Orlando Sá Couto

Isometrias em Teoria de Códigos

Departamento de Matemática

Faculdade de Ciências da Universidade do Porto

2010

Orlando Sá Couto

Isometrias em Teoria de Códigos

Tese submetida à Faculdade de Ciências da
Universidade do Porto para obtenção do grau de Mestre
em Matemática para Professores

Departamento de Matemática
Faculdade de Ciências da Universidade do Porto
2010

Para as minhas filhas e para os meus pais.

Agradecimentos

- ao Professor Doutor Christian Lomp pela disponibilidade, apoio científico e atenção que dedicou à orientação do trabalho;

- aos meus pais e às minhas filhas pelas frequentes perguntas sobre o trabalho e incentivo à finalização do mesmo;

- aos amigos que me motivaram para este desafio e se interessaram, ouvindo-me tanto nas fases mais conseguidas como nas mais difíceis.

Resumo

Esta tese tem por objectivo mostrar a importância da distribuição de pesos e das isometrias na Teoria de Códigos. O estudo é feito para códigos de bloco, em particular para códigos lineares, e foca dois aspectos: por um lado a determinação da distribuição de pesos das palavras de um código linear e as informações que daí resultam em termos de capacidade de detecção e correcção de erros e, por outro, em que medida as isometrias determinam a equivalência de códigos.

São apresentados alguns conceitos fundamentais para a compreensão dos três resultados principais:

- o teorema de Constantinescu, que refere quais as funções que preservam a distância de Hamming;

- a Identidade de MacWilliams, que permite determinar a distribuição de pesos das palavras de um código linear;

- o teorema de MacWilliams para a equivalência de códigos, que estabelece condições para que dois códigos lineares sejam equivalentes e, portanto, mantenham iguais determinadas características.

Em alguns dos exemplos apresentados são referidos códigos importantes, designadamente, os códigos de Hamming e os códigos de Golay.

Conteúdo

Capítulo 1

Códigos: conceitos iniciais

Neste capítulo, faz-se uma breve referência ao aparecimento da Teoria de Códigos. Em seguida, definem-se algumas noções essenciais sobre códigos. Por fim, aborda-se a noção de distância mínima de um código e a sua importância na detecção e correcção de erros.

1.1 Introdução

Em sistemas de comunicação tais como linhas telefónicas, ligações por satélite, sistemas de armazenamento em CD ou DVD, é necessário codificar as mensagens que são enviadas/armazenadas através de canais que podem introduzir distorções, usualmente designadas por ruído. Assim, a informação recebida pode ser diferente da informação enviada. Tal pode acontecer na transmissão de um texto, uma música ou uma imagem, pois falhas humanas ou mesmo imperfeições no equipamento podem introduzir erros na referida mensagem.

No artigo *A Mathematical Theory of Communication* [9], publicado em 1948, o matemático Claude Shannon garantiu ser possível codificar informação de forma a transmiti-la com probabilidade de erro tão pequena quanto se queira. Segundo Raymond Hill [3], este artigo deu origem a duas novas áreas: a Teoria da Informação, que

é uma extensão directa do trabalho de Shannon assente sobretudo em ideias da teoria das probabilidades e a Teoria de Códigos que, apesar de algumas ligações à Teoria da Informação, se desenvolveu de forma independente, apoiada, essencialmente, em ideias da matemática pura.

F.M. Reza [7] refere que, em 1950, o matemático R. W. Hamming deu, também, um importante contributo ao desenvolver o primeiro procedimento de codificação para detecção e correcção de erros, acrescentando um ou mais dados adicionais a cada informação que se pretende transmitir ou armazenar.

A Teoria de Códigos é uma área recente da matemática, relacionada com a ciência de computadores e com aplicações significativas em outras ciências.

1.2 Noções Básicas

Seguem-se algumas noções básicas sobre códigos.

Definição 1.2.1 *1. Um* ***alfabeto*** F *é um conjunto finito com pelo menos dois elementos designados por símbolos ou letras.*

2. Uma ***palavra*** *de comprimento n do alfabeto F é um elemento $u \in F^n$, onde $F^n = F \times F \times ... \times F$ (n vezes).*
Uma palavra será representa por $u = (u_1, \ldots, u_n)$ ou por $u = u_1 \ldots u_n$.

3. Um ***código*** C *é um subconjunto, não vazio, de F^n.*

4. Uma ***palavra-código*** *é um elemento de um código.*

5. O ***comprimento de um código*** C *é n se $C \subseteq F^n$.*

6. O ***tamanho de um código*** C *é o número de palavras que o constituem e representa-se por $|C|$.*

Os códigos assim definidos designam-se por códigos de bloco.

Designam-se por códigos binários, os códigos que têm por alfabeto o conjunto $F_2 = \{0, 1\}$ e por códigos ternários, os que têm por por alfabeto o conjunto $F_3 = \{0, 1, 2\}$.

Exemplo 1.2.2 *O conjunto* $C \subseteq F_2^3$*, definido por* $C = \{000, 110, 101, 011\}$*, é um código binário de comprimento* 3 *e de tamanho* 4*. Os elementos* 000*,* 110*,* 101 *e* 011 *são as palavras-código de* C*.*

Suponha que utiliza este código C para codificar os seguintes atributos Mau, Suficiente, Bom, Excelente. Admita a seguinte codificação:

$$\begin{array}{rcl} \text{Mau} & \rightarrow & 000 \\ \text{Suficiente} & \rightarrow & 110 \\ \text{Bom} & \rightarrow & 101 \\ \text{Excelente} & \rightarrow & 011 \end{array}$$

Considere que a mensagem Bom, codificada por 101, foi transmitida através de um canal sujeito a interferências (ruído), que introduziu alterações, tendo o receptor recebido a palavra-código 000 a que corresponde a mensagem Mau. Supondo que a mensagem tem por objectivo informar a classificação num determinado exame, percebe-se a consequência dos erros introduzidos.

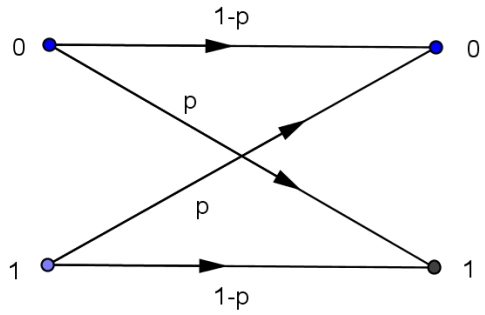
É importante que o sistema possa detectar os erros e corrigi-los ou detectar os erros e, não os conseguindo corrigir, optar por enviar um sinal pedindo a retransmissão da mensagem.

As situações que serão apresentadas acontecem em canais simétricos, ou seja, canais em que se verificam as seguintes condições:

1. todos os símbolos transmitidos têm igual probabilidade p, de serem recebidos errados

2. se um símbolo é recebido errado, a probabilidade de ser qualquer um dos outros é a mesma

Num canal binário simétrico com probabilidade de erro p,



a probabilidade de não ocorrer nenhum erro na transmissão de uma palavra de comprimento n é $(1-p)^n$, uma vez que cada símbolo tem probabilidade $1-p$ de ser recebido correctamente.

A probabilidade da palavra recebida conter erros em k posições específicas é

$$p^k(1-p)^{n-k}$$

Para $p < \frac{1}{2}$, a probabilidade da palavra recebida não ter nenhum erro é maior que qualquer um dos outros casos, isto é,

$$(1-p)^n > p(1-p)^{n-1} > p^2(1-p)^{n-2} > \ldots > p^n$$

Exemplo 1.2.3 *No caso do exemplo anterior, admita que a mensagem Bom, codificada por* 101*, foi transmitida através de um canal binário simétrico com* $p = 0,1$*. A probabilidade de receber a palavra-código* 000*, a que corresponde a mensagem Mau, é* $0,1^2 \times (1-0,1)^1 = 0,009$*, admitindo que ocorreram dois erros.*

A introdução, no processo de codificação de símbolos redundantes, sem qualquer informação, designados por símbolos de verificação, de teste ou de controlo, permite detectar e, eventualmente, corrigir erros que ocorram durante a transmissão. A forma mais simples de codificar informação, tendo em vista a sua recuperação na presença de ruído, é repetir cada símbolo da mensagem um determinado número de vezes.

Exemplo 1.2.4 *Código de tripla repetição*

Suponha que pretende transmitir a palavra 0 *ou* 1 *mas resolve codificá-la repetindo-a três vezes, ou seja,* $0 \to 000$ *e* $1 \to 111$. *Se o receptor receber a palavra* 101, *admitirá que houve erro na transmissão e pode escolher um dos caminhos:*

1. *comunicar o erro e pedir a retransmissão da palavra*
2. *corrigir o erro aproximando a palavra recebida da palavra-código que mais se assemelha, isto é, da palavra-código com o maior número de símbolos coincidentes com a palavra recebida, neste caso* 111

O segundo caminho fundamenta-se na ideia de ser mais provável ter um símbolo errado do que dois. Naturalmente, está a correr alguns riscos pois, existe a possibilidade da palavra enviada ter sido 000 *e terem ocorrido dois erros.*

1.3 Distância mínima de um código

Um parâmetro importante na análise e construção de códigos é o número de símbolos diferentes entre a palavra enviada e a palavra recebida. Para estudo deste parâmetro considera-se uma métrica.

Definição 1.3.1 *Seja* F *um alfabeto. Dadas duas palavras* u *e* v *de* F^n, *chama-se* ***distância de Hamming*** *entre* u *e* v *e representa-se por* $d(u, v)$ *a*

$$d(u, v) = |\{i \in \{1, \ldots, n\} : u_i \neq v_i\}|$$

A distância de Hamming entre duas palavras de F^n é igual ao número de componentes em que as duas palavras diferem.

Exemplo 1.3.2 *Sejam* 0010 *e* 1011 *duas palavras de* F^4. *Estas palavras diferem na primeira e última componentes e, portanto,* $d(0010, 1011) = 2$.

Definição 1.3.3 *Chama-se* ***espaço métrico*** *ao par* (E, d) *onde* E *é um conjunto e* d *é uma métrica.*

Proposição 1.3.4 *Seja* F *um alfabeto. A distância de Hamming,* $d(u, v)$*, é uma métrica pois, para quaisquer* $u, v, w \in F^n$

1. $d(u, v) \geq 0$ *com* $d(u, v) = 0$ *se e só se* $u = v$
2. $d(u, v) = d(v, u)$
3. $d(u, w) \leq d(u, v) + d(v, w)$

Demonstração: As propriedades 1. e 2. resultam da definição de distância de Hamming.

Para verificar a propriedade 3. veja-se o contributo da i-ésima componente dos elementos u, v e w. O contributo da i-ésima componente de u e de w para $d(u, w)$ é zero, se $u_i = w_i$, ou um, se $u_i \neq w_i$. Se for zero, então esse contributo para $d(u, w)$ é menor ou igual ao contributo para $d(u, v) + d(v, w)$ pois $d(u_i, v_i) + d(v_i, w_i)$ é zero, um ou dois. Se for um, então $u_i \neq w_i$ e, portanto, $u_i \neq v_i$ ou $v_i \neq w_i$, caso contrário ter-se-ia $u_i = v_i$ e $v_i = w_i$, donde $u_i = w_i$, que contradiz a hipótese. Então, $d(u_i, w_i) = 1 \leq d(u_i, v_i) + d(v_i, w_i)$. Logo, $d(u, w) \leq d(u, v) + d(v, w)$. □

Definição 1.3.5 *Seja* C *um código, com pelo menos dois elementos. Chama-se* ***distância mínima*** *de* C *e representa-se por* $d(C)$ *ao número*

$$d(C) = min\,\{d(u, v) : u, v \in C \text{ e } u \neq v\}$$

Exemplo 1.3.6 *Seja* C *o código definido por* $C = \{00000, 01011, 11110\}$*. Então,*

$$d(00000, 01011) = 3 \;\; ; \;\; d(00000, 11110) = 4 \;\; ; \;\; d(01011, 11110) = 3$$

Portanto, $d(C) = 3$*.*

Este processo para determinar $d(C)$ pode tonar-se difícil uma vez que obriga a calcular $\binom{|C|}{2}$ distâncias, sendo $|C|$ o tamanho do código.

Definição 1.3.7 *Seja (E, d) um espaço métrico. Dados um elemento $u \in E$ e um número real $r > 0$, chama-se* ***bola fechada de centro*** *u* ***e raio*** *r ao conjunto*

$$B(u; r) = \{v \in E : d(u, v) \leq r\}$$

Proposição 1.3.8 *Seja C um código com distância mínima $d(C)$. Se u e v são duas palavras distintas, do código C, então*

$$B(u; k) \cap B(v; k) = \emptyset \text{ , sendo, } k \leq \left\lfloor \frac{d(C) - 1}{2} \right\rfloor$$

em que $\lfloor s \rfloor$ representa o maior inteiro menor ou igual ao número real s.

Demonstração: Seja $w \in F^n$ tal que $w \in B(u; k) \cap B(v; k)$. Então $d(w, u) \leq k$, $d(w, v) \leq k$, logo

$$\begin{aligned} d(u, v) &\leq d(u, w) + d(w, v) \\ &= d(w, u) + d(v, w) \\ &\leq k + k \\ &= 2k \end{aligned}$$

De $k \leq \lfloor \frac{d(C)-1}{2} \rfloor$ vem $k \leq \frac{d(C)-1}{2}$, isto é, $2k \leq d(C) - 1$. Então, $d(u, v) \leq d(C) - 1$ que é absurdo por definição de $d(C)$. □

A distância mínima de um código é um parâmetro muito relevante no estudo dos Códigos Correctores de Erros pois mede a capacidade do código para detectar e corrigir erros que tenha ocorrido durante a transmissão.

Definição 1.3.9 *Seja C um código com distância mínima $d(C)$. Diz-se que C*

1. *detecta erros numa palavra recebida v, se para todo $u \in C$, $1 \leq d(u, v) < d(C)$*

2. *corrige erros numa palavra recebida v, substituíndo-a por u, se para algum $u \in C$, $d(u,v) \leq \lfloor \frac{d(C)-1}{2} \rfloor$*

3. *não consegue descodificar, com boa margem de segurança, a palavra recebida v, se para todo $u \in C$, $d(u,v) > \lfloor \frac{d(C)-1}{2} \rfloor$*

Com esta terminologia, diz-se que um código C com distância mínima $d(C)$ detecta até $d(C)-1$ erros e corrige até $\lfloor \frac{d(C)-1}{2} \rfloor$ erros.

Exemplo 1.3.10 *O código $C = \{0000, 1111\}$ tem $d(C) = 4$. Assim, este código detecta até $d(C)-1 = 4-1 = 3$ erros e corrige até $\lfloor \frac{d(C)-1}{2} \rfloor = \lfloor \frac{4-1}{2} \rfloor = 1$ erro. Se a palavra recebida for 0001, é detectado erro e é possivel corrigi-lo, substituíndo-a pela palavra código mais próxima, 0000. Recebida a palavra 0011, detecta-se erro mas não é possível corrigi-lo. Repare que $d(0011, 0000) = d(0011, 1111) = 2$.*

Num código será tanto maior a capacidade de detecção e correcção de erros quanto maior for a sua distância mínima e daí a importância deste conceito. Na construção de um código C existe sempre o seguinte problema: o comprimento n de um código deve ser pequeno, para permitir rápidas transmissões, mas ao mesmo tempo deve ser suficientemente grande para que $d(C)$ seja também grande.

Capítulo 2

Isometrias de Hamming

Neste capítulo, define-se isometria de Hamming e referem-se algumas das suas propriedades. Depois, demonstra-se o principal resultado do capítulo que estabelece que as isometrias relativas à métrica de Hamming são compostas de funções de duas famílias específicas de isometrias. Este resultado, da autoria de Ioana Constantinescu, origina uma primeira abordagem à equivalência de códigos.

