Proceeding Series of the Brazilian Society of Applied and Computational Mathematics, v. 6, n. 1, 2018.

Trabalho apresentado no XXXVII CNMAC, S.J. dos Campos - SP, 2017.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos de Hamming Estendidos como Códigos Perfeitos

Luciano Panek[1]
Centro de Engenharias e Ciências Exatas, UNIOESTE, Foz do Iguaçu, PR
Nayene Michele Paião Panek[2]
Centro de Engenharias e Ciências Exatas, UNIOESTE, Foz do Iguaçu, PR

Resumo. Neste trabalho classificaremos as métricas de blocos ordenados que tornam uma classe de códigos binários de Hamming estendidos códigos 1-perfeitos. Em particular reobeteremos a classificação das métricas de blocos ordenados que tornam o código binário de Hamming estendido $[8;4;4]_H$ um código 1-perfeito e apresentaremos a classificação das métricas de blocos ordenados que tornam 1-perfeito o código binário de Hamming estendido $[16;11;4]_H$.

Palavras-chave. Códigos Lineares, Códigos Perfeitos, Métricas Ordenadas, Métricas de Blocos, Métricas de Blocos Ordenados, Códigos de Hamming Estendidos.

1 Introdução

Seja $[n] := \{1, 2, \ldots, n\}$ um conjunto com n elementos e seja $\leq$ uma relação de ordem sobre $[n]$. O par $P := ([n], \leq)$ será chamado de *conjunto ordenado* ou simplesmente de *ordem*. Diremos que k é *menor do que* j se $k \leq j$ e $k \neq j$. Um *ideal* em P é um subconjunto $I \subseteq [n]$ que contém todos os elementos que são menores ou iguais a algum dos seus elementos, isto é, se $j \in I$ e $k \leq j$ então $k \in I$. Dado um subconjuto $X \subset [n]$, denotaremos por $\langle X \rangle$ o menor ideal contendo X, chamado de *ideal gerado por* X. Se $X = \{i\}$, então escreveremos $\langle i \rangle$.

Agora seja

$$\pi : [n] \to \mathbb{N}$$

uma aplicação tal que $\pi(i) > 0$ para todo $i \in [n]$. Chamaremos a aplicação π de *rótulo* sobre $[n]$. Se $k_i := \pi(i)$, definimos V_i como sendo o espaço vetorial $V_i = \mathbb{F}_q^{k_i}$ de todas as k_i-uplas sobre o corpo fintio $\mathbb{F}_q$ e V como sendo a soma direta dos espaços V_i:

$$V := V_1 \oplus V_2 \oplus \ldots \oplus V_n.$$

Podemos identificar V com o espaço $\mathbb{F}_q^N$, onde $N = k_1 + k_2 + \ldots + k_n$. Cada vetor de V pode ser escrito de forma única como

$$v = v_1 + v_2 + \ldots + v_n$$

[1]luciano.panek@unioeste.br
[2]nayene.paiao@unioeste.br

com $v_i \in V_i$, para cada $1 \leq i \leq n$.

Dado uma ordem $P = ([n], \leq)$ e $v = v_1 + v_2 + \ldots + v_n \in V$, o *$\pi$-suporte de v* é o conjunto

$$supp\,(v) := \{i \in [n] : v_i \neq 0\}\,.$$

Definimos o *(P,π)-peso* de v como sendo a cardinalidade do menor ideal gerado por supp(v):

$$w_{(P,\pi)}\,(v) = |\langle supp\,(v)\rangle|\,,$$

onde $\mid X \mid$ denota a cardinalidade do conjunto finito X. Se u e v são vetores de $\mathbb{F}_q^N$, então a *(P,π)-distância* entre u e v é definida por

$$d_{(P,\pi)}\,(x,y) = w_{(P,\pi)}\,(x-y)\,.$$

O conjunto

$$B_{(P,\pi)}\,(u;r) = \left\{v \in V : d_{(P,\pi)}\,(u,v) \leq r\right\}$$

é a *bola de centro u e raio r*. A saber,

$$\left|B_{(P,\pi)}\,(u;r)\right| = 1 + \sum_{i=1}^{r}\sum_{j=1}^{i}\sum_{I\in\Theta_j(i)}\prod_{m\in\mathrm{Max}(I)}\left(q^{k_m}-1\right)\prod_{l<m;m\in\mathrm{Max}(I)}q^{k_l}$$

onde $\Theta_j\,(i) = \{I \subseteq P : I \text{ ideal},\ |I| = i,\ |\mathrm{Max}\,(I)| = j\}$ e $\mathrm{Max}\,(I)$ é o conjunto dos elementos maximais no ideal $I \subseteq P$. O número de vetores em uma bola de raio r não depende do seu centro.

