{2}$ bisecantes. Cada bisecante tem $q+1$ pontos logo se $\#\mathbb{P}^2 > (q+1)\frac{k(k-1)}{2}$ existe $P \in \mathbb{P}^2$ que não está em nenhuma bisecante de K, logo $K \cup \{P\}$ é um arco e K não é completo. Como $\#\mathbb{P}^2 = q^2+q+1$, a proposição segue.

Muito mais difícil é uma cota superior para a cardinalidade de um arco completo não maximal.

(4.4) Teorema: Seja K um arco completo não maximal

(i) Se q é par, $\#K \leq q - \sqrt{q}+1$

(ii) Se q é impar, $\#K \leq q - \sqrt{q}/4+7/4$

(iii) Se q é primo, $\#K \leq 44q/45+2$

Os itens (i) e (ii) são devidos a Segre, ele provou-os relacionando, por um argumento engenhoso, a cardinalidade de K e o número de pontos racionais numa curva algébrica sobre um corpo finito e concluiu o resultado da chamada Hipótese de Riemann para curvas (ver Capítulo VI), os detalhes do argumento de Segre podem ser vistos em [8]. Thas, recentemente, deu uma prova elementar do item (i). O item (iii) foi provado pelo autor ([23]) utilizando-se dos resultados mais finos que a hipótese de Riemann que foram obtidos em [18].

Por outro lado conhecem-se arcos completos não maximais K satisfazendo $\#K = [\frac{q+\sqrt{q}}{2}]$ e $\#K \leq q^{1-1/10}$ (ver [19] e [24], onde outros exemplos também são dados). E também com $K=q-\sqrt{q}+1$ se q é um quadrado (ver [26]).

E o caso $n \geq 3$? Vamos estuda-lo reduzindo-o ao caso $n = 2$. Seja $V \subset \mathbb{P}^n$ um subespaço de dimensão $n-3$ e $W \subset \mathbb{P}^n$ um subespaço de dimensão 2 tal que $V \cap W = \phi$. Definimos $\pi: \mathbb{P}^n \setminus V \to W$, chamada a <u>projeção</u> sobre W ao longo de V, da seguinte maneira. Dado $P \in \mathbb{P}^n \setminus V$ existe um único subespaço V_P de dimensão $n-2$ contendo V e P. Temos ainda que $V_P \cap W$ consiste de um único ponto e é esse ponto que chamamos $\pi(P)$. (Ver ex.3)

Então W como tem dimensão 2 pode ser identificado com $\mathbb{P}^2$. Sjea $K \subsetneq \mathbb{P}^n$ um arco e $P_1,\ldots,P_{n-2} \in K$, defina V como o menor subespaço contendo $P_1,\ldots,P_{n-2}$ e escolha W de dimensão 2 com $V \cap W = \phi$. Ve-se facilmente que $\pi(K\setminus\{P_1,\ldots,P_{n-2}\})$

é um arco em $W = \mathbb{P}^2$. Essa construção permitiu Thas provar o seguinte teorema

(4.5) Teorema: (Thas) Suponha q impar, $q > (4n-5)^2$. Então

(i) $m(n,q) = q+1$

(ii) Se $K \subseteq \mathbb{P}^n$ é um arco maximal então $K = f(K_n)$ onde f é uma transformação projetiva.

(iii) Se K é um arco completo não maximal então $\#K \leq q - \sqrt{q}/4 + n - 1/4$.

A prova completa deste teorema pode ser vista em [20]. A idéia é usar projeções variando os pontos $P_1,\ldots,P_{n-2}$ como acima e usar os teoremas mencionados acima para o caso plano. No caso em que além de $q > (4n-5)^2$, q impar q for primo então podemos melhorar (4.5)(iii) para $\#K \leq 44q/45 + n+2$ usando o Teorema (4.4)(iii).

conjectura-se que $m(n,q) = \begin{cases} q+1, & 3 \leq n \leq q \\ n+1, & n > q \end{cases}$

além dos casos cobertos pelo Teorema (4.5)(i) essa conjectura foi provada apenas para $n = 3,4,5$ $q \geq n+1$ e $q \leq 11$, $n \leq q$, ver [15]. Sabe-se que em geral $m(n,q) \leq q+n-4$, ver [15].

