Notas de
Combinatória e Teoria de Códigos
(2011, revistas e aumentadas em 2014)

Joana Ventura

ÍNDICE

CAPÍTULO 1. Introdução 1
1. Primeiros exemplos e definições 1
2. Canal de transmissão 3
3. Descodificação 4
4. Correcção e detecção de erros 6
Exercícios 8

CAPÍTULO 2. O Problema Principal da Teoria de Códigos 11
1. Enunciado do problema e alguns resultados 11
2. Estimativas 15
Exercícios 18

CAPÍTULO 3. Corpos Finitos e Espaços Vectoriais 21
1. Corpos finitos 21
2. Espaços vectoriais sobre corpos finitos 28
Exercícios 33

CAPÍTULO 4. Códigos Lineares 35
1. Definição, pârametros e peso mínimo 35
2. Matriz geradora e matriz de paridade 36
3. Equivalência linear 39
4. Codificação e descodificação 40
Exercícios 48

CAPÍTULO 5. Construção de Códigos 51
1. Extensão 51
2. Pontuação 52
3. Expansão 52
4. Eliminação ou subcódigos 53
5. Contracção 54
6. Soma directa 55
7. Construção de Plotkin 56
Exercícios 56

CAPÍTULO 6. Exemplos de Códigos Lineares 59

1. Códigos de Hamming 59
2. Códigos de Reed-Muller 63
3. Minorante de Gilbert-Varshamov linear 65
4. Códigos de Golay 66
5. Códigos de distância máxima de separação ou MDS 67
Exercícios 68

CAPÍTULO 7. Códigos Perfeitos e Sistemas de Steiner 71
Exercícios 74

CAPÍTULO 8. Códigos Cíclicos 77
1. Introdução 77
2. Polinómio gerador 78
3. Matriz geradora e matriz de paridade 81
4. Codificação e descodificação 85
5. Erros acumulados 89
6. Entrelaçamento 91
7. Concatenação 92
Exercícios 95

CAPÍTULO 9. Códigos Reed-Solomon 99
1. Distância mínima 100
2. Extensão de códigos Reed-Solomon 102
3. Concatenação de códigos Reed-Solomon 103
Exercícios 105

APÊNDICE A. 107
1. Princípio de Inclusão-Exclusão 107
2. Funções geradoras e relações de recorrência 111
Exercícios 114

APÊNDICE B. 117
1. Polinómios mínimos 117
2. Factorização de $t^n - 1$ 120
Exercícios 122

BIBLIOGRAFIA 123

Introdução

O objectivo destas notas é agrupar num único texto toda a matéria dada na cadeira de Combinatória e Teoria de Códigos. O livro *A Fisrt Course in Coding Theory* de R. Hill [**2**] continua a ser uma referência para esta cadeira, embora não cubra todo o programa. A bibliografia minimal apresentada no final destas notas permite cobrir o programa completo (e muito mais!) assim como rever algumas noções de Álgebra necessárias, que os alunos já terão aprendido.

1. Primeiros exemplos e definições

Consideremos a seguinte situação: fulano X está perdido no meio de uma floresta mas está em contacto com fulano Y que consegue saber onde está X e qual o caminho que este deve tomar. A mensagem que Y gostaria de transmitir a X consiste numa sequência dos símbolos N (Norte), S (Sul), E (Este) e W (Oeste), no entanto o *canal de transmissão* entre Y e X apenas permite usar dois símbolos. Trata-se portanto de *codificar* os quatro pontos cardeais através de um *código binário*. Podemos escolher vários tipos de código.

Exemplo 1.1. Seja $C_1 = \{0, 1, 00, 11\}$ e consideremos a correspondência

$$N \mapsto 0 \qquad S \mapsto 1 \qquad E \mapsto 00 \qquad W \mapsto 11 \tag{1.1}$$

O conjunto C_1 diz-se um *código* binário (em dois símbolos) e a aplicação entre $\{N, S, E, W\}$ e C_1 definida por (1.1) diz-se uma *função de codificação*. Neste exemplo o código não é *unicamente decifrável* pois a mensagem 00 tanto pode significar NN ou E.

Exemplo 1.2. Consideremos agora o código $C_2 = \{0, 01, 011, 0111\}$ e a correspondência

$$N \mapsto 0 \qquad S \mapsto 01 \qquad E \mapsto 011 \qquad W \mapsto 0111 \tag{1.2}$$

Neste caso o código é unicamente decifrável, mas não é *instantâneo* pois é preciso esperar pela próxima palavra, ou pelo fim da mensagem, para se conseguir interpretar cada palavra.

Exemplo 1.3. Consideremos ainda um terceiro código $C_3 = \{0, 10, 110, 1110\}$ e a correspondência

$$N \mapsto 0 \qquad S \mapsto 10 \qquad E \mapsto 110 \qquad W \mapsto 1110 \tag{1.3}$$

Neste caso o código é unicamente decifrável e instantâneo – uma palavra acaba quando se recebe o símbolo 0.

Exemplo 1.4. Consideremos ainda um quarto código $C_4 = \{00, 01, 10, 11\}$ e a correspondência

$$N \mapsto 00 \qquad S \mapsto 01 \qquad E \mapsto 10 \qquad W \mapsto 11 \tag{1.4}$$

Trata-se de um código unicamente decifrável e instantâneo, pois todas as palavras têm o mesmo comprimento. Neste caso C_4 diz-se um *código uniforme*.

Exemplo 1.5. Para finalizar estes exemplos, consideremos o código $C_5 = \{000, 011, 101, 110\}$ e a correspondência

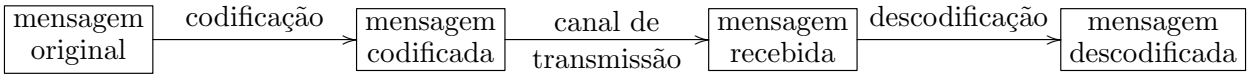
$$N \mapsto 000 \qquad S \mapsto 011 \qquad E \mapsto 101 \qquad W \mapsto 110 \tag{1.5}$$

Tal como no exemplo anterior, C_5 é um código uniforme.

Nesta cadeira iremos considerar apenas códigos uniformes, como os dos Exemplos 1.4 e 1.5. Entre estes, qual o melhor código, C_4 ou C_5? A resposta depende naturalmente do sentido que se der a "melhor". Mas, mesmo sem especificar esse sentido, já podemos comparar C_4 e C_5 nos seguintes aspectos:

- C_4 é um código de comprimento menor do que C_5, portanto é mais rápido transmitir uma mensagem usando C_4.
- C_4 é o conjunto de todas as palavras binárias de comprimento 2 (i.e., $C_4 = (\mathbb{Z}_2)^2$), portanto qualquer palavra recebida é uma palavra de código e, por isso, C_4 não permite detectar erros que ocorram durante a transmissão. Por outro lado, $C_5 \neq (\mathbb{Z}_2)^3$ e portanto C_5 vai permitir detectar alguns erros. Mas será possível corrigi-los?

A situação geral considerada em Teoria de Códigos pode ser esquematizada na seguinte figura:



As mensagens codificada e recebida são ambas formadas por sequências de símbolos do mesmo alfabeto. O canal de transmissão poderá ter ruído, de modo que a mensagem recebida poderá conter erros ou símbolos apagados e não será igual à mensagem enviada. O objectivo é estudar códigos tendo em conta certas características como a rapidez de transmissão, facilidade e eficiência de codificar e descodificar, capacidades detectoras e correctoras de erros, etc.

Comecemos então por definir os termos já usados na discussão anterior.

Definição 1.6.
- Um *alfabeto* é um conjunto finito de símbolos $\mathcal{A}_q = \{a_1, \ldots, a_q\}$.
- Uma *palavra* é uma sequência finita de elementos do alfabeto $\mathcal{A}_q$.
- Um *código q-ário* é um conjunto finito, não vazio, de palavras sobre um alfabeto de $q \geq 1$ elementos.
- Se todas as palavras do código C têm o mesmo comprimento $n \geq 1$, i.e. se $C \subset \mathcal{A}_q^n$, então C diz-se um *código uniforme*.

Notação 1.7. Um código $(n, M)_q$ significa um código uniforme q-ário com M palavras de comprimento n. Também usamos (n, M) para denotar o mesmo tipo de códigos quando o número de símbolos q está subentendido.

Definição 1.8. Um *esquema de codificação* é um par (C, f) onde

- C é um código,
- $f : \mathcal{S} \to C$ é uma aplicação injectiva, chamada *função de codificação*,
- $\mathcal{S}$ diz-se o *alfabeto fonte*.

O alfabeto fonte pode ou não ser o mesmo do código C. Em todos os exemplos anteriores, o conjunto $\{N, S, E, W\}$ é o alfabeto fonte e o alfabeto do código é $\{0, 1\}$. As correspondências (1.1) a (1.5) definem funções de codificação.

Um alfabeto pode ser qualquer conjunto finito de símbolos à nossa escolha. O conjunto das letras $\{a, b, c, \ldots, x, y, z\}$ é naturalmente um alfabeto, e o conjunto de todas as palavras portuguesas formam um código que não é uniforme.

Os anéis $\mathbb{Z}_m = \mathbb{Z}/\langle m \rangle$ (com $m \geq 2$ um número inteiro) são também alfabetos. No caso particular de $\mathbb{Z}_2 = \{0, 1\}$, o código diz-se binário, e se o alfabeto é $\mathbb{Z}_3 = \{0, 1, 2\}$, o código diz-se ternário. Note-se que $\mathbb{Z}_2$ e $\mathbb{Z}_3$ têm uma estrutura de corpo. Os códigos lineares (Capítulo 4) são uma classe de códigos cujos alfabetos são corpos finitos (estes serão definidos/revistos no Capítulo 3).

A partir de agora, iremos condiderar apenas códigos uniformes, assim "código" significará sempre "código uniforme".

Exemplo 1.9. Fixemos um alfabeto $\mathcal{A}_q$ de q elementos, por exemplo, $\mathcal{A}_q = \mathbb{Z}_q$. O *código de repetição q-ário de comprimento n* é o conjunto formado por q palavras em que os símbolos de cada palavra são todos iguais. Concretamente, $\{0000, 1111\}$ é o código de repetição binário de comprimento 4 e tem parâmetros $(4, 2)$, $\{000, 111, 222, 333, 444\}$ é o código de repetição quinquenário de comprimento 3 e tem parâmetros $(3, 5)$, etc. Em geral, os parâmetros (ver Notação 1.7) de um código de repetição q-ário de comprimento n são $(n, q)_q$.

Exemplo 1.10. Os parâmetros de um código não o definem univocamente. Seja $C_1 = \{0000, 1111\}$ o código de repetição binário e seja $C_2 = \{1010, 0101\}$. Estes dois códigos têm parâmetros $(4, 2)$, mas $C_1 \neq C_2$.

2. Canal de transmissão

Definição 1.11. Um *canal de transmissão* consiste num alfabeto $\mathcal{A}_q = \{a_1, a_2, \ldots, a_q\}$ e nas probabilidades de canal $P(\text{recebido } a_j \mid \text{enviado } a_i)$, para $i, j \in \{1, \ldots, q\}$, verificando a seguinte condição

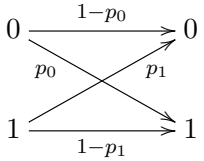
$$\sum_{j=1}^{q} P(\text{recebido } a_j \mid \text{enviado } a_i) = 1 \quad \text{, para cada } i \text{ fixo.}$$

Para simplificar a notação, por vezes escrevemos $P(a_j|a_i)$ para denotar a probabilidade condicionada $P(\text{recebido } a_j \mid \text{enviado } a_i)$, e indicamos as probabilidades do canal através de um grafo onde cada seta representa uma das probabilidades condicionadas da definição

$$a_i \xrightarrow{P(a_j|a_i)} a_j \quad .$$

Vamos agora considerar vários exemplos.

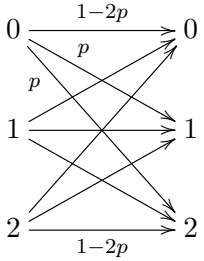
Um *canal de transmissão binário* ($q = 2$) é definido pelos dois valores $p_0 = P(1|0)$ (a probabilidade de troca do símbolo 0) e $p_1 = P(0|1)$ (a probabilidade de troca do símbolo 1), e pode ser representado pelo seguinte esquema



onde o número em cada seta é a probabilidade do símbolo da ponta da seta ser recebido dado que o símbolo da cauda da seta foi enviado. Portanto, neste exemplo, $P(0|0) = 1 - p_0$, $P(1|0) = p_0$, $P(0|1) = p_1$ e $P(1|1) = 1 - p_1$.

Se $p_0 = p_1$, obtém-se um *canal binário simétrico*, um caso particular que iremos usar bastante no resto destas notas. Neste caso, o número $p := p_0 = p_1$ diz-se a *probabilidade de troca de símbolos*.

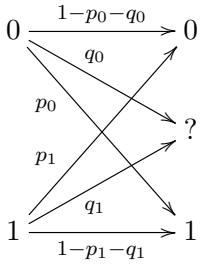
Para $q = 3$, temos o caso particular de um *canal símetrico ternário* com probabilidade de troca $p \in]0, 1[$ definido pelo esquema



onde as setas diagonais têm todas probabilidade p e, portanto, as setas horizontais têm probabilidade $1 - 2p$ (a figura acima está incompleta), ou seja, $P(a_j|a_i) = p$ se $j \neq i$, e $P(a_i|a_i) = 1 - 2p$.

Observação 1.12. Uma vez que, para cada símbolo $a_i \in \mathcal{A}_q$ enviado, se tem $\sum_{j=1}^{q} P(a_j|a_i) = 1$, basta definir as probabilidades $P(a_j|a_i)$ para $i \neq j$. Ou seja, na representação esquemática, basta definir as probabilidades das setas diagonais.

Outro exemplo interessante é o *canal binário de apagamento* definido por



i.e., para além de cada símbolo do alfabeto $\mathcal{A}_2 = \{0, 1\}$ poder ser trocado durante a transmissão, pode ainda ser apagado, o que corresponde a ser enviado para o novo símbolo '?'. É equivalente a usar o alfabeto $\{0, 1, ?\}$ em que o símbolo de apagamento '?' não é usado em nenhuma palavra de código.

Observação 1.13. Nestas notas assumimos sempre que o canal de transmissão é *sem memória*. Por definição, isto quer dizer que a transmissão de cada símbolo é independente das transmissões anteriores, de modo a se verificar a seguinte igualdade

$$P(\text{recebido } y \mid \text{enviado } x) = \prod_{i=1}^{n} P(y_i|x_i) \ , \tag{1.6}$$

onde $x = (x_1, x_2, \ldots, x_n) \in C$ é uma palavra de código e $y = (y_1, y_2, \ldots, y_n) \in \mathcal{A}_q^n$ é uma palavra arbitrária.

3. Descodificação

Fixemos um código q-ário C de comprimento n, isto é, $C \subset \mathcal{A}_q^n$ onde $\mathcal{A}_q$ é um alfabeto com q símbolos.

Definição 1.14. Um *método de descodificação* é uma correspondência entre palavras de $\mathcal{A}_q^n$ (vistas como as palavras recebidas) e palavras do código C. Caso esta correspondência não esteja definida em todas as palavras de $\mathcal{A}_q^n$, a descodificação diz-se *incompleta*.

Nesta secção vamos considerar dois métodos de descodificação.

Definição 1.15. *Descodificação por máxima verosimilhança:* recebido $y \in \mathcal{A}_q^n$, procurar $x' \in C$ tal que

$$P(\text{recebido } y \mid \text{enviado } x') = \max_{x \in C} \{P(\text{recebido } y \mid \text{enviado } x)\} \ .$$

Como C é finito, o conjunto $\{P(\text{recebido } y \,|\, \text{enviado } x) \ : \ x \in C\}$ também é finito e, portanto, o máximo na definição anterior existe sempre, embora possa não ser único.

Exemplo 1.16. Seja $C = \{110, 111\}$ e considere-se um canal binário simétrico com probabilidade de troca $p = 0,03$. Suponhamos que recebemos a palavra 011. Como $011 \notin C$, sabemos que ocorreram erros durante a transmissão. Vamos usar o método de descodificação por máxima verosimilhança.

$$\begin{aligned} P(011 \text{ recebida} \,|\, 110 \text{ enviada}) &= P(0|\,1)P(1|\,1)P(1|\,0) \\ &= p(1-p)p = (0,03)^2 \times 0,97 = 0,000873 \\ P(011 \text{ recebida} \,|\, 111 \text{ enviada}) &= P(0|\,1)P(1|\,0)^2 \\ &= p(1-p)^2 = 0,03 \times (0,97)^2 = 0,028227 \end{aligned}$$

Como a última probabilidade é maior, concluimos que 111 é a palavra de código que provavelmente foi enviada, portanto descodificamos 011 por 111. Note-se que, no primeiro passo no cálculo de cada uma das probabilidades, usou-se a igualdade (1.6).

Exemplo 1.17. Consideremos a mesma situação do exemplo anterior, mudando apenas o código para $C = \{010, 111\}$. Continuamos a ter um canal simétrico binário e a mesma palavra recebida 011.

$$\begin{aligned} P(011 \text{ recebida} \,|\, 010 \text{ enviada}) &= P(0|\,0)P(1|\,1)P(1|\,0) \\ &= (1-p)^2 p \\ P(011 \text{ recebida} \,|\, 111 \text{ enviada}) &= P(0|\,1)P(1|\,1)^2 \\ &= p(1-p)^2 \end{aligned}$$

Como as duas probabilidades são iguais (e nem dependem do valor de p), o método de descodificação por máxima verosimilhança não nos permite tirar conclusões acerca de qual a palavra enviada com maior probabilidade. Temos então duas alternativas. Ou optamos por uma descodificação incompleta, o que quer dizer que não descoficamos a palavra recebida 011; ou escolhemos uma das palavra de código para descodificar 011 sempre que esta seja recebida. Neste último caso, se decidirmos descodificar 011 por 010, por exemplo, da próxima vez que 011 for recebida, teremos que descodificá-la novamente pela mesma palavra $010 \in C$.

Há esquemas de decisão ou descodificação que não envolvem probabilidades, mas usam uma noção de proximidade.

Definição 1.18. Sejam $x, y \in \mathcal{A}_q^n$. Define-se a *distância de Hamming* entre as palavras x e y por

$$\mathrm{d}(x, y) = \#\{i \,:\, x_i \neq y_i\} \ .$$

Ou seja, $\mathrm{d}(x, y)$ é o número de coordenadas em que x e y diferem, ou ainda, $\mathrm{d}(x, y)$ é o número mínimo de trocas de símbolos necessárias para obter y a partir de x. Por exemplo, $\mathrm{d}(00, 01) = 1$ e $\mathrm{d}(111000, 112012) = 3$.

Exemplo 1.19. Considere-se o alfabeto $\mathcal{A}_4 = \{1, 2, 3, 4\}$ e sejam $x = 1234$, $y = 2341$ e $z = 1243$. Então

$$\mathrm{d}(x, y) = 4 \ , \qquad \mathrm{d}(x, z) = 2 \qquad \text{e} \qquad \mathrm{d}(y, z) = 3 \ .$$

Definição 1.20. Seja C um código contendo pelo menos duas palavras. Define-se a *distância mínima de* C por

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

Este parâmetro $\mathrm{d}(C)$ vai ter bastante importância quando discutirmos as capacidades de detecção e correcção de erros de um código C.

Notação 1.21. Se C é um código q-ário com M palavras de comprimento n e distância mínima $\mathrm{d}(C) = d$, dizemos que C é um código $(n, M, d)_q$, ou (n, M, d). Os números n, M e d dizem-se os *parâmetros* de C.

Exemplo 1.22. Consideremos o código $C_5 = \{000, 011, 101, 110\}$ definido no Exemplo 1.5. A distância entre $000 \in C_5$ e qualquer outra palavra (de comprimento 3, claro) é o número de símbolos não nulos nessa palavra, portanto $\mathrm{d}(000, x) = 2$ para qualquer $x \in C \setminus \{000\}$. Calculando a distância entre os restantes pares de palavras de código:

$$\mathrm{d}(011, 101) = 2 \ , \qquad \mathrm{d}(011, 110) = 2 \ , \qquad \mathrm{d}(101, 110) = 2 \ ,$$

conclui-se que $\mathrm{d}(C_5) = 2$ e portanto $(3, 4, 2)_2$ são os parâmetros deste código.

Exemplo 1.23. A distância mímina de um código de repetição q-ário C (definido no Exemplo 1.9) é o comprimento n das palavras, portanto $(n, q, n)_q$ são os parâmetros de C.

Proposição 1.24. *A distância de Hamming é uma métrica, i.e., verifica as seguintes propriedades:*

(i) $\mathrm{d}(x,y) \geq 0 \quad \forall\, x,y \in \mathcal{A}_q^n$,
(ii) $\mathrm{d}(x,y) = 0 \Leftrightarrow x = y$,
(iii) simetria: $\mathrm{d}(x,y) = \mathrm{d}(y,x) \quad \forall\, x,y \in \mathcal{A}_q^n$,
(iv) desigualdade triangular: $\mathrm{d}(x,y) \leq \mathrm{d}(x,z) + \mathrm{d}(z,y) \quad \forall\, x,y,z \in \mathcal{A}_q^n$.

Estas propriedades são consequência directa da definição de distância de Hamming, por isso deixamos a sua demonstração como exercício.

Definição 1.25. *Descodificação por distância mínima:* recebida a palavra $y \in \mathcal{A}_q^n$, procurar $x' \in C$ tal que

$$\mathrm{d}(x',y) = \min\{\mathrm{d}(x,y) \,:\, x \in C\}\ ,$$

ou seja, descodificamos y pela palavra de código mais próxima.

Tal como no caso da descodificação por máxima verosimilhança, por C ser finito, o conjunto $\{\mathrm{d}(x,y) : x \in C\}$ também é finito e o mínimo na definição anterior existe sempre, embora possa não ser único.

Exemplo 1.26. Consideremos o código binário $C = \{0010, 0101, 1010, 1110\}$ e suponhamos que recebemos a palavra 0100. Como

$$\mathrm{d}(0100,0010) = 2\ , \qquad \mathrm{d}(0100,0101) = 1\ , \qquad \mathrm{d}(0100,1010) = 3\ , \qquad \mathrm{d}(0100,1110) = 3\ ,$$

usando o método de descodificação por distância mínima, descodificamos 0100 por 0101.

Exemplo 1.27. Seja $C = \{0000, 1111\}$ o código de repetição de comprimento 4 e consideremos um canal de transmissão binario simétrico com propabilidade de troca $p = \frac{1}{4}$. Pretende-se descodificar a palavra recebida $y = 0010$ pelo dois métodos definidos.

Descodificação por máxima verosimilhança: Temos de calcular as probabilidades condicionadas $P(\text{recebido } y \,|\, \text{enviado } x)$ para $x \in C$. Otém-se

$$\begin{aligned} P(\text{recebido } y \,|\, \text{enviado } 0000) &= (1-p)^3 p = \tfrac{3^3}{4^4} \quad \text{e} \\ P(\text{recebido } y \,|\, \text{enviado } 1111) &= p^3(1-p) = \tfrac{3}{4^4}\ , \end{aligned} \tag{1.7}$$

pois y difere de 0000 em apenas um símbolo e difere de 1111 em três. Como $\frac{3^3}{4^4} > \frac{3}{4^4}$, descodificamos y por 0000.

Descodificação por distância mínima: Temos de calcular as distâncias entre y e cada uma das palavras do código C. Obtêm-se

$$\mathrm{d}(y,0000) = 1 \qquad \text{e} \qquad \mathrm{d}(y,1111) = 3\ ,$$

portanto descodificamos y por 0000, a mesma que se obteve pelo outro método. Não se trata de uma coincidência uma vez que as probabilidades calculadas em (1.7) apenas dependem no número de coordenadas em que x e y diferem, i.e., da distância $\mathrm{d}(x,y)$.

Teorema 1.28. *Para um canal simétrico binário com probabilidade de troca $p < \frac{1}{2}$ os esquemas de descodificação por máxima verosimilhança e por distância mínima coincidem.*

4. Correcção e detecção de erros

Seja $C = \{000, 111\}$ o código de repetição binário de comprimento 3. Se usarmos a descodificação por distância mínima, cada palavra em $\mathcal{A}_2^3$ é descodificada de acordo com a seguinte tabela

recebido	descodificado por
000	000
100, 010, 001	000
011, 101, 110	111
111	111

Caso 1: Se 000 (ou 111) é a palavra enviada e ocorrem erros de transmissão em uma ou duas coordenadas, a palavra recebida y contém exactamente um ou dois símbolos 1. Embora não tenhamos

informação para corrigir o erro (admitindo que não conhecemos a palavra enviada), podemos ainda concluir que ocorreram erros pois y não pertence ao código. Dizemos que C *detecta até dois erros.*

Caso 2: Se a palavra enviada foi 000 e ocorreu um erro na transmissão de um dos símbolos, a palavra recebida foi uma das da segunda linha da tabela, portanto é descodificada correctamente por ela própria. Ou seja, o *erro foi corrigido.* Analogamente para o caso de ocorrer um erro numa das coordenadas de 111. Caso ocorram dois erros na transmissão de 000, a palavra recebida é descodificada incorrectamente por 111 (terceira linha da tabela). Dizemos que C *corrige um erro*, mas não corrige dois.

Definição 1.29. Seja C um código e sejam s e t números inteiros positivos.

- Diz-se que C *detecta s erros* se e só se, quando ocorrem s erros ou menos, a palavra obtida não pertence ao código C.
- Diz-se que C *corrige t erros* se e só se o método de descodificação por distância mínima corrige t, ou menos, erros.

Em particular, "corrigir" quer dizer que há unicidade de mínimo na definição de descodificação, i.e., está-se a usar um método de descodificação incompleta em que não se descodifica a palavra recebida em caso de "empate".

Teorema 1.30. *Seja C um código com distância mínima* $\mathrm{d}(C)$. *Então*

(a) C detecta s erros se e só se $\mathrm{d}(C) \geq s+1$;

(b) C corrige t erros se e só se $\mathrm{d}(C) \geq 2t+1$.

Dem. (a) Suponhamos que $\mathrm{d}(C) \geq s+1$. Seja $x \in C$ a palavra enviada e suponhamos que ocorrem no máximo s erros na transmissão e $y \neq x$ é a palavra recebida. Portanto $0 < d(x,y) \leq s$. Como $0 < \mathrm{d}(x,y) < \mathrm{d}(C)$, conclui-se que $y \notin C$ e os s erros são detectados.

Reciprocamente, se $\mathrm{d}(C) \leq s$, então existem palavras $x, y \in C$ tais que $\mathrm{d}(x,y) = \mathrm{d}(C) \leq s$. Logo é possível x ser a palavra enviada, ocorrerem $\mathrm{d}(C)$ erros e recebermos a palavra y. Como $y \in C$, estes erros não são detectados.

(b)($\Longleftarrow$) Suponhamos que $\mathrm{d}(C) \geq 2t+1$. Seja $x \in C$ a palavra enviada e suponhamos que ocorrem t erros na transmissão e $y \neq x$ é a palavra recebida. Portanto $0 < \mathrm{d}(x,y) \leq t$. Para qualquer $c \in C$, com $c \neq x$, temos

$$\mathrm{d}(x,c) \leq \mathrm{d}(x,y) + \mathrm{d}(y,c)$$

logo

$$\mathrm{d}(y,c) \geq \mathrm{d}(x,c) - \mathrm{d}(x,y) \geq \mathrm{d}(C) - t \geq 2t+1-t = t+1 > \mathrm{d}(x,y) \ ,$$

e assim, usando o método de descodificação por distância mínima, y é descodificada correctamente por x.

(b)($\Longrightarrow$) Seja C um código que corrige t erros e suponhamos que $\mathrm{d}(C) \leq 2t$. Então existem $x, x' \in C$ tais que $\mathrm{d}(x,x') = \mathrm{d}(C) \leq 2t$. Seja x a palavra enviada e seja y a palavra recebida com t erros, ou menos, durante a transmissão. Queremos ver que ou y é descodificada erradamente por x', ou existe outra palavra de código $z \in C$, $z \neq x$, tal que $\mathrm{d}(y,x) = \mathrm{d}(y,z)$ (i.e. não há unicidade de mínimo).

Se $\mathrm{d}(x,x') < t+1$, então podiamos ter $y = x'$ pois ocorreriam t erros no máximo, e estes erros nem seriam detectados porque $x' \in C$. Isto contradiz a hipótese de C corrigir t erros, portanto podemos assumir que $\mathrm{d}(x,x') \geq t+1$.

Sem perda de generalidade, podemos também assumir que x e x' diferem precisamente nas primeiras $d = \mathrm{d}(C)$ coordenadas, com $t+1 \leq d \leq 2t$. Seja

$$y = \underbrace{x'_1 \cdots x'_t}_{\text{como } x'} \underbrace{x_{t+1} \cdots x_d}_{\text{como } x} \underbrace{x_{d+1} \cdots x_n}_{\text{como } x \text{ e } x'} \ .$$

Então as três chavetas contêm t, $d-t$ e $n-d$ coordenadas, repectivamente, e

$$\mathrm{d}(y,x') = d - t \leq t = \mathrm{d}(y,x) \ .$$

Há dois casos a considerar. Ou $\mathrm{d}(y,x') < \mathrm{d}(y,x)$ e y é descodificada incorrectamente por x'. Ou $\mathrm{d}(y,x') = \mathrm{d}(y,x)$ e não podemos decidir entre x e x' na descodificação por distância mínima. □

Corolário 1.31. *Seja C um código de distância mínima $\mathrm{d}(C) = d$. Então C detecta precisamente $d-1$ erros, ou corrige precisamente $\left\lfloor \frac{d-1}{2} \right\rfloor$ erros.*

Uma vez que a distância de Hamming é uma métrica, podemos definir bolas em $\mathcal{A}_q^n$. A bola de centro x e raio t é o conjunto

$$B_t(x) = \{y \in \mathcal{A}_q^n \,:\, \mathrm{d}(y,x) \leq t\} \subset \mathcal{A}_q^n \ .$$

No Teorema 1.30 provámos que, se $\mathrm{d}(C) = 2t+1$, então quaisquer duas bolas de raio t e centro em palavras de código são disjuntas duas a duas. Assim, se soubermos que ocorrem no máximo t erros de transmissão e y é a palavra recebida, então existe um único $x \in C$ tal que $y \in B_t(x)$, nomeadamente, a palavra enviada.

Iremos voltar a usar esta noção de bola no Capítulo 2.

Exercícios

1.1. Na palavra binária

01111000000?001110000?00110011001010111000000000?01110

codificou-se uma data. O sistema utilizado consistiu em escrevê-la primeiro na forma de 6 dígitos decimais seguidos (por exemplo, 290296 quer dizer 29 de Fevereiro de 1996) e passar esse número para a base 2 (no exemplo acima 290296 transforma-se em 1000110110111111000) e em seguida codificar de acordo com a regra

$$\begin{aligned} \{0,1\}^2 &\longrightarrow \mathcal{C} \subset \{0,1\}^6 \\ 00 &\longmapsto 000000 \\ 01 &\longmapsto 001110 \\ 10 &\longmapsto 111000 \\ 11 &\longmapsto 110011 \end{aligned}$$

Na palavra recebida há 3 bits que não se conhecem (foram apagados) e possivelmente outros que estão trocados.

(a) Encontre os 3 bits apagados.
(b) Quantos bits e em que posições estão errados?
(c) De que data se trata?
(d) Repetir o problema trocando os bits das posições 15 e 16, começando a contar da esquerda. (Nota: "trocar um bit na posição i" quer dizer "subtituir um 1 por um 0, e vice-versa, na posição i".)

1.2. Considere o código binário $C = \{01101, 00011, 10110, 11000\}$. Usando descodificação por distância mínima, descodifique as seguintes palavras recebidas:
(a) 00000;
(b) 01111;
(c) 01101;
(d) 11001.

1.3. Considere um canal binário com probabilidades de troca de símbolos

$$P(\text{recebido } 1 \,|\, \text{enviado } 0) = 0,3 \qquad \text{e} \qquad P(\text{recebido } 0 \,|\, \text{enviado } 1) = 0,2 \ .$$

Se for usado o código binário $\{000, 101, 111\}$ para enviar uma mensagem através desse canal, descodifique, usando máxima verosimilhança, as palavras recebidas:
(a) 010;

(b) 011;
(c) 001.

1.4. Prove o Teorema 1.28, ou seja, prove que, para um canal de transmissão binário e simétrico, com probabilidade de troca $p < \frac{1}{2}$, os métodos de descodificação por distância mínima e por máxima verosimilhança coincidem.

1.5. Quais as capacidades de correcção e detecção *simultâneas* de erros de um código de distância mínima d? Enuncie um algoritmo de descodificação que permita corrigir t erros e detectar s erros, e justifique que esse algoritmo funciona.

1.6. O que se poderá fazer e dizer quanto às capacidades correctoras de erros de apagamento e de erros de troca e de apagamento simultaneamente de um código de distância mínima d? Enuncie um algoritmo de descodificação que permita corrigir t erros de troca e a erros de apagamento, e justifique que esse algoritmo funciona.

1.7. (Um Código de Hamming Binário) Codifica-se um vector mensagem de 4 componentes binárias $m = m_1m_2m_3m_4$, com $m_i \in \{0,1\}$, numa palavra de código com 7 componentes binárias $c = c_1c_2c_3c_4c_5c_6c_7$, com $c_j \in \{0,1\}$, definidas por

$$c_3 = m_1 \quad ; \qquad c_5 = m_2 \quad ; \qquad c_6 = m_3 \quad ; \qquad c_7 = m_4$$

e as restantes componentes escolhidas

$$\begin{aligned} &c_4 \text{ tal que } \alpha = c_4 + c_5 + c_6 + c_7 \text{ seja par,} \\ &c_2 \text{ tal que } \beta = c_2 + c_3 + c_6 + c_7 \text{ seja par,} \\ &c_1 \text{ tal que } \gamma = c_1 + c_3 + c_5 + c_7 \text{ seja par.} \end{aligned}$$

Verifique que com este esquema de codificação se constrói um código que permite corrigir um erro em qualquer posição.
Recebido um vector $x = x_1x_2x_3x_4x_5x_6x_7$, calculam-se

$$\left.\begin{aligned} \alpha &= x_4 + x_5 + x_6 + x_7 \\ \beta &= x_2 + x_3 + x_6 + x_7 \\ \gamma &= x_1 + x_3 + x_5 + x_7 \end{aligned}\right\} \mod 2 \ ;$$

$\alpha\beta\gamma$ representa em binário a componente j onde se deu o erro. Se $\alpha\beta\gamma = 000$ assume-se que não há erro.
Estude este exemplo com cuidado.

O Problema Principal da Teoria de Códigos

1. Enunciado do problema e alguns resultados

Definição 2.1. Seja C um código q-ário (n, M, d). Define-se *taxa de transmissão* de C por

$$R(C) = \frac{\log_q(M)}{n} \tag{2.1}$$

e define-se *taxa de correcção de erros*[1] por

$$\delta(C) = \frac{\lfloor \frac{d-1}{2} \rfloor}{n} \ .$$

Exemplo 2.2. Dois casos extremos.

(a) Para o código binário de repetição de comprimento n, que tem parâmetros $(n, 2, n)$,

$$R(C) = \frac{\log_2(2)}{n} = \frac{1}{n} \ .$$

Se $n = 2t + 1$, então o código corrige t erros (pelo Teorema 1.30), e

$$\delta(C) = \frac{t}{n} = \frac{t}{2t+1} \longrightarrow \frac{1}{2} \qquad \text{e} \qquad R(C) = \frac{1}{2t+1} \longrightarrow 0 \qquad \text{quando } t \longrightarrow \infty \ .$$

Por palavras, com n grande, C corrige "quase" metade dos erros, no entanto, a taxa de transmissão é muito baixa – C apenas contém duas plavaras!

(b) Com $C = \mathbb{Z}_2^n$, um código de parâmetros $(n, 2^n, 1)$,

$$R(C) = \frac{\log_2(2^n)}{n} = \frac{n}{n} = 1$$

é a máxima taxa de transmissão possível mas, como $d = 1$, $\delta(C) = 0$ é mínima!

Os três parâmetros n, M e d de um código estão relacinados. Não é possível ter um código "ideal" com M grande (mais mensagens) e d grande (correcção de mais erros) e n pequeno (taxas de transmissão maiores).

[1] Esta é uma noção que varia de autor para autor.

Problema Principal na Teoria de Códigos: Para q, n e d fixos, determinar

$$A_q(n,d) := \max\{M \,:\, \exists \text{ código } q\text{-ário } (n,M,d)\} \ .$$

Ou seja, trata-se de determinar o maior número de palavras possível que um código q-ário de comprimento n e distância mínima d pode conter.

Na continuação do exemplo anterior, podemos deduzir o seguinte resultado.

Proposição 2.3. *Para $n \geq 1$ verifica-se*

- $A_q(n,1) = q^n$,
- $A_q(n,n) = q$ *e*
- $A_q(n,d) \leq q^n$ *para* $1 \leq d \leq n$.

Dem. No primeiro caso, como $d = 1$, todas as palavras são diferentes. O código $C = \mathcal{A}_q^n$ tem q^n palavras e distância mínima 1, logo $A_q(n,1) \geq q^n$. Qualquer outro código de comprimento n é subconjunto deste, logo $A_q(n,1) \leq q^n$.

No segundo caso, como $d = n$, cada palavra tem um símbolo diferente em cada posição (ou coordenada) fixa, logo $A_q(n,n) \leq \#\mathcal{A}_q = q$. Por outro lado, o código de repetição q-ário de comprimento n tem q palavars, logo $A_q(n,n) \geq q$.

No terceiro caso, basta notar que qualquer código C de comprimento n contendo pelo menos duas palavras[2] tem distância mínima $1 \leq d \leq n$ e é subconjunto de $\mathcal{A}_q^n$. Portanto $\#C \leq q^n$, tal como no primeiro caso. □

Para parâmetros n e d arbitrários, determinar $A_q(n,d)$ é um problema extremamente difícil, e conhecem-se poucos resultados concretos. Para sistematizar a procura e construção de códigos, introduz-se uma noção de equivalência.

Definição 2.4. Seja C um código q-ário (n,M,d). C' diz-se um *código equivalente* a C se é obtido de C através da aplicação sucessiva das seguintes operações:

(i) permutar a ordem das coordenadas de todas as palavros do código, i.e., substituir todo o $c = c_1c_2\cdots c_n \in C$ por $c_{\sigma(1)}c_{\sigma(2)}\cdots c_{\sigma(n)}$, onde σ é uma permutação dos índices $\{1,2,\ldots,n\}$;

(ii) permutar os símbolos de todas as palavras na coordenada i (fixa), mais precisamente, substituir todo o $c = c_1c_2\cdots c_n \in C$ por $\pi_1(c_1)\pi_2(c_2)\cdots\pi_n(c_n)$, onde $\pi_1,\pi_2,\ldots,\pi_n$ são permutações do alfabeto $\mathcal{A}_q$.

Recorde que uma permutação de um conjunto finito X é apenas uma aplicação bijectiva de X em X. Assim, as permutações σ e $\pi_1,\ldots,\pi_n$ na definição anterior são aplicações bijectivas da forma

$$\sigma : \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\} \qquad \text{ou} \qquad \pi_i : \mathcal{A}_q \longrightarrow \mathcal{A}_q \ .$$

No caso de uma permutação σ do conjunto $\{1,2,\ldots,n\}$, também escremos

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \ .$$

Por exemplo, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 4 & 6 & 5 \end{pmatrix}$ denota a permutação definida por $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 1$, $\sigma(4) = 4$, $\sigma(5) = 6$ e $\sigma(6) = 5$ – consultar [**1**] para uma revisão mais aprofundada.

Exemplo 2.5. Os códigos binários $C_1 = \{000,111\}$, $C_2 = \{001,110\}$ e $C_3 = \{100,011\}$ são todos equivalentes porque:

- C_2 é obtido de C_1 trocando os símbolos 0 e 1 do alfabeto na terceira coordenada, i.e., na notação da Definição 2.4, aplicou-se a operação (ii) com π_3 dada por $\pi_3(0) = 1$ e $\pi_3(1) = 0$;

[2] Recorde que a distância mínima de um código C só foi definida se $\#C \geq 2$.

- C_3 é obtido de C_2 trocando a primeira e a terceira coordenadas das palavras de código, i.e., aplicou-se a operação (i) da Definição 2.4 com $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Lema 2.6. *(a) Seja C um código de comprimento n com alfabeto $\mathcal{A}_q$ tal que $0 \in \mathcal{A}_q$. Então C é equivalente a um código contendo a palavra $\vec{0} = 00\cdots0 \in \mathcal{A}_q^n$.*

(b) Dados dois códigos C e C' de parâmetros $(n, M, d)_q$ e $(n', M', d')_{q'}$, respectivamente, se C e C' são equivalentes, então $q = q'$, $n = n'$, $M = M'$ e $d = d'$.

Dem. (a) Aplicar permutações de símbolos de modo a uma palavra do código C previamente fixa se transformar em $\vec{0}$. Concretamente, fixar $c = c_1c_2\cdots c_n \in C$, escolher permutações $\pi_1, \ldots, \pi_n$ do alfabeto $\mathcal{A}_q$ tais que $\pi_i(c_i) = 0$ e definir $C' = \{\pi_1(x_1)\cdots\pi_n(x_n) : x_1\cdots x_n \in C\}$. Portanto C' é equivalente a C e, por construção, $\vec{0} = \pi_1(c_1)\cdots\pi_n(c_n) \in C'$.

(b) Directamente da Definição 2.4, tem-se $q = q'$, $n = n'$ e $M = M'$. Só falta ver que $d = d'$.

Trocar a ordem das coordenadas (operação (i)) não altera a distância entre palavras. Analisemos agora a operação (ii). Sejam $x = x_1\cdots x_n$ e $y = y_1\cdots y_n$ duas palavras do código C. Se $x_i = y_i$ então $\pi_i(x_i) = \pi_i(y_i)$ e se $x_i \neq y_i$ então $\pi_i(x_i) \neq \pi_i(y_i)$, porque π_i é uma aplicação bijectiva. Portanto

$$\mathrm{d}(x, y) = \mathrm{d}(\pi_1(x_1)\cdots\pi_n(x_n), \pi_1(y_1)\cdots\pi_n(y_n))$$

e conclui-se que $d = d'$. □

Exemplo 2.7. Vamos provar que $A_2(5, 3) = 4$. (Em [**2**] prova-se também que, a menos de equivalência, existe um único código binário $(5, 4, 3)$.)

1º passo: Mostrar que $A_2(4, 3) = 2$.

Seja C um código $(4, M, 3)$ binário. Sem perda de generalidade, como consequência do Lema 2.6, podemos assumir que $\vec{0} \in C$. Como $\mathrm{d}(C) = 3$ então $\mathrm{d}(x, \vec{0}) \geq 3$ para todo o $x \in C \setminus \{\vec{0}\}$, ou seja, qualquer palavra de código x não nula tem pelo menos três símbolos 1, ou seja, $x \in X := \{1110, 1101, 1011, 0111, 1111\}$. Para quaisquer duas palavras distintas $y, z \in X$, tem-se

$$\mathrm{d}(y, z) = \begin{cases} 1, & \text{se } y = \vec{1} \text{ ou } z = \vec{1} \\ 2, & \text{se } y \neq \vec{1} \text{ e } z \neq \vec{1} \end{cases},$$

em ambos os casos verifica-se que $\mathrm{d}(y, z) < 3 = \mathrm{d}(C)$, portanto C contém no máximo uma palavra de X, ou seja, C tem no máximo duas palavras. Como C é um código $(4, M, 3)_2$ arbitrário, provou-se que $A_2(4, 3) \leq 2$.

Por outro lado $C = \{0000, 1110\}$ é um código binário de parâmetros $(4, 2, 3)$.

2º passo: Mostar que $A_2(5, 3) = 4$.

Seja C um código binário $(5, M, 3)$. Sejam[3]

$$C_1 = \{x = x_1x_2x_3x_4x_4 \in C : x_1 = 1\} \quad \text{e} \quad C_0 = \{x = x_1x_2x_3x_4x_4 \in C : x_1 = 0\}\ .$$

O código C_0 tem parâmetros $(5, M_0, d_0)$, com distância mínima $d_0 = \mathrm{d}(C_0) \geq \mathrm{d}(C) = 3$ e $M_0 \leq \min\{A_2(4, 3), A_2(4, 4)\} = 2$ (justifique). Por simetria, também temos $M_1 \leq 2$. Como $C = C_1 \cup C_0$ e $C_1 \cap C_0 = \varnothing$, ou seja, C_1 e C_0 formam uma partição de C, então $M = M_1 + M_2$ e, portanto, $A_2(5, 3) \leq 4$.

Por outro lado, $C = \{00000, 01101, 10110, 11011\}$ é um código binário $(5, 4, 3)$.

No resto desta secção, vamos considerar apenas códigos binários, ou seja, o alfabeto é $\mathbb{Z}_2 = \{0, 1\}$. Este conjunto tem uma estrutura de corpo com as operações definidas pelas seguintes tabelas:

+	0	1
0	0	1
1	1	0

e

×	0	1
0	0	0
1	0	1

.

[3] Estes códigos C_1 e C_0 dizem-se secções de C.

$\mathbb{Z}_2^n$ tem então uma estrutura de espaço vectorial sobre $\mathbb{Z}_2$, com a soma de vectores e produto por um escalar em $\mathbb{Z}_2$ definidos da maneira habitual, coordenada a coordenada. Nomeadamente, se $x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$, $y = (y_1, y_2, \ldots, y_n) \in \mathbb{Z}_2^n$ e $\lambda \in \mathbb{Z}_2$, então

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n) \qquad \text{e} \qquad \lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_n) \ . \tag{2.2}$$

Uma vez que $-1 = 1$ em $\mathbb{Z}_2$, verifica-se que $x - y = x + y$ para quaisquer vectores $x, y \in \mathbb{Z}_2^n$.

Definição 2.8. Para $x, y \in \mathbb{Z}_2^n$, define-se

- *intersecção:* $x \cap y = (x_1 y_1, x_2 y_2, \ldots, x_n y_n) \in \mathbb{Z}_2^n$
- *peso:* $\mathrm{w}(x) = \#\{i \,:\, x_i \neq 0\} \in \mathbb{N}_0$

onde x_i e y_i são as coordenadas de x e y, respectivamente.

Por exemplo, se $x = (0,1,1,0,1)$ e $y = (0,0,1,1,0)$ ou, abreviadamente, $x = 01101$ e $y = 00110$, a intersecção é o vector $x \cap y = 00100$ e os pesos destes vectores são $\mathrm{w}(x) = 3$, $\mathrm{w}(y) = 2$ e $\mathrm{w}(x \cap y) = 1$. Note que $x \cap y = y \cap x$, pois a multiplicação em $\mathbb{Z}_2$ é uma operação comutativa.

A noção de peso faz sentido para $\mathbb{Z}_q$ com q arbitrário e iremos considerar também estes casos mais tarde. Note-se que, para o alfabeto binário $\mathbb{Z}_2$, o peso de um vector x é também igual ao número de coordenadas iguais a 1.

Directamente das definições, vemos que

$$\mathrm{d}(x, \vec{0}) = \mathrm{w}(x) \qquad \forall\, x \in \mathbb{Z}_2^n \qquad \text{e} \tag{2.3}$$

$$\mathrm{w}(x \cap y) = \#\{i \,:\, x_i = y_i = 1\} \qquad \forall\, x, y \in \mathbb{Z}_2^n \ . \tag{2.4}$$

Para a última igualdade, convém observar que $ab = 1$ em $\mathbb{Z}_2$ se e só se $a = b = 1$.

Proposição 2.9. *Para quaisquer vectores $x, y \in \mathbb{Z}_2^n$*

(i) $\mathrm{d}(x, y) = \mathrm{w}(x - y)$,

(ii) $\mathrm{d}(x, y) = \mathrm{w}(x) + \mathrm{w}(y) - 2\,\mathrm{w}(x \cap y)$.

Deixa-se a demonstração desta proposição como exercício. Apenas se observa que a igualdade (ii) é falsa caso usássemos um outro alfabeto $\mathbb{Z}_q$ com $q \neq 2$. (Ver Exercício 2.6.)

Teorema 2.10. *Seja d um número inteiro positivo ímpar. Então existe um código binário (n, M, d) se e só se existe um código binário $(n+1, M, d+1)$.*

Dem. ($\Longrightarrow$) Seja C um código binário (n, M, d) e, para cada palavra de código $x = x_1 x_2 \cdots x_n$, defina-se

$$\widehat{x} = \begin{cases} x_1 \cdots x_n 0 & \text{se } \mathrm{w}(x) \text{ é par} \\ x_1 \cdots x_n 1 & \text{se } \mathrm{w}(x) \text{ é ímpar} \end{cases}$$

Seja $\widehat{C} = \{\widehat{x} \,:\, x \in C\}$. Por construção, $\widehat{C}$ é um código $(n+1, M, \widehat{d})$ com $d \leq \widehat{d} \leq d+1$ – justifique! Além disso $\mathrm{w}(\widehat{x})$ é sempre par, por definição de $\widehat{x}$, e, portanto, $\mathrm{d}(\widehat{x}, \widehat{y})$ também é par para qualquer $\widehat{x}, \widehat{y} \in \widehat{C}$ pois, por (ii) da Proposição 2.9, têm-se $\mathrm{d}(\widehat{x}, \widehat{y}) = \mathrm{w}(\widehat{x}) + \mathrm{w}\,\widehat{y} - 2\,\mathrm{w}(\widehat{x} \cap \widehat{y})$, onde $\mathrm{w}(\widehat{x})$, $\mathrm{w}(\widehat{y})$ e $2\,\mathrm{w}(\widehat{x} \cap \widehat{y})$ são pares. Daqui se conclui que a distância mínima $d(\widehat{C}) = \widehat{d}$ é par. Atendendo a que $d \leq \widehat{d} \leq d+1$ com d ímpar e $\widehat{d}$ par, concluímos finalmente que $\widehat{d} = d+1$.

($\Longleftarrow$) Seja agora $\widehat{C}$ um código $(n+1, M, d+1)$ e fixemos $\widehat{x}, \widehat{y} \in \widehat{C}$ tais que $\mathrm{d}(\widehat{x}, \widehat{y}) = d+1 = \mathrm{d}(\widehat{C})$. Como esta distância é positiva, podemos escolher uma coordenada i tal que $\widehat{x}_i \neq \widehat{y}_i$. Seja C o código obtido apagando a coordenada i a todas as palavras de $\widehat{C}$, ou seja,

$$C = \{\widehat{z}_1 \cdots \widehat{z}_{i-1} \widehat{z}_{i+1} \cdots \widehat{z}_n \,:\, \widehat{z} \in \widehat{C}\} \ .$$

Deixamos como exercício justificar que o código C contém exactamente M palavras. Quanto à distância mínima $\mathrm{d}(C)$, basta observar que as palavras de C obtidas de $\widehat{x}$ e $\widehat{y}$ estão a uma distância d e usar a definição de $\mathrm{d}(C)$ e $\mathrm{d}(\widehat{C})$. □

As construções de códigos usadas na demonstração anterior são importantes. A primeira é um caso particular de uma *extensão de códigos* chamada *extensão por paridade*, a segunda chama-se *pontuação* – no Capítulo 5 iremos estudar estas e outras construções.

Corolário 2.11. *Para d ímpar, $A_2(n,d) = A_2(n+1,d+1)$ ou, equivalentemente, para $d>0$ par, $A_2(n,d) = A_2(n-1,d-1)$ ou, equivalentemente, para $t \in \mathbb{N}_0$,*

$$A_2(n,2t+1) = A_2(n+1,2t+2) \ .$$

2. Estimativas

Nesta secção apresentamos algumas desigualdades envolvendo $A_q(n,d)$ que, recordando da definição dada na página 12, designa o número máximo de palavras que um código q-ário de comprimento n e distância mínima d pode ter. O alfabeto dos códigos será sempre um conjunto arbitrário $\mathcal{A}_q$ de q elementos, sem qualquer estrutura adicional.

2.1. Estimativa de Singleton

Proposição 2.12. *Para q,n e $d \geq 1$ fixos, tem-se*

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

Dem. Fixemos um código arbitrário C de parâmetros $(n,M,d)_q$. Queremos mostar que $M \leq q^{n-d+1}$. Apagando as últimas $d-1$ coordenadas (ou outras $d-1$ coordenadas fixas à nossa escolha) de todas as palavras de C, obtém-se um código C' com M palavras de comprimento $n-d+1$ todas distintas entre si porque $d-1 < d = \mathrm{d}(C)$. Portanto $M \leq q^{n-d+1} = \#(\mathcal{A}_q)^{n-d+1}$, pois C' é um subconjunto de $\mathcal{A}_q^{n-d+1}$. □

Os códigos lineares $(n,M,d)_q$ que satisfazem a igualdade $M = q^{n-d+1}$ dizem-se *códigos de distância máxima de separação* (ou simplesmente códigos MDS) e iremos estudar alguns exemplos mais tarde.

2.2. Empacotamento de esferas

Recorde que, usando a distância de Hamming d, se $c \in \mathcal{A}_q^n$ e r é um inteiro não negativo, a bola (ou esfera) de centro c e raio r é o subconjunto de $\mathcal{A}_q^n$ definido por

$$B_r(c) = \{x \in \mathcal{A}_q^n \ : \ \mathrm{d}(x,c) \leq r\} \ .$$

Sendo $\mathcal{A}_q$ um conjunto finito, $\mathcal{A}_q^n$ e qualquer seu subconjunto também o são. Define-se *volume de um subconjunto* S de $\mathcal{A}_q^n$ por

$$\mathrm{vol}(S) = \#S \ ,$$

ou seja, o volume de S é o seu cardinal.

Lema 2.13. *O volume da bola $B_r(c)$ é*

$$\mathrm{vol}(B_r(c)) = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j \ ,$$

onde $0 \leq r \leq n$ e $c \in \mathcal{A}_q^n$.

Dem. A bola $B_r(c)$ é a união disjunta dos conjuntos $\{x \in \mathcal{A}_q^n \ : \ \mathrm{d}(x,c) = j\}$ com $j = 0,1,\ldots,r$. Portanto

$$\mathrm{vol}(B_r(c)) = \sum_{j=0}^{r} \#\{x \in \mathcal{A}_q^n \ : \ \mathrm{d}(x,c) = j\} \ .$$

Como

- $\mathrm{d}(x,c) = j$ se e só se x e c diferem exactamente em j coordenadas,
- $\binom{n}{j}$ é o número de maneiras diferentes de escolher j coordenadas em n e

- $q-1$ é o número de símbolos em $\mathcal{A}_q \setminus \{c_i\}$, i.e., o número de escolhas para a coordenada $x_i \neq c_i$,

conclui-se que

$$\#\{x \in \mathcal{A}_q^n \,:\, \mathrm{d}(x,c) = j\} = \binom{n}{j}(q-1)^j \ . \qquad \square$$

Caso $r \geq n$, tem-se obviamente que $B_r(c) = \mathcal{A}_q^n$, cujo volume é q^n.

Exemplo 2.14. Fixemos $\mathcal{A}_2 = \mathbb{Z}_2 = \{0,1\}$. Em $\mathbb{Z}_2^3$, a bola $B_4(001)$ tem volume 8, pois o raio é $r = 4 > 3 = n$, donde $B_4(001) = \mathbb{Z}_2^3$.
A bola de raio 1 e centro na origem em $\mathbb{Z}_2^3$ é o conjunto

$$B_1(000) = \{000, 001, 010, 100\} \ ,$$

sendo 000 o único vector à distância 0 do centro da bola, claro!, e sendo os restantes três elementos 001, 010 e 100 os vectores de $\mathbb{Z}_2^3$ à distância 1 do centro. Portanto $\mathrm{vol}(B_1(000)) = 4$. Também podemos aplicar o Lema 2.13 para o cálculo do volume.

Exemplo 2.15. Calcular o volume de $B_3(1100) \subset \mathbb{Z}_2^4$. Aplicando directamente o lema anterior e notando que $q - 1 = 1$ neste caso, fica

$$\mathrm{vol}(B_3(1100)) = \binom{4}{0} + \binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 1 + 4 + 6 + 4 = 15 \ .$$

Teorema 2.16 (Estimativa de Gilbert-Varshamov ou Minorante de Cobertura de Esferas)**.** *Para $q \geq 2$ e $1 \leq d \leq n$, temos*

$$\boxed{A_q(n,d) \geq \frac{q^n}{\mathrm{vol}(B_{d-1}(c))}} \ . \tag{2.5}$$

Dem. Seja C um código $(n, M, d)_q$ com $M = A_q(n,d)$. Vamos primeiro provar que

$$\forall x \in \mathcal{A}_q^n \quad \exists c \in C \quad \text{tal que} \quad \mathrm{d}(x,c) \leq d-1 \ . \tag{2.6}$$

Suponhamos que não. Nesse caso seja $y \in \mathcal{A}_q^n$ tal que $\mathrm{d}(y,c) \geq d$ para todo o $c \in C$. Em particular $y \notin C$. Então o conjunto $C' = C \cup \{y\}$ é um código $(n, M+1, d)$ (justifique que $\mathrm{d}(C') = d$) o que contradiz a hipótese $M = A_q(n,d)$. Provámos assim (2.6).
Em termos de conjuntos, (2.6) escreve-se na forma

$$\mathcal{A}_q^n = \bigcup_{c \in C} B_{d-1}(c) \ .$$

Como $\mathrm{vol}(\mathcal{A}_q^n) = q^n$ e $\mathrm{vol}(\bigcup_{c\in C} B_{d-1}(c)) \leq M\,\mathrm{vol}(B_{d-1}(c))$ (porque é que não se tem necessarimante a igualdade?), obtém-se a desigualdade do enunciado do teorema. $\square$

Teorema 2.17 (Estimativa de Hamming ou Majorante de Empacotamento de Esferas)**.** *Para $q \geq 2$ e $2t+1 \leq d \leq n$, temos*

$$\boxed{A_q(n,d) \leq \frac{q^n}{\mathrm{vol}(B_t(c))}} \ . \tag{2.7}$$

Dem. Seja C um código $(n, M, d)_q$ com $M = A_q(n,d)$ e $d \geq 2t+1$. Então, pelo Teorema 1.30,

$$B_t(c) \cap B_t(c') = \varnothing \qquad \forall\, c, c' \in C, \text{ com } c \neq c' \ .$$

Ou seja, as M bolas de raio t e centro nas M palavras do código C são disjuntas duas a duas, donde

$$\mathrm{vol}\Big(\bigcup_{c\in C} B_t(c)\Big) = \sum_{c\in C} \mathrm{vol}(B_t(c)) = M\,\mathrm{vol}(B_t(c)) \ , \tag{2.8}$$

uma vez que as bolas com o mesmo raio têm volumes iguais. Como $\mathrm{vol}(\mathcal{A}_q^n) = q^n$, a igualdade (2.8) implica que $M\,\mathrm{vol}(B_t(c)) \leq q^n$. $\square$

Exemplo 2.18. Será que existe um código binário (8,29,3)?
A Estimativa de Singleton dá

$$A_2(8,3) \leq 2^{8-3+1} = 64 \ .$$

É inconclusivo.
Como

$$\mathrm{vol}(B_2(c)) = \binom{8}{0} + \binom{8}{1} + \binom{8}{2} = 1 + 8 + 28 = 37 \ ,$$

o Minorante de Cobertura de Gilbert-Varshamov dá

$$A_2(8,3) \geq \frac{2^8}{\mathrm{vol}(B_2(c))} = \frac{256}{37} = 6,9\ldots$$

logo $A_2(8,3) \geq 7$. Também é inconclusivo.
O Majorante de Empacotamento de Hamming, com $t = \frac{d-1}{2} = 1$, dá

$$A_2(8,3) \leq \frac{2^8}{\mathrm{vol}(B_1(c))} = \frac{256}{9} = 28,4\ldots$$

logo $A_2(8,3) \leq 28$ e, portanto, não existem códigos $(8,29,3)_2$.