Um $\left[N;k;d_{(P,\pi)}\right]$ *código linear* é um subespaço k-dimensional C do espaço $\mathbb{F}_q^N$ onde

$$d_{(P,\pi)} = \min\left\{d_{(P,\pi)}\left(c,c'\right) : c \neq c' \in C\right\}$$

é a *(P,π)-distância mínima* do código C.

A (P,π)-distância é uma métrica sobre V que combina e estende a métrica ordenada, proposta por Brualdi, Graves e Lawrence em [2] e, a métrica de blocos, introduzida por Feng, Xu e Hickernell em [3]. Chamaremos o espaço $(V, d_{(P,\pi)})$ de *espaço métrico de blocos ordenados*. Quando o rótulo π satisfaz $\pi\,(i) = 1$, para todo $i \in [n]$, a (P,π)-distância coincide com a *métrica ordenada d_P* proposta por Brualdi et al. Quando P é a ordem anticadeia (elementos distintos não são comparáveis entre si), a (P,π)-distância coincide com a *métrica de blocos d_π* proposta por Feng et al. No caso em que ambas as condições ocorrem ($\pi\,(i) = 1$ para todo $i \in [n]$ e P é a ordem anticadeia), a métrica de blocos ordenados se reduz a usual *métrica de Hamming d_H*. Neste caso usaremos o índice H para denotar a métrica de Hamming d_H, os parâmetros de um código linear, $[n;k;d_H]_H$, e o suporte $supp_H\,(u) = \{i : u_i \neq 0\}$ de um vetor $u = (u_1, u_2, \ldots, u_N) \in \mathbb{F}_q^N$.

2 Códigos Perfeitos em Espaços de Blocos Ordenados

Seja d uma métrica sobre V e C um subconjunto de V. O *raio de empacotamento* $R_d\,(C)$ de C é o maior inteiro positivo r tal que quaisquer duas bolas de raio r centradas em elementos distintos de C são disjuntas. Diremos que um código C é $R_d(C)$-*perfeito* se a união das bolas de raio $R_d(C)$ centradas nos elementos de C cobrem todo o espaço V. Neste trabalho classificaremos as métricas de blocos ordenados que tornam uma classe de códigos binários de Hamming estendidos códigos 1-perfeitos. Em particular, reobeteremos a classificação das métricas de blocos ordenados que tornam o código binário de Hamming estendido $[8;4;4]_H$ um código 1-perfeito (ver [1]) e, apresentaremos a classificação das métricas de blocos ordenados que tornam 1-perfeito o código binário de Hamming estendido $[16;11;4]_H$.

Seja C um $[N;k]$ código linear e $1 \leq r \leq N-k$. Começaremos exibindo uma família de métricas de blocos ordenados que tornam C um código r-perfeito.

Considere uma partição $[N] = A \cup B$ com $|A| = N-k$ e $|B| = k$. Agora considere uma partição de $[N]$ que refina $A \cup B$, particionando A em r partes, $1 \leq r \leq N-k$, isto é,

$$[N] = A_1 \cup \ldots \cup A_r \cup B_{r+1} \cup \ldots \cup B_n$$

com

$$A = A_1 \cup \ldots \cup A_r \text{ e } B = B_{r+1} \cup \ldots \cup B_n.$$

Seja $\Pi = \{A_1, \ldots, A_r, B_{r+1}, \ldots, B_n\}$ o conjunto dos blocos e $P = ([n], \leq)$ uma estrutura de ordem em Π tal que

$$A_i < B_j, \text{ para todo } i = 1, 2, \ldots, r \text{ e } j = r+1, \ldots, n.$$

Seja $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ o espaço dos blocos ordenados munido com a métrica $d_{(P,\Pi)}$.