EXERCÍCIOS:

1. Prove que $\#\mathbb{P}^n = q^n+q^{n-1}+\ldots+1$.

2. Seja $(\mathbb{P}^n)^V$ o conjunto de hiperplanos de $\mathbb{P}^n$. Associe a $\sum_{i=0}^{n} a_i x_i = 0$ o ponto $(a_o:\ldots:a_n) \in \mathbb{P}^n$. Com isso $(\mathbb{P}^n)^V$ admite uma estrutura de espaço projetivo. Mostre que se $P \in \mathbb{P}^n$ o conjunto dos hiperplanos por P formam um hiperplano em $(\mathbb{P}^n)^V$. Conclua que existem $q^{n-1}+q^{n-2}+\ldots+1$ hiperplanos passando por P.

3. Complete os detalhes da construção de projeção definida no texto.

4. Prove que $m(n,q) \leq q+n+4$.

5. Uma calota $C \subset \mathbb{P}^n$ é um conjunto que não contém três pontos colineares (logo para $n=2$ uma calota é um arco). Associe um código a uma calota e discuta as suas propriedades. Generalize.

6. Prove que um arco plano tem $k(q+2-k)$ unisecantes.

7. Verifique que para $q = 2,4$ todo arco maximal é uma conica mais seu núcleo.

CAPÍTULO V

CÓDIGOS DE GOPPA

Nesse capítulo descreveremos duas classes de códigos que chamaremos de códigos de Goppa. Essas duas classes serão englobadas em uma classe mais ampla no próximo capítulo. Esses códigos tem uma excelente performance.

§1. Seja $g(x) \in \mathbb{F}_{q^m}[x]$, mônico de grau t e $L = \{\gamma_0, \gamma_1, \ldots, \gamma_{n-1}\} \subseteq \mathbb{F}_{q^m}$, $g(\gamma_i) \neq 0$. Definimos o código de Goppa $C(L,g) \subseteq \mathbb{F}_q^n$ como o conjunto $\{(c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n, \sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} \equiv 0 \pmod{g(x)}\}$. A condição $\sum \frac{c_i}{x-\gamma_i} \equiv 0 \pmod{g(x)}$ significa que ao escrevermos a função racional do lado direito como $a(x)/b(x)$, $a,b \in \mathbb{F}_{q^m}[x]$ teremos $(a(x),b(x)) = 1$ e $a(x)$ divisivel por $g(x)$.

(5.1) Teorema: $\dim C(L,g) \geq n-mt$, $w(C(L,g)) \geq t+1$.

Prova: Temos que:

$$\frac{1}{x-\gamma_i} \equiv \frac{-1}{g(\gamma_i)} \left(\frac{g(x)-g(\gamma_i)}{x-\gamma_i}\right) \pmod{g(x)}$$

logo $(c_0, \ldots, c_{n-1}) \in C(L,g)$ se e só se

$$\sum_{i=0}^{n-1} c_i \frac{(g(x)-g(\gamma_i))}{g(\gamma_i)(x-\gamma_i)} \equiv 0 \pmod{g(x)} \qquad i=0,\ldots,n-1$$

Por outro lado, $G_i(x) = \dfrac{g(x)-g(\gamma_i)}{g(\gamma_i)(x-\gamma_i)}$ é um polinomio de grau $t-1$, que podemos escrever como $G_i(x) = \sum_{j=0}^{t-1} g_{ij}x^j$, $g_{ij} \in \mathbb{F}_{q^m}$.

