Breve introdução à Teoria dos Códigos Corretores de Erros

César Polcino Milies
Instituto de Matemática e Estatística
Universidade de Saõ Paulo
Caixa Postal 66.281, CEP 05311-970
São Paulo, SP - Brasil
polcino@ime.usp.br

0

Prefácio

A teoria dos códigos corretores de erros é um tópico particularmente interessante e muito adequado como objeto de um mini-curso.

Por um lado, ela tem um cunho eminentemente prático. Seu objetivo é criar métodos que permitam detectar e corrigir erros que eventualmente possam acontecer durante uma transmissão de dados. Hoje, ela encontra aplicações em campos tão diversos quanto a telefonia, a produção de DVD's ou o envio de dados desde veículos espaciais às estações receptoras na terra.

Por outro lado, a teoria tem, para os estudosos da álgebra, o atrativo de ser um campo de aplicação de técnicas e conceitos originados nos diversos ramos desta ciência. No nível elementar e introdutório em que estas notas foram redigidas, a teoria depende apenas de conceitos muito básicos de álgebra linear e de técnicas de contagem.

Se o leitor se interessar pelo assunto e decidir aprofundar seus conhecimentos, verá, ao continuar seus estudos, que novas áreas da álgebra trazem conribuições fundamentais. Assim, precisará se utilizar, entre outros, de conceitos da teoria de corpos finitos, de anéis de polinômios sobre estes corpos, da geometria algébrica e da teoria de grupos.

Esperamos que estas notas estimulem o leitor a se aprofundar nestes campos da álgebra que são também interessantes em si mesmos e tem muitíssimas aplicações em várias outras direções.

São Paulo, janeiro de 2011

C.P.M.

Capítulo 1

Introdução

1.1 Um Pouco de História

A teoria dos códigos corretores de erros é um campo de pesquisa muito ativo na atualidade em diversas áreas do conhecimento: matemática, computação, engenharia elétrica e estatistíca entre outras.

Na transmissão de dados, na vida real, às vezes ocorrem problemas, como interferências electromagnéticas ou erros humanos (por exemplo, erros de digitação) que chamamos de *ruído* e que fazem com que a mensagem recebida seja diferente daquela que foi enviada. O objetivo da teoria é desenvolver métodos que permitam detectar e corregir estes erros.

A teoria teve início na década de quarenta quando os computadores eram máquinas muito caras e apenas instituições de grande porte como o governo ou as universidades tinham condições de mantê-lo. Eles usando-os para executar tarefas numéricas complexas, como calcular a órbita precisa de Marte ou fazer a evaluação estatística de um censo [1].

O Laboratório Bell de Tecnologia possuia tais computadores e Richard W. Hamming trabalhava com estas máquinas em 1947; porém, para ele o acesso estava restrito apenas aos fins de semana. Na época, os programas eram gravados em cartões perfurados cuja leitura pelo computador permitia detectar erros de digitação. Caso um erro fosse detectado, a leitura era interrompida e o computador passava automaticamente a ler o programa do próximo usuário. Hamming relembra:

> *Em dois finais de semanas consecutivos eu fui e descobri que todas minhas coisas tinham sido descarregadas e nada tinha sido feito. Eu estava realmente aborrecido e irritado porque queria estas respostas e tinha perdido dois finais de semana. E então eu me disse "Maldição, se as máquinas podem detectar um erro, porque não podemos localizar a posição do erro e corrigi-lo."* [1]

[1] R.W. Hamming, Interview, febrero de 1977 [4].

Esta questão foi crucial para o desenvolvimento dos códigos corretores de erros.

Hamming desenvolveu um código capaz de detectar até dois erros e corrigir um erro, se ele for o único. Seu trabalho so foi publicado em abril de 1950 no *"The Bell System Technical Journal"* [5] (A publicação tardia deste artigo ocorreu devido ao pedido de patente destes códigos, feita pelo *Laboratório Bell*).

Durante os três anos transcorridos desde a elaboração destes códigos até a publicação de seu trabalho, Hamming publicou diversos memorandos internos do *Laboratório Bell* conforme sua pesquisa evoluia. Nestes artigos se questionava sobre a possibilidade de criar códigos maios eficiêntes que àquele proposto inicialmente.

A questão foi respondida indiretamente em outubro de 1948, por C. E. Shannon num artigo intitulado *"A Mathematical Theory of Communication"*, também publicado no *"The Bell System Technical Journal"* [6]. O artigo de C. E. Shannon deu inicio a dois novos campos de pesquisa em matemática: a teoria de códigos (em conjunto com o trabalho de Hamming) e a Teoria da Informação. A partir deste artigo, pode-se dizer, que houve um desenvolvimento continuo e significativo da Teoria dos Códigos até hoje.

Mais adiante, Marcel J. E. Golay que trabalhava no *Signal Corps Enginneering Laboratories at Fort Monmouth* , em Nova Jersey, leu a descrição do chamado (7, 4)-código de Hamming dada no artigo de Shannon em 1948, e extendeu o resultado para um código corretor de erro único de comprimento primo p. Seu trabalho foi publicado em julho de 1949 no *Proceedings of the I.R E. (I.E.E.E.)*, o artigo foi intitulado *"Notes on Digital Coding"[3].*

Ainda com base neste artigo, Golay desenvolveu os hoje chamados (23,12) e (11, 6) códigos de Golay. Posteriormente desenvolveu o (24, 4096, 8)-código de Golay que foi usado pela espaçonave Voyager para transmitir fotografias coloridas de Jupiter e Saturno. Seu primeiro artigo é de apenas uma página e é um dos mais importantes na teoria de códigos.

Golay, Hamming e Shannon foram os grandes pioneiros que iniciaram o trabalho com este assunto e desenvolverem estudos e id eias que são usadas até hoje no nosso dia a dia, como por exemplo a comunicação móvel (telefones celulares), aparelhos de armazenamentos de dados (gravador, compact disk, DVD), além de comunicações via satelite, processamento de imagens digitais, proteção de mémoria SRAM (mémoria estatica), internet e radio entre outras.

Atualmente, estes códigos são amplamente utilizados em programas espaciais da NASA[2] e do JPL[3]. Por exemplo na missão Galileo para Júpiter,na missão Cassini para Saturno e na missão Marte [2], mais especificamente, fora utilizado o sistema AICS (*Advanced Imaging Communication System*), que combina técnicas dos códigos Reed-Solomon com o então método padrão denomi-

[2]NASA = National Aeronautics and Space Administration
[3]JPL = Jet Propulsion Laboratory

nado código *convolutional*.

Neste mini-curso pretendemos apenas dar uma idéia de como pode-se desenvolver este tipo de estudo; nos limitaremos a explorar as noções básicas e a descrever o tipo mais simples de códigos corretores de erros: os *códigos lineares*.

1.2 Conceitos básicos

De certa forma, pode-se dizer que a construção de códigos inspira-se no mais comum dos códigos utilizados pelos seres humanos: os idiomas. Na língua portuguesa, por exemplo, usamos um alfabeto de 23 letras e as palavras nada mais são de que seqüências de letras. É claro que a língua não é composta por todas as "palavras" possíveis formadas a partir das letras. Nós reconhecemos algumas delas como fazendo parte da língua e outras como alheias à língua.

Assim, os elementos básicos para se construir um código são os seguintes:

- Um conjunto finito, $\mathcal{A}$ que chamaremos **alfabeto**. Denotaremos por $q = |\mathcal{A}|$ o número de elementos de A. Quando o número de elementos do alfabeto de um código é q, diz-se que o código é *q-ário*. Nos exemplos da seção anterior vimos códigos cujo alfabeto era o conjunto $\mathbb{Z}_2 = \{0, 1\}$, que são os chamados códigos *binários*.

- Seqüências finitas de símbolos do alfabeto, que chamaremos **palavras**. O número de letras de uma palavra chama-se o seu **comprimento**. Para termos um código com o qual seja fácil trabalhar com um certo rigor, faremos a convenção de que todas as palavras que iremos considerar para compor o código terão o mesmo comprimento n. Por esta razão, estes códigos dizem-se *em blocos* mas, como todos os códigos que estudaremos serão em blocos, daqui em diante omitiremos esta palavra.

- Um **código q-ário de comprimento** n será então um subconjunto qualquer (a nossa escolha) de palavras de comprimento n, i.e., um código $\mathcal{C}$ é um subconjunto
$$\mathcal{C} \subset \mathcal{A}^n = \underbrace{A \times A \times \cdots \times A}_{n \text{ vezes}}.$$

Exemplo 1.2.1. *Quando o alfabeto utilizado é o conjunto $\mathbb{Z}_2 = \{0,\ 1\}$ o cõdigo diz-se binário. O conjunto*

$$\mathcal{C}_1 = \{00000, 01011, 10110, 11101\}$$

é um código em blocos, binário, de comprimento 5.

Se consideremos como alfabeto o conjunto $\mathbb{Z}_3 = \{0, 1, 2\}$. O conjunto

$$\mathcal{C}_2 = \{00012, 11022, 10101, 10201, 20202\}$$

é um código em blocos, ternário, de comprimento 5.

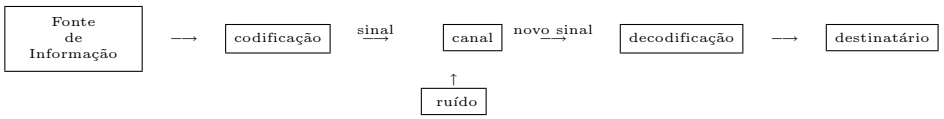
Exemplo 1.2.2.

Dado um alfabeto $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$, o código:

$$\mathcal{C} = \{\underbrace{a_1 a_1 \ldots a_1}_{n \text{ vezes}}, \underbrace{a_2 a_2 \ldots a_2}_{n \text{ vezes}}, \ldots, \underbrace{a_q a_q \ldots a_q}_{n \text{ vezes}}\}$$

chama-se o *código de repetição* q-ário, de comprimento n.

Como já observamos, transmissão de dados em código entre um emissor e um receptor nem sempre é perfeita. No processo podem ocorrer interferências que modifiquem a mensagem enviada. Esta situação foi descrita já pelo próprio Shannon, utilizando o seguinte esquema:



A idéia básica da teoria de códigos corretores de erros é *codificar* a informação inicial, adicionando informação redundante, de forma tal que, ao receber o sinal modificado pelo "ruído" seja possível, de alguma forma, recuperar a mensagem original.

Vamos voltar mais uma vez, ao exemplo da língua portuguesa. Suponhamos que recebemos uma mensagem com a palavra *teorxa*. Imediatamente sabemos que a mensagem contém um erro, pois não reconhecemos esta palavra como pertencente à língua (é precisamente isto que fazem os programas editores de texto com correção ortográfica, que comparam cada palavra escrita com as que constam no seu dicionário interno). Mais ainda, achamos que a mensagem correta deve ser a palavra *teoria*, porque é a palavra da língua mais "próxima" da palavra recebida.

Por outro lado, se recebemos a palavra *wato* também reconhecemos que está errada, mas percebemos que há várias possibilidades de correção; i.e., há várias palavras da língua igualmente "próximas" desta, como por exemplo, *gato, pato, rato, mato,* etc.

Estas observações podem ser expressas em linguagem rigorosa e nos levarão aos primeiros resultados da teoria de códigos.