Teorema 2.1. *Seja C um $[N;k]$ código linear e B um conjunto de informações de C. Então a estrutura de blocos ordenados (P,Π) sobre $V = \mathbb{F}_q^N$ torna C um código r-perfeito.*

Demonstração. Dado $0 \neq c \in C$,

$$c = c_1 + c_2 + \ldots + c_r + c_{r+1} + \ldots + c_n$$

com $c_i \in V_i$, $1 \leq i \leq n$, como B é um conjunto de informações de C, alguma das coordenadas não nulas de c estará contida em B, digamos em B_{j_0}. Como $B_j > A_i$ para todo $i = 1, 2 \ldots, r$, temos que $w_{(P,\Pi)}(c) \geq r+1$. Dado

$$x = x_1 + x_2 + \ldots + x_r + x_{r+1} + \ldots + x_n,$$

se

$$d_{(P,\Pi)}(c, x) \leq r,$$

então $c_j = x_j$ para cada $r+1 \leq j \leq n$ e, em particular $x_{j_0} \neq 0$. Daí que $w_{(P,\Pi)}(x) \geq r+1$ e, consequentemente

$$B_{(P,\Pi)}(0;r) \cap B_{(P,\Pi)}(c;r) = \varnothing.$$

Da estrutura de blocos ordenados, obtemos que

$$B_{(P,\Pi)}(0;r) = \left\{x \in \mathbb{F}_q^N : \langle supp(x) \rangle \subset A\right\} = \left\{x \in \mathbb{F}_q^N : supp(x) \subset A\right\} = V_1 \oplus \cdots \oplus V_r,$$

DOI: 10.5540/03.2018.006.01.0347

donde segue que

$$\left|B_{(P,\Pi)}\left(c;r\right)\right| = \left|B_{(P,\Pi)}\left(0;r\right)\right| = q^{|A|} = q^{N-k}.$$

Isto mostra que as q^k bolas disjuntas de raio r centradas nos elementos de C cobrem o espaço $\mathbb{F}_q^N$. Portanto C é r-perfeito. □

O próximo resultado, elementar, será utilizado na próxima seção. Seja $I^r_{(P,\pi)}$ o conjunto de todos os ideais de cardinalidade r em P.

Proposição 2.1. *Se $I^r_{(P,\pi)} = \{I\}$ e $i \in I$, então $i \leq j$ para todo $j \in P \backslash I$.*

Encerramos esta seção apresentando uma condição necessária para o empacotamento de esferas.

Proposição 2.2. *Seja $I^1_{(P,\pi)} = \{\{i_1\},\{i_2\},\ldots,\{i_r\}\}$ e $k_{i_j} = \pi\left(i_j\right)$ para cada $1 \leq j \leq r$. Se C é um $[N;k]$ código binário linear 1-perfeito, então*

$$2^{k_{i_1}} + 2^{k_{i_2}} + \ldots + 2^{k_{i_r}} = 2^{N-k} - 1 + r.$$

Demonstração. Note inicialmente que

$$\left|B_{(P,\pi)}\left(0;1\right)\right| = 1 + \sum_{j=1}^{r}\left(2^{k_{i_j}} - 1\right) = 1 - r + \sum_{j=1}^{r} 2^{k_{i_j}}.$$

Como C é 1-perfeito, $\left|B_{(P,\pi)}\left(0;1\right)\right| = 2^{N-k}$. Logo

$$2^{k_{i_1}} + 2^{k_{i_2}} + \ldots + 2^{k_{i_r}} = 2^{N-k} - 1 + r.$$

□

3 Códigos Binários de Hamming Estendidos Perfeitos

Seja $\mathcal{H}(m)$ o $[2^m; 2^m - 1 - m; 4]_H$ código binário de Hamming estendido (para maiores detalhes ver [4]). Nesta seção classificaremos as estruturas de blocos ordenados que tornam códigos 1-perfeitos uma classe de códigos binários de Hamming estendidos.

Seja $\mathbf{B} := \{supp(c) : c \in \mathcal{H}(m), w_H(c) = 4\}$ o conjunto dos suportes das palavras-código de $\mathcal{H}(m)$ de peso mínimo e $\mathbf{P} := [2^m]$. É bem conhecido na literatura especializada (ver [4]) que o par $(\mathbf{B},\mathbf{P})$ é um $3-(2^m,4,1)$ *projeto*, isto é, dado um subconjunto $X \subseteq \mathbf{P}$ com três elementos, existe um único bloco $supp(c) \in \mathbf{B}$ tal que $X \subseteq supp(c)$.