Logo, em particular, $\Sigma c_i G_i(x)$ é um polinomio de grau $\leq t-1$ e como $g(x)$ tem grau t, se $g(x)$ divide $\Sigma c_i G_i(x)$ então $\Sigma c_i G_i(x) = 0$, logo $(c_o,\ldots,c_{n-1}) \in C(L,g)$ se e só se

$$(*) \qquad \sum_{i=0}^{n-1} c_i g_{ij} = 0 \qquad j = 0,\ldots,t-1.$$

$\mathbb{F}_{q^m}$ é um espaço m-dimensional sobre $\mathbb{F}_q$ logo tem uma base $\alpha_1,\ldots,\alpha_m$. Podemos escrever $g_{ij} = \sum_{k=1}^{m} \lambda_{ijk}\alpha_k$, $\lambda_{ijk} \in \mathbb{F}_q$. As equações (*) se tornam então:

$$(**) \qquad \sum_{i=0}^{n} c_i \lambda_{ijk} = 0, \qquad j = 0,\ldots,t-1, \quad k = 1,\ldots,m.$$

Isso mostra que $\dim C(L,g) \geq n-mt$. Escolhendo-se um subconjunto máximo linearmente independente das equações (**) podemos construir uma matriz de controle para $C(L,g)$, mas não precisaremos disto aqui.

Para mostrar a estimativa do peso seja $c=(c_o,\ldots,c_{n-1}) \in C(L,g)$ e $M = \{i \mid c_i \neq 0\}$ então

$$\sum_{i=0}^{n-1} \frac{c_i}{x-\gamma_i} = \sum_{i\in M} c_i \prod_{j\in M\setminus\{i\}} (x-\gamma_j) \Big/ \prod_{i\in M} (x-\gamma_i).$$

O numerador desta expressão tem que ser divisivel por $g(x)$, mas o grau do numerador é no máximo $\#M-1$, logo $\#M-1 \geq t$ ou $\#M \geq t+1$. Porém $\#M = |c|$, logo $w(C(L,g)) \geq t+1$, como queriamos demonstrar.

A idéia da demonstração que o peso de $C(L,g)$ é pelo menos $t+1$ pode ser refinada para mostrar que existe uma sequência de códigos de Goppa tão perto quando se queira da cota de Varshomov-Gilbert (Teorema (2.2)).

(5.2) Teorema: Existe uma sequência de códigos de Goppa sobre $\mathbb{F}_q$ que atinge assintoticamente a cota de Varshomov-Gilbert.

Prova: Fixe $n = q^m, t, w$ e ponha $L = \mathbb{F}_{q^m}$. Vamos tentar construir $C(L,g)$ com peso $\geq w$ e g irredutível de grau t. Se $c = (c_0,\ldots,c_{n-1}) \in \mathbb{F}_q^n$ é tal que $|c| = j < w$ então, como na prova do Teorema (5.1), $g(x)$ deve dividir um polinomio de grau $j-1$. Como um polinomio de grau $j-1$ tem, no máximo $[\frac{j-1}{t}]$ divisore de grau t devemos excluir $[\frac{j-1}{t}]$ polinomios para cada $c \in \mathbb{F}_q^n$ com $|c| = j$. Temos então que excluir $\sum_{j=1}^{w-1} [\frac{j-1}{t}](q-1)^j\binom{n}{j}$ polinomios. Porém (ver Capítulo II)

$$\sum_{j=1}^{w-1} (\frac{j-1}{t})(q-1)^j\binom{n}{j} \leq \frac{w}{t} V_q(n,w-1).$$

Se provarmos que $\#[g(x) \in \mathbb{F}_{q^m}[x]$, grau $g(x) \leq t$, g irredutível$] = f(t)$ é tal que $f(t) > \frac{w}{t} V_q(n,w-1)$, então tal

código existirá. Pode-se provar (ver [12]) que $f(t) > \frac{1}{t} q^{mt}(1-q^{-1/2mt+1})$. Basta então exigir que

$$q^{mt}(1-q^{-1/2mt+1}) > w\, V_q(n,w-1).$$

Se $w = [\delta n]$ e n é grande isso valerá se $\lim_{n\to\infty} \frac{mt}{n} > H_q(\delta)$. Mas $\dim C(L,g) \geq n-mt$ logo $\frac{\dim C(L,g)}{n} = 1 - \frac{mt}{n}$. Podemos então escolher t tal que $H_q(\delta) < \frac{mt}{n} < H_q(\delta) + \varepsilon$ e teremos que $\lim_{n\to\infty} C(L,g) \geq 1-H_q(\delta)-\varepsilon$ e $C(L,g)$ está próximo da cota de Varshomov-Gilbert.