2.1 Propriedades das isometrias de Hamming

Definição 2.1.1 *Seja (E, d) um espaço métrico. Diz-se que $\varphi : E \to E$ é uma* ***isometria*** *se preserva a distância, isto é, se para todo $x, y \in E$*

$$d(\varphi(x), \varphi(y)) = d(x, y)$$

onde d representa a distância em E.

Definição 2.1.2 *Uma isometria do espaço métrico (F^n, d), onde F é um alfabeto e d a distância de Hamming, diz-se* ***isometria de Hamming****.*

As proposições seguintes referem algumas propriedades verificadas pelas isometrias de Hamming.

Proposição 2.1.3 *Seja F um alfabeto e φ uma isometria de F^n. Então φ é uma bijecção de F^n.*

Demonstração: Seja $\varphi : F^n \to F^n$ uma isometria. Sejam $x, y \in F^n$ tais que $\varphi(x) = \varphi(y)$. Então, $d(\varphi(x), \varphi(y)) = d(x, y) = 0$ e portanto $x = y$, isto é, φ é injectiva. Como toda a aplicação injectiva de um conjunto finito nele próprio é sobrejectiva resulta que φ é uma bijecção de F^n. □

Definição 2.1.4 *Seja (E, d) um espaço métrico. Designa-se por $Iso(E)$ o* ***conjunto de todas as isometrias bijectivas*** *$\varphi : E \to E$.*

Proposição 2.1.5 *Seja (E, d) um espaço métrico e $\circ$ a operação de composição de funções. Então $(Iso(E), \circ)$ é um grupo.*

Demonstração: $Iso(E)$ é fechado para a operação de composição de funções pois, para todo $\varphi, \chi \in Iso(E)$ e $x, y \in E$

$$\begin{aligned} d((\varphi \circ \chi)(x), (\varphi \circ \chi)(y)) &= d(\varphi(\chi(x)), \varphi(\chi(y))) \\ &= d(\varphi(x), \varphi(y)) \\ &= d(x, y) \end{aligned}$$

isto é, $(\varphi \circ \chi) \in Iso(E)$.
Verifica-se a propriedade associativa pois a composta de funções é associativa.
$Iso(E)$ tem como elemento neutro a isometria id_E definida por

$$\begin{aligned} id_E : E &\to E \\ x &\mapsto x \end{aligned}$$

pois, para todo $x, y \in E$

$$d(id_E(x), id_E(y)) = d(x, y)$$

Todo o elemento $\varphi \in Iso(E)$ tem inverso $\varphi^{-1} \in Iso(E)$ pois, para todo $x, y \in E$

$$\begin{aligned} d(\varphi^{-1}(x), \varphi^{-1}(y)) &= d(\varphi(\varphi^{-1}(x)), \varphi(\varphi^{-1}(y))) \\ &= d(id_E(x), id_E(y)) \\ &= d(x, y) \end{aligned}$$

□

2.2 Teorema de Constantinescu

As duas proposições seguintes determinam duas famílias específicas de isometrias de Hamming.

Proposição 2.2.1 *Seja F um alfabeto, $\varphi : F \to F$ uma bijecção e i um número natural tal que $1 \leq i \leq n$. Então a aplicação*

$$\begin{array}{rccc} T_\varphi^i : & F^n & \to & F^n \\ & (a_1, \ldots, a_i, \ldots, a_n) & \mapsto & (a_1, \ldots, \varphi(a_i), \ldots, a_n) \end{array}$$

é uma isometria de F^n.

Demonstração: Sejam $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n)$ dois elementos de F^n. Então,

$$T_\varphi^i(u) = (u_1, \ldots, \varphi(u_i), \ldots, u_n) \text{ e } T_\varphi^i(v) = (v_1, \ldots, \varphi(v_i), \ldots, v_n)$$

T_φ^i preserva a distância de Hamming pois, para todo $u, v \in F^n$

$$\begin{aligned} d(T_\varphi^i(u), T_\varphi^i(v)) &= d((u_1, \ldots, \varphi(u_i), \ldots, u_n), (v_1, \ldots, \varphi(v_i), \ldots, v_n)) \\ &= d((u_1, \ldots, u_{i-1}, u_{i+1}, \ldots, u_n), (v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_n)) + d(\varphi(u_i), \varphi(v_i)) \end{aligned}$$

Como φ é uma bijecção, $u_i = v_i \Leftrightarrow \varphi(u_i) = \varphi(v_i)$. Logo, $d(\varphi(u_i), \varphi(v_i)) = d(u_i, v_i)$ e, portanto,

$$d(T_\varphi^i(u), T_\varphi^i(v)) = d(u, v)$$

Assim, T_{φ}^{i} é uma isometria de F^n. □

Esta família de isometrias permuta o conteúdo de uma componente de uma palavra.

Proposição 2.2.2 *Seja F um alfabeto e π uma permutação de $\{1,\ldots,n\}$. Então a aplicação*

$$\begin{array}{rccc} T_\pi: & F^n & \to & F^n \\ & (a_1,\ldots,a_n) & \mapsto & (a_{\pi(1)},\ldots,a_{\pi(n)}) \end{array}$$

é uma isometria de F^n.

Demonstração: Sejam $u=(u_1,\ldots,u_n)$ e $v=(v_1,\ldots,v_n)$ dois elementos de F^n. Então,

$$T_\pi(u)=(u_{\pi(1)},\ldots,u_{\pi(n)})=(u_1^{'},\ldots,u_n^{'}) \text{ e } T_\pi(v)=(v_{\pi(1)},\ldots,v_{\pi(n)})=(v_1^{'},\ldots,v_n^{'})$$

T_π preserva a distância de Hamming pois, considerando

$$P=\{j\in\{1,\ldots,n\}: u_j\neq v_j\} \text{ e } Q=\left\{k\in\{1,\ldots,n\}: u_k^{'}\neq v_k^{'}\right\}$$

resulta que, se $u_j\neq v_j$ então $u_{\pi(\pi^{-1}(j))}\neq v_{\pi(\pi^{-1}(j))}$ e, portanto, $u_{\pi^{-1}(j)}^{'}\neq v_{\pi^{-1}(j)}^{'}$, isto é, $u_k^{'}\neq v_k^{'}$, com $k=\pi^{-1}(j)$. Assim, se $j\in P$ então $k=\pi^{-1}(j)\in Q$, isto é, $\pi^{-1}(P)\subseteq Q$. Por um raciocínio análogo, verifica-se que $\pi(Q)\subseteq P$ e, portanto, $P=\pi(Q)$, ou seja, P e Q têm o mesmo número de elementos. Logo, T_π é uma isometria de F^n. □

Esta família de isometrias permuta as componentes de uma palavra.

Proposição 2.2.3 *Seja F um alfabeto e σ e $\sigma^{'}$ duas permutações de $\{1,\ldots,n\}$. Então, para todo $x=(x_1,\ldots,x_n)\in F^n$*

1. $(T_\sigma\circ T_{\sigma'})(x)=T_{\sigma\circ\sigma'}(x)$
2. $(T_\sigma)^{-1}(x)=T_{\sigma^{-1}}(x)$

Demonstração: Seja $x=(x_1,\ldots,x_n)$ um elemento de F^n. Então

1.

$$\begin{aligned}(T_\sigma \circ T_{\sigma'})(x) &= T_\sigma(T_{\sigma'}(x_1, \ldots, x_n)) \\ &= T_\sigma(x_{\sigma'(1)}, \ldots, x_{\sigma'(n)}) \\ &= (x_{\sigma(\sigma'(1))}, \ldots, x_{\sigma(\sigma'(n))}) \\ &= (x_{\sigma\circ\sigma'(1)}, \ldots, x_{\sigma\circ\sigma'(n)}) \\ &= T_{\sigma\circ\sigma'}(x).\end{aligned}$$

2.

$$\begin{aligned}(T_{\sigma^{-1}} \circ T_\sigma)(x) &= T_{\sigma\circ\sigma^{-1}}(x) \\ &= T_{id}(x) \\ &= id_{F^n}(x)\end{aligned}$$

Portanto, $(T_\sigma)^{-1}(x) = T_{\sigma^{-1}}(x)$.

□

A demonstração de cada uma das proposições seguintes e do teorema de Constantinescu foram adaptadas de A. Hefez e M.L.T. Villela [2].

Proposição 2.2.4 *Seja F um alfabeto com q elementos. Dada uma isometria φ de F^n, com $n \geq 2$, e dados $n-1$ elementos $a_1, \ldots, a_{n-1}$ de F, existem $n-1$ elementos $a_1', \ldots, a_{n-1}'$ de F, uma bijecção $\varphi_n : F \to F$ e uma permutação de π de $\{1, \ldots, n\}$ tais que, para todo $x \in F$*

$$(T_\pi \circ \varphi)(a_1, \ldots, a_{n-1}, x) = (a_1', \ldots, a_{n-1}', \varphi_n(x))$$

Demonstração: Considere $a_n \neq b_n \in F$ e sejam u e v dois elementos de F^n definidos por

$$u = (a_1, \ldots, a_{n-1}, a_n) \text{ e } v = (a_1, \ldots, a_{n-1}, b_n)$$

Como φ é uma isometria de F^n resulta que $d(\varphi(u), \varphi(v)) = d(u, v) = 1$. Suponha que $\varphi(u)$ e $\varphi(v)$ diferem na k-ésima componente com $1 \leq k \leq n$. Designe por (i, j) a

transposição de $\{1, \ldots, n\}$ que troca entre si, apenas, os elementos i e j, com $1 \leq i, j \leq n$. Tomando $\pi = (k, n)$, existem $a_1^{'}, \ldots, a_{n-1}^{'}, a_n^{'}$ e $b_n^{'}$ em F, com $a_n^{'} \neq b_n^{'}$, tais que

$$(T_\pi \circ \varphi)(u) = (a_1^{'}, \ldots, a_{n-1}^{'}, a_n^{'}) \quad \text{e} \quad (T_\pi \circ \varphi)(v) = (a_1^{'}, \ldots, a_{n-1}^{'}, b_n^{'})$$

Se $q = 2$, pode, então, definir-se uma bijecção φ_n, tal que $\varphi_n(a_n) = a_n^{'}$ e $\varphi_n(b_n) = b_n^{'}$. Se $q > 2$, seja $w = (a_1, \ldots, a_{n-1}, c_n)$, com $c_n \in F$ e $(T_\pi \circ \varphi)(w) = (w_1^{'}, \ldots, w_{n-1}^{'}, w_n^{'})$. Se $c_n \neq a_n$ e $c_n \neq b_n$ então $d(u, v) = d(v, u) = d(u, w) = 1$. A função $\overline{\varphi} = (T_\pi \circ \varphi)$ é uma isometria de F^n, pois é composta de duas isometrias de F^n, logo $\overline{\varphi}(u)$, $\overline{\varphi}(v)$ e $\overline{\varphi}(w)$ diferem entre si apenas numa componente. Observe que essa diferença ocorre na n-ésima posição. Assim, suponha que $\overline{\varphi}(u)$ e $\overline{\varphi}(w)$ diferem numa outra posição que não a n-ésima, ou seja, que existe um j, com $1 \leq j \leq n-1$, tal que $w_j^{'} \neq a_j^{'}$. Como $\overline{\varphi}(u)$ e $\overline{\varphi}(w)$ não podem ter mais do que uma componente diferente, vem $w_n^{'} = a_n^{'}$. Nesse caso, $w_n^{'} \neq b_n^{'}$, pois $a_n^{'} \neq b_n^{'}$. Então, $w_j^{'} \neq a_j^{'}$, para algum j, com $1 \leq j \leq n-1$, e $w_n^{'} \neq b_n^{'}$, isto é, $d(\overline{\varphi}(v), \overline{\varphi}(w)) \geq 2$ que é absurdo. Portanto, $w_j^{'} = a_j^{'}$, para $1 \leq j \leq n-1$. Assim, para qualquer $w = (a_1, \ldots, a_{n-1}, c_n)$ tem-se $\overline{\varphi}(w) = \left(a_1^{'}, \ldots, a_{n-1}^{'}, w_n^{'}\right)$. Seja $p_n : F^n \to F$ a projecção na n-ésima componente. Então, define-se, para qualquer $x \in F$

$$\varphi_n(x) = (p_n \circ T_\pi \circ \varphi)(a_1, \ldots, a_{n-1}, x)$$

Por definição de φ_n, tem-se

$$(T_\pi \circ \varphi)(a_1, \ldots, a_{n-1}, x) = (a_1^{'}, \ldots, a_{n-1}^{'}, \varphi_n(x))$$

Como $T_\pi \circ \varphi$ é uma isometria, φ_n é injectiva e sendo F finito resulta que φ_n é uma bijecção. □

Proposição 2.2.5 *Seja F um alfabeto. Dada uma isometria ϕ de F^n, suponha que existem $a_1, \ldots, a_{n-1}, a_1^{'}, \ldots, a_{n-1}^{'}$ elementos de F, e, para todo $x \in F$, uma bijecção $\varphi_n : F \to F$ tal que $\phi(a_1, \ldots, a_{n-1}, x) = (a_1^{'}, \ldots, a_{n-1}^{'}, \varphi_n(x))$. Então, para todo $(x_1, \ldots, x_n) \in F^n$, existe uma isometria γ de F^{n-1} tal que*

$$\phi(x_1, \ldots, x_{n-1}, x_n) = (\gamma(x_1, \ldots, x_{n-1}), \varphi_n(x_n))$$

Demonstração: Seja $(b_1, \ldots, b_{n-1})$ um elemento de F^{n-1} com

$$d((a_1, \ldots ..., a_{n-1}), (b_1, \ldots, b_{n-1})) = r.$$

Para qualquer $a_n \in F$, considere $u = (a_1, \ldots, a_{n-1}, a_n)$ e $v = (b_1, \ldots, b_{n-1}, a_n)$. Por hipótese, $\phi(u) = (a_1^{'}, \ldots, a_{n-1}^{'}, \varphi_n(a_n))$. Seja $\phi(v) = (b_1^{'}, \ldots, b_{n-1}^{'}, b_n^{'})$. Verifica-se que $b_n^{'} = \varphi_n(a_n)$. Assim, suponha que $b_n^{'} \neq \varphi_n(a_n)$. Seja $b_n = \varphi_n^{-1}(b_n^{'})$. Então, $b_n \neq a_n$. Considere, agora, $w = (a_1, \ldots, a_{n-1}, b_n)$. Por hipótese, $\phi(w) = (a_1^{'}, \ldots, a_{n-1}^{'}, b_n^{'})$. Ora, $d((a_1, \ldots, a_{n-1}), (b_1, \ldots, b_{n-1})) = d(u, v) = r$. Por outro lado, atendendo a que ϕ é uma isometria de F^n

$$\begin{aligned} d(\phi(v), \phi(w)) &= d((b_1^{'}, \ldots, b_{n-1}^{'}), (a_1^{'}, \ldots, a_{n-1}^{'})) \\ &= d(\phi(v), \phi(u)) - 1 \\ &= d(v, u) - 1 \\ &= r - 1 \end{aligned}$$

Sendo $a_n \neq b_n$

$$\begin{aligned} d(v, w) &= d((b_1, \ldots, b_{n-1}), (a_1, \ldots, a_{n-1})) + 1 \\ &= r + 1 \end{aligned}$$

Obtém-se, então, $d(v, w) = r + 1$ e $d(\phi(v), \phi(w)) = r - 1$ que é absurdo pois ϕ é, por hipótese, uma isometria de F^n. O absurdo resultou de se ter suposto que $b_n^{'} \neq \varphi_n(a_n)$. Logo, $b_n^{'} = \varphi_n(a_n)$ e, portanto, para qualquer $(x_1, \ldots, x_n) \in F^n$, existe um $(y_1, \ldots, y_{n-1}) \in F^{n-1}$ tal que $\phi(x_1, \ldots, x_n) = (y_1, \ldots, y_{n-1}, \varphi_n(x_n))$, ou seja, os elementos $y_1, \ldots, y_{n-1}$ são determinados pelos elementos $x_1, \ldots, x_n$.