Teorema 3.1. *Considere a classe das estruturas de blocos ordenados (P,π) tal que*

$$I^1_{(P,\pi)} = \{\{1\},\{2\},\ldots,\{s\}\}$$

e

$$\sum_{i=i_0}^{s}\binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i\right),$$

onde

$$i_0 = \min\left\{i : 1 \leq i \leq s \text{ e } k_i = \pi(i) \geq 3\right\}.$$

Se (P,π) pertence a essa classe e $R_{d_{(P,\pi)}}(\mathcal{H}\left(m\right)) \geq 1$, então $|I^1_{(P,\pi)}| = 1$.

Demonstração. Mostraremos que se $s > 1$ e

$$\sum_{i=i_0}^{s} \binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i \right),$$

então $R_{d_{(P,\pi)}}(\mathcal{H}(m)) < 1$.

De fato, sejam $V_1, V_2, \ldots, V_s$ os blocos rotulados pelos elementos de $I^1_{(P,\pi)}$. A estrutura de $3-(2^m, 4, 1)$ projeto de $\mathcal{H}(m)$ garante que, para cada três coordenadas $\{x, y, z\}$ em algum V_i, com $i_0 \leq i \leq s$, existe $c \in \mathcal{H}(m)$ de peso mínimo tal que $\{x, y, z\} \in supp_H(c)$. Isto implica que o número total de vetores de peso mínimo com três coordenadas em algum V_i, com $i_0 \leq i \leq s$, é igual

$$\sum_{i=i_0}^{s} \binom{k_i}{3}.$$

O número de coordenadas no complementar de $V_1 \oplus \ldots \oplus V_s$ é igual a

$$2^m - \left(\sum_{i=1}^{s} k_i \right).$$

Se

$$\sum_{i=i_0}^{s} \binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i \right),$$

então existem $c, c' \in \mathcal{H}(m)$ tal que, $c \in V_{i_0} \oplus V_j$, $c' \in V_{i_0+1} \oplus V_j$ para algum $\{j\} \notin I^1_{(P,\pi)}$, com somente uma das coordenadas não nulas de c e c' em V_j. Disto concluímos que $w_H(c + c') = 6$ e as coordenadas não nulas de $c+c'$ estão em $V_{i_0} \oplus V_{i_0+1}$. Sejam $c'' = c+c'$ e u em $\mathbb{F}_2^{2^m}$ tal que $supp_H(u) = supp_H(c'') \cap [k_{i_0}]$. Então

$$u \in B_{(P,\pi)}(0; 1) \cap B_{(P,\pi)}(c''; 1),$$

e, consequentemente, o raio de empacotamento de $\mathcal{H}(m)$ é estritamente menor do que 1. □

Teorema 3.2. *Considere a classe das estruturas de blocos ordenados (P, π) tal que*

$$I^1_{(P,\pi)} = \{\{1\}, \{2\}, \ldots, \{s\}\}$$

e

$$\sum_{i=i_0}^{s} \binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i \right),$$

onde

$$i_0 = \min \{i : 1 \leq i \leq s \text{ e } k_i = \pi(i) \geq 3\}.$$

Uma estrutura de blocos ordenados (P, π) dessa classe torna o código binário de Hamming estendido $\mathcal{H}(m)$ um código 1-perfeito se, e somente se, $I^1_{(P,\pi)} = \{\{i\}\}$, $\pi(i) = m + 1$ e

$$\widehat{V} = V_1 \oplus \ldots \oplus V_{i-1} \oplus V_{i+1} \oplus \ldots \oplus V_n$$

é um conjunto de informações para $\mathcal{H}(m)$.

Demonstração. ($\Leftarrow$) Suponha que $I^1_{(P,\pi)} = \{\{i\}\}$, $\pi(i) = m+1$ e $\widehat{V} = V_1 \oplus \ldots \oplus V_{i-1} \oplus V_{i+1} \oplus \ldots \oplus V_n$ é um conjunto de informações para $\mathcal{H}(m)$. Como $I^1_{(P,\pi)} = \{\{i\}\}$, a Proposição 2.1 assegura que $i < j$ para todo $j \in [n] \setminus \{i\}$. Segue do Teorema 2.1 que $\mathcal{H}(m)$ é um código 1-perfeito.