Códigos de Goppa tem também um algoritmo de decodificação similar ao dos códigos BCH. Sejam $L = \{\gamma_0,\ldots,\gamma_{n-1}\}$ e $g \in \mathbb{F}_{q^m}[x]$ monico de grau t e $C = C(L,g) \subseteq \mathbb{F}_q^n$. Seja $r = (r_0,\ldots,r_{n-1})$ a mensagem recebida e $c = (c_0,\ldots,c_{n-1})$ a mensagem enviada, suponha que $|c-r| \leq t/2$. Seja $(e_0,\ldots,e_{n-1}) = r-c$. Definimos

$M = \{i \mid e_i \neq 0\}$

$e = \#M$

$$\ell(x) = \prod_{i\in M} (x-\gamma_i)$$

$$s(x) = \sum_{i\in M} e_i \prod_{j\in M\setminus\{i\}} (x-\gamma_j)$$

Exatamente como no caso dos códigos BCH e nosso problema é calcular ℓ, s conhecendo apenas r.

$$\text{Seja} \quad S(x) = \sum_{i=0}^{n-1} r_i \frac{-1}{g(\gamma_i)} \frac{(g(x)-g(\gamma_i))}{x-\gamma_i}$$

$$\text{então} \quad S(x) \equiv \sum \frac{r_i}{x-\gamma_i} \equiv \sum \frac{e_i}{x-\gamma_i} \pmod{g(x)}.$$

Temos então que:

$$S(x)\ell(x) \equiv \sum_{i=0}^{n-1} \frac{e_i}{x-\gamma_i} \prod_{j\in M} (x-\gamma_j) \equiv$$

$$\equiv \sum_{i\in M} e_i \prod_{j\in M\setminus\{i\}} (x-\gamma_j) \equiv s(x) \pmod{g(x)}$$

$S(x)$ é conhecido, $g(x)$ também e temos que achar ℓ, s de grau $< t/2$ tais que $S(x)\ell(x) \equiv s(x) \pmod{g(x)}$ e lembramos que o grau de $g(x)$ é t. Isso é uma generalização do problema tratado no caso dos códigos BCH onde tinhamos $g(x) = x^{2n+1}$. A solução neste caso é uma generalização direta do que fizemos anteriormente.

§2. Seja $f(x,y) \in \mathbb{F}_q[x,y]$ um polinomio de grau d, irredutível como polinomio em $\bar{\mathbb{F}}_q[x,y]$. Dizemos que f é absolutamente irredutível. Sejam $P_i = (x_i, y_i)$, $i=1,\ldots,N$ as soluções em $\mathbb{F}_q^2$ da equação $f(x,y) = 0$. Chamaremos os P_i's de pontos racionais da curva $f = 0$.

Definimos $V_m = \{g \in \mathbb{F}_q[x,y]$, grau $g \le m\}$. V_m é um espaço vetorial sobre $\mathbb{F}_q$ de dimensão $\binom{m+2}{2}$. Definimos também $\phi_m: V_m \to \mathbb{F}_q^N$ por

$$\phi_m(g) = (g(P_1),\ldots,g(P_N)).$$

O código de Goppa $C_m(f)$ é definido então como a imagem de ϕ_m.

Para analisar os códigos $C_m(f)$ vamos assumir de agora em diante que $m < N/d$. Precisaremos também do seguinte resultado, que é uma forma fraca do Teorema de Bezóut ([5]).

(5.3) Lema: Sejam $f,g \in k[x,y]$, k um corpo. Seja d o grau de f e m o grau de g. Suponhamos f absolutamente irredutível. Se f não divide g então o número de soluções de $f(x,y) = g(x,y) = 0$ é no máximo md

(5.4) Teorema: Suponha $m < N/d$, então:

$$\dim C_m(f) = \begin{cases} \binom{m+2}{2}, & m < d. \\ md - \frac{d(d-3)}{2}, & m \geq d. \end{cases}$$

e $w(C_m(f)) \geq N-md$.

