

# Grupo Linear de Isometrias com Estrutura de Ordem Parcial

**Luciano Panek**

Depto de Matemática, Universidade Estadual de Maringá, UEM  
87020-900, Maringá, PR  
E-mail: lpanek@uem.br,

**Marcelo Firer**

IMECC-UNICAMP, Universidade Estadual de Campinas  
Caixa Postal: 6065  
13081-970, Campinas, SP  
E-mail: mfirer@ime.unicamp.br

Seja  $\mathbf{F}_q^n$  o espaço vetorial das  $n$ -uplas sobre o corpo finito  $\mathbf{F}_q$  com  $q$  elementos. Um dos principais problemas da teoria dos códigos é determinar a maior distância mínima possível realizada por um código linear de  $\mathbf{F}_q^n$  com uma dada dimensão. Existem muitas métricas definidas sobre  $\mathbf{F}_q^n$ . As mais comuns são as métricas de Hamming e de Lee.

Em 1987 Niederreiter generalizou o problema descrito acima ([8]). Sejam  $n_1, \dots, n_s$  inteiros positivos e

$$H = \{h_{(i,j)} : 1 \leq i \leq s, 1 \leq j \leq n_i\}$$

um sistema com  $n_1 + \dots + n_s$  vetores em  $\mathbf{F}_q^n$  particionados em  $s$  conjuntos ordenados de cardinalidade  $n_1, \dots, n_s$  respectivamente. O problema de Niederreiter baseasse em determinar o número

$$d_q(n_1, \dots, n_s; n) = \max_H d(H),$$

sendo o máximo tomado sobre todos os sistemas  $H$  descritos acima onde

$$d(H) = \min \sum_{i=1}^s d_i,$$

$0 \leq d_i \leq n_i$ ,  $1 \leq i \leq s$ , é tal que  $\{h_{(i,j)} : 1 \leq i \leq s, 1 \leq j \leq d_i\} \subset H$  é um conjunto linearmente dependente. Se  $n_1 = \dots = n_s = 1$ , então  $H = [h_{(1,1)} \dots h_{(s,1)}]$  é uma matriz de ordem  $n \times s$ . Se  $H$  é uma matriz de posto  $n$ , então

$$C = \{v \in \mathbf{F}_q^n : H \cdot v^t = 0\}$$

é um código de dimensão  $s-n$  com distância mínima de Hamming igual a  $d(H)$  (ver [4, pág.13]). Neste caso, estudar o número  $d_q(1, \dots, 1; n)$  é o mesmo que determinar a maior distância mínima de Hamming que pode ser realizada por um código linear sobre  $\mathbf{F}_q$  de dimensão  $s-n$ .

Brualdi, Graves e Lawrence ([2]) em 1995 estenderam o problema de Niederreiter e introduziram o

conceito de *poset*-métricas, objeto de nosso interesse, que descrevemos a seguir.

Seja  $P = \{1, 2, \dots, n\}$  um conjunto parcialmente ordenado com a relação de ordem  $\leq$ . Um ideal de  $P$  é um subconjunto  $I \subset P$  com a propriedade que se  $x \in I$  e  $y \leq x$  então  $y \in I$ . Se  $A \subset P$  então  $\langle A \rangle$  denota o menor ideal contendo  $A$ .

Dado  $x = (x_1, x_2, \dots, x_n) \in \mathbf{F}_q^n$ , o *suporte* de  $x$  é o conjunto

$$\text{supp}(x) := \{i \in P : x_i \neq 0\},$$

e definimos o  $P$ -peso de  $x$  como sendo a cardinalidade do menor ideal contendo  $\text{supp}(x)$ :

$$w_P(x) = |\langle \text{supp}(x) \rangle|.$$

A função  $d_P : \mathbf{F}_q^n \times \mathbf{F}_q^n \rightarrow \mathbf{N}$  definida por  $d_P(x, y) = w_P(x - y)$  é uma métrica em  $\mathbf{F}_q^n$  ([2, Lemma 1.1]), chamada de  $P$ -métrica. Denotamos tal espaço métrico por  $(\mathbf{F}_q^n, d_P)$ .