Definição 1.2.3 (Distância de Hamming)**.** *Dados dois elementos* $x = (x_1, x_2, \ldots, x_n)$ *e* $y = (y_1, y_2, \ldots, y_n)$ *de um espaço* A^n*, chama-se* **distância de Hamming** *de* x *a* y *ao número de coordenadas em que estes elementos diferem; isto é:*

$$d(x, y) = |\ \{i \mid x_i \neq y_i, 1 \leq i \leq n\}\ |$$

Dado um código $\mathcal{C} \subset A^n$ *chama-se* distância mínima *de* $\mathcal{C}$ *ao número*

$$d = min\{d(x, y) \mid x, y \in \mathcal{C}, x \neq y\ \}.$$

Note que, conforme à nossa definição, a distância de Hamming entre duas palavras é sempre um número inteiro.

Pode-se demonstrar facilmente que a distância de Hamming acima definida é, de fato, uma distância no sentido matemático do termo; i.e., que verifica as seguintes condições

(i) $d(x, y) \geq 0$ para todos $x, y \in A^n$ e $d(x, y) = 0$ se e somente se $x = y$.

(ii) $d(x, y) = d(y, x)$, para todos $x, y \in A^n$.

(iii) Dados $x, y, z \in A^n$ tem-se que $d(x, z) \leq d(x, y) + d(y, z)$.

Podem-se definir agora os conceitos de bola e esfera em A^n, tal como é feito em qualquer espaço métrico.

Definição 1.2.4. *Dado um elemento $x \in A^n$ e um inteiro positivo r chama-se* ***bola de centro em*** x ***e raio*** r*, ao conjunto*

$$B(x, r) = \{u \in \mathcal{A}^n : d(u, x) \leq r\}$$

e ***esfera de centro em*** x ***e raio*** r*, ao conjunto*

$$S(x, r) = \{u \in \mathcal{A}^n : d(u, x) = r\}$$

Estamos em condições estabelecer nosso primeiro resultado referente à detecção e correção de erros. Consideraremos que, ao receber um elemento y, podemos detectar se ele contém, ou não, erro se temos um critério clalro para decidir se y pertence, ou não, a $\mathcal{C}$.

Por outro lado, uma vez detectado um erro, nosso critério de correção será substituir o elemento y recebido pelo elemento x do código $\mathcal{C}$ *mais próximo* de y. Para que a correção seja possível será necessário então que não haja ambigüidades quanto à determinação de um tal elemento.

Para enunciarmos nosso critério, precisamos na seguinte notação: dado um número real x, denotaremos por $\lfloor x \rfloor$ *o maior inteiro menor o igual a* x.

Teorema 1.2.5. *Seja $\mathcal{C}$ um código com distância mínima d e seja*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Então, é possível detectar até $d-1$ erros e corrigir até κ erros.

Demonstração. Seja x um elemento de $\mathcal{C}$ e suponhamos que ele foi recebido como um outro elemento y, com $t \leq d-1$ erros. Como o número t de erros acontecidos é precisamente a distância de Hamming de x a y temos que $d(x, y) \leq d-1 < d$. Isto implica que $y \notin \mathcal{C}$ e, portanto, o erro pode ser detectado.

Suponhamos ainda que o número t de erros cometidos é menor que κ. Consideramos a esfera $B(y, \kappa)$, de centro em y e raio κ. Como $d(x, y) = t \leq \kappa$ temos que $x \in B(y, \kappa)$. Afirmamos que x *é o único elemento de* $\mathcal{C}$ *contido nessa esfera.*

De fato, se existisse outro elemento x' de $\mathcal{C}$ em $B(y,\kappa)$, ter-se-ia que

$$d(x,x') \leq d(x,y) + d(y,x') \leq 2\kappa < d,$$

uma contradição. Conseqüentemente, x é *o elemento* de $\mathcal{C}$ mais próximo de y e é possível corrigir o erro. □

O próximo resultado não é mais do que uma re-interpretação do enunciado do teorema acima (e de sua demonstração).

Corolario 1.2.6. *Um código $\mathcal{C}$ pode corrigir até κ erros se e somente se sua distância mínima $d(\mathcal{C})$ verifica a desigualdade*

$$d(\mathcal{C}) \geq 2\kappa + 1.$$

O processo que a cada palavra y, recebida eventualmente com erros, associa uma palavra corrigida x no código chama-se de *decodificação.*

Definição 1.2.7. *Dado um código $\mathcal{C}$ com distância mínima d, o número*

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$$

chama-se a capacidade *de $\mathcal{C}$.*

EXERCÍCIOS

1. Considere o código binário $\mathcal{C}$ de comprimento 4 obtido da sequinte forma: Para cada elemento $ab \in \mathbb{Z}_2^2$ formamos o elemento $abab \in \mathbb{Z}_2^4$. Determinar a distância minima e a capacidade de $\mathcal{C}$.

2. Calcule a distância mínima e a capacidade do código de repetição q-ário de comprimento n. Determine n para que este código possa corrigir 5 erros.

3. Calcule a distância mínima e a capacidade dos códigos dos exemplos 1.2.1 e 1.2.2

4. Prove que a distância de Hamming verifica, de fato, as condições de uma métrica.

5. Prove que a distância de Hamming verifica, de fato, as condições de uma métrica.

6. Calcule a distância mínima e a capacidade do código de repetição q-ário de comprimento n e os mesmos parâmetros para o código con repetição q-ário de comprimento qn.

7. Dado um código $\mathcal{C}$, chama-se **extensão** de $\mathcal{C}$ a qualquer código que se obtém a partir de $\mathcal{C}$ adicionando coordenadas a cada uma das palavras de $\mathcal{C}$. Considere o codigo $\widehat{\mathcal{C}}$, extendido de $\mathcal{C}$, que se obtém adicionando um dígito de verificação de paridade:

$$\widehat{\mathcal{C}} = \left\{ (c_1, c_2, \ldots, c_n, c_{n+1} \mid (c_1, c_2, \ldots, c_n) \in \mathcal{C},\ c_{n+1} = -\sum_{i=1}^{n} c_i \right\}.$$

Prove que, se $\mathcal{C}$ é um (n, M, d)-código, então $\widehat{\mathcal{C}}$ é um $(n+1, M, \widehat{d})$-código, onde $\widehat{d} = d$ ou $\widehat{d} = d + 1$.

8. Dado um código binário $\mathcal{C}$, provar que se $\overline{\mathcal{C}}$ é uma extensão de $\mathcal{C}$ então:

$$d(\overline{\mathcal{C}}) = \begin{cases} = & d(\mathcal{C}) \quad \text{se } d(\mathcal{C}) \text{ é par.} \\ = & d(\mathcal{C}) + 1 \quad \text{se } d(\mathcal{C}) \text{ é ímpar.} \end{cases}$$

e

$$\kappa(\overline{\mathcal{C}}) = \kappa(\mathcal{C}).$$

9. Provar que se existe um (n,M,d)-código binário, com d par, então existe um (n,M,d)-código binário em que todas as palavras têm peso par.

10. Dado um código $\mathcal{C}$, chama-se **código contraído** de $\mathcal{C}$ a qualquer código que se obtém a partir de $\mathcal{C}$ suprimindo coordenadas (sempre nas mesmas posições) de cada uma das palavras de $\mathcal{C}$.

    Dado um (n, N, d)-código q-ário $\mathcal{C}$ provar que, se $\mathcal{C}'$ indica um código contraído de $\mathcal{C}$ suprimindo uma única posição em todas as palavras de $\mathcal{C}$, então $\mathcal{C}'$ é um $(n-1, M, d^*)$-código, com $d^* = d$ ou $d^* = d - 1$. Dar um exemplo para mostrar que a distância mínima pode, efetivamente, diminuir.

11. Seja $\sigma : \mathbb{F}_2 \to \mathbb{F}_2$ a transposição $\sigma = (10)$; isto é, a função tal que $\sigma(0) = 1$ e $\sigma(1) = 0$. Dado um elemento $\mathbf{v} = (a_1, a_2, \ldots, a_n) \in \mathbb{F}_2^n$, chama-se **complemento** de $\mathbf{v}$ ao elemento

$$\mathbf{v}^c = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_n)).$$

    Dado um çodigo binário $\mathcal{C}$ chama-se **complemento** de $\mathcal{C}$ ao código

$$\mathcal{C}^c = \{\mathbf{v}^c \mid \mathbf{v} \in \mathcal{C}\}.$$

    Provar que:

    (i) Se $\mathcal{C}$ é um código binário, então $\mathcal{C}$ e $\mathcal{C}^c$ têm os mesmos parâmetros.

    (ii) Dados $\mathbf{v}$ e $\mathbf{w}$ em $\mathbb{F}_2^n$ tem-se que $d(\mathbf{v}, \mathbf{w^c}) = \mathbf{n} - \mathbf{d}(\mathbf{v}, \mathbf{w})$.

12. Seja $\mathcal{C}$ um $n, M, d)$-código binário e seja

$$d^+ = max\{d(x, y) \mid x, y \in \mathcal{C}\}.$$

    Provar que $d(\mathcal{C} \cup \mathcal{C}^c) = min\{d, n - d^+)$.

13. Sejam $\mathcal{C}$ e $\mathcal{C}'$ dois códigos q-ários. Chama-se **soma direta** destes códigos ao código

$$\mathcal{C} \oplus \mathcal{C}' = \{(c_1, \ldots, c_n, c'_1, \ldots, c'_{n'}) \mid (c_1, \ldots, c_n) \in \mathcal{C},\ (c'_1, \ldots, c'_{n'}) \in \mathcal{C}'\}.$$

    Provar que, se $\mathcal{C}$ e $\mathcal{C}'$ têm parâmetros (n, M, d) e (n', M', d') respectivamente, então $\mathcal{C} \oplus \mathcal{C}'$ tem parâmetros:

$$n_0 = n + n', \quad M_0 = MM', \quad d_0 = min\{d, d'\}.$$

14. Justifique o método de correção de erros do código de Hamming de comprimento 7.

15. Determine a distância mínima e a capacidade de correção de $\mathcal{H}_2(3)$; o código de Hamming de comprimento 7.

1.3 Equivalência de códigos

Tal como vimos na seção anterior, os parâmetros que determinam o comportamento de um código $\mathcal{C}$ são:

- O número q de elementos do alfabeto $\mathcal{A}$.
- O comprimento n das palavras do código.
- O número $M = |\mathcal{C}|$ de palavras que compoem o código.
- A distância mínima d.

Por causa disso, é comum empregar a seguinte terminologia.

Definição 1.3.1. *Um código q-ário de comprimento n, com M palavras e distância mínima d diz-se um* (n,M,d)*-código.*

Interesa-nos estabelecer quando dois códigos têm os mesmos parâmetros. Para isso, introduzimos a seguinte.

Definição 1.3.2. *Sejam $\mathcal{A}$ um conjunto finito e n um inteiro positivo. Uma função $\varphi : \mathcal{A}^n \to \mathcal{A}^n$ diz-se um* isometria de Hamming *ou, brevemente, uma* isometria *de $\mathcal{A}^n$ se preserva a distância de Hamming em $\mathcal{A}^n$; i.e., se:*

$$d(\varphi(\mathbf{x}), \varphi(\mathbf{y})) = d(\mathbf{x}, \mathbf{y}), \qquad \forall \mathbf{x}, \mathbf{y} \in \mathcal{A}^n.$$

Como $d(\mathbf{x}, \mathbf{y}) = 0$ se e somente se $\mathbf{x} = \mathbf{y}$ é fácil ver que uma isometria é, necessariamente, uma função injetora. Ainda, como o conjunto $\mathcal{A}^n$ é finito, segue imediatamente que ela tambem é sobrejetora. Logo, *toda isometria de $\mathcal{A}^n$ é uma função bijetora.*

A próxima proposição segue diretamente da própria definição.

