2
Códigos Lineares

Neste capítulo introduziremos conceitos básicos da teoria de códigos e estabeleceremos algumas propriedades. Um estudo mais profundo desta teoria pode ser encontrado em (Lint).

2.1
Códigos

Vamos começar fixando algumas notações:

• $\mathbb{F}_q$ denotará um corpo finito com q elementos.

• $\mathbb{F}_q^n$ será um espaço vetorial sobre $\mathbb{F}_q$ de dimensão n, cujos elementos serão denotados como n-uplas $a = (a_1, a_2, ..., a_n)$ onde $a_i \in \mathbb{F}_q$.

Definição 2.1 *Um código linear C é um subespaço vetorial de $\mathbb{F}_q^n$ e seus elementos são chamados palavras do código.*

Associado a um código C temos dois parâmetros: n que será chamado de comprimento do código C e a dimensão k de C como $\mathbb{F}_q$-espaço vetorial que será chamada de dimensão do código. Um $[n, k]$-código é um código de comprimento n e dimensão k.

Além do comprimento e da dimensão do código, temos outro parâmetro importante: a distância mínima.

Para introduzirmos este conceito devemos definir uma distância em $\mathbb{F}_q^n$.

Definição 2.2 *Sejam $a = (a_1, ..., a_n), b = (b_1, ..., b_n) \in \mathbb{F}_q^n$. Definimos a distância de Hamming entre a e b como segue:*

$$d(a, b) = |\{i; a_i \neq b_i\}|.$$

A distância de Hamming define uma métrica em $\mathbb{F}_q^n$, logo em particular vale a desigualdade triangular

$$d(a, c) \leq d(a, b) + d(b, c) \quad \text{onde } a, b, c \in \mathbb{F}_q^n.$$

A distância mínima $d(C)$ de um código não-nulo C é definida como

$$d(C) = min\{d(a,b) \mid a,b \in C \; e \; a \neq b\}.$$

Também podemos definir o peso $w(a)$ de um elemento $a \in \mathbb{F}_q^n$ como sua distância à palavra nula, ou seja:

$$w(a) = d(a,0) = |\{i; a_i \neq 0\}|.$$

Como $d(a,b) = d(a-b,0) = w(a-b)$, podemos reescrever a distância mínima da seguinte forma:

$$d(C) = min\{w(c) \mid 0 \neq c \in C\}.$$

Definição 2.3 *Um $[n,k]$-código com distância mínima d é chamado um $[n,k,d]$-código.*

Na prática, ao utilizar códigos para transmitir informação, a palavra recebida difere da palavra transmitida (estes erros são gerados pela canal utilizado na transmissão) e por isso é necessário poder identificar estes erros e corrigí-los. Para isto é desejável trabalhar com códigos cuja distância mínima seja a maior possível já que se C é um código com distância mínima d, então dizemos que C pode corrigir t erros onde $t := \lfloor (d-1)/2 \rfloor$ (como sempre $\lfloor x \rfloor$ denota a parte inteira do número real x).

Associado a um código C temos o chamado código dual $C^\perp$ definido por:

$$C^\perp = \{u \in \mathbb{F}_q \mid u \cdot c = 0, \forall c \in C\}$$

onde $\cdot$ denota o produto interno usual em $\mathbb{F}_q^n$, ou seja,

$$a \cdot b \; = \sum_{i=1}^{n} a_i b_i$$

onde $a = (a_1, ..., a_n)$, $b = (b_1, ..., b_n) \in \mathbb{F}_q^n$.

Dizemos que C é autodual se $C = C^\perp$ e C será dito ortogonal se $C \subseteq C^\perp$.
Note que o dual de um $[n,k]$-código é um $[n, n-k]$-código e que $(C^\perp)^\perp = C$.
Em particular a dimensão de código autodual é $n/2$.

Uma forma simples de escrevermos códigos explicitamente é escrevermos a base de C como espaço vetorial sobre $\mathbb{F}_q$.

Definição 2.4 *Seja C um $[n,k]$-código sobre $\mathbb{F}_q$. Uma matriz geradora de C é uma matriz $k \times n$, cujas linhas formam uma base do espaço vetorial C. Uma matriz H geradora de $C^{\perp}$ é dita uma matriz de paridade de C.*

H é uma matriz $(n-k) \times n$ de posto $n-k$ tal que

$$C = \{u \in \mathbb{F}_q^n | H \cdot u^t = 0\}$$

(onde u^t denota a transposta de u). Na verdade, uma matriz de paridade checa se um vetor $u \in \mathbb{F}_q^n$ é uma palavra do código ou não.

Como foi comentado anteriormente, um dos problemas da teoria de códigos é a construção de códigos cuja dimensão e distância mínima sejam grandes em comparação com seu comprimento. Entretanto, existem algumas restrições. Na verdade, se a dimensão de um código é grande, então sua distância mínima deverá ser pequena.