($\Rightarrow$) Suponha agora que (P, π) é uma estrutura de blocos ordenados que satisfaz as condições do enunciado e que também torna $\mathcal{H}(m)$ um código 1-perfeito. Se existe um bloco V_i com $\{i\} \in I^1_{(P,\pi)}$ tal que $k_i > m+1$, então

$$\left|B_{(P,\pi)}(0;1)\right| \geq 1 + \left(2^{k_i} - 1\right) = 2^{k_i} > 2^{m+1},$$

e, consequentemente, $\mathcal{H}(m)$ não pode ser um código 1-perfeito, já que nesta condição

$$\left|B_{(P,\pi)}(0;1)\right| \cdot \mid \mathcal{H}(m) \mid \geq 2^{k_i} \cdot \mid \mathcal{H}(m) \mid > 2^{m+1} \cdot 2^{2^m-1-m} = 2^{2^m}.$$

Agora como $R_{d_{(P,\pi)}}(\mathcal{H}(m)) = 1$, segue do Teorema 3.1 que $\left|I^1_{(P,\pi)}\right| = 1$. Suponha que $I^1_{(P,\pi)} = \{\{i\}\}$. Já sabemos que $k_i \leq m+1$. Não podemos ter $k_i < m+1$, já que neste caso $\mathcal{H}(m)$ não é perfeito. Assim $k_i = m+1$ e V_i não pode conter nenhuma palavra-código c, caso contrário, $w_{(P,\pi)}(c) = 1$. □

4 Conclusões

A tabela abaixo apresenta várias soluções para a equação

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_s} = 2^m + s - 1 \tag{1}$$

quando $s = 3$, $s = 5$ e $3 \leq m \leq 6$. Como podemos observar, algumas destas soluções não satisfazem a condição

$$\sum_{i=i_0}^{s} \binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i\right), \tag{2}$$

e portanto não podem ser descartadas diretamente na demonstração do Teorema 3.2.

s	m	$(k_1, \ldots, k_s)$	$\sum_{i=i_0}^{s} \binom{k_i}{3}$	$2^m - (\sum_{i=1}^{s} k_i)$
3	3	$(1,3,3)$	2	1
3	4	$(1,4,4)$	8	7
3	5	$(1,5,5)$	20	21
3	6	$(1,6,6)$	40	51
5	4	$(3,3,3,3,2)$	4	2
5	5	$(4,4,4,4,2)$	16	14
5	6	$(5,5,5,5,2)$	40	42
5	4	$(4,3,3,1,1)$	6	4
5	5	$(5,4,4,1,1)$	18	17
5	6	$(6,5,5,1,1)$	40	46
5	5	$(5,4,4,3,2)$	19	13
5	6	$(6,5,5,4,2)$	44	42

A tabela abaixo mostra que para $m = 4$ todas as possíveis soluções de (1) satisfazem a condição (2). Portanto o Teorema 3.2 descreve todas as possíveis estruturas de blocos ordenados que fazem de $\mathcal{H}(4)$ um código 1-perfeito.

s	$\sum_{i=1}^{s} k_i$	$2^{4+1} + s - 1$	$(k_1, \ldots, k_s)$	$\sum_{i=i_0}^{s} \binom{k_i}{3}$	$2^4 - (\sum_{i=1}^{s} k_i)$
3	9	34	$(1, 4, 4)$	8	7
5	12	36	$(1, 1, 3, 3, 4)$	6	4
5	13	36	$(2, 2, 2, 3, 4)$	5	3
5	14	36	$(2, 3, 3, 3, 3)$	4	2
7	14	38	$(1_3, 2, 2, 3, 4)$	5	2
7	15	38	$(1, 2_5, 4)$	4	1
9	15	40	$(1_6, 2, 3, 4)$	5	1
11	15	42	$(1_{10}, 5)$	10	1

O caso $m = 3$ foi estudado em [1]. Para este caso, todas as possíveis soluções de (1) também satisfazem a condição (2).

Referências

[1] M. M .S. Alves, L. Panek and M. Firer, Error-block codes and poset metrics, *Advances in Mathematics of Communications*, 2:95-111, 2008.

[2] R. Brualdi, J. S. Graves and M. Lawrence, Codes with a poset metric, *Discrete Mathematics*, 147:57-72, 1995.

[3] K. Feng, L. Xu, F.J. Hickernell, Linear error-block codes, *Finite Fields and Their Applications*, 12:638-652, 2006.

[4] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, 1997.