Um  $[n, k, \delta_P]_q$   $P$ -código é um subespaço vetorial  $C \subset \mathbf{F}_q^n$  de dimensão  $k$ , onde

$$\delta_P(C) = \min \{w_P(x) : 0 \neq x \in C\}$$

é a *distância mínima* do código  $C$ . Se  $P$  é anticadeia, isto é,  $x \leq y$  se e somente se  $x = y$ , então o  $P$ -peso, a  $P$ -métrica e a distância mínima coincidem com o peso de Hamming, a métrica de Hamming e a distância mínima de Hamming da clássica teoria dos códigos. No caso em que  $P$  é uma união disjunta de cadeias de mesmo comprimento, a métrica  $d_P$  coincide com a métrica de Rosenbloom-Tsfasman, introduzida em [9]. Um dos méritos desta nova teoria é o surgimento de novos códigos perfeitos (ver [1], [2], [5] e [6]).

Assim, em [2], os sistemas  $H = \{h_i : 1 \leq i \leq s\}$  passam a ser indexados por um conjunto parcialmente ordenado  $P = \{1, 2, \dots, s\}$ . Neste caso  $d_P(H)$  é definido como sendo o menor inteiro positivo  $d$  tal que existe um ideal  $I$  de  $P$  de cardinalidade  $d$  com a propriedade que  $\{h_i : i \in I\}$  é um

conjunto linearmente dependente. Note agora que se  $H = [h_1 \dots h_s]$  é a matriz verificação de paridade de algum código linear  $C \subset \mathbf{F}_q^n$  de dimensão  $s - n$ , então a distância mínima  $\delta_P$  de  $C$  é igual a  $d_P(H)$ .

No caso do anel  $\mathbb{Z}_n$ , observamos que se  $n \neq 2, 3$ , então não existe uma ordem parcial  $P = \{1, 2, \dots, m\}$  tal que o  $P$ -peso  $w_P$  coincida com o peso de Lee  $w_{Lee}$ : se  $x = (\overline{x_1}, \dots, \overline{x_m}) \in \mathbb{Z}_n^m$  então

$$w_{Lee}(x) = \sum_{i=1}^m \min\{|x_i|, n - |x_i|\},$$

com  $0 \leq x_i \leq n$  sendo o representante da classe  $\overline{x_i}$ . Se  $n = 2$  ou  $3$  então  $w_{Lee} = w_H$ . Conseqüentemente, se  $P$  é anticadeia e  $n = 2$  ou  $3$ , então  $w_P = w_{Lee}$ . Agora, se  $n \neq 2, 3$ , tomando  $y = \left(\left\lfloor \frac{n}{2} \right\rfloor, \dots, \left\lfloor \frac{n}{2} \right\rfloor\right) \in \mathbb{Z}_n^m$ , sendo  $\lfloor x \rfloor$  a parte inteira de  $x$ , segue que  $w_P(x) = m$  e  $w_{Lee}(x) = m \cdot \left\lfloor \frac{n}{2} \right\rfloor > m$ . Daí  $w_P(x) \neq w_{Lee}(x)$  ( $w_P(x) < w_{Lee}(x)$ ). Em resumo: se  $n \geq 4$  é um inteiro positivo, então não existe uma ordem parcial  $P$  tal que  $w_P = w_{Lee}$  sobre  $\mathbb{Z}_n^m$ .

Passamos agora a descrever o grupo das isometrias lineares do espaço  $(\mathbf{F}_q^n, d_P)$ . Uma *isometria linear*  $T$  do espaço métrico  $(\mathbf{F}_q^n, d_P)$  é uma transformação linear  $T : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$  que preserva a  $P$ -métrica, ou seja,

$$d_P(T(x), T(y)) = d_P(x, y),$$

para todo  $x, y \in \mathbf{F}_q^n$ . Equivalentemente, uma transformação linear  $T : \mathbf{F}_q^n \rightarrow \mathbf{F}_q^n$  é uma isometria se  $w_P(T(x)) = w_P(x)$  para todo  $x \in \mathbf{F}_q^n$ . Denotamos o grupo das isometrias lineares de  $(\mathbf{F}_q^n, d_P)$  por  $GL_P(\mathbf{F}_q^n)$ .