Prova: Vamos primeiro calcular $\dim C_m(f)$. Vejamos então qual é o núcleo de ϕ_m. Se $\phi_m(g) = 0$ então $f = g = 0$ tem N soluções, como estamos assumindo que $md < N$, isso implica, pelo Lema (5.3) que f divide g. Se $m < d$ então $g = 0$ e logo ϕ_m é injetivo para $m < d$ o que prova a formula enunciada neste caso. Para $m \geq d$ e núcleo de ϕ_m é o conjunto $\{fh,\ h \in \mathbb{F}_q[x,y], \text{grau } h \leq m-d\}$, que é isomorfo (via $f.h \to h$) a V_{m-d} logo a dimensão do núcleo de ϕ_m é $\binom{m-d+2}{2}$ logo, para $m \geq d$

$$\dim C_m(f) = \binom{m+2}{2} - \binom{m-d+2}{2} = md - \frac{d(d-3)}{2} .$$

Seja agora $c \in C_m(f)$ com $|c| = r$ e seja $g \in V_m$ tal que $\phi_m(g) = c$. Então g tem $N-r$ zeros em comum com f. Se $c \neq \bar{0}$ devemos ter que f não divide g, logo pelo Lema (5.3) temos $N-r \leq md$ ou $r \geq N-md$, o que prova o teorema.

Pelo teorema, para d e m fixos a dimensão de $C_m(f)$ não depende de N (se $N > md$), então para achar o melhor código entre os $C_m(f)$ é suficiente achar f tal que N é máximo. Discutiremos esse problema no próximo capítulo (mas, por outro lado, veja o exercício 3).

EXERCÍCIOS:

1. Mostre que o código BCH de comprimento n e distância designada δ é o código de Goppa $C(L,g)$ onde

$$L = \{1, \beta^1, \beta^2, \ldots, \beta^{(n-1)}\}, \quad g = x^{\delta-1}.$$

2. Mostre que se $L = \{1, \alpha, \ldots, \alpha^{n-1}\}$, α raiz primitiva n-ésima da unidade em $\mathbb{F}_{q^m}$. Seja $g(x) \in \mathbb{F}_{2^m}[x]$. Prove que se $C(L,g)$ é ciclico então $g(x) = x^t$ para algum t.

3. Seja $f(x,y) = x^4+y^4-1$ sobre $\mathbb{F}_9$. Prove que $C_1(f)$ é um $[24,3]$-código de peso 21 e $C_m(f)$ é um $[24,4m-2]$-código de peso $24-4m$ para $m = 2,\ldots,5$ (sugestão: calcule o peso de $\varphi_m(g)$, $g=y, xy$, $xy(x+y)$, $xy(x+y)(x-y)$, $xy(x+y)(x-y)(x+iy)$, $i^2=-1$).

CAPÍTULO VI

CÓDIGOS DE GOPPA OUTRA VEZ

Neste capítulo daremos a construção de uma família de códigos construida por Goppa ([6], ver também [10]), relacionada com curvas sobre corpos finitos. Essa relação tem provado ser muito importante para as duas áreas. Vamos assumir nesse capítulo que o leitor tem conhecimentos sobre curvas algébricas (ver [5] ou [7]).

Seja X uma curva algébrica de genero g definida sobre $\mathbb{F}_q$. Um resultado importante que será usado no que segue é o seguinte

(6.1) Teorema (Weil): $\quad |\#X(\mathbb{F}_q) - (q+1)| \leq 2g\, q^{1/2}$

Esse resultado é conhecido como a hipótese de Riemann para curvas. Uma demonstração pode ser vista em [2] ou [25].

Sejam $P_1,\ldots,P_n \in X(\mathbb{F}_q)$, pontos distintos e G um divisor de X suposto positivo. Suporemos também que nenhum dos P_i's está no suporte de G. Pomos $D = \sum_{i=1}^{n} P_i$.