E o que é que acontece quando se verifica a igualdade na estimativa de Hamming?

Definição 2.19. Seja C um código q-ário de comprimento n qualquer. Define-se *raio de empacotamento* por

$$\rho_e(C) := \max\{r \in \mathbb{N}_0 \ : \ B_r(c) \cap B_r(c') = \varnothing \quad \forall c, c' \in C, \ \text{com } c \neq c'\}$$

e *raio de cobertura* por

$$\rho_c(C) := \min\{r \in \mathbb{N}_0 \ : \ \bigcup_{c \in C} B_r(c) = \mathcal{A}_q^n\} \ .$$

Assim, o raio de empacotamento $\rho_e(C)$ é o maior raio possível de modo a todas as bolas de centro em palavras do código serem disjuntas duas a duas. Como não há sobreposições, é possível "empacotar" estas bolas no espaço $\mathcal{A}_q^n$. E o raio de cobertura $\rho_c(C)$ é o menor raio r de modo as bolas de raio r e centro nas palavras de código formarem uma cobertura do espaço $\mathcal{A}_q^n$.
Na demonstração do Teorema 2.16 provou-se que $\rho_c(C) \leq d - 1 = \mathrm{d}(C) - 1$ e na do Teorema 2.17 provou-se que $\rho_e(C) \geq t = \left\lfloor \frac{\mathrm{d}(C) - 1}{2} \right\rfloor$. Compare também com o Teorema 1.30 ou o Corolário 1.31.

Definição 2.20. Um código C de parâmetros $(n, M, 2t+1)_q$ diz-se *perfeito* sse $\rho_e(C) = \rho_c(C)$.

Isto é, as bolas de raio $\rho = \rho_c(C) = \rho_e(C)$ e centro em $c \in C$ são disjuntas duas as duas e formam uma cobertura de $\mathcal{A}_q^n$. Diz-se também que estas bolas constituem um *empacotamento perfeito*, sem "sobreposições" nem "espaços vazios".

Exemplo 2.21. Seja $C = \{000, 111\}$. Uma vez que

$$B_1(000) = \{000, 100, 010, 001\} \qquad \text{e} \qquad B_1(111) = \{111, 011, 010, 110\} \ ,$$

verifica-se directamente que

$$\mathbb{Z}_2^3 = B_1(000) \cup B_1(111) \qquad \text{e} \qquad B_1(000) \cap B_1(111) = \varnothing \ ,$$

donde se conclui que $\rho_c(C) = \rho_e(C) = 1$ e, portanto, C é um código perfeito.

O Exercício 2.8 dá uma definição alternativa de código perfeito.

Exemplo 2.22. Códigos perfeitos triviais:

(a) Seja C um código contendo uma palavra apenas, de comprimento n. Neste caso, a distância mínima $\mathrm{d}(C)$ não foi definida, mas como C corrige n erros, convencionamos que $\mathrm{d}(C) = 2n + 1$. Deste modo, os parâmetros de C são $(n, 1, 2n+1)_q$ e C verifica a igualdade na Estimativa de Hamming (2.7) sendo, portanto, um código perfeito.

(b) $C = \mathcal{A}_q^n$, com parâmetros $(n, q^n, 1)_q$, é um código perfeito, porque o raio de empacotamento $\rho_e(C)$ e o raio de cobertura $\rho_c(C)$ são ambos zero.

(c) Os código de repetição binários de comprimento n ímpar também são perfeitos.

Alguns exemplos de códigos perfeitos não triviais, a ver mais tarde, são os códigos de Hamming e os códigos de Golay.

Exemplo 2.23. Será que existe um código perfeito binário de parâmetros $(7, 16, 3)$?
Como

$$\frac{q^n}{\text{vol}(B_1(c))} = \frac{2^7}{\binom{7}{0} + \binom{7}{1}} = \frac{2^7}{1+7} = \frac{2^7}{2^3} = 2^4 = M$$

os parâmetros $(7, 16, 3)$ satisfazem a igualdade na Estimativa de Hamming. Daqui apenas se pode concluir que poderá existir um tal código mas, neste caso, existe mesmo: o código do Exercício 1.7, que é um exemplo de código de Hamming binário, tem parâmetros $(7, 16, 3)$. Deixamos como exercício verificar que a distância mínima deste código é de facto 3.

2.3. Estimativas de Plotkin

Terminamos esta secção com as estimativas de Plotkin, primeiro enunciadas no caso binário no Teorema 2.24, depois generalizadas para o caso q-ário, com q arbitrário, no Teorema 2.25. As demonstrações são deixadas como exercício.

Teorema 2.24. *Seja C um código binário (n, M, d) com $n < 2d$. Então*

$$M \leq \begin{cases} \dfrac{2d}{2d-n} & \text{se } M \text{ é par} \\ \dfrac{2d}{2d-n} - 1 & \text{se } M \text{ é ímpar} \end{cases}.$$

Teorema 2.25. *Seja $\theta = \dfrac{q-1}{q}$. Se $d > \theta n$, então $A_q(n, d) \leq \dfrac{d}{d - \theta n}$.*

Note que, pondo $q = 2$ no Teorema 2.25, obtém-se uma estimativa mais fraca do que no Teorema 2.24 no caso de M ímpar.

Exercícios

2.1. Mostre que $A_q(n, d) < A_{q+1}(n, d)$.

2.2. Verifique que os códigos binários $C_1 = \{0000, 0011, 1100\}$ e $C_2 = \{0000, 0011, 1010\}$ têm os mesmos parâmetros mas não são equivalentes.

2.3. Mostre que, a menos de equivalência, há precisamente n códigos binários de comprimento n contendo duas palavras.

2.4. Mostre que qualquer código de parâmetros $(n, q, n)_q$ é equivalente a um código de repetição.

2.5. Mostre que $A_2(5, 4) = 2$ e $A_2(8, 5) = 4$.

2.6. (a) Demonstre a Proposição 2.9.
(b) Através de um contra-exemplo, mostre que a segunda alínea da Proposição 2.9 não é verdadeira para vectores em $\mathbb{Z}_3^n$, $n > 1$.

2.7. Usando o Lema 2.13, verifique que o volume das bolas de raio n em $\mathcal{A}_q^n$ é de facto q^n.

2.8. Seja C um código $(n, M, d)_q$ com d ímpar. Mostre que C é um código perfeito se e só se $A_q(n, d) = M$ e verifica-se a igualdade na Estimativa de Hamming com $t = \frac{d-1}{2}$.

2.9. Justifique as afirmações do Exemplo 2.22 resolvendo as seguintes alíneas:
(a) Verifique que um código contendo apenas uma palavra satisfaz a igualdade na Estimativa de Hamming.

(b) Para o código $C = \mathcal{A}_q^n$, calcule os raios de empacotamento $\rho_e(C)$ e de cobertura $\rho_c(C)$. Verifique também que C satisfaz a igualdade na Estimativa de Hamming.

(c) Repita a alínea anterior para os código de repetição binários de comprimento ímpar.

2.10. Mostre que não é necessário assumir que a distância mínima é ímpar na Definição 2.20 de código perfeito. Ou seja, mostre que, se C é um código de distância mínima par, então $\rho_e(C) < \rho_c(C)$.

2.11. Estimativas de Plotkin binária e q-ária: demonstre os Teoremas 2.24 e 2.25.

2.12. (a) Dados dois vectores $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_m)$, define-se

$$(u, v) = (u_1, \ldots, u_n, v_1, \ldots, v_m) \ .$$

Sejam C_1 e C_2 códigos binários de parâmetros (n, M_1, d_1) e (n, M_2, d_2), respectivamente. A *Construção de Plotkin* dos códigos C_1 e C_2 é o código dado por

$$C_1 * C_2 = \{(u, u + v) \ : \ u \in C_1, v \in C_2\} \ .$$

Mostre que os parâmteros de $C_1 * C_2$ são $(2n, M_1 M_2, d)$, onde $d = \min\{2d_1, d_2\}$.

(b) A importante família de Códigos de Reed-Muller binários pode ser obtida por recorrência do seguinte modo:

$$\begin{cases} \mathcal{RM}(0, m) = \{\vec{0}, \vec{1}\} & \text{o código de repetição binário de comprimento } 2^m \\ \mathcal{RM}(m, m) = (\mathbb{Z}_2)^{2^m} \\ \mathcal{RM}(r, m) = \mathcal{RM}(r, m-1) * \mathcal{RM}(r-1, m-1) \ , \quad 0 < r < m \end{cases}$$

para qualquer $r, m \in \mathbb{N}_0$, onde $C_1 * C_2$ designa a Construção de Plotkin obtida dos códigos C_1 e C_2.

Mostre que $\mathcal{RM}(r, m)$ tem parâmetros $n = 2^m$, $M = 2^{\delta(r,m)}$, onde $\delta(r, m) = \sum_{i=0}^{r} \binom{m}{i}$, $d = 2^{m-r}$.

Corpos Finitos e Espaços Vectoriais

1. Corpos finitos

Nesta secção começamos por rever a definição e algumas propriedades dos anéis $\mathbb{Z}_m$ e também de anéis quocientes de polinómios. Depois introduzimos uma construção dos corpos finitos. Os anéis quocientes de polinómios são úteis quer na construção de corpos finitos, que faremos de seguida, quer na descrição de códigos cíclicos no Capítulo 8. Alguns dos resultados não serão demonstrados, ou porque os alunos já estudaram as demonstrações numa cadeira de álgebra anterior, ou porque não fazem parte do âmbito desta cadeira. Mas, para os alunos interessados, sugere-se a consulta do livro [**1**].

Seja m um número positivo (bastava assumir que $m \neq 0$, mas com $m > 0$ não precisamos de nos preocupar tanto com os sinais). No anel dos número inteiros $\mathbb{Z}$, temos a seguinte *relação de congruência*:

$$a \equiv a' \pmod{m} \iff a - a' = km \quad \text{para algum } k \in \mathbb{Z}$$

i.e. $a, a' \in \mathbb{Z}$ dizem-se congruentes módulo m se e só se $a - a'$ é divisível por m.

Note-se que, como caso particular, qualquer inteiro a é congruente com o resto r da sua divisão por m. Recorde ainda que, para cada $a \in \mathbb{Z}$, o algoritmo da divisão em $\mathbb{Z}$ garante que o resto r e o quociente q são os *únicos* inteiros tais que

$$a = qm + r \qquad \text{com} \qquad r \in \{0, \ldots, m-1\} \ .$$

Podemos então identificar as classes de equivalência da relação de congruência com os restos da divisão por m. Assim, cada número inteiro pertence exactamente a uma única classe de equivalência e denotamos o conjunto de todas elas por $\mathbb{Z}_m$. Por abuso de linguagem, nem sempre distinguimos entre a classe de equivalência (um conjunto) e os seus representantes (os elementos do conjunto) e escrevemos

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\} \ .$$

Assim, por exemplo, se $m = 3$

$$7 \equiv 4 \equiv -2 \equiv 1 \pmod{3} \ ,$$

o resto da divisão de 7, 4, -2 e 1 por 3 é sempre 1, e estes inteiros pertencem todos à mesma classe de equivalência módulo 3. A sua classe de equivalência é o conjunto

$$\{1 + 3k \ : \ k \in \mathbb{Z}\} = \{\ldots, -5, -2, 1, 4, 7, 11, \ldots\} \ .$$

Com $m = 3$, há mais duas classes de equivalência, nomeadamente

$$\{0 + 3k \,:\, k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 12, \ldots\} \quad \text{e}$$
$$\{2 + 3k \,:\, k \in \mathbb{Z}\} = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\} \,,$$

e identificamos $\mathbb{Z}_3$ com $\{0, 1, 2\}$.

No caso de $m = 2$, há duas classes de equivalência, uma formada pelos números pares, a outra pelos ímpares, que identificamos com os restos 0 e 1, respectivamente, e escrevemos $\mathbb{Z}_2 = \{0, 1\}$, como já temos feito nos capítulos anteriores.

Proposição 3.1. *Se* $a \equiv a' \pmod m$ *e* $b \equiv b' \pmod m$, *então*

(i) $a + b \equiv a' + b' \pmod m$ *e*

(ii) $ab \equiv a'b' \pmod m$.

A proposição anterior permite definir as operações soma e produto em $\mathbb{Z}_m$ à custa das operações respectivas em $\mathbb{Z}$.

Teorema 3.2. *O conjunto* $\mathbb{Z}_m$ *com a soma e produto definidos pelo Proposição 3.1 é um anel comutativo com identidade, i.e., satisfaz as seguintes propriedades:*

(i) $a + b = b + a$ *e* $ab = ba$ *(comutatividade da soma e produto)*

(ii) $(a + b) + c = a + (b + c)$ *e* $(ab)c = a(bc)$ *(associatividade da soma e do produto)*

(iii) $(a + b)c = ac + bc$ *(distributividade da soma em relação ao produto)*

(iv) $a + 0 = a$ *(existência de elemento neutro da soma, ou zero)*

(v) $a \cdot 1 = a$ *(existência de elemento neutro do produto, ou identidade)*

(vi) $\forall\, a \in \mathbb{Z}_m \quad \exists\, -a \in \mathbb{Z}_m \quad$ *tal que* $\quad a + (-a) = 0$ *(existência de simétrico)*

para quaisquer $a, b, c \in \mathbb{Z}_m$.

Definição 3.3. Um *corpo* $\mathbb{F}$ é um anel comutativo com identidade $1 \neq 0$ que satisfaz a seguinte condição: $\forall\, a \in \mathbb{F} \setminus \{0\} \quad \exists\, a^{-1} \in \mathbb{F} \quad$ tal que $\quad a \cdot (a^{-1}) = 1$ (existência de inverso).

Exemplo 3.4.
- $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ são corpos.
- $\mathbb{Z}$ é um anel, mas não é um corpo.
- O conjunto das matrizes 2×2 de entradas reais, $M_2(\mathbb{R})$, é um anel com identidade mas não é comutativo.
- $< 2 >:= \{\text{inteiros pares}\}$ é um anel comutativo sem identidade.

Um corpo verifica ainda as seguintes propriedades.

Proposição 3.5. *Seja* $\mathbb{F}$ *um corpo. Então*

(1) $a \cdot 0 = 0$ *para qualquer* $a \in \mathbb{F}$,

(2) $a \cdot b = 0 \quad \Longrightarrow \quad a = 0 \quad$ *ou* $\quad b = 0$ *(lei do corte).*

Exemplo 3.6.
- $\mathbb{Z}_2 = \{0, 1\}$ é um corpo. O único elemento não nulo, o 1, é o seu próprio inverso.
- $\mathbb{Z}_3 = \{0, 1, 2\}$ é um corpo e tem as seguintes tabelas de operações (ou tabuadas)

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

e

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

.

- $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ não é um corpo porque não satisfaz a lei do corte, pois $2 \times 2 \equiv 0 \pmod 4$ mas $2 \not\equiv 0 \pmod 4$. Em particular, 2 não é invertível. No entanto 3 é invertível e o seu inverso, em $\mathbb{Z}_4$, é o próprio 3 pois

$$3 \times 3 = 9 = 1 + 2 \times 4 \equiv 1 \pmod 4 \,.$$

Teorema 3.7. *$\mathbb{Z}_m$ é um corpo se e só se m é um número primo.*

Nesta secção iremos ver que, embora 4 não seja um número primo, existe um corpo com quatro elementos. E outro com 8, e outro com 9, e muitos mais. Mas não existe nenhum corpo com 6 elementos, nem com 10.

Definição 3.8. Seja $\mathbb{F}$ um corpo finito.

- A *ordem* de $\mathbb{F}$ é o seu cardinal, que passamos a denotar por $|\mathbb{F}|$:
$$|\mathbb{F}| = \#\mathbb{F} = \text{ordem do corpo } \mathbb{F} \ .$$
- Dizemos que $a \in \mathbb{F} \setminus \{0\}$ tem *ordem* $n > 0$, que denotamos por $|a| = n$ ou $\text{ord}(a) = n$, se $a^n = 1$ e $a^k \neq 1$ para $0 < k < n$ ou, equivalentemente,
$$|a| = \min\{n \in \mathbb{N} \,:\, a^n = 1\} \ .$$
- A *característica*[1] de $\mathbb{F}$ é definida por
$$\text{car}(\mathbb{F}) = \min\{n \in \mathbb{N} \,:\, n \cdot 1 := \sum_{i=1}^{n} 1 = 0\} \ ,$$
se este mínimo existe, ou $\text{car}(\mathbb{F}) = 0$ caso contrário.
- $\alpha \in \mathbb{F}$ diz-se um *elemento primitivo*[2] se
$$\mathbb{F} \setminus \{0\} = \{\alpha^i \,:\, i \geq 0\} \ .$$

Notação 3.9. $\mathbb{F}_q$ ou $GF(q)$ (de "Galois Field") designa um corpo de ordem q.

Exemplo 3.10. Os corpos $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ têm característica zero.

Exemplo 3.11. Consideremos o corpo $\mathbb{Z}_2 = \{0, 1\}$, ou $\mathbb{F}_2$. Obviamente tem-se que a sua ordem é $|\mathbb{Z}_2| = \#\mathbb{Z}_2 = 2$. Quando à característica, como $1 \neq 0$ e $2 \cdot 1 = 1 + 1 = 0$ em $\mathbb{Z}_2$, conclui-se que $\text{car}(\mathbb{Z}_2) = 2$. Neste caso só existe um elemento não nulo, a identidade, que é também um elemento primitivo de $\mathbb{Z}_2$.

Exemplo 3.12. Consideremos o corpo $\mathbb{Z}_3 = \{0, 1, 2\}$, ou $\mathbb{F}_3$. Tal como no exemplo anterior, $|\mathbb{Z}_3| = 3$. Também temos que $\text{car}(\mathbb{Z}_3) = 3$, pois
$$1 \neq 0 \ , \qquad 2 \cdot 1 = 1 + 1 = 2 \neq 0 \qquad \text{e} \qquad 3 \cdot 1 = 1 + 1 + 1 = 3 = 0 \qquad \text{em } \mathbb{Z}_3 \ .$$
Como
$$2^2 = 4 \equiv 1 \pmod 3 \ ,$$
então $\mathbb{Z}_3 \setminus \{0\} = \{1, 2\} = \{2, 2^2\}$, donde se conclui que 2 é um elemento primitivo de $\mathbb{Z}_3$.

Exemplo 3.13. Seja p um número primo. Pelo Teorema 3.7 sabemos que $\mathbb{Z}_p$ é um corpo. Da construção de $\mathbb{Z}_p$ tem-se directamente que a sua ordem é $|\mathbb{Z}_p| = p$. Por isso também escrevemos $\mathbb{F}_p$ para designar este corpo.

Vamos agora calcular a característica de $\mathbb{Z}_p$. Seja n um inteiro tal que $0 < n < p$. Identificando n com a sua classe que equivalência módulo p, ou seja, pondo $\mathbb{Z}_p = \{0, 1, 2 \ldots, p-1\}$ como temos feito para $p = 2, 3$, tem-se que
$$\sum_{i=1}^{n} 1 = \underbrace{1 + \cdots + 1}_{n \text{ vezes}} = n \not\equiv 0 \pmod p \ ,$$
e
$$\sum_{i=1}^{p} 1 = \underbrace{1 + \cdots + 1}_{p \text{ vezes}} = p \equiv 0 \pmod p \ ,$$
logo $\text{car}(\mathbb{Z}_p) = p$.

[1] Esta definição faz sentido para qualquer corpo $\mathbb{F}$, não necessáriamente finito.

[2] Também existe a noção de elemento primitivo para corpos não necessarimente finitos, mas a definição aqui apresentada apenas se aplica ao caso finito.

Teorema 3.14. *Seja $\mathbb{F}$ um corpo qualquer. Então ou* $\mathrm{car}(\mathbb{F}) = 0$ *ou* $\mathrm{car}(\mathbb{F}) = p$ *para algum número primo p.*

Dem. Suponhamos que $\mathrm{car}(\mathbb{F}) = n \neq 0$. Suponhamos também que n não é um número primo. Então existem inteiros a e b tais que $n = ab$ e $1 < a, b < n$. Da definição de característica, tem-se

$$0 = \sum_{i=1}^{n} 1 = n \cdot 1 = (ab) \cdot 1 = (a \cdot 1)(b \cdot 1)$$

em $\mathbb{F}$. Pela Lei do Corte, conclui-se que $a \cdot 1 = 0$ ou $b \cdot 1 = 0$, o que contradiz o facto de n ser o menor inteiro positivo tal que $n \cdot 1 = 0$. □

Não é difícil de ver que, se $\mathrm{car}(\mathbb{F}) = 0$, então $\mathbb{F}$ é um corpo infinito. Portanto, pelo teorema anterior, a característica de qualquer corpo finito é um número primo.

A seguinte proposição é bastante útil para averiguar se um dado elemento é primitivo ou não, sem calcular todas as suas potências.

Proposição 3.15. *Seja $\mathbb{F}$ um corpo finito de ordem q. Então*

(i) para todo o $a \in \mathbb{F}$, $a^q = a$,

(ii) para todo o $a \in \mathbb{F} \setminus \{0\}$, $|a|$ divide $q - 1$,

(iii) $a \in \mathbb{F} \setminus \{0\}$ é um elemento primitivo de $\mathbb{F}$ sse $|a| = q - 1$.

Dem. (i) O resultado é trivial se $a = 0$. Seja então $a \neq 0$, e sejam $b_1, \ldots, b_{q-1}$ os elementos não nulos de $\mathbb{F}$, i.e., seja $\mathbb{F} \setminus \{0\} = \{b_1, \ldots, b_{q-1}\}$. Como $a \neq 0$, também temos que $\mathbb{F} \setminus \{0\} = \{ab_1, \ldots, ab_{q-1}\}$. Assim, multiplicando todos os elementos não nulos de $\mathbb{F}$, fica

$$b_1 \cdots b_{q-1} = (ab_1) \cdots (ab_{q-1})$$

ou ainda

$$b_1 \cdots b_{q-1} = (a^{q-1})(b_1 \cdots b_{q-1}) \ ,$$

donde se obtém $a^{q-1} = 1$.

(ii) Fixemos $a \in \mathbb{F} \setminus \{0\}$ e seja m um inteiro positivo tal que $a^m = 1$. Sejam r, s inteiros tais que $m = |a|s + r$ e $0 \leq r < |a|$ (i.e., aplicámos o algoritmo da divisão aos inteiros m e $|a|$). Então

$$1 = a^m = a^{|a|s+r} = (a^{|a|})^s a^r = a^r \ ,$$

portanto $r = 0$, por definição de $|a|$, ou seja, $|a|$ divide m. O resultado agora segue da alínea (i), pois podemos escolher $m = q - 1$.

(iii) Deixamos como exercício justificar que $a \in \mathbb{F} \setminus \{0\}$ tem ordem $q - 1$ se e só se $a, a^2, \ldots, a^{q-1}$ são todos distintos. □

Exemplo 3.16. Consideremos o corpo $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$, ou $\mathbb{F}_7$. Vamos determinar todos os seus elementos primitivos, calculando primeiro a ordem dos seus elementos não nulos.

Como $|\mathbb{Z}_7| = 7$ e, pela Proposição 3.15(iii), $|a|$ divide $|\mathbb{Z}_7| - 1 = 6$, então a ordem de qualquer $a \in \mathbb{Z}_7$, com $a \neq 0$, é 1,2,3 ou 6. Portanto basta calcular as potência a^2 e a^3 para decidir se a é primitivo ou não (porquê?). E basta fazê-lo para $a \neq 1$, uma vez que a identidade tem sempre ordem 1. Assim, temos

$$\begin{aligned}
&2^2 = 4 \ , \quad 2^3 = 8 = 1 && \Longrightarrow \quad |2| = 3 \\
&3^2 = 9 = 2 \ , \quad 3^3 = 3^2 \cdot 3 = 2 \cdot 3 = 6 && \Longrightarrow \quad |3| = 6 \\
&4^2 = (-3)^2 = 3^2 = 2 \ , \quad 4^3 = (-3)^3 = -6 = 1 && \Longrightarrow \quad |4| = 3 \\
&5^2 = (-2)^2 = 4 \ , \quad 5^3 = (-2)^3 = -1 = 6 && \Longrightarrow \quad |5| = 6 \\
&6^2 = (-1)^2 = 1 && \Longrightarrow \quad |6| = 2
\end{aligned}$$

donde se conclui que os elementos primitivos de $\mathbb{Z}_7$ são precisamente o 3 e o 5.

Como se viu no exemplo anterior, pode não haver unicidade de elemento primitivo num corpo $\mathbb{F}_q$. A existência é consequência do próximo lema e das propriedades anteriores.

Lema 3.17. *Sejam $a, b \in \mathbb{F}_q \setminus \{0\}$ tais que $\mathrm{MDC}(|a|, |b|) = 1$. Então $|ab| = |a| \cdot |b|$.*

Dem. Seja $r = |a| \cdot |b|$. Como $|a|$ e $|b|$ dividem r, por definição de ordem de um elemento, tem-se que $a^r = 1$ e $b^r = 1$. Portanto $(ar)^r = a^r b^r = 1$, donde se conclui que

$$|ab| \leq r = |a| \cdot |b| \ .$$

Seja $s = |ab|$. Então

$$1 = (ab)^{s|a|} = \left(a^{|a|}\right)^s b^{s|a|} = b^{s|a|} \ ,$$

logo $|b|$ divide $s|a|$ e, portanto, $|b|$ divide s, pois $\mathrm{MDC}(|a|, |b|) = 1$ por hipótese. Analogamente se prova que $|a|$ divide s. Como $|a|$ e $|b|$ são coprimos e ambos dividem s, conclui-se que

$$|a| \cdot |b| \leq s = |ab| \ . \qquad \square$$

Teorema 3.18. *Qualquer corpo finito $\mathbb{F}_q$ contém um elemento primitivo.*

Dem. Seja m o mínimo múltiplo comum da ordem de todos os $q - 1$ elementos não nulos em $\mathbb{F}_q$. Considere a factorização de m em potências de números primos

$$m = p_1^{e_1} \cdots p_r^{e_r} \ ,$$

onde $p_1, \ldots, p_r$ são primos distintos e $e_1, \ldots, e_r$ são inteiros positivos. Como $p_i^{e_i}$ é um dos factores de m, então $p_i^{e_i} | \operatorname{ord}(a_i)$ para algum $a_i \in \mathbb{F}_q \setminus \{0\}$ e $a_i^{\operatorname{ord}(a_i)/p_i^{e_i}}$ tem ordem $p_i^{e_i}$. Ou seja, provámos que exite $b_i \in \mathbb{F}_q \setminus \{0\}$ com ordem $p_i^{e_i}$, para cada $i = 1, \ldots, r$. Pelo lema anterior, temos que $b = b_1 \cdots b_r$ tem ordem m e, pela alínea (ii) da Proposição 3.15, $m|(q-1)$.

Seja $a \in \mathbb{F}_q \setminus \{0\}$ um elemento não nulo qualquer. Portanto $a^m = 1$, por definição de m, ou seja, a é raiz do polinómio $t^m - 1$ e, portanto[3],

$$m = \operatorname{grau}(t^m - 1) \geq q - 1 = \#(\mathbb{F}_q \setminus \{0\}) \ .$$

Como $m|(q-1)$ e $m \geq q - 1$, tem-se necessariamente que $m = q - 1$, donde se conclui que b é um elemento primitivo de $\mathbb{F}_q$, pela alínea (iii) da Proposição 3.15. $\square$

Note que, embora este teorema garanta a existência de um elemento primitivo, a sua demonstração não nos diz nada acerca de como determiná-lo.

De seguida vamos construir corpos finitos de ordem uma potência de um primo.

Exemplo 3.19. $\mathbb{Z}_4$ não é um corpo porque 4 não é um número primo. Mas será que existe um corpo de ordem 4?

Vamos considerar um conjunto de 4 elementos, $\mathbb{F}_4 = \{0, 1, a, b\}$, com 0 o zero e 1 a identidade de $\mathbb{F}_4$, e tentemos escrever as tabelas para a soma e para o produto de modo a satisfazer as propriedade de corpo.

As propriedades dos elementos zero e identidade forçam a primeira linha da tabela da soma e as duas primeiras linhas da tabela do produto e, por comutatividade das operações, as correspondentes colunas também ficam preenchidas. A lei do corte para o produto força as restantes 4 entradas da tabela do produto. Portanto já se calculou:

$+$	0	1	a	b
0	0	1	a	b
1	1			
a	a			
b	b			

e

$\times$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

A lei do corte para a soma implica que $1 + a = 0$ ou $1 + a = b$. Suponhamos que $1 + a = 0$. Então, multiplicando por b obtém-se $b + 1 = 0$ e, comparando com $1 + a = 0$ novamente, ficava $a = b$, o

[3]Como $\mathbb{F}_q[t]$ é um domínio de factorização única, pois $\mathbb{F}_q$ é um corpo, o número de raízes em $\mathbb{F}_q$ de um polinómio nunca é superior ao seu grau.

que é falso. Logo tem de ser $1 + a = b$. Esta condição, juntamente com as propriedade de corpo e com o produto já definido, permite completar o resto da tabela da soma. Obtém-se, finalmente!, as seguintes tabuadas

$$\begin{array}{c|cccc} + & 0 & 1 & a & b \\ \hline 0 & 0 & 1 & a & b \\ 1 & 1 & 0 & b & a \\ a & a & b & 0 & 1 \\ b & b & a & 1 & 0 \end{array} \qquad \text{e} \qquad \begin{array}{c|cccc} \times & 0 & 1 & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a & b \\ a & 0 & a & b & 1 \\ b & 0 & b & 1 & a \end{array} \; . \tag{3.1}$$

Estas tabelas definem de facto uma estrutura de corpo em $\mathbb{F}_4$. Além disso, da tabela da soma, conclui-se que a $\mathbb{F}_4$ tem característica 2 e, da tabela do produto, conclui-se que a e b são elementos primitivos.

Como se viu neste último exemplo, determinar as tabuadas apenas com base nas propriedades de corpo não é tarefa simples, mesmo se já soubermos que existe um corpo de determinada ordem. Os alunos que já estudaram um pouco de teoria de grupos podiam ter chegado mais rapidamente à tabuada da soma, uma vez que $(\mathbb{F}_4, +)$ é um grupo abeliano e apenas há dois grupos com 4 elementos: a outra escolha para a soma leva às operações de $\mathbb{Z}_4$. Mesmo assim, estas observações nada simplificam no caso de corpos finitos de ordens maiores. Interessa portanto construir os corpos $\mathbb{F}_q$ de uma maneira mais eficiente. Para isso, precisamos de rever primeiro algumas definições e propriedades dos anéis de polinómios.

Seja $\mathbb{F}$ um corpo qualquer. Seja $\mathbb{F}[t]$ o conjunto dos polinómios com coeficientes em $\mathbb{F}$, i.e.

$$\mathbb{F}[t] := \{a(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \, : \, n \in \mathbb{N}_0, \, a_i \in \mathbb{F}\} \; .$$

Este conjunto com a soma e produto usuais de polinómios é um anel comutativo com identidade.
Define-se o *grau* de um polinómio $a(t) = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n$ por

$$\text{grau}(a(t)) = \begin{cases} -\infty & \text{se } a(t) \text{ é o polinómio nulo,} \\ \max\{i \in \mathbb{N}_0 \, : \, a_i \neq 0\} & \text{caso contrário.} \end{cases}$$

À semelhança de $\mathbb{Z}$, o anel $\mathbb{F}[t]$ também tem definido um *algoritmo de divisão*, ou seja,

$$\forall \, a(t), b(t) \in \mathbb{F}[t], \, b(t) \neq 0 \quad \exists \, q(t), r(t) \in \mathbb{F}[t] \quad \text{tais que} \quad a(t) = q(t)b(t) + r(t)$$

onde $\text{grau}(r(t)) < \text{grau}(b(t))$. Naturalmente chamamos quociente a $q(t)$ e resto a $r(t)$.
Fixemos $f(t) \in \mathbb{F}[t] \setminus \{0\}$. Analogamente a $\mathbb{Z}$, definimos uma *relação de congruência* em $\mathbb{F}[t]$ por

$$a(t) \equiv a'(t) \pmod{f(t)} \qquad \Longleftrightarrow \qquad a(t) - a'(t) = k(t) f(t) \quad \text{para algum } k(t) \in \mathbb{F}[t] \; .$$

e definimos ainda o quociente $\mathbb{F}[t]/\langle f(t) \rangle$ como o conjunto das classes de equivalência que, continuando com a analogia a $\mathbb{Z}$, identificamos com os restos $r(t)$ da divisão por $f(t)$:

$$\begin{aligned} \mathbb{F}[t]/\langle f(t) \rangle &= \text{conjunto dos restos da divisão por } f(t) \in \mathbb{F}[t] \\ &= \text{conjunto dos polinómios em } \mathbb{F}[t] \text{ de grau estritamente menor que } \text{grau}(f(t)) \; . \end{aligned}$$

Tal como fizemos para $\mathbb{Z}_m$, sempre que não haja ambiguidades, não distinguimos uma classe de equivalência dos seus representantes. E é isso que fizemos nas igualdades anteriores.

Proposição 3.20. *Seja $f(t) \in \mathbb{F}[t]$ um polinómio não nulo. O quociente $\mathbb{F}[t]/\langle f(t) \rangle$, com a soma e o produto definidos módulo $f(t)$, é um anel comutativo com identidade. Os elementos zero e identidade são representados pelo polinómio nulo $0 \in \mathbb{F}[t]$ e pelo polinómio constante $1 \in \mathbb{F}[t]$, respectivamente.*

Exemplo 3.21. Consideremos o anel dos polinómios com coeficientes em $\mathbb{F}_2$, $\mathbb{F}_2[t]$, e seja $f(t) = t^2 + t + 1$. Como $f(t)$ tem grau 2, temos

$$\mathbb{F}_2[t]/\langle f(t) \rangle = \{a + bt \, : \, a, b \in \mathbb{F}_2\} = \{0, 1, t, t+1\} \; .$$

Deixamos como exercício verificar que as tabelas da soma e produto deste anel são

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

e

$\times$	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	$t+1$	1
$t+1$	0	$t+1$	1	t

.

Portanto, $\mathbb{F}_2[t]/\langle t^2+t+1\rangle$ é um corpo. [Compare com as tabelas (3.1) do Exemplo 3.19.]

Exemplo 3.22. Seja $f(t) = t^2+1 \in \mathbb{F}_2[t]$. Tal como no exemplo anterior, tem-se que

$$\mathbb{F}_2[t]/\langle t^2+1\rangle = \{0, 1, t, t+1\} ,$$

porque $\text{grau}(f(t)) = 2$. Mas as operações soma e produto são agora dadas pelas tabelas

$+$	0	1	t	$t+1$
0	0	1	t	$t+1$
1	1	0	$t+1$	t
t	t	$t+1$	0	1
$t+1$	$t+1$	t	1	0

e

$\times$	0	1	t	$t+1$
0	0	0	0	0
1	0	1	t	$t+1$
t	0	t	1	$t+1$
$t+1$	0	$t+1$	$t+1$	0

.

Em particular, como $(t+1)(t+1) = t^2+2t+1 = t^2+1 \equiv 0 \pmod{t^2+1}$, não se verifica a lei do corte e, portanto, $\mathbb{F}_2[t]/\langle t^2+1\rangle$ não é um corpo.

Pergunta: Quando é que o quociente $\mathbb{F}[t]/\langle f(t)\rangle$ é um corpo?

Definição 3.23. Seja $f(t) \in \mathbb{F}[t] \setminus \{0\}$. Dizemos que $f(t)$ é um *polinómio redutível* se é possível escrever $f(t) = a(t)b(t)$, em $\mathbb{F}[t]$, com $\text{grau}(a(t)) < \text{grau}(f(t))$ e $\text{grau}(b(t)) < \text{grau}(f(t))$. Caso contrário, dizemos que $f(t)$ é *irredutível*.

Exemplo 3.24. (a) Como $t^2+1 = (t+1)(t+1)$ em $\mathbb{F}_2[t]$, o polinómio t^2+1 é redutível em $\mathbb{F}_2[t]$.

(b) t^2+1 é irredutível em $\mathbb{F}_3[t]$. Porquê?

(c) t^2+t+1 é irredutível em $\mathbb{F}_2[t]$. Porquê?

(d) $f(t) = t^4+t^2+1$ é redutível em $\mathbb{F}_2[t]$ porque $f(t) = (t^2+t+1)^2$, mas note que $f(t)$ não possui raízes em $\mathbb{F}_2$: $f(0) = f(1) = 1 \neq 0$.

Teorema 3.25. *Seja $\mathbb{F}$ um corpo e seja $f(t) \in \mathbb{F}[t]$ um polinómio não nulo. Então o quociente $\mathbb{F}[t]/\langle f(t)\rangle$ é um corpo se e só se $f(t)$ é irredutível em $\mathbb{F}[t]$.*

Portanto

- Se $\mathbb{F}$ é um corpo finito de ordem q e $f(t) \in \mathbb{F}[t]$ é um polinómio irredutível de grau $m > 0$, então o quociente $\mathbb{F}[t]/\langle f(t)\rangle$ é um corpo de ordem q^m.
- O Teorema A.16 do Apêndice A implica que, para qualquer inteiro positivo m e para qualquer primo p, existe um polinómio irredutível em $\mathbb{F}_p[t]$ de grau m.

E fica assim justificado que exitem corpos de ordem p^m. (O Exercício 3.6 permite concluir que qualquer corpo finito tem ordem p^m para algum $m \geq 1$ e primo p.) O resultado geral acerca da existência de corpos finitos é o seguinte:

Teorema 3.26. *(i) Existe um corpo de ordem q se e só se $q = p^m$ para algum primo p e algum inteiro $m \geq 1$.*

(ii) Se E e F são corpos finitos com a mesma ordem, então E e F são isomorfos.

A segunda alínea deste teorema quer dizer que só há um corpo de ordem q, a menos de "mudar os nomes dos seus elementos".

Observação 3.27. Atenção! Se p é um número primo, tem-se que $\mathbb{F}_p = \mathbb{Z}_p$. Mas $\mathbb{F}_{p^m} \ncong \mathbb{Z}_{p^m}$, se $m > 1$, porque $\mathbb{Z}_{p^m}$ não é um corpo.

Observação 3.28. Seja $f(t)$ um polinómio de grau m, irredutível em $\mathbb{F}_q[t]$. Seja α uma raiz de $f(t)$. Então o corpo $\mathbb{F}_{q^m} = \mathbb{F}_q[t]/\langle f(t)\rangle$ também pode ser representado por

$$\mathbb{F}_q[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \,:\, a_i \in \mathbb{F}_q\} \,. \tag{3.2}$$

Se, além disso, α for também um elemento primitivo de $\mathbb{F}_{q^m}$, então

$$\mathbb{F}_{q^m} = \{0, \alpha, \alpha^2, \ldots, \alpha^{q^m-1}\} \,. \tag{3.3}$$

A descrição (3.2) é mais útil para determinar a soma de elementos, a descrição (3.3) é mais útil para calcular o produto de elementos no corpo $\mathbb{F}_{q^m}$.

Terminamos esta secção enunciando algumas propriedades úteis sobre polinómios (ir)redutíveis.

Proposição 3.29. *Seja $\mathbb{F}$ um corpo e fixemos $f(t) \in \mathbb{F}[t]$. Então*

(a) $t - a$ divide $f(t)$ se e só se $f(a) = 0$ (i.e., se a é raiz de f),

(b) se $f(t)$ tem grau 2 ou 3, então $f(t)$ é irredutível se e só se não tem raízes em $\mathbb{F}$.

Dem. (a) Se $t - a$ divide $f(t)$, então $f(t) = (t - a)g(t)$ para algum polinómio $g(t) \in \mathbb{F}[t]$. Pondo $t = a$ fica $f(a) = 0$.

Reciprocamente, o algoritmo de divisão implica que exitem polinómios $q(t), r(t) \in \mathbb{F}[t]$ tais que $f(t) = q(t)(t-a) + r(t)$ com $\text{grau}(r(t)) < \text{grau}(t-a) = 1$, ou seja, o resto é um polinómio constante $r(t) = r$. Como $q(a)(a - a) + r = f(a) = 0$, obtém-se $r = 0$.

(b) $f(t)$ é redutível se e só se $f(t) = a(t)b(t)$ com $\text{grau}(a(t)) = 1$ e $\text{grau}(b(t)) = 1$ ou 2, porque $\text{grau}(f(t)) = 2$ ou 3. Logo temos $a(t) = t - a$ para algum $a \in \mathbb{F}$ e, pela alínea (a), a é raiz de $f(t)$. □

A alínea (b) deste teorema permite responder às questões deixadas no Exemplo 3.24 sem recorrer a factorizações de polinómios.

2. Espaços vectoriais sobre corpos finitos

Seja $\mathbb{F}_q$ um corpo finito. A noção de espaço vectorial sobre $\mathbb{F}_q$ é em tudo análoga à estudada na cadeira de Álgebra Linear no caso do corpo dos escalares ser $\mathbb{R}$ e não depende do corpo dos escalares ser finito. Mas precisamente, um espaço vectorial sobre um corpo F é um conjunto $V \neq \varnothing$ com uma operação de adição $+ : V \times V \to V$ e uma multiplicação por escalares $F \times V \to V$ satisfazendo os seguintes axiomas[4]:

(i) $x + (y + z) = (x + y) + z$ (associatividade da soma),
(ii) $x + y = y + x$ (comutatividade da soma),
(iii) $\exists\, 0 \in V \quad \forall\, x \in V \quad x + 0 = x$ (existência de vector nulo),
(iv) $\forall\, x \in V \quad \exists\, -x \in V \quad$ tal que $\quad x + (-x) = 0$ (existência de simétrico),
(v) $a(x + y) = ax + ay$,
(vi) $(a + b)x = ax + bx$,
(vii) $(ab)x = a(bx)$,
(viii) $1x = x$, onde 1 é a identidade de F,

para quaisquer $x, y, z \in V$ e $a, b \in F$. Em particular, não é difícil verificar que o conjunto $(\mathbb{F}_q)^n$ é um espaço vectorial com a soma de vectores e produto por um escalar definidos coordenada a coordenada, respectivamente, por

$$x + y = (x_1 + y_1, \ldots, x_n + y_n) \qquad \text{e} \qquad ax = (ax_1, \ldots, ax_n)$$

onde $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ são vectores em $\mathbb{F}_q^n$ e $a \in \mathbb{F}_q$ é um escalar.

[4] Os axiomas (i) a (iv) dizem-nos que $(V, +)$ é um grupo abeliano.

O espaço vectorial $\mathbb{F}_q^n$ também costuma ser denotado por $V(n,q)$. Os vectores em $\mathbb{F}_q^n$ serão denotados por x, y, etc., ou por $\vec{x}$, $\vec{y}$, etc.

Se V é um espaço vectorial, um *subespaço vectorial* de V é um subconjunto $W \subset V$, não vazio, tal que W é ele próprio um espaço vectorial. Quase todos os espaços vectoriais que iremos considerar nesta cadeira serão subespaços de algum $\mathbb{F}_q^n$.

Tal como se verifica para espaços vectoriais reais, também temos o seguinte resultado quando o corpo dos esclares é $\mathbb{F}_q$ (ou mesmo qualquer corpo, finito ou infinito).

Teorema 3.30. *Seja V um espaço vectorial e $W \subset V$ com $W \neq \varnothing$. Então, W é um subespaço de V se e só se W é fechado para a soma e para o produto por um escalar.*

A demonstração é consequência directa dos axiomas de espaço vectorial.

Exemplo 3.31. Os seguintes conjuntos são espaços vectoriais:

(a) $\{\vec{0}\}$ e $\mathbb{F}_q^n$;

(b) $V_1 = \{(a, a, \ldots, a) : a \in \mathbb{F}_q\} \subset \mathbb{F}_q^n$;

(c) $V_2 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\} \subset \mathbb{F}_2^4$;

(d) $V_3 = \{(0,0,0), (0,1,2), (0,2,1)\} \subset \mathbb{F}_3^3$.

De seguida iremos ver algumas definições e resultados para espaços vectoriais sobre o corpo finito $\mathbb{F}_q$. Muitos deles são completamente análogos aos já estudados na cadeira de Álgebra Linear, e as demonstrações serão omitidas, mas, por vezes, o caso finito tem um comportamento diferente.

Definição 3.32. Seja V um espaço vectorial sobre $\mathbb{F}_q$.

- Uma *combinação linear* dos vectores $v_1, \ldots, v_r \in V$ é um vector da forma $a_1v_1 + \cdots + a_rv_r \in V$, com $a_i \in \mathbb{F}_q$, $i = 1, \ldots, r$.
- Um conjunto de vectores $\{v_1, \ldots, v_r\} \subset V$ diz-se *linearmente independente* se
$$a_1v_1 + \cdots + a_rv_r = \vec{0} \quad \Longrightarrow \quad a_1 = a_2 = \cdots = a_r = 0 \ .$$
- Diz-se que $\{v_1, \ldots, v_r\} \subset V$ é um *conjunto gerador de V* se qualquer vector em V é combinação linear de $v_1, \ldots, v_r$.
- O *espaço gerado* pelo conjunto $\{v_1, \ldots, v_r\} \subset V$ é
$$\langle v_1, \ldots, v_r \rangle = \{a_1v_1 + \cdots + a_rv_r : a_i \in \mathbb{F}_q\} \ ,$$
portanto é o menor subespaço de V que contém os vectores $v_1, \ldots, v_r$.
- Uma *base de V* é um conjunto gerador linearmente independente.

Exemplo 3.33. Continuando o Exemplo 3.31:

- Qualquer conjunto que contém o vector nulo $\vec{0}$ é linearmente dependente.
- O espaço $\{\vec{0}\}$ não contém nenhuma base.
- $\{(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)\}$ é uma base de $\mathbb{F}_q^4$ a que chamamos *base canónica.*
- $\{(1,1,\ldots,1)\}$ é uma base para o espaço V_1 do Exemplo 3.31(b).
- $\{(1,0,1,0), (0,1,0,1)\}$ é uma base para o espaço V_2 do Exemplo 3.31(c) e $\{(1,0,1,0), (1,1,1,1)\}$ é uma outra base para o mesmo espaço.
- $\{(0,1,2)\}$ é uma base para o espaço V_3 do Exemplo 3.31(d).

Teorema 3.34. *Seja $V \neq \{\vec{0}\}$ um espaço vectorial finito sobre $\mathbb{F}_q$. Então qualquer conjunto gerador de V contém uma base e, em particular, V tem uma base.*

Dem. Seja $X = \{v_1, \ldots, v_n\} \subset V$ um conjunto finito gerador de V (pode-se tomar $X = V$). Se X é linearmente independente, então X é uma base. Caso contrário, existem $a_1, \ldots, a_n \in \mathbb{F}_q$, não todos nulos, tais que
$$a_1v_1 + \cdots + a_nv_n = \vec{0} \ .$$

Sem perda de genralidade, suponhamos que $a_n \neq 0$. Então

$$v_n = -a_n^{-1}(a_1 v_1 + \cdots + a_{n-1} v_{n-1})$$

e, portanto, $X_1 := \{v_1, \ldots, v_{n-1}\}$ é um conjunto gerador de V. Repita-se iterativamente o argumento com X_1 em vez de X, etc. Como X é finito e $V \neq \{\vec{0}\}$, o processo termina ao fim de i passos com X_i um conjunto linearmente independente e gerador de V. □

Exemplo 3.35. Seja $V \subset \mathbb{F}_3^4$ o espaço gerado pelo conjunto $\{(0,1,2,1),(1,0,2,2),(1,2,0,1)\}$. Vamos determinar uma base para V. Uma vez que $\mathbb{F}_3$ é um corpo tal como $\mathbb{R}$, o método de eleminação de Gauss continua a ser válido. Aplicando então o método de eleminação de Gauss à matriz (de entradas em $\mathbb{F}_3$) cujas linhas são os vectores do conjunto dado, fica

$$\begin{bmatrix} 1 & 0 & 2 & 2 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix} \xrightarrow{l_2 \mapsto l_2 - l_1} \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 1 & 2 & 1 \end{bmatrix} \xrightarrow{l_3 \mapsto l_3 + l_2} \begin{bmatrix} 1 & 0 & 2 & 2 \\ 0 & 2 & 1 & 2 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

portanto, olhando para a última matriz, conclui-se que $(0,1,2,1)$ é combinação linear de $(1,0,2,2)$ e $(1,2,0,1)$. Conclui-se ainda que $\{(1,0,2,2),(1,2,0,1)\}$ é uma base para V.

Observação 3.36. Tal como no exemplo anterior, assumimos os resultados de Álgebra Linear sobre matrizes reais, generalizados para matrizes de entradas nun corpo $\mathbb{F}$ qualquer, cujas demonstrações usam apenas as propriedades de corpo do conjunto dos reais $\mathbb{R}$. Por exemplo: relação entre colunas/linhas linearmente independentes de uma matriz com os pivots no final da eliminação de Gauss, cálculo do determinante através da regra de Laplace, cálculo da matriz inversa (e a sua existência) usando a matriz dos cofactores ou o método de eliminação de Gauss, etc.

Teorema 3.37. *Seja $V \neq \{\vec{0}\}$ um espaço vectorial finito sobre $\mathbb{F}_q$. Então*

(i) Fixada uma base $\mathcal{B} = \{v_1, \ldots, v_r\}$ de V, qualquer vector $v \in V$ se escreve de maneira <u>única</u> como combinação linear dos vectores da base $\mathcal{B}$, i.e.,

$$\forall\, v \in V \quad \exists!\, a_1, \ldots, a_r \in \mathbb{F}_q \quad \textit{tais que} \quad v = a_1 v_1 + \cdots + a_r v_r \ .$$

(ii) Qualquer base de V tem o mesmo número de elementos.

Definição 3.38. A *dimensão* do espaço vectorial $V \subset \mathbb{F}_q^n$ é o número de elementos de uma base de V, se $V \neq \{\vec{0}\}$, e $\dim(V) = 0$ se V é o espaço nulo.

Note que o Teorema 3.37 garante que a definição anterior não depende da base escolhida para V.

Exemplo 3.39. Consideremos novamente os espaços V_1, V_2 e V_3 do Exemplo 3.31. Então, pelo que foi dito no Exemplo 3.33, $\dim(V_1) = 1$, $\dim(V_2) = 2$ e $\dim(V_3) = 1$.

Tratando-se de um espaço vectorial finito, não é sempre necessário determinar uma base para para calcular a sua dimensão.

Seja $V \neq \{\vec{0}\}$ um subespaço vectorial de $\mathbb{F}_q^n$ e seja k a sua dimensão, que queremos determinar. Também sabemos que V possui uma base com k vectores, e designemos por $v_1, \ldots, v_k$ os vectores dessa base. Quantos elementos é que V contém? Como qualquer $v \in V$ se escreve de maneira única como uma combinação linear de $v_1, \ldots, v_k$ (pelo Teorema 3.37 (i)), então escolhas diferentes de coeficientes escalares dão origem a vectores distintos de V, i.e,

$$a_1 v_1 + \cdots + a_k v_k = b_1 v_1 + \cdots + b_k v_k \ ,$$

com $a_1, \ldots, a_k, b_1, \ldots, b_k \in \mathbb{F}_q$, se e só se $a_i = b_i$ para $i = 1, \ldots, k$. Ou seja V contém exactamente q^k vectores, onde $k = \dim V$. Assim, provámos que o número de elementos em V é uma potência de $q = |\mathbb{F}_q|$ e que a sua dimensão é

$$\boxed{\dim V = \log_q(\#V)} \ . \tag{3.4}$$

Já agora repare que a fórmula (3.4) também é válida quando V é o espaço nulo.

Definição 3.40. Sejam $u, v \in \mathbb{F}_q^n$, de coordenadas $u = (u_1, \ldots, n_n)$ e $v = (v_1, \ldots, v_n)$.

(i) O *produto interno euclideano* dos vectores u e v é o escalar $u \cdot v = u_1v_1 + \cdots + u_nv_n \in \mathbb{F}_q$.

(ii) Dizemos que u é *ortogonal* a v, e escrevemos $u \perp v$, se e só se $u \cdot v = 0$.

Proposição 3.41. *Para quaisquer vectores $u, v, w \in \mathbb{F}_q^n$ e escalares $a, b \in \mathbb{F}_q$, verifica-se*

(i) $u \cdot v = v \cdot u$ *(simetria)*

(ii) $(au + bv) \cdot w = a(u \cdot w) + b(v \cdot w)$ *(linearidade)*

(iii) $u \cdot v = 0$ *para todo o* $u \in \mathbb{F}_q^n$ *se e só se* $v = \vec{0}$ *(não degenerescência)*

Dem. As alíneas (i) e (ii) provam-se aplicando directamente a definição do produto interno euclideano e usando as propriedades de comutatividade e distributividade do corpo $\mathbb{F}_q$.

Na alínea (iii), se $v = \vec{0}$ então, usando outra vez a definição de produto interno, tem-se claramente que $u \cdot v = 0$. Reciprocamente, suponhamos que $v \neq \vec{0}$. Então existe uma coordenada i tal que $v_i \neq 0$. Seja u o vector com todas as coordenadas nulas excepto $u_i = 1$. Então $u \cdot v = u_iv_i = v_i \neq 0$. □

Atenção! Não é verdade, em geral, que $v \cdot v = 0$ apenas para o vector nulo $v = \vec{0}$. Por exemplo, em $\mathbb{F}_3^4$, se $v = (1, 0, 2, 1)$ então $v \cdot v = 1^2 + 0 + 2^2 + 1^2 = 1 + 0 + 1 + 1 = 0$ (as operações são feitas em $\mathbb{F}_3$). Este comportamento "estranho" deve-se ao facto dos corpos finitos $\mathbb{F}_q$ terem característica não nula.

Há outros produtos internos com interesse na Teoria de Códigos (ver o Exercício 3.17 para um exemplo), por isso damos aqui a definição geral.

Definição 3.42. Um *produto interno* em $\mathbb{F}_q^n$ é uma aplicação $\langle \cdot, \cdot \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$ tal que

(i) $\langle u + v, w \rangle = \langle u, w \rangle + \langle v, w \rangle$,

(ii) $\langle u, v + w \rangle = \langle u, v \rangle + \langle u, w \rangle$,

(iii) $\langle u, v \rangle = 0 \quad \forall\, u \in \mathbb{F}_q^n$ se e só se $v = \vec{0}$ e

(iv) $\langle u, v \rangle = 0 \quad \forall\, v \in \mathbb{F}_q^n$ se e só se $u = \vec{0}$,

para quaisquer vectores $u, v, w \in \mathbb{F}_q^n$.

Mas, por defeito, usaremos o produto interno euclideano.

Definição 3.43. Seja V um subespaço vectorial de $\mathbb{F}_q^n$. O *complemento ortogonal* de V é o conjunto $V^\perp = \{w \in \mathbb{F}_q^n \,:\, w \cdot v = 0 \quad \forall\, v \in V\}$.

Note que, tal como no caso dos subespaços de $\mathbb{R}^n$, na definição de $V^\perp$ basta verificar a condição de ortogonalidade para os vectores v numa base de V, porque o produto interno euclideano é linear.

Teorema 3.44. *Seja V um subespaço de $\mathbb{F}_q^n$. Então o complemento ortognal $V^\perp$ é também um subespaço de $\mathbb{F}_q^n$ e*

$$\dim V + \dim V^\perp = n \ . \tag{3.5}$$

Dem. Se V é o espaço nulo, então $V^\perp = \mathbb{F}_q^n$ e o teorema é válido. Suponhamos agora que $V \neq \{\vec{0}\}$. Seja $k = \dim V$ e seja $\{v_1, \ldots, v_k\}$ uma base de V. Como o produto interno é linear, se $x, y \in V^\perp$ e $a, b \in \mathbb{F}_q$, então

$$(ax + by) \cdot v_i = a(x \cdot v_i) + b(y \cdot v_i) = 0, \qquad \text{para} \quad i = 1, \ldots, k \ ,$$

donde se conclui que $ax + by \in V^\perp$, logo $V^\perp$ é um subespaço vectorial de $\mathbb{F}_q^n$.

Se escrevermos as igualdades $v_1 \cdot x = \cdots = v_k \cdot x = 0$ em notação matricial, ficamos com $V^\perp = \mathcal{N}(A)$, onde A é a matriz $k \times n$ cuja linha i é formada pelas coordenadas do vector v_i:

$$A = \begin{bmatrix} \text{——} & v_1^T & \text{——} \\ & \vdots & \\ \text{——} & v_k^T & \text{——} \end{bmatrix}_{k \times n}$$

(v_1^T designa o transposto[5] de v_1.) Portanto, a dimensão de $V^\perp$ é o número de variáveis livres no sistemas de equações $Ax = 0$, que é igual à diferença entre o número de colunas de A e o número de linhas linearmente independentes. Neste caso fica $\dim V^\perp = n - k = n - \dim V$. □

ATENÇÃO! Contrariamente ao que estamos habituados no caso real, não é verdade que $V \oplus V^\perp = \mathbb{F}_q^n$ para todo o subespaço $V \subset \mathbb{F}_q^n$.

Recorde que a *soma* de dois subespaços $V, W \subset \mathbb{F}_q^n$ é definida por

$$V + W = \{v + w \in \mathbb{F}_q^n \,:\, v \in V, w \in W\} \tag{3.6}$$

e é um subespaço de $\mathbb{F}_q^n$. Quando se verifica que $V \cap W = \{\vec{0}\}$, dizemos que o espaço soma é a *soma directa* de V e W e escrevemos $V \oplus W$. Assim, $\mathbb{F}_q^n = V \oplus W$ se e só se $\mathbb{F}_q^n = V + W$ e ainda $V \cap W = \{\vec{0}\}$. Recorde ainda que a intersecção $V \cap W$ dos subespaços V e W é sempre um espaço vectorial – ver Exercício 3.16.

Exemplo 3.45. $\{\vec{0}\}^\perp = \mathbb{F}_q^n$ e, neste caso, tem-se trivialmente a decomposição em soma directa $\{\vec{0}\} \oplus \{\vec{0}\}^\perp = \mathbb{F}_q^n$.

Exemplo 3.46. Seja $V = \langle (1,1,1,1) \rangle \subset \mathbb{F}_2^4$. Então $V^\perp = \{x \in \mathbb{F}_2^4 \,:\, \mathrm{w}(x) \text{ é par}\}$, porque $x \in V^\perp$ se e só se $x \cdot (1,1,1,1) = 0$ se e só se $x_1 + x_2 + x_3 + x_4 = 0$ em $\mathbb{F}_2$, i.e., se e só se $\mathrm{w}(x) = x_1 + x_2 + x_3 + x_4 \equiv 0 \pmod 2$.

Da equação $x_1 + x_2 + x_3 + x_4 = 0$, ou $x_1 = x_2 + x_3 + x_4$, que descreve $V^\perp$, também se tira que $\{(1,1,0,0), (1,0,1,0), (1,0,0,1)\}$ é uma base de $V^\perp$ – o primeiro vector é obtido subtituindo $x_2 = 1$ e $x_3 = x_4 = 0$, o segundo substituindo $x_3 = 1$ e $x_2 = x_4 = 0$, etc.

Quanto às dimensões, temos que $\dim V = 1$, pois V é gerado por um único vector não nulo, nomeadamente $(1,1,1,1)$, e $\dim V^\perp = 3$, aplicando o Teorema 3.44 ou directamente da definição de dimensão, uma vez que já temos uma base para $V^\perp$.