Veja-se, agora, que γ existe, isto é, que os elementos $y_1, \ldots, y_{n-1}$ dependem apenas dos elementos $x_1, \ldots, x_{n-1}$. Assim, seja $z_n \in F$, com $z_n \neq x_n$, e suponha que

$$\phi(x_1, \ldots, x_{n-1}, z_n) = (y_1^{'}, \ldots, y_{n-1}^{'}, \varphi_n(z_n))$$

Como ϕ é uma isometria de F^n,

$$\begin{aligned} d((y_1, \ldots, y_{n-1}, \varphi_n(x_n)), (y_1^{'}, \ldots, y_{n-1}^{'}, \varphi_n(z_n))) &= d(\phi(x_1, \ldots, x_{n-1}, x_n), \phi(x_1, \ldots, x_{n-1}, z_n)) \\ &= d((x_1, \ldots, x_{n-1}, x_n), (x_1, \ldots, x_{n-1}, z_n)) \\ &= 1 \end{aligned}$$

De $x_n \neq z_n$ e, atendendo a que φ_n é uma bijecção, resulta que $\varphi_n(x_n) \neq \varphi_n(z_n)$. Logo, para todo $1 \leq i \leq n$, $y_i^{'} = y_i$. Concluí-se, então, que para todo $(x_1, \ldots, x_n) \in F^n$ existe $\gamma : F^{n-1} \to F^{n-1}$ tal que $\phi(x_1, \ldots, x_n) = (\gamma(x_1, \ldots, x_{n-1}), \varphi_n(x_n))$.

Resta provar que γ é uma isometria de F^{n-1}. Assim, sejam $(a_1, \ldots, a_{n-1})$ e $(b_1, \ldots, b_{n-1})$ dois elementos de F^{n-1} e seja $a_n \in F$. Então

$$\begin{aligned} d((a_1, \ldots, a_{n-1}), (b_1, \ldots, b_{n-1})) &= d((a_1, \ldots, a_{n-1}, a_n), (b_1, \ldots, b_{n-1}, a_n)) \\ &= d(\phi(a_1, \ldots, a_{n-1}, a_n), \phi(b_1, \ldots, b_{n-1}, a_n)) \\ &= d((\gamma(a_1, \ldots, a_{n-1}), \varphi_n(a_n)), (\gamma(b_1, \ldots, b_{n-1}), \varphi_n(a_n))) \\ &= d(\gamma(a_1, \ldots, a_{n-1}), \gamma(b_1, \ldots, b_{n-1})) \end{aligned}$$

e, portanto, γ é uma isometria de F^{n-1}. □

O teorema seguinte determina que as isometrias de Hamming são compostas das funções definidas nas proposições 2.2.1 e 2.2.2.

Teorema 2.2.6 (Constantinescu) *Seja F um alfabeto e $\varphi : F^n \to F^n$ uma isometria de F^n. Então, existe uma permutação π de $\{1, \ldots, n\}$ e, para $1 \leq i \leq n$, bijecções φ_i de F tais que*

$$\varphi = T_\pi \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n}$$

com π e φ_i unicamente determinados.

Demonstração: A demonstração vai ser feita por indução sobre n. Se $n = 1$, o resultado é trivial pois φ_1 é uma bijecção de F, isto é, $\varphi = T^1_{\varphi_1}$.

Suponha que $n > 1$ e que o resultado é válido para $n - 1$. Sejam $a_1, \ldots, a_{n-1}$ elementos de F. Da proposição 2.2.4, sabe-se que existem $a_1^{'}, \ldots, a_{n-1}^{'}$ elementos de F, uma bijecção $\varphi_n : F \to F$ e uma permutação σ de $\{1, \ldots, n\}$ tais que, para todo $x \in F$,

$$(T_\sigma \circ \varphi)(a_1, \ldots, a_{n-1}, x) = (a_1^{'}, \ldots, a_{n-1}^{'}, \varphi_n(x))$$

Da proposição 2.2.5, sabe-se que existe uma isometria γ de F^{n-1} tal que, para todo $(x_1, \ldots, x_n) \in F^n$,

$$(T_\sigma \circ \varphi)(x_1, \ldots, x_n) = (\gamma(x_1, \ldots, x_{n-1}), \varphi_n(x_n)) \tag{2.1}$$

Por hipótese de indução, existe uma permutação δ' de $\{1, \ldots, n-1\}$ e bijecções $\varphi_1, \ldots, \varphi_{n-1}$ de F tais que

$$\gamma = (T_{\delta'})' \circ (T^1_{\varphi_1})' \circ \ldots \circ (T^{n-1}_{\varphi_{n-1}})' \tag{2.2}$$

onde

$$\begin{array}{rccc} (T_{\delta'})' : & F^{n-1} & \to & F^{n-1} \\ & (x_1, \ldots, x_{n-1}) & \mapsto & (x_{\delta'(1)}, \ldots, x_{\delta'(n-1)}) \end{array}$$

e

$$\begin{array}{rccc} (T^i_{\varphi_i})' : & F^{n-1} & \to & F^{n-1} \\ & (x_1, \ldots, x_i, \ldots, x_{n-1}) & \mapsto & (x_1, \ldots, \varphi_i(x_i), \ldots, x_{n-1}) \end{array}$$

Definindo a permutação δ de $\{1, \ldots, n\}$ por

$$\delta(i) = \begin{cases} \delta'(i) & \text{se } 1 \leq i \leq n-1 \\ n & \text{se } i = n \end{cases}$$

e considerando

$$\begin{array}{rccc} T_\delta : & F^n & \to & F^n \\ & (x_1, \ldots, x_n) & \mapsto & (x_{\delta(1)}, \ldots, x_{\delta(n)}) \end{array}$$

e

$$\begin{array}{rccc} T^i_{\varphi_i} : & F^n & \to & F^n \\ & (x_1, \ldots, x_i, \ldots, x_n) & \mapsto & (x_1, \ldots, \varphi_i(x_i), \ldots, x_n) \end{array}$$

obtém-se de (2.1) e (2.2)

$$T_\sigma \circ \varphi = T_\delta \circ T^1_{\varphi_1} \circ \ldots \circ T^{n-1}_{\varphi_{n-1}} \circ T^n_{\varphi_n}$$

Da proposição 2.2.3 resulta que, para todo $(x_1, \ldots, x_n) \in F^n$,

$$\begin{aligned} \varphi(x_1, \ldots, x_n) &= (T^{-1}_\sigma \circ T_\delta \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n})(x_1, \ldots, x_n) \\ &= (T_{\sigma^{-1}} \circ T_\delta \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n})(x_1, \ldots, x_i, \ldots, x_n) \\ &= (T_{\sigma^{-1} \circ \delta} \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n})(x_1, \ldots, x_n) \end{aligned}$$

Fazendo $\pi = \sigma^{-1} \circ \delta$ obtém-se

$$\varphi(x_1, \ldots, x_n) = (T_\pi \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n})(x_1, \ldots, x_n)$$

Resta provar que π e φ_i são unicamente determinados, isto é, se existe uma permutação σ e, para $1 \leq i \leq n$, bijecções ψ_i, tais que $\varphi = T_\sigma \circ T^1_{\psi_1} \circ \ldots \circ T^n_{\psi_n}$, então, $\pi = \sigma$ e, para todo $1 \leq i \leq n$, $\varphi_i = \psi_i$.

Note que, para quaisquer duas bijecções β e τ de F e $1 \leq i \neq j \leq n$, as componentes de $\left(T^i_\beta \circ T^j_\tau\right)(x)$ são

$$\left((T^i_\beta \circ T^j_\tau)(x)\right)_k = \begin{cases} \beta(x_i) & \text{se } k = i \\ \tau(x_j) & \text{se } k = j \\ x_k & \text{se } k \neq i, j \end{cases}$$

e as componentes de $\left(T^j_\tau \circ T^i_\beta\right)(x)$ são

$$\left((T^j_\tau \circ T^i_\beta)(x)\right)_k = \begin{cases} \beta(x_i) & \text{se } k = i \\ \tau(x_j) & \text{se } k = j \\ x_k & \text{se } k \neq i, j \end{cases}$$

Logo

$$T^i_\beta \circ T^j_\tau = T^j_\tau \circ T^i_\beta \tag{2.3}$$

Suponha, então, que

$$T_\pi \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n} = T_\sigma \circ T^1_{\psi_1} \circ \ldots \circ T^n_{\psi_n} \tag{2.4}$$

Multiplicando, à esquerda, ambos o membros da equação (2.4) por $T_{\sigma^{-1}}$ e utilizando a proposição 2.2.3 resulta

$$T_{(\sigma^{-1} \circ \pi)} \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n} = T^1_{\psi_1} \circ \ldots \circ T^n_{\psi_n} \tag{2.5}$$

Multiplicando, à direita, ambos os membros de (2.5) por $T^1_{\psi_1^{-1}} \circ \ldots \circ T^n_{\psi_n^{-1}}$ e utilizando (2.3) obtém-se

$$T_{(\sigma^{-1} \circ \pi)} \circ T^1_{(\varphi_1 \circ \psi_1^{-1})} \circ \ldots \circ T^n_{(\varphi_n \circ \psi_n^{-1})} = id_{F^n} \tag{2.6}$$

Considerando $\rho = (\sigma^{-1} \circ \pi)$ e, para todo $1 \leq i \leq n$, $\alpha_i = (\varphi_i \circ \psi_i^{-1})$, a equação (2.6) toma a forma

$$T_\rho \circ T^1_{\alpha_1} \circ \ldots \circ T^n_{\alpha_n} = id_{F^n}$$

Assim, para todo $x = (x_1, \ldots, x_n) \in F^n$, tem-se

$$\begin{aligned} x &= \left(T_\rho \circ T^1_{\alpha_1} \circ \ldots \circ T^n_{\alpha_n}\right)(x) \\ &= T_\rho\left(\alpha_1(x_1), \ldots, \alpha_n(x_n)\right) \\ &= \left(\alpha_{\rho(1)}(x_{\rho(1)}), \ldots, \alpha_{\rho(n)}(x_{\rho(n)})\right) \end{aligned}$$

ou seja, para todo $1 \leq i \leq n$,

$$x_i = \alpha_{\rho(i)}(x_{\rho(i)}) \tag{2.7}$$

Suponha que existe algum $1 \leq j \neq i \leq n$, tal que $j = \rho(i)$. Como F tem pelo menos dois elementos diferentes, pode-se escolher um vector x tal que $x_{\rho(i)} = \alpha^{-1}_{\rho(i)}(j)$. Mas isto contradiz a equação (2.7). Assim, para todo $1 \leq i \leq n$, $\rho(i) = i$, isto é, $\rho(i) = id_F$ e, então, para todo $x_i \in F$ a equação (2.7) é equivalente a

$$x_i = \alpha_i(x_i)$$

Logo, $\alpha_i = id_F$. Como, para todo $1 \leq i \leq n$, $(\varphi_i \circ \psi_i^{-1}) = \alpha_i = id_F$, resulta $\varphi_i = \psi_i$ e de $(\sigma^{-1} \circ \pi) = \rho = id_{F^n}$ obtém-se $\sigma = \pi$. □

Proposição 2.2.7 *Seja F um alfabeto com q elementos. Em F^n, existem $(q!)^n \times n!$ isometrias diferentes.*

Demonstração: o teorema de Constantinescu estabelece que as isometrias de F^n são da forma

$$\varphi = T_\pi \circ T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n}$$

e garante que π e, para todo $1 \leq i \leq n$, φ_i, são unicamente determinadas. Então, para $1 \leq i \leq n$, cada bijecção $T^i_{\varphi_i}$ tem $q!$ possibilidades diferentes e, portanto, para $T^1_{\varphi_1} \circ \ldots \circ T^n_{\varphi_n}$ existem $(q!)^n$ diferentes possibilidades. π define uma permutação de

n elementos logo, para T_π, existem $n!$ possibilidades diferentes. Então, φ pode ser formada de $(q!)^n \times n!$ maneiras diferentes. □

No caso binário, isto é, para $q = 2$, existem $(2!)^n \times n!$ isometrias diferentes.

Denota-se por F_q um corpo com q elementos.

Exemplo 2.2.8 *Considere, para $i = 1, 2, 3$ e $u_i \in F_2$ as bijecções id_{F_2} e $\overline{id}_{F_2}$, com $\overline{id}_{F_2}$ definida por*

$$\overline{id}_{F_2}(u_i) = \begin{cases} 0 & se\ u_i = 1 \\ 1 & se\ u_i = 0 \end{cases}$$

As isometrias ψ_1, ψ_2 e ψ_3 definidas por

$$\psi_1(u_1, u_2, u_3) = (id_{F_2}(u_1), id_{F_2}(u_2), id_{F_2}(u_3))\,;$$

$$\psi_2(u_1, u_2, u_3) = (id_{F_2}(u_2), id_{F_2}(u_1), id_{F_2}(u_3))\,;$$

$$\psi_3(u_1, u_2, u_3) = \left(\overline{id}_{F_2}(u_3), \overline{id}_{F_2}(u_2), id_{F_2}(u_1)\right)$$

são exemplos de três das $(2!)^3 \times 3! = 48$ isometrias diferentes de F_2^3.

2.3 Equivalência de Códigos

Definição 2.3.1 *Sejam C e D dois códigos definidos em F^n. Os **códigos** C e D dizem-se **equivalentes** se existir uma isometria φ de F^n tal que $\varphi(C) = D$.*

Exemplo 2.3.2 *Os códigos $C, D \subseteq F_2^3$ definidos por*

$$C = \{000, 100, 011, 111\} \quad e \quad D = \{101, 100, 011, 010\}$$

são equivalentes.

A isometria $\varphi : F_2^3 \to F_2^3$ tal que $\varphi = T_\pi \circ T^1_{\varphi_1} \circ T^2_{\varphi_2} \circ T^3_{\varphi_3}$, com $\varphi_1 = \varphi_2 = \overline{id}_{F_2}$, $\varphi_3 = id_{F_2}$ e

$$\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

verifica

$$\varphi(000) = T_\pi(110) = 101$$

$$\varphi(100) = T_\pi(010) = 100$$

$$\varphi(011) = T_\pi(101) = 011$$

$$\varphi(111) = T_\pi(001) = 010$$

isto é, $\varphi(C) = D$.

Capítulo 3

Códigos Lineares

Neste capítulo, define-se uma classe importante de códigos, designados por códigos lineares, e estuda-se as suas principais características, sendo que algumas delas são consequência directa dos resultados da álgebra linear. Como referem Ling e Xing [5], estes códigos são espaços vectoriais e, portanto, as suas estruturas algébricas tornam-os mais fáceis de descrever e de aplicar que os códigos não lineares. Por fim, analisa-se, com algum detalhe, uma caraterística relevante de um código linear, o seu peso mínimo, e de que forma está relacionado com a sua distância mínima.

3.1 Código linear. Matriz geradora.

Seja F um corpo finito. Dados dois vectores $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in F^n$ e um escalar $\lambda \in F$, considere as operações adição de vectores e multiplicação de um vector por um escalar definidas por

$$u + v = (u_1 + v_1, \ldots, u_n + v_n) \text{ e } \lambda u = (\lambda u_1, \ldots, \lambda u_n)$$

Definição 3.1.1 *Diz-se que C é um **código linear** de comprimento n sobre um corpo F se C for um subespaço vectorial do espaço vectorial F^n.*

Assim, nos códigos lineares, é garantido que a soma de duas palavras-código e o produto de um escalar por uma palavra-código é, ainda, uma palavra-código. Pode-se, então, afirmar que para quaisquer $a, b \in C$ e $\lambda, \mu \in F$, $\lambda a + \mu b \in C$.