Definimos os códigos de Goppa $C(D,G)$, $C'(D,g) \subseteq \mathbb{F}_q^n$ da seguinte maneira:

$C(D,g)$ = imagem de $\phi_{D,G}$

$\phi_{D,G}: L(G) \to \mathbb{F}_q^n$, $\phi_{D,G}(f) = (f(P_1),\ldots,f(P_n))$

$C'(D,G)$ = imagem de $\psi_{D,G}$

$\psi_{D,G}: \Omega'(-G+D) \to \mathbb{F}_q^n$

$\psi_{D,G}(w) = (\mathrm{res}_{P_1} w,\ldots,\mathrm{res}_{P_n}(w))$

Lembramos que $L(G) = \{f$, função em $X, (f)+G \geq 0\}$ $\Omega'(-G+D) = \{w$, diferencial em $X, (w)-G+D \geq 0\}$ e $\mathrm{res}_P w$ denota o residuo da forma diferencial w em P. $\ell(G) = \dim L(G)$.

O código $C(D,G)$ generaliza os códigos $C_m(f)$ do Capítulo V. $C_m(f) = C(D,G)$ onde X é a curva plana $f = 0$, $P_1,\ldots,P_n$ são os pontos afins de X e $G = mH$ onde H é o divisor cortado pela reta no infinito em X.

O código $C'(D,G)$ generaliza os códigos $C(L,g)$ no caso particular que $L \subseteq \mathbb{F}_q$, $g \in \mathbb{F}_q[x]$. Neste caso $X = \mathbb{P}^1$, $L = \{P_1,\ldots,P_n\}$ e G é o divisor de zeros de g. Deixamos para o leitor generalizar a definição dos $C'(D,G)$ de modo a englobar todos os $C(L,g)$.

(6.2) Teorema (Goppa): (i) Se grau $G < n$ então $\dim C(D,G) = \ell(G) \geq$ grau $G+1-g$, $w(C(D,G)) \geq n-$grau G.

(ii) Se $2g-2 <$ grau $G < n+g-1$ então

dim $C'(D,G)$ = dim $\Omega'(-G+D) \geq$ n-grau G+g-1. $w(C'(D,G)) \geq$ $\geq$ grau G-2g+2.

Prova: (i) Vamos mostrar que $\varphi = \varphi_{D,G}$ é injetivo. De fato, se $\varphi(f) = 0$ então f tem n zeros em $P_1,\ldots,P_n$ mas $f \in L(G)$, logo f tem no máximo grau G polos. Como grau $G < n$, temos que $f = 0$. Logo dim $C(D,G) = \ell(G)$. A desigualdade segue do teorema de Riemann-Roch. Do mesmo modo se $|\varphi(f)| = r$ então f tem pelo menos n-r zeros e logo $n-r \leq$ $\leq$ grau G. Isso prova que $w(C(D,G)) \geq$ n-grau G.

(ii) Notemos que se $w \in \Omega'(D-G)$ então w não tem polos fora de $\{P_1,\ldots,P_n\}$ e tem no máximo polos simples nestes pontos.

Vamos mostrar que $\psi = \psi_{D,G}$ é injetiva. Se $w \neq 0$ e $\psi(w) = 0$ então w não tem polos, mas teremos $(w) \geq G$ e como grau $G > 2g-2$, isso é um absurdo, logo φ é injetiva e dim $C'(D,G)$ = dim $\Omega'(D-G) \geq$ n-grau G+g-1 por Riemann-Roch. Similarmente ao que já foi feito vemos também que $w(C'(D,G)) \geq$ $\geq$ grau G-2g+2.

Se $f_1,\ldots,f_r$, $r = \ell(G)$ é uma base de L(G) então a matriz $(f_i(P_j))$ é uma matriz geradora para C(L,G). Similarmente se $w_1,\ldots,w_s$ é uma base de $\Omega'(D-G)$ então a matriz $(\mathrm{res}_{P_j}(w_i))$ gera $C'(L,G)$. Quanto ao controle lembremos a formula dos residuos:

$$\sum_{P \in X} \mathrm{res}_P w = 0$$

para qualquer forma diferencial w em X. Então temos que se $f \in L(G)$ e $w \in \Omega'(D-G)$ temos

$$0 = \sum_{P \in X} \operatorname{res}_P fw = \sum_{i=1}^{n} f(P_i) \operatorname{res}_{P_i} w \qquad (*)$$

Quando $2g-2 <$ grau $G <$ n, contando as dimensões verifica-se rapidamente que as equações (*) para $f=f_1,\ldots,f_r$ nos dá uma matriz de controle para $C'(D,G)$, isto é, a matriz de controle de $C'(D,G)$ é a matriz geradora de $C(D,G)$. Podemos ver também por (*) que a matriz geradora de $C'(D,G)$ é a matriz de controle de $C'(D,G)$. C e C' são duais no sentido do ex. 6 do Capítulo I.