Mas como $(1,1,1,1) \in V^\perp$, porque o seu peso é 4, conclui-se que $\boxed{V \subset V^\perp}$.

Exemplo 3.47. Seja V o subespaço de $\mathbb{F}_2^4$ gerado pelos vectores $u = (1,0,1,0)$ e $v = (0,1,0,1)$. Como u e v são linearmente independentes (já visto num exemplo anterior), conclui-se que V tem dimensão 2. Calculemos o complemento ortogonal $V^\perp$. Usando a definição

$$\begin{aligned} V^\perp &= \{x \in \mathbb{F}_2^4 \,:\, x \cdot u = 0,\, x \cdot v = 0\} \\ &= \{(x_1, x_2, x_3, x_4) \in \mathbb{F}_2^4 \,:\, x_1 = x_3,\, x_2 = x_4\} \,, \end{aligned}$$

donde se conclui que $V^\perp = \langle (1,0,1,0), (0,1,0,1) \rangle$, ou seja, $\boxed{V = V^\perp}$.

Teorema 3.48. *Seja V um subespaço vectorial de $\mathbb{F}_q^n$. Então $(V^\perp)^\perp = V$.*

Dem. 1º PASSO: Mostrar que $V \subset (V^\perp)^\perp$.

Seja $v \in V$. Então, para todo o $w \in V^\perp$ verifica-se $v \cdot w = 0$ (pela definição de $V^\perp$), mas isto também quer dizer que $v \in (V^\perp)^\perp$.

2º PASSO: Comparar dimensões.

Aplicando o Teorema 3.37 duas vezes, fica

$$\dim (V^\perp)^\perp = n - \dim V^\perp = n - (n - \dim V) = \dim V \,.$$

Logo, os espaços vectoriais V e $(V^\perp)^\perp$ têm o mesmo número de elementos (justifique), e como um é subconjunto do outro (pelo 1º passo), conclui-se que são iguais. □

[5] Em notação matricial, identificamos vectores com matrizes colunas. Assim, se v é um vector ou uma coluna, o seu transposto v^T é uma linha.

Exercícios

3.1. (a) Verifique que as tabelas dos Exemplos 3.21 e 3.22 estão correctas.
(b) Determine um isomorfismo (de anéis) entre $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ e $\mathbb{F}_2[t]/\langle t^2+t\rangle$.

3.2. Determine um elemento primitivo de cada um dos seguintes corpos: $\mathbb{F}_5$, $\mathbb{F}_{11}$ e $\mathbb{F}_{13}$.

3.3. Construção do corpo $\mathbb{F}_{16}$:
(a) Verifique que o polinómio t^4+t+1 é irredutível em $\mathbb{F}_2[t]$.
(b) Construa então $\mathbb{F}_{16} = \mathbb{F}_2[t]/\langle t^4+t+1\rangle$ idenficando os seus elementos e esboçando as respectivas tabelas de adição e multiplicação. Identifique um elemento primitivo deste corpo. Sugestão: na Observação 3.28, use (3.2) para descrever a soma e (3.3) para descrever o produto de dois elementos. Portanto, em vez de escrever duas tabelas de 16×16 precisa apenas de uma correspondência entre (3.2) e (3.3), identificando primeiro um elemento primitivo $\alpha \in \mathbb{F}_{16}$.

3.4. Escreva todos os polinómios irredutíveis em $\mathbb{F}_2[t]$ de graus 2, 3 e 4.

3.5. Seja $I(p,n)$ o número de polinómios mónicos irredutíveisde de grau n em $\mathbb{F}_p[t]$.
(a) Mostre que $I(p,2) = \binom{p}{2}$.
(b) Mostre que $I(p,3) = \frac{p(p^2-1)}{3}$.
(c) Estude a Secção 2.2 do Apêndice A para a demonstração de uma fórmula para $I(p,n)$.

3.6. Seja $\mathbb{F}$ um corpo de característica p, onde p é um número primo. Mostre que $\mathbb{F}$ é um espaço vectorial sobre $\mathbb{F}_p$. Conclua que a ordem de qualquer corpo finito é uma potência de um número primo.

3.7. (a) Justifique que os polinómios t^3+t+1 e t^3+t^2+1 são irredutíveis em $\mathbb{F}_2[t]$.
(b) Justifique que os quocientes $A = \mathbb{F}_2[t]/\langle t^3+t+1\rangle$ e $B = \mathbb{F}_2[t]/\langle t^3+t^2+1\rangle$ são ambos isomorfos ao corpo $\mathbb{F}_8$, e determine um isomorfismo $\phi : A \longrightarrow B$.
Sugestão: seja $\alpha \in A$ uma raiz de $1+t+t^3$ e $\beta \in B$ uma raiz de $1+t^2+t^3$. Encontre uma relação entre α e β ou, mais precisamente, determine uma raiz de $1+t^2+t^3$ em A.
(c) Para a descrição A de $\mathbb{F}_8$, determine um elemento primitivo. Justifique ainda que A é um espaço vectorial sobre $\mathbb{F}_2$ e indique uma base.

3.8. Seja V um subespaço vectorial de $\mathbb{F}_q^n$ de dimensão k, com $1 \le k \le n$.
(a) Quantos vectores contém V?
(b) Quantas bases diferentes tem V?

3.9. (a) Calcule o número de matrizes quadradas não singulares[6] $n \times n$ com entradas num corpo finito $\mathbb{F}_q$.
(b) Qual é a probabilidade $P(q,n)$ de uma matriz quadrada $n \times n$ sobre $\mathbb{F}_q$ ser não singular?

3.10. Considere o espaço vectorial $\mathbb{F}_q^n$ sobre $\mathbb{F}_q$. Designando por $\begin{bmatrix} n \\ k \end{bmatrix}_q$ o número de subspaços de dimensão k de $\mathbb{F}_q^n$:
(a) Mostre que
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)} \ .$$
(b) Mostre que
$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q \ .$$
(c) Justifique que
$$\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k} \ .$$

[6] Recorde que uma matriz quadrada A, com entradas num corpo qualquer, é não singular, ou invertível, se e só se $\det(A) \neq 0$ se e só se as suas colunas (ou linhas) são linearmente independentes.

3.11. (a) Mostre que $\mathbb{F}_{q^m}$ é um espaço vectorial sobre $\mathbb{F}_q$, com a soma e o produto por um escalar definidos à custa das operações em $\mathbb{F}_{q^m}$.
(b) Seja $f(t) \in \mathbb{F}_q[t]$ um polinómio de grau m, irredutível em $\mathbb{F}_q[t]$, e seja $\alpha \in \mathbb{F}_{q^m}$ uma raiz de $f(t)$. Mostre que $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ é uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$.

3.12. Seja V um espaço vectorial de dimensão finita sobre $\mathbb{F}_{q^m}$.
(a) Mostre que V é também um espaço vectorial sobre $\mathbb{F}_q$ e

$$\dim_{\mathbb{F}_q}(V) = m \dim_{\mathbb{F}_{q^m}}(V) \ ,$$

onde $\dim_{\mathbb{F}}(V)$ designa a dimensão de V como espaço vectorial sobre o corpo $\mathbb{F}$.
(b) Seja $\{v_1, \ldots, v_k\}$ uma base de V sobre $\mathbb{F}_{q^m}$ e $\{\alpha_1, \ldots \alpha_m\}$ uma base de $\mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. Mostre que $\{\alpha_i v_j \ : \ i = 1, \ldots, m \, ; \, j = 1, \ldots, k\}$ é uma base de V sobre $\mathbb{F}_q$.

3.13. (a) Demonstre a *Fórmula do Caloiro*: $(a+b)^p = a^p + b^p$, para quaisquer $a, b \in \mathbb{F}_q$, onde p é a característica de $\mathbb{F}_q$.
(b) Mostre que $(a+b)^{q^i} = a^{q^i} + b^{q^i}$ para quaisquer $a, b \in \mathbb{F}_{q^m}$ e $i \in \mathbb{N}$.
(c) Justifique que, para qualquer $a \in \mathbb{F}_{q^m}$, $a \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$ se e só se $a^q = a$.
(d) Para cada $x \in \mathbb{F}_{q^m}$, definimos o seu traço por $\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}$. Mostre que $\mathrm{Tr}(x) \in \mathbb{F}_q$ para todo o $x \in \mathbb{F}_{q^m}$.
(e) Mostre que $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$, $x \longmapsto \mathrm{Tr}(x)$, é uma aplicação linear sobre $\mathbb{F}_q$.

3.14. Considere $\mathbb{F}_{16} = \mathbb{F}_2[t]/\langle t^4 + t + 1 \rangle$, i.e., $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$ onde $\alpha^4 = \alpha + 1$.
(a) Identifique $\mathbb{F}_4$ como subcorpo de $\mathbb{F}_{16}$.
Sugestão: poderá querer usar a alínea (c) do Exercício 3.13.
(b) Determine um polinómio $f(t) \in \mathbb{F}_4[t]$ tal que $\mathbb{F}_{16} = \mathbb{F}_4[t]/\langle f(t) \rangle$.
(c) Será $\mathbb{F}_8$ um subcorpo de $\mathbb{F}_{16}$? Justifique.

3.15. Dados dois corpos $\mathbb{F}_{q^m}$ e $\mathbb{F}_{q^n}$, com $m > n$, quando é que $\mathbb{F}_{q^n}$ é subcorpo de $\mathbb{F}_{q^m}$?

3.16. Sejam V e W subespaços de $\mathbb{F}_q^n$. Mostre que a soma $V + W$, definida em (3.6), e a intersecção $V \cap W$ são espaços vectoriais. Mostre ainda que a soma $V + W$ é o espaço vectorial gerado por V e W.

3.17. Considere a aplicação $\langle \cdot, \cdot \rangle_H : \mathbb{F}_{q^2}^n \times \mathbb{F}_{q^2}^n \longrightarrow \mathbb{F}_{q^2}$ definida por

$$\langle u, v \rangle_H = \sum_{i=1}^{n} u_i v_i^q \ ,$$

onde $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^2}^n$. Mostre que $\langle \cdot, \cdot \rangle_H$ é um produto interno em $\mathbb{F}_{q^2}^n$. Nota: $\langle \cdot, \cdot \rangle_H$ diz-se o *produto interno hermítico*. O *dual hermítico* do espaço vectorial C é definido por

$$C^{\perp_H} = \{v \in \mathbb{F}_{q^2}^n \ : \ \langle v, c \rangle_H = 0 \quad \forall \, c \in C\} \ .$$

3.18. Recorde que $\mathbb{F}_4 = \mathbb{F}_2[t]/\langle t^2 + t + 1 \rangle = \{0, 1, \alpha, \alpha^2\}$, onde α é uma raiz de $t^2 + t + 1 \in \mathbb{F}_2[t]$. Mostre que os seguintes espaços vectoriais sobre $\mathbb{F}_4$ são auto-duais em relação ao produto interno hermítico definido no problema anterior:
(a) $C_1 = \langle (1, 1) \rangle \subset \mathbb{F}_4^2$,
(b) $C_2 = \langle (1, 0, 0, 1, \alpha, \alpha), (0, 1, 0, \alpha, 1, \alpha), (0, 0, 1, \alpha, \alpha, 1) \rangle \subset \mathbb{F}_4^6$.
Serão estes espaços vectoriais auto-duais em relação ao produto interno euclideano?

Códigos Lineares

1. Definição, pârametros e peso mínimo

Seja $\mathbb{F}_q$ o corpo de ordem q.

Definição 4.1.
- Um *código linear* q-ário, de comprimento n, é um subespaço vectorial de $\mathbb{F}_q^n$.
- Se C é um código linear, $C^\perp$ diz-se o *código dual* de C.
- Se $C = C^\perp$, C diz-se um *código auto-dual*.
- Se $C \subset C^\perp$, C diz-se um *código auto-ortogonal*.

O espaço vectorial do Exemplo 3.47, do capítulo anterior, é um código auto-dual, e o do Exemplo 3.46 é auto-ortogonal.

Exemplo 4.2. O código de repetição q-ário de parâmetros $(n, q, n)_q$ é linear. É o subespaço de $\mathbb{F}_q^n$ gerado pelo vector $\vec{1} = (1, \ldots, 1)$, i.e., $C = \langle \vec{1} \rangle \subset \mathbb{F}_q^n$. O código dual de C é

$$C^\perp = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n \, : \, \sum_{i=1}^{n} x_i = 0\} \, .$$

Para $q = 2$, obtém-se o código dos pesos pares $C^\perp = \{x \in \mathbb{F}_2^n \, : \, \mathrm{w}(x) \text{ é par}\}$, também denotado por E_n (de "even").

Proposição 4.3. *Seja C um código linear de comprimento n sobre $\mathbb{F}_q$. Então*

(i) $|C| = q^{\dim C}$, *i.e.,* $\dim C = \log_q |C|$

(ii) $\dim C + \dim C^\perp = n$

(iii) $(C^\perp)^\perp = C$

Esta proposição já foi demonstrada no capítulo anterior – ver fórmula (3.4) e Teoremas 3.44 e 3.48.

Como o número de palavras que C contém está directamente relacionado com a sua dimensão, definimos que os parâmetros de um código linear são $[n, k, d]_q$ (ou simplesmente $[n, k, d]$, ou ainda apenas $[n, k]$), onde $k = \dim C$, e n e d são respectivamente o comprimento e a distância mínima, como anteriormente. Portanto, um código linear $[n, k, d]_q$ é também um código $(n, q^k, d)_q$.

Recorde que qualquer código, linear ou não, é equivalente a outro contendo a palavra (vector) $\vec{0} \in \mathbb{F}_q^n$, pelo Lema 2.6. No caso de um código linear, este contém necessariamente o vector nulo.

Definição 4.4. Seja C um código qualquer, não necessarimanete linear. Definimos o *peso mínimo* de C por

$$\mathrm{w}(C) = \min\{\mathrm{w}(x) \, : \, x \in C \setminus \{\vec{0}\}\} \, ,$$

se $C \neq \{\vec{0}\}$, e $\mathrm{w}(C) = 0$ se $C = \{\vec{0}\}$.

Teorema 4.5. *Seja $C \neq \{\vec{0}\}$ um código linear. Então* $\mathrm{d}(C) = \mathrm{w}(C)$.

Dem. Como $C \neq \{\vec{0}\}$, C contém pelo menos duas palavras e, de acordo com a definição de distância mínima, $\mathrm{d}(C) = \min\{\mathrm{d}(x,y) : x,y \in C, x \neq y\}$. Sejam então $x, y \in C$ tais que $\mathrm{d}(x,y) = \mathrm{d}(C)$. Portanto

$$\mathrm{d}(C) = \mathrm{d}(x,y) = \mathrm{w}(x-y) \geq \mathrm{w}(C) \ .$$

Na desigualdade usou-se o facto de $x - y \in C$, por C ser linear, e $x - y \neq \vec{0}$.

Seja agora $x \in C$ tal que $\mathrm{w}(x) = \mathrm{w}(C)$. Portanto

$$\mathrm{w}(C) = \mathrm{w}(x) = \mathrm{d}(x, \vec{0}) \geq \mathrm{d}(C) \ .$$

Na desigualdade usou-se o facto de $\vec{0} \in C$, por C ser linear. □

Por definição, para calcular a distância mínima $\mathrm{d}(C)$ de um código C contendo M palavras é preciso calcular a distância $\mathrm{d}(x,y)$ para $\binom{M}{2} = \frac{M(M-1)}{2}$ pares de palavras. Se C é linear, o teorema anterior diz-nos que basta calcular o peso $\mathrm{w}(x)$ de $M-1$ palavras.

Exemplo 4.6. Continuação do Exemplo 4.2. O código de repetição $C \subset \mathbb{F}_q^n$ tem dimensão 1. Como $\mathrm{w}(x) = n$ para qualquer palavra de código $x \in C \setminus \{\vec{0}\}$, então $\mathrm{d}(C) = n$. Portanto C é um código q-ário $[n, 1, n]$. Com $q = 2$ e $n \geq 2$, $E_n = C^\perp$, logo $\dim E_n = n - 1$. Também se tem que $\mathrm{w}(x)$ é par para qualquer $x \in E_n$. Por outro lado $(1, 1, 0, \ldots, 0) \in E_n$ e tem peso 2. Logo o peso mínimo é $\mathrm{w}(E_n) = 2$ e E_n é um código binário de parâmetros $[n, n-1, 2]$.

2. Matriz geradora e matriz de paridade

Definição 4.7. Seja C um código q-ário $[n,k]$.

- Se $\{v_1, \ldots, v_k\}$ é uma base de C, a matriz
$$G = \begin{bmatrix} \text{——} & v_1^T & \text{——} \\ & \vdots & \\ \text{——} & v_k^T & \text{——} \end{bmatrix}$$
diz-se uma *matriz geradora* de C.
- H diz-se uma *matriz de paridade* de C se é uma matriz geradora do código dual $C^\perp$.

Em particular, $\dim C > 0$ para haver uma matriz geradora, e $\dim C < n$ para haver uma matriz de paridade.

Note-se que uma matriz geradora tem k linhas e n colunas, e uma matriz de paridade tem $n-k$ linhas e também n colunas.

Observação 4.8. Da definição de matriz geradora G e de paridade H, tem-se que C é o espaço das linhas de G e é também o núcleo de H. Analogamente, o código dual $C^\perp$ é o espaço das linhas de H e o núcleo de G.

Exemplo 4.9. $G = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix}$ é uma matriz geradora do código de repetição $C \subset \mathbb{F}_5^4$. Por definição de complemento ortogonal,

$$\begin{aligned} C^\perp &= \{x \in \mathbb{F}_5^4 : x \cdot \vec{1} = 0\} \\ &= \{(x_1, x_2, x_3, x_4) : x_1 + x_2 + x_3 + x_4 = 0\} \\ &= \{(-x_2 - x_3 - x_4, x_2, x_3, x_4) : x_2, x_3, x_4 \in \mathbb{F}_5\} \end{aligned}$$

logo $\{(4,1,0,0), (4,0,1,0), (4,0,0,1)\}$ é uma base de $C^\perp$ e

$$H = \begin{bmatrix} 4 & 1 & 0 & 0 \\ 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz de paridade para C.

Exemplo 4.10. Qualquer matriz $n \times n$, não singular[1], G é uma matriz geradora do código $\mathbb{F}_q^n$. Em particular, podemos escolher $G = I_n$, a matriz identidade.

Definição 4.11. Seja C um código linear de dimensão k e comprimento n.

- Uma matriz geradora $G_{k\times n}$ do código C diz-se na *forma canónica* se $G = \begin{bmatrix} I_k & A \end{bmatrix}$, onde A é uma matriz $k \times (n-k)$.
- Uma matriz de paridade $H_{(n-k)\times n}$ do código C diz-se na *forma canónica* se $H = \begin{bmatrix} B & I_{n-k} \end{bmatrix}$, onde B é uma matriz $(n-k) \times k$.

Lema 4.12. *Seja C um código $[n,k]$ sobre $\mathbb{F}_q$ com matriz geradora G. Então H é uma matriz de paridade para C se e só se $HG^T = 0$ e as linhas de H são linearmente independentes.*

Dem. Seja $\{v_1, \ldots, v_k\}$ a base de C obtida à custa da matriz geradora G, mais precisamente, o vector v_j é a linha j de G. Sejam $w_1, \ldots, w_{n-k}$ as linhas da matriz H. Então, a entrada (i,j) da matriz produto HG^T é $w_i v_j$, que podemos ainda escrever como o produto interno $w_i \cdot v_j$ dos vectores $w_i, v_j \in \mathbb{F}_q^n$.
($\Longrightarrow$) Se H é uma matriz de paridade de C, as suas linhas são linearmente independentes, por definição de matriz de paridade, e $w_i \cdot v_j = 0$ para todo o i e j porque $w_i \in C^\perp$ e $v_j \in C$. Donde sai que $HG^T = 0$.
($\Longleftarrow$) Seja C' o espaço das linhas de H. Então $\dim C' = n-k$ porque as linhas de H são linearmente independentes. Como $w_i \cdot v_j = 0$ para quaisquer i, j (estamos a assumir que $HG^T = 0$) e o conjunto $\{v_1, \ldots, v_k\}$ é uma base de C, conclui-se que C' é um subespaço de $C^\perp$. Mas como C' e $C^\perp$ têm ambos dimensão $n-k$, temos necessariamente que $C' = C^\perp$ e, portanto, H é uma matriz de paridade de C. □

No enunciado, a igualdade $HG^T = 0$ é equivalente a $GH^T = 0$, pois $(AB)^T = B^T A^T$, $(A^T)^T$ e a transposta de uma matriz nula é ainda uma matriz nula.

Se aplicarmos o lema anterior ao código dual $C^\perp$ obtém-se o resultado análogo para matrizes geradoras:

Lema 4.13. *Seja C um código $[n,k]$ sobre $\mathbb{F}_q$ com matriz de paridade H. Então G é uma matriz geradora de C se e só se $HG^T = 0$ e as linhas de G são linearmente independentes.*

Teorema 4.14. *Seja C um código $[n,k]_q$ com uma matriz geradora $G = \begin{bmatrix} I_k & A \end{bmatrix}$ na forma canónica. Então $H = \begin{bmatrix} -A^T & I_{n-k} \end{bmatrix}$ é uma matriz de paridade na forma canónica para C.*

Dem. Como as últimas $n-k$ colunas de H formam a matriz identidade, tem-se imediatamente que as linhas de H são linearmente independentes. Calculando o produto HG^T fica

$$HG^T = \begin{bmatrix} -A^T & I_{n-k} \end{bmatrix} \begin{bmatrix} I_k \\ A^T \end{bmatrix} = -A^T I_k + I_{n-k} A^T = -A^T + A^T = 0 \ .$$

Aplicando o Lema 4.12, conclui-se que H é de facto uma matriz de paridade para C. □

Como consequência, tendo uma matriz geradora G na forma canónica, obtemos directamente uma base para o código dual, nomeadamente, as linhas da matriz de paridade associada a G.

Exemplo 4.15. Seja C o código binário linear gerado pelo conjunto

$$S = \{11101, 10110, 01011, 11010\} \ .$$

Vamos determinar uma matriz geradora e uma de paridade para C. Seja M a matriz cujas linhas são os vectores do conjunto S, e apliquemos o método de eliminação de Gauss a M:

$$M = \begin{bmatrix} 1&1&1&0&1 \\ 1&0&1&1&0 \\ 0&1&0&1&1 \\ 1&1&0&1&0 \end{bmatrix} \overset{\substack{l_2 \mapsto l_2+l_1 \\ l_4 \mapsto l_4+l_1}}{\longrightarrow} \begin{bmatrix} 1&1&1&0&1 \\ 0&1&0&1&1 \\ 0&1&0&1&1 \\ 0&0&1&1&1 \end{bmatrix} \overset{l_3 \mapsto l_3+l_2}{\longrightarrow} \begin{bmatrix} 1&1&1&0&1 \\ 0&1&0&1&1 \\ 0&0&0&0&0 \\ 0&0&1&1&1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1&1&1&0&1 \\ 0&1&0&1&1 \\ 0&0&1&1&1 \\ 0&0&0&0&0 \end{bmatrix}$$

[1] Recorde da cadeira de Álgebra Linear que uma matriz quadrada é *não singular* se e só se tem determinante não nulo.

Daqui já podemos concluir que $\dim C = 3$, pois há apenas três linhas de M linearmente independentes. Continuando a eliminação de Gauss a partir da última matriz obtida, mas agora "de baixo para cima", de modo a tentar obter a matriz identidade no canto superior esquerdo da matriz, fica

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{l_1 \mapsto l_1+l_2+l_3} \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} = \overline{M}$$

Como a matriz $\overline{M}$ foi obtida de M aplicando apenas operações nas linhas (i.e., não houve trocas de colunas), M e $\overline{M}$ têm o mesmo espaço de linhas. Portanto

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

é uma matriz geradora do código C e está na forma canónica, logo

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

é uma matriz de paridade para C e está na forma canónica. Aplicou-se o Teorema 4.14 a G para obter H.

Teorema 4.16. *Seja C um código $[n,k]$ sobre $\mathbb{F}_q$, com matriz de paridade H. Então*

(i) $\mathrm{d}(C) \geq d$ *se e só se quaisquer $d-1$ colunas de H são linearmente independentes,*

(ii) $\mathrm{d}(C) \leq d$ *se e só se existem d colunas de H linearmente dependentes.*

Dem. Pelo Teorema 4.5, sabemos que $\mathrm{d}(C) = \mathrm{w}(C)$. Designemos por $c_1, \ldots, c_n$ as colunas da matriz de paridade H. Seja $x = (x_1, \ldots, x_n)$ uma palavra do código $C \subset \mathbb{F}_q^n$ com peso $\mathrm{w}(x) = e > 0$ e suponhamos que as componentes de x não nulas se encontram nas coordenadas $i_1, \ldots, i_e$. Como $C = \mathcal{N}(H)$, temos

$$\begin{aligned} x \in C &\iff Hx = \vec{0} \\ &\iff \sum_{i=1}^{n} x_i c_i = \vec{0} \\ &\iff x_{i_1} c_{i_1} + \cdots + x_{i_e} c_{i_e} = \vec{0} \qquad \text{com } x_{i_1}, \ldots, x_{i_e} \neq 0 \\ &\iff \text{existem } e = \mathrm{w}(x) \text{ colunas de } H \text{ linearmente dependentes.} \qquad (*) \end{aligned}$$

(i) Por definição de peso mínimo, $\mathrm{w}(C) \geq d$ se e só se $\mathrm{w}(x) \geq d$ para todas as palavras de código $x \in C \setminus \{\vec{0}\}$, ou seja, se e só se C não contém nenhuma palavra x não nula com peso $\mathrm{w}(x) \leq d-1$. Esta última afirmação é ainda equivalente a dizer que, por $(*)$, quaisquer $d-1$ colunas de H são linearmente independentes.

(ii) Analogamente à alínea (i), $\mathrm{w}(C) \leq d$ se e só se existe uma palavra não nula x do código C com $0 < \mathrm{w}(x) \leq d$, o que é equivalente, por $(*)$, a existir um conjunto linearmente dependente de d colunas de H. □

Juntando as duas afirmações deste teorema, podemos dizer que a distância mínima de um código linear C com matriz de paridade H é dada por

$$\boxed{\mathrm{d}(C) = \text{ número mínimo de colunas de } H \text{ linearmente dependentes}}\ .$$

Exemplo 4.17. Seja C o código linear binário com a seguinte matriz de paridade

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

Qual a distância mínima de C? Designemos por c_i a coluna i de H. Como H tem três linhas (ou seja, cada coluna é um vector em $\mathbb{F}_2^3$), quaisquer 4 colunas são linearmente dependentes, portanto, $\mathrm{d}(C) \leq 3$. Por outro lado

- como não há colunas nulas, qualquer coluna é linearmente independente,
- como não há colunas repetidas, i.e., como $c_i \neq c_j$ se $i \neq j$, então $c_i + c_j \neq \vec{0}$ para $i \neq j$, e quaisquer duas colunas são linearmente independentes,
- como $c_2 + c_4 + c_5 = \vec{0}$, há três colunas linearmente dependentes (também podiamos escolher $c_1 + c_2 + c_3 = \vec{0}$).

Donde se conclui, pelo Teorema 4.16, que $\mathrm{d}(C) = 3$.

3. Equivalência linear

Considere os três seguintes códigos ternários, de comprimento 3:

$$C_1 = \{000, 121, 212\}\ , \qquad C_2 = \{000, 111, 222\} \qquad \text{e} \qquad C_3 = \{001, 122, 210\}\ .$$

De acordo com a definição de equivalência dada no Capítulo 2 (ver Definição 2.4), estes três códigos são equivalentes entre si pois:

- C_2 é obtido de C_1 aplicando a permutação de símbolos $\pi_2 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{smallmatrix}\right)$ na segunda coordenada, e
- C_3 é obtido de C_2 aplicando a permutação de símbolos $\pi_3 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{smallmatrix}\right)$ na terceira coordenada.

No entanto, os códigos C_1 e C_2 são lineares, mas C_3 não é. Ou seja, a operação (ii) na Definição 2.4 nem sempre preserva a linearidade de um código. Interessa, portanto, restringir as operações permitidas na noção de equivalência já dada, de modo a se obter ainda códigos lineares.

Definição 4.18. Seja C um código linear q-ário $[n, k, d]$. C' diz-se um *código linearmente equivalente* a C se é obtido de C através da aplicação sucessiva das seguintes operações:

(i) permutar a ordem das coordenadas de todas as palavras do código, i.e., substituir todo o $c = c_1c_2\cdots c_n \in C$ por $(c_{\sigma(1)}, c_{\sigma(2)}, \ldots, c_{\sigma(n)})$, onde σ é uma permutação dos índices $\{1, 2, \ldots, n\}$;

(ii) multiplicar a coordenada i (fixa) de todas as palavras do código por um escalar não nulo $\lambda_i \in \mathbb{F}_q \backslash \{0\}$, mais precisamente, substituir todo o $c = c_1c_2\cdots c_n \in C$ por $(\lambda_1c_1, \lambda_2c_2, \ldots, \lambda_nc_n)$.

No exemplo do início desta secção, aplicar a permutação $\pi_2 = \left(\begin{smallmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{smallmatrix}\right)$ corresponde a multiplicar por $\lambda_2 = 2$. A permutação π_3 não corresponde à multiplicação por nenhum escalar, porque $\pi_3(0) \neq 0$.

Observação 4.19. As operações (i) e (ii) na Definição 4.18 podem ser traduzidas por aplicações lineares bijectivas:

(i) Dada uma permutação σ dos índices $\{1, \ldots, n\}$, seja P_σ a matriz cuja coluna i é o vector $\vec{e}_{\sigma(i)}$. Como σ é uma bijecção, P_σ é obtida da matriz identidade permutando colunas, portanto $\det(P_\sigma) = \pm 1 \neq 0$, donde concluímos que P_σ é invertível e

$$\begin{aligned} \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ x &\mapsto P_\sigma x = (x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) \end{aligned}$$

é uma aplicação linear bijectiva.

(ii) Dados $\lambda_i \in \mathbb{F}_q \setminus \{0\}$, para $i = 1, \ldots, n$, seja Λ a matriz diagonal com entradas $\lambda_1, \ldots, \lambda_n$ na diagonal principal. Portanto $\det(\Lambda) = \lambda_1 \cdots \lambda_n \neq 0$, donde concluímos que Λ é invertível e

$$\begin{aligned} \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ x &\mapsto \Lambda x = (\lambda_1 x_1, \lambda_2 x_2, \ldots, \lambda_n x_n) \end{aligned}$$

é uma aplição linear bijectiva.

Proposição 4.20. *Seja C um código linear e seja C' um código linearmente equivalente a C. Então, C' é também linear.*

Dem. Pela observação anterior, o código C' é a imagem de C por aplicacões lineares (correspondentes às operações (i) e (ii) de equivalência linear de códigos). Como a imagem de um subespaço linear por aplicações lineares é ainda um subespaço linear, concluímos que C' é um código linear. □

Teorema 4.21. *Qualquer código linear $C \neq \{\vec{0}\}$ é linearmente equivalente a outro com uma matriz geradora na forma canónica.*

Dem. Apenas fazemos um esboço da demonstração e deixamos como exercício justificar com detalhe todos os passos do argumento apresentado. Seja G uma matriz geradora de C. Se G não está na forma canónica, aplicamos o método de eleminação de Gauss, usando apenas operações nas linhas, e obtemos uma matriz $\bar{G}$ na forma

$$\bar{G} = \begin{bmatrix} 0 & \cdots & 0 & 1 & * & 0 & * & 0 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 1 & * & 0 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & * & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & \ddots & 0 & * \\ 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & * \end{bmatrix},$$

que ainda gera o mesmo código C, porque G e $\bar{G}$ têm exactamente o mesmo espaço de linhas. Permutando agora as colunas de $\bar{G}$ de modo a colocar os pivots nas primeiras colunas, obtém-se uma matriz geradora G' na forma canónica. O código C' gerado pelas linhas da matriz G' pode não ser igual a C, mas é certamente equivalente a este, pois permutar colunas numa matriz geradora corresponde a aplicar a operação (i) da definição de equivalência linear. □

Exemplo 4.22. Considere os códigos binários lineares $C = \langle 1100, 0011\rangle$ e $C' = \langle 1010, 0101\rangle$. As matrizes

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix} \qquad \text{e} \qquad G' = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$$

são matrizes geradoras de C e de C', respectivanemte. G' está na forma canónica. G não está, nem nenhuma outra matriz geradora de C está na forma canónica (justifique). Mas estes dois códigos são equivalentes: se aplicarmos a operacão (i) da Definição 4.18 a C com $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right)$ obtemos C'.

Exemplo 4.23. A forma canónica de uma matriz geradora pode não ser única: seja C o código binário com matriz geradora

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

Se aplicarmos a operação (i) da Definição 4.18 com $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 2 & 3 & 5 \end{smallmatrix}\right)$, obtemos um código C_1 com a seguinte matriz geradora

$$G_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

que está na forma canónica. Se usarmos a permutação $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 2 & 3 & 4 \end{smallmatrix}\right)$, obtemos um código C_2 com a seguinte matriz geradora

$$G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

que também está na forma canónica, mas $G_1 \neq G_2$.

4. Codificação e descodificação

4.1. Codificação sistemática

Seja C um código $[n, k]$ sobre $\mathbb{F}_q$. Como C contém $M = q^k$ palavras distintas, qualquer vector $m \in \mathbb{F}_q^k$ poder ser codificado por C.

Seja $\mathcal{B} = \{v_1, \ldots, v_k\} \subset \mathbb{F}_q^n$ uma base de C e considere-se o vector mensagem $m = (m_1, \ldots, m_k) \in \mathbb{F}_q^k$. Seja $x = \sum_{i=1}^k m_i v_i$, ou seja, x é a combinação linear dos vectores da base $\mathcal{B}$ tendo por coeficientes as coordenadas do vector mensagem m, logo $x \in C$. O vector x também se pode escrever $x = G^T m$, onde G é a matriz cujas linhas são os vectores de $\mathcal{B}$. Fica então definida uma aplicação

$$\begin{aligned} f : \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ m &\longmapsto x = G^T m \ . \end{aligned}$$

Esta aplicação f é injectiva e a sua imagem é C, pois as colunas de G^T formam a base $\mathcal{B}$ de C. Portanto, depois de restringirmos o conjunto de chegada para C, obtemos uma função de codificação $f : \mathbb{F}_q^k \longrightarrow C$ (ver a Definição 1.8).

Suponhamos agora que a matriz geradora G está na forma canónica: $G = \begin{bmatrix} I_k & A \end{bmatrix}$, com A uma matriz $(n-k) \times k$. Então o vector codificado x toma a forma

$$x = G^T m = \begin{bmatrix} I_k \\ A^T \end{bmatrix} m = (m, A^T m) \ . \tag{4.1}$$

Como as k componentes do vector mensagem m são também componentes do vector codificado x, dizemos que se trata de uma *codificação sistemática*. A essas compomentes de x chamamamos *dígitos de mensagem*. Às restantes componentes de x chamamos *dígitos de verificação ou de redundância*, e ao seu número $r = n - k$ chamamos *redundância* do código C. Escrevendo explicitamente as coordenadas em (4.1):

$$x = (\underbrace{m_1, \ldots, m_k}_{\text{dígitos de mensagem}}, \overbrace{x_{k+1}, \ldots, x_n}^{\text{dígitos de verificação ou de redundância}}) \ , \tag{4.2}$$

onde $(x_{k+1}, \ldots, x_n) = A^T m$. Dado um vector codificado $x \in C$, a mensagem original m é obtida simplesmente apagando os dígitos de verificação.

Exemplo 4.24. O código ISBN é definido por

$$\text{ISBN} = \left\{ x_1 x_2 \cdots x_{10} \ : \ x_i \in \{0, \ldots, 9\}, \text{ com } 1 \leq i \leq 9, \text{ e } \ x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11} \right\} \ .$$

Quando se obtém 10 na última coodenada das palavras de código, escrevemos $x_{10} = X$. Este código não é linear, mas pode ser obtido a partir do seguinte código linear

$$C = \{(x_1, \ldots, x_{10}) \in \mathbb{F}_{11}^{10} \ : \ x_{10} = \sum_{i=1}^{9} i x_i\} \ .$$

Como a condição $x_{10} = \sum_{i=1}^{9} i x_i$ é equivalente a $\sum_{i=1}^{10} (-i) x_i + x_{10} = 0$, a seguinte matriz

$$\begin{aligned} H &= \begin{bmatrix} -1 & -2 & \cdots & -9 & 1 \end{bmatrix} \\ &= \begin{bmatrix} X & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{bmatrix} \end{aligned}$$

é uma matriz de paridade para C e está na forma canónica $\begin{bmatrix} B & I_1 \end{bmatrix}$ com

$$B = \begin{bmatrix} X & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \end{bmatrix} \ .$$

Pelo Teorema 4.14, $G = \begin{bmatrix} I_9 & -B^T \end{bmatrix}$ é uma matriz geradora de C. Usando esta matriz G para codificar os vectores $m \in \mathbb{F}_{11}^9$, fica

$$x = G^T m = (m_1, \ldots, m_9, x_{10})$$

onde a última componente é dada por

$$x_{10} = -Bm = \sum_{i=1}^{9} i m_i = \sum_{i=1}^{9} i x_i$$

e esta é precisamente a condição imposta na definição do código C (e também na do código ISBN). Recupera-se a mensagem original m a partir da mensagem codificada x apagando o dígito de verificação x_{10}. Em particular obtém-se

$$\text{ISBN} = \{G^T m \,:\, m \in (\mathbb{F}_{11} \setminus \{X\})^9\} \ .$$

4.2. Descodificação por Tabelas de Slepian

Seja C um código linear $[n,k]$ sobre $\mathbb{F}_q$. Para cada vector $a \in \mathbb{F}_q^n$, definimos a *classe* ou *coconjunto* de a por

$$a + C := \{a + x \,:\, x \in C\} \ . \tag{4.3}$$

Observação 4.25. A operação soma de vectores num espaço vectorial V satisfaz todos os axiomas de um grupo abeliano. Assim, quando ignoramos a operação produto por um escalar, o que sobra é o grupo abeliano $(V,+)$. Em particular, $(\mathbb{F}_q^n,+)$ é um grupo abeliano e um código C é um subgrupo $(C,+)$, necessariamente normal. Assim, fica definida uma relação de equivalência em $\mathbb{F}_q^n$ do seguinte modo: a e b são equivalentes se e só se $a-b \in C$, cujas classes de equivalência são precisamente os conjuntos em (4.3). Além disso, por C ser um subgrupo normal de $\mathbb{F}_q^n$, as classes de equivalência formam ainda um grupo.

Em vez de usarmos a maquinaria de Teoria de Grupos, podemos simplesmente definir primeiro as classes (4.3) e provar de seguida o seguinte resultado, cuja demonstração elementar pode ser consultada em [**2**] ou em [**1**].

Teorema 4.26. *Sejam $a, b \in \mathbb{F}_q^n$ vectores arbitrários. Então:*

(i) Qualquer vector $a \in \mathbb{F}_q^n$ pertence a uma classe.

(ii) Todas as classes contêm o mesmo número de elementos, i.e., $|a+C| = |C| = q^k$.

(iii) $b \in a + C$ se e só se $a + C = b + C$

(iv) Ou $a + C = b + C$ ou $(a + C) \cap (b + C) = \varnothing$.

(v) Existem precisamente q^{n-k} classes distintas.

(vi) $a - b \in C$ se e só se a e b pertencem à mesma classe.

Uma consequência directa deste teorema é o conjunto

$$\mathbb{F}_q^n / C := \{a + C \,:\, a \in \mathbb{F}_q^n\}$$

conter exactamente q^{n-k} classes e ser um espaço vectorial sobre $\mathbb{F}_q$ com as oprerações soma e produto por escalares dadas respectivamente por

$$(a + C) + (b + C) = (a + b) + C \qquad \text{e} \qquad \lambda(a + C) = (\lambda a) + C \ ,$$

onde $a, b \in \mathbb{F}_q^n$ e $\lambda \in \mathbb{F}_q$.
A um representante da classe $a + C$ com o menor peso possível chamamos *chefe de classe*, mais precisamente,

$$c_a \in a + C \quad \text{é um chefe de classe se e só se} \quad \mathrm{w}(x) \geq \mathrm{w}(c_a) \quad \forall\, x \in a + C \ .$$

Uma classe pode conter mais do que um chefe de classe. No entanto, a classe do vector nulo $\vec{0}+C = C$ contém um único chefe de classe, nomeadamente, o próprio vector nulo.

Exemplo 4.27. Considere o código linear binário $C = \langle 1011, 0101\rangle = \{0000, 1011, 0101, 1110\}$. A classe de 0001 é o conjunto

$$0001 + C = \{0001, 1010, 0100, 1110\} \ .$$

Como $\mathrm{w}(0001) = \mathrm{w}(0100) = 1$, $\mathrm{w}(1010) = 2$ e $\mathrm{w}(1110) = 3$, os vectores 0001 e 0100 são ambos chefes da classe $0001 + C$.

Considere o seguinte algoritmo de descodificação:

Recebido $y \in \mathbb{F}_q^n$, procuramos o chefe de classe $c_y \in y + C$ e descodificamos y por $y - c_y$. (Caso não haja unicidade de chefe de classe, devemos indicar a priori qual o que vamos usar para o algoritmo, ou então optar por uma descodificação incompleta.)

Para aplicar este algoritmo sistematicamente, construimos uma *Tabela (Padrão) de Slepian*:

- enumeramos as plavaras de código $C = \{x_1, x_2, \ldots, x_{q^k}\}$;
- escolhemos chefes de classes $a_0 = \vec{0}$, $a_1, a_2, \ldots, a_{s-1}$, onde $s = q^{n-k}$ é o número de classes distintas;
- escrevemos uma tabela

$$\begin{array}{rcccccc}
a_0 + C = C: & x_1 & x_2 & \cdots & x_j & \cdots & x_{q^k} \\
a_1 + C: & a_1 + x_1 & a_1 + x_2 & \cdots & a_1 + x_j & \cdots & a_1 + x_{q^k} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a_i + C: & a_i + x_1 & a_i + x_2 & \cdots & a_i + x_j & \cdots & a_i + x_{q^k} \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
a_{s-1} + C: & a_{s-1} + x_1 & a_{s-1} + x_2 & \cdots & a_{s-1} + x_j & \cdots & a_{s-1} + x_{q^k}
\end{array}$$

$\left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\end{array}}\right\}$ $s = q^{n-k}$ linhas

$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{q^k \text{ colunas}}$

Note que nesta tabela encontram-se todos os vectores de $\mathbb{F}_q^n$, sem repetições, e na primeira linha encontram-se as palavras do código C. Assim, o algoritmo de descodificação também pode ser descrito da seguinte maneira:

> Recebido um vector $y \in \mathbb{F}_q^n$, encontrar a sua posição na Tabela de Slepian, i.e., encontrar a entrada (i, j) tal que $y = a_i + x_j$, assumir o erro a_i e descodificar y por $y - a_i = x_j \in C$.

Estamos a assumir que o erro ocorrido é o chefe de classe a_i que, por definição, tem peso mínimo entre os elementos da sua classe. Portanto, ao usarmos este algoritmo, estamos a descodificar por distância mínima. Conclui-se também que os vectores erro que este algoritmo permite corrigir são precisamente os chefes de classe escolhidos $a_1, a_2, \ldots, a_{s-2}$ e a_{s-1}.

Exemplo 4.28. Continuando com o Exemplo 4.27, sejam $x_0 = 0000$, $x_1 = 1011$, $x_2 = 0101$ e $x_3 = 1110$ as quatro palavras do códiogo C, que formam a primeira linha duma Tabela de Slepian. Para escrevermos a segunda linha, temos de esolher uma palavra de peso mínimo em $\mathbb{F}_2^4 \backslash C$. Qualquer palavra de peso 1 serve. Por exemplo, pondo $a_1 = 0001$, a segunda linha da tabela fica

$$0001 + C: \quad 0001 \quad 1010 \quad 0100 \quad 1111$$

Para a próxima linha, escolhemos para a_2 uma palavra de peso mínimo entre os vectores de $\mathbb{F}_q^n$ que ainda não aparecem em nenhuma das linhas anteriores já escritas. Continuando este procedimento, obtemos a seguinte Tabela de Slepian:

$$\begin{array}{rcccc}
C: & 0000 & 1011 & 0101 & 1110 \\
0001 + C: & 0001 & 1010 & 0100 & 1111 \\
0010 + C: & 0010 & 1001 & 0111 & 1100 \\
1000 + C: & 1000 & 0011 & 1101 & 0110
\end{array}$$

(Outra possível Tabela de Slepian, seria escolhermos 0100 para chefe da classe $0001 + C$. Nas outras três classes, há apenas uma escolha possível.)

Para descodificar a palavra recebida $y = 1101$, localizamos $y = 1000 + 0101 = a_3 + x_2$ na tabela e descodificamo-la pela palavra no topo da coluna correspondente, neste caso por $x_2 = 0101$.

Como se pode imaginar, construir uma Tabela de Slepian é um procedimento moroso e não muito prático se $\mathbb{F}_q^n$ contiver um número elevado de palavras. No entanto, sabermos quais são os chefes de classe (que corresponde a ter a primeira coluna da tabela, se escolhermos $x_0 = \vec{0}$) já nos dá alguma informação sobre a distância mínima do código. No exemplo acima, sabendo apenas que os chefes de classe não nulos são $a_1 = 0001$, $a_2 = 0010$ e $a_3 = 1000$ e têm todos peso 1, mas não incluem

todos os vectores de $\mathbb{F}_2^4$ com este peso, já nos permite concluir que a distância mínima do código é $\mathrm{d}(C) < 3$, pois o código não corrige todos os erros de peso 1.

Proposição 4.29. *Se* $\mathrm{d}(C) = d$*, então todas as palavras de peso menor ou igual a* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$ *são chefes de classes distintas.*

Deixamos a demostração desta proposição como exercício.

4.3. Probabilidade de descodificação (in)correcta e de detecção de erros

Seja C um código, não necessariamente linear, de parâmetros $(n, M)_q$. A probabilidade de erro na descodificação associada a C é definida por

$$P_{err}(C) := \sum_{x \in C} P(\text{descodificação errada} \,|\, x \text{ enviado}) P(x \text{ enviado}) \ . \tag{4.4}$$

Naturalmente, precisamos das probabilidades $P(x \text{ enviado})$. Estas probabilidades definem a distribuição de entrada e não dependem de C, mas sim da situação concreta em que o código é usado. No entanto, verifica-se sempre que

$$\sum_{x \in C} P(x \text{ enviado}) = 1 \ .$$

A probabilidade condicionada $P(\text{descodificação errada} \,|\, x \text{ enviado})$ que ocorre na definição (4.4) denota a probabilidade da palavra enviada x ser descodificada por uma outra palavra de código qualquer diferente de x. Estas probabilidades condicionadas dependem do canal de transmissão usado e também podem depender da palavra $x \in C$.

Exemplo 4.30. Consideremos o código binário de repetição de comprimento três, $C = \{000, 111\}$, e um canal de transmissão simétrico binário com probabilidade de troca p. Se 000 é a palavra enviada, a descodificação é incorrecta se ocorrerem erros de transmissão em pelo menos dois símbolos, portanto

$$\begin{aligned} P(\text{descodificação errada} \,|\, 000 \text{ enviado}) &= P(\text{recebido } 110, 101, 110 \text{ ou } 111 \,|\, 000 \text{ enviado}) \\ &= 3p^2(1-p) + p^3 \ . \end{aligned}$$

Analogamente

$$\begin{aligned} P(\text{descodificação errada} \,|\, 111 \text{ enviado}) &= P(\text{recebido } 001, 010, 100 \text{ ou } 000 \,|\, 111 \text{ enviado}) \\ &= 3p^2(1-p) + p^3 \ . \end{aligned}$$

Neste caso (e não é por acaso) as probabilidades $P(\text{descodificação errada} \,|\, x \text{ enviado})$ não dependem de $c \in C$. A probabilidade de descodificação incorrecta é então dada por

$$P_{err}(C) = (3p^2(1-p) + p^3)\big(P(000 \text{ enviado}) + P(111 \text{ enviado})\big) = 3p^2(1-p) + p^3 = 3p^2 - 2p^3 \ .$$

Quando $P(\text{descodificação errada} \,|\, x \text{ enviado})$ não depende de $x \in C$, independentemente da distribuição de entrada, a fórmula (4.4) simplifica-se para

$$P_{err}(C) = P(\text{descodificação errada} \,|\, x \text{ enviado})$$

escolhendo uma palavra de código c qualquer.

A probabilidade de descodificação correcta é definida por

$$P_{corr}(C) := \sum_{x \in C} P(\text{descodificação correcta} \,|\, x \text{ enviado}) P(x \text{ enviado}) \ . \tag{4.5}$$

Nas definições (4.4) e (4.5) assume-se sempre uma descodificação completa, portanto tem-se

$$P_{corr}(C) + P_{err}(C) = 1 \ .$$

Exemplo 4.31. Considere a mesma situação do Exemplo 4.30: código de repetição $C = \{000, 111\}$ e canal de transmissão binário simétrico com probabilidade de troca p. Se 000 é a palavra enviada, a descodificação é correcta se ocorrer no máximo um erro de transmissão, portanto

$$\begin{aligned} P(\text{descodificação correcta} \,|\, 000 \text{ enviado}) &= P(\text{recebido } 100, 010, 001 \text{ ou } 000 \,|\, 000 \text{ enviado}) \\ &= 3p(1-p)^2 + (1-p)^3 \ . \end{aligned}$$

Analogamente

$$\begin{aligned} P(\text{descodificação correcta} \,|\, 111 \text{ enviado}) &= P(\text{recebido } 110, 101, 011 \text{ ou } 111 \,|\, 111 \text{ enviado}) \\ &= 3p(1-p)^2 + (1-p)^3 \ . \end{aligned}$$

A probabilidade de descodificação correcta é então dada por

$$\begin{aligned} P_{corr}(C) &= (3p(1-p)^2 + (1-p)^3)\big(P(000 \text{ enviado}) + P(111 \text{ enviado})\big) \\ &= 3p(1-p)^2 + (1-p)^3 = (1-p)^2(2p+1) \ , \end{aligned}$$

e portanto

$$P_{err}(C) = 1 - P_{corr}(C) = 1 - (1-p)^2(2p+1) = 3p^2 - 2p^3 \ ,$$

que coincide com o resultado obtido no Exemplo 4.30.

Suponhamos que C é usado apenas para detectar erros. A probabilidade de C não detectar erros de transmissão é definida por

$$P_{undetect}(C) := \sum_{x \in C} P(\text{receber } y \in C \setminus \{x\} \,|\, x \text{ enviado}) P(x \text{ enviado}) \ . \tag{4.6}$$

A probabilidade de detecção de erros é então definida por $P_{detect}(C) = 1 - P_{undetect}(C)$.

Consideremos agora um código linear binário C e um canal de transmissão binário simétrico, com probabilidade de troca de símbolos $p < \frac{1}{2}$. A probabilidade de ocorrer um vector erro $\vec{e}$ de peso $\mathrm{w}(\vec{e}) = i$ é $p^i(1-p)^{n-i}$, pois ocorreram precisamente i trocas de símbolos. Seja

$$\alpha_i := \#\{\text{chefes de classe } a_j \text{ com peso } \mathrm{w}(a_j) = i\} \ . \tag{4.7}$$

Portanto, a probabilidade de descodificar correctamente a palavra recebida y pela palavra de código enviada $x \in C$ é

$$P_{corr}(\text{descodificação correcta} \,|\, x \text{ enviado}) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i} \ ,$$

pois corresponde à probabilidade do vector erro $\vec{e} = y - x$ ser um chefe de classe, e não depende de $x \in C$. Portanto

$$P_{corr}(C) = \sum_{i=0}^{n} \alpha_i p^i (1-p)^{n-i} \ . \tag{4.8}$$

Note que $P_{corr}(C)$ apenas depende dos chefes de classe do código C. Em relação ao número destes, temos o seguinte resultado.

Proposição 4.32. *Seja* $t = \lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor$. *Então* $\alpha_i = \binom{n}{i}$, *para qualquer* $0 \leq i \leq t$.

Suponhamos agora que o código C é usado apenas para detecção de erros. Se $x \in C$ é a palavra enviada e y é a palavra recebida, o vector erro $\vec{e} = y - x$ não é detectado se e só se $\vec{e} \in C \setminus \{\vec{0}\}$. Portanto $P(\text{receber } y \in C \setminus \{x\} \,|\, x \text{ enviado})$ não depende da palavra enviada x e a probabilidade de C não detectar erros é

$$P_{undetec}(C) = \sum_{i=1}^{n} A_i p^i (1-p)^{n-i} \ , \tag{4.9}$$

onde

$$A_i := \#\{x \in C \,:\, \mathrm{w}(x) = i\} \ . \tag{4.10}$$

Note que $A_0 = 1$, porque $\vec{0}$ é a única palavra em C de peso zero, e que o somatório em (4.9) não inclui o índice $i = 0$ pois $\vec{e} = \vec{0}$ significa que não ocorreram erros durante a transmissão.

4.4. Descodificação por síndrome

A descodificação por síndrome é também um método de descodificação por distância mínima, é equivalente ao algoritmo usando um Tabela de Slepian, mas muitíssimo mais eficiente.

Fixemos um código linear C, de parâmetros $[n,k]_q$, com matriz de paridade H.

Definição 4.33. O *sintoma* de $x \in \mathbb{F}_q^n$ é o vector $S(x) = Hx \in \mathbb{F}_q^{n-k}$.

Como habitualmente, identificamos um vector x com a matriz coluna cujas entradas são as coordenadas de x.

Lema 4.34. *Dois vectores $x, y \in \mathbb{F}_q^n$ têm o mesmo sintoma se e só se pertencem à mesma classe de C, i.e., $S(x) = S(y)$ se e só se $x + C = y + C$.*

Dem. $S(x) = S(y) \Leftrightarrow Hx = Hy \Leftrightarrow H(x-y) = \vec{0} \Leftrightarrow x - y \in \mathcal{N}(H) = C \Leftrightarrow x + C = y + C$. □

Por definição, a aplicação

$$\begin{aligned} S : \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^{n-k} \\ x &\longmapsto S(x) = Hx \end{aligned}$$

é uma aplicação linear. O lema anterior garante que esta aplicação S induz uma aplicação $\tilde{S}$ (necessariamente linear) no espaço quociente $\mathbb{F}_q^n/C$

$$\begin{aligned} \tilde{S} : \mathbb{F}_q^n/C &\longrightarrow \mathbb{F}_q^{n-k} \\ x + C &\longmapsto S(x) = Hx \end{aligned}$$

e que $\tilde{S}$ é injectiva. Como $\mathbb{F}_q^n/C$ contém precisamente q^{n-k} classes distintas, então $\tilde{S}$ também é sobrejectiva, logo é bijectiva, i.e., $\tilde{S}$ é um isomorfismo de espaços lineares.

Portanto, para definir um algoritmo de descodificação é preciso determinar a aplicação inversa de $\tilde{S}$ e escolher um representante de cada classe $x + C$ (estes representantes vão ser os erros corrigidos pelo algoritmo), por exemplo, os chefes de classe a_i também usados nas Tabelas de Slepian. Para facilitar a descodificação, começamos por escrever uma *tabela de síndrome*:

a_i	$S(a_i)$
$a_0 = \vec{0}$	$S(a_0) = \vec{0}$
a_1	$S(a_1)$
$\vdots$	$\vdots$
a_{s-1}	$S(a_{s-1})$

onde $s = q^{n-k}$ é o número de classes distintas e $a_0 = \vec{0}, a_1, \ldots, a_{s-1}$ são chefes de classe. O algoritmo de *descodificação por síndrome* é o seguinte:

> Recebido um vector $y \in \mathbb{F}_q^n$, calcular o sintoma $S(y)$, determinar o chefe de classe a_i tal que $S(y) = S(a_i)$, assumir o erro a_i e descodificar y por $y - a_i = x_j \in C$.

Exemplo 4.35. Considere novamente o código linear $C = \langle 1011, 0101 \rangle$ do Exemplo 4.28. Já determinámos chefes de classe $a_0 = 0000$, $a_1 = 0001$, $a_2 = 0010$ e $a_3 = 1000$. Agora precisamos de uma matriz de paridade para calcularmos os sintomas. Como a matriz geradora

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

está na forma canónica, conclui-se imediatamente que

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

é uma matriz de paridade para C. A tabela de síndrome fica então

a_i	$S(a_i)$
0000	00
0001	01
0010	10
1000	11

(Note que na coluna dos sintomas $S(a_i)$ aparecem exactamente os quatro vectores em $\mathbb{F}_2^2$.) Seja $y = 0110$ a palavra recebida. Como $S(0110) = 11 = S(1000)$, descodificamos y por $y - 1000 = 1110 \in C$.

Por vezes não é necessário escrevermos a tabela de síndrome para aplicarmos o algoritmo.

Exemplo 4.36. Seja C o código linear sobre $\mathbb{F}_{11} = \{0, 1, 2, \ldots, 9, X\}$ com a seguinte matriz de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix}$$

A coluna i de H é $c_i = \begin{bmatrix} 1 & i \end{bmatrix}^T$, portanto

$$\det \begin{bmatrix} | & | \\ c_i & c_j \\ | & | \end{bmatrix} = \det \begin{bmatrix} 1 & 1 \\ i & j \end{bmatrix} = j - i \neq 0 \qquad \forall i \neq j$$

donde concluimos que quaisquer duas colunas distintas são linearmente independentes. Como as colunas de H são vectores em $\mathbb{F}_{11}^2$, quaisquer três colunas são linearmente dependentes (bastava haver três colunas linearmente dependentes). Aplicando o Teorema 4.16, obtêm-se que $\mathrm{d}(C) = 3$ e, portanto, o código C pode ser usado para corrigir qualquer erro simples de troca de símbolos.

Vamos ver que, usando uma descodificação incompleta, para além de corrigir os erros simples, C também permite detectar os erros duplos de transposição.

Seja $x = (x_1, \ldots, x_{10}) \in C$ a palavras transmitida, e seja $y = (y_1, \ldots, y_{10}) \in \mathbb{F}_{11}^{10}$ a palavra recebida. No caso de ocorrer um erro simples, então $y = x + (0, \ldots, 0, k, 0, \ldots, 0)$ com $k \in \mathbb{F}_{11} \setminus \{0\}$ na coordenada j. Pondo

$$A = \sum_{i=1}^{10} y_i \qquad \text{e} \qquad B = \sum_{i=1}^{10} i y_i$$

fica $S(y) = (A, B)$. No caso particular do vector recebido, ainda fica

$$A = \sum_{i=1}^{10} x_i + k = k \qquad \text{e} \qquad B = \sum_{i=1}^{10} i x_i + jk = jk$$

porque $S(x) = 0$. Portanto ambas as componentes do sintoma $S(y)$ são não nulas e podemos ainda concluir que ocorreu um erro de *amplitude* $k = A$ na coordenada $j = BA^{-1}$.

No caso de ocorrer um erro de transposição, o vector recebido é

$$y = (x_1, \ldots, x_{j-1}, x_k, x_{j+1}, \ldots, x_{k-1}, x_j, x_{k+1}, \ldots, x_{10})$$

para algum par de coordenadas $1 \leq j < k \leq 10$, com $x_j \neq x_k$ na palavra enviada (se $x_k = x_j$ e se permutarmos as coordenadas j e k, não alteramos o vector x). Portanto, as coordenadas do sintoma $S(y)$ são agora dadas por

$$A = \sum_{i=1}^{10} y_i = \sum_{i=1}^{10} x_i = 0 \qquad \text{e}$$

$$B = \sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + (j x_k + k x_j) - (j x_j + k x_k) = (k - j)(x_j - x_k) \neq 0$$

Portanto, $S(y) = (0, B)$ com $B \neq 0$, mas não conseguimos determinar o tipo de erro ocorrido apenas conhecendo o valor de B. No entanto os sintomas obtidos neste caso são todos diferentes de qualquer um dos sintomas dos erros simples.