Proposição 1.3.3.
(i) A função identidade é uma isometria.
(ii) A inversa de uma isometria é uma isometria.
(iii) A composição de duas de isometrias é também uma isometria.

Conseqüentemente, se $\mathcal{C} \subset \mathcal{A}^n$ é um código e $\varphi : \mathcal{A}^n \to a^n$ é uma isometria, temos que $|\mathcal{C}| = |\varphi(\mathcal{C})|$ e, claramente, ambos conjuntos têm a mesma distância mínima, logo ambos códigos têm os mesmos parâmetros. Esta observação justifica nossa proxima definição.

Definição 1.3.4. *Dados dois códigos $\mathcal{C}$ e $\mathcal{C}'$ em $\mathcal{A}^n$ diz-se que $\mathcal{C}$ é* **equivalente** *a $\mathcal{C}'$ se existe uma isometria $\varphi : \mathcal{A}^n \to \mathcal{A}^n$ tal que $\varphi(\mathcal{C}) = \varphi(\mathcal{C}')$.*

Para indicar que $\mathcal{C}$ é equivalente a $\mathcal{C}'$ escreveremos $\mathcal{C} \cong \mathcal{C}'$.

Usando a Proposição 1.3.3, o leitor poderá verificar facilmente que esta é, de fato, uma relação de equivalência; isto é, que verifica as seguintes propriedades:

(*i*) (Reflexiva) $\mathcal{C} \cong \mathcal{C}$ para todo código $\mathcal{C} \subset \mathcal{A}^n$.
(*ii*) (Simétrica) Se $\mathcal{C} \cong \mathcal{C}'$ entã $\mathcal{C}' \cong \mathcal{C}$.
(*iii*) (Transitiva) Se $\mathcal{C} \cong \mathcal{C}'$ e $\mathcal{C}' \cong \mathcal{C}''$ então $\mathcal{C} \cong \mathcal{C}''$.

Note, porém, que existem códigos com os mesmos parâmetros que não são equivalentes (veja o exercício 2).

Exemplo 1.3.5.

Seja π uma *permutação* do conjunto de inteiros $\{1, 2, \ldots, n\}$, isto é, uma função bijetora deste conjunto em si mesmo. Então a função $\varphi_\pi : \mathcal{A}^n \to \mathcal{A}^n$ dada por

$$\varphi_\pi(a_1, a_2, \ldots, a_n) = (a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)})$$

é uma isometria. Deixamos a demonstração a cargo do leitor.

Exemplo 1.3.6.

Seja $f : \mathcal{A} \to \mathcal{A}$ uma bijeção de $\mathcal{A}$. Fixado um índice i, $1 \leq i \leq n$, definimos uma função $\varphi_f^{(i)} : \mathcal{A}^n \to \mathcal{A}^n$ por

$$(a_1, \ldots, a_i, \ldots a_n) \ \mapsto \ (a_1, \ldots, f(a_i), \ldots a_n).$$

É muito fácil verificar que esta função é uma isometria.

Usando a parte (*iii*) da Proposição 1.3.3 segue diretamente que, se $F = \{f_1, f_2, \ldots, f_n\}$ é uma família de n isometrias de $\mathcal{A}^n$, então a função $\varphi_F : \mathcal{A}^n \to \mathcal{A}^n$ dada por

$$(a_1, a_2, \ldots, a_n) \ \mapsto \ (f_1(a_1), f_2(a_2), \ldots, f_n(a_n))$$

também é uma isometria.

Pode-se demonstrar que toda isometria é de um dos dois tipos acima, ou uma composição de isometrias de esses tipos. Mais precisamente, vale o seguinte.

Teorema 1.3.7. *Dada uma isometria $\varphi : \mathcal{A}^n \to \mathcal{A}^n$ existem uma permutação π do conjunto $\{1, 2, \ldots, n\}$ e bijeções $f_i : \mathcal{A} \to A$, $1 \leq i \leq n$, tais que*

$$\varphi = \varphi_\pi \circ \varphi_F$$

onde $F = \{f_1, f_2, \ldots, f_n\}$ e φ_π e φ_F estão definidas como nos exemplos 1.3.5 e 1.3.6 respectivamente.

EXERCÍCIOS

1. Sejam $\mathcal{A}$ um conjunto finito e n um inteiro positivo. Dados dois elementos $\mathbf{x}$ e $\mathbf{y}$ em $\mathcal{A}^n$ mostrar que sempre existe uma isometria $\varphi : \mathcal{A}^n \to \mathcal{A}^n$ tal que $\varphi(\mathbf{x}) = \mathbf{y}$.

2. Sejam $\mathcal{C} = \{0000, 0100, 0101\}$ e $\mathcal{C}' = \{0000, 0010, 0111\}$ dois códigos de $\mathbb{Z}_2^4$. Mostrar que eles têm os mesmos parâmetros mas não são equivalentes.

3. Dado o alfabeto $\mathcal{A} = \{0, 1, 2, 3, 4, 5\}$, construir dois códigos de $\mathcal{A}^5$ equivalentes ao código $\mathcal{C} = \{01234, 00222, 01354, 15522\}$.

4. Sejam f e g isometrias de um conjunto finito $\mathcal{A}$ com n elementos e σ e π permutações de $\{1, 2, \ldots, n\}$. Sejam ainda $i \neq j$ inteiros positivos, menores que n. Com a notação dos Exemplo 1.3.5 e 1.3.6, provar que

   (i) $\varphi_\sigma \circ \varphi_\pi = \varphi_{\sigma\circ\pi}$.

   (ii) $(\varphi_\sigma)^{-1} = \varphi_{\sigma^{-1}}$.

   (iii) $\varphi_f^{(i)} \circ \varphi_g^{(i)} = \varphi_{f\circ g}^{(i)}$.

   (iv) $\left(\varphi_f^{(i)}\right)^{-1} = \varphi_{f^{-1}}^{(i)}$.

   (v) $\varphi_f^{(i)} \circ \varphi_g^{(j)} = \varphi_g^{(j)} \circ \varphi_f^{(i)}$ se $i \neq j$.

   (vi) $\varphi_\sigma \circ \varphi_f^{(i)} = \varphi_f^{\sigma(i)} \circ \varphi_\sigma$.

   (vii) $\varphi_f^{(i)} \circ \varphi_\sigma = \varphi_\sigma \circ \varphi_f^{\sigma^{-1}(i)}$.

5. Provar que o código binário $\mathcal{C} = \{00100, 00011, 11111, 11000\}$ é equivalente ao código $\mathcal{C}' = \{00000, 01101, 10110, 11011\}$. (Sugestão: considere a bijeção f de $\{0, 1\}$ diferente da identidade, a permutação σ de $\{1, 2, 3, 4, 5\}$ que intercâmbia 2 e 4 e fixa os outros elementos e aplique $\varphi_\sigma \circ \varphi_f^{(3)}$).

6. Seja $\mathcal{C} = \{012, 120, 201\} \subset \mathbb{Z}_3^3$. Provar que $\mathcal{C}$ é equivalente ao código de repetição de comprimento 3 sobre $\mathbb{Z}_3$. (Sugestão: procure bijeções adequadas para usar na segunda e terceira posição).

7. Seja $\mathcal{C}$ um (n,M,d)-código sobre um alfabeto $\mathcal{A} = \{a_1, a_2, \ldots, a_q\}$. Provar que $\mathcal{C}$ é equivalente a um código que contém o elemento $\alpha = \underbrace{aa\ldots a}_{n\ vezes}$.

8. Provar que o número de códigos binários, contendo duas palavras, de comprimento n, não equivalentes, é n.

9. Provar qe todo (n,q,n)-código q-ário é equivalente a um código de repetição.

10. Seja E^n o conjunto de todos os elementos de $\mathbb{Z}_2^n$ que tem um número par de coordenadas iguais a 1. Provar que E^n é o subconjunto que resulta de extender o código formado por todas as palavras de $\mathbb{Z}_2^{n-1}$

1.4 O problema principal da teoria de códigos

Um dos objetivos importantes a se ter em conta ao desenhar um (n,M,d)-código é o de que ele seja de alta eficiência, no sentido de que o número M de palavras no código seja relativamente grande, para poder transmitir bastante informação, e que tenha uma distância mínima d também relativamente grande, para ter uma boa capacidade de correção de erros. (O outro aspecto importante a se ter en conta é possua um algoritmo de decodificação razoavelmente simples e rápido).

Infelizmente, estes objetivos são conflitantes entre si, pois ao aumentar o número de palavras de um código, naturalmente irá a diminuir a distância mínima entre elas. A questão de achar valores satisfatórios para ambas é conhecida como o **problema principal da teoria de códigos**.

Há várias formas de se olhar para a relação entre os parâmetros de um código. Inicialmente, vamos imaginar n pré-fixado e estudar a relação entre M e d.

Note que, como as distâncias são sempre inteiros positivos, dentro de uma bola de centro x de raio r estão contidas todas as esferas do mesmo centro cujos raios são inteiros menores o iguais a r. Logo, temos que:

$$B(x,r) = \bigcup_{t=0}^{r} S(x,r).$$

Dado um ponto x, um outro ponto y estará a distância r de x se diferir dele em r posições. Digamos que escolhemos r posições fixas entre as que compoem x. Como em cada uma destas posições podemos ter $q-1$ letras do alfabeto, diferentes da letra correspondente em x, existem $(q-1)^r$ palavras de A^n que diferem de x nas r posições fixadas. Ainda, podemos escolher r posições entre as n posições do elemento x de $\binom{n}{r}$ maneiras distintas. Portanto, existem exatamente $\binom{n}{r}(q-1)^r$ pontos na esfera $S(x,r)$.

Podemos então calcular o número de pontos na bola de centro x e raio r:

$$|B(x,r)| = \sum_{t=0}^{r} \binom{n}{t}(q-1)^t.$$

Deste resultado segue imediatamente o seguinte

Corolario 1.4.1. *Todas as esferas de raio r em $\mathcal{A}^n$ contém o mesmo número de elementos.*

O mesmo estilo de argumento utilzado na demonstração do Teorema 1.2.5 mostra que esferas com centro em pontos diferentes do código $\mathcal{C}$ e raio κ tem interseção vazia e, como

$$\bigcup_{x\in\mathcal{C}} B(x,\kappa) \subset \mathcal{A}^n$$

segue que

$$\sum_{x\in\mathcal{C}} |B(x,\kappa)| \leq q^n$$

e, como trata-se de M esferas contendo igual número de pontos, temos:

$$M\left[\sum_{t=0}^{\kappa}\binom{n}{t}(q-1)^t\right] \leq q^n.$$

Estas observações permitem obter diretamente uma limitação para o número possível de palavras num código, dados seu comprimento e sua distância mínima.

Teorema 1.4.2. (Cota de Hamming) *Dado um (n,M,d)-código, tem-se que*

$$M \leq \frac{q^n}{\sum_{t=0}^{\kappa}\binom{n}{t}(q-1)^t}.$$

Dado um código $\mathcal{C}$, uma situação ideal se da quando *toda* palavra de A^n pode ser decodificada a uma palavra de $\mathcal{C}$; isto é, quando toda palavra de $\mathcal{A}^n$ pertence a uma única esfera de raio κ e centro em alguma palavra do código. Isto justifica a seguinte.