(6.3) Proposição: Nas hipóteses do Teorema (6.2) se $g=0$ os códigos $C(D,G)$, $C'(D,G)$ são MDS.

Prova: Temos, para $C(D,G)$ que, pelo Teorema (6.2)

$$w(C(D,G)) \geq n-\text{grau } G =$$

$$= n-(\text{grau } G+1)+1 \geq n-\dim C(D,G)+1.$$

Pela cota de Singleton (Corolário 1.3), temos também

$$w(C(D,G)) \leq n-\dim C(D,G)+1.$$

Logo vale a igualdade e $C(D,G)$ é M.D.S.. A prova para $C'(D,G)$ é analoga.

Recordemos (ver [5]) que quando $g=1$, podemos definir uma lei de grupo abeliana $\oplus$ em X, fixando um ponto arbitrá-

ria $0 \in X$, da seguinte maneira. Pomos $P \oplus Q = R$ se R é o único ponto de X tal que $P+Q-R-0 = (f)$ para alguma função f em X.

Se $G = \sum_{i=1}^{m} n_i Q_i$, definimos $P_G = n_1 Q_1 \oplus \ldots \oplus n_m Q_m$,

então temos:

(6.4) Proposição: (Driencourt-Michon) Nas hipóteses do Teorema (6.2) se $g=1$, então: $\dim C(D,G) =$ grau G, $\dim C'(D,G) =$ $n-$grau G. Se existirem $i_1,\ldots,i_r$, $r =$ grau G, $i_1,\ldots,i_r \in$ $\in \{1,\ldots,n\}$ tais que $P_G = P_{i_1} \oplus \ldots \oplus P_{i_r}$ então $w(C(D,G)) =$ $n-$grau G, $w(C'(D,G)) =$ grau G. Caso contrário, $C(D,G)$, $C'(D,G)$ são MDS.

Prova: As igualdades nas dimensões seguem do Teorema de Riemann-Roch. Se existir $f \in L(G)$ tal que $|\varphi(f)| = n-$grau G. Isso significa que f tem grau G zeros entre $P_1,\ldots,P_n$. Sejam $P_{i_1},\ldots,P_{i_r}$ estes zeros, então $(f) \geq P_{i_1} + \ldots + P_{i_r} - G$, como grau$(f) = 0$ isso implica que $(f) = P_{i_1} + \ldots + P_{i_r} - G$ o que equivale a $P_G = P_{i_1} \oplus \ldots \oplus P_{i_r}$. Isso completa a demonstração no que concerne a $C(D,G)$. O caso de $C'(D,G)$ é analogo.

Driencourt e Michon deram também no caso $g=1$ um eficiente algoritmo de decodificação (ver [3]).

Suponhamos agora que $\{P_1,\ldots,P_n\} = X(\mathbb{F}_q)$. Temos então que

$$\frac{\dim C+w(C)}{n} \geq 1 - \frac{g-1}{n} \quad \text{pelo Teorema (6.2)}$$

para $C = C(D,G)$ ou $C'(D,G)$. Uma maneira de se obter bons códigos é maximizar este número. Par isso temos que maximizar n/g para $\mathbb{F}_q$ fixo. Pelo Teorema de Weil (6.1) temos $n/g \leq \frac{q+1}{g} + 2q^{1/2}$. Esse resultado nem sempre é o melhor possivel, especialmente para g grande. De fato Drinfeld e Vladut ([4]) mostraram que $n/g \leq q^{1/2}-1+f(g)$ onde $f(g) \to 0$ quando $g \to \infty$. Por outro lado Ihara ([9]) e Tsfasman-Vladut-Zink ([22]) construiram uma sequência de curvas para cada q quadrado, $\sqrt{q} \geq 7$, tendo $n/g \to q^{1/2}-1$. Esses códigos são assintóticamente os melhores conhecidos estando inclusive acima da cota de Varshamov-Gilbert. Outros autores mostraram também que estes exemplos podem ser calculados eficientemente [27]. Para outros resultados sobre o número de pontos de uma curva sobre um corpo finito, ver [9], [16] e [18].