Acabámos de provar que o seguinte algoritmo de descodificação incompleta corrige erros simples e detecta erros duplos de transposição:

1. Recebido $y \in \mathbb{F}_{11}^{10}$, calcular o sintoma $S(y) = (A, B) \in \mathbb{F}_{11}^2$.
2. Se $(A, B) = (0, 0)$, então assumir que não ocorreram erros de transmissão e descodificar a palavra y por ela própria, uma vez que $y \in C$.
3. Se $A \neq 0$ e $B \neq 0$, assumir que ocorreu um erro simples na posição $j = BA^{-1}$ de amplitude A, e descodificar y por $y - (0, \ldots, 0, A, 0, \ldots, 0)$ (A na coordenada j).
4. Se $A \neq 0$ ou $B \neq 0$ (mas não $A \neq 0$ e $B \neq 0$), assumir pelo menos dois erros e pedir retransmissão.

A descodificação por síndrome, assim como a descodificação pelas tabelas de Slepian, pode ser usada para corrigir outro tipo de erros em vez de chefes de classes. A condição a impor aos erros que se pretendem corrigir é estes não serem palavras de código e pertencerem a classes $a + C$ distintas. Ou seja, os erros a corrigir têm sintomas não nulos e são distintos entre si.

Exemplo 4.37. Seja C o código linear binário com a seguinte matriz de paridade

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

Considere os seguintes vectores $v_1 = 1000000$, $v_2 = 1100000$, $v_3 = 1110000$, $v_4 = 1111000$, $v_5 = 1111100$, $v_6 = 1111110$ e $v_7 = 1111111$. Como $v_{i+1} = v_i + e_i$, para $i = 2, \ldots, 6$, onde e_i são os vectores da base canónica de $\mathbb{F}_2^7$, podemos calcular os sintomas de v_i recursivamente calculando apenas $S(v_1)$ e somando a coluna $i + 1$ de H a $S(v_i)$ para obter $S(v_{i+1})$. Obtém-se:

$$S(v_1) = 001,\ S(v_2) = 010,\ S(v_3) = 011,\ S(v_4) = 100,\ S(v_5) = 101,\ S(v_6) = 110 \text{ e } S(v_7) = 111\ .$$

Em particular, conclui-se que estes v_i não são palavras de código e pertencem a classes distintas, pois os seus sintomas são todos diferentes entre si (e nenhum é zero). Logo C pode ser usado para corrigir os vectores $v_1, \ldots, v_7$. Usando C para corrigir os erros v_i, $i = 1, \ldots, 7$, vamos descodificar o vector recebido $y = 0011111$: como $S(y) = 101 = S(v_5)$, descodificamos y pela palavra de código $x = y - v_5 = 11000011$.

Exercícios

4.1. Seja C um código linear $[n, k]$ sobre $\mathbb{F}_q$. Para cada $i \in \{1, \ldots, n\}$ fixo, mostre que, ou $x_i = 0$ para todo o $x = (x_1, \ldots, x_n) \in C$, ou o número de palavras em C com $x_i = a$, para $a \in \mathbb{F}_q$ fixo, é $\frac{|C|}{q} = q^{k-1}$.

4.2. Seja C um código linear binário. Mostre que, ou todas as palavras de C têm peso par, ou metade das palavras tem peso par e a outra metade tem peso ímpar.

4.3. Seja C um código linear binário de parâmetros $[n, k, 2t + 1]$ e seja $C' = \{x \in C : \mathrm{w}(x) \text{ é par}\}$ o subcódigo de C das palavras de peso par.
   (a) Justifique que C' é um código linear.
   (b) Determine, justificando detalhadamente, a dimensão de C'.

4.4. Seja C um código binário, linear e auto-dual.
   (a) Mostre que, se os pesos de $x, y \in C$ são múltiplos de 4, então o peso de $x + y$ também é um múltiplo de 4.
   (b) Mostre que ou todas as palavras de C têm peso um múltiplo de 4, ou metade tem peso um múltiplo de 4 e a outra metade tem peso par mas não divisível por 4.
   (c) Mostre que $\vec{1} = (1, \ldots, 1) \in C$.
   (d) Se o código C tem comprimento 6, determine a distância mínima $\mathrm{d}(C)$.

4.5. Determine uma matriz geradora e uma matriz de paridade, e indique os parâmetros $[n, k, d]$ para o menor código linear sobre $\mathbb{F}_q$ contendo o conjunto S, quando

(a) $q = 3$, $S = \{110000, 011000, 001100, 000110, 000011\}$;
(b) $q = 2$, $S = \{10101010, 11001100, 11110000, 01100110, 00111100\}$.

4.6. Seja C um código linear $[N, K, D]$ sobre $\mathbb{F}_{q^m}$.
(a) Definimos o *código traço* por

$$\mathrm{Tr}(C) := \{(\mathrm{Tr}(x_1), \ldots, \mathrm{Tr}(x_N)) \,:\, (x_1, \ldots, x_N) \in C\} \ ,$$

onde $\mathrm{Tr} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q$ é a aplição traço definida no Exercício 3.13. Mostre que $\mathrm{Tr}(C)$ é um código linear q-ário, de comprimento N e dimensão $k \leq mK$.
(b) Definimos o *subcódigo subcorpo* por

$$C|_{\mathbb{F}_q} := C \cap \mathbb{F}_q^N \ .$$

Justifique que $C|_{\mathbb{F}_q}$ é um código linear sobre $\mathbb{F}_q$.

4.7. Considere o código linear $C = \langle(\alpha, \alpha^2, \alpha^4, 1, \alpha^3, \alpha^6, \alpha^5)\rangle$ sobre $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, onde $\alpha^3 = 1 + \alpha$.
(a) Indique os parâmetros de C.
(b) Determine uma matriz geradora do código traço $\mathrm{Tr}(C)$ (ver Exercício 4.6).
(c) Indique os parâmetros do código dual $\mathrm{Tr}(C)^\perp$.
(d) Será $\mathrm{Tr}(C)$ um código auto-ortogonal ou auto-dual?
(e) Determine uma matriz geradora para o código dual $C^\perp$ e para o subcódigo subcorpo $(C^\perp)|_{\mathbb{F}_2}$.
(f) Verifique[2] que $(C^\perp)|_{\mathbb{F}_2} = \mathrm{Tr}(C)^\perp$.

4.8. Seja C um código linear binário de comprimento $n \geq 4$. Seja H uma matriz de paridade para C tal que as colunas de H são todas distintas e têm todas peso ímpar. Prove que $\mathrm{d}(C) \geq 4$.

4.9. A menos de equivalência linear, determine quantos códigos lineares, sobre $\mathbb{F}_3$, de comprimento n e dimensão 1 existem.

4.10. Seja C um código linear de parâmetros $[n, k]_q$, com $k \geq 1$, e seja G uma matriz geradora. Mostre que $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$, $m \longmapsto G^T m$, é uma codificação sistemática de C se e só se todas as colunas da matriz identidade $k \times k$ são colunas de G.

4.11. (a) Demonstre a Proposição 4.29: para um código linear q-ário de comprimento n e distância mínima d, mostre que os vectores $x \in \mathbb{F}_q^n$ com peso $\mathrm{w}(x) \leq \lfloor \frac{d-1}{2} \rfloor$ são chefes de classes distintas deste código.
(b) Seja C um código perfeito com $\mathrm{d}(C) = 2t + 1$. Mostre que os únicos chefes de classe de C são os determinados na alínea anterior.
(c) Assumindo que o código perfeito C da alínia (b) é binário, seja $\widehat{C}$ o código obtido de C acrescentando um dígito de paridade, i.e.,

$$\widehat{C} = \left\{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \ldots, x_n) \in C \,,\, \sum_{i=1}^{n+1} x_i = 0\right\} \ .$$

Mostre que qualquer chefe de classe de $\widehat{C}$ tem peso menor ou igual a $t + 1$.

4.12. Considere o código linear sobre $\mathbb{F}_{11}$ de matriz de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & X^2 \end{bmatrix} \ .$$

(a) Determine os parâmetros $[n, k, d]$ deste código.
Sugestão: comece por verificar que em qualquer corpo $\mathbb{F}$

$$\begin{vmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{vmatrix} = (a_3 - a_1)(a_2 - a_1)(a_3 - a_2) \ , \qquad \forall\, a_1, a_2, a_3 \in \mathbb{F} \ .$$

(b) Escreva uma matriz geradora do código.
(c) Descreva pormenorizadamente um Algoritmo de Descodificação para este código que permita corrigir 1 erro e detectar 2 erros em qualquer posição.

[2] Esta relação entre os códigos traço e subcorpo é válida para qualquer código linear C sobre $\mathbb{F}_{q^m}$, é o Teorema de Delsarte.

(d) Utilize o algoritmo da alínea anterior para descodificar os vectores recebidos

$$x = 0204000910 \qquad \text{e} \qquad y = 0120120120\ .$$

4.13. Resolva o problema análogo ao anterior para o código linear sobre $\mathbb{F}_{11}$ de matriz de paridade

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \\ 1^2 & 2^2 & 3^2 & 4^2 & 5^2 & 6^2 & 7^2 & 8^2 & 9^2 & X^2 \\ 1^3 & 2^3 & 3^3 & 4^3 & 5^3 & 6^3 & 7^3 & 8^3 & 9^3 & X^3 \end{bmatrix}\ .$$

Descodifique também o vector recebido $z = 1204000910$.

4.14. Seja C o código linear sobre $\mathbb{F}_5$ com a seguinte matriz de paridade

$$H = \begin{bmatrix} 3 & 2 & 1 & 0 & 0 & 2 \\ 1 & 0 & 1 & 0 & 3 & 2 \\ 0 & 4 & 1 & 4 & 1 & 3 \end{bmatrix}\ .$$

(a) Mostre que C pode ser usado para corrigir os erros da forma

$$aa0000\,, \quad 0aa000\,, \quad 00aa00\,, \quad 000aa0 \quad \text{e} \quad 0000aa\ ,$$

para $a \in \mathbb{F}_5 \setminus \{0\}$, e descodifique os seguintes vectores recebidos $y = 100011$ e $z = 023333$.

(b) Poderá C ser usado para corrigir todos os erros duplos?

4.15. Determine um código linear binário $[7, k]$ com a taxa de transmissão máxima que permita corrigir os seguintes vectores de erro: 1000000, 1000001, 1100001, 1100011, 1110011, 1110111 e 1111111.

4.16. Considere um código linear ternário C (i.e., sobre o alfabeto $\mathbb{F}_3 = \{0, 1, 2\}$) tendo como matriz de paridade

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

(a) Determine, justificando, os parâmetros $[n, k, d]$ de C.

(b) Calcule uma matriz geradora na forma canónica do código C.

(c) Diga quais as capacidades correctoras de C para erros de apagamento, justificando cuidadosamente a resposta.

(d) Descodifique, se possível, as palavras recebidas

$$x = 2101??\ , \qquad y = 1???12 \qquad \text{e} \qquad z = ???210\ .$$

4.17. Demonstre a Proposição 4.32. Mostre ainda que, no caso de um código perfeito, também se tem que $\alpha_i = 0$ para qualquer $i > t$.

4.18. Seja C um código linear binário perfeito, de comprimento n, e seja

$$\widehat{C} = \{(x_1, \ldots, x_n, x_{n+1}) \in \mathbb{F}_2^{n+1} : (x_1, \ldots, x_n) \in C\,,\ \sum_{i=1}^{n+1} x_i = 0\}$$

a sua extensão por paridade. Para um canal de transmissão binário e simétrico, com probabilidade de troca de símbolos $0 < p < \frac{1}{2}$, mostre que $P_{corr}(C) = P_{corr}(\widehat{C})$.

4.19. Recorde a definição do código ISBN do Exemplo 4.24.

(a) Mostre que a distância mínima do código ISBN é 2.

(b) Quantas palavras do código ISBN terminam no símbolo $X \in \mathbb{F}_{11}$?

(c) Quantas palavras do código ISBN terminam no símbolo $a \in \{0, 1, \ldots, 9\} \subset \mathbb{F}_{11}$?

(d) Seja C o código linear sobre $\mathbb{F}_{11}$ definido no Exemplo 4.36 e seja $C' \subset C$ o subcódigo definido por

$$C' = \{x \in C\ :\ x_i \neq X \quad \forall\, i = 1, \ldots, 10\}\ .$$

Mostre que $|C'| = 82644629$.

Sugestão: use o Princípio de Inclusão-Exclusão (Teorema A.1) e o resultado do Exerício 4.1.

Construção de Códigos

Alguns casos particulares das construções apresentadas neste capítulo já foram usadas, quer em demonstrações, quer em exemplos. Começamos por apresentar construções envolvendo um código apenas (Secções 1 a 5), as restantes envolvem dois códigos ou mais.

1. Extensão

Dado um código C de parâmetros $(n, M, d)_q$, linear ou não, constrói-se um novo código $\widehat{C}$ de parâmetros $(n+s, M, \widehat{d})_q$ acrescentando s componentes a cada uma das palavras de C, podendo estas s componentes ser definidas à custa das n primeiras. $\widehat{C}$ diz-se uma *extensão* de C.
Um caso particular importante é a *extensão por paridade* de C, usada na demonstração do Teorema 2.10 para códigos binários. Para códigos q-ários a definição é a seguinte

$$\widehat{C} = \{(x_1, \ldots, x_n, x_{n+1}) : (x_1, \ldots, x_n) \in C, \quad \sum_{i=1}^{n+1} x_i \equiv 0 \pmod q\} ,$$

onde a ditância mínima de $\widehat{C}$ satisfaz $d \leq \widehat{d} \leq d+1$.

Lema 5.1. *Seja C um código binário linear $[n, k, d]$ com matriz de paridade H. Então a extensão por paridade $\widehat{C}$ é linear, tem parâmetros $[n+1, k, \widehat{d}]$, com $\widehat{d}$ par e*

$$\widehat{H} = \left[\begin{array}{ccc|c} & & & 0 \\ & H & & \vdots \\ & & & 0 \\ \hline 1 & \cdots & 1 & 1 \end{array}\right] \tag{5.1}$$

é uma matriz de paridade para $\widehat{C}$.

Dem. Seja $\widehat{x} = (x, x_{n+1}) \in \mathbb{F}_2^{n+1}$ com $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. Então

$$\widehat{x} \in \widehat{C} \iff x \in C \text{ e } \mathrm{w}(\widehat{x}) \text{ é par} \iff x \in \mathcal{N}(H) \text{ e } \vec{1} \cdot \widehat{x} = 0 \iff \widehat{x} \in \mathcal{N}(\widehat{H}) ,$$

ou seja, $\widehat{C} = \mathcal{N}(\widehat{H})$, logo $\widehat{C}$ é um código linear e, como as linhas de $\widehat{H}$ são linearmente independentes (porquê ?), $\widehat{H}$ é uma matriz de paridade para a extensão por paridade de C.
A distância $\widehat{d} = \mathrm{d}(\widehat{C}) = \mathrm{w}(\widehat{C})$ é par pois

$$\mathrm{w}(\widehat{x}) = \vec{1} \cdot \widehat{x} \pmod 2 \qquad \forall\, \widehat{x} \in \mathbb{F}_2^{n+1} ,$$

logo $\mathrm{w}(\widehat{x})$ é par para qualquer $\widehat{x} \in \widehat{C}$. □

Exemplo 5.2. A extensão por paridade do código binário $\mathbb{F}_2^n$ é o código dos pesos pares

$$E_{n+1} = \{x \in \mathbb{F}_2^{n+1} \,:\, \mathrm{w}(x) \text{ é par}\} \subset \mathbb{F}_2^{n+1} \ .$$

Como consequência, temos o seguinte lema.

Lema 5.3. *Seja C um código binário, de comprimento n, com $\mathrm{d}(C) = d$ ímpar. Então a extensão por paridade $\widehat{C} \subset E_{n+1}$ tem distância mínima $\mathrm{d}(\widehat{C}) = d + 1$.*

Dem. Basta observar que $C \subset \mathbb{F}_2^n$ e que a extensão $\widehat{C}$ tem distância par, pois $\widehat{C} \subset E_{n+1}$. □

Como exemplos, iremos ver no Capítulo 6 a extensão por paridade dos códigos de Hamming binários.

2. Pontuação

Dado um código C de parâmetros $(n, M, d)_q$, contrói-se outro código $\mathring{C}$ com parâmetros $(n-s, M, \mathring{d})_q$ eliminando $s < d$ componentes a cada uma das palavras de C, portanto $\mathring{d} \leq d$. Ao código $\mathring{C}$ assim obtido chamados o *pontuado* de C.
Esta construção já foi usada na demonstração do Teorema 2.10, com $s = 1$, e também para provar a desigualdade de Singleton (Proposição 2.12) com $s = d - 1$.

Lema 5.4. *Seja C um código linear $[n, k, d]_q$, com matriz geradora G. Seja $\mathring{C}$ o pontuado de C em s coordenadas e $\mathring{G}$ a matriz que se obtem de G apagando as s colunas correspondentes às s coordenadas eliminadas. Então $\mathring{C}$ é um código linear e $\mathring{G}$ é uma matriz geradora para $\mathring{C}$.*

No Capítulo 6, iremos definir os códigos de Golay G_{23} e G_{11} como os pontuados na última componente de G_{24} e G_{12}, respectivamente.

3. Expansão

Dado o código C de parâmetros $(n, M, d)_q$, obtém-se um novo código $\overline{C}$ com parâmetros $(n, \overline{M}, \bar{d})_q$, acrescentando palavras a C. Portanto $\overline{M} \geq M$ e $\bar{d} \leq d$.

Exemplo 5.5. Seja C um código binário (n, M, d) e defina-se o código complementar

$$C^c = \{x^c \stackrel{\text{def}}{=} \vec{1} - x \,:\, x \in C\} \ ,$$

onde $\vec{1}$ denota o vector com todas as componentes iguais a 1. Por exemplo, com $x = 01011$, o vector "complementar" é $x^c = 10100$. Ou seja, obtém-se C^c trocando os 0 e os 1 em todas as palavras de C. Seja $\overline{C} = C \cup C^c$. Este código $\overline{C}$ tem parâmetros $(n, \overline{M}, \bar{d})$ com $\overline{M} \leq 2M$, mais precisamente

$$\overline{M} = 2M - |C \cap C^c| \qquad \text{e} \qquad \bar{d} = \min\{d, n - \max\{d(x, y) \,:\, x, y \in C,\, x \neq y^c\}\} \ . \tag{5.2}$$

No caso de C ser um código linear $[n, k, d]_q$, uma extensão de C é um subespaço $\overline{C} \subset \mathbb{F}_q^n$ que contenha C. Se G é uma matriz geradora de C, obtém-se uma uma matriz geradora $\overline{G}$ de $\overline{C}$ acrescentado linhas a G, mais precisamente, dada uma base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de C, completa-se $\mathcal{B}$ para obter uma base $\bar{\mathcal{B}} = \{v_1, \ldots, v_k, w_1, \ldots, w_l\}$ para $\overline{C}$.

Exemplo 5.6. Considere o código binário $C = \{000000, 010010, 001100, 011110\}$. Este código é linear e uma base pode ser, por exemplo, $\{010010, 001100\}$. O código complementar de C é $C^c = \{111111, 101101, 110011, 100001\}$, que não é linear pois não contém o vector nulo. A reunião deste dois códigos é

$$C \cup C^c = \{000000, 010010, 001100, 011110, 111111, 101101, 110011, 100001\}$$

e tem parâmetros $(8, 8, 2)$, pois $\mathrm{d}(C) = 2$. Note que, neste caso, $C \cup C^c$ é um código linear e

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

é uma matriz geradora – justifique.

4. Eliminação ou subcódigos

Dado um código C de parâmetros $(n, M, d)_q$, eliminando palavras em C obtém-se um novo código $\underline{C}$ de parâmetros $(n, \underline{M}, \underline{d})_q$. Portanto $\underline{M} \leq M$ e $\underline{d} \geq d$. $\underline{C}$ diz-se um subcódigo de C.

Exemplo 5.7. (i) As *secções* de C

$$C_{i,a} = \{x = (x_1, \ldots, x_n) \in C : x_i = a\} , \tag{5.3}$$

com $i \in \{1, \ldots, n\}$ e $a \in \mathcal{A}_q$ fixos, são subcódigos de C.

(ii) O código ISBN é obtido do código linear C, sobre $\mathbb{F}_{11}$, com matriz de paridade

$$H = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix}$$

usando eliminação – ver Exemplo 4.24. No entanto, o código ISBN não é uma secção de C.

No caso linear, a eliminação corresponde a tomar um subespaço $\underline{C}$ de C.

Atenção! Uma matriz geradora de $\underline{C}$ não é necessariamente obtida de uma matriz geradora de C apagando linhas.

Lema 5.8. *Seja C um código linear. Então $C_{i,a} = \{x \in C : x_i = 0\}$ é um código linear se e só se $a = 0$, e*

$$\dim C - 1 \leq \dim C_{i,0} \leq \dim C \qquad \forall\, i.$$

Dem. Se $a \in \mathbb{F}_q \setminus \{0\}$, então $\vec{0} \notin C_{i,a}$, logo $C_{i,a}$ não é linear. Se $a = 0$ então $x \in C_{i,0}$ se e só se $x \in C$ e $\vec{e}_i \cdot x = x_i = 0$ (onde $\vec{e}_i = (0, \ldots, 0, 1, 0, \ldots, 0$ com 1 na coordenada i), ou seja $C_{i,0}$ é o núcleo da matriz

$$M = \left[\begin{array}{c} \\ H \\ \\ \hline 0 \quad \ldots \quad 0 \quad 1 \quad 0 \quad \ldots \quad 0 \end{array}\right]$$

logo C é linear. Se as linhas de H e $\vec{e}_i$ são linearmente independentes, M é uma matriz de paridade para $C_{i,0}$ e $\dim C_{i,0} = \dim C - 1$. Caso contrário, H é uma matriz de paridade para $C_{i,0}$, donde $C_{i,0} = C$. □

Exemplo 5.9. Seja C o código binário com matriz geradora

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

Vamos determinar uma matriz geradora $\underline{G}$ para a secção $C_{6,0} = \{x \in C : x_6 = 0\}$. Note que, se apagarmos as linhas de G que não estão em $C_{6,0}$, obteriamos uma matriz linha geradora de um código de dimensão 1, que não é $C_{6,0}$, pois esta secção é um espaço vectorial de dimensão 2 (justifique).

Como G está na forma canónica $\begin{bmatrix} I & A \end{bmatrix}$, então

$$H = \begin{bmatrix} -A^T & I \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

é uma matriz de paridade para C. A condição $x_6 = 0$ traduz-se numa linha $\begin{bmatrix}0 & \cdots & 0 & 1\end{bmatrix}$, donde

$$\underline{H} = \left[\begin{array}{c} H \\ \hline 0\ 0\ 0\ 0\ 0\ 1 \end{array}\right] = \begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&1\\0&0&0&0&0&1\end{bmatrix}$$

é uma matriz de paridade para $C_{6,0}$, se as suas linhas forem linearmente independentes. Aplicando o método de eleminação de Gauss a $\underline{H}$ para tentar obter uma forma canónica:

$$\underline{H} \xrightarrow{l_3 \mapsto l_3+l_4} \begin{bmatrix}1&1&0&1&0&0\\1&0&1&0&1&0\\0&1&1&0&0&0\\0&0&0&0&0&1\end{bmatrix} \xrightarrow[\text{linhas}]{\text{permutar}} \begin{bmatrix}0&1&1&0&0&0\\1&1&0&1&0&0\\1&0&1&0&1&0\\0&0&0&0&0&1\end{bmatrix} \xrightarrow{l_3 \mapsto l_3+l_1} \begin{bmatrix}0&1&1&0&0&0\\1&1&0&1&0&0\\1&1&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}$$

logo podemos concluir que as 4 linhas de $\underline{H}$ são linearmente independentes e que

$$\underline{G} = \begin{bmatrix} I_2 & -B^T \end{bmatrix} = \begin{bmatrix}1&0&0&1&1&0\\0&1&1&1&1&0\end{bmatrix}$$

é uma matriz geradora de $C_{6,0}$.

5. Contracção

Uma contracção de um código C é obtida aplicando as construções de eliminação e pontuação. Um exemplo importante é a pontuação de uma secção, que passamos a descrever.

Dado um código C de parâmetros $(n, M, d)_q$, pontuando na componente i da secção $C_{i,a}$ de C (definida em (5.3)), obtém-se um *código contraído* C' de parâmetros $(n-1, M', d')_q$ com $M' \leq M$ e $d' \geq d$.

No caso de um código linear $[n, k, d]_q$, a secção $C_{i,a}$ (com $i \in \{1, \ldots, n\}$ e $a \in \mathbb{F}_q$ fixos) não é necessariamente um subespaço vectorial de C, mas contém q^{k-1} palavras se $C \neq C_{i,0}$ (consequência do Exercício 4.1). Supondo então que $C_{i,0} \neq C$, $C_{i,0}$ é um código de parâmetros $(n, q^{k-1}, d')_q$ com $d' \geq d$. Pontuando $C_{i,0}$ na componente i, obtemos um código linear C' de parâmetros $[n-1, k-1, d']_q$ e uma matriz de paridade para C' pode ser obtida apagando a coluna i de uma matriz de paridade para C – Exercício 5.4.

Exemplo 5.10. Considere o código ternário C, de parâmetros $[6, 3]$, com matriz geradora

$$G = \begin{bmatrix}1&0&0&0&2&1\\0&1&0&2&1&0\\0&0&1&1&0&2\end{bmatrix}.$$

O pontuado $\overset{\circ}{C}$ de C na quinta coordenada é gerado pelos vectores que se obtêm das linhas de G apagando a quinta coordenada, portanto

$$\overset{\circ}{G} = \begin{bmatrix}1&0&0&0&1\\0&1&0&2&0\\0&0&1&1&2\end{bmatrix}$$

é uma matriz geradora deste código (note que as linhas de $\overset{\circ}{G}$ ainda são linearmente independentes) e $[5, 3]$ são os seus parâmetros. Vamos agora determinar uma contracção de C na quinta coordenada, mais concretamente, vamos deteminar uma matriz de paridade para o pontuado na quinta coordenada da secção $C_{5,0}$. Como G está na forma canónica,

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

é uma matriz de paridade para C e

$$H_{5,0} = \begin{bmatrix} 0 & 1 & 2 & 1 & 0 & 0 \\ 1 & 2 & 0 & 0 & 1 & 0 \\ 2 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

é uma matriz de paridade para $C_{5,0}$ (acrescentou-se o vector $\vec{e}_5$ na última linha) e $[6, 2]$ são os seus parâmetros. Recorrendo ao Lema 4.13, é fácil verificar que

$$G_{5,0} = \begin{bmatrix} 1 & 1 & 0 & 2 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 2 \end{bmatrix}$$

é uma matriz geradora e, portanto,

$$\mathring{G}_{5,0} = \begin{bmatrix} 1 & 1 & 0 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 \end{bmatrix}$$

é uma matriz geradora da contracção $C' = \mathring{C}_{5,0}$, que tem parâmetros $[5, 2]$, e recorrendo ao Lema 4.12 verifica-se que a matriz que se obtém de H apagando a quinta coluna, i.e., que

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

é uma matriz de paridade para C'.

Usando várias das contruções que definimos até agora, podemos provar o seguinte teorema.

Teorema 5.11. *Se existe um código linear de parâmetros $[n, k, d]_q$, então também existe um código linear de parâmetros $[n + r, k - s, d - t]_q$, para quaisquer $r \geq 0$, $0 \leq s \leq k - 1$ e $0 \leq t \leq d - 1$.*

Dem. Seja C um código $[n, k, d]_q$.
(i) Fixemos $r \geq 0$. Usando extensão por zeros, ou seja, acrescentando r componentes todas nulas a cada palavra do código C, obtemos um novo código de parâmetros $[n + r, k, d]_q$.
(ii) Fixemos $0 \leq s \leq k-1$. Seja $x \in C$ uma palavra com peso $\mathrm{w}(x) = d = \mathrm{d}(C)$. Seja $\{v_1, v_2, \ldots, v_k\}$ uma base de C com $v_1 = x$. Então o subespaço $C' = \langle v_1, \ldots, v_{k-s} \rangle \subset C$ é um código $[n, k - s, d]_q$. Para justificar que $\mathrm{d}(C') = d$, basta observar que $x \in C'$ pois $k - s \geq 1$.
(iii) Fixemos $0 \leq t \leq d - 1$. Seja $x \in C$ com peso $\mathrm{w}(x) = d = \mathrm{d}(C)$. Pontuando em t componentes $1 \leq i_1 < i_2 < \cdots < i_t \leq n$ tais que $x_{i_k} \neq 0$ para $k = 1, \ldots, t$ (que existem porque $t \leq d - 1 < \mathrm{w}(x)$), obtemos um código $\mathring{C}$ de parâmetros $[n-t, k, d-t]_q$. Aplicando agora a alínea (i) desta demonstração ao código $\mathring{C}$ com $r = t$, obtemos um código de parâmetros $[n, k, d - t]_q$. □

6. Soma directa

Dados dois códigos q-ários C_1 e C_2 de parâmetros (n_1, M_1, d_1) e (n_2, M_2, d_2), respectivamente, define-se o *código soma* por

$$C_{1\oplus 2} = C_1 \oplus C_2 = \{(x_1, x_2) \,:\, x_1 \in C_1,\, x_2 \in C_2\} \,.$$

Portanto, o código soma contém $M_1 M_2$ palavras de comprimento $n_1 + n_2$.

Lema 5.12. *A distância mínima de $C_1 \oplus C_2$ é $d = \min\{d_1, d_2\}$.*

Dem. Sem perda de generalidade, suponhamos que $d_1 \leq d_2$. Sejam $x_1, y_1 \in C_1$ tal que $\mathrm{d}(x_1, y_1) = d_1 = \mathrm{d}(C_1)$ e seja $x_2 \in C_2$. Como $(x_1, x_2), (y_1, x_2) \in C_{1\oplus 2}$, então

$$\mathrm{d}(C_{1\oplus 2}) \leq \mathrm{d}((x_1, x_2), (y_1, x_2)) = \mathrm{d}(x_1, y_1) = d_1 \,.$$

Por outro lado, para quaisquer palavras $(x_1, x_2), (y_1, y_2) \in C_{1\oplus 2}$ distintas , tem-se

$$\begin{aligned} \mathrm{d}((x_1,x_2),(y_1,y_2)) &\geq \mathrm{d}(x_1,y_1) \geq d_1 && \text{se } x_1 \neq y_1 \ , \\ \mathrm{d}((x_1,x_2),(y_1,y_2)) &\geq \mathrm{d}(x_2,y_2) \geq d_2 \geq d_1 && \text{se } x_2 \neq y_2 \ , \end{aligned}$$

portanto, tomando o mínimo entre pares de palavras distintas, $\mathrm{d}(C_{1\oplus 2}) \geq d_1$. □

No caso de C_1 e C_2 serem códigos lineares de parâmetros $[n_1, k_1, d_1]_q$ e $[n_2, k_2, d_2]_q$, respectivamente, $C_1 \oplus C_2$ é a soma directa de espaços vectoriais, portanto é ainda um espaço vectorial. Como $|C_1 \oplus C_2| = M_1 M_2 = q^{k_1+k_2}$, conclui-se que $\dim(C_1 \oplus C_2) = k_1 + k_2$. Resolva o Exercício 5.7 para obter uma matriz geradora de $C_1 \oplus C_2$ à custa de matrizes geradoras de C_1 e C_2.

7. Construção de Plotkin

Dados dois códigos q-ários C_1 e C_2 de parâmetros (n, M_1, d_1) e (n, M_2, d_2), respectivamente, define-se um novo código por[1]

$$C_{1*2} = C_1 * C_2 = \{(x, x+y) \,:\, x \in C_1,\, y \in C_2\} \ .$$

Os parâmteros de $C_1 * C_2$ são $(2n, M_1 M_2, d)$, onde $d = \min\{2d_1, d_2\}$ – a distância mínima foi calculada no Exercício 2.12.

No caso de C_1 e C_2 serem códigos lineares, então a construção de Plotkin C_{1*2} também é um código linear: basta verificar o fecho da soma de vectores e do produto de um vector por um escalar, pois C_{1*2} é um subconjunto não-vazio do espaço vectorial $\mathbb{F}_q^{2n}$. Para matrizes geradoras e de paridade, resolva o Exercício 5.8.

Exemplo 5.13. Seja $C_1 = E_2 = \{x \in \mathbb{F}_2^3 \,:\, \mathrm{w}(x) \text{ é par}\}$ e seja C_2 o código de repetição binário de comprimento 3. Então $C_1 = \langle 110, 101\rangle$ e $C_2 = \langle 111\rangle$ têm parâmetros $[3, 2, 2]$ e $[3, 1, 3]$, respectivamente. Portanto, $\{110110, 101101, 000111\}$ é uma base de $C_1 * C_2$ – justifique – e os parâmetros deste código são $[6, 3, 3]$.

Exercícios

5.1. Demonstre o Lema 5.4.

5.2. Verifique as igualdades (5.2) no Exemplo 5.5.

5.3. Mostre que, se C é um código linear binário, então o código $\overline{C} = C \cup C^c$ do Exemplo 5.5 é linear, e determine os seus parâmetros.

5.4. (a) Seja C um código linear $[n, k]_q$ e seja C' a contracção de C obtida pontuando a coordenada i da secção $C_{i,0}$, onde $i \in \{1, \ldots, n\}$. Mostre que C' é um código linear, determine a sua dimensão e uma matriz de paridade.

(b) Seja $C = E_n$ o código binário dos pesos pares de comprimento $n \geq 2$. Justifique que o pontuado da secção $C_{i,1}$ não é um código linear.

5.5. Mostre que se existir um código $[n, k, d]_q$ então também existe um código $[n - r, k - r, d]$ para qualquer $1 \leq r \leq k - 1$.

5.6. Dado um código C $[n, k, d]_q$,

(a) será que existe sempre um código $[n + 1, k, d + 1]_q$?

(b) será que existe sempre um código $[n + 1, k + 1, d]_q$?

5.7. (a) Sejam G_1 e G_2 matrizes geradoras dos códigos lineares q-ários C_1 e C_2, respectivamente. Mostre que

$$G = \begin{bmatrix} G_1 & 0 \\ 0 & G_2 \end{bmatrix}$$

[1] Embora não se exija que C_1 e C_2 sejam lineares, a definição da construção de Plotkin assume que esteja definida uma operação soma no alfabeto dos códigos.

é uma matriz geradora do código soma $C_1 \oplus C_2$.

(b) Escreva uma matriz de paridade para $C_1 \oplus C_2$ em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

5.8. Repita o exercício anterior para a Construção de Plotkin:

(a) Se C_1 e C_2 são códigos lineares, verifique que $C_1 * C_2$ também é linear.

(b) Sejam G_1 e G_2 matrizes geradoras dos códigos lineares q-ários C_1 e C_2, respectivamente, ambos de comprimento n. Mostre que

$$G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$$

é uma matriz geradora do código $C_1 * C_2$.

(c) Escreva uma matriz de paridade para $C_1 * C_2$ em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

5.9. Considere dois códigos lineares C_1 e C_2 sobre $\mathbb{F}_q$, de comprimento n e dimensões $\dim(C_i) = k_i$, $i = 1, 2$, e defina

$$C = \{(a + x, b + x, a + b + x) \,:\, a, b \in C_1, x \in C_2\} \,.$$

(a) Mostre que C é um código linear de parâmetros $[3n, 2k_1 + k_2]$.

(b) Escreva uma matriz geradora de C em termos de matrizes geradoras G_1 e G_2 de C_1 e C_2, respectivamente.

(c) Escreva uma matriz de paridade de C em termos de matrizes de paridade H_1 e H_2 de C_1 e C_2, respectivamente.

Exemplos de Códigos Lineares

1. Códigos de Hamming

Recorde que a *redundância* de um código linear $[n, k, d]_q$ é $r = n - k$, ou seja, é o número de linhas de uma matriz de paridade.

Seja H uma matriz cujas colunas são todos os vectores não nulos do espaço vectorial $\mathbb{F}_2^r$. Portanto H tem r linhas e $2^r - 1$ colunas. Além disso, como os vectores da base canónia $\vec{e_1}, \ldots, \vec{e_r}$ são colunas de H, a matriz identidade I_r é uma submatriz de H com deteminante $\det(I_r) = 1 \neq 0$, portanto as r linhas de H são linearmente independentes, e H é uma matriz de paridade de um código binário.

Definição 6.1. Seja H uma matriz $r \times (2^r - 1)$ cujas colunas são todos os vectores em $\mathbb{F}_2^r \setminus \{\vec{0}\}$. O código binário $\mathrm{Ham}(r, 2)$ com esta matriz de paridade H diz-se um *código de Hamming binário de redundância* r.

Exemplo 6.2. (a) O código de Hamming binário de redundância 2, $\mathrm{Ham}(2, 2)$, tem matriz de paridade

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

Pelo Lema 4.13, $G = \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$ é uma matriz geradora e, portanto, $\mathrm{Ham}(2, 2)$ é o código de repetição binário de comprimento 3, de parâmetros $[3, 1, 3]$.

(b) A matriz

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

é uma matriz de paridade de um código $\mathrm{Ham}(3, 2)$. Este código tem parâmetros $[7, 4, 3]$ – podemos determinar a distância mínima aplicando o Teorema 4.16.

Teorema 6.3. *Seja $r \geq 2$. Então*

(i) $\mathrm{Ham}(r, 2)$ *tem parâmetros* $[2^r - 1, 2^r - r - 1, 3]$*;*

(ii) $\mathrm{Ham}(r, 2)$ *é um código perfeito.*

Dem. (i) Por construção, $\mathrm{Ham}(r, 2)$ tem comprimento $|\mathbb{F}_2^r \setminus \{\vec{0}\}| = 2^r - 1$ e dimensão $k = n - r = 2^r - r - 1$. Só falta ver que a distância mínima é $d = 3$. Sejam c_i, com $i = 1, \ldots, 2^r - 1$, as colunas de uma matriz de paridade H para $\mathrm{Ham}(r, 2)$. Por construção, $c_i \neq c_j$ para quaisquer $i \neq j$, e nenhuma coluna é o vector nulo, logo quaisquer duas colunas de H são linearmente independentes. Por outro lado $c_i = (0, \ldots, 0, 0, 1)$, $c_j = (0, \ldots, 0, 1, 0)$ e $c_k = (0, \ldots, 0, 1, 1)$ são colunas de H, se

$r \geq 2$. Como $c_k = c_i + c_j$, estas três colunas são linearmente dependentes. Logo, pelo Teorema 4.16, $\mathrm{d}(\mathrm{Ham}(r,2)) = 3$.

(ii) Basta ver que os parâmetros determinados em (i) satisfazem a igualdade no majorante de empacotamento de esferas de Hamming. Como $n = 2^r - 1$, $M = 2^{n-r}$ e $d = 3$, então $t = \lfloor \frac{d-1}{2} \rfloor = 1$ e

$$M \,\mathrm{vol}(B_t(x))) = 2^{n-r}\left(\binom{n}{0} + \binom{n}{1}\right) = 2^{n-r}(1+n) = 2^{n-r}2^r = 2^n \ . \qquad \square$$

Observação 6.4. (i) Para r fixo, os códigos $\mathrm{Ham}(r,2)$ são todos equivalentes (basta permutar as colunas numa matriz de paridade) e qualquer código linear com os mesmos parâmetros é equivalente a um $\mathrm{Ham}(r,2)$.

(ii) Existem códigos binários não lineares com parâmetros $(n, 2^{n-r}, 3)$ com $n = 2^r - 1$ (ver Exercício 6.8).

Algoritmo de descodificação para os códigos de Hamming binários

Como $\mathrm{Ham}(r,2)$ é um código perfeito de distância mínima 3, os chefes de classe são precisamente os vectores $x \in \mathbb{F}_2^n$ de peso $\mathrm{w}(x) = 1 = \lfloor \frac{d-1}{2} \rfloor$ (pela Proposição 4.29 e pelo Exercício 4.11). Supondo que as colunas de H estão ordenadas por ordem crescente, i.e., a i-ésima coluna é o número $i \in \{1, \ldots, n = 2^r - 1\}$ escrito na base 2 (como foi feito no Exemplo 6.2(b)), se $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$, com 1 na coordenada i, então o sintoma $S(e_i)$ é a representação binária de i. Assim, temos o seguinte algoritmo de descodificação para $\mathrm{Ham}(r,2)$:

1. Recebido $y \in \mathbb{F}_2^n$, calcular o sintoma $S(y) = Hy$.
2. Se $S(y) = 0$, assumir que não ocorreram erros de transmissão e descodificar y por y.
3. Se $S(y) \neq 0$, então $S(y)$ é uma coluna de H e, se estas estão por ordem crescente, assumir que ocorreu um erro na coordenada i correspondente ao número $S(y)$ na base 2, e descodificar y por $y - e_i$.

Exemplo 6.5. Seja $C = \mathrm{Ham}(4,2)$, portanto $n = 15$. Seja $y = 001100000100000 \in \mathbb{F}_2^{15}$ o vector recebido. As coordenadas 1 de y estão nas posições 3, 4 e 10. Como $3_{(10)} = 0011_{(2)}$, $4_{(10)} = 0100_{(2)}$ e $10_{(10)} = 1010_{(2)}$, fica

$$S(y) = c_3 + c_4 + c_{10} = \begin{bmatrix}0\\0\\1\\1\end{bmatrix} + \begin{bmatrix}0\\1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\0\\1\\0\end{bmatrix} = \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = c_{13}$$

pois $13_{(10)} = 1101_{(2)}$. Descodificamos y por $y - e_{13} = 001100000100100 \in C$.

Como se pode ver neste exemplo, a vantagem de assumir que as colunas de H estão escritas por ordem crescente é não ser necessário escrever a matriz H para se calcular os sintomas.

Códigos de Hamming binários estendidos

Consideremos a extensão por paridade $\widehat{\mathrm{Ham}}(r,2)$ do código de Hamming binário $\mathrm{Ham}(r,2)$ definida na Secção 1 do Capítulo 5. Portanto o código estendido $\widehat{\mathrm{Ham}}(r,2)$ é linear e, pelo Lema 5.3, tem parâmetros $[2^r, 2^r - r - 1, 4]$.

Como $\mathrm{d}(\widehat{\mathrm{Ham}}(r,2)) = 4$, este código apenas corrige um erro, tal como $\mathrm{Ham}(r,2)$, mas o código estendido pode ser usado para simultaneamente corrigir qualquer erro simples e detectar qualquer erro duplo. Deixamos como exercício descrever um tal algoritmo.

Códigos de Hamming q-ários

Um código de Hamming q-ário de redundância r, $\mathrm{Ham}(r,q)$, é um código de parâmetros

$$\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1}-r, 3\right] .$$

Para mostrar que existem, vamos determinar uma matriz de paridade H para $\mathrm{Ham}(r,q)$. Para termos $\mathrm{d}(\mathrm{Ham}(r,q))=3$, quaisquer duas colunas de H têm de ser linearmente independentes e têm de existir três colunas linearmente dependentes. Seja

$$M_v = \{\lambda v \,:\, \lambda \in \mathbb{F}_q \setminus \{0\}\} ,$$

com $v \in \mathbb{F}_q^r \setminus \{\vec{0}\}$. Ou seja, M_v é o conjunto dos múltiplos escalares não nulos do vector $v \neq \vec{0}$. Portanto $|M_v| = q-1$ e dois vectores v_1 e v_2 são linearmente independentes se e só se $M_{v_1} \cap M_{v_2} = \varnothing$, donde se conclui que há precisamente

$$\frac{|\mathbb{F}_q^r \setminus \{\vec{0}\}|}{|M_v|} = \frac{q^r-1}{q-1}$$

classes de vectores linearmente independentes dois a dois em $\mathbb{F}_q^r$. As colunas de H são obtidas escolhendo um vector em cada classe M_v. Por outro lado, os vectores $(0,\ldots,0,0,a)$, $(0,\ldots,0,b,0)$ e $(0,\ldots,0,c,c)$ são colunas de H, para alguma escolha $a,b,c \in \mathbb{F}_q \setminus \{0\}$, e são linearmente dependentes. Pelo Teorema 4.16, um código com esta matriz de paridade tem distância mínima 3.

Agora só falta ver que as linhas de H são linearmente independentes, para H ser de facto uma matriz de paridade. Deixamos essa verificação como exercício.

Observação 6.6. Tal como no caso binário, os códigos $\mathrm{Ham}(r,q)$, com r e q fixos, são todos linearmente equivalentes por construção: qualquer matriz de paridade é obtida a partir de outra permutando colunas (escolher vectores em classes distintas M_v por ordens diferentes) e/ou multiplicando colunas por escalares não nulos (escolher dois vectores diferentes na mesma classe M_v, para matrizes H diferentes).

Exemplo 6.7. $\mathrm{Ham}(2,3)$ é um código ternário (ou é uma classe de códigos) com parâmetros $[4,2,3]$. Como as classes de vectores linearmente independentes são

$$M_{(0,1)} = \{(0,1),(0,2)\},\ M_{(1,0)} = \{(1,0),(2,0)\},\ M_{(1,1)} = \{(1,1),(2,2)\} \text{ e } M_{(1,2)} = \{(1,2),(2,1)\}.$$

as matrizes

$$H_1 = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \end{bmatrix},\ H_2 = \begin{bmatrix} 0 & 1 & 2 & 1 \\ 2 & 0 & 2 & 2 \end{bmatrix},\ H_3 = \begin{bmatrix} 2 & 0 & 1 & 2 \\ 0 & 2 & 1 & 1 \end{bmatrix} \text{ e } H_4 = \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 2 \end{bmatrix}$$

são matrizes de paridade destes códigos equivalentes.

Exemplo 6.8. $\mathrm{Ham}(3,3)$ tem parâmetros $n = \frac{3^3-1}{3-1} = 13$, $k = n-r = 10$ e $d = 3$, e

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

é uma matriz de paridade para este código.

Teorema 6.9. *Os códigos de Hamming* $\mathrm{Ham}(r,q)$ *são perfeitos.*

A demonstração é análoga ao caso binário. Como consequência, tem-se que, para $n = \dfrac{q^r-1}{q-1}$,

$$A_q(n,3) = q^{n-r} \quad \forall r \geq 2 .$$

Algoritmo de descodificação para os códigos de Hamming q-ários

Vamos assumir que a matriz de paridade H tem as colunas escritas por ordem lexicográfica e que a primeira entrada não nula de cada coluna é 1. No Exemplo 6.7 escolheriamos a matriz H_1, no Exemplo 6.8 a matriz H está na forma pretendida.

Como $\mathrm{Ham}(q,r)$ é um código perfeito de distância mínima 3, o sintoma de qualquer vector y é $S(y)=\vec{0}$ ou $S(y)=S(\lambda e_i)$ para algum $\lambda\in\mathbb{F}_q$ e $e_i=(0,\ldots,0,1,0,\ldots,0)$ com 1 na coordenada $i\in\{1,\ldots,n\}$. Portanto:

1. Recebido $y\in\mathbb{F}_q^n$, calcular o sintoma $S(y)$.
2. Se $S(y)=0$, então assumir que não houve erros de transmissão.
3. Caso contrário, $S(y)=\lambda c_i\neq 0$ para alguma coluna c_i de H e escalar não nulo λ. Assumir que o vector de erro é λe_i e descodificar y por $y-\lambda e_i$.

O algoritmo descrito para os códigos de Hamming binários é um caso particular deste, onde se tem necessarimante $\lambda=1$.

Exemplo 6.10. Seja $C=\mathrm{Ham}(3,3)$ com a matriz de paridade do Exemplo 6.8. Supondo que recebemos o vector $y=1101112211201\in\mathbb{F}_3^{13}$, como

$$S(y)=Hy=\begin{bmatrix}2\\0\\1\end{bmatrix}=2\begin{bmatrix}1\\0\\2\end{bmatrix}\ ,$$

assumimos que ocorreu um erro na coordenada 7 e descodificamos y por $y-2e_7=1101110211201$.

Se aplicarmos a construção contracção definida na Secção 5 do Capítulo 5 a um código de Hamming $\mathrm{Ham}(r,q)$ obtêm-se códigos $[n-s,n-r-s,d]$ com $d\geq 3$. Se a redundância r for pequena, em muitos casos ainda ficamos com códigos de distância mínima $d=3$ mas, em geral, com maior capacidade de detecção de erros.

Exemplo 6.11. Consideremos o código $C=\mathrm{Ham}(2,11)$, sobre $\mathbb{F}_{11}$, com matriz de paridade

$$H=\begin{bmatrix}0&1&1&1&1&1&1&1&1&1&1&1\\1&0&1&2&3&4&5&6&7&8&9&X\end{bmatrix}\ .$$

Contraíndo nas duas primeiras coordenadas, obtemos o código C' com matriz de paridade

$$H'=\begin{bmatrix}1&1&1&1&1&1&1&1&1&1\\1&2&3&4&5&6&7&8&9&X\end{bmatrix}\ ,$$

ou seja, o código contraído é o código já estudado no Exemplo 4.36. Como foi visto, $\mathrm{d}(C')=3$ mas C' pode ser usado para corrigir erros simples e, simultâneamente, detectar erros duplos de transposição.

Códigos simplex

Por definição, um código *simplex* é o dual de um código de Hamming

$$S(r,q)\stackrel{\mathrm{def}}{=}\mathrm{Ham}(r,q)^{\perp}\ ,$$

portanto, $S(r,q)$ é um código de comprimento $n=\frac{q^r-1}{q-1}$ e dimensão r.

Proposição 6.12. *Se $x\in S(r,q)\setminus\{\vec{0}\}$, então $\mathrm{w}(x)=q^{r-1}$. Em particular, $\mathrm{d}(S(r,q))=q^{r-1}$.*

Dem. Seja G uma matriz geradora de $S(r,q)$, portanto G é uma matriz de paridade de $\mathrm{Ham}(r,q)$ e, por construção dos códigos de Hamming, cada uma das colunas de G pertence a uma classe $M_x=\{\lambda x:\lambda\in\mathbb{F}_q\setminus\{0\}\}$, com $x\in\mathbb{F}_q^r\setminus\{\vec{0}\}$. Como já se observou anteriormente, cada uma das $n=\frac{q^r-1}{q-1}$ classes M_x contém $q-1$ vectores. Logo, se $v\in\mathbb{F}_q^r$ é um vector não nulo, então $\langle v\rangle^{\perp}\setminus\{\vec{0}\}$

é a união disjunta de $\frac{q^{r-1}-1}{q-1}$ classes M_x (porque o código dual $\langle v\rangle^\perp$ tem dimensão $r-1$), o que implica que $c\cdot v=0$ para as $\frac{q^{r-1}-1}{q-1}$ colunas de G pertencentes às classes M_x contidas em $\langle v\rangle^\perp$.
Por outro lado, sendo c_i, com $i=1,\ldots,n$ as colunas de G, como $S(r,q)$ é o espaço das linhas de G, os vectores em $S(r,q)$ são da forma

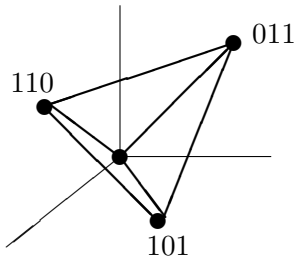
$$G^T v=\begin{bmatrix} c_1\cdot v \\ \vdots \\ c_n\cdot v\end{bmatrix}$$

onde $v\in\mathbb{F}_q^r$. Donde se conclui que as palavras não nulas em $S(r,q)$ têm peso

$$\mathrm{w}(G^T v)=n-\frac{q^{r-1}-1}{q-1}=\frac{q^r-1}{q-1}-\frac{q^{r-1}-1}{q-1}=q^{r-1}\ .$$ □

O nome simplex destes códigos, no caso binário, é justificado pela proposição anterior: as palavras de $S(r,2)$ são os vértices de um símplice-n regular (para a distância de Hamming) em $\mathbb{F}_2^n$, com $n=2^r-1$. Um símplice-2 é um triângulo e tem três vértices, um símplice-3 é um tetraedro e tem quatro vértices. Em geral, um símplice-n em $\mathbb{F}_2^n$ (ou $\mathbb{R}^n$ ou $\mathbb{F}_q^n$ ou ...) é formado por $n+1$ vértices tais que o hiperplano definido por quaisquer n dos vértices não contém o outro vértice.

Exemplo 6.13. Para $r=2$, temos $n=2^r-1=3$ e $|S(r,2)|=2^r=4=n+1$, portanto $S(2,2)=\{000,110,101,011\}\subset\mathbb{F}_2^3$ e podemos representar as palavras deste código na figura



2. Códigos de Reed-Muller

No Exercício 2.12, já definimos a família dos códigos de Reed-Muller por:

$$\begin{aligned}\mathcal{RM}(0,m)&=\{\vec{0},\vec{1}\}=\text{código binário de repetição de comprimento } 2^m\ ;\\ \mathcal{RM}(m,m)&=(\mathbb{F}_2)^{2^m}\ ;\\ \mathcal{RM}(r,m)&=\mathcal{RM}(r,m-1)*\mathcal{RM}(r-1,m-1)\ ,\quad 0<r<m\ .\end{aligned}$$

Uma vez que os códigos de repetição e que $(\mathbb{F}_2)^{2^m}$ são todos códigos lineares, qualquer $\mathcal{RM}(r,m)$ é também um código linear, pois a construção de Plotkin preserva a linearidade, e, como foi visto no Exercícico 2.12, os seus parâmetros são $[2^m,\sum_{i=0}^r\binom{m}{i},2^{m-r}]$.

Proposição 6.14. *Seja $m\in\mathbb{N}$. Seja $x\in\mathcal{RM}(1,m)$. Então $x=\vec{0}$ ou $x=\vec{1}$ ou $\mathrm{w}(x)=2^{m-1}$.*

Dem. Resolva o Exercício 6.7(b). □

Em particular, $\mathcal{RM}(1,m)$ contém $2^{m+1}-2$ vectores de peso 2^{m-1}.

Proposição 6.15. *Seja $0\le r<m$. Então $\mathcal{RM}(r,m)^\perp=\mathcal{RM}(m-r-1,m)$.*

Dem. Resolva o Exercício 6.7(a). □

Proposição 6.16. *Seja $m\ge 1$. Então $\mathcal{RM}(1,m)^\perp$ é equivalente ao código de Hamming binário estendido $\widehat{Ham}(m,2)$.*

Dem. Uma maneira de provar este resultado, que deixamos como exercício (alínea (c) do Exercício 6.7), é obtê-lo como corolário da Proposição 6.15. Aqui apresentamos uma demonstração que usa a Proposição 6.14 e matrizes geradoras dos códigos Reed-Muller e de paridade dos códigos de Hamming binários estendidos.

Uma matriz de paridade para $\mathcal{RM}(1,m)^\perp$ é uma matriz geradora G_m para $\mathcal{RM}(1,m)$. Como $\mathcal{RM}(1,1)=\mathbb{F}_2^2$, podemos escolher

$$G_1=\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}$$

como matriz geradora. Como $\vec{1}\in\mathcal{RM}(1,m)$, pela Proposição 6.14, podemos escolher uma matriz geradora de $\mathcal{RM}(1,m)$ na forma

$$G_m=\left[\begin{array}{c|ccc}1 & 1 & \cdots & 1\\ \hline 0 & & & \\ \vdots & & H_m & \\ 0 & & & \end{array}\right]$$

para alguma matriz H_m. Note que G_1 também está nesta forma. Seja

$$G'_m=\left[\begin{array}{ccc|c} & & & 0\\ & H_m & & \vdots\\ & & & 0\\ \hline 1 & \cdots & 1 & 1\end{array}\right].$$

Então G'_m gera um código equivalente a $\mathcal{RM}(1,m)$ e é uma matriz de paridade de um código estendido $\widehat{C}$, onde $C=\mathcal{N}(H_m)$. Vamos agora provar, por indução matemática em m, que H_m é uma matriz de paridade para $\mathrm{Ham}(m,2)$, ou seja, vamos mostrar que as colunas de H_m são todos os vectores não nulos em $\mathbb{F}_2^m$.

<u>$m=1$:</u> De G_1 vem que $H_1=\begin{bmatrix}1\end{bmatrix}$ que é a matriz de paridade de $\mathrm{Ham}(1,2)$.

<u>$m\Rightarrow m+1$:</u> Suponhamos agora que H_m é uma matriz de paridade de $\mathrm{Ham}(m,2)$. Como

$$G_{m+1}=\left[\begin{array}{ccc|ccc} & G_m & & & G_m & \\ \hline 0 & \cdots & 0 & 1 & \cdots & 1\end{array}\right]=\left[\begin{array}{c|ccc|c|ccc}1 & 1 & \cdots & 1 & 1 & 1 & \cdots & 1\\ \hline 0 & & & & 0 & & & \\ \vdots & & H_m & & \vdots & & H_m & \\ 0 & & & & 0 & & & \\ \hline 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1\end{array}\right]$$

então

$$H_{m+1}=\left[\begin{array}{ccc|c|ccc} & & & 0 & & & \\ & H_m & & \vdots & & H_m & \\ & & & 0 & & & \\ \hline 0 & \cdots & 0 & 1 & 1 & \cdots & 1\end{array}\right].$$

Por hipótese de indução, as colunas de H_m são todos os vectores em $\mathbb{F}_2^m\setminus\{\vec{0}\}$, i.e., representam os números em $\{1,\ldots,2^m-1\}$ na base 2. As colunas de H_{m+1} são

$$\left[\begin{array}{c}|\\ c\\ |\\ \hline 0\end{array}\right],\qquad \left[\begin{array}{c}0\\ \vdots\\ 0\\ \hline 1\end{array}\right]\qquad\text{e}\qquad \left[\begin{array}{c}|\\ c\\ |\\ \hline 1\end{array}\right],$$

onde c é uma coluna de H_m. Estes três tipos de coluna representam, respectivamente, qualquer número par $2i$ com $i\in\{1,\ldots,2^m-1\}$, o número 1 e os números $2i+1$ com $i\in\{1,\ldots,2^m-1\}$, donde se conclui que H_{m+1} é de facto uma matriz de paridade para um código de Hamming binário $\mathrm{Ham}(m,2)$. □

3. Minorante de Gilbert-Varshamov linear

O método usado para construir uma matriz de paridade para $\mathrm{Ham}(r,q)$ permite obter minorantes para $A_q(n,d)$, onde q é uma potência de um número primo.

Teorema 6.17 (Gilbert-Varshamov)**.** *Seja q uma potência de um número primo, $2 \leq d \leq n$ e $1 \leq k \leq n$. Se*

$$\sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i < q^{n-k} \tag{6.1}$$

então existe um código linear $[n,k,d']$ sobre $\mathbb{F}_q$ com $d' \geq d$.