Todos os códigos lineares contêm a palavra-código zero, $\overline{0} = 00 \cdots 0$.

Definição 3.1.2 *A **dimensão de um código linear** C é a dimensão de C enquanto espaço vectorial sobre um corpo F.*

Definição 3.1.3 *Designa-se por $(n, k)-$código linear C, um código linear C de comprimento n e dimensão k.*

Um (n, k)-código linear, construído a partir de um alfabeto com q elementos, tem q^k palavras-código.

Um espaço vectorial é gerado pelos vectores da base. Assim, dado um $(n, k)-$código linear C sobre um corpo F, seja $\{v_1, v_2, \ldots, v_k\}$ uma das suas bases. Então, qualquer elemento $u \in C$ pode ser escrito de forma única $u = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k$, com $\lambda_1, \lambda_2, \ldots, \lambda_k \in F$, isto é, qualquer palavra-código é combinação linear das palavras-código da base. É usual apresentar os vectores da base como linhas de uma matriz.

Definição 3.1.4 *Seja C um $(n, k)-$código linear sobre o corpo F.*
*Chama-se **matriz geradora** de C a qualquer matriz $k \times n$ cujas linhas formam uma base de C.*

Assim, se $\{v_1, \ldots, v_k\}$ é uma base de C, uma matriz geradora G de C é a matriz cujas linhas são, para $i = 1, \ldots, k$, os vectores $v_i = (v_{i1}, \ldots, v_{in})$, isto é,

$$G = \begin{pmatrix} v_{11} & v_{12} & \ldots & v_{1n} \\ v_{21} & v_{22} & \ldots & v_{2n} \\ \vdots & \vdots & & \vdots \\ v_{k1} & v_{k2} & \ldots & v_{kn} \end{pmatrix}$$

O processo seguinte descreve como se pode obter as palavras-código a partir da matriz geradora. Sendo C um $(n,k)-$código linear sobre um corpo F com matriz geradora G, as palavras-código são combinações lineares das linhas de G, isto é, $C = \left\{uG : u \in F^k\right\}$. Então uma regra simples de codificação que transforma palavras em palavras-código é $u \to uG$ em que u é a palavra de comprimento k escrita como vector linha. Uma característica importante da álgebra linear é permitir representar por matrizes as transformações lineares. Se considerar matrizes cujas linhas formam uma base, isto é, cujos vectores são linearmente independentes, pode definir-se um código como imagem da transformação linear

$$\begin{array}{rccc} T: & F^k & \to & F^n \\ & u & \mapsto & uG \end{array}$$

Para a palavra $u = (u_1, \ldots, u_k)$ resulta a codificação

$$T(u) = uG = u_1 v_1 + \ldots + u_k v_k$$

Exemplo 3.1.5 *O $(4,2)-$código linear binário $C = \{0000, 1100, 0011, 1111\}$ admite como base $\{1100, 0011\}$.*

Assim

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

é uma matriz geradora de C.

As restantes palavras do código são combinações lineares das palavras da base, isto é,

$$C = \left\{uG : u \in F_2^2\right\}$$

Na verdade,

$$(00)\,G = (0000)\ ;\ (10)\,G = (1100)\ ;\ (01)\,G = (0011)\ \ e\ \ (11)\,G = (1111)$$

Pode entender-se C como imagem da transformação linear

$$\begin{array}{rccc} T: & F_2^2 & \to & F_2^4 \\ & (u_1, u_2) & \mapsto & (u_1, u_1, u_2, u_2) \end{array}$$

Cada palavra $u = (u_1, u_2) \in F_2^2$ é associada à palavra-código $uG = (u_1, u_1, u_2, u_2)$.

Os códigos lineares são, assim, fáceis de codificar.

A transformação linear $u \rightarrow uG$ pode ser simplificada efectuando operações elementares sobre as linhas da matriz G. Assim, realizando troca entre duas linhas, multiplicação de uma linha por um escalar não nulo, adição de um múltiplo de uma linha a outra linha, pode obter-se uma matriz equivalente à inicial. Como um espaço vectorial sobre um corpo pode ter várias bases diferentes, pode ter-se matrizes geradoras diferentes para o mesmo código. No entanto, todas as bases têm o mesmo número de elementos e, portanto, todas as matrizes geradoras têm a mesma dimensão. Faz sentido escolher matrizes geradoras tão simples quanto possível.

Definição 3.1.6 *Seja C um $(n,k)-$código linear com matriz geradora G. Diz-se que a* ***matriz geradora*** *está* ***na forma canónica*** *se $G = (I_k|A)$ onde I_k é a matriz identidade $k \times k$ e A uma qualquer matriz $k \times (n-k)$.*

Uma das vantagens da matriz na forma canónica é que codificando a palavra $u = (u_1, \ldots, u_k)$ obtém-se uma palavra-código cujas primeiras k componentes coincidem com as de u e as últimas $n-k$ são as componentes de controlo. Caso não se consiga obter uma matriz geradora na forma canónica para um código linear C através de operações elementares sobre linhas, pode efectuar-se permutações das colunas da mesma, obtendo assim uma matriz geradora na forma canónica de um código $\overline{C}$ não necessariamente igual a C mas obrigatoriamente equivalente a C.

Exemplo 3.1.7 *No caso do código do exemplo anterior (exemplo 3.1.5) a matriz geradora*

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

não está na forma canónica.

Recorrendo a uma permutação das colunas dois e três obtém-se a matriz

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

que é a matriz geradora na forma canónica do código $\overline{C} = \{0000, 1010, 0101, 1111\}$. *Os códigos* C *e* $\overline{C}$ *não são iguais mas são equivalentes pois, para* $u \in C$ *a transformação*

$$\varphi(u) = T_\pi(u)$$

com

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

verifica $\varphi(C) = \overline{C}$.

3.2 Matriz de controlo. Código dual.

Existe uma outra matriz, importante, associada a um código linear.

Definição 3.2.1 *Dado um* $(n,k)-$*código linear* C *sobre um corpo* F *e uma palavra* $v \in F^n$, *chama-se* ***matriz de controlo*** *de* C *a uma matriz* H *tal que*

$$vH^T = \overline{0} \;\; \textit{se e só se} \;\; v \in C$$

Uma das principais razões para o uso de códigos lineares tem a ver com a facilidade de verificar, através da matriz de controlo, se uma palavra recebida é ou não uma palavra-código. Assim, em vez de resolver o sistema $uG = v$, com $u \in F^k$, que pode ter um custo elevado, pode obter-se a resposta determinando a matriz de controlo e calculando vH^T. Se o resultado for o vector nulo, $v \in C$. Se o resultado for diferente do vector nulo, $v \notin C$. A matriz de controlo H para um $(n,k)-$código linear C sobre um corpo F, com matriz geradora na forma canónica $G = (I_k|A)$, é dada por $H = (-A^T|I_{n-k})$ tendo H dimensão $(n-k) \times n$. Facilmente se verifica que $GH^T = (I_k|A) \binom{-A}{I_{n-k}} = -A + A = (\mathbf{0})$.

Exemplo 3.2.2 *Seja C um código sobre F_2 com matriz geradora*

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

$G = (I_3|A)$ com

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad e \quad A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$$

A matriz de controlo H é igual a

$$H = \left[-A^T|I_2\right] = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

A palavra $u = (10101) \in C$ visto que

$$uH^T = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \end{pmatrix} = \overline{0}$$

A palavra $v = (11011) \notin C$ já que

$$vH^T = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \end{pmatrix} \neq \overline{0}$$

O próximo conceito desempenha, um papel fundamental na teoria dos códigos lineares.

Definição 3.2.3 *Seja C um $(n,k)-$código linear sobre um corpo F. Chama-se* ***código dual*** *de C e representa-se por $C^\perp$ ao conjunto*

$$C^\perp = \{v \in F^n : v.u = 0 \ \text{para todo} \ u \in C\}$$

Proposição 3.2.4 *Seja C um $(n,k)-$código linear sobre um corpo F, com matriz geradora G. Então*

1. *$C^{\perp}$ é um subespaço vectorial de F^n*
2. *$v \in C^{\perp}$ se e só se $vG^T = \overline{0}$*
3. *$dim(C^{\perp}) = n - k$*

Demonstração: Sejam $u, v \in C^{\perp}$ e $\lambda, \mu \in F$.

1. Para qualquer $w \in C$, vem que

$$(\lambda u + \mu v).w = \lambda(u.w) + \mu(v.w) = \lambda.0 + \mu.0 = 0$$

   e, portanto, $(\lambda u + \mu v) \in C^{\perp}$. Logo, $C^{\perp}$ é um subespaço vectorial de F^n.

2. Qualquer elemento $v \in C^{\perp}$ é ortogonal a todos os elementos de C, isto é, é ortogonal a todos os elementos de qualquer base de C. Assim, sendo $\{u_1, \ldots, u_k\}$ uma base de C, vem, para todo $1 \leq i \leq k$, $v.u_i = 0$, ou seja, $vG^T = \overline{0}$ já que as linhas de G são os vectores da base de C. Por outro lado, se $vG^T = \overline{0}$ então, para todo $1 \leq i \leq k$, $v.u_i = 0$, isto é, v é ortogonal a todos os vectores linha de G. Como estes vectores linha formam uma base de C, resulta que v é ortogonal a todos os elementos de C, ou seja $v \in C^{\perp}$.

3. Se $C = \{\overline{0}\}$ então $k = 0$ e $C^{\perp} = F^n$. Logo, $dim(C^{\perp}) = n - k$.
   Se $C \neq \{\overline{0}\}$, seja

$$\begin{array}{rccc} f: & F^n & \rightarrow & F^k \\ & u & \mapsto & uG^T \end{array}$$

   $Kerf = C^{\perp}$ e como $dim(Imf) = CarG = dimC = k$, do teorema A.4.3, resulta que $dim(C^{\perp}) = n - k$.

□

A relação entre um código e o seu dual vai mais além e, assim, se G for a matriz geradora na forma canónica de um código linear C de dimensão k, então H é a matriz geradora do código dual $C^{\perp}$ de dimensão $n-k$.

Exemplo 3.2.5 *O código C do exemplo 3.2.2 tem matriz de controlo*

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

e, portanto, $\{10110, 00101\}$ *é uma base para o código dual $C^{\perp}$. O código dual é então*

$$C^{\perp} = \{10110, 00101, 00000, 10011\}$$

e tem dimensão dois. O código C associado tem por base $\{10010, 01000, 00111\}$*. Então*

$$C = \{00000, 10010, 01000, 00111, 11010, 10101, 01111, 11101\}$$

É fácil confirmar que qualquer elemento de $C^{\perp}$ é ortogonal a todos os elementos de C.

3.3 Peso de Hamming

Segue-se uma outra noção importante, a de peso mínimo de um código linear, e a sua relação com a distância mínima de um código linear.

Definição 3.3.1 *Seja u uma palavra de F^n. Chama-se* ***peso de Hamming*** *de u e representa-se por $wt(u)$ ao número de componentes não nulas em u, isto é,*

$$wt(u) = |\{i \in \{1, \ldots, n\} : u_i \neq 0\}|$$

Em particular, se $n = 1$ e $k \in F$

$$wt(k) = \begin{cases} 0 & \text{se } k = 0 \\ 1 & \text{se } k \neq 0 \end{cases} \tag{3.1}$$

Sendo d a distância de Hamming e $\overline{0} = 00\ldots0$, vem $wt(u) = d(u, \overline{0})$.

A proposição seguinte estabelece uma relação entre distância de Hamming e peso de Hamming.

Proposição 3.3.2 *Sejam u e v duas palavras de F^n. Então*

$$d(u, v) = wt(u - v)$$

Demonstração: Sejam $u, v \in F^n$. Então

$$\begin{aligned} d(u,v) &= |\{i \in \{1,\ldots,n\} : u_i \neq v_i\}| \\ &= |\{i \in \{1,\ldots,n\} : u_i - v_i \neq 0\}| \\ &= wt(u - v) \end{aligned}$$

□

Exemplo 3.3.3 *Considere as palavras $u = 110$ e $v = 001$ de F_2^3. Então, $d(u, v) = 3$ e como $u - v = 111$ resulta que $wt(u - v) = 3$, ou seja, $d(u, v) = wt(u - v)$.*

Definição 3.3.4 *Seja C um $(n, k)-$código linear, não nulo, sobre um corpo F. Chama-se **peso mínimo** de C e representa-se por $wt(C)$ ao menor dos pesos de todas as palavras-código não nulas.*

Proposição 3.3.5 *Seja C um código linear sobre um corpo F. Então*

$$d(C) = wt(C)$$

Demonstração: Para quaisquer duas palavras $u, v \in C$, $d(u, v) = wt(u - v)$. Por definição de distância mínima de um código, existem $u', v' \in C$ tais que $d(C) = d(u', v')$, logo

$$d(C) = d(u', v') = wt(u' - v') \geq wt(C) \tag{3.2}$$

Por outro lado, por definição de peso mínimo de um código, existe um $w \in C \setminus \{\overline{0}\}$ tal que $wt(C) = wt(w)$ e portanto

$$wt(C) = wt(w) = d(w, \overline{0}) \geq d(C) \tag{3.3}$$

De (3.2) e (3.3) resulta $d(C) = wt(C)$. □

Assim, para códigos lineares pode obter-se a distância mínima de um código analisando no máximo $|C| - 1$ palavras em vez das eventuais $\binom{|C|}{2}$ referidas no Capítulo 1.

Exemplo 3.3.6 *Determinando o peso das três palavras não nulas do código linear* $C = \{0000, 1010, 0101, 1111\}$*, concluí-se que* $wt(C) = 2$ *e portanto* $d(C) = 2$*.*

A proposição seguinte estabelece uma relação entre a distância mínima de um código e a independência linear das colunas da matriz de controlo.

Proposição 3.3.7 *Seja* C *um* $(n, k)-$*código linear sobre um corpo* F *e* H *a matriz de controlo. Então, o código* C *tem distância mínima* d *se e só se, em* H*, existem* d *colunas linearmente dependentes mas quaisquer* $d - 1$ *colunas são linearmente independentes.*

Demonstração: Pela proposição 3.3.5, $d = wt(C)$. Seja $u = (u_1, \ldots, u_n)$ uma palavra-código. Ora,

$$u \in C \Leftrightarrow uH^T = \overline{0} \Leftrightarrow u_1H_1 + u_2H_2 + \ldots + u_nH_n = \overline{0}$$

onde $H_1, H_2, \ldots, H_n$ representam as colunas da matriz de controlo H. Assim, a cada palavra-código u de peso d corresponde um conjunto de d colunas linearmente dependentes. Portanto, H tem d colunas linearmente dependentes.

Por outro lado, suponha que H tem $d - 1$ colunas linearmente dependentes,

$$H_{i_1}, H_{i_2}, \ldots, H_{i_{d-1}}$$

Então, existem escalares $u_{i_1}, u_{i_2}, \ldots, u_{i_{d-1}}$, não todos nulos, tais que

$$u_{i_1}H_{i_1} + u_{i_2}H_{i_2} + \ldots + u_{i_{d-1}}H_{i_{d-1}} = \overline{0}$$

isto é, o vector $u = (0, \ldots, 0, u_{i_1}, 0, \ldots, 0, u_{i_2}, 0 \ldots, 0, u_{i_{d-1}}, 0, \ldots, 0)$ com u_{i_j} na i_j-ésima posição para $j = 1, 2, \ldots, d-1$ e zero nas restantes, satisfaz $uH^T = \overline{0}$. Logo, $u \in C$ e $wt(u) < d$ que é absurdo. Portanto, quaisquer $d-1$ colunas de H são linearmente independentes. □

O exemplo seguinte recorre a um código linear, chamado código de Hamming. Os códigos desta família são, segundo S. Roman [8], talvez os mais famosos códigos correctores de erros, tendo sido descobertos de forma independente, em 1949, por M.Golay e, em 1950, por R. Hamming.