Proposição 2.1.1 (Limitação de Singleton) *Para um $[n,k,d]$-código C em $\mathbb{F}_q^n$ temos que*

$$k + d \leq n + 1.$$

Prova:

Considere um subespaço linear $W \subseteq \mathbb{F}_q^n$ dado por

$$W = \{(a_1, ..., a_n) \in \mathbb{F}_q^n \mid a_i = 0, \forall i \geq d\}.$$

Note que para $a \in W$ temos que $w(a) \leq d-1$, portanto $W \cap C = \{0\}$.
Como $dim\, W = d-1$ temos

$$\begin{aligned} dim\, C + dim\, W &= dim\, (C+W) + dim\, (C \cap W) \\ &= dim\, (C+W) \\ &\leq n. \end{aligned}$$

Logo $k + d - 1 \leq n$, isto é, $k + d \leq n + 1$.

□

Códigos satisfazendo a igualdade na cota de Singleton, ou seja, onde $k+d = n+1$, são de certa forma excelentes, tais códigos são chamados códigos

MDS (MDS vem do inglês *maximum distance separable*). Se $n \leq q+1$, existem códigos MDS sobre $\mathbb{F}_q$ para todas dimensões $k \leq n$.

A limitação de Singleton não envolve o tamanho do alfabeto. Existem outras limitações superiores para os parâmetros k e d que envolvem o tamanho do alfabeto. Essas limitações são muito boas se n é grande em relação a q (ver por exemplo (Lint)).

Em geral é mais difícil obter uma limitação inferior para a distância mínima de um código, tal limitação somente é conhecida para algumas classes de códigos, por exemplo: códigos BCH ou códigos clássicos de Goppa. Uma das razões de nosso interesse em códigos geométricos de Goppa é que para essa classe de códigos uma boa limitação inferior para a distância mínima é conhecida.

2.2 Exemplos de Códigos

Uma classe importante de códigos são os chamados códigos de Reed-Solomon e veremos que tais códigos são MDS.

Sejam $n = q-1$ e $\beta \in \mathbb{F}_q$ um elemento primitivo do grupo multiplicativo $\mathbb{F}_q^*$, isto é, $\mathbb{F}_q^* = \{\beta, \beta^2, ..., \beta^n = 1\}$.
Seja $k \in \mathbb{Z}$ tal que $1 \leq k \leq n$ e consideremos o seguinte espaço vetorial:

$$\mathcal{L}_k = \{f \in \mathbb{F}_q[X] \mid deg\, f \leq k-1\}.$$

Este espaço vetorial tem dimensão exatamente k e a aplicação de avaliação $av : \mathcal{L}_k \longrightarrow \mathbb{F}_q^n$ dada por

$$av(f) = (f(\beta), f(\beta^2), ..., f(\beta^n)). \tag{2-1}$$

é uma aplicação injetiva já que $deg\, f < n$ e logo qualquer elemento de $\mathcal{L}_k$ possui no máximo $k-1 < n$ zeros.

Agora podemos definir o código C_k sobre $\mathbb{F}_q$:

$$C_k = \{(f(\beta), f(\beta^2), ..., f(\beta^n)) \mid f \in \mathcal{L}_k\}.$$

C_k é chamado um código de Reed-Solomon e pela própria definição resulta ser um $[n, k]$-código.

Neste caso, o peso de uma palavra não-nula $c = av(f)$ para algum polinômio $f \in \mathcal{L}_k$ é dado por:

$$\begin{aligned} w(c) &= n - |\{i \in \{1, ..., n\}; f(\beta^i) = 0\}| \\ &\geq n - deg\, f \\ &\geq n - (k-1) \\ &\geq n - k + 1. \end{aligned}$$

Portanto a distância mínima d de C_k satisfaz

$$d \geq n - k + 1.$$

Por outro lado a proposição 2.1.1 nos diz que $d \leq n - k + 1$. Logo $d = n - k + 1$, o que implica que os códigos de Reed-Solomon são MDS-códigos.

Outros códigos muito conhecidos são os chamados códigos de Reed-Muller e a sua construção é muito parecida com a anterior:

Sejam $P_1, \ldots, P_n$ uma enumeração de todos os pontos de $\mathbb{F}_q^m$. O código de Reed-Muller $RM_q(r, m)$ é dado por:

$$RM_q(r, m) := \{(f(P_1), \ldots, f(P_n)) \mid f \in \mathbb{F}_q[X_1, \ldots, X_m] \text{ com } deg\, f \leq r\}.$$

Os dois exemplos anteriores foram construidos "avaliando"certas funções em pontos do corpo finito considerado.