Definição 1.4.3. *Um codigo $\mathcal{C} \subset \mathcal{A}^n$ com distância mínima d e capacidade $\kappa = \lfloor (d-1)/2 \rfloor$ diz-se* **perfeito** *se*

$$\bigcup_{x\in\mathcal{C}} B(x,\kappa) = \mathcal{A}^n$$

Da Cota de Hamming, resulta claro que vale a seguinte caracterização.

Proposição 1.4.4. *Um (n,M,d)-código $\mathcal{C}$ é perfeito se e somente se tem-se que*

$$M\left[\sum_{t=0}^{\kappa}\binom{n}{t}(q-1)^t\right] = q^n.$$

A condição acima é chamada de *condição de empacotamento de esferas* Para outra caracterização equivalente, veja o exercício 4.

Vamos considerar agora o problema principal da teoria de códigos desde outro ponto de vista. Dado um alfabeto q-ário $\mathcal{A}$ Vamos tentar achar o maior código con comprimento n e distância mínima d dados. Definimos o número:

$$A_q(n,d) = max\{M \mid \text{ existe um } (n,\mathrm{M},d)\text{-código em } \mathcal{A}^n\}$$

Definição 1.4.5. *Um (n,M,d)-código q-ário diz-se* **ótimo** *se $M = A_q(n,d)$.*

Em outras palavras, um código $\mathcal{C}$ em $\mathcal{A}^n$ é ótimo se é de tamanho máximo entre os códigos que têm distância mínima igual a d.

Infelizmente, sabe-se pouco sobre os valores de $A_q(n,d)$. Porém, é possível determinar limitações para estes valores.

Seja $\mathcal{C}$ um (n,M,d)-código q-ário ótimo. Como $\mathcal{C}$ tem tamanho máximo, para cada elemento $\mathbf{x} \in \mathcal{A}^n$ deve existir pelo menos uma palavra $\mathbf{c} \in \mathcal{C}$ tal que $d(\mathbf{x},\mathbf{c}) < d$ pois, em caso contrário, adicionando $\mathbf{x}$ a $\mathcal{C}$ ter-se-ia um $(n,\ \mathrm{M}+1,\ d)$-código.

Consequentemente, todo elemento $\mathbf{x} \in \mathcal{A}^n$ pertence a pelo menos uma esfera de centro em alguma palavra de $\mathcal{C}$ e raio $d-1$. Logo, temos que

$$\mathcal{A}^n \subset \bigcup_{\mathbf{c}\in\mathcal{C}} B(c,d-1)$$

o que implica que

$$q^n \leq \sum_{\mathbf{c}\in\mathcal{C}} |B(c, d-1)|.$$

Lembrando que todas as bolas do mesmo raio tem o mesmo número de elementos e que, como $\mathcal{C}$ é ótimo, temos que $M = A_q(n, d)$ tem-se imediatamente o seguinte.

Teorema 1.4.6. (Cota de Gilbert-Varshamov)
Dados n e d, vale a seguinte desigualdade.

$$\frac{q^n}{\sum_{t=0}^{d-1} \binom{n}{r}(q-1)^t} \leq A_q(n, d).$$

Ainda, como $A_q(n, d)$ é o número de elementos de um código dado em $\mathcal{A}^n$, levando em consideração a cota de Hamming, temos:

$$\frac{q^n}{\sum_{t=0}^{d-1} \binom{n}{r}(q-1)^t} \leq A_q(n, d) \leq \frac{q^n}{\sum_{t=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{r}(q-1)^t}.$$

Podemos ainda obter outras limitações para $A_q(n, d)$.

Teorema 1.4.7. (Cota de Singleton)

$$A_q(n, d) \leq q^{n-d+1}.$$

Demonstração. Seja $\mathcal{C}$ um (n, M, d)-código ótimo; i.e., com $M = A_q(n, d)$. Afirmamos que se $\mathbf{c}_1$ e $\mathbf{c}_2$ são duas palavras distintas de $\mathcal{C}$, então as palavras $\mathbf{c}'_1$ e $\mathbf{c}'_2$ que resultam destas eliminando as últimas $d-1$ posições devem ser também distintas. De fato, se $\mathbf{c}'_1 = \mathbf{c}'_2$, então $\mathbf{c}_1$ e $\mathbf{c}_2$ podem diferir apenas em posições que se encontram entre as $d-1$ que foram suprimidas. Isto significaria que $d(\mathbf{c}_1, \mathbf{c}_2) \leq d-1$, uma contradição.

Seja $\mathcal{C}'$ o codigo de comprimento $n-d+1$ que resulta de $\mathcal{C}$ encurtando todas suas palavras pela eliminação das últimas $d-1$ posições. O argumento acima mostra que $|\mathcal{C}'| = |\mathcal{C}|$. Como $\mathcal{C}' \subset \mathcal{A}^{n-d+1}$ temos imediatamente que

$$A_q(n, d) = |\mathcal{C}| \leq a^{n-d+1}.$$

□

Exemplo 1.4.8.

Vamos avaliar o número $A_q(4, 3)$. Para um código com distância mínima 3 a capacidade é

$$\kappa = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$$

Utilizando a cota de Hamming, vem que

$$A_q(4, 3) \leq \frac{q^4}{(q-1)^0 + 4(q-1)} = \frac{q^4}{4q-3}.$$

Por outro lado, a cota de Singleton nos da:

$$A_q(4,3) \leq q^2.$$

É fácil ver que se $q \geq 4$, a cota de Singleton da uma limitação bem melhor que a cota de Hamming.

EXERCÍCIOS

1. Prove que todo código de repetição binário de comprimento ímpar é perfeito. Prove que os códigos que contém uma única palavra ou os códigos iguais a todo $\mathcal{A}^n$ são perfeitos. Estes são chamados os códigos perfeitos *triviais*.

2. Calcule os parâmetros do código de Hamming introduzido na seção §1.2 e mostre que é perfeito.

3. Seja $\mathcal{C}$ um código com capacidade κ. Diz-se que um inteiro positivo r é admissível para $\mathcal{C}$ se as esferas de centro em cada eleemnto de $\mathcal{C}$ e raio r são dois a dois disjuntas. Prove que

$$r = max\{r \in \mathbb{Z} \mid r \text{ é admissível } \}.$$

   (Por causa disso, r chama-se também o **raio de empacotamento** do código).

4. Chama-se **raio de recobrimento** de um código $\mathcal{C} \subset \mathcal{A}^n$ ao menor inteiro positivo r tal que

$$\bigcup_{c \in \mathcal{C}} B(c,r) = \mathcal{A}^n.$$

   Prove que $\mathcal{C}$ é perfeito se e somente se o seu raio de empacotamento é igual ao seu raio de recobrimento.

5. Provar que

   (i) $A_q(n,d) \leq q^n$, para todo inteiro positivo $d \leq n$.

   (ii) $A_q(n,1) = q^n$.

   (iii) $A_q(n,n) = q$.

6. Provar que $A_q(n,d) \leq qA_q(n-1,d)$ para todo $n \geq 2$ e todo inteiro positivo $d \leq n$.

7. Mostrar que $A_2(3,2) = 8$.

8. Mostrar que $A_2(6,5) = A_2(7,5) = 2$.

9. Prove que, se $d \leq d'$ então $A_q(n,d) \geq A_n(n,d')$.

10. Provar que, se d é um inteiro positivo ímpar, então $A_2(n+1,d+1) = A_2(n,d)$ e que, se d é par, então $A_2(n,d) = A_2(n-1,d-1)$.

Capítulo 2

Códigos lineares

Nesta seção, vamos construir um código binário de comprimento 6 de modo que as três primeiras componentes c_1, c_2, c_3 de cada palavra sejam de informação e vamos adicionar três outros dígitos de redundância. Para isso usaremos o fato de que, em $\mathbb{Z}_2 = \{0, 1\}$ existe uma operação de soma: *a soma módulo* 2. Definimos então os dígitos de redundância de acordo com a seguinte regra:

$$\begin{aligned} c_4 &= c_1 + c_2 \\ c_5 &= c_1 + c_3 \\ c_6 &= c_2 + c_3 \end{aligned} \qquad (1)$$

Usando a notação vetorial para as palavras do código, podemos dizer que elas são da forma

$$\mathbf{c} = (c_1, c_2, c_3, c_1 + c_2, c_1 + c_3, c_2 + c_3).$$

Podemos descrever o processo que transforma a informação na palavra $\mathbf{c}$ do código, usando notação matricial:

$$(c_1, c_2, c_3) \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix} = (c_1,\ c_2,\ c_3,\ c_1 + c_2,\ c_1 + c_3,\ c_2 + c_3).$$

Desta forma, quando (c_1, c_2, c_3) percorre todos os elementos de $\mathbb{Z}_2^3$, as res pectivas imagens produzem todas as palavras do código. Por este motivo, costuma-se chamar a matriz acima de **matriz geradora** do código.

Ainda, podemos re-escrever o sistema (1) na forma:

$$\begin{aligned} c_1 + c_2 + c_4 &= 0 \\ c_1 + c_3 + c_5 &= 0 \\ c_2 + c_3 + c_6 &= 0 \end{aligned}$$

o que significa que um vetor $\mathbf{y} = (y_1, y_2, y_3, y_4, y_5, y_6) \in \mathbb{Z}_2^6$ está no código se e somente se

$$(y_1, y_2, y_3, y_4, y_5, y_6) \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = (0, 0, 0).$$

Desta forma, temos um critério simples para decidir se um dado vetor recebido pertence, ou não, ao código. Por causa disso, a matriz acima diz-se uma **matriz de verificação** do código.

Como veremos adiante, este exemplo ilustra, de fato, uma situação geral.

2.1 Conceitos básicos

Para construir códigos de uma maneira eficiente e poder elaborar alguma teoria, resulta natural introduzir mais "estrutura algébrica". Inspirados no exemplo anterior faremos o seguinte:

- Tomaremos como alfabeto $\mathcal{A}$ um corpo finito com q elementos, que denotaremos por $\mathbb{F}$.
- Neste caso, o espaço ambiente, o conjunto $\mathbb{F}^n$ tem, de forma natural, uma estrutura de espaço vetorial de dimensão n sobre $\mathbb{F}$.
- Tomaremos então como códigos, não subconjuntos quaisquer de $\mathbb{F}^n$, mas apenas *subespaços* de $\mathbb{F}^n$, de dimensão $m < n$.

Se a dimensão de $\mathcal{C}$ é m, e $|\mathbb{F}| = q$, segue facilmente que o número de palavras de $\mathcal{C}$ é $M = q^m$. Neste caso, ao descrever o código, em vez de citar o número de palavras que ele contém vamos apenas citar sua dimensão.

Definição 2.1.1. *Um código $\mathcal{C}$ nas condições acima diz-se um* **(n,m)-código lineal** *sobre $\mathbb{F}$ e, se sua distância mínima d é conhecida, então ele diz-se também um (n,m,d)-código linear.*

Uma primeira vantagem dos códigos lineares é aparente quando queremos calcular sua distância mínima. Como um código linear $\mathcal{C}$ é um subespaço vetorial, se denotamos por $\mathbf{0}$ o elemento neutro da soma no espaço vetorial, temos que $\mathbf{0} \in \mathcal{C}$. Podemos então introduzir a seguinte.