Exemplo 3.3.8 *H é uma matriz de controlo para o $(4,2)-$código de Hamming sobre o corpo F_3*

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

Este código é formado por $3^2 = 9$ palavras.
Representando por H_1, H_2, H_3, H_4 cada uma das quatro colunas de H pode afirmar-se que $H_3 = H_1 + H_2$, isto é, existem três colunas linearmente dependentes. Verifica-se que, quaisquer duas colunas de H são linearmente independentes. Aplicando a proposição anterior, conclui-se que este código tem distância mínima igual a 3.

A proposição 3.3.7 permite determinar a distância mínima de um código linear a partir da matriz de controlo. Mais ainda, permite construir uma matriz de controlo e, por consequência, um código linear que verifique uma determinada distância mínima previamente fixada.

Capítulo 4

Enumerador de pesos

Neste capítulo, define-se distribuição de pesos de um código linear, característica que, apesar de não determinar a unicidade de um código, fornece informação relevante sobre o mesmo. Seguem-se algumas proposições necessárias à demonstração do teorema fundamental do capítulo. Este resultado, conhecido por Identidade de MacWilliams, foi segundo W.C. Huffman [4], obtido por Florence Jessie MacWilliams e estabelece uma relação entre o enumerador de pesos de um código linear C e do seu dual $C^{\perp}$. Ao longo dos anos tem-se revelado como uma das principais ferramentas no estudo dos códigos lineares, em particular, do peso das suas palavras. O teorema é primeiro demonstrado para códigos binários, pois são muito utilizados, designadamente no mundo digital, e depois é demonstrado para códigos lineares mais gerais sobre um corpo F_p, com p primo. Esta opção deve-se também às particularidades de cada uma das demonstrações.

4.1 Enumerador de pesos de um código linear

Definição 4.1.1 *Seja C um $(n,k)-$código linear sobre um corpo F e A_i o número de palavras de C com peso i. Chama-se* ***distribuição de pesos*** *de C aos números $A_0, A_1, \ldots, A_n$.*

É claro que $A_i \geq 0$ para todo $0 \leq i \leq n$, $A_0 = 1$ pois $wt(u) = 0$ se e só se $u = \overline{0}$ e

$$A_0 + A_1 + \ldots + A_n = |C|$$

Definição 4.1.2 *Seja C um $(n,k)-$código linear sobre um corpo F e, para $1 \leq i \leq n$, A_i o número de palavras de C com peso i. Chama-se* ***enumerador de pesos do código*** *C ao polinómio W_C, nas variáveis x e y, definido por*

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{u \in C} x^{n-wt(u)} y^{wt(u)} \tag{4.1}$$

Exemplo 4.1.3 *Seja $C \subseteq F_2^3$ o código linear definido por $C = \{000, 011, 101, 110\}$. Assim,*

$$A_0 = 1\ ,\ A_1 = 0\ ,\ A_2 = 3\ ,\ A_3 = 0$$

e, por conseguinte,

$$W_C(x,y) = x^3 + 3xy^2$$

Facilmente se verifica que $C^\perp = \{000, 111\}$. Então, para $C^\perp$,

$$A_0 = 1\ ,\ A_1 = 0\ ,\ A_2 = 0\ ,\ A_3 = 1$$

e, portanto,

$$W_{C^\perp}(x,y) = x^3 + y^3$$

4.2 Identidade de MacWilliams para códigos lineares binários

Proposição 4.2.1 *Seja C um $(n,k)-$código linear binário e $v \in F_2^n \setminus C^\perp$. Sejam $P = \{u \in C : u.v = 0\}$ e $Q = \{u \in C : u.v = 1\}$. Então $|P| = |Q|$.*

Demonstração: Seja v uma palavra de $F_2^n \setminus C^\perp$. Como $v \notin C^\perp$ existe em C uma palavra-código w tal que $w.v = 1$. Considere

$$w + P = \{w + u : u \in P\} \quad \text{e} \quad w + Q = \{w + u : u \in Q\}$$

Então, $w + P \subseteq Q$ pois para todo $u \in P$

$$(w + u).v = w.v + u.v = 1 + 0 = 1$$

isto é, $w + u \in Q$.

Analogamente, $w + Q \subseteq P$ visto que para todo $u \in Q$

$$(w + u).v = w.v + u.v = 1 + 1 = 0$$

ou seja, $w + u \in P$.

Então, $|P| = |w + P| \leq |Q|$ e $|Q| = |w + Q| \leq |P|$ donde $|P| = |Q|$. □

Definição 4.2.2 *Seja V um espaço vectorial e $f : F_2^n \to V$.*
Chama-se ***transformada de Hadamard de f*** *e representa-se por $\hat{f}$ à função definida, para qualquer $u \in F_2^n$, por*

$$\hat{f}(u) = \sum_{v \in F_2^n} (-1)^{u.v} f(v)$$

Proposição 4.2.3 *Seja C um $(n, k)-$código linear binário. Então*

$$\sum_{u \in C} \hat{f}(u) = |C| \sum_{v \in C^\perp} f(v)$$

sendo $\hat{f}$ a transformada de Hadamard de f.

Demonstração:

$$\begin{aligned}
\sum_{u \in C} \hat{f}(u) &= \sum_{u \in C} \sum_{v \in F_2^n} (-1)^{u.v} f(v) \\
&= \sum_{v \in F_2^n} f(v) \sum_{u \in C} (-1)^{u.v} \\
&= \sum_{v \in C^\perp} f(v) \sum_{u \in C} (-1)^{u.v} + \sum_{v \notin C^\perp} f(v) \sum_{u \in C} (-1)^{u.v}
\end{aligned}$$

Se $v \in C^\perp$, $u.v = 0$ para todo $u \in C$ e, portanto,

$$\sum_{u \in C} (-1)^{u.v} = |C|$$

Se $v \notin C^{\perp}$, pela proposição 4.2.1,

$$\sum_{u \in C}(-1)^{u.v} = \sum_{\substack{u \in C \\ u.v=0}} 1 + \sum_{\substack{u \in C \\ u.v=1}} (-1) = \frac{|C|}{2} \times 1 + \frac{|C|}{2} \times (-1) = 0$$

Então

$$\sum_{u \in C} \hat{f}(u) = |C| \sum_{v \in C^{\perp}} f(v)$$

□

Proposição 4.2.4 *Sejam A um anel comutativo e $\{a_{i,j} \in A : i \in \mathbb{N} \ \ e \ \ j \in \{0, \ldots, q-1\}\}$ um subconjunto de A. Para todo $n \in \mathbb{N}$ tem-se que*

$$\prod_{i=1}^{n} \sum_{j=0}^{q-1} a_{i,j} = \sum_{v_1=0}^{q-1} \cdots \sum_{v_n=0}^{q-1} \prod_{i=1}^{n} a_{i,v_i}$$

Demonstração: Para $n = 1$ vem

$$\prod_{i=1}^{1} \sum_{j=0}^{q-1} a_{i,j} = a_{1,0} + \ldots + a_{1,q-1} = \sum_{v_1=0}^{q-1} \prod_{i=1}^{1} a_{i,v_i}$$

Suponha que $n > 1$ e que o resultado é válido para $n - 1$. Então

$$\begin{aligned}
\sum_{v_1=0}^{q-1} \cdots \sum_{v_n=0}^{q-1} \prod_{i=1}^{n} a_{i,v_i} &= \sum_{v_1=0}^{q-1} \cdots \sum_{v_{n-1}=0}^{q-1} \left(\prod_{i=1}^{n-1} a_{i,v_i} (a_{n,0} + a_{n,1} + \ldots + a_{n,q-1}) \right) \\
&= \left(\sum_{v_1=0}^{q-1} \cdots \sum_{v_{n-1}=0}^{q-1} \prod_{i=1}^{n-1} a_{i,v_i} \right) \left(\sum_{j=0}^{q-1} a_{n,j} \right) \\
&= \prod_{i=1}^{n-1} \sum_{j=0}^{q-1} a_{i,j} \left(\sum_{j=0}^{q-1} a_{n,j} \right) \\
&= \prod_{i=1}^{n} \sum_{j=0}^{q-1} a_{i,j}
\end{aligned}$$

ou seja, pelo princípio da indução, o resultado é válido para todo $n \in \mathbb{N}$. □

A demonstração do teorema seguinte foi adaptada da que é apresentada por MacWilliams e Sloane [6].

Teorema 4.2.5 *Seja C um $(n,k)-$código linear binário e $C^{\perp}$ o seu dual. Então*

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$$

Esta identidade é conhecida por ***Identidade de MacWilliams****.*

Demonstração: Considere o anel de polinómios em x e y com coeficientes racionais, $\mathbb{Q}[x,y]$, e f definida por

$$\begin{array}{rccc} f: & F_2^n & \to & \mathbb{Q}[x,y] \\ & v & \mapsto & x^{n-wt(v)} y^{wt(v)} \end{array}$$

Para $u \in F_2^n$, a transformada de Hadamard de f é

$$\hat{f}(u) = \sum_{v \in F_2^n} (-1)^{u.v} x^{n-wt(v)} y^{wt(v)}$$

Então

$$\begin{aligned} \hat{f}(u) &= \sum_{v \in F_2^n} (-1)^{u.v} x^{n-wt(v)} y^{wt(v)} \\ &= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} (-1)^{u_1 v_1 + \ldots + u_n v_n} x^{n-(v_1+\ldots+v_n)} y^{v_1+\ldots+v_n} \\ &= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} (-1)^{u_1 v_1} x^{1-v_1} y^{v_1} \cdot \ldots \cdot (-1)^{u_n v_n} x^{1-v_n} y^{v_n} \\ &= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_i v_i} x^{1-v_i} y^{v_i} \\ &= \sum_{v_1=0}^{1} \cdots \sum_{v_n=0}^{1} \prod_{i=1}^{n} (-1)^{u_i v_i} x^{1-v_i} y^{v_i} \\ &= \prod_{i=1}^{n} \sum_{k=0}^{1} (-1)^{u_i k} x^{1-k} y^{k} \quad \text{, pela proposição 4.2.4} \end{aligned}$$

Mas

$$\sum_{k=0}^{1} (-1)^{u_i k} x^{1-k} y^{k} = x + (-1)^{u_i} y$$

Assim,

$$\begin{aligned}\hat{f}(u) &= \prod_{i=1}^{n}(x+(-1)^{u_i}y) \\ &= \left(\prod_{u_i=0}(x+y)\right)\left(\prod_{u_i=1}(x-y)\right) \\ &= (x+y)^{n-wt(u)}(x-y)^{wt(u)}\end{aligned}$$

Pela proposição 4.2.3 tem-se

$$|C|\sum_{v\in C^{\perp}} f(v) = \sum_{u\in C}\hat{f}(u) = \sum_{u\in C}(x+y)^{n-wt(u)}(x-y)^{wt(u)} \tag{4.2}$$

e, por definição de f

$$|C|\sum_{v\in C^{\perp}} f(v) = |C|\sum_{v\in C^{\perp}} x^{n-wt(v)}y^{wt(v)} \tag{4.3}$$

De (4.2) e (4.3) resulta que

$$\sum_{v\in C^{\perp}} x^{n-wt(v)}y^{wt(v)} = \frac{1}{|C|}\sum_{u\in C}(x+y)^{n-wt(u)}(x-y)^{wt(u)}$$

ou seja,

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|}W_C(x+y,x-y)$$

□

Exemplo 4.2.6 *O* $(7,4)-$*código linear binário de Hamming é formado por* $2^4 = 16$ *palavras e tem a seguinte matriz geradora*

$$G = (I_4|A) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

O seu dual tem como matriz geradora

$$H = (-A^T|I_3) = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Na tabela seguinte estão representadas as $2^3 = 8$ *palavras do dual e os respectivos pesos.*

Palavra	peso
0000000	0
0111100	4
1011010	4
1101001	4
1100110	4
0110011	4
1010101	4
0001111	4

Tabela 4.1: Palavras e pesos do dual do $(7,4)-$código binário de Hamming

Assim, o enumerador de pesos para o dual do $(7,4)-$*código de Hamming é*

$$W_{C^\perp}(x,y) = x^7 + 7x^3y^4$$

A partir da identidade de MacWilliams pode obter-se o enumerador de pesos de C

$$\begin{aligned} W_C(x,y) &= \frac{1}{|C^\perp|} W_{C^\perp}(x+y, x-y) \\ &= \frac{1}{8}((x+y)^7 + 7(x+y)^3(x-y)^4) \\ &= x^7 + 7x^4y^3 + 7x^3y^4 + y^7 \end{aligned}$$

Logo, C *tem uma palavra de peso* 0*, sete palavras de peso* 3*, sete de peso* 4 *e uma de peso* 7*. Neste caso, atendendo a que* C *é formado por apenas* 16 *palavras, este resultado podia ter sido obtido determinando o peso de cada uma delas.*

Palavra	peso
0000000	0
1000011	3
0100101	3
0010110	3
1001100	3
0101010	3
0011001	3
1110000	3
0001111	4
1100110	4
1010101	4
0110011	4
1101001	4
1011010	4
0111100	4
1111111	7

Tabela 4.2: Palavras e pesos do $(7,4)-$código linear binário de Hamming

4.3 Identidade de MacWilliams para códigos lineares sobre F_p, com p primo

A Identidade de MacWilliams é válida não apenas sobre o corpo F_2, mas sobre qualquer corpo F_p, com p primo.

Definição 4.3.1 *Seja C um $(n,k)-$código linear sobre um corpo F_p. Para $i \in F_p$ e $v \in F_p^n$,*

$$C_i = \{u \in C : u.v = i\}$$

Proposição 4.3.2 *Seja C um $(n,k)-$código linear sobre um corpo F_p. Então, $v \notin C^{\perp}$ se e só se para todo $i \in F_p$ existe pelo menos um $u \in C$ tal que*

$$C_i = u + C_0$$

Demonstração: Suponha que $v \in C^{\perp}$. Então, para todo $u \in C$, $u.v = 0$ e, por consequência, para $i \neq 0$, $C_i = \emptyset$. Portanto, não existe nenhum $u \in C$ tal que $C_i = u + C_0$.

Se $v \notin C^{\perp}$, existe $w = (w_1, \ldots, w_n) \in C$ tal que $w.v = k$, com $k \in F_p \setminus \{0\}$. Para qualquer $i \in F_p$

$$(ik^{-1}w).v = ik^{-1}(w.v) = i(k^{-1}k) = i(1) = i$$

ou seja, $ik^{-1}w \in C_i$. Considerando $u = ik^{-1}w$, verifica-se que $u \in C$, isto é, para todo $i \in F_p$, $C_i \neq \emptyset$.

Sejam s e t dois elementos de C_i. Então, existe pelo menos um $v \in F_p^n$ tal que

$$(s-t).v = s.v - t.v = i - i = 0, \text{ ou seja, } s - t = z \in C_0$$

Como $s = t + z$, conclui-se que

$$C_i = u + C_0$$

□

Desta proposição resulta que $|C_i| = |C_0|$.

Exemplo 4.3.3 *Seja $C \subseteq F_3^3$ o código linear definido por*

$$C = \{000, 100, 200, 011, 022, 111, 122, 211, 222\}$$

O seu dual é $C^{\perp} = \{000, 012, 021\}$.