Dem. Assumindo a desigualdade (6.1), vamos provar que existe uma matriz $H_{n-k,n}$ tal que quaisquer $d-1$ colunas são linearmente independentes. Seja $r = n-k$ e seja c_j a coluna j de H. Escolhemos

$$c_1 \in \mathbb{F}_q^r \setminus \{\vec{0}\} \ , \qquad c_2 \in \mathbb{F}_q^r \setminus \langle c_1 \rangle \ , \qquad c_3 \in \mathbb{F}_q^r \setminus \langle c_1, c_2 \rangle \ .$$

Para $2 \leq j \leq n$, c_j pode ser qualquer vector em $\mathbb{F}_q^r$ que não seja combinação linear de $d-2$ (ou menos) colunas $c_1, \ldots, c_{j-1}$ já escolhidas. Portanto, sendo $N(j)$ o número de vectores em $\mathbb{F}_q^r$ que não podem ser escolhidos para c_j, tem-se

$$N(j) = 1 + \binom{j-1}{1}(q-1) + \binom{j-1}{2}(q-1)^2 + \cdots + \binom{j-1}{d-2}(q-1)^{d-2}$$

onde a primeira parcela conta o vector nulo, a segunda parcela conta os múltiplos não nulos das $j-1$ colunas já escolhidas, etc, a i-ésima parcela conta o número de combinações lineares de $i-1$ das colunas já escolhidas com todos os coeficientes não nulos. Ou seja

$$N(j) = \sum_{i=0}^{d-2} \binom{j-1}{i} (q-1)^i \ .$$

É possível escolher a j-ésima coluna c_j se e só se $N(j) < q^r = |\mathbb{F}_q^r|$. Por hipótese, $N(n) < q^r$, logo existe uma matriz $H_{n-k,n}$ tal que quaisquer $d-1$ colunas são linearmente independentes, como pretendiamos. No entanto não temos garantia de que as linhas de H sejam linearmente independentes para poder ser uma matriz de paridade de um código, mas podemos ainda tomar $C = \mathcal{N}(H)$. O núcleo de uma matriz é sempre um espaço vectorial, portanto C é um código linear de comprimento n, dimenão $\dim C \geq k$ (igualdade apenas se as linhas de H são linearmente independentes) e $\mathrm{d}(C) \geq d$ pelo Teorema 4.16. Aplicando agora o Teorema 5.11 sabemos que existe um código C' de parâmetros $[n,k,d']$ com $d' \geq \mathrm{d}(C) \geq d$. □

Corolário 6.18. *Seja q uma potência de um número primo e $2 \leq d \leq n$. Então*

$$A_q(n,d) \geq q^m \qquad \textit{onde} \qquad m = \max\left\{ k \in \mathbb{N} \,:\, q^k \leq \frac{q^n}{\sum_{i=0}^{d-2} \binom{n-1}{i}(q-1)^i} \right\} .$$

Dem. Pelo teorema anterior, sabemos que existe um código C de parâmetros $[n,m,d']$ sobre $\mathbb{F}_q$, com $d' \geq d$. Aplicando o Teorema 5.11 a C com $r = s = 0$ e $t = d - d'$, obtemos um código $[n,m,d]$, que contém q^m palavras, logo $A_q(n,d) \geq q^m$. □

4. Códigos de Golay

Seja G_{24} o código binário com matriz geradora na forma canónica $G = \begin{bmatrix} I_{12} & A \end{bmatrix}$, onde

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

G_{24} diz-se o código de Golay binário estendido.

Lema 6.19. *(i) G_{24} é um código auto-dual, i.e., $G_{24}^{\perp} = G_{24}$;*
(ii) $\begin{bmatrix} A & I_{12} \end{bmatrix}$ é uma matriz geradora de G_{24};
(iii) $\forall\, x \in G_{24}, \mathrm{w}(x) \equiv 0 \mod 4$;
(iv) $\forall\, x \in G_{24}, \mathrm{w}(x) \neq 4$;

Para a demostração deste lema, consultar [**2**].

Teorema 6.20. *O código de Golay binário G_{24} tem parâmetros $[24, 12, 8]$.*

Dem. Por construção, tem-se directamente que G_{24} tem comprimento 24 e dimensão 12. Atendendo a que qualquer linha da matriz geradora $G = \begin{bmatrix} I_{12} & A \end{bmatrix}$, excepto a primeira, tem peso 8, as alíneas (iii) e (iv) do Lema 6.19 implicam que $\mathrm{d}(G_{24}) = 8$. □

O código de Golay G_{23} é o pontuado, na última coordenada, do código G_{24}, portanto os seus parâmetros são $[23, 12, d]$, ou $(23, 2^{12}, d)$, com $7 \leq d \leq 8$. Uma vez que a primeira linha de G é uma palavra de G_{24} com peso 8 e última coordenada igual a 1, o código G_{23} contém uma palavra de peso 7, donde se conclui que G_{23} tem distância mínima $d = 7$ e é um código perfeito. Note ainda que a extensão por paridade de G_{23} é $\widehat{G}_{23} = G_{24}$.

A definição dos códigos de Golay ternários é análoga à dos binários. Seja $G = \begin{bmatrix} I_6 & B \end{bmatrix}$, onde

$$B = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 \\ 1 & 2 & 1 & 0 & 1 & 2 \\ 1 & 2 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 2 & 1 & 0 \end{bmatrix}.$$

Seja G_{12} o código ternário com matriz geradora G. Deixamos a demonstração do seguinte teorema como exercício.

Teorema 6.21. *(i) G_{12} é um código auto-dual;*
(ii) O código de Golay ternário G_{12} tem parâmetros $[12, 6, 6]$.

Definimos G_{11} como o pontuado do código G_{12} na última coordenada, portanto os seus parâmetros são $[11, 6, 5]$, ou $(11, 3^6, 5)$, e é um código perfeito.

5. Códigos de distância máxima de separação ou MDS

A estimativa de Singleton 2.12 para códigos lineares $[n,k,d]_q$ pode ser provada de outra maneira usando o Teorema 4.16: como as colunas de uma matriz de paridade são vectores em $\mathbb{F}_q^{n-k}$ e quaisquer $d-1$ colunas são linearmente dependentes, tem-se necessariamente que $d-1 \leq n-k$, ou seja $d \leq n-k+1$.

Definição 6.22. Um código linear de parâmetros $[n,k,d]$ tal que $d = n-k+1$ diz-se um *código de distância máxima de separação*, ou MDS.

Exemplo 6.23. (i) $C = \mathbb{F}_q^n$ tem parâmetros $[n,n,1]$, é MDS.

(ii) O código de repetição $\langle \vec{1} \rangle \subset \mathbb{F}_q^n$ tem parâmetros $[n,1,n]$, e também é MDS.

(iii) O dual de um código de repetição tem parâmetros $[n,n-1,2]$, e também é MDS.

Definição 6.24. Qualquer código equivalente a um dos do Exemplo 6.23 diz-se um *código MDS trivial*.

O código $[10,8,3]$ sobre $\mathbb{F}_{11}$ do Exemplo 4.36 e os dos Exercícios 4.12 e 4.13 são exemplos de códigos MDS não triviais.

Lema 6.25. *Seja C um código linear $[n,k]_q$ com matriz de paridade H. Então C é MDS se e só se quaisquer $n-k$ colunas de H são linearmente independentes.*

Dem. ($\Longrightarrow$) É consequência imediata do Teorema 4.16.

($\Longleftarrow$) $\mathrm{d}(C) \geq n-k+1$, pelo Teorema 4.16, e $\mathrm{d}(C) \leq n-k+1$, pela estimativa de Singleton. □

Teorema 6.26. *O dual de um código MDS é também um código MDS.*

Dem. Seja C um código linear $[n,k,d]_q$ com $d = n-k+1$. Seja H uma matriz de paridade para C, portanto H é uma matriz geradora do código dual $C^\perp$, de parâmetros $[n,n-k,d']$. Queremos ver que $d' = k+1$. Como $d' \leq k+1$, pela estimativa de Singleton, basta ver que $d' \geq k+1$. Como $\mathrm{d}(C^\perp) = \mathrm{w}(C^\perp)$, basta ver que $\mathrm{w}(x) \geq k+1$ para todo o $x \in C^\perp \setminus \{\vec{0}\}$.

Seja $x \in C^\perp$ tal que $\mathrm{w}(x) \leq k$. Sem perda de generalidade, como x tem no máximo $n-k$ coordenadas nulas, podemos assumir que $x = (x', \vec{0})$ com $x' \in \mathbb{F}_q^k$ e $\vec{0} \in \mathbb{F}_q^{n-k}$. Seja H' a submatriz de H formada pelas últimas $n-k$ colunas desta, ou seja

$$H = \begin{bmatrix} A & H' \end{bmatrix}$$

com A uma matriz $(n-k) \times k$ e H' uma matriz quadrada. Pelo Lema 6.25, porque C é um código MDS, as colunas de H' são linearmente independentes, logo as linhas de H' também são linearmente independentes, porque o espaço das linhas e o espaço das colunas duma matriz têm a mesma dimensão.

Por outro lado, o vector $x = (x', \vec{0})$ é combinação linear das linhas de H, i.e., se $l_1, \ldots, l_{n-k}$ são as linhas de H, então

$$x = \sum_{i=1}^{n-k} \alpha_i l_i \ ,$$

onde os coeficientes $\alpha_i \in \mathbb{F}_q$ são unicamente determinados por x, donde

$$\vec{0} = \sum_{i=1}^{n-k} \alpha_i l'_i \ ,$$

onde l'_i é a i-ésima linha de H' (portanto as entradas de l'_i são as últimas $n-k$ entradas de l_i), logo $\alpha_i = 0$ para todo o i, porque $\{l'_1, \ldots, l'_{n-k}\}$ é um conjunto linearmente independente. Donde se conclui que $x = \vec{0}$ e, portanto, as palavras não nulas de $C^\perp$ têm peso pelo menos $k+1$. □

A alínea (iii) do Exemplo 6.23 é um caso particular deste teorema.

Outra construção que preserva códigos MDS é a pontuação.

Teorema 6.27. *Seja $C \neq \{0\}$ um código $[n,k,d]_q$. Então C é MDS se e só se o pontuado em quaisquer $d-1$ coordenadas é o código trivial $\mathbb{F}_q^k$.*

Dem. Seja $\mathring{C}$ um pontuado de C em $d-1$ coordenadas. Então, por construção, os parâmetros de $\mathring{C}$ são $[n-d+1,k,\mathring{d}]_q$ com $1 \leq \mathring{d} \leq d$. Note que $|\mathring{C}| = |C|$ pois $d-1 > 0$.

($\Leftarrow$) Se $\mathring{C} = \mathbb{F}_q^k$ então os seus parâmetros são $[n-d+1,k,\mathring{d}] = [k,k,1]$, donde $n-d+1 = k$ e concluímos que C é MDS.

($\Rightarrow$) Assumindo agora que C é MDS, i.e., que $d = n-k+1$, o comprimento de $\mathring{C}$ é $n-d+1 = k$, portanto $\mathring{C}$ é um subespaço vectorial de $\mathbb{F}_q^k$ de dimensão k, logo $\mathring{C} = \mathbb{F}_q^k$. □

Corolário 6.28. *Se C é um código MDS de parâmetros $[n,k,d]_q$, então*

(i) dado um subconjunto qualquer de d coordenadas, há exactamente $q-1$ palavras em C de peso d com entradas não nulas nessas coordenadas;

(ii) o número de palavra em C de peso d é

$$A_d = \binom{n}{d}(q-1) \ .$$

Dem. **(i)** Dadas $d = n-k+1$ coordenadas, fixar uma delas, chamemos-lhe i, e pontuar nas restantes $d-1$. Pelo Teorema 6.27, o código pontuado obtido é $\mathring{C} = \mathbb{F}_q^k$. As palavras de C de peso d nas d coordenadas inicialmente fixas dão origem a palavras de peso 1 no código pontuado $\mathring{C}$, mas com a coordenada não nula na posição i fixada. Portanto, há $q-1$ palavras de C nas condições do enunciado, que correspondem exactamente aos múltiplos escalares não nulos do vector com um 1 na posição i e 0 nas restantes.

(ii) É consequência imediata de (i) pois $\binom{n}{d}$ é o número de escolhas de d coordenadas em n. □

O mesmo tipo de argumentos usados na demonstracão do corolário anterior permite obter a seguinte proposicão, cuja demonstração deixamos como exercício.

Proposição 6.29. *Se C é um código MDS de parâmetros $[n,k,d]_q$, então o número de palavras de código com peso $d+1$ é*

$$A_{d+1} = \binom{n}{d+1}\left((q^2-1) - \binom{d+1}{d}(q-1)\right) \ .$$

Exercícios

6.1. Seja C o código binário de Hamming $\mathrm{Ham}(3,2)$ do Exemplo 6.2. Descodifique os vectores recebidos $y = 1101101$ e $z = 1111111$.

6.2. Seja C um código $\mathrm{Ham}(5,2)$ e assuma que a coluna j da matriz de paridade é a representação binária do número j. Indique os parâmetros de C e descodifique o vector recebido $y = \vec{e}_1 + \vec{e}_3 + \vec{e}_{15} + \vec{e}_{20}$, onde $\vec{e}_i$ é o vector cuja coordenada i é 1 e as restantes são nulas.

6.3. Indique os parâmetros e escreva uma matriz de paridade H para $\mathrm{Ham}(2,5)$. Usando a matriz H que escreveu, descodifique o vector recebido $y = 3\vec{e}_1 + \vec{e}_3 + 2\vec{e}_4$.

6.4. Indique os parâmetros e escreva uma matriz de paridade para $\mathrm{Ham}(3,4)$.

6.5. Descreva um algoritmo de descodificação para o código de Hamming binário estendido $\widehat{\mathrm{Ham}}(r,2)$ que permita corrigir qualquer erro simples e detectar erros duplos simultameamente.

6.6. Seja C o código binário com a seguinte matriz de paridade

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

(a) Determine os parâmetros $[n, k, d]$ do código C.
(b) Mostre que C pode ser usado para corrigir todos os erros de peso 1 e todos os erros de peso 2 com a última coordenada não nula. Poderá este código ser usado para corrigir simultaneamente os erros anteriores e mais algum erro de peso 2?
(c) Descreva um algoritmo de descodificação que corrija os erros indicados na alínea anterior e descodifique o vector recebido $y = 10111011$.

6.7. (a) Mostre que

$$\mathcal{RM}(r, m)^{\perp} = \mathcal{RM}(m - r - 1, m), \forall\, 0 \leq r < m.$$

(b) Mostre que $\mathcal{RM}(1, m)$ contém uma única palavra de peso 0, nomeadamante a palavra nula, uma única de peso 2^m, nomeadamente a palavra com 1 em todas as posições, e $2^{m+1} - 2$ palavras de peso 2^{m-1}.
(c) Mostre que $\mathcal{RM}(1, m)$ é equivalente ao dual de um código de Hamming binário estendido.
(d) Conclua que o dual de um código de Hamming binário de redundância r tem todas as palavras equidistantes e de peso igual a 2^{r-1}.

6.8. Dado um código binário C de parâmetros (n, M, d), com $d \geq 3$, define-se

$$C_\lambda = \{(x, x + c, \pi(x) + \lambda(c)) \,:\, x \in \mathbb{F}_2^n, c \in C\} ,$$

onde $\lambda : C \longrightarrow \mathbb{F}_2$ é uma aplicação qualquer e $\pi : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$ é definido por

$$\pi(x) = \begin{cases} 0 & \text{se } \mathrm{w}(x) \text{ é par,} \\ 1 & \text{se } \mathrm{w}(x) \text{ é ímpar .} \end{cases}$$

(a) Determine, justificando, os parâmetros (n', M', d') de C_λ.
(b) Se C é um código linear, mostre que C_λ é linear se e só se λ é uma aplicação linear.
(c) Assumindo que C é um código linear com uma matriz geradora G e que λ é uma aplicação linear, determine uma matriz geradora para C_λ.
(d) Mostre que, se C é um código perfeito com $\mathrm{d}(C) = 3$, então C_λ é perfeito.
(e) Seja $C = \mathrm{Ham}(r, 2)$, com $r \geq 2$, e seja λ a aplicação nula. Será C_λ um código de Hamming? Justifique.
(f) Seja $C = \mathrm{Ham}(r, 2)$, com $r \geq 2$, e seja λ a aplicação constante igual a $1 \in \mathbb{F}_2$. Será C_λ um código de Hamming? Justifique.
(g) Seja $C = \vec{e}_1 + \mathrm{Ham}(r, 2) := \{\vec{e}_1 + c \,:\, c \in \mathrm{Ham}(r, 2)\}$, com $r \geq 2$ e $\vec{e}_1 = (1, 0, \ldots, 0)$, e seja λ a aplicação nula. Será C_λ um código de Hamming? Justifique.

6.9. Justifique que os códigos de Hamming $\mathrm{Ham}(2, q)$, de redundância 2, são códigos MDS.

6.10. Seja $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$, onde α é uma raiz de $1 + t + t^2$. Seja C um código linear sobre $\mathbb{F}_4$ com matriz geradora

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix} .$$

Escreva uma matriz geradora para o código dual $C^{\perp}$. Mostre que C e $C^{\perp}$ são códigos MDS.

6.11. Mostre que os únicos códigos MDS binários são os triviais.

6.12. Seja C um código q-ário MDS de parâmetros $[n, k]$ com $k < n$.
(a) Mostre que existe um código q-ário MDS de comprimento n e dimensão $n - k$.
(b) Mostre que existe um código q-ário MDS de comprimento $n - 1$ e dimensão k.

6.13. Em cada uma das seguintes alíneas, mostre que o código linear C sobre $\mathbb{F}_q$ com matriz de paridade H é MDS, onde $\mathbb{F}_q = \{0, a_1, a_2, \ldots, a_{q-1}\}$ e

(a)
$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_{q-1} \\ a_1^2 & a_2^2 & \alpha_3^2 & \cdots & a_{q-1}^2 \\ \vdots & \vdots & \vdots & & \vdots \\ a_1^{r-1} & a_2^{r-1} & a_3^{r-1} & \cdots & a_{q-1}^{r-1} \end{bmatrix} , \quad 1 \leq r \leq q-2 \ ;$$

(b)
$$H = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 0 \\ a_1 & a_2 & a_3 & \cdots & a_{q-1} & 0 & 0 \\ a_1^2 & a_2^2 & \alpha_3^2 & \cdots & a_{q-1}^2 & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots & 0 & 0 \\ a_1^{r-1} & a_2^{r-1} & a_3^{r-1} & \cdots & a_{q-1}^{r-1} & 0 & 1 \end{bmatrix} , \quad 2 \leq r \leq q-1 \ .$$

6.14. Seja C o código sobre $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ (onde $\alpha^2 = 1 + \alpha$) com matriz de paridade
$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & \alpha & \alpha^2 & 0 & 1 & 0 \\ 1 & \alpha^2 & \alpha & 0 & 0 & 1 \end{bmatrix} .$$
Mostre que C é um código MDS.
Tente generalizar este exemplo, ou justificar que tal não pode ser feito, para obter um código sobre um corpo $\mathbb{F}_q$ arbitrário, de comprimento $q+2$ e redundância $3 \leq r \leq q-1$.

6.15. Seja C um código MDS de parâmetros $[n, k, d]_q$. Prove que
(i) $q^2 - 1$ é o número de palavras em C de peso d ou $d+1$ com as entradas não nulas em $d+1$ coordenadas fixas;
(ii) $\binom{d+1}{d}(q-1)$ é o número de palavras de peso d com as entradas não nulas em $d+1$ coordenadas fixas.
Conclua que o número de palavras do código C de peso $d+1$ é o indicado na Proposição 6.29.

6.16. Determine A_d e A_{d+1} para um código C com os seguintes parâmetros:
(a) $[n, n-1, 2]_2$;
(b) $[n, n-1, 2]_3$;
(c) $[4, 2, 3]_3$.
Dê um exemplo de um código com os parâmetros dados em cada uma das alíneas anteriores.

6.17. (a) Determine todos os códigos MDS $[n, k, d]_q$ com $d = n$.
(b) Se $d < n$, mostre que não existem códigos MDS $[n, k, d]_q$ com $d > q$.
Sugestão: use a Proposição 6.29.

Códigos Perfeitos e Sistemas de Steiner

Sistemas de Steiner são um caso particular de configurações (ou designs). Neste capítulo pretende-se apenas fazer uma breve introdução aos sistemas de Steiner e à sua relação com os códigos perfeitos. Para uma abordagem muitíssimo mais completa, consultar, por exemplo, o livro "A Course in Combinatorics" de van Lint e de Wilson [**3**].

Definição 7.1. Um *sistema de Steiner* $S(t, k, v)$ é formado por

- um conjunto $\mathcal{P}$ contendo v elementos chamados *pontos* e
- uma colecção $\mathcal{B}$ de subconjuntos de $\mathcal{P}$ chamados *blocos*, cada um contendo k pontos,

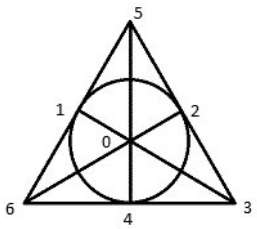
tais que qualquer subconjunto de $\mathcal{P}$ com t elementos está contido precisamente num único bloco.

Para simplificar a terminologia, chama-se *subconjunto-i* a qualquer subconjunto contendo i elementos. Assim, a última condição da definição de sistema de Steiner também se pode enunciar como "qualquer subconjunto-t de $\mathcal{P}$ está contido precisamente num único bloco."
Como consequência imediata da definição, tem-se $t \leq k \leq v$.

Exemplo 7.2. Com $\mathcal{P} = \{p_1, \ldots, p_v\}$ e com um único bloco B contendo todos os pontos, i.e., com $\mathcal{B} = \{\mathcal{P}\}$, definimos um sistema de Steiner $S(t, v, v)$, para qualquer $t \leq v$.

Exemplo 7.3. Com $\mathcal{P} = \{p_1, \ldots, p_v\}$ e v blocos contendo um único ponto, i.e., $\mathcal{B} = \{B_i : i = 1, \ldots, v\}$, onde $B_i = \{p_i\}$, definimos um sistema de Steiner $S(1, 1, v)$.

Exemplo 7.4. Seja $\mathcal{P} = \mathbb{Z}_7$ e $B_x = \{x, x+1, x+3\}$ para cada $x \in \mathbb{Z}_7$. O conjunto de pontos $\mathcal{P}$ e os blocos B_x definem um sistema de Steiner $S(2, 3, 7)$, a que se chama o Plano de Fano, e podemos representá-lo como na seguinte figura



onde as linhas (seis segmentos de recta e uma circunferência) representam os blocos.

O nome "plano" neste último exemplo deve-se ao facto de se definir *plano projectivo de ordem* $k-1$ como um Sistema de Steiner $S(2, k, v)$ onde o número de blocos é igual ao número de pontos. Neste caso, os blocos passam a designar-se por *rectas* e, como $t = 2$, temos que cada par de pontos

distintos definem uma recta pois, por definição de sistema de Steiner, existe um único bloco (ou recta) contendo um dado subconjunto de 2 pontos. O Plano de Fano é o único plano projectivo de ordem 2.

Proposição 7.5. *Num sistema de Steiner $S(t,k,v)$ há*

$$b = \frac{\binom{v}{t}}{\binom{k}{t}}$$

blocos. Em particular $\binom{v}{t}/\binom{k}{t} \in \mathbb{Z}$.

Dem. Considere o conjunto

$$X = \{(P,B) \,:\, P \subset \mathcal{P} \text{ com } |P| = t,\ B \in \mathcal{B} \text{ tais que } P \subset B\}\ .$$

Vamos contar os elementos de X de duas maneiras diferentes. Para cada subconjunto-t $P \subset \mathcal{P}$, existe um único bloco B que o contém. Logo X contém exactamente $\binom{v}{t}$ (= número de subconjuntos-t de $\mathcal{P}$) elementos. Por outro lado, cada bloco B contém $\binom{k}{t}$ subconjuntos-t. Logo X contém $b\binom{k}{t}$ elementos. Igualando as duas expressões para $|X|$, obtém-se o número de blocos b. □

Proposição 7.6. *Para cada $0 \le i \le t$, num sistema de Steiner $S(t,k,v)$ há*

$$b_i = \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}}$$

blocos contendo um dado conjunto-i $I \subset \mathcal{P}$. Em particular $\binom{v-i}{t-i}/\binom{k-i}{t-i} \in \mathbb{Z}$.

Dem. O resultado demonstra-se contando o número de pares (P,B), com $I \subset P \subset \mathcal{P}$ e $B \in \mathcal{B}$ um bloco contendo I, de duas maneiras diferentes, tal como se fez na demonstração da Proposição 7.5 □

Corolário 7.7. *Seja $S(t,k,v)$ um sistema de Steiner com $\mathcal{P}$ o conjunto de pontos e $\mathcal{B}$ o conjunto de blocos. Seja I um subconjunto-i de $\mathcal{P}$, com $i \le t$. Então o conjunto de pontos $\mathcal{P} \setminus I$ e a colecção de blocos $\{B \setminus I \,:\, B \in \mathcal{B}, I \subset B\}$ definem um sistema de Steiner $S(t-i, k-i, v-i)$.*

Definição 7.8. Dado um sistema de Steiner $S(t,k,v)$, definimos uma matriz A cujas entradas são

$$a_{ij} = \begin{cases} 1 & \text{se } p_i \in B_j \\ 0 & \text{se } p_i \notin B_j \end{cases}$$

onde $p_1, \ldots, p_v$ são os pontos e $B_1, \ldots, B_b$ são os blocos de $S(t,k,v)$. A esta matriz A chamamos *matriz de incidência* de $S(t,k,v)$.

Portanto, se A é uma matriz de incidência de $S(t,k,v)$, então

(1) cada coluna tem exactamente k entradas não nulas,

(2) quaisquer duas colunas têm no máximo $t-1$ entradas 1 em comum (na mesma posição).

Exemplo 7.9. As matrizes de incidência dos Exemplos 7.2 e 7.3 são, respectivamente, a matriz coluna com v entradas iguais a 1 e a matriz identidade $v \times v$.

Exemplo 7.10. A matriz de incidência para $S(2,3,7)$ do Exemplo 7.4 é

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

Definição 7.11. Dados $u, v \in \mathbb{F}_2^n$, diz-se que u *cobre* v, ou u é uma *cobertura* de v, se $u \cap v = v$.

Facilmente se vê que a condição $u \cap v = v$ é equivalente a $v_i = 1 \Rightarrow u_i = 1$ para $i = 1, \ldots, n$.

Lema 7.12. *Sejam $x, y \in \mathbb{F}_q^n$. Então*

(a) $\mathrm{w}(x - y) \geq \mathrm{w}(x) - \mathrm{w}(y)$;

(b) $\mathrm{d}(x, y) = \mathrm{w}(x) - \mathrm{w}(y)$ *se e só se x cobre y.*

Teorema 7.13. *Se existe um código perfeito binário de comprimento n e distância mínima $2t + 1$, então existe um sistema de Steiner $S(t + 1, 2t + 1, n)$.*

Dem. Seja C um código perfeito binário de comprimento n e distância mínima $2t+1$. Sem perda de generalidade, assumimos que C contém o vector nulo. Seja M a matriz cujas colunas são as palavras do código C com peso $2t + 1$. Vamos provar que M é uma matriz de incidência de um sistema de Steiner $S(t + 1, 2t + 1, n)$. Ou seja, pondo $\mathcal{P} = \{1, \ldots, n\}$ e definindo um bloco $B_x = \{i : x_i = 1\}$ para cada $x \in C$ com peso $\mathrm{w}(x) = 2t + 1$, vamos ver que obtemos um $S(t + 1, 2t + 1, n)$. Por construção, o número de pontos é n e cada bloco contém $2t + 1$ pontos. Só falta mostrar que, para cada subconjunto-$(t + 1)$, existe um único bloco que o contém, ou seja, queremos ver que

$$\forall\, y \in \mathbb{F}_2^n\,,\ \mathrm{w}(y) = t + 1 \quad \exists!\, x \in C \quad \text{tal que} \quad \mathrm{w}(x) = 2t + 1 \quad \text{e} \quad x \text{ cobre } y. \tag{7.1}$$

Como C é um código perfeito corrector de t erros, dado $y \in \mathbb{F}_2^n$, existe uma única palavra de código $x \in C$ tal que $y \in B_t(x)$, i.e., tal que $\mathrm{d}(y, x) \leq t$. Se $\mathrm{w}(y) = t + 1$, então

$$t \geq \mathrm{d}(x, y) = \mathrm{w}(x - y) \geq \mathrm{w}(x) - \mathrm{w}(y) = \mathrm{w}(x) - (t + 1)\ , \tag{7.2}$$

onde se usou o Lema 7.12(a) na segunda desigualdade, donde $\mathrm{w}(x) \leq 2t + 1$. Portanto, como $x \in C$, ou $x = 0$, ou $\mathrm{w}(x) = 2t + 1$. Mas, se $x = 0$, teríamos $t + 1 = \mathrm{w}(y) = \mathrm{d}(y, x) \leq t$, o que é impossível. Assim, como $\mathrm{w}(x) = 2t + 1$, as desigualdades em (7.2) são de facto igualdades, logo $\mathrm{d}(x, y) = \mathrm{w}(x) - \mathrm{w}(y)$ e, pelo Lema 7.12(b), conclui-se que x cobre y, ficando assim provada a afirmação (7.1). □

Exemplo 7.14. Para os códigos perfeitos triviais: os sistemas de Steiner associados ao código de repetição binário de comprimento n e ao código $\mathbb{F}_2^n$, com $n = 2t+1$, são, respectivamente, $S(t+1, n, n)$ e $S(1, 1, n)$, definidos nos Exemplos 7.2 e 7.3.

Exemplo 7.15. O sistema de Steiner associado ao código de Hamming binário $\mathrm{Ham}(3, 2)$ é o plano de Fano $S(2, 3, 7)$ do Exemplo 7.4.

Corolário 7.16. *Seja C um código perfeito binário, de comprimento n e distância mínima $2t + 1$. Então, o número de palavras de código com peso $2t + 1$ é*

$$A_{2t+1} = \frac{\binom{n}{t+1}}{\binom{2t+1}{t+1}}\ .$$

Dem. Como se viu na demonstação do Teorema 7.13, como C é um código perfeito com distância mínima $2t+1$, as palavras de peso $2t+1$ formam os blocos de um sistema de Steiner $S(t+1, 2t+1, n)$. O resultado segue agora da Proposição 7.5. □

Podemos generalizar algumas das afirmações anteriores para códigos perfeitos não necessariamente binários.

Definição 7.17. Dados $x, y \in \mathbb{F}_q^n$, dizemos que x *cobre* y se $y_i = x_i$, quando $y_i \neq 0$, para todo o $i = 1, \ldots, n$.

Proposição 7.18. *Seja C um código perfeito q-ário, de comprimento n e distância mínima $2t + 1$, então, dado $y \in \mathbb{F}_q^n$ com peso $\mathrm{w}(y) = t + 1$, existe um único $x \in C$ com peso $\mathrm{w}(x) = 2t + 1$ tal que x cobre y.*

A demonstração desta proposição é exactamente a mesma da afirmação (7.1). Embora se tenha assumido que o alfabeto do código é $\mathcal{A}_q = \mathbb{F}_q$, não foram usadas propriedades específicas de um corpo, apenas se usou haver uma operação soma definida no alfabeto, e o código conter a palavra nula. Poderiamos ter enunciado o resultado com $\mathcal{A}_q = \mathbb{Z}_q$ e q um inteiro positivo qualquer.

Corolário 7.19. *Seja C um código perfeito q-ário, de comprimento n e distância mínima $2t+1$. Então, o número de palavras de código com peso $2t+1$ é*

$$A_{2t+1} = \frac{\binom{n}{t+1}(q-1)^{t+1}}{\binom{2t+1}{t+1}} \ .$$

Dem. A demonstração é análoga à da Proposição 7.5.

Seja $X = \{(x,y) \in C \times \mathbb{F}_q^n : \mathrm{w}(x) = 2t+1, \mathrm{w}(y) = t+1, x \text{ cobre } y\}$. O número de vectores em $\mathbb{F}_q^n$ de peso $t+1$ é $\binom{n}{t+1}(q-1)^{t+1}$ – escolhem-se $t+1$ coordenadas em n e, para cada uma destas, escolhe-se um escalar não nulo em $\mathbb{F}_q$. Pela proposição 7.18, há exactamente uma palavra de código de peso $2t+1$ que cobre um dado vector arbitrário (mas fixo) de peso $t+1$. Portanto $|X| = \binom{n}{t+1}(q-1)^{t+1}$. Por outro lado, cada vector de $\mathbb{F}_q^n$ de peso $2t+1$ cobre $\binom{2t+1}{t+1}$ vectores em $\mathbb{F}_q^n$ de peso $t+1$ – escolhem-se $t+1$ coordenadas entre as $2t+1$ coordenadas do primeiro vector. Portanto $|X| = \binom{2t+1}{t+1}A_{2t+1}$. Igualando as duas expressões para $|X|$, obtém-se o resultado pretendido. □

Outros códigos perfeitos

Para além dos códigos perfeitos triviais, já vimos que os códigos de Hamming $\mathrm{Ham}(r,q)$ e os códigos de Golay G_{23} e G_{11} são perfeitos. Os parâmetros $(90, 2^{78}, 5)_2$ também satisfazem a igualdade no majorante de Hamming.

Teorema 7.20. *Não existem códigos binários com parâmetros* $(90, 2^{78}, 5)$.

Dem. Suponhamos que existe um código binário $(90, 2^{78}, 5)$. Como este código é perfeito, pelo Teorema 7.13, existe um sistema de Steiner $S(3,5,90)$ e, pela Proposição 7.6,

$$b_2 = \frac{\binom{88}{1}}{\binom{3}{1}} = \frac{88}{33} \notin \mathbb{Z} \ ,$$

o que contradiz a existência de $S(3,5,90)$. □

Terminamos o capítulo enunciando alguns factos sobre a existência de outros códigos perfeitos.

van Lint e Tietäväinen mostraram que um código perfeito q-ário, onde q é uma potência de um primo, não trivial tem os mesmo parâmetros de um código de Hamming ou de um código de Golay. Por construção, códigos perfeitos lineares com os mesmos parâmetros de um código de Hamming têm de ser necessariamente equivalentes a um destes. Mas conhecem-se códigos perfeitos não lineares com os mesmos parâmetros dos códigos de Hamming – Vasil'ev (1962) para os binários, Schömheim (1968) e Lindström (1969) para qualquer potência de um primo (ver Exercício 6.8 para alguns exemplos). No entanto, os únicos códigos de parâmetros $(23, 2^{12}, 7)_2$ ou $(11, 3^6, 5)_3$ são os códigos de Golay G_{23} e G_{11}.

Exercícios

7.1. Demonstre o Lema 7.12: Sejam $x, y \in \mathbb{F}_q^n$. Mostre que
   (a) $\mathrm{w}(x-y) \geq \mathrm{w}(x) - \mathrm{w}(y)$;
   (b) $\mathrm{d}(x,y) = \mathrm{w}(x) - \mathrm{w}(y)$ se e só se x cobre y.

7.2. Considere o espaço vectorial $V = \mathbb{F}_q^3$.
   (a) Mostre que V contém $\frac{q^3-1}{q-1} = q^2+q+1$ subespaços vectoriais de dimensão 1.
   (b) Mostre que V contém $\frac{q^3-1}{q-1} = q^2+q+1$ subespaços vectoriais de dimensão 2.
   (c) Seja $\mathcal{P}$ o conjunto dos subespaços de dimensão 1 e seja $\mathcal{B}$ o conjunto dos subespaços de dimensão 2. Mostre que $\mathcal{P}$ (o conjunto dos pontos) e $\mathcal{B}$ (o conjunto dos blocos), com a relação $P \in \mathcal{P}$ pertence a $B \in \mathcal{B}$ se P é subespaço de B, definem um sistema de Steiner $S(2, q+1, q^2+q+1)$.

Observação: Como o número de pontos e o número de blocos é o mesmo, este sistema de Steiner diz-se uma geometria projectiva de dimensão 2 (ou um plano projectivo) de ordem q, e é geralmente denotado por $PG(2,q)$ ou $PG_2(q)$.

7.3. A partir do código de Golay extendido G_{24}, construa um sistema de Steiner $S(5,8,24)$.

7.4. (Generalização do exercício anterior.) Seja C um código binário perfeito de comprimento n e distância mínima $2t+1$. Mostre que existe um sistema de Steiner $S(t+2, 2t+2, n+1)$.

7.5. Mostre que o código de Hamming q-ário $\mathrm{Ham}(r,q)$ contém

$$A_3 = \frac{q(q^r-1)(q^{r-1}-1)}{6}$$

palavras de peso 3.

7.6. Quantas palavras de peso 7 há em G_{23}?

7.7. Quantas palavras de peso 5 há em G_{11}?

7.8. Para qualquer código C define-se o *polinómio enumerador de pesos*[1] por

$$W_C(t) = \sum_{i\geq 0} A_i t^i \ , \quad \text{onde} \quad A_i = \#\{x \in C \,:\, \mathrm{w}(x) = i\} \ .$$

Se C é um código binário, de comprimento n, mostre que

(a) $W_{C'}(t) = \frac{1}{2}\big(W_C(t) + W_C(-t)\big)$, onde $C' = \{x \in C \,:\, \mathrm{w}(x) \text{ é par}\}$;

(b) $W_{\widehat{C}}(t) = \frac{1}{2}\big((1+t)W_C(t) + (1-t)W_C(-t)\big)$, onde $\widehat{C}$ é a extensão por paridade de C.

7.9. Determine o polinómio enumerador de pesos do código C quando

(a) $C = \widehat{\mathrm{Ham}}(3,2)$;

(b) $C = G_{24}$ [sugestão: mostre que $\vec{1} \in G_{24}$];

(c) $C = G_{23}$.

7.10. (a) Seja $C \subset \mathbb{F}_2^8$ um código linear auto-dual. Determine todos os possíveis polinómios enumeradores de pesos para C. Dê um exemplo de um código auto-dual para cada um dos polinómios encontrados. [Sugestão: Exercício 4.4.]

(b) Mostre que, se C e C' são códigos binários auto-duais de comprimento 8 com o mesmo polinómio enumerador de pesos, então C e C' são códigos equivalentes.

7.11. Seja p um primo e seja $\zeta \in \mathbb{C}$ uma raiz-p primitiva da unidade, i.e., $\zeta^p = 1$ e $\zeta^i \neq 1$ para $1 \leq i \leq p-1$. Dada uma função $f\colon \mathbb{F}_p^n \to V$ qualquer, onde V é um espaço vectorial complexo, define-se $\widehat{f}\colon \mathbb{F}_p^n \to V$ por[2]

$$\widehat{f}(x) = \sum_{y \in \mathbb{F}_p^n} f(y)\zeta^{x\cdot y} \ ,$$

onde $x \cdot y$ denota o produto interno euclideano em $\mathbb{F}_p^n$. Seja $C \subset \mathbb{F}_p^n$ um código linear.

(a) Define-se $C_i(y) = \{x \in C \,:\, x \cdot y = i\}$, para $y \in \mathbb{F}_p^n$ e $i \in \mathbb{F}_p$. Mostre que $C = \cup_{i\in\mathbb{F}_p} C_i(y)$. Mostre também que $C_i(y)$ é uma classe de $C_0(y)$ em C se e só se $y \notin C^\perp$, ou seja, mostre que

$$\Big(\forall\, i \in \mathbb{F}_p \quad \exists\, c_i \in C \quad \text{t.q.} \quad C_i(y) = c_i + C_0(y)\Big) \Longleftrightarrow y \notin C^\perp \ .$$

(b) Mostre que

$$\sum_{x\in C} \zeta^{x\cdot y} = \begin{cases} |C| & \text{se } y \in C^\perp, \\ 0 & \text{se } y \notin C^\perp. \end{cases}$$

(c) Mostre que, para $y \in \mathbb{F}_p^n$,

$$f(y) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_p^n} \widehat{f}(x)\zeta^{-x\cdot y} \ .$$

---

[1] Note que o polinómio $W_C(t)$ não é mais que a função geradora da sucessão $\{A_i\}_{i\in\mathbb{N}_0}$

[2] Neste exercício, identificamos uma classe em $\mathbb{F}_p = \mathbb{Z}_p$ com o respectivo representante inteiro entre 0 e $p-1$.

(d) Mostre que

$$\sum_{y\in C^{\perp}} f(y) = \frac{1}{|C|}\sum_{x\in C}\widehat{f}(x)\ .$$

(e) Seja $f(y) = t^{\mathrm{w}(y)} \in \mathbb{C}[t]$. Mostre que, para $x \in \mathbb{F}_p^n$,

$$\widehat{f}(x) = \big(1+(p-1)t\big)^{n-\mathrm{w}(x)}(1-t)^{\mathrm{w}(x)}\ .$$

(f) Prove a *Identidade de MacWilliams*[3] para os polinómios enumeradores de pesos de C e do seu dual $C^{\perp}$:

$$W_{C^{\perp}}(t) = \frac{1}{|C|}\big(1+(p-1)t\big)^n W_C\Big(\frac{1-t}{1+(p-1)t}\Big)\ .$$

(g) Escreva o polinómio enumerador de pesos para $\mathrm{Ham}(r,p)$.
Sugestão: Recorde que $\mathrm{Ham}(r,p) = S(r,p)^{\perp}$ e determine $W_{S(r,p)}(t)$.

[3] A Identidade de MacWilliams é válida para o corpo $\mathbb{F}_q$, com q não necessariamente um primo. Para uma demonstração geral pode consultar [**4**]. Em [**2**] apenas é feito o caso binário.

Códigos Cíclicos

1. Introdução

Um código linear C tem várias vantagens em relação a um código arbitrário sem qualquer estrutura adicional: C fica completamente descrito por uma matriz geradora (apenas k palavras em vez da lista de todas as q^k palavras de código), é mais fácil testar se uma dada palavra pertence ao código através de uma matriz de paridade, há algoritmos de descodificacão que requerem "pouca informação armazenada" (pelo menos em relação a um código arbitrário). Os códigos cíclicos são uma subclasse dos códigos lineares que ainda requerem menos informação para se poder descrever todas as palavras de código, basta um polinómio de grau menor do que o comprimento das palavras, e com algoritmos de descodificação mais eficientes. Além disso, os códigos de Hamming binários, os códigos de Golay G_{11} e G_{23}, e outras famílias importantes (como, por exemplo, os códigos BCH, Reed-Solomom e Goppa) são códigos cíclicos.

Definição 8.1. Um código C diz-se *cíclico* se

(i) C é linear (portanto C é subespaço de algum $\mathbb{F}_q^n$) e

(ii) se $x = (x_1, x_2, \ldots, x_{n-1}, x_n) \in C$, então $(x_n, x_1, x_2, \ldots, x_{n-1}) \in C$.

O vector $(x_n, x_1, x_2, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ diz-se um *desvio cíclico* de $x \in \mathbb{F}_q^n$, e iremos denotá-lo por $\sigma(x)$. Portanto, um código é cíclico se é linear e se contém os desvios cíclicos de todas as palavras de código. Mais geralmente, se C é um código cíclico, então $\sigma^i(c) \in C$ para todo o $c \in C$ e todo o $i \in \mathbb{Z}$ – ver Exercício 8.1.

Exemplo 8.2.
- Os códigos triviais $\{\vec{0}\}$ e $\mathbb{F}_q^n$ são cíclicos.
- O código binário $E_2 = \{000, 110, 101, 011\}$ é cíclico.
- O código simplex $S(3,2) = \{0000000, 1011100, 0101110, 0010111, 1001011, 1100101, 1110010, 0111001\}$ é cíclico.
- $C_1 = \{0000, 1010, 0101, 1111\}$ é um código cíclico binário.
- O código binário $C_2 = \{0000, 1001, 0110, 1111\}$ não é cíclico, embora seja linear, e é equivalente ao código C_1 do ponto anterior.
- O código binário $C_3 = \{0000, 1010, 0101\}$ não é cíclico porque não é linear, mas contém todos os desvios cíclicos da todas as suas palavras.
- $\mathrm{Ham}(2,3)$ não é cíclico nem equivalente a um código cíclico – ver Exercício 8.6.

Teorema 8.3. *O dual de um código cíclico é ainda um código cíclico.*

Dem. Seja C um código cíclico de comprimento n. Como o dual de um código linear é linear, só temos de verificar a condição (ii) na definição de código cíclico para $C^\perp$. Por definição de dual e

porque C é cíclico,

$$x \in C^\perp \iff x \cdot \sigma^{-1}(c) = 0 \quad \forall\, c \in C \ ,$$

mas como

$$x \cdot \sigma^{-1}(c) = \sum_{i=1}^{n} x_i c_{i+1} = \sigma(x) \cdot c \ ,$$

onde os índices são tomados módulo n, fica

$$x \in C^\perp \iff \sigma(x) \in C^\perp \ . \qquad \square$$

Como consequência deste teorema e do terceiro ponto do Exemplo 8.2, o código de Hamming binário $\mathrm{Ham}(3,2)$ é cíclico. Iremos ver que qualquer código de Hamming binário é equivalente a um código cíclico. Tal não se verifica, em geral, para os códigos de Hamming q-ários.

2. Polinómio gerador

Iniciamos esta secção apresentando algumas noções de álgebra de que iremos precisar já de seguida. Os anéis que iremos considerar no resto do capítulo são o anel dos polinómios $\mathbb{F}_q[t]$ e quocientes deste, por isso vamos sempre assumir que R é um anel comutativo com identidade.

Definição 8.4. O subconjunto não vazio $I \subset R$ diz-se um *ideal* de R se é fechado para a soma e para o produto por qualquer elemento de R, mais precisamente, se $a + b \in I$ e $ar \in I$ para todo o $a, b \in I$ e $r \in R$.

Dado $a \in R$, o conjunto $\langle a \rangle := \{ar : r \in R\}$ é um ideal (verifique) e diz-se o *ideal gerado por* r e o elemento a diz-se um *gerador* do ideal, e pode não ser único. Mais geralmente, o conjunto $\langle a_1, \ldots, a_N \rangle := \{\sum_i a_i r_i : r_i \in R\}$ é um ideal e $\{a_1, \ldots, a_N\}$ diz-se um conjunto gerador.

Definição 8.5. Um ideal $I \subset R$ diz-se um *ideal principal* se $I = \langle a \rangle$ para algum $a \in R$. Se todos os ideais são principais, R diz-se um *anel de ideais principais*[1].

Exemplo 8.6.
- O conjunto $\{0\}$ e o próprio anel $R = \langle 1 \rangle$ são ideais principais.
- Se R é um corpo, $\{0\}$ e R são os únicos ideais.
- No anel dos inteiros $\mathbb{Z}$, o conjunto dos números pares é um ideal e também é principal: $\langle 2 \rangle = \{2x : x \in \mathbb{Z}\}$. O inteiro -2 também é um gerador deste ideal.
- Em $\mathbb{Z}[t]$, o ideal $\langle 2, t \rangle$ não é principal.

Teorema 8.7. *$\mathbb{F}_q[t]$ é um anel de ideais principais[2]. Mais concretamente, se $I \neq \{0\}$ é um ideal, então $I = \langle g(t) \rangle$, onde $g(t)$ é um polinómio mónico de grau mínimo em I. Além disso, este $g(t)$ é único.*

Dem. Seja $I \neq \{0\}$ um ideal de $\mathbb{F}_q[t]$. Seja $g(t)$ um polinómio não nulo de grau mínimo em I. Sem perda de generalidade, podemos assumir que $g(t)$ é mónico (caso não seja, multiplicamos $g(t)$ pelo inverso do coeficiente de maior grau). Queremos ver que este $g(t)$ é um gerador do ideal I. Seja $a(t)$ um elemento em I qualquer. Pelo algoritmo da divisão em $\mathbb{F}_q[t]$, existem polinómios $q(t)$ e $r(t)$ tais que $a(t) = g(t)q(t) + r(t)$, com $\mathrm{grau}(r(t)) < \mathrm{grau}(g(t))$, portanto $r(t) = a(t) - g(t)q(t) \in I$. Como $g(t)$ tem grau mínimo entre os polinómios não nulos em I, então o resto $r(t)$ é nulo e $a(t) = g(t)q(t) \in \langle g(t) \rangle$. Como $a(t) \in I$ é arbitário, conclui-se que $I \subset \langle g(t) \rangle$. E como $g(t) \in I$, também se verifica a inclusão inversa $I \supset \langle g(t) \rangle$, donde $I = \langle g(t) \rangle$.

Deixamos como exercício verificar que existe um único polinómio mónico gerador do ideal I. $\square$

[1] E se R for um domínio integral onde todos os ideias são principais, dizemos que R é um domínio de ideais principais ou, abreviadamente, um d.i.p.

[2] Este resultado verifica-se para $\mathbb{K}[t]$, onde $\mathbb{K}$ é um corpo qualquer, não necessarimente finito

Com o mesmo tipo de demonstração, usando o algoritmo da divisão para os inteiros, também se prova que $\mathbb{Z}$ é um anel de ideais principais. O caso do anel $\mathbb{F}_q[t]$ vai ser útil no contexto dos códigos cíclicos.

Vamos agora traduzir a condição combinatórica dos desvios cíclicos na Definição 8.1 numa condição algébrica. Considere o anel quociente $R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$. Este anel tem uma estrutura natural de espaço vectorial sobre $\mathbb{F}_q$. Considere a aplicação linear, sobre $\mathbb{F}_q$,

$$\begin{aligned} \varphi : \mathbb{F}_q^n &\longrightarrow R_n \\ a = (a_0, a_1, \ldots, a_{n-1}) &\longmapsto a(t) = a_0 + a_1 t + \cdots + a_{n-2}t^{n-2} + a_{n-1}t^{n-1} \end{aligned}$$

Como cada classe em R_n tem um único representate em $\mathbb{F}_q[t]$ de grau menor ou igual a $n-1$ (nomeadamente o resto da divisão por $t^n - 1$), a aplicação φ é um isomorfismo vectorial (verifique!), além disso

$$\begin{aligned} \varphi(\sigma(a)) &= \varphi(a_{n-1}, a_0, a_1, \ldots, a_{n-2}) \\ &= a_{n-1} + a_0 t + \cdots + a_{n-2}t^{n-1} \\ &= ta(t) \ , \end{aligned}$$

onde se usou $t^n = 1$, em R_n, no último passo. Portanto

$$\boxed{\varphi(\sigma(a)) = t\varphi(a)} \tag{8.1}$$

ou seja, tomar o desvio cíclico $\sigma(a)$ em $\mathbb{F}_q^n$ corresponde à multiplicação por t em R_n.

Teorema 8.8. *Um subconjunto $C \subset \mathbb{F}_q^n$ não vazio é um código cíclico se e só se $I = \varphi(C)$ é um ideal de R_n.*

Dem. ($\Longleftarrow$) Como I é um ideal, então I é fechado para a soma e para o produto por escalares (que são identificados com os polinómio constantes em R_n), ou seja, I é um subespaço vectorial de R_n, portanto $C = \varphi^{-1}(I)$ é um subespaço vectorial de $\mathbb{F}_q^n$. Como I é fechado para o produto por t, porque é um ideal, então, por (8.1), C é fechado para desvios cíclicos.

($\Longrightarrow$) Como qualquer elemento de R_n é combinação linear de $1, t, \ldots, t^{n-1}$ e I é um subespaço vectorial de R_n, basta verificar que I é fechado para o produto por t^k, com $0 < k < n$.

Por indução em k:

$k = 1$: Seja $a(t) \in I$ e seja $a = \varphi^{-1}(a(t)) \in C \subset \mathbb{F}_q^n$. Como C é cíclico, então $\sigma(a) \in C$, logo $\varphi(\sigma(a)) = ta(t) \in I$, por (8.1).

$k \Rightarrow k+1$: Se $a(t) \in I$, então $t^k a(t) \in I$, por hipótese de indução, logo $t^{k+1}a(t) = t(t^k a(t)) \in I$, pela base de indução. □

Exemplo 8.9. (a) Ao código trivial $C = \{\vec{0}\} \subset \mathbb{F}_q^n$ corresponde o ideal trivial $I = \{0\} \subset R_n$.

(b) Ao código trivial $C = \mathbb{F}_q^n$ corresponde o ideal trivial $I = R_n$.

(c) Para o código dos pesos pares $E_3 = \{000, 110, 101, 011\} \subset \mathbb{F}_2^3$, tem-se

$$I = \varphi(E_3) = \{0, 1+t, 1+t^2, t+t^2\} \subset R_3 = \mathbb{F}_2[t]/\langle t^3 - 1\rangle \ .$$

Como $t + t^2 = t(1+t)$ e $1 + t^2 \equiv t^2(1+t) \pmod{t^3-1}$, então $I = \langle 1+t\rangle$. Mas também é verdade que $I = \langle 1+t^2\rangle = \langle t+t^2\rangle$, como ideal em R_3.

(d) Para o código binário $C_1 \subset \mathbb{F}_2^4$ do Exemplo 8.2, o ideal correspondente em R_4 é $I = \varphi(C) = \{0, 1+t^2, t+t^3, 1+t+t^2+t^3\} = \langle 1+t^2\rangle$, que também é gerado por $t+t^3$.

Tendo em conta o Teorema 8.8, interessa caracterizar os ideais de R_n. Considere a aplicação quociente, que é um homomorfismo de anéis,

$$\pi : \mathbb{F}_q[t] \longrightarrow R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle \ .$$

Lema 8.10. *Se J é um ideal em $\mathbb{F}_q[t]$ então $\pi(J)$ é um ideal em R_n. Se I é um ideal em R_n, então $\pi^{-1}(I)$ é um ideal em $\mathbb{F}_q[t]$ que contém $t^n - 1$.*

Dem. O resultado segue da definição de ideal, tendo em conta que a imagem e a pré-imagem de conjuntos são, respectivamente,

$$\pi(J) := \{\pi(j) \in R_n \,:\, j \in J\} \qquad \text{e} \qquad \pi^{-1}(I) := \{i \in \mathbb{F}_q[t] \,:\, \pi(i) = [i] \in I\} \,. \qquad \square$$

Como consequência deste lema, a aplicação π define uma correspondência biunívoca[3] entre os ideais no quociente R_n e os ideais contendo $t^n - 1$ no anel dos polinómios $\mathbb{F}_q[t]$.

Exemplo 8.11. Considere o ideal $I = \langle 1 + t\rangle \subset R_3$ associado ao código E_3 (ver Exemplo 8.9). De acordo com o Lema 8.10, $\pi^{-1}(I) = \langle 1 + t, 1 + t^2, t + t^2, t^3 - 1\rangle$, mas como

$$1 + t^2 = (1 + t)^2 \,, \qquad t + t^2 = (t + 1)t \qquad \text{e} \qquad t^3 - 1 = (t + 1)(1 + t + t^2) \,,$$

ou seja, como os três polinómios $1+t^2$, $t+t^2$ e t^3-1 são múltiplos de $t+1$, então $\pi^{-1}(I) = \langle 1+t\rangle \subset \mathbb{F}_2[t]$.

Observação 8.12. Nota à notação e terminologia: Recorde que os elementos de R_n são classes de equivalência de polinómios, geralmente identificados com um representante muito "especial", o resto da divisão por $t^n - 1$. Definimos, portanto, grau de um elemento de R_n como o grau deste representante. Rigorosamente, para qualquer $f(t) \in \mathbb{F}_q[t]$, definimos o grau da classe $[f(t)] \in R_n$ por

$$\text{grau}([f(t)]) := \min\{\text{grau}(k(t)) \,:\, k(t) \equiv f(t) \pmod{t^n - 1}\} \,.$$

Portanto, o grau dos elementos de R_n é sempre menor do que n. Note ainda que em $\mathbb{F}_q[t]$ é sempre verdade que $\text{grau}(a(t)b(t)) = \text{grau}(a(t)) + \text{grau}(b(t))$, mas em R_n apenas se verifica que

$$\text{grau}(a(t)b(t)) \leq \text{grau}(a(t)) + \text{grau}(b(t)) \quad \forall\, a(t), b(t) \in R_n \,.$$

Por exemplo, em R_3, $t - 1$ e $1 + t + t^2$ têm graus 1 e 2 respectivamente, mas o seu produto $(t - 1)(1 + t + t^2) = t^3 - 1$ representa a classe nula em R_3, tendo portanto grau $-\infty$ e não grau 3.

Teorema 8.13. *R_n é um anel de ideais principais. Mais concretamente, se $I \neq \{0\}$ é um ideal em R_n, então $I = \langle g(t)\rangle$, onde $g(t)$ é um polinómio mónico de grau mínimo em I. Além disso, este $g(t)$ é único, $g(t)|t^n - 1$ e $g_0 = g(0) \neq 0$.*

Dem. Seja $I \neq \{0\}$ um ideal em R_n e seja $J = \pi^{-1}(I)$. Pelo Lema 8.10, J é um ideal em $\mathbb{F}_q[t]$ que contém $t^n - 1$. Pelo Teorema 8.7, existe um único polinómio mónico $g(t)$ de grau mínimo em J tal que $J = \langle g(t)\rangle \subset \mathbb{F}_q[t]$. Como $t^n - 1 \in J$, então $g(t)$ divide $t^n - 1$ e, como consequência, também se verifica que $g(0) \neq 0$ (caso contrário t seria um divisor de $t^n - 1$ em $\mathbb{F}_q[t]$). Aplicando o Lema 8.10 novamente, $I = \pi(J)$ é gerado pela classe $[g(t)]$ (note que $\pi(\pi^{-1}(A)) = A$, para qualquer $A \subset R_n$, porque π é uma aplicação sobrejectiva). $\square$

Definição 8.14. O polinómio $g(t) \in \mathbb{F}_q[t]$ no Teorema 8.13 diz-se o *polinómio gerador* do código cíclico $C = \varphi(I)$.

Exemplo 8.15. Continuação do Exemplo 8.9:

(a) O polinómio gerador de E_3 é $1 + t$, os outros dois geradores de $I = \varphi(E_3)$ têm grau 2. Note que o polimónio gerador $1 + t$ é precisamente o gerador mónico de $\pi^{-1}(I)$, como se viu no Exemplo 8.11.

(b) O polinómio gerador do código cíclico $\langle 1010, 0101\rangle \subset \mathbb{F}_2^4$ é $1 + t^2$.

A partir de agora identificamos I e C sem fazer necessariamente referência ao isomorfismo vectorial $\varphi : \mathbb{F}_q^n \longrightarrow R_n$.

Lema 8.16. *Seja $g(t) \in \mathbb{F}_q[t]$ tal que $g(t)|t^n - 1$. Então $a(t) \equiv g(t)x(t) \pmod{t^n - 1}$ se e só se $g(t)$ divide $a(t)$ em $\mathbb{F}_q[t]$.*

[3] Esta caracterização dos ideais no anel quociente R/A é válida para qualquer anel comutativo R e qualquer ideal $A \subset R$, não necessariamente principal.

Dem. Seja $h(t) \in \mathbb{F}_q[t]$ tal que $g(t)h(t) = t^n - 1$. Então

$$\begin{aligned} a(t) \equiv g(t)x(t) \pmod{t^n-1} & \\ \iff & \quad a(t) = g(t)x(t) + (t^n-1)y(t) \ , \quad \text{para algum } y(t) \in \mathbb{F}_q[t] \\ \iff & \quad a(t) = g(t)x(t) + g(t)h(t)y(t) = g(t)(x(t)+h(t)y(t)) \end{aligned}$$

ou seja, $g(t)$ divide $a(t)$. □

Teorema 8.17. *Seja $f(t) \in \mathbb{F}_q[t]$. Então $f(t)|t^n - 1$ e $f(t)$ é mónico se e só se $f(t)$ é o polinómio gerador de algum código cíclico.*

Dem. ($\Longleftarrow$) Consequência imediata do Teorema 8.13.
($\Longrightarrow$) Seja $a(t) \in \mathbb{F}_q[t]$ tal que $f(t)a(t) = t^n - 1$, seja $C = \langle f(t) \rangle$ e seja $g(t)$ o polinómio gerador do código C. Queremos ver que $f(t) = g(t)$. Como $g(t) \in \langle f(t) \rangle \subset R_n$, então existe $b(t) \in \mathbb{F}_q[t]$ tal que $g(t) \equiv f(t)b(t) \pmod{t^n-1}$, portanto, pelo Lema 8.16, $f(t)$ divide $g(t)$ em $\mathbb{F}_q[t]$. Como $g(t)$ é o polinómio mónico de grau mínimo em C e $f(t)$ é mónico, conclui-se que $f(t) = g(t)$. □

O teorema anterior permite-nos classificar todos os códigos cíclicos q-ários de comprimento n à custa da factorização de $t^n - 1$ em polinómios irredutíveis em $\mathbb{F}_q[t]$.