Definição 2.1.2. *Dado um elemento $\mathbf{x}$ num código linear $\mathcal{C}$, chama-se* **peso** *de $\mathbf{x}$ ao número:*

$$w(\mathbf{x}) = d(\mathbf{x}, \mathbf{0}).$$

e chama-se **peso** *do código $\mathcal{C}$ ao número*

$$w(\mathcal{C}) = min\{w(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}, \mathbf{x} \neq \mathbf{0}\}.$$

Note que, dados $\mathbf{x} = (x_1, x_2, \ldots, x_n), \mathbf{y} = (y_1, y_2, \ldots, y_n) \in \mathcal{C}$ temos:

$$\begin{aligned} d(\mathbf{x}, \mathbf{y}) &= |\{i \mid x_i \neq y_i, 1 \leq i \leq n\}| = |\{i \mid x_i - y_i \neq 0, 1 \leq i \leq n\}| \\ &= d(\mathbf{x} - \mathbf{y}, \mathbf{0}) = w(\mathbf{x} - \mathbf{y}). \end{aligned}$$

Esta observação mostra que *toda* distância entre elementos do código $\mathcal{C}$ é também o peso de algum elemento. Conseqüentemente, temos que

$$\boxed{d(\mathcal{C}) = w(\mathcal{C}).} \tag{2.1}$$

Note que, para conhecer a distância mínima de um código com M palavras precisamos, teoricamente, avaliar $\binom{M}{2} = M(M-1)/2$ distâncias, em quanto que, para conhecer seu peso, precisamos apenas avaliar $M - 1$ distâncias (de cada um dos $M - 1$ elementos não nulos ao elemento $\mathbf{0}$).

Exemplo 2.1.3.

O conjunto $\mathcal{C} = \{0000, 1011, 0110, 1101\}$ é um subespaço vetorial de $\mathbb{Z}_2^4$. O conjunto

$$\mathcal{B} = \{1011, 1101\}$$

é uma base de $\mathcal{C}$.

Temos que:

$$w(1011) = 3, \qquad w(0110) = 2, \qquad w(1101) = 3,$$

portanto a distância mínima de $\mathcal{C}$ é 2 e trata-se de um (4,2,2)-código.

Vamos formalizar agora as idéias desenvolvidas no exemplo da seção anterior. Suponhamos que desejamos enviar mensagens com k dígitos de informação e $n-k$ dígitos de redundância. Podemos considerar que o *vetor de informação* é um elemento do espaço vetorial $\mathbb{F}^k$ e que o vetor já codificado, é um elemento do $\mathbb{F}^n$. Nosso código será então um subespaço $\mathcal{C} \subset \mathbb{F}^n$ de dimensão k.

Se $\{e_1, \ldots, e_k\}$ é a base canônica de de $\mathbb{F}^k$ e $\{c_1, \ldots, c_k\}$ é uma base de $\mathcal{C}$, a função linear

$$\nu : \mathbb{F}^k \longrightarrow \mathbb{F}^n \quad \text{tal que} \quad \nu(e_i) = c_i,\ 1 \leq i \leq k$$

é bijetora e $Im(\nu) = \mathcal{C}$.

Esta aplicação pode ser visualizada no seguinte diagrama:

$$\begin{array}{ccc} \mathbb{F}^k & \xrightarrow{\nu} & \mathbb{F}^n \\ | & & | \\ \mathbb{F}^k & \xrightarrow{\nu|_{\mathbb{F}^k}} & Im(\nu) = \mathcal{C} \end{array}$$

Vamos determinar a matriz G que representa a transformação linear ν nas bases canônicas de $\mathbb{F}^k$ e $\mathbb{F}^n$ respectivamente.[1]

Para isso, escrevemos os elementos da base de $\mathcal{C}$ na da base canônica de $\mathbb{F}^n$, que denotaremos por $B = \{f_1, \ldots, f_n\}$:

$$\left\{ \begin{array}{rcl} c_1 &=& b_{11}f_1 + b_{21}f_2 + \ldots + b_{n1}f_n \\ c_2 &=& b_{12}f_1 + b_{22}f_2 + \ldots + b_{n2}f_n \\ \vdots & & \vdots \quad \vdots \quad \vdots \\ c_k &=& b_{1k}f_1 + b_{2k}f_2 + \ldots + b_{nk}f_n \end{array} \right.$$

onde os coeficientes b_{ij} são elementos de $\mathbb{F}$.

Então a matriz procurada é:

$$G = \begin{bmatrix} b_{11} & b_{21} & \cdots & b_{k1} \\ b_{12} & b_{22} & \cdots & b_{k2} \\ \vdots & \vdots & & \vdots \\ b_{1n} & b_{2n} & \cdots & b_{kn} \end{bmatrix}$$

[1] Nós vamos descrever a função linear como uma multiplicação *à direita* pela matriz G, tal como é usual nos textos de teoria de códigos. Desta forma, a matriz que obteremos será *a transposta* daquela que é normalmente apresentada nos cursos de Álgebra Linear.

Note que cada linha da matriz G corresponde a um vetor que pertence ao código $\mathcal{C}$, ou seja, pode-se dizer que $\mathcal{C}$ é o subespaço de $\mathbb{F}^n$ gerado pelas linhas da matriz G (que formam, na realidade, uma base de $\mathcal{C}$). Os elementos de $\mathcal{C}$ são então todos as vetores $y \in \mathbb{F}^n$ da forma $x.G = y$, $\forall\ x \in \mathbb{F}^k$.

Definição 2.1.4. *Uma matriz $G \in \mathbb{M}_{n\times k}(\mathbb{F})$ cujas linhas formam uma base para $\mathcal{C}$ diz-se uma* **matriz de codificação** *de $\mathcal{C}$.*

Note que, para cada escolha de uma base para $\mathcal{C}$ obtemos uma matriz de codificação G diferente, de modo que esta matriz não é única.

Exemplo 2.1.5.

Seja $\mathbb{F}$ o corpo finito com dois elementos. Considere a transformação linear injetora

$$\begin{array}{rccc} \nu: & \mathbb{F}^3 & \longrightarrow & \mathbb{F}^5 \\ & (x_1,x_2,x_3) & \longmapsto & (x_1,x_3,x_1+x_2,x_2+x_3,x_2) \end{array}$$

Seja $\mathcal{C} = Im(\nu)$.

Sejam $\{e_1,e_2,e_3\}$ a base canônica de $\mathbb{F}^3$ e $\{f_1,f_2,f_3,f_4,f_5\}$ a base canônica de $\mathbb{F}^5$.

Vamos encontrar uma matriz G que representa a transformação linear ν.

Assim,

$$\begin{array}{rcccl} \nu(e_1) & = & (1,0,1,0,0) & = & 1f_1+0f_2+1f_3+0f_4+0f_5 \\ \nu(e_2) & = & (0,0,1,1,1) & = & 0f_1+0f_2+1f_3+1f_4+1f_5 \\ \nu(e_3) & = & (0,1,0,1,0) & = & 0f_1+1f_2+0f_3+1f_4+0f_5 \end{array}$$

Portanto, uma matriz de codificação G é da forma

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Exemplo 2.1.6.

Seja novamente $\mathbb{F}$ o corpo finito com dois elementos. Considere o código linear binário $\mathcal{C} \subset \mathbb{F}^5$ definido pela transformação linear injetora

$$\begin{array}{rccc} \nu: & \mathbb{F}^3 & \longrightarrow & \mathbb{F}^5 \\ & (x_1,x_2,x_3) & \longmapsto & (x_1,x_2,x_3,x_1+x_3,x_1+x_2) \end{array}$$

Sejam $\{e_1,e_2,e_3\}$ a base canônica de $\mathbb{F}^3$ e $\{f_1,f_2,f_3,f_4,f_5\}$ a base canônica de $\mathbb{F}^5$.

Vamos encontrar uma matriz G que representa a transformação linear ν.

Assim,

$$\begin{array}{rcccl} \nu(e_1) & = & (1,0,0,1,1) & = & 1f_1+0f_2+0f_3+1f_4+1f_5 \\ \nu(e_2) & = & (0,1,0,0,1) & = & 0f_1+1f_2+0f_3+0f_4+1f_5 \\ \nu(e_3) & = & (0,0,1,1,0) & = & 0f_1+0f_2+1f_3+1f_4+0f_5 \end{array}$$

Portanto, uma matriz de codificação G é da forma

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Seja $v \in \mathcal{C}$. Observe que as três primeiras coordenadas são os dígitos de informação logo, neste código, é muito fácil ler a informação enviada: por exemplo, se recebemos a palavra (10101), então a mensagem enviada foi (101).

Matrizes de codificação com a forma apresentada no exemplo acima recebe um nome especial na teoria dos códigos.

Definição 2.1.7. *Diz-se que uma matriz de codificação G de um código $\mathcal{C}$ está na* **forma padrão** *se ela é da forma $G = (I_k \ A)$, onde I_k é a matriz identidade de $M_k(\mathbb{F})$ e $A \in M_{(n-k)\times k}(\mathbb{F})$.*

Note que dado o código linear $\mathcal{C}$, como ele é um subespaço de $\mathbb{F}^n$de dimensão k, pode-se determinar uma função linear sobrejetora $\pi : \mathbb{F}^n \longrightarrow \mathbb{F}^{n-k}$ tal que $Ker(\pi) = \mathcal{C}$, por exemplo como descrevemos a seguir.

Dada uma base $\{c_1, \ldots, c_k\}$ de $\mathcal{C}$, ela pode ser extendida a uma base $\{c_1, \ldots, c_k, v_1, \ldots, v_{n-k}\}$ de $\mathbb{F}^n$.

Dado um vetor $v \in \mathbb{F}^n$ele pode ser escrito na forma

$$v = \lambda_1 c_1 + \cdots + \lambda_k c_k + \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k}$$

onde $\lambda_i \in \mathbb{F}$, $1 \leq i \leq n$.

Definimos então $\pi : \mathbb{F}^n \longrightarrow \mathbb{F}^{n-k}$ por

$$v \mapsto v' = \lambda_{k+1} v_1 + \cdots + \lambda_n v_{n-k}$$

e é fácil verificar que $Ker(\pi) = \mathcal{C}$.

Podemos representar esta função no seguinte diagrama:

$$\begin{array}{ccc} \mathbb{F}^n & \xrightarrow{\pi} & \mathbb{F}^{n-k} \\ | & & | \\ Ker(\pi) = \mathcal{C} & \longrightarrow & 0 \end{array}$$

Denotaremos por $H = (h_{ij})_{i,j} \in M_{n\times(n-k)}(\mathbb{F})$ a matriz de posto $(n-k)$ que representa a transformação linear π nas bases canônicas de $\mathbb{F}^n$e $\mathbb{F}^{n-k}$.

Como $Ker(\pi) = \mathcal{C}$ temos que o código linear $\mathcal{C}$ é, precisamente, o conjunto de todas as palavras $x \in \mathbb{F}^n$ tais que $x.H = 0$, de modo que multiplicar pela matriz H é uma forma de decidir se um dado vetor pertence, ou não, ao código $\mathcal{C}$.

Definição 2.1.8. *A matriz H construida acima diz-se uma* **matriz de verificação** *do código linear $\mathcal{C}$.*

Exemplo 2.1.9.

