CAPÍTULO 7

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,

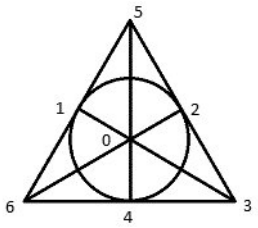
tais que qualquer subconjunto de $\mathcal{P}$ com t elementos está contido precisamente num único bloco.

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. com $B_i = \{p_i\}$ para $i = 1, \ldots, v$, 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 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

$$X = \{(P,B) \,:\, P \subseteq \mathcal{P} \text{ com } |P| = t,\, B \in \mathcal{B} \text{ tais que } P \subseteq B\}\ .$$

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 $0 \leq i \leq t$, 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 $I \subseteq \mathcal{P}$. 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 $I \subseteq P \subseteq \mathcal{P}$ 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 $i \leq t$. Então o conjunto de pontos $\mathcal{P} \setminus I$ e a colecção de blocos $\{B \setminus I \,:\, B \in \mathcal{B}, I \subseteq B\}$ 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 $i = 1, \ldots, n$.

Teorema 7.12. *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

$$t \geq \mathrm{d}(x,y) = \mathrm{w}(x-y) \geq \mathrm{w}(x) - \mathrm{w}(y) = \mathrm{w}(x) - (t+1)\,, \tag{7.2}$$

porque $\mathrm{w}(x-y) \geq \mathrm{w}(x) - \mathrm{w}(y)$ para todo o x, y, 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 daqui conclui-se que x cobre y, ficando assim provada a afirmação (7.1). □

Exemplo 7.13. 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 7.14. 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 7.15. *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 7.12, 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 7.16. 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 7.17. *Seja C um código perfeito q-ário, de comprimento n e distância mínima $2t+1$, então, dado $y \in \mathbb{F}_q^n$, 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 7.18. *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 7.17, 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 7.19. *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 7.12, 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. 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. Sejam $x, y \in \mathbb{F}_q^n$.
   (a) Mostre que $\mathrm{w}(x - y) \geq \mathrm{w}(x) - \mathrm{w}(y)$.
   (b) Mostre que $\mathrm{d}(x, y) = \mathrm{w}(x) - \mathrm{w}(y)$ se e só se x cobre y.
   (Estas propriedades foram usadas na demonstração do Teorema 7.12.)

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 $S(2, q + 1, q^2 + q + 1)$. 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. 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.

7.4. Quantas palavras de peso 7 há em G_{23}?

7.5. Quantas palavras de peso 5 há em G_{11}?

7.6. Para um código C qualquer, define-se $A_i = \#\{x \in C : \mathrm{w}(x) = i\}$. Determine os números A_i para o código de Golay estendido G_{24}.

BIBLIOGRAFIA

[1] R.L. Fernandes, M. Ricou, *Introdução à Álgebra*, IST Press.

[2] R. Hill, *A Fisrt Course in Coding Thery*, 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.