Exemplo 8.18. Como $t^3 - 1 = (1+t)(1+t+t^2)$ e $1+t+t^2$ é irredutível em $\mathbb{F}_2[t]$ (porque tem grau 2 e não possui raízes em $\mathbb{F}_2$), então os únicos códigos cíclicos binários de comprimento 3 são

$$R_3 = \langle 1 \rangle \ , \quad \langle 1+t \rangle \ , \quad \langle 1+t+t^2 \rangle = \{0, 1+t+t^2\} \quad \text{e} \quad \langle t^3-1 \rangle = \{0\} \ ,$$

ou, vistos como subespaços vectoriais de $\mathbb{F}_2^3$, os único códigos cíclicos de comprimento 3 são $\mathbb{F}_2^3$, o código dos pesos pares E_3, o código de repetição $\{000, 111\}$ e o código nulo $\{\vec{0}\}$.

3. Matriz geradora e matriz de paridade

Nesta secção recuperamos as características lineares de um código cíclico à custa do seu polinómio gerador.

Teorema 8.19. *Seja $g(t) = g_0 + g_1 t + \cdots + g_r t^r$ o polinómio gerador do código cíclico $C \subset R_n$. Então*

$$G_{(n-r)\times n} = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix} = \begin{bmatrix} — & g(t) & — \\ — & tg(t) & — \\ & \vdots & \\ — & t^{n-r-1}g(t) & — \end{bmatrix}$$

é uma matriz geradora de C e $\dim C = n - r = n - \text{grau}(g(t))$, ou seja, o grau de g(t) é a redundância do código C.

Dem. Como $g_0 \neq 0$, as linhas de G são linearmente independentes. Vamos ver que as linhas também formam um conjunto gerador, como espaço vectorial, do código C. Seja $a(t) \in C = \langle g(t) \rangle$. Então $\text{grau}(a(t)) < n$ e, pelo Lema 8.16, $a(t) = g(t)q(t)$ para algum polinómio $q(t) \in \mathbb{F}_q[t]$. Como $\text{grau}(a(t)) = \text{grau}(g(t)q(t)) = \text{grau}(g(t)) + \text{grau}(q(t))$, então $\text{grau}(q(t)) < n - r$, ou seja,

$$\begin{aligned} q(t) &= q_0 + q_1 t + \cdots + q_{n-r-1}t^{n-r-1} \qquad \text{e} \\ a(t) &= g(t)q(t) = q_0 g(t) + q_1 t g(t) + \cdots + q_{n-r-1}t^{n-r-1}g(t) \ , \end{aligned}$$

ou seja, $a(t)$ é combinação linear de $g(t), tg(t), \ldots, t^{n-r-1}g(t)$, que são precisamente as linhas da matriz G.

Uma vez que as $n - r$ linhas de G formam uma base de C, conclui-se C tem dimensão $n - r$. □

Exemplo 8.20. Já vimos que $g(t) = 1+t^2+t^3+t^4$ é o polinómio gerador do código simplex $S(3,2)$. Pelo teorema anterior,

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

é uma matriz geradora deste código. Note que as colunas de G são de facto os sete vectores não nulos de $\mathbb{F}_2^3$, como devia ser, pois $S(3,2)^\perp = \mathrm{Ham}(3,2)$.

Definição 8.21. Se C é um código cíclico, de comprimento n, com polinómio gerador $g(t)$, então $h(t) = \dfrac{t^n-1}{g(t)} \in \mathbb{F}_q[t]$ diz-se o *polinómio de paridade* de C.

Uma vez que $g(t)$ é mónico, então $h(t)$ também é, pois $h(t)g(t) = t^n - 1$.

Atenção! O polinómio de paridade de um código cíclico C não é, em geral, o polinómio gerador do código dual $C^\perp$, embora este seja cíclico, pelo Teorema 8.3.

Exemplo 8.22. Para o código simplex $S(3,2)$, com polinómio gerador $g(t) = 1 + t^2 + t^3 + t^4$, o polinómio de paridade é $h(t) = \dfrac{t^7-1}{1+t^2+t^3+t^4} = 1 + t^2 + t^3$. Pelos Teoremas 8.17 e 8.19, este $h(t)$ é o polinómio gerador de um código cíclico C com matriz geradora

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

Seja G a matriz geradora de $S(3,2)$ do exemplo anterior. Então, como $G_h G^T \neq 0$, a matriz G_h não é uma matriz de paridade para $S(3,2)$, logo $C \neq S(3,2)^\perp$. No entanto, C e $S(3,2)^\perp$ são códigos linearmente equivalentes – verifique!

Proposição 8.23. *$c(t) \in C$ se e só se $c(t)h(t) \equiv 0 \pmod{t^n-1}$.*

Dem. Seja $c(t) \in \mathbb{F}_q[t]$ um polinómio qualquer. Então

$$\begin{aligned} c(t)h(t) \equiv 0 \pmod{t^n-1} \quad &\iff \quad c(t)h(t) = b(t)(t^n-1)\ , \quad \text{para algum } b(t) \in \mathbb{F}_q[t], \\ &\iff \quad c(t) = b(t)g(t) \\ &\iff \quad c(t) \in \langle g(t) \rangle = C \end{aligned}$$

onde, na última equivalência, se usou o Lema 8.16. □

Teorema 8.24. *Seja C um código cíclico, de comprimento n e dimensão k, com polinómio de paridade $h(t) = h_0 + h_1 t + \cdots + h_k t^k$. Então*

(i) a matriz

$$H = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & \cdots & 0 \\ 0 & k_k & h_{k-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 & 0 \\ 0 & \cdots & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

é uma matriz de paridade para C;

(ii) $\bar{h}(t) := h_0^{-1} t^k h(t^{-1}) \in \mathbb{F}_q[t]$ é o polinómio gerador de $C^\perp$.

Dem. (i) Como $h_k = 1 \neq 0$ (lembre-se que $h(t)$ é um polinómio mónico), as linhas de H são linearmente independentes. Portanto, para mostrar que H é uma matriz de paridade para C, basta ver que $Hc = 0$ se e só se $c \in C$.

Pela Proposição 8.23, $c(t) = c_0 + c_1 t + \cdots + c_{n-1}t^{n-1} \in C$ se e só se $c(t)h(t) \equiv 0 \pmod{t^n - 1}$. Desenvolvendo o produto em $\mathbb{F}_q[t]$, fica

$$\begin{aligned} c(t)h(t) =& c_o h_o + (c_0 h_1 + c_1 h_0) + \cdots + \Big(\sum_{i+j=k} c_i h_j\Big)t^k + \cdots + \Big(\sum_{i+j=n-1} c_i h_j\Big)t^{n-1} \\ &+ \Big(\sum_{i+j=n} c_i h_j\Big)t^n + \cdots + c_{n-1}h_k t^{n+k-1} \ . \end{aligned} \tag{8.2}$$

Módulo $t^n - 1$, os termos de graus n a $n + k - 1$ tansformam-se em termos de graus 0 a $k - 1$, respectivamente, portanto, os termos de graus k a $n - 1$ em (8.2) já estão correctos módulo $t^n - 1$ e os seus coeficientes têm de ser zero. Logo, $c = (c_0, c_1 \ldots, c_{n-1}) \in C$ se e só se é solução do seguinte sistema de equações lineares

$$\begin{aligned} c_0 h_k + c_1 k_{k-1} + \cdots + c_k h_0 &= 0 \\ c_1 h_k + \cdots + c_k h_1 + c_{k+1} h_0 &= 0 \\ \ddots \qquad &\vdots \\ c_{n-k-1} k_k + \cdots + c_{n-1} h_0 &= 0 \end{aligned}$$

que, em notação matricial, se escreve $Hc = 0$.

(ii) Só falta ver que $\bar{h}(t)|t^n - 1$, pois $\bar{h}(t)$ é mónico e $h_0 \neq 0$. Mas $h(t^{-1})g(t^{-1}) = t^{-n} - 1$, porque $h(t)g(t) = t^n - 1$, logo $t^k h(t^{-1})t^{n-k}g(t^{-1}) = t^n(t^{-n} - 1) = 1 - t^n$, logo $h_0^{-1}t^k h(t^{-1}) = \bar{h}(t)$ divide $t^n - 1$. □

Observação 8.25. Ao polinómio $t^k a(t^{-1}) \in \mathbb{F}_q[t]$, onde $k = \operatorname{grau} a(t)$, costuma-se chamar *polinómio recíproco* de $a(t)$. Deixamos como exercício verificar que, se $a(t)$ divide $t^n - 1$, então $a(t)$ e o seu recíproco geram códigos equivalentes – ver Exercício 8.12.

Exemplo 8.26. Para o código simplex $S(3, 2)$, o polinómio de paridade é $h(t) = 1+t^2+t^3$. Portanto

$$\bar{h}(t) = t^3 h(t^{-1}) = t^3(1 + t^{-2} + t^{-3}) = t^3 + t + 1$$

é o polinómio recíproco de $h(t)$ e também o polinómio gerador do código dual $S(3, 2)^\perp = \operatorname{Ham}(3, 2)$.

Exemplo 8.27. Em $\mathbb{F}_2[t]$, temos a seguinte factorização $t^{23} - 1 = (t - 1)g_1(t)g_2(t)$, onde

$$g_1(t) = 1 + t^2 + t^4 + t^5 + t^6 + t^{10} + t^{11} \qquad \text{e} \qquad g_2(t) = 1 + t + t^5 + t^6 + t^7 + t^9 + t^{11} \ .$$

Seja $C_1 = \langle g_1(t)\rangle$ e $C_2 = \langle g_2(t)\rangle$. Como $\bar{g}_1(t) := t^{11}g_1(t^{-1}) = g_2(t)$, então, pelo Exercício 8.12, C_1 e C_2 são códigos equivalentes com parâmetros $[23, 12]$. Se mostrarmos que $\mathrm{d}(C_1) = 7$ (Exercício 8.13), podemos concluir que C_1 é equivalente ao código de Golay binário G_{23}.

Exemplo 8.28. Em $\mathbb{F}_3[t]$, $t^{11} - 1 = (t - 1)g_1(t)g_2(t)$, onde

$$g_1(t) = -1 + t^2 - t^3 + t^4 + t^5 \qquad \text{e} \qquad g_2(t) = -1 - t + t^2 - t^3 + t^5 \ .$$

Como $\bar{g}_1(t) = -t^5 g_1(t^{-1}) = g_2(t)$, os códigos gerados pelos polinómios $g_1(t)$ e $g_2(t)$ são equivalentes com parâmetros $[11, 6]_3$. Se mostrarmos que a distância mínima deste(s) código(s) é 5 (ver [**2**]), podemos concluir que o código de Golay ternário G_{11} é equivalente a estes códigos cíclicos.

3.1. Códigos de Hamming binários revisitados

Terminamos esta secção mostrando que os códigos de Hamming binários $\operatorname{Ham}(r, 2)$ são cíclicos.

Seja $p(t) \in \mathbb{F}_2[t]$ um polinómio irredutível de grau r, portanto $\mathbb{F}_{2^r} = \mathbb{F}_2[t]/\langle p(t)\rangle$. Seja $\alpha \in \mathbb{F}_{2^r}$ um elemento primitivo, portanto

$$\mathbb{F}_{2^r} = \{0, 1 = \alpha^0, \alpha, \alpha^2, \ldots, \alpha^{2^r-2}\} \ .$$

Como $\mathbb{F}_{2^r}$ é um espaço vectorial de dimensão r sobre $\mathbb{F}_2$ (ver Exercício 3.11) e

$$a(t) = a_0 + a_1 t + \cdots + a_{r-1}t^{r-1} \longmapsto (a_0, \ldots, a_{r-1})$$

define um isomorfismo vectorial, podemos identificar o elemento $a_0+a_1t+\cdots+a_{r-1}t^{r-1} \in \mathbb{F}_2[t]/\langle p(t)\rangle$ com o vector coluna

$$\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{r-1} \end{bmatrix} \in \mathbb{F}_2^r \ .$$

Com esta identificação, considere a matriz

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^r-2} \end{bmatrix}_{r\times(2^r-1)} \ ,$$

ou seja, as colunas de H são os elementos não nulos do corpo $\mathbb{F}_{2^r}$, donde H é uma matriz de paridade de um código de Hamming binário de redundância r e comprimento $n = 2^r - 1$. Só falta mostrar que este código C é cíclico. Tem-se que

$$\begin{aligned} C = \mathcal{N}(H) &= \{x \in \mathbb{F}_2^n \,:\, Hx = 0\} \\ &= \{(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n \,:\, x_0 1 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1} = 0 \text{ em } \mathbb{F}_{2^r}\} \\ &= \{x(t) \in R_n \,:\, x(\alpha) = 0 \pmod{p(t)}\} \ . \end{aligned} \tag{8.3}$$

Agora é fácil verificar, usando a definição de ideal, que C é um ideal em R_n, logo, pelo Teorema 8.8, concluimos que C é um código cíclico. Já agora vamos determinar o polinómio gerador $g(t)$ de C.

Definição 8.29. Seja $\alpha \in \mathbb{F}_{q^m}$ e seja $f(t) \in \mathbb{F}_q[t]$ um polinómio mónico.

(i) f diz-se um *polinómio mínimo* para α sobe $\mathbb{F}_q$ se $f(\alpha) = 0$ e se f é irredutível em $\mathbb{F}_q[t]$;

(ii) se α é um elemento primitivo de $\mathbb{F}_{q^m}$, o seu polinómio mínimo diz-se um *polinómio primitivo*.

No Apêndice B estudam-se algumas propriedades dos polinómios mínimos – ver em particular a Definição B.1 e o Teorema B.3.

Proposição 8.30. *Seja $p(t) \in \mathbb{F}_2[t]$ um polinómio primitivo de grau $r > 2$. Então $p(t)$ é o polinómio gerador de um código* $\mathrm{Ham}(r, 2)$.

Dem. Sem perda de generalidade vamos supor que α é um elemento primitivo de $\mathbb{F}_{2^r}$ e $p(\alpha) = 0$. Pela igualdade (8.3), sabemos que

$$\mathrm{Ham}(r, 2) = \{x(t) \in R_n \,:\, x(\alpha) = 0 \text{ em } \mathbb{F}_2[t]/\langle p(t)\rangle\} \ .$$

Como $p(\alpha) = 0$, temos $p(t) \in \mathrm{Ham}(r, 2)$. Se $x(\alpha) = 0$ então, por definição de polinómio mínimo, $p(t) \mid x(t)$. Logo $\mathrm{Ham}(r, 2) = \langle p(t)\rangle$.

Seja $g(t)$ o polinómio gerador de $\mathrm{Ham}(r, 2)$. Logo, pelo Lema 8.16, $g(t)$ divide $p(t)$ no anel $\mathbb{F}_2[t]$ e, portanto, temos necessariamente que $g(t) = p(t)$, porque $p(t)$ é irredutível e mónico. □

Exemplo 8.31. Com $r = 3$ fica $n = 7$ e $t^7 - 1 = (t - 1)(t^3 + t^3 + 1)(t^3 + t + 1)$ é a factorização de $t^7 - 1$ em polinómios irredutíveis em $\mathbb{F}_2[x]$. Como $|\mathbb{F}_8 \setminus \{0\}| = 7$ é um primo, qualquer elemento em $\mathbb{F}_8 \setminus \{0, 1\}$ é primitivo, portanto $t^3 + t^2 + 1$ e $t^3 + t + 1$ são polinómios primitivos sobre $\mathbb{F}_2$ e os códigos $\langle t^3 + t^2 + 1\rangle$ e $\langle t^3 + t + 1\rangle$ são ambos equivalentes a $\mathrm{Ham}(3, 2)$.

Exemplo 8.32. Com $r = 4$ fica $n = 15$ e $t^{15} - 1 = (t-1)(t^2+2+1)(t^4+t^3+1)(t^4+t+1)(t^4+t^3+t^2+t+1)$ é a factorização de $t^{15} - 1$ em polinómios irredutíveis em $\mathbb{F}_2[x]$ (verifique!). Neste caso $t^4 + t^3 + 1$ e $t^4 + t + 1$ são polinómios primitivos (verifique!) mas $t^4 + t^3 + t^2 + t + 1$ não é primitivo (verifique!) apesar de ser irredutível. Portanto $\langle t^4 + t^3 + 1\rangle$ e $\langle t^4 + t + 1\rangle$ são ambos equivalentes a $\mathrm{Ham}(4, 2)$.

Exemplo 8.33. Quantos códigos cíclicos binários de comprimento $n = 15$ e redundância $r = 4$ existem? Quais os seus parâmetros?

Pelo exemplo anterior, dada a factorização de $t^{15} - 1$ em $\mathbb{F}_2[t]$, há três códigos nas condições pedidas, dois deles equivalentes a $\mathrm{Ham}(4, 2)$, de parâmetros $[15, 11, 3]_2$, e o terceiro, chamemos-lhe C, com polinómio gerador $g(t) = 1 + t + t^2 + t^3 + t^4$. Como

$$g(t) = \frac{t^5 - 1}{t - 1} \qquad \text{e} \qquad t^{15} - 1 = (t^5)^3 - 1 = (t^5 - 1)(1 + t^5 + t^{10}) \ ,$$

obtemos

$$h(t) = \frac{t^{15}-1}{g(t)} = (t-1)(1+t^5+t^{10}) = 1+t+t^5+t^6+t^{10}+t^{11}$$

e a matriz de paridade de C é

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

donde podemos concluir que $\mathrm{d}(C) = 2$ pois, por exemplo, a primeira e sexta colunas de H são iguais.

4. Codificação e descodificação

Como um código cíclico também é linear, já conhecemos algoritmos de codificação e descodificação. O objectivo desta secção é descrever esses algoritmos, e/ou deduzir outros, à custa do polinómio gerador.

Seja $C \subset R_n = \mathbb{F}_q[t]/\langle t^n - 1\rangle$ um código cíclico q-ário $[n,k]$, com polinómio gerador $g(t) = g_0 + g_1 t + \cdots + g_r t^r$. Portanto $r = n-k$, $g_r = 1$ e

$$G' = \begin{bmatrix} g_0 & g_1 & \cdots & g_r & 0 & \cdots & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_r & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_r & 0 \\ 0 & \cdots & \cdots & 0 & g_0 & g_1 & \cdots & g_r \end{bmatrix}$$

é uma matriz geradora de C, pelo Teorema 8.19. Se aplicarmos o método de eliminação de Gauss para "matarmos" as entradas por baixo de cada $g_r = 1$, usando apenas operações nas linhas, obtemos uma matriz na forma

$$G_{k\times n} = \begin{bmatrix} R_{k\times r} & I_k \end{bmatrix} , \tag{8.4}$$

que é ainda uma matriz geradora do mesmo código C. Se designarmos por $-\rho_i(t)$ o polinómio correspondente à linha $i+1$ (com $i = 0,\ldots,k-1$) da matriz R, à linha $i+1$ de G corresponde o polinómio $-\rho_i(t) + t^{r+i}$, onde $\mathrm{grau}(\rho_i(t)) \leq r-1$, porque R é uma matriz de r colunas.

Por outro lado, cada linha de G é uma palavra do código C, logo um múltiplo de $g(t)$ pelo Lema 8.16, donde

$$-\rho_i(t) + t^{r+i} = g(t)q_i(t),$$

para algum polinómio $q_i(t)$. Ou seja,

$$t^{r+i} = g(t)q_i(t) + \rho_i(t) \qquad \forall\, i \in \{0,\ldots,k-1\} \tag{8.5}$$

com $\mathrm{grau}(\rho(t)) \leq r-1 < r = \mathrm{grau}(g(t))$, i.e., $\rho_i(t)$ é o resto da divisão de t^{r+i} por $g(t)$.

Um algoritmo de codificação sistemática:

Dada a mensagem $m(t) = m_0 + m_1 t + \cdots + m_{k-1}t^{k-1} \in \mathbb{F}_q[t]$ ou, equivalentemente, dado o vector mensagem $(m_0,\ldots,m_{k-1}) \in \mathbb{F}_q^k \cong C$:

- determinar o resto $\rho(t)$ da divisão de $t^r m(t)$ por $g(t)$, i.e., determinar $\rho(t)$ tal que

$$t^r m(t) = g(t)q(t) + \rho(t) \quad \text{e} \quad \mathrm{grau}(\rho(t)) \leq r-1 \ ;$$

- codificar $m(t)$ pelo polinómio de código

$$c(t) = -\rho(t) + t^r m(t) \in \langle g(t)\rangle = C$$

Trata-se de facto de uma codificação sistemática pois o polinómio de código obtido é da forma

$$c(t) = -\rho_0 - \rho_1 t - \cdots - \rho_{r-1}t^{r-1} + m_0 t^r + m_1 t^{r+1} + \cdots + m_{k-1}t^{n-1} \in R_n$$

porque grau$(\rho(t)) \leq r-1$, ou, equivalentemente, o vector código é da forma

$$c = (\underbrace{-\rho_0, -\rho_1, \ldots, -\rho_{r-1}}_{\text{símbolos de verificação ou de redundância}}, \overbrace{m_0, \ldots, m_{k-1}}^{\text{símbolos de mensagem}}) \in C \ .$$

Os símbolos de mensagem aparecem agora nas últimas componentes do vector – comparar com a expressão (4.2). Note que, tal como em (4.1), o vector c também se escreve

$$c = G^T m = (R^T m, m) \ .$$

Note ainda que, para se codificar $m(t)$ (ou $m \in \mathbb{F}_q^k$), não foi necessário conhecermos uma matriz geradora, bastou calcular o resto da divisão pelo polinómio gerador $g(t)$ do código cíclico C.

Passemos agora à descodificação. Recorde que, na descodificação por síndrome para códigos lineares, o primeiro passo é sempre calcular o sintoma $S(y)$ do vector recebido $y \in \mathbb{F}_q^n$.

Teorema 8.34. *O sintoma $S(y(t))$ é o resto da divisão de $y(t)$ pelo polinómio gerador $g(t)$.*

Dem. Uma vez que $G = \begin{bmatrix} R & I_k \end{bmatrix}$ é uma matriz geradora, $H = \begin{bmatrix} I_r & -R^T \end{bmatrix}$ é uma matriz de paridade, pelo Lema 4.12, e as colunas de $-R^T$ são os vectores correspondentes aos polinómios $\rho_0(t)$, …, $\rho_{k-1}(t)$ determinados anteriormente, i.e. $\rho_i(t)$ é o resto da divisão de t^{r+i} por $g(t)$.
Seja $y = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_q^n$ e seja $y(t) = y_0 + y_1 t + \cdots y_{n-1}t^{n-1}$ o polinómio correspondente. O sintoma de y é $S(y) = Hy \in \mathbb{F}_q^r$. Portanto, em notacção polinomial, $S(y(t))$ é um polinómio de grau menor ou igual a $r-1$ e, usando a matriz de paridade $H = \begin{bmatrix} I_r & -R^T \end{bmatrix}$, fica

$$\begin{aligned} S(y(t)) &= y_0 + y_1 t + \cdots + y_{r-1}t^{r-1} + y_r\rho_0(t) + \cdots + y_{n-1}\rho_{k-1}(t) \\ &= y(t) - \sum_{i=0}^{k-1} y_{r+i}(\rho_i(t) - t^{r+i}) \\ &= y(t) - \Big(\sum_{i=0}^{k-1} y_{r+i}q_i(t)\Big)g(t) \ , \end{aligned}$$

usando as igualdades (8.5). Pondo $q(t) = -\sum_{i=0}^{k-1} y_{r+i}q_i(t)$, obtem-se $S(y(t)) = y(t) - g(t)q(t)$, ou seja,

$$y(t) = g(t)q(t) + S(y(t)) \ .$$

Como grau$(S(y(t))) \leq r-1$, da última igualdade conclui-se que $S(y(t))$ é o resto da divisão de $y(t)$ por $g(t)$. □

Define-se o peso $\mathrm{w}(x(t))$ de um elemento $x(t) \in R_n$ como o peso do vector correspondente $x \in \mathbb{F}_q^n$, ou equivalentemente, $\mathrm{w}(x(t))$ é o peso do único representante de grau menor ou igual a $n-1$.

Corolário 8.35. *Seja $s(t) = S(y(t))$. Se $\mathrm{w}(s(t)) \leq T := \left\lfloor \frac{\mathrm{d}(C)-1}{2} \right\rfloor$, então $s(t)$ é um chefe de classe de $y(t) + C$ e, portanto, descodificamos $y(t)$ por $x(t) = y(t) - s(t) \in C$.*

Exemplo 8.36. Seja C o código cíclico binário, de comprimento 7, com polinómio gerador $g(t) = 1 + t + t^3$. Como C é um código de Hamming binário Ham$(3, 2)$ – ver Exemplo 8.26 – então C é um código perfeito de distância mínima $\mathrm{d}(C) = 3$, portanto $T = 1$ e os chefes de classe são precisamente os elementos de R_7 peso 1.

(i) Seja $y(t) = t + t^2 + t^3 + t^5 \in R_7$ o vector recebido. Como $y(t) = t + t^2(1 + t + t^3)$, então $s(t) := S(y(t)) = t$, pelo Teorema 8.34. Além disso, como $\mathrm{w}(s(t)) = 1$, $s(t)$ é um chefe de classe e podemos descodificar $y(t)$ por $y(t) - s(t) = t^2 + t^3 + t^5$, pelo Corolário 8.35.

(ii) Seja agora $z(t) = 1+t^4$ o vector recebido. Como $z(t) = t(1+t+t^3)+1+t+t^2$, então o sintoma de $z(t)$ é $S(z(t)) = 1 + t + t^2$, que tem peso $3 > T = 1$. Não se pode aplicar o Corolário 8.35. No entanto,

$$z(t) = 1 + t^4 \equiv t^7 + t^4 = t^4(t^3 + 1) = t^4(t^3 + t + 1) + t^5 \pmod{t^7 - 1}$$

ou seja, $z(t) = t^4 g(t) + t^5$. O resto da divisão de $z(t)$ pelo polinómio gerador não é t^5, pois $\text{grau}(t^5) = 5 \geq 3 = \text{grau}(g(t))$, mas, como $\text{w}(t^5) = 1$, t^5 é o chefe da classe $z(t) + C$. Portanto descodificamos $z(t)$ por $z(t) - t^5 = 1 + t^4 + t^5 = t^4 g(t) \in C$.

Como se viu neste exemplo, determinar o chefe de classe pode não ser imediato usando apenas o sintoma, se este tem peso maior do que T.

Note que $t^i y(t) \in R_n$ contém a mesma informação que $y(t)$. Logo, se conseguirmos descodificar $t^i y(t)$ para algum i, então também descodificamos $y(t)$. Interessa, portanto, sabermos calcular os sintomas dos desvios cíclicos $t^i y(t)$ e também sabermos quando vai exitir um destes sintomas de peso menor ou igual a T. É o que faremos de seguida.

Teorema 8.37. *Dado $y(t) \in R_n$, o sintoma do desvio cíclico de $y(t)$ é*

$$S(ty(t)) = tS(y(t)) - s_{r-1} g(t) \ ,$$

onde s_{r-1} é o coeficiente do termo de grau $r-1$ de $S(y(t))$.

Dem. Seja $s(t) = S(y(t))$ o sintoma de $y(t)$. Portanto $y(t) = q(t)g(t)+s(t)$, com $\text{grau}(s(t)) \leq r-1$, para algum $q(t)$. Pondo $s(t) = s_{r-1}t^{r-1} + s'(t)$ e $g(t) = t^r + g'(t)$, onde $\text{grau}(s'(t)) < r-1$ e $\text{grau}(g'(t)) < r$ (recorde que $g(t)$ é mónico e tem grau r), fica

$$\begin{aligned} ty(t) &= tq(t)g(t) + ts(t) \\ &= t(q(t) + s_{r-1})g(t) + (ts(t) - s_{r-1}g(t)) \end{aligned}$$

e $ts(t) - s_{r-1}g(t) = ts'(t) - s_{r-1}g'(t)$ tem grau menor do que r. Logo, pelo Teorema 8.34, o sintoma de $ty(t)$ é $ts(t) - s_{r-1}g(t)$. □

Exemplo 8.38. Para o código do Exemplo 8.36, o sintoma de $z(t) = 1 + t^4$ é $S(z(t)) = 1 + t + t^2$, logo, pelo teorema anterior, os sintomas dos restantes desvios cíclicos de $z(t)$ são

$$\begin{aligned} S(tz(t)) &= 1 + t^2 \ , & S(t^2 z(t)) &= 1 \ , \\ S(t^3 z(t)) &= t \ , & S(t^4 z(t)) &= t^2 \ , \\ S(t^5 z(t)) &= 1 + t \ , & S(t^6 z(t)) &= t + t^2 \ . \end{aligned}$$

Definição 8.39. Diz-se que $x = (x_0, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ contém uma *sequência cíclica de k zeros*, se existe $j \leq n-1$ tal que $x_j = x_{j+1} = \cdots = x_{j+k-1} = 0$, onde os índices são calculados módulo n.

Exemplo 8.40.

- $(1, 1, 0, 0, 0, 1, 0) \in \mathbb{F}_2^7$ contém uma sequência de três zeros.
- $x = (0, 0, 1, 0, 5, 0, 0, 0, 0) \in \mathbb{F}_7^9$ contém uma sequência cíclica de $k = 6$ zeros. Tomando dois desvios cíclicos para a esquerda (ou sete desvios cíclcicos para a direita), obtemos um vector $x' = (1, 0, 5, 0, 0, 0, 0, 0, 0)$ com zeros nas últimas 6 coordenadas. Ou seja, no anel R_9, se $x(t) = t^2 + 5t^4$, então $t^{-2}x(t) \equiv t^7 x(t) = 1 + 5t^2$ tem grau $n - k - 1 = 2$.

Lema 8.41. *O vector $x \in \mathbb{F}_q^n$ contém uma sequência cíclica de k zeros se e só se existe $i \in \{0, 1, \ldots, n-1\}$ tal que $\text{grau}(t^i x(t)) \leq n - k - 1$.*

Dem. Basta permutar ciclicamente as coordenadas de x até os k zeros consecutivos ocuparem as últimas k componentes de x. O vector assim obtido corresponde a um polinómio em R_n de grau menor ou igual a $n - k - 1$. □

Lema 8.42. *Seja $\vec{e} \in \mathbb{F}_q^n$, com peso $\text{w}(\vec{e}) \leq T$, contendo uma sequência cíclica de k zeros. Então $\text{w}(S(t^i e(t))) \leq T$, para algum $i \in \{0, \ldots, n-1\}$.*

Dem. Pelo lema anterior, seja $i \in \{0,1,\ldots,n-1\}$ tal que $t^i e(t)$ tem grau menor ou igual a $n-k-1 = r-1$. Portanto, pelo Teorema 8.34, o sintoma do desvio cíclico $t^i e(t)$ é $S(t^i e(t)) = t^i e(t)$. Como permutações das coordenadas não alteram o peso de um vector, também se verifica que

$$\mathrm{w}(S(t^i e(t))) = \mathrm{w}(t^i e(t)) = \mathrm{w}(e(t)) \leq T \ . \qquad \square$$

Podemos finalmente justificar o seguinte algoritmo de descodificação.

Algoritmo Caça ao Erro:

Seja C um código cíclico $[n,k,d]_q$ com polinómio gerador $g(t)$ de grau $r = n-k$. Seja $T = \left\lfloor \frac{d-1}{2} \right\rfloor$. Recebido $y(t) \in R_n$:

1. Calcular os sintomas $s_i(t) := S(t^i y(t))$;
2. Se $\mathrm{w}(s_i(t)) \leq T$ para algum $i \in \{0,1,\ldots,n-1\}$, então assumimos que $t^{n-i}s_i(t)$ é o vector erro e descodificamos $y(t)$ por $y(t) - t^{n-i}s_i(t)$;
3. Caso contrário, o erro ocorrido não é corrigível.

Antes de mais, convém observar que $y(t) - t^{n-i}s_i(t) \in C$, pois

$$\begin{aligned} t^i(y(t) - t^{n-i}s_i(t)) &= t^i y(t) - t^n s_i(t) \\ &= q(t)g(t) + s_i(t) - t^n s_i(t) \qquad \text{porque } s_i(t) = S(t^i y(t)) \\ &= q(t)g(t) + (1-t^n)s_i(t) \\ &\equiv q(t)g(t) \pmod{t^n-1} \end{aligned}$$

donde $t^i(y(t) - t^{n-i}s_i(t)) \in C$ e também $y(t) - t^{n-i}s_i(t) \in C$, porque o código C é cíclico.

Além disso, este Algoritmo Caça ao Erro corrige todos os vectores erro de peso T no máximo, que contenham uma sequência cíclica de $k = \dim C$ zeros.

Justificação: Seja $x(t) \in C$ o vector enviado e $y(t) \in R_n$ o vector recebido. Pelos resultados anteriores, se o erro ocorrido $e(t) = y(t) - x(t)$ contém uma sequência cíclica de k zeros, então existe i tal que $S(t^i e(t))$ tem peso T no máximo e $S(t^i e(t)) = t^i e(t)$. Logo

$$s_i(t) := S(t^i y(t)) = S(t^i x(t)) + S(t^i e(t)) = 0 + t^i e(t) = t^i e(t) \ ,$$

e o algoritmo descodifica $y(t)$ correctamente por $y(t) - t^{n-i}s_i(t) = y(t) - e(t) = x(t)$.

Exemplo 8.43. Continuação do Exemplo 8.36: Aplicando o Algoritmo Caça ao Erro ao vector recebido $z(t) = 1 + t^4$, uma vez que já calculámos os sintomas de $t^i z(t)$ no Exemplo 8.38 e que $T = 1$, assumimos que o erro ocorrido é $t^{7-2}s_2(t) = t^5$ e descodificamos $z(t)$ por

$$z(t) - t^5 = 1 + t^4 + t^5 \ ,$$

que foi o que já obtivémos anteriormente.

Exemplo 8.44. Seja C o código binário $[15,7]$ com polinómio gerador $g(t) = 1 + t + t^2 + t^4 + t^8$. Deixamos como exercício verificar que $\mathrm{d}(C) = 5$. Portanto $T = 2$ e o Algoritmo Caça ao Erro permite corrigir todos os erros simples e duplos que contenham uma sequência cíclica de $k = 7$ zeros.

- Se $\mathrm{w}(\vec{e}) = 1$, então $\vec{e}$ é uma permutação cíclica de $(1,0,\ldots,0)$ e, portanto, contém uma sequência cíclica de 14 zeros.
- Se $\mathrm{w}(\vec{e}) = 2$, então $\vec{e}$ é uma permutação cíclica de um vector da forma

  $$\vec{f} = (1, \underbrace{0,\ldots,0}_{l \text{ zeros}}, 1, \underbrace{0,\ldots,0}_{13-l \text{ zeros}}) \ .$$

  Se $l \geq 7$, o vector $\vec{f}$ contém obviamente sete zeros seguidos. Se $l \leq 6$, então $13 - l \geq 7$ e $\vec{f}$ também contém sete zeros seguidos. Em qualquer caso, concluimos que $\vec{e}$ contém uma sequência cíclica de sete zeros.

Para este código C, o Algoritmo Caça ao Erro corrige todos os vectores erros $\vec{e}$ com peso $\mathrm{w}(\vec{e}) \leq 2$.

Exemplo 8.45. Seja C o código binário $[15, 7, 5]$ do exemplo anterior. Vamos descodificar o vector recebido $y = 111110110010101$.

Para uma aplicação pragmática do Algoritmo Caça ao Erro, vamos apenas calcular os sintomas $s_i(t) = S(t^i y(t))$, com $i = 0, 1, \ldots, n-1$, até encontrarmos um com peso menor ou igual a $T = 2$. Como $y(t) = 1 + t + t^2 + t^3 + t^4 + t^6 + t^7 + t^{10} + t^{12} + t^{14} = g(t)(t^6 + t^4) + (1 + t + t^2 + t^3 + t^5 + t^6)$, aplicando os Teorema 8.34 e 8.37 (o último várias vezes), obtem-se

$$\begin{aligned} s_0(t) =& 1 + t + t^2 + t^3 + t^5 + t^6 && \text{tem peso } 6 > T, \\ s_1(t) =& t + t^2 + t^3 + t^4 + t^6 + t^7 && \text{tem peso } 6 > T, \\ s_2(t) =& 1 + t + t^3 + t^5 + t^7 && \text{tem peso } 5 > T, \\ s_3(t) =& 1 + t^6 && \text{tem peso } 2 \leq T, \end{aligned}$$

por isso assumimos que o erro ocorrido foi $t^{15-3}s_3(t) = t^{12}(1 + t^6) \equiv t^3 + t^{12} \pmod{t^{15} - 1}$, e descodificamos $y(t)$ por $y(t) - t^3 - t^{12} = 1 + t + t^2 + t^4 + t^6 + t^7 + t^{10} + t^{14}$, ou seja, descodificamos o vector y por 111010110010001.

5. Erros acumulados

Definição 8.46. O vector $e = (e_1, \ldots, e_n) \in \mathbb{F}_q^n$ diz-se um *erro-l acumulado*, ou um *erro acumulado de comprimento l*, se existe $i \in \{1, \ldots, n\}$ tal que $e_i \neq 0$ e $e_{i+l-1} \neq 0$, e $e_j = 0$ para todo o $j \notin \{i, \ldots, i + l - 1\}$, onde os índices são calculados módulo n.

Ou seja, as coordenas não nulas de um vector erro-l acumulado estão contidas numa sequência cíclica de comprimento l, sendo a primeira e última coordenadas desta sequência não nulas.

Aqui considerámos apenas erros acumulados no caso cíclico – compare com o exercício 8.24 para o caso de erros acumulados no sentido estrito.

Exemplo 8.47. Os vectores 00111000, 10100000 e 01000001 são erros-3 acumulados em $\mathbb{F}_2^8$.

Exemplo 8.48. Se $l = 2$, um vector erro-2 acumulado é da forma

$$e = (0, \ldots, e_i, e_{i+1}, 0, \ldots, 0) \quad \text{ou} \quad e = (e_1, 0, \ldots, 0, e_n) \ ,$$

com $e_i \neq 0$, $e_{i+1} \neq 0$, $e_1 \neq 0$ e $e_n \neq 0$, e diz-se um *erro duplo adjacente*.

Teorema 8.49. *Seja C um código linear $[n, k]_q$, não necessariamente cíclico, tal que C corrige todos os erros-m acumulados com $m \leq l$. Então*

(i) C não contém nenhum vector erro-m acumulado com $m \leq 2l$;

(ii) ***Estimativa de Reigner:*** *$n - k \geq 2l$.*

Dem. (i) Seja $\vec{e}$ um vector erro-m acumulado com $m \leq 2l$. Então

$$\vec{e} = (\vec{0}, a, \vec{u}, \vec{v}, b, \vec{0}) \ ,$$

com $a, b \in \mathbb{F}_q \setminus \{0\}$ e $\vec{u}, \vec{v}$ vectores de comprimento menor ou igual a $l - 1$. Sejam

$$\vec{x} = (\vec{0}, a, \vec{u}, \vec{0}, 0, \vec{0}) \qquad \text{e} \qquad \vec{y} = -(\vec{0}, 0, \vec{0}, \vec{v}, b, \vec{0}) \ .$$

Então $\vec{x}$ e $\vec{y}$ são erros acumulados de comprimento menor ou igual a l. Como C corrige estes erros por hipótese, então $\vec{x}$ e $\vec{y}$ pertencem a classes distintas, i.e., $\vec{x} + C \neq \vec{y} + C$, ou ainda, $\vec{e} = \vec{x} - \vec{y} \notin C$.

(ii) Seja H uma matriz de paridade para C. Sejam $u_1, u_2, \ldots, u_{r+1}$ as primeiras $r + 1$ colunas de H. Como pertencem a $\mathbb{F}_q^r$, os $r + 1$ vectores $u_1, \ldots, u_{r+1}$ são linearmente dependentes, logo existem escalares $c_1, \ldots, c_{r+1} \in \mathbb{F}_q$, não todos nulos, tais que

$$c_1 u_1 + c_2 u_2 + \cdots + c_{r+1} u_{r+1} = \vec{0} \ .$$

Seja $c = (c_1, c_2, \ldots, c_{r+1}, 0, \ldots, 0) \in \mathbb{F}_q^n$. Então c é um erro-m acumulado com $m \leq r + 1$ e, como $Hc = 0$, $c \in C$. Por (i), tem-se $m > 2l$, portanto $r + 1 > 2l$, o que é equivalente a $n - k = r \geq 2l$. □

Corolário 8.50. *Um código linear $[n,k]_q$ corrige no máximo todos os erros-m acumulados com $m \leq \lfloor \frac{n-k}{2} \rfloor$.*

Este corolário é uma consequência directa da Estimativa de Reigner.

Exemplo 8.51. Seja C o código binário cíclico $[15,9]$, com polinómio gerador $g(t) = 1+t+t^2+t^3+t^6$. Em notação polinomial, os erros-m acumulados com $m \leq 3$ são:

$$t^i \text{ para } m=1, \quad t^i(1+t) \text{ para } m=2, \quad t^i(1+t^2) \text{ e } t^i(1+t+t^2) \text{ para } m=3,$$

onde $0 \leq i \leq 14$ nos quatro casos. São 60 polinómios no total, mas todos pertencem a classes diferentes pois têm sintomas distintos dois a dois (exercício: verifique esta última afirmação, de preferência com a ajuda de um programa de computador). Portanto C corrige todos os erros-m acumulados com $m \leq 3$. Por outro lado, a Estimativa de Reigner dá $l \leq \lfloor \frac{n-k}{2} \rfloor = \lfloor \frac{15-9}{2} \rfloor = 3$. Ou seja, C atinge a igualdade na Estimativa de Reigner, e esta não pode ser melhorada.

Por definição, um erro-l acumulado é um vector da forma

$$e = (0, \ldots, e_i, *, \ldots, *, e_{i+l-1}, 0, \ldots, 0) \ ,$$

onde $e_i \neq 0$, $e_{i+l-1} \neq 0$ e as $l-2$ componentes assinaladas com $*$ podem ser nulas ou não, logo um erro-l acumulado contém uma sequência cíclica de $n-l$ zeros. Se C é um código cíclico $[n,k]_q$ que corrige todos os erros acumulados de comprimento $m \leq l$, então, pela Estimativa de Reigner, $k \leq n-2l \leq n-l$. Vamos, portanto, poder usar o Algoritmo Caça ao Erro, mas ignorando a condição $\mathrm{w}(\vec{e}) \leq T$, para corrigir todos estes erros.

Algoritmo Caça ao Erro Acumulado:

Seja C um código cíclico $[n,k]_q$, corrector de todos os erros-m acumulados com $m \leq l$. Recebido $y(t) \in R_n$:

1. Calcular os sintomas $s_i(t) := S(t^i y(t))$;
2. Se $s_i(t)$ é um erro-m acumulado, com $m \leq l$, para algum $i \in \{0,1,\ldots,n-1\}$, então assumimos que $t^{n-i}s_i(t)$ é o vector erro e descodificamos $y(t)$ por $y(t) - t^{n-i}s_i(t)$;
3. Caso contrário, o erro ocorrido não é corrigível.

Note que $y(t) - t^{n-i}s_i(t) \in C$, tal como já acontecia com o Algoritmo Caça ao Erro.

Deixamos como exercício justificar que este algoritmo corrige os erros enunciados.

Exemplo 8.52. Seja C o código cíclico binário $[15,9]$, do Exemplo 8.51, com polinómio gerador

$$g(t) = 1+t+t^2+t^3+t^6 \ .$$

Já sabemos que este código corrige todos os erros acumulado de comprimento $m \leq 3$, pois estes vectores pertencem a classes distintas. Vamos descodificar o vector recebido

$$y = 110000011101110 \qquad \text{ou} \qquad y(t) = 1+t+t^7+t^8+t^9+t^{11}+t^{12}+t^{13} \ .$$

Calculemos os sintomas $s_i(t) = S(t^i y(t))$, com $i = 0, \ldots, n-1$, até encontrarmos um que seja um erro-m acumulado com $m \leq 3$:

$$\begin{aligned} s_0(t) &= 1+t^2+t^4+t^5 && \text{é um erro-6 acumulado,} \\ s_1(t) &= ts_0(t) - g(t) = 1+t^2+t^5 && \text{é um erro-6 acumulado,} \\ s_2(t) &= ts_1(t) - g(t) = 1+t^2 && \text{é um erro-3 acumulado.} \end{aligned}$$

Portanto assumimos que o erro ocorrido é $e(t) = t^{15-2}s_2(t) = t^{13}(1+t^2) \equiv 1+t^{13} \pmod{t^{15}-1}$, e descodificamos $y(t)$ por $y(t) - e(t)$, ou y por

$$y - 100000000000010 = 010000011101100 \ .$$

6. Entrelaçamento

O entrelaçamento de um código é uma construção que permite aumentar a capacidade de correcção de erros acumulados.

Definição 8.53. O *entrelaçamento* de s vectores $x_1, \ldots, x_s \in \mathbb{F}_q^n$ é o vector

$$x^{(s)} = (\underbrace{x_{1,1}, x_{2,1}, \ldots, x_{s,1}}_{\text{a 1ª coordenada de cada } x_i}, \overbrace{x_{1,2}, x_{2,2}, \ldots, x_{s,2}}^{\text{a 2ª coordenada de cada } x_i}, \ldots, \underbrace{x_{1,n}, x_{2,n}, \ldots, x_{s,n}}_{\text{a última coordenada de cada } x_i}) \in \mathbb{F}_q^{ns} \ ,$$

onde $x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$.

Exemplo 8.54. O entrelaçamento dos três vectores $x_1 = 0000$, $x_2 = 1111$, $x_3 = 3456 \in \mathbb{F}_7^4$ é

$$x^{(3)} = 013014015016 \in \mathbb{F}_7^{12} \ .$$

Se escrevermos uma matriz cujas linhas são vectores x_1, x_2 e x_3

$$X = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 3 & 4 & 5 & 6 \end{bmatrix} \ ,$$

podemos obter o vector entrelaçado lendo as entradas da matriz X de cima para baixo e da esquerda para a direita.

Em geral, escrevendo uma matriz X cujas linhas são os vectores $x_i \in \mathbb{F}_q^n$, com $1 \leq i \leq s$,

$$X = \begin{bmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n} \\ \vdots & \vdots & & \vdots \\ x_{s,1} & x_{s,2} & \cdots & x_{s,n} \end{bmatrix}_{s \times n} \ , \tag{8.6}$$

o vector entrelaçado são as colunas de X escritas consecutivamente como as entradas de um vector em $\mathbb{F}_q^{ns}$

Definição 8.55. Seja C um código linear $[n,k]_q$. O código $C^{(s)}$ obtido entrelaçando quaisquer s palavras do código C diz-se o *código entrelaçado de grau s*.

Exemplo 8.56. Seja $C = \langle 111 \rangle$ o código binário de repetição de comprimento 3. Para obter $C^{(2)}$, vamos descrever o vector entrelaçado dos pares ordenados de palavras de C. Os quatro casos possíveis estão descritos na seguinte tabela:

x_1	000	000	111	111
x_2	000	111	000	111
$x^{(2)}$	000000	010101	101010	111111

Portanto, $C^{(2)} = \langle 010101, 101010 \rangle \subset \mathbb{F}_2^6$ e é um código linear e cíclico. Note que, apesar do código entrelaçado ter comprimento maior, $\mathrm{d}(C^{(2)}) = 3 = \mathrm{d}(C)$, portanto $C^{(2)}$ tem as mesmas capacidades de correcção que C para erros aleatórios.

Teorema 8.57. *(a) Se C é um código linear $[n,k]$, então $C^{(s)}$ é um código linear $[ns, ks]$.*

(b) Se $C \subset R_n$ é um código cíclico com polinómio gerador $g(t)$, então $C^{(s)} \subset R_{ns}$ é um código cíclico com polinómio gerador $g(t^s)$.

(c) Se C é um código cíclico corrector de todos os erros-m acumulados com $m \leq l$, então $C^{(s)}$ é um código corrector de todos os erros-m acumulados com $m \leq ls$.

Dem. (a) Por construção, $C^{(s)}$ é um subconjunto de $\mathbb{F}_q^{ns}$ e $|C^{(s)}| = |C|^s = q^{ks}$. Portanto, se $C^{(s)}$ é linear, então $\dim C^{(s)} = \log_q(|C^{(s)}|) = ks$. Para ver que $C^{(s)}$ é linear, basta ver que é fechado para a soma de vectores e produto por um escalar. Seja $x^{(s)} \in C^{(s)}$ o entrelaçado dos vectores $x_1, \ldots, x_s \in C$, seja $y^{(s)} \in C^{(s)}$ o entrelaçado de $y_1, \ldots, y_s \in C$, e seja $a \in \mathbb{F}_q$. Deixamos como

exercício verificar que $x^{(s)}+y^{(s)}$ e $ax^{(s)}$ são os entrelçados de $x_1+y_1,\ldots,x_s+y_s$ e de $ax_1,\ldots,ax_s$, respectivamente – use a notação das matrizes (8.6). Logo $x^{(s)}+y^{(s)}, ax^{(s)} \in C^{(s)}$, porque C é um código linear.

(b) Uma vez que $C^{(s)}$ é linear, pela aínea (a), só falta ver que $C^{(s)}$ é fechado para os desvios cíclicos. Seja $x^{(s)} \in C^{(s)}$ o entrelaçado dos vectores $x_1,\ldots,x_s \in C$. Como C é cíclico, $\sigma(x_s) \in C$ e, portanto, o vector y obtido entrelaçando $\sigma(x_s), x_1, \ldots, x_{s-1}$ é uma palavra do código $C^{(s)}$. Explicitando as coordenadas de y e pondo $x_i = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$, obtém-se

$$y = (\underbrace{x_{s,n}, x_{1,1}, \ldots, x_{s-1,1}}_{s \text{ coordenadas}}, \underbrace{x_{s,1}, x_{1,2}, \ldots, x_{s-1,2}}_{s \text{ coordenadas}}, \ldots, \underbrace{x_{s,n-1}, x_{1,n}, \ldots, x_{s-1,n}}_{s \text{ coordenadas}}) \ ,$$

ou seja, $y = \sigma(x^{(s)}) \in C^{(s)}$.

Para determinarmos o polinómio gerador, temos de encontrar um polinómio mónico de grau $ns-ks$ (a redundância de $C^{(s)}$), que divida $t^{ns}-1$, e que pertença ao código $C^{(s)}$. Seja $g(t) = g_0 + g_1 t + \cdots + g_r t^r$, com $r = n-k$, o polinómio gerador de C, e seja $g = (g_0, g_1, \ldots, g_r, 0, \ldots, 0) \in \mathbb{F}_q^n$ o vector correspondente. Então, o entrelaçado de g com $s-1$ vectores nulos $\vec{0} \in \mathbb{F}_q^n$ é um elemento de $C^{(s)}$ e as suas coordenadas são

$$g^{(s)} = (\underbrace{g_0, 0, \ldots, 0}_{s \text{ coord.}}, \underbrace{g_1, 0, \ldots, 0}_{s \text{ coord.}}, \ldots, \underbrace{g_r, 0, \ldots, 0}_{s \text{ coord.}}) \ ,$$

que, em notação polinomial, se escreve

$$g^{(s)}(t) = g_0 + g_1 t^s + g_2 t^{2s} + \cdots + g_r t^{rs} = g(t^s) \ .$$

Portanto $g(t^s) \in C^{(s)}$ é mónico ($g_r = 1$ porque $g(t)$ é mónico), tem grau $rs = ns - ks$ e divide $t^{ns}-1$ porque

$$g(t)h(t) = t^n - 1 \quad \Longrightarrow \quad g(t^s)h(t^s) = (t^s)^n - 1 = t^{sn} - 1 \ .$$

(c) Seja $\vec{e} \in \mathbb{F}_q^{ns}$ um erro-m de acumulação com $m \leq ls$. O vector $\vec{e}$ é da forma

$$\vec{e} = (0, \ldots, 0, \underbrace{e_i, \ldots, e_{i+ls-1}}_{ls \text{ coordenadas}}, 0, \ldots, 0) \ .$$

Seja E a matriz $s \times n$ que se obtem escrevendo as coordendas de $\vec{e}$ por ordem ao longo das colunas, ou seja, o entrelaçado das linhas de E é o vector erro $\vec{e}$. Portanto, cada linha não nula de E contém no máximo l entradas não nulas. Portanto, C corrige os vectores erro correspondentes às linhas de E, logo $C^{(s)}$ corrige o vector erro-m acumulado $\vec{e}$. □

Exemplo 8.58. Continuação do Exemplo 8.56: As palavras de $C^{(2)}$ correspondem aos polinómios

$$0 \ , \quad t + t^3 + t^5 \ , \quad 1 + t^2 + t^4 \quad \text{e} \quad 1 + t + t^2 + t^3 + t^4 + t^5 \ ,$$

logo $g_2(t) = 1 + t^2 + t^4$ é o polinómio gerador de $C^{(2)}$, ou, aplicando o Teorema 8.57, como $g(t) = 1 + t + t^2$ é o polinómio gerador de C, então $g_2(t) = g(t^2) = 1 + t^2 + t^4$ é o polinómio gerador do código entrelaçado. Quanto às capaciadades correctoras, C corrige apenas os erros simples, pois $\mathrm{d}(C) = 3$ e C é um código perfeito mas, pelo Teorema 8.57, $C^{(2)}$ pode ser usado para corrigir todos os erros simples e todos os erros duplos adjacentes.

7. Concatenação

Tal como no caso dos códigos traço e subcódigo subcorpo (ver Exercício 4.6), a concatenação permite obter um código sobre $\mathbb{F}_q$ à custa de um código sobre $\mathbb{F}_{q^m}$. Tal como o entrelaçamento, a concatenação aumenta a capacidade de correcção de erros acumulados.

Recorde que o corpo $\mathbb{F}_{q^m}$ é um espaço vectorial de dimensão m sobre $\mathbb{F}_q$. Se $f(t) \in \mathbb{F}_q[t]$ é um polinómio irredutível de grau m, então $\mathbb{F}_{q^m} = \mathbb{F}_q[t]/\langle f(t) \rangle$. Se $\alpha \in \mathbb{F}_{q^m}$ é uma raiz de $f(t)$ então ainda podemos escrever

$$\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \ : \ a_i \in \mathbb{F}_q\} \ .$$

Portanto, a aplicação

$$\begin{aligned} \phi : \mathbb{F}_{q^m} &\longrightarrow (\mathbb{F}_q)^m \\ a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} &\longmapsto (a_0, a_1, \ldots, a_{m-1}) \end{aligned} \tag{8.7}$$

é um isomorfismo linear sobre $\mathbb{F}_q$, i.e., ϕ é uma aplicação linear bijectiva. Recorde ainda que $\{1, \alpha, \ldots, \alpha^{m-1}\}$ é uma base de $\mathbb{F}_{q^m}$ como espaço vectorial sobre $\mathbb{F}_q$, por isso, para definir ϕ, basta dar $\phi(\alpha^i) = \vec{e}_{i+1}$, com $i \in \{0, 1, \ldots, m-1\}$, onde $\vec{e}_j \in \mathbb{F}_q^m$ é o vector com 1 na componente j e 0 nas restantes. Seja ϕ^* a aplicação definida por

$$\begin{aligned} \phi^* : \overbrace{\mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}}^{N \text{ vezes}} = \mathbb{F}_{q^m}^N &\longrightarrow (\mathbb{F}_q^m)^N = \mathbb{F}_q^{mN} \\ x = (x_1, \ldots, x_N) &\longmapsto (\phi(x_1), \ldots, \phi(x_N)) \end{aligned} \tag{8.8}$$

Então ϕ^* também é uma aplicação linear sobre $\mathbb{F}_q$. Além disso, usando apenas a injectividade de ϕ, tem-se

$$\phi^*(x_1, \ldots, x_n) = 0 \iff \phi(x_i) = 0 \ \ \forall\, i \iff x_i = 0 \ \ \forall\, i \iff (x_1, \ldots, x_n) = 0 \ ,$$

portanto ϕ^* é injectiva.

1º caso: concatenação com um código trivial

Seja A um código linear $[N, K, D]$ sobre $\mathbb{F}_{q^m}$. Em particular A é um subespaço vectorial de $\mathbb{F}_{q^m}^N$ e podemos aplicar ϕ^* às palavras de A. Seja

$$A^* := \phi^*(A) = \{(\phi(x_1), \phi(x_2), \ldots, \phi(x_N)) \,:\, (x_1, \ldots, x_N) \in A\} \ .$$

A^* diz-se a *concatenação* de A com o código trivial $\mathbb{F}_q^m$. Como A é um código linear e ϕ^* é uma aplicação linear sobre $\mathbb{F}_q$, a concatenação $A^* = \phi^*(A)$ é ainda um código linear (a imagem de um subespaço vectorial por uma aplicação linear é um espaço vectorial).

Exemplo 8.59. Seja $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ onde α é uma raiz do polinómio $1 + t + t^2 \in \mathbb{F}_2[t] \subset \mathbb{F}_4[t]$, ou seja, $\alpha^2 = 1 + \alpha$. A aplicação $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2$ é definida por $\phi(0) = 00$, $\phi(1) = 10$, $\phi(\alpha) = 01$ e $\phi(\alpha^2) = \phi(1 + \alpha) = 11$. Atendendo a que $\{1, \alpha\}$ é uma base de $\mathbb{F}_4$ como espaço vectorial sobre $\mathbb{F}_2$, bastava indicar $\phi(1)$ e $\phi(\alpha)$ para definir a aplicação linear ϕ.

Seja A o código de repetição binário de comprimento 3 sobre $\mathbb{F}_4$, portanto A é um código cíclico. A concatenação de A com $\mathbb{F}_2^2$ é o código binário

$$A^* = \phi^*(A) = \{000000, 010101, 101010, 111111\} = \langle 010101, 101010 \rangle \ . \tag{8.9}$$

Neste caso, A^* é ainda um código cíclico.

Exemplo 8.60. Ainda sobre $\mathbb{F}_4$ como no exemplo anterior, considere o código

$$A = \langle (1, \alpha, \alpha^2) \rangle = \{(0,0,0), (1, \alpha, \alpha^2), (\alpha, \alpha^2, 1), (\alpha^2, 1, \alpha)\} \ .$$

A concatenação de A é o código binário

$$A^* = \phi^*(A) = \{000000, 100111, 011110, 111001\} = \langle 100111, 011110 \rangle \ . \tag{8.10}$$

Neste caso, A^* não é cíclico, apesar de C ser um código cíclico.

2º caso: concatenação de dois códigos

Consideremos dois códigos lineares: um código A de parâmetros $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e um código B de parâmetros $[n, m, d]$ sobre $\mathbb{F}_q$. Como $\dim B = m = \dim \mathbb{F}_{q^m}$, então B e $\mathbb{F}_{q^m}$ são isomorfos como espaços vectoriais sobre $\mathbb{F}_q$. Fixemos, então um isomorfismo linear

$$\phi : \mathbb{F}_{q^m} \longrightarrow B$$

e seja ϕ^* a aplicação definida como em (8.8) à custa deste ϕ. Portanto ϕ^* é $\mathbb{F}_q$-linear, injectiva, e, como $\phi(x_i) \in B$ para qualquer $x_i \in \mathbb{F}_{q^m}$, a sua imagem é um subespaço de B^N.