Seja $\mathbb{F}$ o corpo finito com dois elementos. Considere a transformação linear sobrejetora

$$\begin{array}{rccc} \pi: & \mathbb{F}^3 & \longrightarrow & \mathbb{F}^2 \\ & (x_1, x_2, x_3) & \longmapsto & (x_1 + x_2, x_3) \end{array}$$

cujo núcleo é $\mathcal{C} = Ker(\pi) = \{(x_1, x_1, 0) \mid x_1 \in \mathbb{F}\}$.

Agora, considere as bases canônicas $\{e_1, e_2, e_3\}$ e $\{f_1, f_2\}$, de $\mathbb{F}^3$ e $\mathbb{F}^2$ respectivamente.

Vamos achar a matriz H que representa a transformação linear π nessas bases.

Temos que

$$\begin{array}{rcccl} \pi(e_1) & = & \pi(100) & = & 1f_1 + 0f_2 \\ \pi(e_2) & = & \pi(010) & = & 1f_1 + 0f_2 \\ \pi(e_3) & = & \pi(001) & = & 0f_1 + 1f_2 \end{array}$$

Portanto, a matriz é:

$$H = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Dado um vetor qualquer $y \in \mathbb{F}^3$, para verificarmos se ele pertence ao código $\mathcal{C}$, precisamos verificar se a condição $y.H = 0$ é satisfeita.

Dados $y = (1, 1, 1)$ e $z = (1, 1, 0) \in \mathbb{F}^3$, como

$$y.H = (0,\ 1) \quad \text{e} \quad z.H = (0,\ 0)$$

temos que $y \notin \mathcal{C}$ e $z \in \mathcal{C}$.

A matriz de verificação de um código contém informações que permitem determinar o peso do mesmo. como veremos a seguir.

Lema 2.1.10. *Seja H uma matriz de verificação de um código $\mathcal{C}$. Se existe $v \in \mathcal{C}$ de peso $\omega(v) = t$ então existem t colunas de H que são linearmente dependentes.*

Demonstração. Seja $y = (y_1, y_2, \ldots, y_n) \in \mathcal{C}$ um vetor de peso t e sejam $L_1, l_2, \ldots L_n$ as linhas de H. Como $y \in \mathcal{C}$ e H é uma matriz de verificação de $\mathcal{C}$, temos que

$$0 = yH = (y_1, y_2, \ldots, y_n) \begin{bmatrix} L_1 \\ L_2 \\ \cdots \\ L_n \end{bmatrix} = y_1 L_1 + y_2 L_2 + \cdots + y_n L_n.$$

Como há exatamente t coeficientes não nulos na equação acima, isso significa que as t linhas correspondentes são linearmente dependentes. □

Lema 2.1.11. *Seja H uma matriz de verificação de um código $\mathcal{C}$. Se existem t colunas de H que são linearmente dependentes, então $\omega(\mathcal{C}) \leq t$.*

Demonstração. Suponhamos que existem t linhas $L_{i_1}, L_{i_2}, \ldots L_{i_t}$ de H que são linearmente dependentes. então existem escalares $y_{i_1}, y_{i_2}, \ldots, y_{i_t}$, não todos nulos, tais que

$$y_{i_1} L_{i_1} + y_{i_2} L_{i_2} + \cdots + y_{i_t} L_{i_t} = 0.$$

Seja então $y \in \mathbb{F}^n$ o vetor que tem coordenada y_{i_j} na posição i_j, $1 \leq j \leq t$, e coordenada igual a 0 nas outras posições. Então $y \neq 0$ e

$$yH = y_{i_1} L_{i_1} + y_{i_2} L_{i_2} + \cdots + y_{i_t} L_{i_t} = 0.$$

Isto significa que $y \in \mathcal{C}$. Como no máximo t coodenadas de y são não nulas, temos que $\omega(y) \leq t$. Ainda

$$\omega(\mathcal{C}) \leq \omega(y)$$

donde segue a tese. □

Dos dois lemas acima resulta imediatamente o seguinte.

Teorema 2.1.12. *Seja H uma matriz de verificação de um código $\mathcal{C}$. Então, o peso de $\mathcal{C}$ é igual a um inteiro d, se e somente se, qualquer conjunto de $d-1$ linhas de H é linearmente independentes e existem d linhas de H que são linearmente dependentes.*

A cota de Singleton para um código linear.

Mostramos, no Teorema 1.4.7 que o número máximo de palavras de um código q-ário de comprimento n, com distância mínima d, é

$$A_q(n, d) \leq q^{n-d+1}.$$

Como já observamos, se o código em questão é linear, de dimensão m, então o número de palavras no código é $M = q^m$. Portanto, temos que

$$q^m \leq q^{n-d+1}$$

donde

$$m \leq n - d + 1.$$

Assim, obtemos uma cota para o valor da dimensão de um código, dado o comprimento e a distância mínima.

Definição 2.1.13. *labelmds Um código diz-se* **separável pela distância máxima** *ou um* **código MDS**[2] *se vale a igualdade*

$$m = n - d + 1.$$

[2]Do inglês: maximum distance separable.

Exemplo 2.1.14.

Considere o código da seção §3.1 que, como vimos, tem matriz de codificação

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

e matriz de verificação

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Como estamos trabalhando sobre $\mathbb{F}_2$, tem-se que duas linhas são dependentes se e somente se são iguais. Portanto, é imediato verificar que quaisquer duas linhas de H são independentes.

Por outro lado, é fácil verificar que as três primeiras linhas de H são linearmente dependentes (pois a terceira é a soma das duas primeiras). Logo, pelo Teorema 2.1.12 temos que a distância mínima de $\mathcal{C}$ é $d = 3$. Como $n = 6$ e $m = 3$ temos que $n - d + 1 = 6 - 3 + 1 = 4 > m$, logo este não é um código MDS.

Exemplo 2.1.15.

Considere agora o código $\mathcal{C}$ cuja matriz de codificação é

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 10 & 1 & \end{bmatrix}$$

e matriz de verificação

$$H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}.$$

Novamente vemos que duas linhas de G são sempre linearmente independentes e a terceira é soma das duas primeiras donde ô peso deste código é $d = 3$. Claramente $n = 6$ e $m = 4$. Então temos: $n - d + 1 = 6 - 3 + 1 = 4 = m$. Consequentemente, este é um código MDS.

EXERCÍCIOS

1. Dado um corpo finito $\mathbb{F}$, considere o código de repetição:

$$\mathcal{C} = \{\underbrace{aa\ldots a}_{\text{n vezes}} \mid a \in \mathbb{F}\}.$$

Provar que este é um código linear, determinar seus parâmetros e exibir uma matriz de codificação e uma matriz de veificação de $\mathcal{C}$.

2. Dado um corpo finito $\mathbb{F}$, considere o código de repetição:

$$\mathcal{C} = \{\underbrace{a_1a_1\ldots a_1}_{\text{n vezes}}, \ldots, \underbrace{a_ta_t\ldots a_t}_{\text{n vezes,}} \mid a_i \in \mathbb{F}, 1 \leq i \leq t\}.$$

Provar que este é um código linear, determinar seus parâmetros e exibir uma matriz de codificação e uma matriz de veificação de $\mathcal{C}$.

3. Considere o código binário *de verificação de paridade*:

$$\mathcal{C} = \left\{(c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n \mid c_n = \sum_{i=1}^{n-1} c_i\right\}.$$

Provar que este é um código linear, determinar seus parâmetros e exibir uma matriz de codificação e uma matriz de veificação de $\mathcal{C}$.

4. Seja V um espaço vetorial de dimensão n sobre um corpo $\mathbb{F}$ com q elementos. Provar que existem

$$\frac{1}{n!}\prod_{i=0}^{n}(q^n - q^i)$$

bases diferentes em V.

(Sugestão: observe que, para construir uma base $\{b_1, b_2, \ldots b_n\}$ de V, podemos escolher como b_1 qualquer vetor não nulo de V; já b_2 pode ser qualquer vetor não nulo de V que não seja um múltiplo escalar de b_1, etc.)

5. Seja $\mathcal{C}$ um código binário com matriz de verificação

$$H = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Determinar todas as palavras de $\mathcal{C}$.

6. Seja $\mathcal{C}$ um código binário com matriz de codificação

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Determinar uma matriz de verificação para $\mathcal{C}$

7. Seja $\mathcal{C}$ um código linear binário. Provar que a função $\omega : \mathcal{C} \to \mathbb{F}_2$ que a cada palavra $c \in \mathcal{C}$ associa o seu peso $\omega(c) \in \mathbb{F}_2$ é uma função linear.

8. Seja $\mathcal{C}_i$ um (n_1, m_i, d_i)-código linear, com matriz geradora G_i $i = 1, 2$. Provar que o código com matriz geradora

$$\begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix},$$

é a soma direta dos códigos $\mathcal{C}_1$ e $\mathcal{C}_2$, como definida no exercício 13 do Capítulo 1 e, consequentemente, um $(n_1 + n_2, m_1 + m_2, d)$-código, onde $d = min(d_1, d_2)$.

9. Seja $\mathcal{C}$ um código linear de $\mathbb{F}_2^n$. Se $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ e $\mathbf{v} = ((v_1, v_2, \ldots, v_n)$ são elementos de $\mathcal{C}$, define-se a **interseção** de ambos como o vetor $\mathbf{u} \cap \mathbf{v}$ que tem um coeficiente igual a 1 na posição i se e somente se $u_i = v_i = 1$, $1 \leq i \leq n$. Provar que

   (i) $\mathbf{u} \cap \mathbf{v} = (u_1 v_1, u_2 v_2, \ldots, u_n v_n)$.

   (ii) $\omega(\mathbf{u} + \mathbf{v}) = \omega(\mathbf{u}) + \omega(\mathbf{v}) - 2\omega(\mathbf{u} + \mathbf{v})$.

10. Seja $\mathcal{C}$ um código linear binário. Provar que se $\mathcal{C}$ contém uma palavra de peso ímpar, então metade das palavras de $\mathcal{C}$ têm peso ímpar e a outra metade têm peso par.

11. Um **código expurgado** de um código $\mathcal{C}$ é qualquer código $\mathcal{C}'$ que se obtém a partir de $\mathcal{C}$ simplesmente suprimindo alguma de suas palavras. Usar o exercício anterior para provar que se $\mathcal{C}$ é um $(n.m.d)$-código linear binário que contém uma palavra de peso ímpar, então o código que se obtém expurgando de $\mathcal{C}$ todas as palavras de peso ímpar é um $(n, m-1, d')$-código, com $d' \geq d$ e que, se d é ímpar, então $d' > d$.

12. Seja $\mathcal{C}$ um código linear binário. Provar que, se $\mathbf{1} = (1, 1, , \ldots, 1) \in \mathcal{C}$ então $\mathcal{C} = \mathcal{C}^c$ e que se $\mathbf{1} \notin \mathcal{C}$ então $\mathcal{C} \cap \mathcal{C}^c = \emptyset$.

13. Mostre que se uma matriz geradora de um $(n.m)$-código linear está na forma $G = [A \mid I_{m \times m}] \in M_{m \times n}$, então a matriz

$$H = \begin{bmatrix} I_{(n-m)\times(n-m)} \\ -A^t \end{bmatrix},$$

   onde A^t indica a matriz transposta de A, é uma matriz de verificação deste código.