Tome $v \in C^{\perp}$, por exemplo, $v = 012$. Como, para todo $u \in C$, $u.v = 0$, concluí-se que

$$C_1 = C_2 = \emptyset \text{ e } C = C_0$$

Portanto, não existe $i \in F_3 \setminus \{0\}$ tal que $C_i = u + C_0$.

Por outro lado, considerando $v \notin C^{\perp}$, por exemplo, $v = 120$, obtém-se

$C_0 = \{000, 111, 222\}$; $C_1 = \{100, 022, 211\}$; $C_2 = \{200, 011, 122\}$

Verifica-se, ainda, que

$$C_0 = u + C_0 \ \textit{para qualquer} \ u \in C_0;$$

$$C_1 = u + C_0 \ \textit{para qualquer} \ u \in C_1;$$

$$C_2 = u + C_0 \ \textit{para qualquer} \ u \in C_2;$$

$$e, \quad |C_0| = |C_1| = |C_2|$$

Proposição 4.3.4 *Seja C um $(n,k)-$código linear sobre um corpo F_p e ζ uma raíz primitiva índice p da unidade, em $\mathbb{C}$. Então, para $v \in F_p^n$*

$$\sum_{u \in C} \zeta^{u.v} = \begin{cases} |C| & \textit{se } v \in C^{\perp} \\ 0 & \textit{se } v \notin C^{\perp} \end{cases}$$

Demonstração: Se $v \in C^{\perp}$, então $\zeta^{u.v} = \zeta^0 = 1$ e, portanto, $\sum_{u \in C} \zeta^{u.v} = |C| \, .1 = |C|$.

Se $v \notin C^{\perp}$, então

$$\begin{aligned} \sum_{u \in C} \zeta^{u.v} &= \sum_{i=0}^{p-1} \sum_{u \in C_i(v)} \zeta^{u.v} \\ &= \sum_{i=0}^{p-1} |C_i(v)| \, \zeta^i \\ &= |C_0(v)| \sum_{i=0}^{p-1} \zeta^i \end{aligned}$$

Mas $\sum_{i=0}^{p-1} \zeta^i = \zeta^0 + \ldots + \zeta^{p-1} = \dfrac{1-\zeta^p}{1-\zeta}$. Como ζ é raíz primitiva índice p da unidade, em $\mathbb{C}$, resulta que $1 - \zeta^p = 0$ e $1 - \zeta \neq 0$, ou seja, $\sum_{i=0}^{p-1} \zeta^i = 0$. Então, se $v \notin C^{\perp}$

$$\sum_{u \in C} \zeta^{u.v} = |C_0(v)| \times 0 = 0$$

□

Definição 4.3.5 *Seja f uma função definida de F_p^n em $\mathbb{C}[x,y]$ e seja ζ uma raíz primitiva da unidade. Chama-se* ***transformada de Fourier de f*** *e representa-se por $\widehat{f}$, à função definida para todo $u \in F_p^n$ por*

$$\begin{array}{rccc} \widehat{f}: & F_p^n & \to & \mathbb{C}[x,y] \\ & u & \mapsto & \displaystyle\sum_{v \in F_p^n} f(v)\, \zeta^{u.v} \end{array}$$

Proposição 4.3.6 *Para uma dada função $f : F_p^n \to \mathbb{C}[x,y]$, com $w \in F_p^n$ e ζ raíz primitiva da unidade, tem-se*

$$f(w) = \frac{1}{p^n} \sum_{u \in F_p^n} \widehat{f}(u)\, \zeta^{-u.w}$$

Demonstração:

$$\begin{aligned} \frac{1}{p^n} \sum_{u \in F_p^n} \widehat{f}(u)\, \zeta^{-u.w} &= \frac{1}{p^n} \sum_{u \in F_p^n} \sum_{v \in F_p^n} f(v)\, \zeta^{u.v} \zeta^{-u.w} \\ &= \frac{1}{p^n} \sum_{u \in F_p^n} \sum_{v \in F_p^n} f(v)\, \zeta^{u.(v-w)} \\ &= \frac{1}{p^n} \sum_{v \in F_p^n} f(v) \sum_{u \in F_p^n} \zeta^{u.(v-w)} \end{aligned}$$

Considerando $C = F_p^n$ vem $C^{\perp} = \{00\ldots0\}$. Aplicando a proposição 4.3.4 e notando que para $v - w \in C^{\perp}$ vem $v = w$ resulta que

$$\begin{aligned} \frac{1}{p^n} \sum_{v \in F_p^n} f(v) \sum_{u \in F_p^n} \zeta^{u.(v-w)} &= \frac{1}{p^n} \sum_{v=w} f(v) \sum_{u \in F_p^n} \zeta^{u.(v-w)} + \frac{1}{p^n} \sum_{v \neq w} f(v) \sum_{u \in F_p^n} \zeta^{u.(v-w)} \\ &= \frac{1}{p^n} f(w).\left|F_p^n\right| \\ &= \frac{1}{p^n} f(w) p^n \\ &= f(w) \end{aligned}$$

□

Proposição 4.3.7 *Seja C um $(n,k)-$código linear sobre um corpo F_p, f uma função definida de F_p^n em $\mathbb{C}[x,y]$ e $\widehat{f}$ a transformada de Fourier de f. Então,*

$$\sum_{v\in C^\perp} f(v) = \frac{1}{|C|}\sum_{u\in C}\widehat{f}(u)$$

Demonstração:

$$\begin{aligned}
\frac{1}{|C|}\sum_{u\in C}\widehat{f}(u) &= \frac{1}{|C|}\sum_{u\in C}\sum_{v\in F_p^n} f(v)\,\zeta^{u.v} \\
&= \frac{1}{|C|}\sum_{v\in F_p^n}\sum_{u\in C} f(v)\,\zeta^{u.v} \\
&= \frac{1}{|C|}\sum_{v\in F_p^n} f(v)\sum_{u\in C}\zeta^{u.v} \\
&= \frac{1}{|C|}\left(\sum_{v\in C^\perp} f(v)\sum_{u\in C}\zeta^{u.v} + \sum_{v\notin C^\perp} f(v)\sum_{u\in C}\zeta^{u.v}\right)
\end{aligned}$$

Aplicando a proposição 4.3.4 resulta

$$\begin{aligned}
\frac{1}{|C|}\sum_{u\in C}\widehat{f}(u) &= \frac{1}{|C|}\sum_{v\in C^\perp} f(v)\,|C| \\
&= \sum_{v\in C^\perp} f(v)
\end{aligned}$$

□

Teorema 4.3.8 (Identidade de MacWilliams) *Seja C um $(n,k)-$código linear sobre um corpo F_p e $C^\perp$ o seu dual. Então*

$$W_{C^\perp}(x,y) = \frac{1}{|C|}W_C\left(x+(p-1)y, x-y\right)$$

Demonstração: Seja f definida por

$$\begin{array}{rccc} f: & F_p^n & \to & \mathbb{C}[x,y] \\ & w & \mapsto & x^{n-wt(w)}y^{wt(w)} \end{array}$$

Então

$$\sum_{v\in C^\perp} f(v) = \sum_{v\in C^\perp} x^{n-wt(v)}y^{wt(v)} = W_{C^\perp}(x,y) \tag{4.4}$$

Por outro lado, da definição de transformada de Fourier, vem para todo $u \in F_p^n$

$$\begin{aligned}
\widehat{f}(u) &= \sum_{w \in F_p^n} f(w) \\
&= \sum_{w \in F_p^n} x^{n-wt(w)} y^{wt(w)} \zeta^{u.w} \\
&= \sum_{w_1=0}^{p-1} \cdots \sum_{w_n=0}^{p-1} x^{n-wt(w_1,\ldots,w_n)} y^{wt(w_1,\ldots,w_n)} \ \zeta^{(u_1w_1+\ldots+u_nw_n)} \\
&= \sum_{w_1=0}^{p-1} \cdots \sum_{w_n=0}^{p-1} x^{1-wt(w_1)} y^{wt(w_1)} \zeta^{(u_1w_1)} \ldots x^{1-wt(w_n)} y^{wt(w_n)} \zeta^{(u_nw_n)} \\
&= \sum_{w_1=0}^{p-1} \cdots \sum_{w_n=0}^{p-1} \prod_{i=1}^{n} x^{1-wt(w_i)} y^{wt(w_i)} \zeta^{(u_iw_i)} \\
&= \prod_{i=1}^{n} \sum_{k=0}^{p-1} x^{1-wt(k)} y^{wt(k)} \zeta^{(u_ik)} \quad \text{, pela proposição 4.2.4} \\
&= \prod_{i=1}^{n} \left(x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}\right) \\
&= \prod_{\substack{i=1 \\ u_i=0}}^{n} (x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}) \prod_{\substack{i=1 \\ u_i \neq 0}}^{n} (x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)})
\end{aligned}$$

Para $u_i = 0$,

$$\left(x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}\right) = x + y(p-1)$$

Para $u_i \neq 0$,

$$\begin{aligned}
\left(x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}\right) &= x + y\zeta^{u_i} \frac{1 - (\zeta^{u_i})^{p-1}}{1 - \zeta^{u_i}} \\
&= x + y \frac{\zeta^{u_i} - (\zeta^{u_i})^{p}}{1 - \zeta^{u_i}}
\end{aligned}$$

Como ζ é raíz primitiva índice p da unidade, $(\zeta^{u_i})^p = (\zeta^p)^{u_i} = 1$ e $\zeta^{u_i} \neq 1$ pois $0 < u_i < p$, vem que

$$x + y \frac{\zeta^{u_i} - (\zeta^{u_i})^{p}}{1 - \zeta^{u_i}} = x + y(-1) = x - y$$

Assim,

$$\begin{aligned} & \prod_{\substack{i=1 \\ u_i=0}}^{n} (x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}) \prod_{\substack{i=1 \\ u_i\neq 0}}^{n} (x + y\zeta^{u_i} + \ldots + y\zeta^{u_i(p-1)}) \\ = \; & (x + (p-1)y)^{n-wt(w)} (x-y)^{wt(w)} \end{aligned}$$

Portanto,

$$\begin{aligned} \frac{1}{|C|} \sum_{u \in C} \widehat{f}(u) &= \frac{1}{|C|} \sum_{u \in C} (x + (p-1)y)^{n-wt(u)} (x-y)^{wt(u)} \\ &= \frac{1}{|C|} W_C (x + (p-1)y, x-y) \end{aligned}$$

Finalmente, aplicando a proposição 4.3.7 a (4.4) e ao resultado anterior concluí-se que

$$W_{C^\perp}(x,y) = \frac{1}{|C|} W_C (x + (p-1)y, x-y)$$

□

Exemplo 4.3.9 *O código linear C definido por $C = \{000, 021, 012\}$ sobre o corpo F_3 tem enumerador de pesos de Hamming igual a*

$$W_C(x,y) = x^3 + 2xy^2$$

Aplicando a generalização da Identidade de MacWilliams obtém-se o enumerador de pesos do dual de C

$$\begin{aligned} W_{C^\perp}(x,y) &= \frac{1}{3} W_C(x+2y, x-y) \\ &= \frac{1}{3} \left((x+2y)^3 + 2(x+2y)(x-y)^2 \right) \\ &= x^3 + 2x^2y + 2xy^2 + 4y^3 \end{aligned}$$

Como o dual de C é

$$C^\perp = \{000, 100, 200, 011, 022, 111, 122, 211, 222\}$$

facilmente se confirma o resultado obtido.

Segundo Roman [8], Marcel Golay introduziu, em 1949, alguns códigos lineares, actualmente designados por códigos de Golay. Estes códigos são normalmente definidos pela matriz de controlo. No exemplo seguinte vai determinar-se o enumerador de pesos de um deles.

Exemplo 4.3.10 *O* $(11,6)-$*código ternário de Golay é formado por* $3^6 = 729$ *palavras e, por isso, a determinação do seu enumerador de pesos é uma tarefa trabalhosa. A partir da matriz de controlo*

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

pode obter-se mais rapidamente a distribuição de pesos para as $3^5 = 243$ *palavras que constituem o dual. O dual do* $(11,6)-$*código de Golay tem o seguinte enumerador de pesos*

$$W_{C^\perp}(x,y) = x^{11} + 132x^5y^6 + 110x^2y^9$$

Através da Identidade de MacWilliams (teorema 4.3.8), obtém-se

$$\begin{aligned} W_C(x,y) &= \frac{1}{243} W_{C^\perp}(x+2y, x-y) \\ &= \frac{1}{243}\left((x+2y)^{11} + 132(x+2y)^5(x-y)^6 + 110(x+2y)^2(x-y)^9\right) \\ &= x^{11} + 132x^6y^5 + 132x^5y^6 + 330x^3y^8 + 110x^2y^9 + 24y^{11} \end{aligned}$$

Este código tem distância mínima igual a 5 pois 5 é o menor peso de uma palavra-código não nula. Assim, permite detectar até 4 erros e corrigir até 2 erros.

A Identidade de MacWilliams revela-se, assim, muito útil para obter o enumerador de pesos de um $(n, k)-$código linear C sobre um corpo F_p sem ter que determinar o peso de todas as suas p^k palavras, pois, a menos que k seja relativamente pequeno esta é tarefa pode tornar-se muito difícil. Se k for muito grande será, naturalmente, $n - k$ pequeno e assim o enumerador de pesos de um código linear C pode obter-se a partir do enumerador de pesos do seu dual.

Capítulo 5

Equivalência de Códigos Lineares

Neste capítulo, define-se transformação monomial como resultado das restrições impostas às isometrias de Hamming, definidas no Capítulo 2, para que estas preservem a linearidade. Em seguida, mostra-se que as transformações monomiais são as únicas transformações lineares que preservam os pesos das palavras-código e demonstra-se o teorema da equivalência de códigos que, estabelece condições para a equivalência de códigos lineares. Este teorema, atribuído a F. J. MacWilliams, é o principal resultado deste capítulo. Por fim, apresenta-se a conclusão deste trabalho.

5.1 Transformação monomial

As propriedades básicas de um código estão ligadas à noção de distância de Hamming. Assim, parece razoável pensar na equivalência de códigos através de isometrias de Hamming. Essa ideia de equivalência foi abordada no Capítulo 2, tendo-se concluído que as isometrias de Hamming eram compostas de dois tipos de transformações:

- permutação do conteúdo de uma componente
- permutação das componentes

No entanto, a imagem de um código linear através de uma isometria não é necessariamente linear pois, em geral, a permutação do conteúdo de uma componente não preserva a linearidade. No exemplo 2.3.2, a isometria φ transforma o código linear C num código D não linear. Assim, interessa analisar as isometrias que são lineares.

Proposição 5.1.1 *Seja F um corpo. Então, para qualquer $b \in F \setminus \{0\}$*

1. *A função*

$$\begin{array}{rccc} \eta_b : & F & \to & F \\ & a & \mapsto & ab \end{array}$$

   é uma bijecção linear cuja inversa é $\eta_{b^{-1}}$.

2. *Qualquer bijecção linear é da forma $f = \eta_b$.*

Demonstração:

1. Para quaisquer $a, c, \lambda, \mu \in F$ e $b \in F \setminus \{0\}$

$$(\eta_{b^{-1}} \circ \eta_b)(a) = \eta_{b^{-1}}(ab) = (ab)b^{-1} = a(b^{-1}b) = a$$

   e, analogamente, $(\eta_b \circ \eta_{b^{-1}})(a) = a$. Portanto, $\eta_{b^{-1}}$ é a inversa de η_b. Também,

$$\eta_b(\lambda a + \mu c) = (\lambda a + \mu c)b = \lambda(ab) + \mu(cb) = \lambda\eta_b(a) + \mu\eta_b(c)$$

   Portanto, η_b é uma bijecção linear.