Em 2002 Skriganov ([10]) definiu algumas isometrias lineares sobre o espaço de Rosenbloom-Tsfasman e questionou sobre a possibilidade das mesmas gerarem o grupo de isometrias. A questão de Skriganov foi respondida afirmativamente por Lee em 2003 (ver [7]): o grupo das isometrias lineares do espaço de Rosenbloom-Tsfasman  $\mathbf{F}_q^{n \cdot s}$  é o produto semi-direto de  $T_s \times \dots \times T_s$  ( $T_s$  denota o grupo das matrizes triangulares superiores de ordem  $s$  com elementos da diagonal não nulos) com o grupo simétrico  $\mathbf{S}_n$  ( $\mathbf{S}_n$  age permutando as componentes de  $T_s \times \dots \times T_s$ ). Em [3] Cho e Kim determinam o grupo das isometrias lineares do espaço  $\mathbf{F}_q^{2m}$  munido com a métrica ponderada pela ordem crown  $C$ : se  $D_m$  denota o grupo diedral de ordem  $2m$ , então  $GL_C(\mathbf{F}_q^{2m}) \simeq (D_m \times (\mathbf{F}_q^\times)^{2m}) \times \mathbf{F}_q^{2m}$  ( $D_m$  age permutando a ordem crown  $C$ ).

Em nosso trabalho damos uma descrição completa do grupo das isometrias lineares  $GL_P(\mathbf{F}_q^n)$  para uma ordem parcial  $P$  arbitrária. A propriedade de permutar cadeias de mesmo comprimento, mostrada por Lee ([7]), no caso da métrica de Rosenbloom-Tsfasman, corresponde no

caso geral de uma ordem parcial qualquer ao resultado de que toda isometria  $T \in GL_P(\mathbf{F}_q^n)$  induz um automorfismo na ordem  $P$ . Em outras palavras: seja  $P = \{1, 2, \dots, n\}$  parcialmente ordenado e  $\{e_1, e_2, \dots, e_n\}$  a base canônica do espaço  $\mathbf{F}_q^n$ ; então  $T \in GL_P(\mathbf{F}_q^n)$  se e somente se

$$T(e_j) = \sum_{i \in (j)} x_{ij} e_{\phi(i)}$$

onde  $\phi : P \rightarrow P$  é um automorfismo da ordem e  $x_{jj} \neq 0$ , para todo  $j \in \{1, 2, \dots, n\}$ . Conseqüentemente, existe um par de bases ordenadas  $\beta$  e  $\beta'$  de  $\mathbf{F}_q^n$  tal que  $T \in GL_P(\mathbf{F}_q^n)$  relativa a estas bases é representada por uma matriz  $n \times n$  triangular superior  $(a_{ij})_{1 \leq i, j \leq n}$  com  $a_{ii} \neq 0$  para todo  $i \in \{1, 2, \dots, n\}$ .

A propriedade fundamental usada para provar o resultado descrito acima é o lema que assegura que  $\langle \text{supp}(T(u)) \rangle \subseteq \langle \text{supp}(T(v)) \rangle$  se  $\langle \text{supp}(u) \rangle \subseteq \langle \text{supp}(v) \rangle$ ,  $u, v \in \mathbf{F}_q^n$ .

A estrutura (produto semi-direto) do grupo  $GL_P(\mathbf{F}_q^n)$  é dada por: existe uma base ordenada  $\beta$  do espaço  $\mathbf{F}_q^n$  tal que  $T \in GL_P(\mathbf{F}_q^n)$  relativa a esta base é representada pelo produto  $A \cdot U$  de matrizes, sendo  $U$  uma matriz monomial correspondendo a um automorfismo da ordem  $P$  e  $A$  uma matriz triangular superior.

Se  $\Gamma^{(m)}(P) = \{i \in P : w_P(e_i) = m\}$ , da descrição acima segue que

$$\begin{aligned} |GL_P(\mathbf{F}_q^n)| &= \\ &= (q-1)^n \cdot \left( \prod_{i=1}^k q^{(i-1)|\Gamma^{(i)}(P)|} \right) \cdot |Aut(P)| \end{aligned}$$

com  $k = \max\{m : \Gamma^{(m)}(P) \neq \emptyset\}$  e  $Aut(P)$  denotando o grupo dos automorfismos da ordem  $P$ .