14. Seja $\mathcal{C}$ um código binário, de comprimento $n \geq 4$ com matriz de verificação H. Provar que, se as linhas de H são diferentes duas a duas e todas elas têm peso ímpar, então o peso de $\mathcal{C}$ é pelo menos igual a 4.

15. Seja $\mathcal{C}$ um código linear com matriz geradora G. Seja G_0 a matriz que se obtém a partir de G executando um número finito de operações do seguinte tipo:

    (a) (ℓ_1) Permutar duas linhas de G.

    (b) (ℓ_2) Multiplicar uma linha por um escalar não nulo.

    (c) (ℓ_3) Somar duas linhas.

    Provar que G_0 é também uma matriz de codificação de $\mathcal{C}$.

16. Seja $\mathcal{C}$ um código linear com matriz geradora G. Seja G_1 a matriz que se obtém a partir de G executando um número finito de operações do tipo (ℓ_1), (ℓ_1) e (ℓ_1) acima e também operações do seguinte tipo:

    (a) (c_1) Permutação de duas colunas.

(b) (c_2) Multiplicação de uma coluna por um escalar não nulo.

Provar que G_1 é uma matriz de codificação de um código $\mathcal{C}_1$ equivalente a $\mathcal{C}$.

17. Usar o exercício anterior para mostrar que todo código $\mathcal{C}$ é equivalente a um código $\mathcal{C}_1$ que tem uma matriz geradora na forma padrão.

18. Seja G uma matriz de codificação de um código linear $\mathcal{C}$ de dimensão m sobre um corpo $\mathbb{F}$ e seja $A \in M_n(\mathbb{F})$ uma matriz inversível. Provar que AG é também uma matriz de codificação de $\mathcal{C}$.

19. Seja G uma matriz de codificação de um código linear $\mathcal{C}$ de dimensão m sobre um corpo $\mathbb{F}$ e seja $P \in M_n(\mathbb{F})$ uma matriz de permutação (i.e. uma matriz que tem exatamente um coeficiente igual a 1 em cada linha e em cada coluna e os demais coeficientes são todos iguais a 0). Provar que PG é uma matriz de codificação de um codigo $\mathcal{C}'$ equivalente a $\mathcal{C}$.

20. Prove que um $(q+1, q^2, q)$-código q-ário, com q ímpar, é perfeito se e somente se $q+3$.

21. Mostre que todo código linear com parámetros $(n, n, 1)$, $(n, 1, n)$ ou $(n, n-1, 2)$ é MDS (estes são chamados *códigos MDS triviais*).

22. Prove que um código $\mathcal{C}$ com matriz de verificação H é um código MDS se e somente se todo conjunto com $n-m$ linhas de H é linearmente independente.

2.2 Decodificação

Chama-se decodificação ao procedimento de detecção e correção de erros num determinado código. Suponhamos que um vetor x transmitido sofreu a influência de um "ruído" e foi recebido como outro vetor y.

Definição 2.2.1. *O vetor diferença e entre um vetor recebido y e o vetor transmitido x chama-se o* **vetor erro**, *isto é,*

$$e = y - x.$$

Note que o peso do vetor erro corresponde, precisamente, ao número de erros ocorridos numa palavra recebida. É claro que, ao receber o vetor y, deve se multiplicar pela matriz H para saber se ele contém, ou não, erros.

Definição 2.2.2. *Seja $\mathcal{C}$ um (n,k)-código linear, com matriz de teste H. Dado um vetor $y \in \mathbb{F}^n$, o vetor*

$$S(y) = y.H$$

é chamada de **síndrome** *de y.*

Então o vetor y recebido é efetivament uma palavra do código se e somente se o seu síndrome é o vetor nulo. Se y é um vetor recebido, com vetor de erro e, tem-se que

$$y.H = (x+e).H = x.H + e.H = e.H.$$

Assim, *o vetor recebido e o vetor erro têm ambos o mesmo síndrome.*

O próximo resultado é de verificação imediata.

Lema 2.2.3. *Dois vetores x e y de $\mathbb{F}^n$ tem a mesma síndrome se, e somente se, $x \in y+\mathcal{C}$.*

Definição 2.2.4. *O subconjunto $y+\mathcal{C}$ de $\mathbb{F}^n$ chama-se a* **classe lateral** *de y determinada por $\mathcal{C}$.*

Um vetor de peso mínimo numa classe lateral diz-se um **líder** *da classe.*

Exemplo 2.2.5.

Considere o $(6,3)$-código binário $\mathcal{C}$ cuja matriz de codificação é

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

Então, $\mathcal{C}$é o seguinte subespaço de $\mathbb{F}^6$:

$$\mathcal{C} = \{000000,\ 100110,\ 010101,\ 001011,\ 011110,\ 101101,\ 110011,\ 111000\}$$

e as classes laterais segundo $\mathcal{C}$ são:

$$\begin{array}{lcl} 000000+\mathcal{C} & = & \{000000,\ 100110,\ 010101,\ 001011,\ 011110,\ 101101,\ 110011,\ 111000\} \\ 000001+\mathcal{C} & = & \{000001,\ 100111,\ 010100,\ 001010,\ 011111,\ 101100,\ 110010,\ 111001\} \\ 000010+\mathcal{C} & = & \{000010,\ 100100,\ 010111,\ 001001,\ 011100,\ 101111,\ 110001,\ 111010\} \\ 000100+\mathcal{C} & = & \{000100,\ 100010,\ 010001,\ 001111,\ 011010,\ 101001,\ 110111,\ 111100\} \\ 001000+\mathcal{C} & = & \{001000,\ 101110,\ 011101,\ 000011,\ 010110,\ 100101,\ 111011,\ 110000\} \\ 010000+\mathcal{C} & = & \{010000,\ 110110,\ 000101,\ 011011,\ 001110,\ 111101,\ 100011,\ 101000\} \\ 100000+\mathcal{C} & = & \{100000,\ 000110,\ 110101,\ 101011,\ 111110,\ 001101,\ 010011,\ 011000\} \\ 000111+\mathcal{C} & = & \{000111,\ 100001,\ 010010,\ 001100,\ 011001,\ 101010,\ 110100,\ 111111\} \end{array}$$

Neste caso temos que:

000000 é o líder de $\mathcal{C}$;
000001 é o líder de 000001+ $\mathcal{C}$;
000010 é o líder de 000010+ $\mathcal{C}$;
000100 é o líder de 000100+ $\mathcal{C}$;
001000 é o líder de 001000+ $\mathcal{C}$;
010000 é o líde de 010000+ $\mathcal{C}$;
100000 é o líder de 100000+ $\mathcal{C}$;
$100001, 010010, 001100$ são líderes de 000111+ $\mathcal{C}$.

O exemplo acima mostra que uma determinada classe lateral pode ter mais de um líder. Porém, podem-se demonstrar os seguintes resultados.

Teorema 2.2.6. *Seja $\mathcal{C}$ um código linear em $\mathbb{F}^n$ com distância mínima d. Se um vetor $x \in \mathbb{F}^n$ é tal que $\omega(x) \leq \kappa$ então x é o único líder de sua classe.*

Teorema 2.2.7. *Seja $\mathcal{C}$ um código linear em $\mathbb{F}^n$ com distância mínima d e seja $y \in \mathbb{F}^n$. Então existe $x \in \mathcal{C}$ tal que $d(y,x) \leq \kappa$ se, e somente se, existe $e \in y + \mathcal{C}$ tal que $\omega(e) \leq \kappa$. E neste caso, e é o vetor erro e a palavra enviada é $x = y - e$.*

Estes resultados permitem formular um algoritmo para determinar se uma palavra recebida contém erros e, em caso afirmativo, efetuar a correção correspondente:

- Recebida uma palavra y, deve-se calcular seu síndrome $S(y) = y.H$.
- Se $S(y) = 0$ então a palavra recebida não contém erros. Se $S(y) \neq 0$ então a palavra y não pertence ao código.
- Neste último caso, deve-se procurar a classe lateral de y determinada por $\mathcal{C}$ e achar seu líder e.
- O vetor enviado é $x = y - e$.

Exemplo 2.2.8.

Considereo código do Exemplo 2.2.5. Uma matriz de verificação deste código é:

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

Usando o Teorema 2.1.12 vemos que $d = 3$ e, portanto, $\kappa = 1$.

Os vetores de peso menor ou igual a 1 com as suas respectivas síndromes estão relacionados na tabela abaixo

líder	síndrome
000000	000
000001	001
000010	010
000100	100
001000	011
010000	101
100000	110

Suponhamos que a foi recebida a palavra $y = (010111)$.

Calculamos: $y.H = (0\ 1\ 0)$.

Verificamos então que $e = (000010)$ e a palavra enviada é, portanto:

$$x = y - e = (010101).$$

EXERCÍCIOS

1. Seja $\mathcal{C}$o código linear binário gerado pelos vetores

$$\{10001,\ 01010,\ 00100,\ 101010\}.$$

Determine uma matriz de verificação para $\mathcal{C}$', as classes laterais de $\mathcal{C}$ em $\mathbb{F}_2^5$ e a tabela de síndromes correspondente.

2. Idem, para o código $\mathcal{C}$ de $\mathbb{F}_3^4$ gerado pelos vetores

$$\{1010, 0101\}$$

3. Seja $\mathcal{C}$ o código linear que tem por matriz de verificação a matriz

$$H = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

(i) Determinar sua distância mínima, sua capacidade, os síndromes e os respectivos líderes.

(ii) Se as palavras $\mathbf{u} = 100011$ e $\mathbf{v} = 111111$ foram recebidas, quais foram as palavras enviadas?

4. Seja $\mathcal{C}$ um código com matriz de codificação

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

(i) Determinar os parâmetros de $\mathcal{C}$ e uma matriz de verificação.

(ii) Achar as classes laterais de $\mathcal{C}$ e seus respectivos líderes.

(iii) Decodificar a palavra $y = 1110$.

5. Achar a dimensão e distância mínima do código com matriz de codificação

$$G = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

Determinar as classes laterais deste código, os respectivos líderes e decodificar as palavras $y_1 = 11111$ e $y_2 = 10000$.

6. Considere o código binário $\mathcal{C}$ com matriz de codificação

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

(i) Determinar a dimensão de $\mathcal{C}$.

(ii) Achar uma matriz de verificação para $\mathcal{C}$ e calcular o peso deste código.

(iii) Determine o número de classes de $\mathcal{C}$ e os síndromes correspondentes.

7. Seja $\mathcal{C}$ um código linear com peso d par. Mostrar que existe alguma classe lateral de $\mathcal{C}$ que contém dois vetores de peso

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor$$

2.3 O dual de um código linear

Dado um corpo $\mathbb{F}$, no espaço vetorial $\mathbb{F}^n$ pode-se definir um **produto interno** de forma natural:

Dados dois vetores $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ e $\mathbf{y} = (y_1, y_2, \ldots, y_n)$ definimos:

$$\mathbf{x} \cdot \mathbf{y} = x_1y_1 + x_2y_2 + \cdots + x_ny_n.$$

ou, considerandoambos vetores como matrizes-linha, também podemos escrever

$$\mathbf{x} \cdot \mathbf{y} = \mathbf{x} \cdot \mathbf{y}^t$$

onde $\mathbf{y}^t$ indica a transposta de $\mathbf{y}$; isto -e, $\mathbf{y}$ escrito como vetor-coluna.

O leitor poderá demonstrar, sem dificuldade, que o produto interno assim definido tem propriedades similares as do produto interno de espaços vetoriais sobre os reais, que ele provavelmente conhece dos cursos de álgebra linaer, que enunciamos a seguir.