2. Seja $f : F \to F$ uma bijecção linear. Então, para todo $a \in F$

$$f(a) = af(1) = \eta_{f(1)}(a) \ \text{, com} \ f(1) \neq 0$$

   pois f é injectiva. Portanto, tomando $b = f(1)$, conclui-se $f = \eta_b$.

□

Proposição 5.1.2 *Seja F um corpo. Para qualquer permutação π, a isometria*

$$\begin{array}{rccc} T_\pi : & F^n & \to & F^n \\ & (u_1, \ldots, u_n) & \mapsto & (u_{\pi(1)}, \ldots, u_{\pi(n)}) \end{array}$$

é uma transformação linear de F^n.

Demonstração: Sejam $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n) \in F^n$, $\lambda, \mu \in F$ e $z = \lambda u + \mu v = (\lambda u_1 + \mu v_1, \ldots, \lambda u_n + \mu v_n)$. Então

$$\begin{aligned} T_\pi(\lambda u + \mu v) &= T_\pi(z) \\ &= (z_{\pi(1)}, \ldots, z_{\pi(n)}) \\ &= (\lambda u_{\pi(1)} + \mu v_{\pi(1)}, \ldots, \lambda u_{\pi(n)} + \mu v_{\pi(n)}) \\ &= \lambda(u_{\pi(1)}, \ldots, u_{\pi(n)}) + \mu(v_{\pi(1)}, \ldots, v_{\pi(n)}) \\ &= \lambda T_\pi(u) + \mu T_\pi(v) \end{aligned}$$

ou seja, T_π é uma isometria linear em F^n. □

Assim, são lineares as isometrias compostas por transformações de dois tipos

1. multiplicação do conteúdo de uma componente por um escalar não nulo (prop.5.1.1)

2. permutação das componentes (prop.5.1.2)

As funções compostas por transformações do tipo 1. podem ser representadas por uma matriz diagonal, D, pois para todo $b_1, \ldots, b_n \in F \setminus \{0\}$

$$\begin{array}{rccc} f : & F^n & \to & F^n \\ & (u_1, \ldots, u_n) & \mapsto & (u_1 b_1, \ldots, u_n b_n) \end{array}$$

pode ser escrita na forma

$$\begin{array}{rccc} f : & F^n & \to & F^n \\ & (u_1, \ldots, u_n) & \mapsto & (u_1, \ldots, u_n)D \end{array}$$

sendo

$$D = \begin{pmatrix} b_1 & 0 & \dots & 0 \\ 0 & b_2 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & b_n \end{pmatrix}$$

Por outro lado, a transformação referida em 2. está associada a uma matriz de permutação, P, pois

$$\begin{array}{rccc} f: & F^n & \to & F^n \\ & (u_1, \dots, u_n) & \mapsto & (u_{\pi(1)}, \dots, u_{\pi(n)}) \end{array}$$

pode ser definida por

$$\begin{array}{rccc} f: & F^n & \to & F^n \\ & (u_1, \dots, u_n) & \mapsto & (u_1, \dots, u_n)P \end{array}$$

sendo P a matriz cujas colunas são $e_{\pi(1)}, \dots, e_{\pi(n)}$, em que para todo $i = 1, \dots, n$, $e_{\pi(i)}$ representa o $\pi(i)$-ésimo vector da base canónica de F^n.

Existem, $q-1$ bijecções lineares em F e $(q-1)^n \times n!$ isometrias lineares em F_q^n.

Definição 5.1.3 *Chama-se* ***transformação monomial*** *a qualquer isometria linear e* ***matriz monomial****, à matriz* Λ *associada a uma transformação monomial.*

A matriz Λ é da forma $\Lambda = DP$ onde D é uma matriz diagonal e P é uma matriz de permutação, isto é, Λ tem exactamente uma entrada não nula em cada linha e cada coluna.

Faz sentido estudar as transformações, entre dois códigos, que preservem os pesos das palavras.

Em seguida, prova-se que tais transformações têm que ser transformações monomiais. A demonstração apresentada é adaptada de Bogart, Goldberg e Gordon [1].

5.2 Teorema de MacWilliams para a equivalência de códigos

Definição 5.2.1 *Dois (n,k)-**códigos lineares** C e D sobre um corpo F dizem-se **equivalentes** se existe uma transformação monomial $\Phi : F^n \to F^n$ tal que $\Phi(C) = D$.*

Seja F_q um corpo. Denota-se por $L_1, \ldots, L_{\mu(k)}$ os distintos subespaços vectoriais de dimensão um do espaço vectorial F_q^k e por $u_1, \ldots, u_{\mu(k)}$ os respectivos geradores.

Proposição 5.2.2 *Seja F_q um corpo. O número de subespaços vectoriais distintos de dimensão um de F_q^k é dado por*

$$\mu(k) = \frac{q^k - 1}{q - 1}$$

Demonstração: F_q^k é formado por q^k vectores sendo $q^k - 1$ não nulos.
Fixado um vector não nulo $u \in F_q^k$ ele tem $q - 1$ múltiplos não nulos que são $u, 2u, \ldots, (q-1)u$. Então, o número de subespaços de dimensão um de F_q^k é dado por

$$\mu(k) = \frac{q^k - 1}{q - 1}$$

□

Definição 5.2.3 *Dois quaisquer subespaços L_i e L_j dizem-se **subespaços vectoriais ortogonais** e escreve-se $L_i \perp L_j$, se $u_i.u_j = 0$.*

É óbvio que, se para algum u_i e algum u_j, $u_i.u_j = 0$, então $u.u^{'} = 0$ para todos os vectores não nulos u e $u^{'}$ pertencentes a L_i e L_j, respectivamente.

Proposição 5.2.4 *Seja F_q um corpo. Fixado um qualquer L_i*

$$|\{j \in \{1, \ldots, \mu(k)\} : L_j \perp L_i\}| = \mu(k-1)$$

Demonstração: Fixado um qualquer L_i

$$|\{j \in \{1, \ldots, \mu(k)\} : L_j \perp L_i\}|$$

corresponde ao número de subespaços de dimensão um de

$$M = \left\{u \in F_q^k : u.u_i = 0\right\}$$

Seja f a transformação linear definida por

$$\begin{array}{rcl} f : F_q^k & \rightarrow & F_q \\ u & \mapsto & u.u_i \end{array}$$

Ora, $Kerf = M$ e $Imf = F_q$. Então, $dim(M) = k - 1$. Logo, M é formado por $q^{k-1} - 1$ vectores não nulos, ou seja, M tem $\frac{q^{k-1}-1}{q-1} = \mu(k-1)$ subespaços de dimensão um. □

Proposição 5.2.5 *Seja F_q um corpo. Fixados dois quaisquer L_i e L_j*

$$|\{s \in \{1, \ldots, \mu(k)\} : L_s \perp L_i \ \ e \ \ L_s \perp L_j\}| = \mu(k-2)$$

Demonstração: Fixados dois quaisquer L_i e L_j

$$|\{s \in \{1, \ldots, \mu(k)\} : L_s \perp L_i \ \text{ e } \ L_s \perp L_j\}|$$

corresponde ao número de subespaços de dimensão um de

$$N = \left\{u \in F_q^k : (u.u_i, u.u_j) = (0, 0)\right\}$$

Seja g a transformação linear definida por

$$\begin{array}{rcl} g : F_q^k & \rightarrow & F_q^2 \\ u & \mapsto & (u.u_i, u.u_j) \end{array}$$

Ora, $Kerg = N$ e $Img = F_q^2$. Então, $dim(N) = k-2$. Logo, N é formado por $q^{k-2} - 1$ vectores não nulos, a que correspondem $\frac{q^{k-2}-1}{q-1} = \mu(k-2)$ subespaços de dimensão um. □

Seja $T = (t_{ij})_{1 \leq i,j \leq \mu(k)}$ a matriz definida por

$$t_{ij} = \begin{cases} 0 & \text{se } L_i \perp L_j \\ 1 & \text{caso contrário} \end{cases}$$

Esta matriz descreve a relação de ortogonalidade entre os subespaços de dimensão um de F_q^k.

Proposição 5.2.6 *Seja F_q^k um espaço vectorial sobre um corpo F_q e, para $i = 1, \ldots, \mu(k)$, seja e_i o i-ésimo vector da base canónica de $\mathbb{Q}^{\mu(k)}$, sendo $\mathbb{Q}$ o conjunto dos números racionais.*

1. *A soma de todas as linhas da matriz T é o vector $x = q^{k-1} \sum_{i=1}^{\mu(k)} e_i$.*
2. *A soma de todas as linhas da matriz T com entrada igual a zero na posição j é o vector $y(j) = q^{k-2} \sum_{\substack{i=1 \\ i \neq j}}^{\mu(k)} e_i$.*

Demonstração:

1. Seja $x = (x_1, \ldots, x_{\mu(k)})$ o vector soma de todas as linhas de T. Então, para $i = 1, \ldots, \mu(k)$,

$$\begin{aligned} x_i &= t_{1i} + t_{2i} + \ldots + t_{\mu(k)i} \\ &= |\{j \in \{1, \ldots, \mu(k)\} : L_j \not\perp L_i\}| \\ &= \mu(k) - |\{j \in \{1, \ldots, \mu(k)\} : L_j \perp L_i\}| \\ &= \mu(k) - \mu(k-1) \quad \text{pela proposição 5.2.4} \\ &= \frac{q^k - 1}{q - 1} - \frac{q^{k-1} - 1}{q - 1} \\ &= \frac{q^k - q^{k-1}}{q - 1} \\ &= q^{k-1} \end{aligned}$$

Logo, $x = q^{k-1} \sum_{i=1}^{\mu(k)} e_i$.

2. Seja $y(j) = (y_1, \ldots, y_{\mu(k)})$ o vector soma de todas as linhas com entrada igual a zero na posição j. Então, para $i = 1, \ldots, \mu(k)$ e $i \neq j$

$$\begin{aligned} y_i &= |\{s \in \{1, \ldots, \mu(k)\} : L_s \perp L_j \text{ e } L_s \not\perp L_i\}| \\ &= |\{s \in \{1, \ldots, \mu(k)\} : L_s \perp L_j\}| - |\{s \in \{1, \ldots, \mu(k)\} : L_s \perp L_j \text{ e } L_s \perp L_i\}| \\ &= \mu(k-1) - \mu(k-2) \quad \text{pelas proposições 5.2.4 e 5.2.5} \\ &= \frac{q^k - 1}{q-1} - \frac{q^{k-2} - 1}{q-1} \\ &= q^{k-2} \end{aligned}$$

Logo, $y(j) = q^{k-2} \sum_{\substack{i=1 \\ i \neq j}}^{\mu(k)} e_i$.

□

Proposição 5.2.7 *A matriz T é invertível em $\mathbb{Q}$.*

Demonstração: Qualquer vector $e_1, \ldots, e_{\mu(k)}$ da base canónica de $\mathbb{Q}^{\mu(k)}$ é combinação linear das linhas da matriz T pois para $j = 1, \ldots, \mu(k)$

$$\frac{x}{q^{k-1}} - \frac{y(j)}{q^{k-2}} = \sum_{i=1}^{\mu(k)} e_i - \sum_{\substack{i=1 \\ i \neq j}}^{\mu(k)} e_i = e_j$$

Logo, T tem característica $\mu(k)$ e, portanto, é invertível. □

Definição 5.2.8 *Sejam $X_1, X_2, \ldots, X_n$ as n colunas da matriz geradora X, de um $(n,k)-$código linear C sobre um corpo F_q. O vector coluna $r^X = (r_1^X, \ldots, r_{\mu(k)}^X)^T$ com*

$$r_i^X = \left|\left\{j \in \{1, \ldots, n\} : X_j^T \in L_i \text{ e } X_j^T \neq \overline{0}\right\}\right|$$

indica o número de colunas não nulas de X que pertencem a cada um dos subespaços vectoriais L_i, isto é, r_i^X indica quantas colunas de X são múltiplos escalares não nulos de u_i.

O número de colunas não nulas de X é dado por $\sum_{i=1}^{\mu(k)} r_i^X$ e, portanto, X tem $n - \sum_{i=1}^{\mu(k)} r_i^X$ colunas que são nulas.

Seja X uma matriz geradora de um $(n,k)-$código linear C sobre um corpo F_q e, para todo $u \in F_q^k$, $f : F_q^k \to C$ a função linear definida por $f(u) = uX$. Sendo $u_1, \ldots, u_{\mu(k)}$ os geradores de $L_1, \ldots, L_{\mu(k)}$ de F_q^k, então $f(u_1), \ldots, f(u_{\mu(k)})$ são os geradores dos subespaços vectoriais de dimensão um de C. Assim, $f(L_i) =< f(u_i) >$.

O resultado seguinte prova que o peso de qualquer palavra-código, $wt\,(f(u_i))$, a menos da multiplicação por escalar não nulo é a i-ésima componente de Tr^X.

Proposição 5.2.9 *Para qualquer* $1 \leq i \leq \mu(k)$ *tem-se*

$$(Tr^X)_i = wt(f(u_i))$$

Demonstração:

$$\begin{aligned}
(Tr^X)_i &= \sum_{j=1}^{\mu(k)} t_{ij} r_j^X \\
&= \sum_{\substack{j=1 \\ L_j \not\subset L_i}}^{\mu(k)} r_j^X \\
&= \sum_{\substack{j=1 \\ L_j \not\subset L_i}}^{\mu(k)} \left|\left\{k \in \{1,\ldots,n\} : X_k^T \in L_j \text{ e } X_k^T \neq \overline{0}\right\}\right| \\
&= \sum_{j=1}^{\mu(k)} \left|\left\{k \in \{1,\ldots,n\} : X_k^T \in L_j \text{ e } u_i.X_k^T \neq 0\right\}\right| \\
&= \left|\left\{k \in \{1,\ldots,n\} : u_i.X_k^T \neq 0\right\}\right| \\
&= wt(u_i X) \\
&= wt(f(u_i))
\end{aligned}$$

Assim, o vector coluna Tr^X determina o peso de cada um dos subespaços de dimensão um de C. □

Considere um isomorfismo φ de C em D que preserve os pesos e a função linear $g : F_q^k \to D$ definida por $g = \varphi \circ f$. Então, para todo $u \in F_q^k$, $g(u) = (\varphi \circ f)(u) = \varphi(f(u)) = \varphi(uX)$. A matriz Y de g relativamente à base canónica de F_q^k é uma matriz geradora de D. Pela proposição 5.2.9, pode afirmar-se que $(Tr^Y)_i = wt(g(u_i))$ sendo r^Y o vector coluna para Y obtido de forma análoga ao vector r^X para X.