Para finalizar apresentaremos exemplos do grupo  $GL_P(\mathbf{F}_q^n)$  nos casos mais comuns de ordens parciais: união disjunta de cadeias e ordem fraca.

Seja  $P = P_1 \dot{\cup} P_2 \dot{\cup} \dots \dot{\cup} P_s$  uma ordem parcial consistindo de uma união disjunta de  $s$  cadeias. Denotamos por  $\mu_i$  a cardinalidade da  $i$ -ésima cadeia,  $i \in \{1, 2, \dots, s\}$ . Para cada  $j \in \{1, 2, \dots, n\}$  seja  $\nu_j = |\{P_i : |P_i| = j\}|$ . Então existe uma base ordenada  $\beta$  do espaço  $\mathbf{F}_q^n$  tal que  $T \in GL_P(\mathbf{F}_q^n)$  relativa a esta base é representada pelo produto  $A \cdot U$  de matrizes de ordem  $n$ , sendo  $U$  uma matriz monomial que age permutando os subespaços com suportes isomorfos e

$$A = \begin{pmatrix} A_1 & 0 & 0 & \dots & 0 \\ 0 & A_2 & 0 & \dots & 0 \\ 0 & 0 & A_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & A_s \end{pmatrix},$$

onde cada  $A_i$  é uma matriz  $\mu_i \times \mu_i$  triangular superior com elementos da diagonal não nulos. Neste

caso

$$|GL_P(\mathbb{F}_q^n)| = (q-1)^n \cdot \left( \prod_{k=1}^n \nu_k! \right) \cdot \left( \prod_{j=1}^s q^{\frac{\mu_j(\mu_j-1)}{2}} \right).$$

Agora sejam  $n_1, \dots, n_t$  inteiros positivos tais que  $n_1 + \dots + n_t = n$ . Então  $W = n_1\mathbf{1} \oplus \dots \oplus n_t\mathbf{1}$  denota a *order fraca* dada pela soma ordinária das anticadeias  $n_i\mathbf{1}$  com  $n_i$  elementos:

$$\{1, 2, \dots, n\} = n_1\mathbf{1} \cup n_2\mathbf{1} \cup \dots \cup n_t\mathbf{1},$$

$$n_i\mathbf{1} = \{n_1 + \dots + n_{i-1} + 1, n_1 + \dots + n_{i-1} + 2, \dots, n_1 + \dots + n_{i-1} + n_i\}$$

e

$$x < y \Leftrightarrow x \in n_i\mathbf{1}, y \in n_j\mathbf{1} \text{ para todo } i, j, i < j.$$

Para a ordem fraca  $W = n_1\mathbf{1} \oplus \dots \oplus n_t\mathbf{1}$  temos que  $\Gamma^{(m)}(W) = n_s\mathbf{1}$  se  $m = n_1 + n_2 + \dots + n_{s-1} + 1$ , para todo  $s \in \{1, 2, \dots, t\}$ , e  $\Gamma^{(m)}(W) = \emptyset$  caso contrário. O grupo dos automorfismos de ordem  $Aut(W)$  é isomorfo ao produto cartesiano

$$\mathbf{S}_{n_1} \times \mathbf{S}_{n_2} \times \dots \times \mathbf{S}_{n_t}.$$

Daí segue que

$$|GL_W(\mathbb{F}_q^n)| = (q-1)^n \cdot$$

$$\left( \prod_{i=2}^t q^{n_i(n_1+n_2+\dots+n_{i-1}+1)} \right) \cdot n_1! \cdot n_2! \cdot \dots \cdot n_t!.$$