Proposição 2.3.1. *Sejam $\mathbb{F}$ um corpo, sejam $\mathbf{x}, \mathbf{y}$ e $\mathbf{z}$ vetores de $\mathbb{F}^n$ e λ um escalar de $\mathbb{F}$. Então, valem as seguintes propriedades:*
(i) $(\mathbf{x} + \mathbf{y}) \cdot \mathbf{z} = \mathbf{x} \cdot \mathbf{z} + \mathbf{y} \cdot \mathbf{x}$.
(ii) $\mathbf{x} \cdot (\mathbf{y} + \mathbf{z}) = \mathbf{x} \cdot \mathbf{y} + \mathbf{x} \cdot \mathbf{z}$.
(iii) $(\lambda\mathbf{x}) \cdot \mathbf{y} = \mathbf{x} \cdot (\lambda\mathbf{y}) = \lambda(\mathbf{x} \cdot \mathbf{y})$.
(iv) $\mathbf{x} \cdot \mathbf{y} = \mathbf{y} \cdot \mathbf{x}$.
(v) $\mathbf{x} \cdot \mathbf{y} = 0$, *para todo* $\mathbf{x} \in V$, *se e somente se* $\mathbf{y} = 0$.
(v) $\mathbf{x} \cdot \mathbf{y} = 0$, *para todo* $\mathbf{y} \in V$, *se e somente se* $\mathbf{x} = 0$.

Há, porém, uma diferença notável. No caso do produto interno sobre os reais tem-se que $\mathbf{x} \cdot \mathbf{x} = 0$ se e somente se $\mathbf{x} = 0$. Isto não é necessáriamente verdadeiro no caso de corpos arbitrários. Considere, por exempo, o vetor $\mathbf{x} = (1, 0, , 1, 1, 0, 1) \in \mathbb{F}_2^6$. Neste caso, temos que

$$\mathbf{x} \cdot \mathbf{x} = 1 + 1 + 1 + 1 = 0 \quad \text{em } F_2.$$

Definição 2.3.2. *Seja $\mathcal{C}$ um (n,k)-código linear q-ário. O conjunto*

$$\mathcal{C}^\perp = \{\mathbf{u} \in \mathbb{F}_q^n \mid \mathbf{u} \cdot \mathbf{v} = 0, \forall \mathbf{v} \in \mathcal{C}\}.$$

diz-se o **código dual** *do código $\mathcal{C}$.*

Teorema 2.3.3. *Se G é uma matriz geradora de um código linear $\mathcal{C}$ sobre um corpo $\mathbb{F}$, então a matriz transposta G^t é uma matriz de verificação para o código dual $\mathcal{C}^\perp$.*

Demonstração.
Se $\mathcal{C}$ é um (n, m)-código e $G \in M_{m\times n}(\mathbb{F})$ é a matriz geradora de $\mathcal{C}$, então pôsto(G)=m e

$$\mathcal{C} = \{\mathbf{x}G \mid \mathbf{x} \in \mathbb{F}^m\}.$$

Então, um vetor $\mathbf{y}$ pertence a $\mathcal{C}^\perp$ se e somente se $\mathbf{x}G \cdot \mathbf{y}^t = 0$ para todo $\mathbf{x} \in \mathbb{F}^m$ ou, equivalentemente, se e só se

$$0 = \mathbf{y} \cdot G^t\mathbf{x} = \mathbf{y}G^t \cdot \mathbf{x} \quad \text{para todo} \quad \mathbf{x} \in \mathbb{F}^m.$$

Comforme observado na parte (v) da Proposiçãp 2.3.1, isto implicqa que $yG^t = 0$. Assim $y \in \mathcal{C}^\perp$ se e somente se $yG^y = 0$ donde G^t é uma matriz de verificação para $\mathcal{C}^\perp$. □

O leitor deve lembrar que, no caso de espaços vetoriais sobre o corpo dos números reais, para um subespaço $\mathcal{C}$ de $\mathbb{R}^n$ vale que $\mathcal{C} \cap \mathcal{C}^\perp = \{0\}$ e $\mathcal{C} \oplus \mathcal{C}^\perp = \mathbb{R}^n$. ainda, desta última equação resulta que, se $dim(\mathcal{C}) = m$ então $dim(\mathcal{C}^\perp) = n-m$. Nosso próximo exemplo mostrará que duas equaçãoes acima não valem no caso dos corpos finitos.

Exemplo 2.3.4.

Considere o conjunto $\mathcal{C} = \{0000,\ 1111\}$ que é, claramente, um subespaço de $\mathbb{F}_2^4$. É fácil provar diretamente que se $y \in \mathcal{C}^\perp$ então, em particular deve ser $y \cdot (1111) = 0$ donde

$$\mathcal{C}^\perp = \{0000,\ 1111,\ 1010,\ 0101,\ 1001,\ 0110]).$$

consequentemente

$$\mathcal{C} \cap \mathcal{C}^\perp = \mathcal{C} \neq \{0\} \quad \text{e} \quad \mathcal{C} \oplus \mathcal{C}^\perp = \mathcal{C}^\perp \neq \mathbb{F}_2^4.$$

Porém, ainda ainda vale o cálculo da dimensão.

Proposição 2.3.5. *Seja $\mathbb{F}$ um corpo finito e seja $\mathcal{C}$ um subespaço de dimensão m de $\mathbb{F}^n$. Então*

$$dim(\mathcal{C}^\perp) = n - m.$$

Demonstração. Note que, se G é uma matriz geradora de $\mathcal{C}$ então pôsto(G)=m, donde pôsto(G^t)=m. Pelo Teorema 2.3.3, G^t é a matriz de verificação de $\mathcal{C}^\perp$; logo

$$dim(\mathcal{C}^\perp) = n - \text{pôsto}(G) = n - m$$

□

Corolario 2.3.6. *Se $\mathcal{C}$ é um código linear, então*

$$\mathcal{C}^{\perp\perp} = \mathcal{C}.$$

Demonstração. Das próprias definições, segue que $\mathcal{C} \subset \mathcal{C}^{\perp\perp}$. Ainda,

$$dim(\mathcal{C}^{\perp\perp}) = n - (n - m) = m.$$

donde segue a tese. □

Seja $\mathcal{C}$ um código linear com matriz geradora G e seja H_1 uma matriz geradora de $\mathcal{C}^\perp$. Como G^t é uma matriz de verificação para $\mathcal{C}^\perp$ temos que $H_1 G^t = 0$, o que implica que $GH_1^t = 0$.

Ainda, como pôsto(H_1^t) = pôsto(H_1) = dim$(\mathcal{C}^\perp)$=$n - m$, temos que H_1^t é uma matriz de verificação para $\mathcal{C}$.

Definição 2.3.7. *Uma matriz geradora do código $\mathcal{C}^\perp$ chama-se uma* **matriz de teste de paridade** *para o código $\mathcal{C}$.*

Note que, conforme nossas definições, uma matriz de verificação é sempre a transposta de uma matriz de teste de paridade. Muitos livros utilizam esta idéia para falar em detecção e correção de erros e, consequentemente, os resultados que obtivemos neste capítulo aparecem trocando linhas por colunas. Em particular, o Teorema 2.1.12 aparece na seguinte forma.

Teorema 2.3.8. *Seja H uma matriz de teste de paridade de um código $\mathcal{C}$. Então, o peso de $\mathcal{C}$ é igual a um inteiro d, se e somente se, qualquer conjunto de $d-1$ colunas de H é linearmente independentes e existem d colunas de H que são linearmente dependentes.*

EXERCÍCIOS

1. Provar diretamente, a partir das definições correspondentes, que si $\mathcal{C}$ é um código linear, então $\mathcal{C}^{\perp}$ é um subespaço.

2. Prove que, se $\mathcal{C}_1$ e $\mathcal{C}_2$ são dois códigos de um mesmo espaço vetorial, então
$$(\mathcal{C}_1 + \mathcal{C}_2)^{\perp} = \mathcal{C}_1^{\perp} \cap \mathcal{C}_2^{\perp}.$$

3. Prove que H é uma matriz de verificação de um código linear $\mathcal{C}$, se e somente se H^t é uma matriz geradora do código $\mathcal{C}^{\perp}$.

4. Provar que, se H é uma matriz de verificação para um código linear $\mathcal{C}$, então H^t é uma matriz geradora para o código $\mathcal{C}^{\perp}$.

5. Mostrar que o código binário
$$\mathcal{C} = \{0000, 1100, 0011, 1111\}.$$
é um $(4,2)$-código linear e calcular dua distância mínima. Achar uma matriz geradora e uma matriz de verificação para $\mathcal{C}$ e também para $\mathcal{C}^{\perp}$.

6. Prove que o código $\mathcal{C}$ do Exemplo 2.3.4 é auto-ortogonal e o código $\mathcal{C}^{\perp}$ é auto-dual.

7. Seja $\mathcal{C}$ um código de $\mathbb{F}^n$ de dimensão m. Provar que

   (i) Se $\mathcal{C}$ é auto-ortogonal, então $m \leq n/2$.

   (ii) Se $\mathcal{C}$ é auto-ortogonal, então $m = n/2$.

8. Seja $\mathcal{C}$ um código binário. Prove que:

   (i) $\mathcal{C}$ é auto-ortogonal se e somente se as linhas de uma matriz geradora são otogonais duas a duas e o peso de cada uma delas é múltiplo de 2.

   (ii) Se $\mathcal{C}$ é auto-ortogonal, então todo vetor de $\mathcal{C}$ tem peso par. (Sugestão: utilice indução e o exercício 9).

   (iii) Se as linhas de uma matriz geradora de $\mathcal{C}$ são otogonais duas a duas e o peso de cada uma delas é múltiplo de 4, então $\mathcal{C}$ é auto-ortogonal e todos os vetores de $\mathcal{C}$ têm peso m;ultiplo de 4.

9. Provar que, se $\mathcal{C}$ é un código binário auto-dual, então:

   (i) O vetor $\mathbf{1} = 1111\cdots1$ pertence a $\mathcal{C}$.

   (ii) Se existe algúm vetor de $\mathcal{C}$ cujo peso não é multiplo de 4, então metade dos vetores de $\mathcal{C}$ tem peso que é múltiplo de 4 e os da outra metade tem peso que não é múltiplo de 4.

10. (i) Provar que se um código ternário $\mathcal{C}$ é auto-ortogonal, então todos os vetores de $\mathcal{C}$ tem peso divisível por 3.

    (ii) Dar um exemplo de um código auto-ortogonal sobre $\mathbb{F}_5$ que contém vetores com peso que não é múltiplo de 5.

11. Provar que o código $\mathcal{C}$ com matriz geradora

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

    é um código auto-dual.

Referências Bibliográficas

[1] www.microprocessadores.hpg.ig.com.br

[2] www.jpl.nasa.gov

[3] Golay, M.J.E., Notes on digital coding, *Proceedings of the I. R. E. (I. E. E. E.)*, **27** (1948) 657.

[4] Hamming, R.W., Interview, February 3 - 4, 1977.

[5] Hamming, R.W., Error Detecting and Error Correcting Codes, The Bell System Technical Journal, vol. XXVI, pg 379 - 423, 623 - 656, July, October, 1948.

[6] Shannon, C.E., A Mathematical Theory of communication, The Bell System Technical Journal, vol. XXVIII, april, 1950, n.o 2.