REFERÊNCIAS

[1] Berlekamp,E.R., Algebraic Coding Theory, McGraw-Hill New York, 1968.

[2] Bombieri,E., Hilbert's 8^{th} problem an analogue, in Mathematical developments arising from Hilbert's problems, F. Browder, ed., Proc. Sym. Pure Math. vol. 28, AMS, 1976, 269-274.

[3] Driencourt,Y., Michon,J.F., Binary elliptic codes, Preprint, Universite de Nice, 1985.

[4] Drinfeld,V.G., Vladut,S.G., Sobre o número de pontos de uma curva algébrica (em russo) Func. Anal. and Appl. 17 (1983), 68-69.

[5] Fulton,W., Algebraic curves, Benjamin, New York, 1969.

[6] Goppa,V.D., Algebraico - Geometric codes, Math. URSS Izvestiya, 21 (1983), 75-91.

[7] Harshorne,R., Algebraic Geometry, Springer, New York, 1977.

[8] Hirschfeld,J.W.P., Projective Geometries over finite fields, Clarendon Press, Oxford, 1979.

[9] Ihara,Y., Some remarks on the number of rational points of algebraic curves over finite fields J. Fac. Sci. Tokio, Ser. IA, Math. 28 (1981), 721-724.

[10] Lachaud,G. Les codes Géométriques de Goppa, Asterisque 133-134 (1986), 189-207.

[11] Lidl,R. Niederreiter,H., Finite fields, Addison-Wesley Reading, 1983.

[12] Van Lint,J.H., Introduction to coding theory, Springer, New York, 1982.

[13] Manin,Y.I., What is the maximum number of points on a curve over $\mathbb{F}_2$? J. Fac. Sci. Tokio, Ser. IA, Math. 28 (1981), 715-720.

[14] Mc Eliece, The theory of information and coding, Addison-Wesley, Reading, 1977.

[15] Mc Williams,F.J., Sloane,N. .A., The theory of error correcting codes, North Holland, Amsterdam 1977.

[16] Serre,J.P., Sur le nombre des points rationneles d'une courbe algebrique sur un corps fini, C.R. Acad. Sci. Paris t. 296, Serie I (1983) 397-402.

[17] Sloane,N.J.A., Error correcting codes and cryptography, in the Mathematical Gardner, D.A. Klarner, ed., Wadsworth, Belmont 1981, pp. 346-382.

[18] Stöhr,K.O., Voloch,J.F., Weierstrass points and curves over finite fields. Proc. Lon. Math. Soc. (3)52 (1986), 1-19.

[19] Szönyi,T., Small complete arcs in Galois Planes, Geom. Dedicata 18 (1985), 161-172.

[20] Thas,J.A., Normal rational curves and k-arcs in Galois Spaces, Rend. di Mat. (3-4) 1 (1968), 331-334.

[21] Thompson,T.M., From error-correcting codes through sphere packings to simple groups. Mathematical Association of America, 1983.

[22] Tsfasfman,M.A., Vladut,S.G., Zink,I., Modular curves, Shimura curves and Goppa codes better than Varshamov-Gilbert bound, Math. Nach. 109 (1982), 21-28.

[23] Voloch,J.F., Arcs in projective planes over prime fields, J. of Geometry, a aparecer.

[24] Voloch,J.F., On the completeness of certain plane arcs, Europ J. of Combinatorics, a aparecer.

[25] Weil,A., Courbes algébriques et variétés abeliénnes Hermann, Paris, 1971.

[26] Fischer,J.C., Hirschfeld,J.W.P. e Thas,J.A., Complete arcs in planes of square order, Annals of Discrete Mathematics 30 (1986), 243-250.

[27] Vladut,S.G. e Manin,Y., Códigos lineares e curvas modulares (em russo), pré-publicação.

Impresso na Gráfica do
impa