Por fim, se  $T \in GL_W(\mathbb{F}_q^n)$  então existe um par de bases ordenadas  $\beta$  e  $\beta'$  de  $\mathbf{F}_q^n$  tal que a matriz  $[T]_{\beta, \beta'}$  é igual a

$$\begin{pmatrix} D_{n_1 \times n_1} & * & * & \cdots & * \\ 0 & D_{n_2 \times n_2} & * & \cdots & * \\ 0 & 0 & D_{n_3 \times n_3} & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & D_{n_t \times n_t} \end{pmatrix}$$

sendo

$$D_{n_s \times n_s} = \text{diag}(a_{\Sigma n_{s-1}+1, \Sigma n_{s-1}+1},$$

$$a_{\Sigma n_{s-1}+2, \Sigma n_{s-1}+2}, \dots, a_{\Sigma n_{s-1}+n_s, \Sigma n_{s-1}+n_s})$$

uma matriz diagonal para cada  $s = 1, 2, \dots, t$ , e  $\Sigma n_{j-1} := n_1 + n_2 + \dots + n_{j-1}$ .

Se  $\mathcal{R}$  é uma união disjunta de  $m$ 's  $W = 1\mathbf{1} \oplus \dots \oplus 1\mathbf{1}$ , então  $w_{\mathcal{R}}$  coincide com o peso de Rosenbloom-Tsfasman definido no espaço das matrizes  $M_{n \times m}(\mathbf{F}_q)$  de ordem  $n \times m$  sobre  $\mathbf{F}_q$ : se  $(a_{ij}) \in M_{n \times m}(\mathbf{F}_q)$ , então

$$w_{\mathcal{R}}((a_{ij})) = \sum_{j=1}^m |\langle \text{supp}(a_{1j}, a_{2j}, \dots, a_{nj}) \rangle|$$

com

$$\text{supp}(a_{1j}, a_{2j}, \dots, a_{nj}) = \{i : a_{ij} \neq 0\}.$$

Também temos que

$$GL_{\mathcal{R}}(M_{n \times m}(\mathbf{F}_q)) \simeq (T_n)^m \rtimes \mathbf{S}_m$$

sendo  $(T_n)^m$  o produto direto de  $m$  cópias do grupo  $T_n$  de todas as matrizes triangulares superiores de ordem  $n$  sobre  $\mathbf{F}_q$  com elementos da diagonal não nulos.

Se  $\mathcal{W}$  é uma união de  $m$ 's  $W = n_1\mathbf{1} \oplus \dots \oplus n_t\mathbf{1}$ , temos então o *espaço generalizado de Rosenbloom-Tsfasman*  $(\mathbf{F}_q^n, d_{\mathcal{W}})$ . Neste caso

$$GL_{\mathcal{W}}(\mathbb{F}_q^n) \simeq (T_W \rtimes \times_{i=1}^t \mathbf{S}_{n_i}) \rtimes \mathbf{S}_m.$$

## Referências

- [1] J. Ahn, H. K. Kim, J. S. Kim and M. Kim, Classification of perfect linear codes with crown poset structure, *Discrete Mathematics* 268 (2003) 21-30.
- [2] R. Brualdi, J. S. Graves and M. Lawrence, Codes with a poset metric, *Discrete Mathematics* 147 (1995) 57-72.
- [3] S. H. Cho and D. S. Kim, Automorphism group of the crown-weight space, *Eur. J. Combin.*, in press.
- [4] W. C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, *Cambridge University Press*, 2003.
- [5] Y. Jang and J. Park, On a MacWilliams Type Identity and a Perfectness for a Binary Linear  $(n, n-1, j)$ -poset code, *Discrete Mathematics* 265 (2003) 85-104.
- [6] J. Y. Hyun and H. K. Kim, The poset structures admitting the extended binary Hamming code to be a perfect code, *Discrete Mathematics* 288 (2004) 37-47.
- [7] K. Lee, Automorphism group of the Rosenbloom-Tsfasman space, *Eur. J. Combin.* 24 (2003) 607-612.
- [8] H. Niederreiter, A combinatorial problem for vector spaces over finite fields, *Discrete Mathematics* 96 (1991) 221-228.
- [9] M. Yu Rosenbloom and M. A. Tsfasman, Codes for the  $m$ -metric, *Probl. Inf. Transm.* 33 (1997) 45-52.
- [10] M. M. Skriganov, Coding theory and uniform distributions, *St. Petersburg Math. J.* 13 (2002) 301-337.