Teorema 5.2.10 *Sejam C e D dois $(n,k)-$códigos lineares e X a matriz geradora de C. Sejam $f : F_q^k \to C$ tal que $f(u) = uX$, φ um isomorfismo de C em D que preserve os pesos, isto é, para todo $u \in C$, $wt(\varphi(u)) = wt(u)$ e $g : F_q^k \to D$ definida por $g = \varphi \circ f$. Então, existe uma matriz monomial, Λ, tal que $X\Lambda = Y$ sendo Y a matriz de g relativamente à base canónica de F_q^k.*

Demonstração: Para todo $i \in \{1, \ldots, \mu(k)\}$

$$\begin{aligned} wt(g(u_i)) &= wt(\varphi(f(u_i))) \\ &= wt(f(u_i)) \quad \text{pois } \varphi \text{ preserva os pesos} \end{aligned}$$

Pela proposição 5.2.9, vem para todo $i \in \{1, \ldots, \mu(k)\}$, $(Tr^X)_i = (Tr^Y)_i$, isto é, $Tr^X = Tr^Y$. Como a matriz T é invertível (proposição 5.2.7), resulta que $r^X = r^Y$. Sendo r^X e r^Y vectores coluna cujas componentes indicam o número de colunas não nulas das matrizes X e Y, respectivamente, que pertencem aos subespaços de dimensão um de F_q^k, concluí-se que X e Y têm o mesmo número de colunas não nulas e, por consequência, o mesmo número de colunas nulas. Como, para todo $i = 1, \ldots, \mu(k)$, $r_i^X = r_i^Y$, resulta que a matriz X e a matriz Y têm exactamente o mesmo número de colunas pertencentes a cada um dos subespaços L_i. Logo, essas colunas ou são iguais ou são múltiplos escalares não nulos. Finalmente, a definição de r^X e de r^Y não determina a ordem das colunas de X e Y e, portanto, as colunas de X ou são iguais ou são permutações das de Y. Então, $Y = X\Lambda$ com $\Lambda = DP$, em que D é uma matriz diagonal $n \times n$ que especifica a multiplicação por escalar não nulo e P uma matriz de dimensão $n \times n$ que define a permutação de colunas. $\square$

Estes resultados provam o teorema seguinte, conhecido por teorema de MacWilliams para a equivalência de códigos.

Teorema 5.2.11 (Teorema de MacWilliams para a equivalência de códigos) *Sejam C e D dois (n,k)-códigos lineares sobre um corpo F e $\varphi : C \to D$ um isomorfismo que preserva os pesos. Então, existe uma transformação monomial $\Phi : F^n \to F^n$ tal que $\Phi|_C = \varphi$, isto é, para todo $u \in C$, $\Phi(u) = \varphi(u)$.*

Exemplo 5.2.12 *Sejam X e Y, respectivamente, as matrizes geradoras dos $(3,2)-$códigos lineares C e D sobre F_3*

$$X = \begin{pmatrix} 1 & 0 & 2 \\ 2 & 1 & 1 \end{pmatrix} \quad ; \quad Y = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 2 & 1 \end{pmatrix}$$

F_3^2 tem $3^2 = 9$ elementos e $\mu(2) = \frac{3^2-1}{3-1} = 4$ subespaços de dimensão um

$$L_1 =< 10 > \; ; \; L_2 =< 01 > \; ; \; L_3 =< 11 > \; ; \; L_4 =< 12 >$$

O vector coluna $r^X = (0,1,0,2)^T$ é igual ao vector coluna $r^Y = (0,1,0,2)^T$. A matriz Y têm exactamente o mesmo número de colunas, pertencentes a cada um dos subespaços L_i, que a matriz X. Essas colunas ou são iguais ou são múltiplos escalares não nulos das colunas de X, eventualmente numa outra ordem. Verifica-se que, $Y = X\Lambda$ com

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

A transformação monomial Φ definida por

$$\begin{aligned} \Phi : F_3^3 &\to F_3^3 \\ (x,y,z) &\mapsto (2y,x,z) \end{aligned}$$

é tal que $\Phi(C) = D$ e portanto os códigos lineares C e D são equivalentes.

A partir do vector coluna Tr^X de um $(n,k)-$código linear C sobre um corpo F_p, é possível obter a distribuição de pesos das palavras do código e construir um código que verifique a referida distribuição de pesos.

Na verdade, para $i \in \{1,\ldots,n\}$, considerando A_i o número de palavras do código com peso i, verifica-se que

$$A_i = \left|\left\{j \in \{1,\ldots,\mu(k)\} : (Tr^X)_j = i\right\}\right| \times (q-1)$$

sendo, naturalmente, $A_0 = 1$.

Exemplo 5.2.13 *Seja C o código linear-$(3,2)$ sobre o corpo F_3 com $Tr^X = (3,2,2,2)^T$. Então a distribuição de pesos das 9 palavras de C é*

$$\begin{aligned}
A_0 &= 1 \\
A_1 &= \left|\left\{j \in \{1,\ldots,4\} : (Tr^X)_j = 1\right\}\right| \times (3-1) = 0 \times 2 = 0 \\
A_2 &= \left|\left\{j \in \{1,\ldots,4\} : (Tr^X)_j = 2\right\}\right| \times (3-1) = 3 \times 2 = 6 \\
A_3 &= \left|\left\{j \in \{1,\ldots,4\} : (Tr^X)_j = 3\right\}\right| \times (3-1) = 1 \times 2 = 2
\end{aligned}$$

Considere-se os subespaços de dimensão um de F_3^2

$$L_1 =< 10 > \ ; \ L_2 =< 01 > \ ; \ L_3 =< 11 > \ ; \ L_4 =< 12 >$$

e por conseguinte a matriz T

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

Então

$$r^X = T^{-1}(Tr^X) = \begin{pmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{1}{3} & \frac{1}{3} \\ -\frac{2}{3} & \frac{1}{3} & \frac{1}{3} & \frac{1}{3} \\ \frac{1}{3} & \frac{1}{3} & \frac{1}{3} & -\frac{2}{3} \\ \frac{1}{3} & \frac{1}{3} & -\frac{2}{3} & \frac{1}{3} \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Logo a matriz X geradora do código C ou de um código equivalente a C tem três colunas não nulas sendo cada uma delas um múltiplo escalar dos geradores de L_1, L_3 e L_4. A matriz geradora de C pode ser

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

sendo C o código definido por

$$C = \{000, 012, 021, 111, 120, 102, 222, 201, 210\}$$

5.3 Conclusão

Com esta tese pretendeu-se mostrar a importância da distribuição de pesos das palavras de um código e das isometrias no desenvolvimento dos códigos, em especial dos códigos lineares. As noções de distância entre palavras e peso de uma palavra permitem determinar a capacidade de detecção e correcção de erros e, portanto, o conhecimento da distribuição dos pesos de um código revela-se particularmente útil para conhecer a eficiência de um código relativamente a esses dois importantes aspectos. As isometrias permitem verificar a equivalência de códigos, ajudando a determinar em que circunstâncias se mantêm os principais parâmetros. Assim, as conclusões a que chegaram Ioana Constantinescu e Florence Jessie MacWilliams, designadamente nos três resultados que constituiram o objecto fundamental desta tese, revelaram-se contributos importantes para o desenvolvimento da Teoria de Códigos.

Apêndice A

A.1 Corpos Finitos

Definição A.1.1 *Seja F um conjunto não vazio com duas operações binárias, uma operação de adição $(+)$ e uma operação de multiplicação $(\times)$. Uma estrutura $(F, +, \times)$ diz-se um* ***anel comutativo*** *se para todo $u, v, w \in F$:*

1. *$(F, +, 0)$ é um grupo abeliano, isto é,*
   - *(a) $u + v = v + u$*
   - *(b) $(u + v) + w = u + (v + w)$*
   - *(c) existe um elemento $0 \in F$ tal que $u + 0 = u$*
   - *(d) existe um elemento $(-u) \in F$ tal que $u + (-u) = 0$*
2. *$(F, \times)$ é um semigrupo abeliano*
3. *$u \times (v + w) = u \times v + u \times w$*

Uma estrutura $(F, +, \times)$ diz-se um ***corpo*** *se é um anel comutativo e $(F \setminus \{0\}, \times, 1)$ é um grupo abeliano.*

Definição A.1.2 *Sejam a, b e $m > 1$ números inteiros. Diz-se que a é congruente com b para o módulo m e escreve-se $a \equiv b \pmod m$ se m divide $a - b$.*
Denota-se por $x \pmod m$ o resto da divisão de x por m.

Teorema A.1.3 *Sendo p um número primo, o conjunto $F_p = \{0, 1, \ldots, p-1\}$ munido das operações $a + b \ (mod\ p)$ e $a \times b \ (mod\ p)$, para $a, b \in F_p$ é um corpo.*

A.2 Espaços Vectoriais

Definição A.2.1 *Seja F um corpo e V um conjunto não-vazio com operações de adição e multiplicação por escalar que determinam para quaisquer $u, v \in V$ uma soma $u + v \in V$ e para quaisquer $u \in V$, $\lambda \in F$ um produto $\lambda u \in V$.*
O conjunto V chama-se um ***espaço vectorial sobre o corpo*** *F se $(V, +, \overline{0})$ é um grupo abeliano e para quaisquer $u, v, w \in V$ e $\lambda, \mu \in F$*

1. $\lambda(u + v) = \lambda u + \lambda v$
2. $(\lambda\mu)u = \lambda(\mu u)$
3. $(\lambda + \mu)u = \lambda u + \mu u$
4. $1u = u$

Os elementos de V dizem-se vectores e os de F dizem-se escalares.

$\overline{0}$ diz-se o vector nulo.

O conjunto F^n com as operações adição de vectores e multiplicação por escalar definidas, para quaisquer $(u_1, \ldots, u_n)$,$(v_1, \ldots, v_n) \in F^n$ e $\lambda \in F$, respectivamente por,

$$(u_1, \ldots, u_n) + (v_1, \ldots, v_n) = ((u_1 + v_1), \ldots, (u_n + v_n))$$

e

$$\lambda(u_1, \ldots, u_n) = (\lambda u_1, \ldots, \lambda u_n)$$

é um espaço vectorial sobre o corpo F.

Teorema A.2.2 *Seja W um subconjunto não vazio de um espaço vectorial V sobre um corpo F. W diz-se um* ***subespaço vectorial*** *de V se for*

1. *fechado para a adição de vectores, isto é, se* $u, v \in W$ *então* $u + v \in W$

2. *fechado para a multiplicação por escalar, isto é, se* $u \in W$ *e* $\lambda \in F$ *então* $\lambda u \in W$

Definição A.2.3 *Seja* V *um espaço vectorial sobre um corpo* F *e sejam* $v_1, v_2, \ldots, v_k$ *vectores em* V*. O vector* v *diz-se* ***combinação linear*** *de* $v_1, v_2, \ldots, v_k$ *se*

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k \ \ , com \ \ \lambda_1, \lambda_2, \ldots, \lambda_k \in F$$

Definição A.2.4 *Seja* V *um espaço vectorial sobre um corpo* F*. Os vectores* $v_1, v_2, \ldots, v_k$ *dizem-se* ***linearmente dependentes*** *se existem escalares* $\lambda_1, \lambda_2, \ldots, \lambda_k \in F$ *não todos nulos tais que* $\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k = \overline{0}$*.*

Definição A.2.5 *Seja* V *um espaço vectorial sobre um corpo* F*. Os vectores* $v_1, v_2, \ldots, v_k$ *dizem-se* ***linearmente independentes*** *se*

$$\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_k v_k = \overline{0} \ \ \Rightarrow \ \ \lambda_1 = 0, \lambda_2 = 0, \ldots, \lambda_k = 0$$

Definição A.2.6 *Seja* S *um subconjunto não-vazio do espaço vectorial* V *sobre um corpo* F*. Chama-se* ***subespaço gerado*** *por* S *ao conjunto de todas as combinações lineares dos vectores de* S*.*

Definição A.2.7 *Seja* V *um espaço vectorial sobre um corpo* F*. Diz-se que o espaço vectorial tem* ***dimensão*** k *e escreve-se* $dim(V) = k$ *se existem, em* V*,* k *vectores,* $v_1, v_2, \ldots, v_k$*, linearmente independentes que geram* V*. O conjunto* $\{v_1, v_2, \ldots, v_k\}$ *diz-se uma* ***base*** *de* V*. O espaço vectorial* $\left\{\overline{0}\right\}$ *tem dimensão zero.*

Teorema A.2.8 *Todas as bases de um espaço vectorial de dimensão finita,* V*, têm o mesmo número de elementos.*

A.3 Produto Interno

Definição A.3.1 *Sejam $u = (u_1, \ldots, u_n)$, $v = (v_1, \ldots, v_n)$ vectores de um espaço vectorial F^n sobre um corpo F. Chama-se* ***produto interno (ou produto escalar)*** *de u por v e escreve-se $u.v$, ao número dado por*

$$u.v = u_1v_1 + \ldots + u_nv_n$$

Definição A.3.2 *Dois* ***vectores*** *$u, v \in F^n$ dizem-se* ***ortogonais*** *se $u.v = 0$.*

Teorema A.3.3 *Seja F^n espaço vectorial sobre um corpo F. Para todo $u, v, w \in F^n$ e $\lambda, \mu \in F$ verifica-se*

1. $u.v = v.u$
2. $(\lambda u + \mu v).w = \lambda(u.w) + \mu(v.w)$

A.4 Aplicações Lineares

Definição A.4.1 *Sejam U e V dois espaços vectoriais sobre o mesmo corpo F. Chama-se* ***transformação linear*** *a uma função $\varphi : U \to V$ que satisfaça*

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$ *para quaisquer* $a, b \in U$
2. $\varphi(\lambda a) = \lambda\varphi(a)$ *para qualquer* $a \in U$ *e* $\lambda \in F$

Definição A.4.2 *Sejam U e V dois espaços vectoriais sobre o mesmo corpo F. Seja $\varphi : U \to V$ uma transformação linear.*
Chama-se ***núcleo*** *de φ e escreve-se $Ker\ \varphi$ ao conjunto*

$$Ker\,\varphi = \{u \in U : \varphi(u) = 0\}$$

Chama-se ***imagem*** *de φ e escreve-se $Im\ \varphi$ ao conjunto*

$$Im\ \varphi = \{v \in V : \varphi(u) = v \ \text{ para algum } \ u \in U\}$$

Teorema A.4.3 *Sejam U e V dois espaços vectoriais sobre um corpo F e $dim(U) = n$. Seja $\varphi : U \to V$ uma transformação linear. Então*

$$dim(Ker\ \varphi) + dim(Im\ \varphi) = n$$

Teorema A.4.4 *Uma transformação linear é injectiva se e só se $Ker\ \varphi = \{\overline{0}\}$*

A.5 Matrizes

Teorema A.5.1 *Qualquer matriz A, $n \times m$, sobre um corpo F está associada a uma transformação linear $\varphi : F^n \to F^m$ definida por $u \to uA$.*

Definição A.5.2 *Chama-se **característica de uma matriz** G e escreve-se $carG$, ao número máximo de linhas (ou de colunas) linearmente independentes da matriz G.*

A.6 Raízes Primitivas em $\mathbb{C}$

Definição A.6.1 *Em $\mathbb{C}$, conjunto dos números complexos, a q-ésima raíz da unidade, ζ, diz-se uma **raíz primitiva índice q da unidade**, se e só se $\zeta^q = 1$ e para $0 < i < q$, $\zeta^i \neq 1$, com $q \in \mathbb{N}$.*

Proposição A.6.2 *Em $\mathbb{C}$, a equação $\zeta^q - 1 = 0$, com $q \in \mathbb{N}$, tem pelo menos uma raíz primitiva, $\zeta = cis\ \frac{2\pi}{q}$.*

Bibliografia

[1] K. Bogart, D. Goldberg, J. Gordon, *An Elementary Proof of The MacWilliams Theorem on Equivalence of Codes*, Information and Control, Vol.37, pp. 19-22 (1978).

[2] A. Hefez, M.L.T. Villela, *Códigos Correctores de Erros*, IMPA (2002).

[3] R. Hill, *A First Course in Coding Theory*, Oxford University Press (2003).

[4] W.C. Huffman, V. Pless, *Fundamentals of Error-Correcting Codes*, Cambridge University Press (2003).

[5] S. Ling, C. Xing, *Coding Theory-A First Course*, Cambridge University Press (2004).

[6] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error Correcting Codes*, North Holland (1993).

[7] F.M. Reza, *An Introduction to Information Theory*, Dove Publications (2003).

[8] S. Roman, *Coding and Information Theory*, Springer-Verlag (1992).

[9] C. Shannon, A Mathematical Theory of Communication, Bell System Technical Journal, Vol.27, pp. 379-423 e 623-656 (1948).