Como o código A é um subespaço vectorial de $\mathbb{F}_{q^m}^N$ sobre $\mathbb{F}_{q^m}$ e como este corpo é um espaço vectorial sobre $\mathbb{F}_q$, então A é também um subespaço vectorial sobre $\mathbb{F}_q$ (trata-se de um caso particular do Exercício 3.12) e, portanto, $\phi^*(A)$ é um subespaço de $\mathbb{F}_q^{mN}$ sobre $\mathbb{F}_q$ porque ϕ^* é uma aplicação $\mathbb{F}_q$-linear.

Definição 8.61. Dado o *código exterior* A de parâmetros $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e o *código interior* B de parâmetros $[n, m, d]$ sobre $\mathbb{F}_q$, e um isomorfismo vectorial $\phi : \mathbb{F}_{q^m} \longrightarrow B$, o código linear $C = \phi^*(A)$ diz-se a *concatenação* de A e B.

Exemplo 8.62. Seja $\mathbb{F}_8 = \mathbb{F}_2[t]/\langle 1+t+t^3\rangle = \mathbb{F}[\alpha]$, onde α é uma raiz do polinómio $1+t+t^3$. Seja A o código linear sobre $\mathbb{F}_8$ gerado pelo vector $(1, \alpha) \in \mathbb{F}_8^2$, e seja $B = \mathbb{F}_2^3$. Considere as aplicações lineares $\phi_1, \phi_2 : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^3 = B$ definidas por

$$\phi_1(1) = 001,\ \phi_1(\alpha) = 010,\ \phi_1(\alpha^2) = 100 \qquad \text{e} \qquad \phi_2(1) = 111,\ \phi_2(\alpha) = 100,\ \phi_2(\alpha^2) = 110\ .$$

ϕ_1 e ϕ_2 são isomorfismos, por isso podemos formar as concatenações $C_1 = \phi_1^*(A)$ e $C_2 = \phi_2^*(A)$, que são códigos binários de parâmetros $[6, 3, 2]$ e $[6, 3, 3]$, respectivamente – justifique! Logo C_1 e C_2 não são códigos equivalentes, apesar dos códigos exterior A e interior B serem os mesmos.

Proposição 8.63. *Se A e B são códigos $[N, K, D]_{q^m}$ e $[n, m, d]_q$, respectivamente, então a concatenação C é um código $[nN, mK, d']_q$, onde $d' \geq dD$.*

Dem. Por construção, o comprimento do código concatenação é nN, uma vez que $C \subset \mathbb{F}_q^{nN}$.

Como ϕ^* é uma aplicação injectiva e $C = \phi^*(A)$, então $|C| = |A| = (q^m)^{\dim A} = q^{mK}$, logo $\dim C = \log_q |C| = mK$.

Quanto à distância mínima, pelo Teorema 4.5, basta ver que $\mathrm{w}(y) \geq dD$ para qualquer $y \in C \setminus \{\vec{0}\}$. Seja $(x_1, \ldots, x_N) \in A \setminus \{\vec{0}\}$ com $x_i \in \mathbb{F}_{q^m}$. Para cada j tal que $x_j \neq 0$, tem-se $\phi(x_j) \neq \vec{0}$, porque ϕ é injectiva e linear. Portanto $\mathrm{w}(\phi(x_i)) \geq d = \mathrm{d}(B)$ porque $\phi(x_i) \in B \setminus \{\vec{0}\}$. Por outro lado, $\mathrm{w}(x_1, \ldots, x_N) \geq D = \mathrm{d}(A)$, donde

$$\mathrm{w}(y) = \mathrm{w}(\phi^*(x_1, \ldots, x_n)) = \mathrm{w}(\phi(x_1), \ldots, \phi(x_N)) \geq dD\ ,$$

porque há pelo menos D coordenadas x_j não nulas. Como $y = \phi^*(x_1, \ldots, x_N)$ é uma palavra arbitrária de C, conclui-se que $\mathrm{d}(C) \geq dD$. □

Corolário 8.64. *Se existe um código $[N, K, D]_{q^m}$, então também existe um código $[mN, mK, D]_q$.*

Dem. Seja A um código $[N, K, D]$ sobre $\mathbb{F}_{q^m}$ e seja $B = \mathbb{F}_q^m$ sobre $\mathbb{F}_q$. Como os parâmetros de B são $[m, m, 1]_q$, pela Proposição 8.63, a concatenação C de A e B é um código $[mN, mK, d']_q$ com $d' \geq D$. Pelo Teorema 5.11 aplicado a C com $t = d' - D \geq 0$ e $s = r = 0$, obtemos um código $[mN, mK, D]_q$ como pretendiamos. □

Exemplo 8.65. No Exemplo 8.59, o código exterior A e o código interior $B = \mathbb{F}_2^2$ tem parâmetros $[3, 1, 3]_4$ e $[2, 2, 1]_2$, respectivamente. Os parâmetros da concatenação podem ser determinados directamente da lista das palavras em (8.9) e são $[6, 2, 3]_2$. Neste caso $d' = 3 = dD$. No Exemplo 8.60, o código interior é o mesmo B, o código exterior A é diferente, mas tem também parâmetros $[3, 1, 3]_4$ (na realidade, este A é equivalente ao código de repetição). A concatenação A^* tem parâmetros $[6, 2, 4]_2$ – ver a lista das palavras em (8.10). Neste caso $d' = 4 > 3 = dD$.

Quanto à capacidade de erros acumulados, temos o seguinte resultado.

Teorema 8.66. *Seja C um código linear sobre $\mathbb{F}_{q^m}$. Então a concatenação $C^* = \phi^*(C)$, de C com o código trivial $\mathbb{F}_q^m$, corrige os erros acumulados de comprimento até $m(T-1)+1$, onde $T = \lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor$.*

Dem. Seja n o comprimento do código C e seja $l = m(T-1)+1$. Vamos ver que todos os erros acumulado de comprimento menor ou igual a l pertencem a classes $z + C^*$ distintas.

Sejam $\vec{e}, \vec{f} \in \mathbb{F}_q^{mn}$ dois erros acumulados, distintos, de comprimento $\leq l$. Se $\phi : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q^m$ é um isomorfismo linear sobre $\mathbb{F}_q$, $\phi^* : (\mathbb{F}_{q^m})^n \longrightarrow \mathbb{F}_q^{mn}$ também é. Sejam $\vec{x} = (\phi^*)^{-1}(\vec{e})$ e $\vec{y} = (\phi^*)^{-1}(\vec{f})$.

Pondo $\vec{x} = (x_1, \ldots, x_n)$, com $x_i \in \mathbb{F}_{q^m}$, fica

$$\vec{e} = (\phi(x_1), \ldots, \phi(x_n)) = (0, 0, \ldots, 0, \underbrace{a, *, \ldots, *, b}_{\leq l \text{ coordenadas}}, 0, \ldots, 0) \ ,$$

onde $a, b \neq 0$ e cada $\phi(x_i) \in \mathbb{F}_q^m$. Identificar $\phi(x_1), \ldots, \phi(x_n)$ no vector dado $\vec{e}$ corresponde a separar as mn coordenadas de $\vec{e}$ em blocos de comprimento m. O caso com mais $\phi(x_i)$ não nulos acontece quando a primeira coordenada não nula de $\vec{e}$ é a última coordenada de um bloco $\phi(x_j)$. Portanto há no máximo $1 + \left\lceil \frac{l-1}{m} \right\rceil$ blocos $\phi(x_i)$ que podem conter coordenadas não nulas de $\vec{e}$. Como ϕ é injectiva, $\phi(x_i) = 0$ se e só se $x_i = 0$, tem-se

$$\mathrm{w}(\vec{x}) \leq 1 + \left\lceil \frac{l-1}{m} \right\rceil = T \ .$$

E analogamente se tem $\mathrm{w}(\vec{y}) \leq T$. Como $\vec{x} \neq \vec{y}$, porque $\vec{e} \neq \vec{f}$, e como ambos têm peso $\leq T$, então $\vec{x}$ e $\vec{y}$ são chefes de classes de C distintas (pela Proposição 4.29) e, usando a injectividade de ϕ^*, conclui-se que $\vec{e}$ e $\vec{f}$ pertencem a classes de C^* distintas. □

Exercícios

8.1. (a) Mostre que a aplicação *desvio cíclico* $\sigma : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$ definida por $\sigma(x_1, \ldots, x_{n-1}, x_n) = (x_n, x_1, \ldots, x_{n-1})$ é linear e bijectiva.
(b) Mostre que um código linear C é cíclico se e só se $\sigma^i(C) = C$ para todo o $i \in \mathbb{Z}$.

8.2. (a) No Exemplo 8.6, mostre que $\langle 2, t \rangle$ não é um ideal principal em $\mathbb{Z}[t]$.
(b) Mostre que $\langle x, y \rangle$ não é um ideal principal no anel dos polinómios de duas variáveis[4] $\mathbb{F}_q[x, y]$.

8.3. Para $a \in \mathbb{F}_q$ fixo, mostre que o conjunto $I = \{f(t) \in \mathbb{F}_q[t] \ : \ f(a) = 0\}$ é um ideal em $\mathbb{F}_q[t]$. Determine um gerador de I.

8.4. Os ideais nas seguintes alíneas são ideais do anel $R_n = \mathbb{F}_q[t]/\langle t^n - 1 \rangle$. Assumindo que $g(t) | t^n - 1$ em $\mathbb{F}_q[t]$, mostre que
(a) $\langle f_1(t) \rangle \subset \langle f_2(t) \rangle$ se e só se $f_2(t)$ divide $f_1(t)$ em R_n;
(b) $\langle f(t) \rangle = \langle g(t) \rangle$ se e só se existe $a(t) \in \mathbb{F}_q[t]$ tal que $f(t) \equiv a(t)g(t) \pmod{t^n - 1}$ e $\mathrm{MDC}(a(t), h(t)) = 1$, onde $h(t)g(t) = t^n - 1$;

8.5. Factorize o polinómio $t^7 - 1$ em $\mathbb{F}_2[t]$ e identifique todos os códigos binários cíclicos de comprimento 7.

8.6. Classifique todos os códigos cíclicos de comprimento 4 sobre $\mathbb{F}_3$. Conclua que o código de Hamming ternário $\mathrm{Ham}(2, 3)$ não é equivalente a um código cíclico.

8.7. (a) Factorize $t^{12} - 1$ no produto de polinómios irredutíveis em $\mathbb{F}_2[t]$.
(b) Quantos códigos cíclicos binários de comprimento 12 existem?
(c) Determine para que valores de k existe um código cíclico binário $[12, k]$.
(d) Quantos códigos cíclicos binários com parâmetros $[12, 9]$ existem?
(e) Determine todos os códigos cíclicos binários auto-duais de comprimento 12, indicando os respectivos polinómios geradores.

8.8. Seja C um código cíclico binário com polinómio gerador $g(t)$.
(a) Mostre que, se $t - 1$ divide $g(t)$, então todas as palavras de código têm peso par.
(b) Assumindo que o comprimento de C é ímpar, mostre que C contém uma palavra de peso ímpar se e só se o vector $\vec{1} = (1, \ldots, 1)$ é uma palavra de código.

8.9. (a) Determine o polinómio gerador e a dimensão do menor código cíclico binário que contém a palavra $c = 1110010 \in \mathbb{F}_2^7$.
(b) Escreva uma matriz geradora, o polinómio de paridade e uma matriz de paridade para o código que determinou na alínea anterior.

[4] Podia ser $\mathbb{K}[x, y]$, com $\mathbb{K}$ um corpo qualquer.

8.10. Determine o polinómio gerador e a dimensão do menor código cíclico ternário que contém a palavra $c = 220211010000 \in \mathbb{F}_3^{12}$.

8.11. Seja C um código cíclico, de comprimento n, com polinómio gerador $g(t)$. Mostre que, se $C = \langle f(t) \rangle$, i.e., se $f(t)$ é um gerador do ideal C, então $g(t) = \text{MDC}(f(t), t^n - 1)$. Em particular, conclua que o polinómio gerador do menor código cíclico, de comprimento n, que contém $f(t)$ é $g(t) = \text{MDC}(f(t), t^n - 1)$.

8.12. Se $g(t)$ é o polinómio gerador de um código cíclico, mostre que $\langle g(t) \rangle$ e $\langle \overline{g}(t) \rangle$ são códigos equivalentes. Conclua que o código gerado pelo polinómio de paridade de um código cíclico C é equivalente ao código dual $C^\perp$.

8.13. Suponha que, em $\mathbb{F}_2[t]$,

$$t^n - 1 = (t-1)g_1(t)g_2(t)$$

e que $\langle g_1(t) \rangle$ e $\langle g_2(t) \rangle$ são códigos equivalentes. Mostre que:

(a) Se $c(t)$ é uma palavra de código de $\langle g_1(t) \rangle$ de peso w ímpar, então:
  (i) $w^2 \geq n$;
  (ii) Se, além disso, $g_2(t) = \overline{g}_1(t)$, então $w^2 - w + 1 \geq n$.

(b) Se n é um número primo ímpar, $g_2(t) = \overline{g}_1(t)$ e $c(t)$ é uma palavra de código de $\langle g_1(t) \rangle$ de peso w par, então:
  (i) $w \equiv 0 \pmod 4$;
  (ii) $n \neq 7 \Rightarrow w \neq 4$.

(c) Mostre que o código cíclico binário de comprimento 23 gerado pelo polinómio $g(t) = 1 + t^2 + t^4 + t^5 + t^6 + t^{10} + t^{11}$ é um código perfeito $[23, 12, 7]$ — *Código de Golay binário.*

8.14. (a) Seja $g(t)$ o polinómio gerador de um código de Hamming binário $\text{Ham}(r, 2)$, com $r \geq 3$. Mostre que $C = \langle (t-1)g(t) \rangle$ é um código de parâmetros $[2^r - 1, 2^r - r - 2, 4]$.
Sugestão: use o exercício 8.8.

(b) Mostre que o código C pode ser usado para corrigir todos os erros duplos adjacentes, i.e., em posições consecutivas.

(c) (Generalização da alínea anterior.) Seja $C = \langle (t+1)f(t) \rangle$ um código cíclico binário de comprimento n, onde $(t+1)f(t) \mid t^n - 1$, mas $f(t) \nmid t^k - 1$, para $1 \leq k \leq n-1$. Mostre que C corrige todos os erros simples e também os erros duplos adjacentes.

8.15. Seja C o código cíclico binário de comprimento $n = 15$ gerado pelo polinómio

$$g(t) = 1 + t^4 + t^6 + t^7 + t^8 \ .$$

(a) Justifique que $g(t)$ é de facto o polinómio gerador do código C.

(b) Escreva uma matriz geradora, o polinómio de paridade e uma matriz de paridade para C.

(c) Escreva, justificando, uma matriz geradora na forma $G = \begin{bmatrix} R & I \end{bmatrix}$ para aquele código e a correspondente matriz de paridade.
Sugestão: use a fórmula (8.5) (e o Teorema 8.37) para determinar as linhas de R.

(d) Codifique sistematicamente o vector mensagem $m = 1001001$.

(e) Sabendo que o código tem distância mínima $\text{d}(C) = 5$, descodifique os vectores recebidos

$$y = 000101011110000 \qquad \text{e} \qquad z = 011001001001111 \ .$$

8.16. (a) Verifique que $g(t) = 2 + t^2 + 2t^3 + t^4 + t^5$ divide $t^{11} - 1$ em $\mathbb{F}_3[t]$.

(b) Seja C o código cíclico ternário gerado por $g(t)$. Sabendo que se trata de um código $[11, 6, 5]_3$, use o Algoritmo Caça ao Erro para descodificar o vector recebido $y = 20121020112$.

(c) Qual é a proporção de erros de peso 2 que são corrigidos por este algoritmo?

8.17. Considere de novo o código cíclico binário de comprimento $n = 15$ com polinómio gerador $g(t) = 1 + t^4 + t^6 + t^7 + t^8$ do Exercício 8.15.

(a) Justifique que, embora seja um código de distância mínimma 5, se trata de um código corrector de até erros-3 acumulados.

(b) Utilizando essa capacidade correctora, descodifique pelo Algoritmo Caça ao Erro Acumulado o vector recebido $y = 100000110111110$.

8.18. (a) Seja C um código cíclico $[n,k,d]_q$ com polinómio gerador $g(t)$. Como C é também um código linear, pela independência linear das colunas de uma matriz de paridade, já sabemos que C corrige todos os erros de apagamento até $d-1$ símbolos, usando descodificação por síndrome. Usando agora as propriedades cíclicas do código e o Algoritmo Caça ao Erro, quais os tipos de erros de apagamento que C pode corrigir? Considere não só o número de símbolos apagados mas também a sua distribuição na palavra recebida.

(b) Considere novamente o código binário de comprimento $n = 15$ com polinómio gerador $g(t) = 1 + t^4 + t^6 + t^7 + t^8$ do Exercício 8.15. A distância mínima deste código é $d = 5$. Descodifique, se possível, os seguintes vectores recebidos

$$y = 000??????111000 \qquad \text{e} \qquad z = ?0101?0101?0000 \ .$$

8.19. Seja C o código cíclico sobre $\mathbb{F}_5$ e de comprimento 15 com o seguinte polinómio gerador

$$g(t) = 1 + 3t + t^2 + 2t^3 + t^4 + 3t^5 + t^6 \in \mathbb{F}_5[t] \ .$$

(a) Quantos códigos cíclicos, sobre $\mathbb{F}_5$, de comprimento 15 e com a mesma dimensão de C é que existem? Indique os respectivos polinómios geradores.

(b) Sabendo que C corrige todos os erros-l acumulados com $l \leq 3$, descodifique o vector recebido

$$y = 042201213100000 \in \mathbb{F}_5^{15} \ ,$$

usando o Algoritmo Caça ao Erro Acumulado.

(c) Sabendo que ocorreram apenas erros de apagamento, corrija, se possível, os seguintes vectores recebidos

$$z = ?20?04031000000 \qquad \text{e} \qquad w = 0000?0000?0000?$$

Sugestão: poderá querer verificar que o sintoma de t^{10} é $S(t^{10}) = 4t^5 + 4$.

8.20. Mostre que o código entrelaçado de grau s, $C^{(s)}$, é equivalente ao código soma $C \oplus \cdots \oplus C$ de s cópias de C. Conclua que $\mathrm{d}(C^{(s)}) = \mathrm{d}(C)$.

8.21. Conclua a demonstração do Teorema 8.57 (a): Seja C um código linear q-ário e sejam $x^{(s)}$ e $y^{(s)}$ os entrelaçados de $x_1, \ldots, x_s \in C$ e de $y_1, \ldots, y_s \in C$, respectivamente. Mostre que

(i) $x^{(s)} + y^{(s)}$ é o entrelaçado dos vectores $x_1 + y_1, \ldots, x_s + y_s$;

(ii) $ax^{(s)}$ é o entrelaçado dos vectores $ax_1, \ldots, ax_s$, onde $a \in \mathbb{F}_q$.

8.22. Seja $C = \mathrm{Ham}(3,2)$ o código de Hamming binário de redundância 3, com polinómio gerador $g(t) = 1 + t + t^3$.

(a) Determine os parâmetros $[n,k,d]$ de $C^{(3)}$.

(b) Determine o polinómio gerador e o de paridade de $C^{(3)}$.

(c) Mostre que o código $C^{(3)}$ corrige todos os erros-m acumulados com $m \leq 3$, mas não corrige todos os erros acumulados de comprimento 4.

(d) Usando o Algoritmo Caça ao Erro Acumulado, descodifique o vector recebido

$$y(t) = t + t^3 + t^4 + t^9 + t^{13} \ .$$

8.23. Um código cíclico q-ário de comprimento n diz-se *degenerado* se existe $r \in \mathbb{N}$ tal que r divide n e cada palavra do código se escreve na forma $c = c'c' \cdots c'$ com $c' \in \mathbb{F}_q^r$, isto é, cada palavra do código consiste em n/r cópias idênticas de uma sequência c' de comprimento r.

(a) Mostre que o entrelaçamento $C^{(s)}$ de um código de repetição C é um código degenerado.

(b) Mostre que o polinómio gerador de um código cíclico degenerado de comprimento n é da forma

$$g(t) = a(t)(1 + t^r + t^{2r} + \cdots + t^{n-r}) \ .$$

(c) Mostre que um código cíclico de comprimento n e polinómio de paridade $h(t)$ é degenerado se e só se existe $r \in \mathbb{N}$ tal que r divide n e $h(t)$ divide $t^r - 1$.

8.24. Seja C o código binário linear com a seguinte matriz de paridade

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

(a) Determine a distância mínima $\mathrm{d}(C)$ e indique a capacidade de detecção e de correcção de erros aleatórios deste código.

(b) Mostre que C detecta todos os erros-m acumulados com $m \leq 3$.
Nota: Neste exercício considera-se apenas vectores erros-m acumulados no sentido "estrito", i.e., vectores da forma $(0, \ldots, 0, 1, *, \ldots, *, 1, 0, \ldots, 0)$ com as coordenadas não nulas entre os índices $i \geq 1$ e $i + m - 1 \leq n$.

(c) Seja C' o pontuado, na última coordenada, do código dual $C^{\perp}$. Mostre que C' é um código cíclico e degenerado, e determine o seu polinómio gerador.

8.25. Determine todos os códigos binários, cíclicos e degenerados de comprimento 9, indicando os respectivos polinómios geradores e a correspondente sequência de comprimento r.

8.26. Considere o código linear $A = \langle (1, \alpha^2, 0), (\alpha, 0, 1) \rangle$ sobre $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, onde $\alpha^2 = 1 + \alpha$, e o código linear binário $B = \langle 1010, 0101 \rangle$. Seja A^* a concatenação de A e B em relação à aplicação linear $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^4$ definida por $\phi(1) = 1010$ e $\phi(\alpha) = 1111$.

(a) Determine uma base para o código A^*.

(b) Determine os parâmetros $[n, k, d]$ do código A^*.

8.27. Seja $C = \langle (0, \alpha, \alpha^2, 1), (1, 1, 1, 1) \rangle \subset \mathbb{F}_4^4$, onde $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$ com $\alpha^2 = 1 + \alpha$.

(a) Determine uma matriz geradora e os parâmetros do código concatenação $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_4 \longrightarrow \mathbb{F}_2^2$ é a aplicação linear sobre $\mathbb{F}_2$ definida por $\phi(1) = 10$ e $\phi(\alpha) = 01$.

(b) Justifique que o código C^* é equivalente a $\widehat{\mathrm{Ham}}(3, 2)^{\perp}$.

8.28. Seja $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, onde α é uma raiz do polinómio $1 + t^2 + t^3$, e considere o código sobre $\mathbb{F}_8$

$$A = \langle (\alpha + 1, \alpha^2 + 1, 1) \rangle \ .$$

(a) Considere a aplicação $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ definida por $\phi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3)$, onde $a_1, a_2, a_3 \in \mathbb{F}_2$. Quais os parâmetros de $A^* = \phi^*(A)$?

(b) Considere a aplicação $\psi : \mathbb{F}_8 \to \mathbb{F}_2^4$ definida por $\psi(a_1 + a_2\alpha + a_3\alpha^2) = (a_1, a_2, a_3, a_1 + a_2 + a_3)$, onde $a_1, a_2, a_3 \in \mathbb{F}_2$. Quais os parâmetros de $A' = \psi^*(A)$?
Sugestão: A' é a concatenação de A com um código binário B; comece por identificar B.

(c) O que pode concluir acerca da capacidade de correção de erros aleatórios e/ou erros acumulados de A^* e de A'?

8.29. Seja C o código de repetição de comprimento n sobre $\mathbb{F}_{q^m}$ e seja C^* o código concatenação de C com o código trivial q-ário $(\mathbb{F}_q)^m$. Mostre que C^* é um código q-ário cíclico e indique os seus parâmetros $[N, K, D]$.

Códigos Reed-Solomon

Um dos problemas na Teoria de Códigos é determinar a distância mínima de um dado código. Tratando-se de códigos cíclicos, por vezes conseguimos controlar a distância mínima com uma "boa escolha" do polinómio gerador. É este o caso dos códigos Reed-Solomon. Estes códigos são MDS, ou seja, para o comprimento e a dimensão fixos, têm a maior distância mínima possível, e são ainda muito importantes na correcção de erros acumulados.

Definição 9.1. Um código Reed-Solomon q-ário é um código cíclico, de comprimento $q-1$, com polinómio gerador

$$g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1}) \ ,$$

com $a \geq 0$ e $2 \leq \delta \leq q-1$, onde α é um elemento primitivo de $\mathbb{F}_q$.

Observação 9.2. (i) Pela Proposição 3.15, sabemos que $x^{q-1} = 1$ para qualquer $x \in \mathbb{F}_q \setminus \{0\}$, logo, se α é um elemento primitivo de $\mathbb{F}_q$, o polinómio $t^{q-1}-1 \in \mathbb{F}_q[t]$ tem a seguinte factorização

$$t^{q-1} - 1 = (t-1)(t-\alpha)(t-\alpha^2) \cdots (t-\alpha^{q-2}) \ . \tag{9.1}$$

Portanto, o polinómio $g(t)$ na Definição 9.1 é um divisor de $t^{q-1}-1$ e $g(t)$ é de facto o polinómio gerador de um código cíclico. Além disso, as raízes de $g(t)$ são todas distintas.

(ii) Como $\text{grau}(g(t)) = \delta - 1$, a dimensão de C é $\dim(C) = n - (\delta - 1) = q - \delta$. Em particular $1 \leq \dim(C) \leq q-2$, logo os códigos triviais $\mathbb{F}_q^{q-1}$ e $\{\vec{0}\}$ não são códigos Reed-Solomon.

(iii) Não há códigos Reed-Solomon binários, pois $2 \leq \delta \leq q-1 \Rightarrow q \geq 3$.

Exemplo 9.3. Como 3 é um elemento primitivo de $\mathbb{F}_7$,

$$g(t) = (t-3^2)(t-3^3)(t-3^4) = 1 + 2t + 2t^2 + t^3$$

é o polinómio gerador de um código Reed-Solomon de parâmetros $[6, 3]$.

$$G = \begin{bmatrix} 1 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix}$$

é uma matriz geradora, $h(t) = \frac{t^6-1}{g(t)} = 6 + 2t + 5t^2 + t^3$ é o polinómio de paridade e

$$H = \begin{bmatrix} 1 & 5 & 2 & 6 & 0 & 0 \\ 0 & 1 & 5 & 2 & 6 & 0 \\ 0 & 0 & 1 & 5 & 2 & 6 \end{bmatrix}$$

é uma matriz de paridade. A partir de H, aplicando o Teorema 4.16, podemos concluir que $\mathrm{d}(C) = 4$ e, portanto, trata-se de um código MDS.

1. Distância mínima

Nesta secção iremos ver que os códigos Reed-Solomon são MDS.

Proposição 9.4. *Seja C um código Reed-Solomon q-ário, com polinómio gerador $g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1})$. Então*

$$C = \{x(t) \in R_{q-1} \,:\, x(\alpha^i) = 0\,, \forall\, i = a+1, \ldots, a+\delta-1\}\ .$$

Dem. (i) Pelo Lema 8.16, $x(t) \in C$ se e só se $x(t) = a(t)g(t)$ para algum $a(t) \in \mathbb{F}_q[t]$, portanto as raízes de g(t) são também raízes de qualquer palavra de código $x(t)$.
(ii) Seja agora $x(t) \in R_{q-1}$ tal que $x(\alpha^i) = 0$ para $i = a+1, \ldots, a+\delta-1$. Portanto $t - \alpha^i$ divide $x(t)$ (no anel $\mathbb{F}_q[t]$), para $i = a+1, \ldots, a+\delta-1$, e como estes α^i são todos distintos, podemos concluir que $g(t)$ divide $x(t)$, logo $x(t) \in C$. □

Note que a parte (i) da demonstração anterior é válida para qualquer código cíclico, e na parte (ii) apenas se usou o facto das raízes do polinómio gerador serem todas distintas. Podemos portanto generalizar a Proposição 9.4, com a mesma demonstração, para o seguinte resultado:

Teorema 9.5. *Se C é um código q-ário de comprimento n tal que o seu polinómio gerador $g(t)$, de grau r, tem raízes distintas $\alpha_1, \ldots, \alpha_r$ (não necessarimante em $\mathbb{F}_q$), então*

$$C = \{x(t) \in R_n \,:\, c(\alpha_i) = 0\,, \forall\, i = 1, \ldots, r\}\ .$$

Exemplo 9.6. Seja $C = \mathrm{Ham}(3, 2)$ com polinómio gerador $g(t) = 1 + t + t^3$. O comprimento de C é $n = 7$. No anel $\mathbb{F}_8$, o polinómio $t^7 - 1$ factoriza-se no produto de termos lineares distintos (ver alínea (i) na Observação 9.2), portanto as raízes de $g(t)$ são distintas, porque $g(t) | t^7 - 1$. Pelo Teorema 9.5,

$$C = \{x(t) \in R_7 \,:\, x(\beta) = 0\,, \forall\ \beta \text{ raiz de } g(t)\}\ .$$

Como todos os elementos de $\mathbb{F}_8 \setminus \{0, 1\}$ são raízes de $x(t) = 1 + t + t^2 + t^3 + t^4 + t^5 + t^6 = \dfrac{t^7 - 1}{t - 1}$, então as raízes de $g(t)$ são também raízes de $x(t)$, donde $x(t) \in C \subset R_7$, ou seja $\vec{1} \in C \subset \mathbb{F}_2^7$.

Teorema 9.7. *Seja C um código Reed-Solomon de parâmetros $[q-1, q-\delta]_q$. Então* $\mathrm{d}(C) \geq \delta$.

Dem. Seja $g(t) = (t - \alpha^{a+1})(t - \alpha^{a+2}) \cdots (t - \alpha^{a+\delta-1})$ o polinómio gerador de C. Suponhamos, por absurdo, que $\mathrm{d}(C) = d < \delta$ e seja $x(t) = x_0 + x_1 t + \cdots + x_{n-1} t^{n-1} \in C$ com peso $\mathrm{w}(x(t)) = d$. Seja $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_q^n$ o vector correspondente a $x(t)$.

Pela Proposição 9.4, $x(\alpha^i) = 0$ para qualquer $i = a+1, \ldots, a+\delta-1$. Por outro lado,

$$x(\alpha^i) = x_0 + x_1\alpha^i + \cdots + x_{n-1}(\alpha^i)^{n-1} = (1, \alpha^i, (\alpha^i)^2, \ldots, (\alpha^i)^{n-1}) \cdot x\ .$$

Portanto $Ax = 0$, onde

$$A = \begin{bmatrix} 1 & \alpha^{a+1} & (\alpha^{a+1})^2 & \cdots & (\alpha^{a+1})^{n-1} \\ 1 & \alpha^{a+2} & (\alpha^{a+2})^2 & \cdots & (\alpha^{a+2})^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{a+\delta-1} & (\alpha^{a+\delta-1})^2 & \cdots & (\alpha^{a+\delta-1})^{n-1} \end{bmatrix}$$

é uma matriz com $\delta - 1$ linhas e n colunas. Sejam $i_1, \ldots, i_d$ os índices tais que $x_{i_j} \neq 0$. Seja A' a matriz formada pelas colunas $i_1 + 1, i_2 + 1, \ldots, i_d + 1$ de A. Então A' tem $\delta - 1$ linhas e d colunas. Como $d \leq \delta - 1$, a matriz A'' formada pelas d primeiras linhas de A' é uma matriz quadrada $d \times d$ e

$$A'' \begin{bmatrix} x_{i_1} \\ \vdots \\ x_{i_d} \end{bmatrix} = 0\ ,$$

portanto $\det(A'') = 0$, porque $(x_{i_1}, \ldots, x_{i_d})$ é uma solução não nula do sistema linear homogénio $A''y = 0$. Por outro lado, como

$$A'' = \begin{bmatrix} (\alpha^{a+1})^{i_1} & (\alpha^{a+1})^{i_2} & \cdots & (\alpha^{a+1})^{i_d} \\ (\alpha^{a+2})^{i_1} & (\alpha^{a+2})^{i_2} & \cdots & (\alpha^{a+2})^{i_d} \\ \vdots & \vdots & & \vdots \\ (\alpha^{a+d})^{i_1} & (\alpha^{a+d})^{i_2} & \cdots & (\alpha^{a+d})^{i_d} \end{bmatrix},$$

usando as propriedade de multilinearidade do determinante nas colunas obtém-se

$$\begin{aligned} \det(A'') &= \prod_{j=1}^{d} (\alpha^{a+1})^{i_j} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_d} \\ \vdots & \vdots & & \vdots \\ (\alpha^{d-1})^{i_1} & (\alpha^{d-1})^{i_2} & \cdots & (\alpha^{d-1})^{i_d} \end{bmatrix} \\ &= \prod_{j=1}^{d} (\alpha^{a+1})^{i_j} \prod_{1 \le k < l \le d} (\alpha^{i_l} - \alpha^{i_k}) \ . \end{aligned}$$

Logo, $\det(A'') \neq 0$ pois $\alpha^{i_l} \neq \alpha^{i_k}$, porque α é um elemento primitivo e $d \le \delta - 1 \le q - 2$. Como não podemos ter simultaneamente $\det(A'') = 0$ e $\det(A'') \neq 0$, concluimos que $d \ge \delta$. □

Observação 9.8. Na demonstração do teorema anterior apenas se usou o facto de C ser o conjunto dos elementos $x(t) \in R_n$ que se anulam em todas as raízes do polinómio gerador $g(t)$ (o qual foi provado para qualquer código cíclico tal que as raízes de $g(t)$ são todas distintas) e o facto de $\delta - 1$ potências consecutivas de um elemento primitivo $\alpha \in \mathbb{F}_q$ serem raízes de $g(t)$ (para se obter uma matriz de Vandermonde no segundo cálculo de $\det(A'')$). Os códigos cíclicos que satisfazem estas condições dizem-se *códigos BCH*[1]. Os códigos Reed-Solomon são uma subfamília dos códigos BCH. (Ver Apêndice B, em particular a Definição B.13.)

Exemplo 9.9. Seja C o código de comprimento 7, binário, com polinómio gerador $g(t) = 1 + t + t^3 \in \mathbb{F}_2[t]$. Como $g(t)$ é irredutível em $\mathbb{F}_2[t]$, podemos considerar $\mathbb{F}_8 = \mathbb{F}_2[t]/\langle g(t) \rangle$. Seja $\alpha \in \mathbb{F}_8$ uma raiz de $g(t)$. Então

$$g(t) = (t - \alpha)(t - \alpha^2)(t - \alpha^4) \ .$$

C não é um código Reed-Solomon, mas satisfaz as condições na Observação 9.8 com $\delta - 1 = 2$. Portanto podemos concluir que $\mathrm{d}(C) \ge \delta = 3$. Como $\mathrm{w}(g(t)) = 3$ (e $g(t) \in C$, claro!), então $\mathrm{d}(C) = 3$, resultado já conhecido pois $C = \mathrm{Ham}(3, 2)$.

Corolário 9.10. *Os códigos Reed-Solomon são códigos MDS.*

Dem. Seja C um código Reed-Solomon de parâmetros $[q-1, q-\delta]_q$. O polinómio gerador tem grau $r = \delta - 1$. Então $\mathrm{d}(C) \ge \delta$, pelo Teorema 9.7, e $\mathrm{d}(C) \le \delta$, pela desigualdade de Singleton. □

Exemplo 9.11. Considere o código Reed-Solomon C sobre $\mathbb{F}_{16}$ com polinómio gerador $g(t) = \prod_{i=1}^{6} (t - \alpha^i)$, onde α é um elemento primitivo de $\mathbb{F}_{16}$. O código C tem comprimento $n = q - 1 = 15$, dimensão $n - \mathrm{grau}(g(t)) = 9$ e, pelo teorema anterior, distância mínima $\mathrm{d}(C) = 7$. Para determinarmos $\mathrm{d}(C)$ usando o Teorema 4.16, como uma matriz de paridade H tem 6 linhas e 15 colunas, teriamos que verificar que

$$\binom{15}{6} = 5005$$

conjuntos de 6 colunas de H são linearmente independentes.

[1] Estes códigos foram descobertos por A. Hocquenghem em 1959 e, de forma independente, por R. C. Bose e D. K. Ray-Chaudhuri em 1960

2. Extensão de códigos Reed-Solomon

Recorde que, para um código C qualquer com alfabeto $\mathbb{F}_q$, a extensão por paridade é definida por

$$\widehat{C} = \left\{ (x, x_{n+1}) \in \mathbb{F}_q^{n+1} \,:\, x \in C,\, x_{n+1} = -\sum_{i=1}^{n} x_i \right\}$$

e, se C é linear de parâmetros $[n, k, d]$, a sua extensão $\widehat{C}$ também é linear e os seus parâmetros são $[n+1, k, \widehat{d}]$, com $d \leq \widehat{d} \leq d+1$.

Teorema 9.12. *Seja C um código Reed-Solomon com polinómio gerador*

$$g(t) = (t-\alpha)(t-\alpha^2)\cdots(t-\alpha^{\delta-1}) \ ,$$

com $2 \leq \delta \leq q-1$ e α um elemento primitivo de $\mathbb{F}_q$. Então o código estendido $\widehat{C}$ é MDS.

Dem. Como o código C tem parâmetros $[q-1, q-\delta, \delta]_q$, porque é MDS, queremos mostrar que $\mathrm{d}(\widehat{C}) = \delta + 1$. Pela observação anterior ao teorema, ou pela desigualdade de Singleton, já sabemos que $\mathrm{d}(\widehat{C}) \leq \delta + 1$. Vamos então mostrar a desigualdade contrária. Seja

$$x(t) = \sum_{i=0}^{q-2} x_i t^i \in C \setminus \{0\} \qquad \text{e} \qquad \widehat{x} = (x_0, x_1, \ldots, x_{q-2}, -\sum_{i=0}^{q-2} x_i) \in \widehat{C} \ .$$

Então $\widehat{x} \neq 0$, porque $x(t) \neq 0$, e $\widehat{x} = (x_0, x_1, \ldots, x_{q-2}, -x(1))$, porque $x(1) = \sum_{i=0}^{q-1} x_i$. Como $x(t) \in C = \langle g(t) \rangle$, então $x(t) = f(t)g(t)$, para algum $f(t) \in \mathbb{F}_q[t]$ e, portanto, $x(1) = f(1)g(1)$. Também temos que $g(1) \neq 0$, porque as raízes de $g(t)$ são $\alpha, \alpha^2, \ldots, \alpha^{\delta-1}$ com $\delta - 1 \leq q-2$, ou seja, nenhuma das raízes é 1 porque α tem ordem $q-1$. Há dois casos a considerar.

Caso 1: Se $f(1) \neq 0$, então $-x(1) \neq 0$, logo $\mathrm{w}(\widehat{x}) = \mathrm{w}(x) + 1 \geq \delta + 1$, pois $x \in C \setminus \{0\}$.

Caso 2: Se $f(1) = 0$, então $f(t) = u(t)(t-1)$ para algum $u(t) \in \mathbb{F}_q[t]$, donde $x(t) = u(t)(t-1)g(t)$ e, como $(t-1)g(t)$ divide $t^n - 1$ pois $g(1) \neq 0$, $(t-1)g(t)$ é o polinómio gerador de um código C' e $x(t) \in \langle (t-1)g(t) \rangle = C'$. Facilmente se vê que

$$(t-1)g(t) = (t-\alpha^{a+1})(t-\alpha^{a+2})\cdots(t-\alpha^{a+\delta}) \ ,$$

com $a = q-2 \geq 0$, e ainda $\mathrm{grau}(g(t)) \leq q-2$, pois, caso contrário, teriamos $(t-1)g(t) = t^{q-1} - 1$ e $C' = \langle t^{q-1} - 1 \rangle = \{0\}$, o que é impossível porque $x \in C'$ e $x \neq 0$. Como consequência, $(t-1)g(t)$ é o polinómio gerador de um código Reed-Solomon de parâmetros $[q-1, q-\delta']$, onde $\delta' = \delta + 1 \leq q-2$, logo $\mathrm{d}(C') = \delta'$ e, portanto, $\mathrm{w}(\widehat{x}) = \mathrm{w}(x) \geq \delta' = \delta + 1$.

Em ambos os casos, provámos que $\mathrm{w}(\widehat{x}) \geq \delta + 1$ para qualquer palavra de código $\widehat{x} \in \widehat{C}$ não nula, ou seja, $\mathrm{d}(\widehat{C}) = \mathrm{w}(\widehat{C}) \geq \delta + 1$. □

Exemplo 9.13. Considere o código Reed-Solomon, sobre $\mathbb{F}_7$, com o polinómio gerador $g(t) = (t-3^2)(t-3^3)(t-3^4)$ do Exemplo 9.3. Como C tem parâmetros $[6, 3, 4]$, o código estendido $\widehat{C}$ tem parâmetros $[7, 3, 5]$, pelo teorema anterior. C corrige qualquer erro simples porque $\lfloor \frac{\mathrm{d}(C)-1}{2} \rfloor = 1$, mas $\widehat{C}$ corrige qualquer erro de peso ≤ 2 porque $\lfloor \frac{\mathrm{d}(\widehat{C})-1}{2} \rfloor = 2$.

Exemplo 9.14. Considere o código Reed-Solomon C, sobre $\mathbb{F}_7$, com o polinómio gerador $g(t) = (t-3^0)(t-3^1) = (t-1)(t-3)$. Portanto, C é um código $[6, 4, 3]$, $h(t) = (t^6-1)/g(t) = 2+5t+6t^2+4t^3+t^4$ é o polinómio de paridade,

$$H = \begin{bmatrix} 1 & 4 & 6 & 5 & 2 & 0 \\ 0 & 1 & 4 & 6 & 5 & 2 \end{bmatrix}$$

é uma matriz de paridade para C, e

$$\widehat{H} = \begin{bmatrix} 1 & 4 & 6 & 5 & 2 & 0 & 0 \\ 0 & 1 & 4 & 6 & 5 & 2 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

é uma matriz de paridade para $\widehat{C}$. Por definição de extensão de paridade, os parâmetros de $\widehat{C}$ são $[7, 4, \widehat{d}]$, com $3 \leq \widehat{d} \leq 4$. Além disso, se c_i denota a i-ésima coluna de $\widehat{H}$, como $c_1 + c_3 + 5c_6 = 0$ então $\widehat{d} \leq 3$, pelo Teorema 4.16, donde se conclui que $\widehat{d} = 3$ e, portanto, $\widehat{C}$ não é um código MDS. Porque é que este exemplo não contradiz o Teorema 9.12?

Não basta assumir que $t - 1$ não divide $g(t)$ nas hipóteses do Teorema 9.12, como mostram os próximos dois exemplos.

Exemplo 9.15. Ainda sobre $\mathbb{F}_7$, seja C o código Reed-Solomon com polinómio gerador $g(t) = (t - 3^2)(t - 3^3)(t - 3^4) = (t - 2)(t - 6)(t - 4)$. Note que $g(t)$ não está na forma exigida no teorema anterior e, além disso, nenhuma das raízes de $g(t)$ é um elemento primitivo em $\mathbb{F}_7$. (É fácil verificar que os únicos elementos primitivos em $\mathbb{F}_7$ são o 3 e o 5.)

O polinómio de paridade de C é $h(t) = 6 + 2t + 5t^2 + t^3$, portanto $\widehat{H}$ é uma matriz de paridade para o código extensão $\widehat{C}$, onde

$$\widehat{H} = \begin{bmatrix} 1 & 5 & 2 & 6 & 0 & 0 & 0 \\ 0 & 1 & 5 & 2 & 6 & 0 & 0 \\ 0 & 0 & 1 & 5 & 2 & 6 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} .$$

Como C é um código $[6, 3, 4]$, os parâmetros de $\widehat{C}$ são $[7, 3, \widehat{d}]$, com $4 \leq \widehat{d} \leq 5$. Denotando por c_i a i-ésima coluna de $\widehat{H}$, tem-se que $c_1 - c_3 - c_4 + c_6 = 0$, ou seja, há quatro colunas de $\widehat{H}$ linearmente dependentes, portanto $\widehat{C}$ tem distância mínima $\widehat{d} \leq 4$ (pelo Teorema 4.16) e não é um código MDS.

Exemplo 9.16. Seja C o código Reed-Solomon, sobre $\mathbb{F}_{17}$, com polinómio gerador

$$g(t) = (t - 3^2)(t - 3^3)(t - 3^4) = (t - 9)(t - 10)(t + 4) .$$

(Verifique que 3 é um elemento primitivo em $\mathbb{F}_{17}$.) Neste caso, 1 não é raiz de $g(t)$, mas uma das suas raízes, o 10, é um elemento primitivo. O polinómio de paridade de C é

$$\begin{aligned} h(t) &= \frac{t^{16} - 1}{(t - 9)(t - 10)(t + 4)} \\ &= t^{13} - 2t^{12} + 7t^{11} - 6t^{10} + 5t^9 + 2t^8 - 5t^7 + t^6 - 6t^5 - 4t^4 + 4t^3 - 2t^2 - 6t - 6 , \end{aligned}$$

e uma matriz de paridade para $\widehat{C}$ é

$$\widehat{H} = \begin{bmatrix} 1 & -2 & 7 & -6 & 5 & 2 & -5 & 1 & -6 & -4 & 4 & -2 & -6 & -6 & 0 & 0 & 0 \\ 0 & 1 & -2 & 7 & -6 & 5 & 2 & -5 & 1 & -6 & -4 & 4 & -2 & -6 & -6 & 0 & 0 \\ 0 & 0 & 1 & -2 & 7 & -6 & 5 & 2 & -5 & 1 & -6 & -4 & 4 & -2 & -6 & -6 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} .$$

Como

$$4(c_4 + c_5) + c_{11} + 8c_{16} = 4 \begin{bmatrix} -1 \\ 1 \\ 5 \\ 2 \end{bmatrix} + \begin{bmatrix} 4 \\ -4 \\ -6 \\ 1 \end{bmatrix} + \begin{bmatrix} 0 \\ 0 \\ 3 \\ 8 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} ,$$

onde c_i é a i-ésima coluna de $\widehat{H}$, conclui-se que $d(\widehat{C}) \leq 4$, donde os parâmetros de $\widehat{C}$ são $[17, 13, 4]$ (porque os de C são $[16, 13, 4]$), e $\widehat{C}$ não é MDS.

3. Concatenação de códigos Reed-Solomon

Como já se observou anteriormente, não existem códigos Reed-Solomon binários. No entanto, códigos binário são importantes do ponto de vista das aplicações. Nesta secção vamos estudar alguns códigos binários obtidos à custa de códigos Reed-Solomon. Seja então C um código Reed-Solomon de parâmetros $[2^m - 1, 2^m - \delta, \delta]$ sobre $\mathbb{F}_{2^m}$.

Caso 1: A concatenação de C com o código trivial $\mathbb{F}_2^m$ é um código binário C^* de parâmetros $[m(2^m - 1), m(2^m - \delta), d^*]$, com $d^* = \mathrm{d}(C^*) \geq \delta$, porque $\mathbb{F}_2^m$ é um código $[m, m, 1]_2$.

Caso 2: A concatenação de C com o código dos pesos pares $E_{m+1} = \{x \in \mathbb{F}_2^{m+1} : \mathrm{w}(x) \text{ é par}\}$ é um código binário C' de parâmetros $[(m+1)(2^m-1), m(2^m-\delta), d']$, com $d' = \mathrm{d}(C') \geq 2\delta$, porque E_{m+1} é um código $[m+1, m, 2]_2$.

Em ambos os casos aplicámos a Propoposição 8.63 sobre concatenação de códigos lineares.

Note que C^* e C' têm a mesma dimensão, mas $\mathrm{d}(C')$ pode ser cerca do dobro de $\mathrm{d}(C^*)$. Por isso, o código C' é mais útil para correcção de erros aleatórios, mas C^* é mais útil para correcção de erros acumulados – ver Teorema 8.66.

Recordando, da Secção 8.7, a definição de concatenação: Seja $\phi : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^m$ um isomorfismo linear sobre $\mathbb{F}_2$, então

$$C^* = \phi^*(C) = \{(\phi(c_1), \ldots, \phi(c_n)) \, : \, (c_1, \ldots, c_n) \in C\} \, .$$

Seja $\widehat{\phi} : \mathbb{F}_{2^m} \longrightarrow \mathbb{F}_2^{m+1}$ definido por $\widehat{\phi}(x) = (\phi(x), y_{m+1})$, onde $\phi(x) = (y_1, \ldots, y_m)$ e $y_{m+1} = \sum_{i=1}^m y_i$, ou seja, $y_{m+1} \in \mathbb{F}_2$ é escolhido de modo ao peso $\mathrm{w}(\widehat{\phi}(x))$ ser par. Portanto

$$\widehat{\phi} : \mathbb{F}_{2^m} \longrightarrow E_{m+1}$$

é um isomorfismo vectorial sobre $\mathbb{F}_2$, donde concluimos que o código $C' = \widehat{\phi}^*(C)$ tem distância mínima par.

Exemplo 9.17. Seja $\mathbb{F}_8 = \mathbb{F}[t]/\langle 1 + t + t^3 \rangle$ e $\alpha \in \mathbb{F}_8$ uma raiz de $1 + t + t^3$. Seja $\phi : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^3$ definido por $\phi(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2)$. Considere o código Reed-Solomon C com polinómio gerador

$$g(t) = (t-\alpha)(t-\alpha^2)\cdots(t-\alpha^6) = 1 + t + t^2 + \cdots + t^6 \, .$$

Uma base de C como espaço vectorial sobre $\mathbb{F}_2$ é

$$\{(1,1,1,1,1,1,1), (\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2)\} \, .$$

Logo, $C^* = \phi^*(C)$ é o espaço vectorial sobre $\mathbb{F}_2$ gerado por

$$\begin{aligned} \phi^*(1,1,1,1,1,1,1) &= (100, 100, \ldots, 100) \, , \\ \phi^*(\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha) &= (010, 010, \ldots, 010) \ \text{ e} \\ \phi^*(\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2) &= (001, 001, \ldots, 001) \, . \end{aligned} \tag{9.2}$$

Como C é um código $[7, 1, 7]$ sobre $\mathbb{F}_8$, os parâmetros de C^* são $[21, 3, d^*]$ com $d^* \geq 7$. Neste caso temos mesmo $d^* = 7$ – justifique! A partir de ϕ, definimos $\widehat{\phi} : \mathbb{F}_8 \longrightarrow \mathbb{F}_2^4$ por

$$\widehat{\phi}(a_0 + a_1\alpha + a_2\alpha^2) = (a_0, a_1, a_2, a_0 + a_1 + a_2) \, .$$

Portanto $C' = \widehat{\phi}^*(C)$ é gerado por

$$\begin{aligned} \widehat{\phi}^*(1,1,1,1,1,1,1) &= (1001, 1001, \ldots, 1001) \, , \\ \widehat{\phi}^*(\alpha,\alpha,\alpha,\alpha,\alpha,\alpha,\alpha) &= (0101, 0101, \ldots, 0101) \ \text{ e} \\ \widehat{\phi}^*(\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2,\alpha^2) &= (0011, 0011, \ldots, 0011) \, , \end{aligned} \tag{9.3}$$

ou seja, a cada bloco de comprimento 3 dos vectores (9.2) da base de C^* acrescentou-se um dígito de paridade, para obter os blocos de comprimento 4 dos vectores (9.3) da base de C'.

O código C^* corrige apenas erros aleatórios de peso $\leq 3 = T$ mas, pelo Teorema 8.66, corrige todos os erros acumulados de comprimento $\leq 7 = m(T-1)+1$.

Exercícios

9.1. Escreva uma matriz geradora e uma matriz de paridade para um código Reed-Solomon $[6, 4]$, e determine a distância mínima desse código.

9.2. Determine o polinómio gerador de um código Reed-Solomon, sobre $\mathbb{F}_{16}$, de dimensão 11. Escreva uma matriz de paridade para este código.

9.3. Mostre que o dual de um código Reed-Solomon é também um código Reed-Solomon.

9.4. Seja C o código Reed-Solomon sobre $\mathbb{F}_8$ com polinómio gerador $g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)$, onde $\alpha \in \mathbb{F}_8$ é uma raiz de $1+t+t^3$.
(a) Justifique que α é um elemento primitivo de $\mathbb{F}_8$.
(b) Determine os parâmetros de C.
(c) Determine os parâmetros do código dual $C^\perp$.
(d) Determine os parâmetros da extensão $\widehat{C}$.
(e) Determine os parâmetros da concatenação $C^* = \phi^*(C)$, onde $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ é a aplicação linear definida por $\phi(1) = 100$, $\phi(\alpha) = 010$ e $\phi(\alpha^2) = 101$.

9.5. Considere o código Reed-Solomon C sobre $\mathbb{F}_8$ com o seguinte polinómio gerador:

$$g(t) = (t-\alpha)(t-\alpha^2)(t-\alpha^3)(t-\alpha^4) = \alpha^3 + \alpha t + t^2 + \alpha^3 t^3 + t^4 \ ,$$

onde identificamos $\mathbb{F}_8$ com o quociente $\mathbb{F}_2[t]/\langle 1+t+t^3\rangle$, e $\alpha \in \mathbb{F}_8$ é uma raiz de $1+t+t^3$.
(a) Indique, justificando, os parâmetros $[n, k, d]$ de C.
(b) Utilize o Algoritmo Caça ao Erro para descodificar os vectores recebidos
$$y = (0, 1, 0, \alpha^2, 0, 0, 0) \quad \text{e} \quad z = (0, \alpha^3, 0, 1, \alpha^3, 1, 1).$$
(c) Seja $\phi : \mathbb{F}_8 \to \mathbb{F}_2^3$ um isomorfismo vectorial sobre $\mathbb{F}_2$. O que pode concluir sobre a capacidade de correcção de erros acumulados do código concatenação $C^* = \phi^*(C)$?

9.6. Considere o código linear sobre $\mathbb{F}_{11}$ com matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & X \end{bmatrix} \ .$$

(a) Mostre que este código é equivalente a um código cíclico C.
(b) Determine o polinómio gerador e conclua que C é um código Reed-Solomon.

9.7. (Generalização do exercício anterior.) Seja C um código $[q-1, k]$ sobre $\mathbb{F}_q$ com matriz geradora

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \alpha^{3(k-1)} & \cdots & \alpha^{(q-2)(k-1)} \end{bmatrix} \ ,$$

onde α é um elemento primitivo de $\mathbb{F}_q$ e $1 \leq k \leq q-2$.
(a) Mostre que C é um código cíclico.
(b) Determine o polinómio gerador e conclua que C é um código Reed-Solomon.

9.8. Seja $C \subset \mathbb{F}_5^4$ o código cíclico com polinómio gerador $g(t) = (t-2)(t-4)$.
(a) Justifique que C é um código Reed-Solomon e indique os seus parâmetros.
(b) Indique os parâmetros e uma matriz geradora da extensão $\widehat{C}$.
(c) Seja $\widetilde{C}$ um código cíclico de comprimento 5 e dimensão 2. Escreva uma matriz geradora para $\widetilde{C}$ e mostre que este código é linearmente equivalente a $\widehat{C}$.
(d) Conclua que qualquer código cíclico, não nulo, de comprimento 5 sobre $\mathbb{F}_5$ é MDS.

9.9. Recorde que um código linear C diz-se *auto-ortogonal* se $C \subset C^\perp$. Determine o polinómio gerador de todos os códigos Reed-Solomon, sobre $\mathbb{F}_{16}$, auto-ortogonais. Quais desses códigos são auto-duais?

APÊNDICE A

Neste apêndice pretende-se introduzir alguns tópicos de combinatória, tendo como objectivo principal deduzir uma fórmula para o número de polinómios irredutíveis de grau n com coeficientes num corpo finito[1], usando um método relativamente elementar, sem recorrer à Teoria de Galois. Em particular, esta fórmula permite concluir a existência de corpos finitos de ordem uma potência p^k de um primo p qualquer.

1. Princípio de Inclusão-Exclusão

O Princípio de Inclusão-Exclusão é uma generalização da conhecida relação

$$|A \cup B| = |A| + |B| - |A \cap B| \ ,$$

onde A e B são subconjutos de um conjunto finito S. Alternativamente, tomando complementares, podemos enunciar a igualdade anterior na forma

$$|S \setminus (A \cup B)| = |S| - |A| - |B| + |A \cap B| \ .$$

Teorema A.1. *Seja S um conjunto finito e sejam $E_1, \ldots, E_r$ subconjuntos de S. Então*

$$|S \setminus \left(\cup_{i=1}^{r} E_i \right)| = |S| - \sum_{i=1}^{r} |E_i| + \sum_{1 \leq i < j \leq r} |E_i \cap E_j| - \cdots + (-1)^r |E_1 \cap E_2 \cap \cdots \cap E_r| \ . \qquad (*)$$

Dem. Se $x \in S$ não pertence a nenhum dos conjuntos E_i, então este elemento contribui com 1 na soma da expressão $(*)$.

Se $x \in S$ pertence exactamente a k dos conjuntos E_i, com $1 \leq k \leq r$, então x contribui com

$$1 - \binom{k}{1} + \binom{k}{2} - \cdots + (-1)^k \binom{k}{k} = \sum_{i=1}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0 \ ,$$

onde se usou a fórmula do binómio de Newton na penúltima igualdade. □

Exemplo A.2. Quantos inteiros $1 \leq n \leq 100$ não são divisíveis por 2, 3 ou 5?

Seja $S = \{n \in \mathbb{N} : n \leq 100\}$ e sejam E_1, E_2 e E_3 os conjuntos formados pelos elementos de S que são divisíveis por 2, 3 e 5, respectivamente.

Os elementos de E_1 são precisamente os números pares entre 1 e 100, portanto $|E_1| = \lfloor \frac{100}{2} \rfloor = 50$. Analogamente $|E_2| = \lfloor \frac{100}{3} \rfloor = 33$ e $|E_3| = \lfloor \frac{100}{5} \rfloor = 20$. Os elementos de $E_1 \cap E_2$ são os múltiplos de

[1] Esta fórmula, no caso do corpo $\mathbb{F}_p$, p um primo, já era conhecida por Gauss.

2 e 3. Como $\mathrm{MMC}(2,3)=6$, então $|E_1\cap E_2|=\lfloor\frac{100}{6}\rfloor=16$ e

$$\begin{aligned}|E_1\cap E_3| &= \left\lfloor\frac{100}{10}\right\rfloor = 10 \quad \text{porque } \mathrm{MMC}(2,5)=10\ ,\\ |E_2\cap E_3| &= \left\lfloor\frac{100}{15}\right\rfloor = 6 \quad \text{porque } \mathrm{MMC}(3,5)=15\ ,\\ |E_1\cap E_2\cap E_3| &= \left\lfloor\frac{100}{30}\right\rfloor = 3 \quad \text{porque } \mathrm{MMC}(2,3,5)=30\ .\end{aligned}$$

Portanto o número pedido é

$$N = 100-(50+33+20)+(16+10+6)-3 = 26\ .$$

Exemplo A.3. Quantas permutações das 26 letras do alfabeto não contêm as palavras *faz*, *ver*, *sim* e *tudo*?

Neste exemplo, S é o conjunto de todas as permutações de 26 símbolos, logo $|S|=26!$. Sejam E_1, E_2, E_3 e E_4 os conjuntos formados pelas permutações das 26 letras que contêm as palavras *faz*, *ver*, *sim* e *tudo*, respectivamente. Note que estas quatro palavras não contêm letras em comum.

Os elementos de E_1 são as permutações de 24 símbolos, nomeadamente *faz* e as restantes 23 letras. Repetindo o raciocínio para os outros três conjuntos, obtém-se

$$|E_1|=|E_2|=|E_3|=24! \qquad \text{e} \qquad |E_4|=23!\ .$$

Os elementos de $E_1\cap E_2$ são as permutações de *faz*, *ver* e as restantes 20 letras, portanto $|E_1\cap E_2|=22!$. Procedendo do mesmo modo para as outras intersecções dos conjuntos E_i:

$$\begin{aligned}|E_1\cap E_2|=|E_1\cap E_3|=|E_2\cap E_3|=22! \quad \text{e} \qquad & |E_i\cap E_4|=21! \ \text{ para } i=1,2,3\ ,\\ |E_1\cap E_2\cap E_3|=20! \quad \text{e} \qquad & |E_i\cap E_j\cap E_4|=19! \ \text{ para } 1\le i<j\le 3\ ,\\ |E_1\cap E_2\cap E_3\cap E_4|=17!\end{aligned}$$

obtendo-se, finalmente, que

$$\begin{aligned}N &= 26!-(3\cdot 24!+23!)+(3\cdot 22!+3\cdot 21!)-(20!+3\cdot 19!)+17!\\ &= 3160461970\cdot 19! = 38445471367894498811904000 \sim 3{,}8\times 10^{24}\end{aligned}$$

é o número de permutações pedido.

Exemplo A.4. Se X e Y são conjuntos finitos, quantas funções sobrejectivas $f: X\longrightarrow Y$ existem? Seja $X=\{x_1,\ldots,x_n\}$ e $Y=\{y_1,y_2,\ldots,y_m\}$, com $|X|=n$ e $|Y|=m$. Seja S o conjunto de todas as funções de X em Y (sobrejectivas ou não) e defina-se $E_i=\{f: X\longrightarrow Y \mid y_i\notin f(X)\}$.

Portanto

$$\begin{aligned}|S| &= m^n && m \text{ escolhas para cada } f(x_i)\in Y\ ,\\ |E_i| &= (m-1)^n && m-1 \text{ escolhas para cada } f(x_k)\in Y\setminus\{y_i\}\ ,\\ |E_i\cap E_j| &= (m-2)^n && m-2 \text{ escolhas para cada } f(x_k)\in Y\setminus\{y_i,y_j\} \text{ com } i\neq j\ ,\\ &\vdots\\ |E_{i_1}\cap\cdots E_{i_j}| &= (m-j)^n && m-j \text{ escolhas para cada } f(x_k)\in X\setminus\{y_{i_1},\ldots,y_{i_j}\}\ .\end{aligned}$$

Como há $\binom{m}{j}$ interseccções $E_{i_1}\cap\cdots\cap E_{i_j}$, conclui-se que o número de funções sobrejectivas de X em Y é

$$\sum_{j=0}^{m}(-1)^j\binom{m}{j}(m-j)^n\ .$$

Em particular, provou-se que

$$\sum_{j=0}^{m}(-1)^j\binom{m}{j}(m-j)^n=\begin{cases}0 & \text{se } m>n\\ n! & \text{se } m=n\end{cases}\ ,$$

pois não há funções sobrejectivas se $|Y| > |X|$ e, se $|X| = |Y| = n$, então f é sobrejectiva se e só se é bijectiva, ou seja, f é uma permutação de n elementos.

1.1. Funções de Euler e de Möbius

Recorde que a função de Euler, definida para número inteiro positivo $n \in \mathbb{N}$, é o número de inteiros $1 \leq k \leq n$ tais que $\mathrm{MDC}(k, n) = 1$, ou seja, $\phi(n) = |\mathbb{Z}_n^\times|$.

Proposição A.5. *A função de Euler satisfaz as seguintes propriedades:*

(i) Se p é um número primo, então $\phi(p) = p - 1$ e $\phi(p^k) = p^k - p^{k-1}$.

(ii) Se $n = ab$ com $\mathrm{MDC}(a, b) = 1$, então $\phi(n) = \phi(a)\phi(b)$.

Esta proposição, assim como a existência e unicidade de factorização de $n \in \mathbb{N}$ em potências de primos, é consequência do Lema de Euclides no anel dos inteiros $\mathbb{Z}$.

A partir da factorização em potências de primos, e usando a proposição anterior, deduz-se facilmente uma fórmula para $\phi(n)$. Alternativamente, podemos usar o Princípio de Inclusão-Exclusão para obter a mesma fórmula, como se faz no seguinte exemplo.

Exemplo A.6. Se $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, com $p_1, \ldots, p_r$ primos distintos e $e_i \geq 1$, é a factorização de $n \in \mathbb{N}$ em primos, seja $S = \{1, \ldots, n\}$ e seja $E_i = \{x \in S : p_i | x\}$, com $1 \leq i \leq r$. Como $|E_i| = n/p_i$, $|E_i \cap E_j| = n/(p_i p_j)$, etc., o Princípio de Inclusão-Exclusão aplicado a este caso fica:

$$\phi(n) = n - \sum_{i=1}^{r} \frac{n}{p_i} + \sum_{1 \leq i < j \leq r} \frac{n}{p_i p_j} + \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) . \tag{A.1}$$

Teorema A.7. *Para todo o $n \in \mathbb{N}$,*

$$\sum_{d|n} \phi(d) = n \ .$$

Dem. Seja $S = \{1, 2, \ldots, n\}$. Vamos caracterizar os elementos de S usando a função ϕ.

Para qualquer $m \in S$, tem-se que $\mathrm{MDC}(m, n) | n$. A condição $\mathrm{MDC}(m, n) = d$ é equivamente a $m = m_1 d$, $n = n_1 d$ e $\mathrm{MDC}(n_1, m_1) = 1$. Portanto, o número de elementos $m \in S$ tais que $\mathrm{MDC}(m, n) = d$ é exactamente $\phi(n_1) = \phi(\frac{n}{d})$ (contam-se os m_1 tais que $\mathrm{MDC}(m_1, n_1) = 1$), donde

$$n = \sum_{d|n} \phi(\frac{n}{d}) = \sum_{d|n} \phi(d) \ . \qquad \square$$

Outra função relacionada com divisores de n é a função de Möbius.

Definição A.8. A função de Möbius é definida por

$$\mu(n) = \begin{cases} 1 & \text{se } n \text{ é o produto de um número par de primos distintos ou } n = 1, \\ -1 & \text{se } n \text{ é o produto de um número ímpar de primos distintos,} \\ 0 & \text{caso contrário.} \end{cases}$$

O último caso na definição de μ verifica-se precisamente quando n é divisível por um quadrado de um número primo.

Por exemplo, como $10 = 2 \times 5$, $12 = 2^2 \times 3$ e $70 = 2 \times 5 \times 7$, então $\mu(10) = 1$, $\mu(12) = 0$ e $\mu(70) = -1$. No caso geral, considerando novamente a factorização $n = p_1^{e_1} \cdots p_r^{e_r}$ em primos, com $e_i \geq 1$. Se $e_i = 1$, para todo o i, então $\mu(n) = (-1)^r$, e $\mu(n) = 0$ se existe algum $e_i > 1$. Em particular $\mu(1) = 1$ – é o caso com $r = 0$.

Teorema A.9. *Temos*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \textit{se } n = 1, \\ 0 & \textit{caso contrário.} \end{cases}$$

Dem. Se $n = 1$, como $\mu(1) = 1$, não há nada a provar. Caso contrário, $n = p_1^{e_1} \cdots p_r^{e_r}$ com $r \geq 1$, p_i primos distintos e $e_i \geq 1$. Qualquer divisor (positivo) de n é da forma $d = p_1^{f_1} \cdots p_r^{f_r}$, onde $0 \leq f_i \leq e_i$. Se existe algum $f_i \geq 2$, então $\mu(d) = 0$; caso contrário $f_i \leq 1$ para todo o i, e $\mu(d) = (-1)^j$, onde j é o número de expoentes $f_i = 1$ e há precisamente $\binom{r}{j}$ divisores d nestas condições. Portanto

$$\sum_{d|n} \mu(d) = \sum_{j=0}^{r} \binom{r}{j} (-1)^j = (1-1)^r = 0 \ . \qquad \square$$

As funções ϕ e μ satisfazem a seguinte curiosa relação

$$\frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d} \ , \tag{A.2}$$

que pode ser verificada retomando a primeira igualdade em (A.1): como $\mu(p_i) = -1$, $\mu(p_i p_j) = 1$, etc. (por definção de μ), então

$$\begin{aligned} \frac{\phi(n)}{n} &= 1 - \sum_{i=1}^{r} \frac{1}{p_i} + \sum_{1 \leq i < j \leq n} \frac{1}{p_i p_j} + \cdots + (-1)^r \frac{1}{p_1 \cdots p_r} \\ &= \mu(1) + \sum_{i=1}^{r} \frac{\mu(p_i)}{p_i} + \sum_{1 \leq i < j \leq n} \frac{\mu(p_i p_j)}{p_i p_j} + \cdots + \frac{\mu(p_1 \cdots p_r)}{p_1 \cdots p_r} = \sum_{d|n} \frac{\mu(d)}{d} \ , \end{aligned}$$

pois $\mu(d) = 0$ se algum $p_i^2 | n$.

Teorema A.10 (Fórmula de Inversão de Möbius)**.** *Se f e g são funções definidas em $\mathbb{N}$ tais que*

$$f(n) = \sum_{d|n} g(d) \ , \qquad \textit{então} \qquad g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) \ .$$

Dem.

$$\begin{aligned} \sum_{d|n} \mu(d) f(\frac{n}{d}) &= \sum_{d|n} \mu(\frac{n}{d}) f(d) && \text{permutando } d \text{ e } n/d \\ &= \sum_{d|n} \mu(\frac{n}{d}) \Big(\sum_{d'|d} g(d') \Big) && \text{pela hipótese em } f \\ &= \sum_{d'|n} g(d') \Big(\sum_{m|\frac{n}{d'}} \mu(m) \Big) && \text{trocando a ordem dos sumatórios.} \qquad (*) \end{aligned}$$

Neste último passo, note que d' percorre todos os divisores de n pois d também o faz – isto justifica o sumatório "exterior". Quanto ao somatório "interior", basta ver qual é a relação entre $m = n/d$ e d':

$$d'|d \quad \Longleftrightarrow \quad d'|\frac{n}{m} \quad \Longleftrightarrow \quad m|\frac{n}{d'} \ .$$

Pelo Teorema A.9, a única contribuição não-nula do somatório interior em $(*)$ vale 1 e ocorre quando $n/d' = 1$, obtendo-se

$$\sum_{d'|n} g(d') \Big(\sum_{m|\frac{n}{d'}} \mu(m) \Big) = g(n) \ . \qquad \square$$

A igualdade (A.2) é um caso particular da Fórmula de Inversão de Möbius aplicada a $n = \sum_{d|n} \phi(d)$, pondo $f(n) = n$ e $g(n) = \phi(n)$.

2. Funções geradoras e relações de recorrência

Dada uma sucessão $\{a_n\}$ de números inteiros (ou reais), podemos representá-la através de uma série de potências formal

$$f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Z}[[x]] \quad (\text{ou } \mathbb{R}[[x]]) \ ,$$

e dizemos que $f(x)$ é a *função geradora* da sucessão $\{a_n\}$.

As funções geradoras são bastante úteis para resolver relações de recorrência, e são muito usadas em problemas de contagem. Também podem ser usadas indirectamente para deduzir desenvolvimentos de certas funções em séries de potências.

Exemplo A.11. O já conhecido desenvolvimento

$$(1+x)^m = \sum_{n=0}^{m} \binom{m}{n} x^n$$

indica-nos que $(1+x)^m$ é a função geradora da sucessão $a_n = \binom{m}{n}$. Por convenção $\binom{m}{n} = 0$ sempre que $n > m$.

Exemplo A.12. A factorização em $\mathbb{Z}[[x]]$

$$1 = (1-x)(1+x+x^2+x^3+\cdots) = (1-x)\sum_{n=0}^{\infty} x^n$$

implica que a função geradora da sucessão constante $a_n = 1$ é $f(x) = \dfrac{1}{1-x}$.

Usando derivadas (formais) podemos facilmente obter funções geradoras de outras sucessões.

Por exemplo

$$\frac{1}{(1-x)^2} = \left(\frac{1}{1-x}\right)' = 1 + 2x + 3x^2 + \cdots = \sum_{n=0}^{\infty} (n+1)x^n \tag{A.3}$$

portanto $f(x) = \dfrac{1}{(1-x)^2}$ é a função geradora da sucessão $a_n = n+1$ e, multiplicando (A.3) por x, obtém-se a função geradora da sucessão $a_n = n$, i.e.,

$$\frac{x}{(1-x)^2} = 0 + 1x + 2x^2 + 3x^3 + \cdots = \sum_{n=0}^{\infty} nx^n \ . \tag{A.4}$$

Usando indução matemática (Exercício A.12), prova-se que

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{k-1+n}{n} x^n \ . \tag{A.5}$$

Exemplo A.13. Considere o seguinte problema: de quantas maneiras podemos colocar n bolas em k caixas? Temos que separar n objectos idênticos em k grupos, portanto o problema é equivalente a colocar $k-1$ "separadores" entre as n bolas, como se ilustra na figura:

$$\underbrace{\bigcirc\cdots\bigcirc}_{1^{\text{a}}\text{ caixa}} \mid \underbrace{\bigcirc\cdots\bigcirc}_{2^{\text{a}}\text{ caixa}} \mid \cdots \mid \underbrace{\bigcirc\,\bigcirc\cdots\bigcirc}_{k^{\text{a}}\text{ caixa}}$$

Portanto há um total de $n + (k-1)$ posições das quais temos de escolher $k-1$ para colocar os separadores (ou escolher n para as bolas), e a resposta é $\binom{n+k-1}{k-1} = \binom{n+k-1}{n}$.

Daqui se conclui que a função geradora da sucessão a_n (= resposta do problema para n bolas, considerando o número de caixas $k \in \mathbb{N}$ fixo) é

$$f(x) = \sum_{n=0}^{\infty} \binom{n+k-1}{k-1} x^n \ . \tag{A.6}$$

Por outro lado, a função geradora também é dada pelo produto de k termos

$$f(x) = (1 + x + x^2 + \cdots)(1 + x + x^2 + \cdots) \cdots (1 + x + x^2 + \cdots) \tag{A.7}$$

onde cada um dos termos está associado a uma das caixa. Mais precisamente, a configuração com n_1 bolas na primeira caixa, n_2 bolas na segunda, etc, corresponde ao produto de x^{n_1} no primeiro termo, com x^{n_2} no segundo, etc. Portanto o número de configurações para n bolas em k caixas é o termo de grau $n = n_1 + n_2 + \cdots + n_k$ na expressão (A.7). Usando agora o desenvolvimento de $\frac{1}{1-x}$ do Exemplo A.12, (A.7) escreve-se

$$f(x) = \Big(\frac{1}{1-x}\Big)^k$$

e, comparando com a expressão (A.6), obtém-se novamente a igualdade (A.5).

Exemplo A.14. Quatro amigos têm 24 pastilhas. De quantas maneiras as podem partilhar se cada um ficar com pelo menos 3 pastilhas, mas nenhum com mais do que 8?

O polinómio (série) para cada um dos amigos é $x^3 + x^4 + \cdots + x^8$, portanto a função geradora associada ao problema é

$$f(x) = (x^3 + x^4 + \cdots + x^8)^4$$

e a resposta é o coeficiente do termo de grau 24. Como

$$\begin{aligned} f(x) = (x^3)^4(1 + x + x^2 + \cdots + x^5)^4 &= x^{12}\Big(\sum_{n=0}^{\infty} x^n - \sum_{n=6}^{\infty} x^n\Big)^4 \\ &= x^{12}\left(\frac{1-x^6}{1-x}\right)^4 , \end{aligned}$$

temos de determinar o coeficiente do termo de grau 12 em $\dfrac{(1-x^6)^4}{(1-x)^4}$. Como

$$(1-x^6)^4 \cdot \frac{1}{(1-x)^4} = \left(1 - \binom{4}{1}x^6 + \binom{4}{2}x^{12} - \binom{4}{3}x^{18} + x^{24}\right)\sum_{n=0}^{\infty}\binom{n+3}{n}x^n ,$$

a resposta pedida é

$$\binom{15}{12} - \binom{4}{1}\binom{9}{6} + \binom{4}{2}\binom{3}{0} = 125 .$$

2.1. Relações de recorrência

A relação de recorrência

$$\begin{cases} a_0 = 3 \\ a_n = 2a_{n-1} \quad n \geq 1 \end{cases}$$

define a progressão geométrica de razão $a_n/a_{n-1} = 2$ e termo inicial $a_0 = 3$, portanto o seu termo geral é $a_n = 3 \cdot 2^n$, $n \geq 0$, como facilmente se prova por indução. Se for

$$\begin{cases} a_0 = 3 \\ a_n = 2 + a_{n-1} \quad n \geq 1 \end{cases} ,$$

então a solução é a progressão aritmética $a_n = 3 + 2n$, $n \geq 0$. Noutros casos poderá não ser tão fácil adivinhar a resposta e um método possível para obter o termo geral duma sucessão definida por recorrência é usar a função geradora associada.

Exemplo A.15. Determine o termo geral da sucessão

$$a_n - 2a_{n-1} = n \qquad (n \geq 1)$$

dado que $a_0 = 1$.

Seja $f(x) = \sum_{n=0}^{\infty} a_n x^n$ a função geradora. Multiplicando a igualdade acima por x^n, e usando a definição de $f(x)$, obtém sucessivamente

$$\begin{aligned} & a_n x^n - 2a_{n-1}x^n = nx^n \qquad \forall\, n \geq 1 \\ \iff & \sum_{n=1}^{\infty} a_n x^n - \sum_{n=1}^{\infty} 2a_{n-1}x^n = \sum_{n=1}^{\infty} nx^n \\ \iff & (f(x) - a_0) - 2xf(x) = \sum_{n=0}^{\infty} nx^n \end{aligned}$$

De (A.4), temos que $\dfrac{x}{(1-x)^2}$ é a função geradora da sucessão $0, 1, 2, 3, \ldots$. Portanto

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

e resolvendo em ordem a $f(x)$ fica

$$f(x) = \frac{1}{1-2x} + \frac{x}{(1-2x)(1-x)^2} \ .$$

Agora precisamos de determinar o coeficiente do termo de grau n do desenvolvimento desta função em série de potências. Usando o método das fracções simples:

$$\frac{x}{(1-2x)(1-x)^2} = \frac{A}{1-2x} + \frac{B}{1-x} + \frac{Cx}{(1-x)^2}$$

com A, B e C constantes. A solução é $A = 2$, $B = -2$ e $C = -1$, logo

$$\begin{aligned} f(x) &= \frac{3}{1-2x} - \frac{2}{1-x} - \frac{x}{(1-x)^2} = 3\sum_{n=0}^{\infty} 2^n x^n - 2\sum_{n=0}^{\infty} x^n - \sum_{n=0}^{\infty} nx^n \\ &= \sum_{n=0}^{\infty} (3 \cdot 2^n - 2 - n)x^n \ , \end{aligned}$$

donde se conclui que $a_n = 3 \cdot 2^n - 2 - n$, para $n \geq 0$.

2.2. Polinómios irredutíveis

Terminamos esta secção contando o número de polinómios mónicos irredutíveis de grau n em $\mathbb{F}_q[t]$, onde $\mathbb{F}_q$ é um corpo contendo $q \geq 2$ elementos.

Seja $\{f_1, f_2, f_3, \ldots\}$ uma sucessão com todos os polinómios mónicos irredutíveis em $\mathbb{F}_q[t]$ de graus $d_1, d_2, d_3, \ldots$, respectivamente, com $d_k \geq 1$ para todo o $k \in \mathbb{N}$. Seja $I(q, n)$ o número de polinómios mónicos irredutíveis de grau n em $\mathbb{F}_q[t]$, portanto $I(q, n) = \#\{i : d_i = n\}$.

Para qualquer sucessão $\{i_1, i_2, \ldots\} \subset \mathbb{N}_0$, com apenas um número finito de termos não nulos,

$$f = f_1^{i_1} f_2^{i_2} \cdots$$

é um produto finito e é um polinómio de grau $n = i_1 d_1 + i_2 d_2 + \cdots$. Por unicidade de factorização em $\mathbb{F}_q[t]$ (pois $\mathbb{F}_q$ é um corpo), qualquer polinómio mónico é desta forma e a sucessões diferentes de expoentes $\{i_1, i_2, \ldots\}$ correspondem polinómios diferentes. Ou seja, a seguinte correspondência

$$\left\{ \begin{array}{c} \text{polinómios} \\ \text{mónicos} \\ \text{de grau } n \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{sucessões } \{i_k\} \subset \mathbb{N}_0 \text{ com um} \\ \text{número finito de termos não nulos} \\ \text{tais que } n = i_1 d_1 + i_2 d_2 + \cdots \end{array} \right\}$$

é bijectiva e estes dois conjuntos têm o mesmo número de elementos.

Como o conjunto da esquerda tem q^n elementos, a função geradora para o número de polinómios mónicos é

$$1 + qx + q^2x^2 + \cdots + q^n x^n + \cdots = \sum_{n=0}^{\infty} (qx)^n = \frac{1}{1-qx} \ .$$

Por outro lado, o número de sucessões $\{i_k\}$ tais que $n = i_1d_1 + i_2d_2 + \cdots$ é o coeficiente de x^n na série de potência dada por

$$(1 + x^{d_1} + x^{2d_1} + \cdots)(1 + x^{d_2} + x^{2d_2} + \cdots)\cdots = \frac{1}{1 - x^{d_1}}\frac{1}{1 - x^{d_2}}\cdots = \prod_{i=1}^{\infty}\frac{1}{1 - x^{d_i}} \ .$$

Portanto

$$\frac{1}{1 - qx} = \prod_{i=1}^{\infty}\frac{1}{1 - x^{d_i}} = \prod_{d=1}^{\infty}\Big(\frac{1}{1 - x^d}\Big)^{I(q,d)} \ . \tag{A.8}$$

No último passo agruparam-se os termos com o mesmo expoente d_i em x (recorde que $I(q, d) = \#\{i : d_i = d\}$). Uma vez que (pelo Exercício A.17)

$$\log\Big(\frac{1}{1 - x}\Big) = x + \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 + \cdots = \sum_{n=1}^{\infty}\frac{x^n}{n} \ ,$$

aplicando o logaritmo em (A.8) fica

$$\sum_{n=1}^{\infty}\frac{(qx)^n}{n} = \sum_{d=1}^{\infty} I(q, d)\Big(\sum_{j=1}^{\infty}\frac{(x^d)^j}{j}\Big) \ .$$

Igualando os coeficientes do termo de grau n e pondo $j = n/d$, obtém-se

$$\frac{q^n}{n} = \sum_{d|n}\frac{d}{n}I(q, d) \ ,$$

que simplificando dá

$$q^n = \sum_{d|n} dI(q, d) \ .$$

Aplicando a fórmula de inversão de Möbius (Teorema A.10) a esta última igualdade, termina-se a demonstração do seguinte teorema.

Teorema A.16. *O número de polinómios mónicos de grau n irredutíveis em* $\mathbb{F}_q[t]$ *é*

$$I(q, n) = \frac{1}{n}\sum_{d|n}\mu\big(\frac{n}{d}\big)q^d \ . \tag{A.9}$$

Exercícios

A.1. Demonstre o Princípio de Inclusão-Exclusão usando indução matemática no número de conjuntos excluídos E_i, $1 \le i \le r$.

A.2. Quantos números inteiros entre 1 e 1000 não são divisíveis por 2,3 ou 5, mas são divisíveis por 7?

A.3. Quantas permutações de $\{a, b, c, \ldots, x, y, z\}$ não contêm as palavras *sim*, *riso*, *mal* e *cabe*?

A.4. Qual o número de soluções inteiras de $x_1 + x_2 + x_3 + x_4 = 21$ tais que
(a) $x_i \ge 0$, para $i = 1, 2, 3, 4$;
(b) $0 \le x_i \le 8$, para $i = 1, 2, 3, 4$;
(c) $0 \le x_1 \le 5$, $0 \le x_2 \le 6$, $3 \le x_3 \le 8$, $4 \le x_4 \le 9$.

A.5. Determine o número de polinómios mónicos de grau n em $\mathbb{F}_q[t]$ sem raízes em $\mathbb{F}_q$, onde $\mathbb{F}_q$ é um corpo com q elementos.

A.6. (a) Quantos inteiros n entre 1 e 15000 satisfazem $\mathrm{MDC}(n, 15000) = 1$?
(b) Quantos inteiros n entre 1 e 15000 têm pelo menos um divisor primo em comum com 15000?

A.7. Calcule $\phi(n)$ e $\mu(n)$ para: (i) 51, (ii) 82, (iii) 200, (iv) 420 e (v) 21000.

A.8. Determine todos os inteiros positivos $n \in \mathbb{N}$ tais que

(a) $\phi(n)$ é ímpar;
(b) $\phi(n)$ é uma potência de 2;
(c) $\phi(n)$ é um múltiplo de 4.

A.9. Mostre que $\phi(n^m) = n^{m-1}\phi(n)$, para $n, m \in \mathbb{N}$.

A.10. Demonstre a Proposição A.5 e use-a para deduzir a igualdade (A.1).

A.11. Determine a série de potência para $\dfrac{1}{1-ax}$, $a \neq 0$, ou seja, calcule o inverso de $1-ax$ no anel $\mathbb{Z}[[x]]$ (ou $\mathbb{R}[[x]]$).

A.12. Use derivadas formais e indução matemática para provar que

$$\frac{1}{(1-x)^k} = \sum_{n=0}^{\infty} \binom{k-1+n}{n} x^n \ , \qquad \text{para } k \in \mathbb{N} \ .$$

A.13. Um dado é lançado 12 vezes. Qual a probabilidade da soma das faces ser 30?

A.14. O Zé vai comprar n berlindes azuis, vermelhos ou brancos (a loja possui uma grande quantidade em cada uma destas cores). De quantas maneiras pode o Zé escolher os n berlindes de modo a comprar um número par de azuis?

A.15. A Ana, o Bernardo, a Carla e o David organizaram um churrasco e compraram 12 febras e 16 sardinhas. De quantas maneiras podem dividir as febras e as sardinhas entre eles se:
(a) Cada um deles fica com pelo menos uma febra e duas sardinhas.
(b) O Bernardo fica com pelo menos uma febra e três sardinhas, e cada um dos outros fica com pelo menos duas febras mas não mais do que cinco sardinhas.

A.16. Seja $f_0(x)$ a função geradora da sucessão $1, 1, 1, \ldots$ e, para $k \geq 1$, seja $f_k(x)$ a função geradora da sucessão $0^k, 1^k, 2^k, 3^k, \ldots$. Já se mostrou que $f_0(x) = \frac{1}{1-x}$. Prove agora que

$$f_k(x) = x\big(f_{k-1}(x)\big)' \qquad \text{para } k \geq 1 \ .$$

Escreva explicitamente as funções f_1, f_2 e f_3.

A.17. Verifique que $\log\left(\dfrac{1}{1-x}\right) = \displaystyle\sum_{n=1}^{\infty} \frac{x^n}{n}$.

A.18. Usando funções geradoras, resolva a seguinte relação de recorrência: $a_n = 2a_{n-2}$, se $n \geq 2$, e $a_0 = 1$, $a_1 = 2$.

A.19. Através de funções geradoras, determine o termo geral da sucessão de Fibonacci

$$\begin{cases} a_0 = a_1 = 1 \\ a_n = a_{n-1} + a_{n-2} \quad n \geq 2 \end{cases} .$$

A.20. Seja d_n o determinante da seguinte matriz $n \times n$ ($n \geq 1$)

$$A_n = \begin{bmatrix} 2 & -1 & 0 & 0 & \cdots & 0 & 0 \\ -1 & 2 & -1 & 0 & & & 0 \\ 0 & -1 & 2 & \ddots & \ddots & & \vdots \\ 0 & 0 & \ddots & \ddots & \ddots & 0 & 0 \\ \vdots & & \ddots & \ddots & 2 & -1 & 0 \\ 0 & & & 0 & -1 & 2 & -1 \\ 0 & 0 & \cdots & 0 & 0 & -1 & 2 \end{bmatrix} .$$

Encontre uma relação de recorrência para d_n e resolva-a.

A.21. Repita o exercício anterior para a matriz que se obtém de A_n
(a) subtituíndo 2 por 3, e -1 por $\sqrt{2}$;
(b) subtituíndo 2 por 0 e mantendo as entradas -1.

A.22. Encontre uma relação de recorrência para $s_n = \sum_{i=0}^{n} i^2$ e resolva-a.

A.23. Uma *relação de recorrência linear homogénea de ordem k com coeficientes constantes* é uma relação da forma

$$c_0 a_n + c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} = 0 \quad (n \geq k) \ ,$$

onde $c_0, c_1, \ldots, c_k \in \mathbb{R}$ são constantes, $c_0 \neq 0$. Define-se o *polinómio característico* da relação homogénea por

$$p(x) = c_0 x^k + c_1 x^{k-1} + \cdots + c_{k-1} x + c_k \ \in \mathbb{R}[x],$$

e as suas raízes dizem-se *raízes características*. Assuma que $c_k \neq 0$, i.e., 0 não é uma raiz característica.

(a) Mostre que a solução geral da relação homogénea de primeira ordem é $a_n = a_0 r^n$, $n \geq 0$, onde $r = -\frac{c_1}{c_0}$, i.e., r é a raiz do polinómio característico associado.

(b) Estude o caso quadrático (segunda ordem) homogéneo provando as seguintes afirmações:

(i) Se as raízes características r_1 e r_2 são reais e distintas, então a solução geral é dada por

$$a_n = A(r_1)^n + B(r_2)^n \ ,$$

onde $A, B \in \mathbb{R}$ são constantes, i.e., $(r_1)^n$ e $(r_2)^n$ são duas soluções linearmente independentes.

(ii) Se há apenas uma raiz característica $r \in \mathbb{R}$ (de multiplicidade 2), então a solução geral é dada por

$$a_n = Ar^n + Bnr^n \ ,$$

onde $A, B \in \mathbb{R}$ são constantes.

(iii) Se há duas raízes complexas $r_1, r_2 \in \mathbb{C}$, então r_1 e r_2 são números conjugados e a solução geral é dada por

$$a_n = A(r_1)^n + B(r_2)^n \ ,$$

onde $A, B \in \mathbb{C}$ são constantes (tal como no caso real). Mostre ainda que, se $a_0, a_1 \in \mathbb{R}$, então A e B são números complexos conjugados e $a_n \in \mathbb{R}$, para todo o $n \geq 0$.
Sugestão: recorde que qualquer $z \in \mathbb{C} \setminus \{0\}$ se pode escrever na forma $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$ e que $(\cos(\theta) + i\,\mathrm{sen}(\theta))^n = \cos(n\theta) + i\,\mathrm{sen}(n\theta)$.

(c) Generalize a alínea anterior para relações de ordem k:

(i) Mostre que, se $r \in \mathbb{R}$ é uma raiz característica de multiplicidade m, então a parte da solução geral relativa a r é dada por

$$a_n^{(r)} = A_0 r^n + A_1 n r^n + A_2 n^2 r^n + \cdots + A_{m-1} n^{m-1} r^n \ ,$$

onde $A_0, A_1, \ldots, A_{m-1} \in \mathbb{R}$ são constantes.

(ii) Se $r \in \mathbb{C}$ é uma raiz característica complexa de multiplicidade m, qual a forma da parte da solução geral relativa a r e ao seu conjugado $\bar{r}$?

A.24. Use os resultados do exercício anterior para resolver as seguintes relações de recorrência:

(a) $a_n = 2a_{n-1} + 3a_{n-2}$, $n \geq 2$, e $a_0 = 3$, $a_1 = 5$;

(b) $4a_n - 4a_{n-1} + a_{n-2} = 0$, $n \geq 2$, e $a_0 = 5$, $a_1 = 4$;

(c) $a_n - 2a_{n-1} + 2a_{n-2} = 0$, $n \geq 2$, e $a_0 = a_1 = 4$;

(d) $a_n = a_{n-1} + 5a_{n-2} + 3a_{n-3}$, $n \geq 3$, e $a_0 = a_1 = 3$, $a_2 = 7$.

A.25. Mostre que a expressão (A.9) que se obteve para $I(q, n)$ é sempre positiva, ou seja, mostre que para $q \geq 2$ e $n \geq 1$, se tem

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) q^d > 0 \ .$$

(Não necessário a existência de um corpo de q elementos.)

APÊNDICE B

Neste apêndice vamos deduzir algumas propriedades sobre polinómios com coeficientes em corpos finitos e, portanto, assumimos os resultados do Capítulo 3.

1. Polinómios mínimos

Recorde que o corpo finito $\mathbb{F}_q$ é subcorpo de $\mathbb{F}_{q^m}$, portanto o anel dos polinómio $\mathbb{F}_q[t]$ é um subanel de $\mathbb{F}_{q^m}[t]$.

Definição B.1. Um *polinómio mínimo* de $a \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$ é um polinómio mónico $f(t) \in \mathbb{F}_q[t]$ de grau mínimo tal que $f(a) = 0$.

Note que um polinómio mónico é necessarimante não-nulo. Além disso, $f(a) = 0$ implica que $t - a \mid f(t)$ em $\mathbb{F}_{q^m}[t]$ logo, não só um polinómio mínimo é não-nulo, como tem pelo menos grau 1.

Exemplo B.2.
- Se $a \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$, então $t - a \in \mathbb{F}[t]$ é um polinómio mínimo de a sobre $\mathbb{F}_q$.
- Seja $\mathbb{F}_4 = \mathbb{F}_2[\alpha]$, onde $\alpha^2 = \alpha + 1$. Como t e $t + 1$ são os únicos polinómio de grau 1 em $\mathbb{F}_2[t]$ e não se anulam em α, um polinómio mínimo de α tem pelo menos grau 2. Como $t^2+t+1 \in \mathbb{F}_2[t]$ se anula em α, podemos então concluir que $t^2 + t + 1$ é um polinómio mínimo de α sobre $\mathbb{F}_2$.

Teorema B.3. *(a) Para cada $a \in \mathbb{F}_{q^m}$ existe um único polimómio mínimo $f(t)$ sobre $\mathbb{F}_q$. Além disso, o polinómio mínimo é irredutível em $\mathbb{F}_q[t]$.*

(b) Se $f(t) \in \mathbb{F}_q[t]$ é mónico, irredutível e $f(a) = 0$, com $a \in \mathbb{F}_{q^m}$, então $f(t)$ é o polinómio mínimo de a sobre $\mathbb{F}_q$.

Dem. (a) Existência: Pela Proposição 3.15 (i), a é raiz do polinómio $t^{q^m} - t$, portanto o conjunto

$$\{f(t) \in \mathbb{F}_q[t] \setminus \{0\} \mid f(a) = 0\,,\, \text{grau}(f(t)) \leq q^m\}$$

é não vazio e finito, porque $\mathbb{F}_q$ é finito, portanto existe polinómio mínimo para a.

Unicidade: Sejam $f_1(t)$ e $f_2(t)$ polinómios mínimos de a sobre $\mathbb{F}_q$. Pelo algoritmo de divisão em $\mathbb{F}_q[t]$, temos que

$$f_1(t) = f_2(t)q(t) + r(t)\ , \quad \text{com } q(t), r(t) \in \mathbb{F}_q[t] \text{ e } \text{grau}(r(t)) < \text{grau}(f_2(t))\ .$$

Logo $f_1(a) = f_2(a)q(a) + r(a)$ e $r(a) = 0$, pois $f_1(a) = f_2(a) = 0$. Como o grau de $f_2(t)$ é mínimo entre os polinómio não-nulos que se anulam em a, temos que o resto $r(t)$ tem de ser o polinómio nulo, logo $f_2 \mid f_1$. Analogamente, trocando f_1 e f_2 no argumento anterior, também temos que $f_1 \mid f_2$, donde se conclui que $f_1 = f_2$, pois ambos são mónicos.

Irreducibilidade: Seja $f(t)$ o polinómio mínimo de a sobre $\mathbb{F}_q$. Suponhamos que $f(t)$ não é irredutível, i.e., que existem $g(t)$ e $h(t)$ mónicos com graus estritamente menores que grau$(f(t))$ tais que $f(t) = g(t)h(t)$. Portanto $g(a)h(a) = f(a) = 0$, donde $g(a) = 0$ ou $h(a) = 0$, o que contradiz $f(t)$ ter grau mínimo.

(b) Seja $g(t)$ o polinómio mínimo de a sobre $\mathbb{F}_q$. Pelo algoritmo de divisão em $\mathbb{F}_q[t]$, temos que $f(t) = g(t)q(t) + r(t)$, com $q(t), r(t) \in \mathbb{F}_q[t]$ e $\text{grau}(r(t)) < \text{grau}(g(t))$. Calculando em a, obtemos $r(a) = 0$, pois $f(a) = g(a) = 0$, donde o resto $r(t)$ é o polinómio nulo, por minimalidade no grau de $g(t)$ e, portanto, $g(t)$ divide $f(t)$. Como $f(t)$ é irredutível e mónico, temos necessariamente que $f(t) = g(t)$. □

Como consequência deste teorema, se $f(t)$ é mónico e irredutível em $\mathbb{F}_q[t]$, e se $\alpha \in \mathbb{F}_q[t]/\langle f(t)\rangle = \mathbb{F}_{q^m}$, onde $m = \text{grau}(f(t))$, é uma raiz de f, então $f(t)$ é o polinómio mínimo de α sobre $\mathbb{F}_q$.

Exemplo B.4. O polinómio $f(t) = t^3 + 2t + 1$ é irredutível em $\mathbb{F}_3[t]$ porque tem grau 3 e não tem raízes em $\mathbb{F}_3$. Seja $\mathbb{F}_{27} = \mathbb{F}_3[\alpha]$, onde $\alpha^3 = \alpha + 2$, ou seja, $\alpha \in \mathbb{F}_{27}$ é uma raiz de $f(t)$. Portanto $f(t)$ é o polinómio mínimo de α sobre $\mathbb{F}_3$.

De seguida determinamos os polinómios mínimos, sobre $\mathbb{F}_q$, dos elementos em $\mathbb{F}_{q^m}$.

Definição B.5. Se $\text{MDC}(n, q) = 1$, definimos a *classe ciclotómica-q* de i módulo n por

$$C_i := \{iq^k \mod n \mid k \in \mathbb{N}_0\} \subset \mathbb{Z}_n \ .$$

Lema B.6. *Seja $n \in \mathbb{N}$ tal que $\text{MDC}(n, q) = 1$. Então*

(i) duas classes ciclotómicas-q ou são iguais ou são disjuntas;

(ii) as classes ciclotómicas-q módulo n formam uma partição de $\mathbb{Z}_n$.

Dem. (i) Sejam C_i e C_j duas classes ciclotómicas-q módulo n e suponhamos que $C_i \cap C_j \neq \varnothing$. Então existem $k_i, k_j \in \mathbb{N}_0$ tais que $iq^{k_i} \equiv jq^{k_j} \mod n$. Como $\text{MDC}(n, q) = 1$, q é invertível módulo n, logo q^{k_i} também é. Portanto

$$iq^{k_i} \equiv jq^{k_j} \mod n \iff i \equiv jq^{k_j - k_i} \mod n \implies iq^k \equiv jq^{k+k_j-k_i} \mod n \quad \forall\, k \in \mathbb{N}_0 \ ,$$

donde $C_i \subset C_j$. Trocando i e j no argumento anterior, também temos que $C_j \subset C_i$.
(ii) É consequência imediata de (i). □

Exemplo B.7. (a) As classes ciclotómicas-2 módulo $n = 15$ são

$$C_0 = \{0\} \ , \quad C_1 = \{1, 2, 4, 8\} \ , \quad C_3 = \{3, 6, 12, 9\} \ , \quad C_5 = \{5, 10\} \quad \text{e} \quad C_7 = \{7, 14, 13, 11\} \ .$$

(b) Classes ciclotómicas-5 módulo $n = 4$: como $5 \equiv 1 \mod 4$, $C_i = \{i\}$ para todo o i.

(c) As classes ciclotómicas-3 módulo $n = 5$ são

$$C_0 = \{0\} \qquad \text{e} \qquad C_1 = \{1, 3, 4, 2\} \ .$$

(d) As classes ciclotómicas-3 módulo $n = 8$ são

$$C_0 = \{0\} \ , \qquad C_1 = \{1, 3\} \ , \qquad C_2 = \{2, 6\} \ , \qquad C_4 = \{4\} \qquad \text{e} \qquad C_5 = \{5, 7\} \ .$$

Observação B.8. Se $n = q^m - 1$, para algum $m \geq 1$, como $q^m \equiv 1 \mod (q^m - 1)$, temos que $|C_i| \leq m$. Note ainda que $\text{MDC}(q^m - 1, q) = 1$ para todo o $m \geq 1$.

A observação anterior aplica-se a (a), (b) e (d) do Exemplo B.7.

Lema B.9. *Se $f(t) \in \mathbb{F}_q[t]$ tem uma raiz $a \in \mathbb{F}_{q^m}$, então $a^q \in \mathbb{F}_{q^m}$ também é raiz de $f(t)$.*

Dem. Pondo $f(t) = f_0 + f_1 t + \cdots + f_n t^n$, com coeficientes $f_i \in \mathbb{F}_q$, e calculando em a^q, obtém-se

$$\begin{aligned} f(a^q) &= f_0 + f_1 a^q + \cdots + f_k (a^q)^n \\ &= (f_0)^q + (f_1)^q a^q + \cdots + (f_n)^q (a^n)^q && \text{porque} \quad f_i^q = f_i \ , \quad \text{porque} \quad f_i \in \mathbb{F}_q \\ &= \big(f(a)\big)^q && \text{pela Fórmula do Caloiro} \\ &= 0 && \text{por hipótese em } f. \end{aligned}$$

□

Teorema B.10. *Seja $\alpha \in \mathbb{F}_{q^m}$ um elemento primitivo. Então o polinónio mínimo sobre $\mathbb{F}_q$ de α^i é*

$$m_i(t) := \prod_{j \in C_i} (t - \alpha^j) \ , \tag{B.1}$$

onde C_i é a classe ciclotómica-q de i módulo $q^m - 1$.

Dem. 1º passo: $m_i(\alpha^i) = 0$ pela definição (B.1) de $m_i(t)$, pois $i \in C_i$.

2º passo $m_i(t) \in \mathbb{F}_q[t]$**:** Seja $m_i(t) = a_0 + a_1 t + \cdots + a_k t^k$, com $k = |C_i|$ e $a_l \in \mathbb{F}_{q^m}$ – note que o produto em (B.1) é feito em $\mathbb{F}_{q^m}[t]$. Portanto o coeficiente a_l é o polinómio simétrico, de grau l, nas raízes α^j, com $j \in C_i$. Seja

$$m_{iq}(t) := \prod_{j \in C_{iq}} (t - \alpha^j) = \prod_{j \in C_i} (t - \alpha^{qj}) \ .$$

Pondo $m_{iq}(t) = b_0 + b_1 t + \cdots + b_k t^k$, o coeficiente $b_l \in \mathbb{F}_{q^m}$ é o polinómio simétrico, de grau l, nas raízes $\alpha^{qj} = (\alpha^j)^q$, com $j \in C_i$. Aplicando a Fórmula do Caloiro aos coeficientes b_l e comparando com os coeficientes a_l de $m_i(t)$, obtemos $b_l = a_l^q$, para todo o $l = 0, \ldots, k$. Por outro lado, como $iq \in C_i$, temos ainda que $C_{iq} = C_i$, logo $m_i(t) = m_{iq}(t)$, donde $a_l^q = a_l$ e, pela Proposição 3.15 (i), concluímos que $a_l \in \mathbb{F}_q \subset \mathbb{F}_{q^m}$.

3º passo: Para provarmos que $m_i(t)$ é o polinómio mínimo de α^i, atendendo aos 1º e 2º passos, só falta ver que $m_i(t)$ tem grau mínimo ou, equivalentemente, que qualquer outro polinómio mónico em $\mathbb{F}_q[t]$ que se anula em α^i é um múltiplo de $m_i(t)$. Seja então $f(t) \in \mathbb{F}_q[t]$ mónico tal que $f(\alpha^i) = 0$. Como as raízes em $\mathbb{F}_{q^m}$ de $m_i(t)$ são simples (i.e., são todas distintas porque α é um elemento primitivo de $\mathbb{F}_{q^m}$), basta ver que cada uma delas também é raiz de $f(t)$, para concluirmos que $m_i(t) \mid f(t)$. Por definição de classe ciclotómica, cada $j \in C_i$ é da forma $j \equiv iq^k \mod q^m - 1$ para algum $k \in \mathbb{N}_0$, logo $\alpha^j = (\alpha^i)^{q^k}$ e, pelo Lema B.9, temos que α^j é raiz de $f(t)$. □

Note que, nas condições do teorema anterior, α^i e α^j têm o mesmo polinómio mínimo se e só se i e j pertencem à mesma classe ciclotómica-q módulo $q^m - 1$.

Observação B.11. (i) O Lema B.9 diz-nos como obter raízes de um polinómio $f(t) \in \mathbb{F}_q[t]$ a partir de uma raiz $a \in \mathbb{F}_{q^m}$, nomeadamente tomando a potência q de a e voltando a fazer o mesmo às novas raízes encontradas: a, a^q, a^{q^2}, etc. No entanto, $f(t)$ poderá ter outras raízes.

(ii) O Teorema B.10 diz-nos que, no caso do polinómio mínimo $m_i(t)$ de $\alpha^i \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$, este não tem mais raízes que as "dadas" pelo Lema B.9 e que todas as raízes são simples.

(iii) Note ainda que, no caso de polinómios com coeficientes no corpo do reais $\mathbb{R}$, já se conhece um resultado análogo ao do Lema B.9: se $r \in \mathbb{C}$ é uma raiz de $f(t) \in \mathbb{R}[t]$, então o conjugado $\bar{r}$ é outra raiz. Além disso, se $r \in \mathbb{C} \setminus \mathbb{R}$, então $(t - r)(t - \bar{r}) \in \mathbb{R}[t]$. Por analogia, os elementos α^j com $j \in C_i$ (a classe ciclotómica-q de i) dizem-se os *conjugados* de $a = \alpha^i$, pois α^j são precisamente os elementos da forma a^{q^k} como se viu na demonstração do Teorema B.10.

Exemplo B.12. Seja $\mathbb{F}_{16} = \mathbb{F}_2[\alpha]$, onde $\alpha^4 = \alpha + 1$. (Verifique que α é um elemento primitivo de $\mathbb{F}_{16}$). Portanto temos $q = 2$ e $m = 4$. Aproveitando as classes ciclotómicas calculadas no Exemplo B.7(a), o polinómio mínimo $m_i(t)$ de cada α^i sobre $\mathbb{F}_2$ é

$$\begin{aligned}
m_0(t) &= t - 1 = t + 1 \ , \\
m_1(t) &= (t - \alpha)(t - \alpha^2)(t - \alpha^4)(t - \alpha^8) = t^4 + t + 1 = m_2(t) = m_4(t) = m_8(t) \ , \\
m_3(t) &= (t - \alpha^3)(t - \alpha^6)(t - \alpha^9)(t - \alpha^{12}) = t^4 + t^3 + t^2 + t + 1 = m_6(t) = m_9(t) = m_{12}(t) \ , \\
m_5(t) &= (t - \alpha^5)(t - \alpha^{10}) = t^2 + t + 1 = m_{10}(t) \ , \\
m_7(t) &= (t - \alpha^7)(t - \alpha^{11})(t - \alpha^{13})(t - \alpha^{14}) = t^4 + t^3 + 1 = m_{11}(t) = m_{13}(t) = m_{14}(t) \ .
\end{aligned}$$

Note que, uma vez que $\alpha^4 = \alpha + 1$, temos que α é raiz de $t^4 + t + 1$ e, como este polinómio é irredutível em $\mathbb{F}_2[t]$ (verifique!), também podemos concluir que $m_1(t) = t^4 + t + 1$ aplicando o Teorema B.3.

Uma aplicação dos polinómios mínimos é podermos definir código BCH, já mencionado no Capítulo 9, à custa do seu polinómio gerador.

Definição B.13. Seja $\alpha \in \mathbb{F}_{q^m}$ um elemento primitivo. Sejam $m_a(t), m_{a+1}(t), \ldots, m_{a+\delta-2}(t) \in \mathbb{F}_q[t]$ os polinómios mínimos sobre $\mathbb{F}_q$ de $\alpha^a, \alpha^{a+1}, \ldots, \alpha^{a+\delta-2} \in \mathbb{F}_{q^m}$, onde $\delta \geq 2$ e $a \geq 0$. Um código BCH é um código cíclico q-ário de comprimento $n = q^m - 1$ com polinómio gerador

$$g(t) = \text{MMC}(m_a(t), m_{a+1}(t), \ldots, m_{a+\delta-2}(t)) \ .$$

Observação B.14. (i) O Teorema B.10 garante que as raízes de um polinómio mínimo são todas distintas, i.e., todas têm multiplicidade um e, juntamente com o Lema B.6, dois polinómios mínimos ou são iguais ou não têm raízes em comum. Portanto, ao tomarmos o MMC na definição anterior, garantimos que $g(t)$ é um produtos dos $m_{a+i}(t)$ mas SEM repetições.

(ii) Como consequência de (i), $g(t) \mid t^{q^m-1} - 1$ e, portanto, $g(t)$ é de facto o polinómio gerador de um código cíclico de comprimento $q^m - 1$.

(iii) Outra consequência de (i) é as raízes de $g(t)$ serem todas distintas. Alem disso, como α^{a+i} é raiz de $m_{a+i}(t)$, há $\delta - 1$ potências consecutivas de um elemento primitivo que são raízes de $g(t)$. Podemos então concluir que $\text{d}(C) \geq \delta$ para qualquer código BCH nas condições da definição anterior – ver Observação 9.8.

Exemplo B.15. Se $m = 1$, então $\alpha \in \mathbb{F}_{q^m} = \mathbb{F}_q$ e $m_{a+i}(t) = t - \alpha^{a+i}$. Neste caso, se $2 \leq \delta \leq q - 1$, os códigos BCH são os códigos Reed-Solomon estudados no Capítulo 9.

2. Factorização de $t^n - 1$

Nesta secção aproveitamos os resultados anteriores para obter uma factorização em polinómios irredutíveis em $\mathbb{F}_q[t]$ de $t^n - 1$, polinómio importante do ponto de vista dos códigos cíclicos no Capítulo 8. Recorde que a seguinte factorização

$$t^n - 1 = (t - 1)(1 + t + \cdots + t^{n-1}) \tag{B.2}$$

é válida[1] em $\mathbb{F}_q[t]$, mas $1 + t + \cdots + t^{n-1}$, dependendo de n e q, poderá não ser irredutível.

Da Proposição 3.15 (i), o polinómio $t^{q^m-1} - 1$ tem como raízes todos os elementos não nulos em $\mathbb{F}_{q^m}$ e, como $\alpha \in \mathbb{F}_{q^m}$ é primitivo, $\mathbb{F}_{q^m} \setminus \{0\} = \{1, \alpha, \ldots, \alpha^{q^m-2}\}$ portanto o Teorema B.10 diz-nos que

$$t^{q^m-1} - 1 = \prod_{r=1}^{s} m_{i_r}(t) \ , \tag{B.3}$$

onde s é o número de classes ciclotómicas-q módulo $q^m - 1$ distintas e $i_1, \ldots, i_s$ são representantes dessas classes.

Exemplo B.16. Continuando o Exemplo B.12, a factorização de $t^{15} - 1$ em factores irredutíveis em $\mathbb{F}_2[t]$ é

$$t^{15} - 1 = (t + 1)(t^2 + t + 1)(t^4 + t + 1)(t^4 + t^3 + 1)(t^4 + t^3 + t^2 + t + 1) \ .$$

A factorização (B.3) é generalizada no próximo teorema.

Teorema B.17. *Dados $n \in \mathbb{N}$ tal que $\text{MDC}(n, q) = 1$ e $m \in \mathbb{N}$ tal que $n \mid (q^m - 1)$, seja $\alpha \in \mathbb{F}_{q^m}$ um elemento primitivo e $m_i(t) \in \mathbb{F}_q[t]$ o polinómio mínimo de α^i sobre $\mathbb{F}_q$. Então*

$$t^n - 1 = \prod_{r=1}^{s} m_{li_r}(t) \ ,$$

onde $l = \frac{q^m-1}{n}$ e $\{i_1, \ldots, i_s\}$ é um conjunto de representantes das s classes ciclotómicas-q módulo n.

[1] De facto, esta factorização é válida em qualquer anel com identidade $1 \neq 0$.

Dem. Seja $l \in \mathbb{N}$ tal que $nl = q^m - 1$, então

$$t^{q^m-1} - 1 = \left(t^l\right)^n - 1 \ ,$$

donde α^{il}, com $i = 0, \ldots, n-1$, são as raízes em $\mathbb{F}_{q^m}$ de $t^n - 1$, e são todas simples pois α é um elemento primitivo de $\mathbb{F}_{q^m}$ e, por definição de polinómio mínimo, temos que $m_{il}(t) \mid t^n - 1$. Portanto, basta encontrar os $m_{il}(t)$, $i = 0, \ldots, n-1$, distintos que dividem $t^n - 1$. (Note que, como os polinómios mínimos são irredutíveis sobre $\mathbb{F}_q$, dados dois, estes ou são iguais ou são coprimos em $\mathbb{F}_q[t]$.) Mas $m_{il}(t) = m_{jl}(t)$ se e só se $C_{il} = C_{jl}$, como classes ciclotómicas-q módulo $q^m - 1$, se e só se $C_i = C_j$, como classes ciclotómicas-q módulo-n. □

Observação B.18. Nos resultados desta secção assumiu-se sempre que $\mathrm{MDC}(n, q) = 1$. Caso isso não aconteça, como $q = p^i$ para algum $i \in \mathbb{N}$ e algum primo p (nomeadamente p é a característica do corpo finito $\mathbb{F}_q$), então $n = lp^j$, com $j, l \in \mathbb{N}$ e $\mathrm{MDC}(l, q) = 1$, donde

$$t^n - 1 = \left(t^l\right)^{p^i} - 1 = \left(t^l - 1\right)^{p^i} \ ,$$

onde se aplicou a Fórmula do Caloiro no último passo. Como $\mathrm{MDC}(l, q) = 1$, aplicamos o Teorema B.17 para factorizar $t^l - 1$, escolhendo um inteiro m tal que $l \mid (q^m - 1)$ – ver Exercício B.2.

Exemplo B.19. Vamos decompor $t^9 - 1$ em polinómios irredutíveis em $\mathbb{F}_2[t]$. Neste caso temos que $q = 2$ e $n = 9$ são coprimos e $9 \mid 2^6 - 1$, portanto aplicamos o Teorema B.17 com $m = 6$ e $l = 7$. Seja α um elemento primitivo de $\mathbb{F}_{64}$, logo $\zeta = \alpha^7$ é uma raiz-9 primitiva. As classes ciclotómicas-2 módulo 9 são

$$C_0 = \{0\} \ , \quad C_1 = \{1, 2, 4, 8, 7, 5\} \quad \text{e} \quad C_3 = \{3, 6\} \ ,$$

portanto

$$\begin{aligned} m_0(t) &= t - 1 \ , \\ m_7(t) &= (t - \zeta)(t - \zeta^2)(t - \zeta^4)(t - \zeta^8)(t - \zeta^7)(t - \zeta^5) \quad \text{e} \\ m_{21}(t) &= (t - \zeta^3)(t - \zeta^6) = (t - \alpha^{21})(t - \alpha^{42}) = t^2 + (\alpha^{21} + \alpha^{42})t + 1 \end{aligned}$$

são os polinómios mínimos de $\zeta^0 = 1$, $\zeta = \alpha^7$ e $\zeta^3 = \alpha^{21}$, respectivamente, e são os factores irredutíveis de $t^9 - 1$ sobre $\mathbb{F}_2$. Como $m_{21}(t)$ é irredutível e $t^2 + t + 1$ é o único polinómio de grau 2 irredutível em $\mathbb{F}_2[t]$, temos[2] necessariamente que $m_{21}(t) = t^2 + t + 1$. Quanto a $m_7(t)$, ou determinamos um elemento primitivo e simplificamos a expressão anterior dada à custa das suas raízes em $\mathbb{F}_{64}$ ou, uma vez que já temos os outros factores de $t^9 - 1$, podemos simplesmente fazer o quociente de $t^9 - 1$ por $m_0(t)m_{21}(t) = t^3 - 1$ e obtemos $m_7(t) = t^6 + t^3 + 1$. Conclusão

$$t^9 - 1 = (t + 1)(t^2 + t + 1)(t^6 + t^3 + 1) \quad \text{em } \mathbb{F}_2[t] \ .$$

Por vezes é mais fácil obter a factorização de $t^n - 1$ em polinómios irredutíveis sobre $\mathbb{F}_q$ por métodos mais elementares, sem recorrer ao Teorema B.17.

Exemplo B.20. Em $\mathbb{F}_7[t]$ temos

$$t^{28} - 1 = (t^4)^7 - 1 = (t^4 - 1)^7$$

e, como

$$t^4 - 1 = (t^2)^2 - 1 = (t^2 - 1)(t^2 + 1) \ ,$$

obtém-se

$$t^{28} - 1 = (t - 1)^7 (t + 1)^7 (t^2 + 1)^7 \ .$$

Repare que $t^2 + 1$ é irredutível em $\mathbb{F}_7[t]$ pois tem grau 2 e não tem raízes em $\mathbb{F}_7$.

Exemplo B.21. Em $\mathbb{F}_2[t]$ temos

$$t^{10} - 1 = (t^5)^2 - 1 = (t^5 - 1)^2 = (t - 1)^2 (1 + t + t^2 + t^3 + t^4)^2 \ ,$$

onde apenas se usou a Fórmula do Caloiro no primeiro passo e a factorização (B.2) no segundo. Já se encontrou $1 + t + t^2 + t^3 + t^4 \in \mathbb{F}_2[t]$ como polinómio mínimo sobre $\mathbb{F}_2[t]$ de algum elemento em $\mathbb{F}_{16}$, de modo que podemos concluir que este polinómio é irredutível sobre $\mathbb{F}_2$.

[2] Alternativamente, também temos que $\alpha^{21} + \alpha^{42} = 1$ porque $\{0, 1, \alpha^{21}, \alpha^{42}\}$ é o subcorpo $\mathbb{F}_4 \subset \mathbb{F}_{64}$ – justifique.

Exercícios

B.1. Determine as classe ciclotómicas-q módulo n nos seguintes casos:
(a) $q = 2$, $n = 9$;
(b) $q = 3$, $n = 13$.

B.2. Dado $n \in \mathbb{N}$ tal que $\mathrm{MDC}(n, q) = 1$, mostre que existe $m \in \mathbb{N}$ tal que $n \mid q^m - 1$.

B.3. Determine a factorização em polinómios irredutíveis de $t^n - 1$ nos sequintes casos:
(a) $t^{q-1} - 1$ em $\mathbb{F}_q[t]$;
(b) $t^q - 1$ em $\mathbb{F}_q[t]$;
(c) $t^8 - 1$ em $\mathbb{F}_3[t]$;
(d) $t^{13} - 1$ em $\mathbb{F}_3[t]$.

B.4. Mostre que $t^{q^n-1} - 1$ divide $t^{q^m-1} - 1$ em $\mathbb{F}_q[t]$ se e só se $n \mid m$.
Sugestão: Resolva primeiro o Exercício 3.15.

B.5. (a) Determine as classes ciclotómicas-9 módulo 10.
(b) Determine o número de códigos cíclicos sobre $\mathbb{F}_9$, de comprimento 10 e dimensão 7.

BIBLIOGRAFIA

[1] R.L. Fernandes, M. Ricou, *Introdução à Álgebra*, IST Press.

[2] R. Hill, *A Fisrt Course in Coding Theory*, Oxford Applied Mathematics and Computing Science Series, 1996, Oxford University Press.

[3] J.H. van Lint, R.M. Wilson, *A course in Combinatorics*, 2nd edition, Cambridge University Press, 2001.

[4] S. Roman, *Coding and Information Theory*, Graduate Texts in Mathematics, 134, Springer-Verlag, 1992.