Trabalho apresentado no XXXVIII CNMAC, Campinas - SP, 2018.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos de Codimensão m como m-Perfeitos e Códigos Fortemente 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, introduzidas por Alves, Panek e Firer em 2008 [1], que tornam um código de codimensão m um código m-perfeito. Mostraremos também que os códigos MDS são os únicos códigos fortemente perfeitos em relação à estrutura de blocos ordenados (P, Π) introduzida em [7].

Palavras-chave. Códigos Lineares, Códigos Perfeitos, Métricas de Ordem, Métricas de Blocos, Métricas de Blocos Ordenados, Códigos Fortemente Perfeitos, Códigos MDS.

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, e escreveremos $k < j$, 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 subconjunto $X \subset [n]$, 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

$$\pi : [n] \to \mathbb{N} \tag{1}$$

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 finito $\mathbb{F}_q$ e V como sendo a soma direta dos espaços V_i:

$$V := V_1 \oplus V_2 \oplus \ldots \oplus V_n. \tag{2}$$

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

$$v = v_1 + v_2 + \ldots + v_n \tag{3}$$

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

DOI: 10.5540/03.2018.006.02.0263

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

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

$$supp(v) := \{i \in [n] : v_i \neq 0\}. \tag{4}$$

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

$$w_{(P,\pi)}(v) = |\langle supp(v) \rangle|, \tag{5}$$

onde $| X |$ 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

$$d_{(P,\pi)}(x, y) = w_{(P,\pi)}(x - y). \tag{6}$$

O conjunto

$$B_{(P,\pi)}(u; r) = \left\{v \in V : d_{(P,\pi)}(u, v) \leq r\right\} \tag{7}$$

é a *bola de centro* u *e raio* r. É possível mostrar que o número de elementos em uma bola 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

$$d_{(P,\pi)} = \min\left\{d_{(P,\pi)}\left(c, c'\right) : c \neq c' \in C\right\} \tag{8}$$

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

A (P, π)-distância, introduzida em [1] por Alves, Panek e Firer, 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 a condição $\pi(i) = 1$ 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 m-perfeito um código de codimensão m. Também determinaremos os códigos fortemente perfeitos relativos à estrutura de blocos ordenados (P, Π) introduzida em [7].

DOI: 10.5540/03.2018.006.02.0263

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,

$$[N] = A_1 \cup \ldots \cup A_r \cup B_{r+1} \cup \ldots \cup B_n \tag{9}$$

com

$$A = A_1 \cup \ldots \cup A_r \text{ e } B = B_{r+1} \cup \ldots \cup B_n. \tag{10}$$

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

$$A_i < B_j \text{ para todo } i = 1, 2, \ldots, r \text{ e } j = r+1, \ldots, n. \tag{11}$$

Seja $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ o espaço dos blocos ordenados munido com a métrica $d_{(P,\Pi)}$. Em [7] estabelecemos os seguintes resultados:

Teorema 2.1 (Teorema 2.1, [7])**.** *Seja C um $[N;k]$ código linear e B um conjunto de informações de C. Então a estrutura de blocos ordenados (P,Π) sobre $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ torna C um código r-perfeito.*

Seja $I^r_{(P,\pi)}$ o conjunto de todos os ideais de cardinalidade r em P.

Proposição 2.1 (Proposição 2.1, [7])**.** *Se $I^r_{(P,\pi)} = \{I\}$ e $i \in I$, então $i \leq j$ para todo $j \in P \backslash I$.*

3 Códigos de Codimensão m como m-Perfeitos

Nesta seção classificaremos todas as métricas de blocos ordenados que tornam um código de codimensão m um código m-perfeito. Começamos com um resultado auxiliar:

Teorema 3.1. *Seja C um $[N; N-m]$ código linear de codimensão m tal que $R_{d_{(P,\pi)}}(C) = m$. Então existe um único ideal $I \in I^m_{(P,\pi)}$ e $\dim(V_i) = 1$ para todo $i \in I$.*

Demonstração. A cada ideal $I \in I^m_{(P,\pi)}$ podemos associar q^m vetores com suporte em I. Estes vetores, por construção, estão na bola $B_{(P,\pi)}(\mathbf{0}, m)$. Sendo assim, se $|I^m_{(P,\pi)}| > 1$, então

$$\left|B_{(P,\pi)}(\mathbf{0}; m)\right| > q^m, \tag{12}$$

e daí que

$$|C| \cdot \left|B_{(P,\pi)}(\mathbf{0}; m)\right| > q^{N-m} \cdot q^m = q^N, \tag{13}$$

contrariando a hipótese de que $R_{d_{(P,\pi)}}(C) = m$. Logo $|I^m_{(P,\pi)}| = 1$.

Seja $I \in I^m_{(P,\pi)}$ o único ideal de cardinalidade m em P. Digamos que $I = \{1, \ldots, m\}$ e que $k_1 = \dim(V_1) > 1$. Então existem ao menos q^{k_1+m-1} vetores em $B_{(P,\pi)}(\mathbf{0}, m)$, e daí que

$$\left|B_{(P,\pi)}(\mathbf{0}; m)\right| \geq q^{k_1+m-1} > q^m, \tag{14}$$

contrariando novamente o fato de que $R_{d_{(P,\pi)}}(C) = m$. Portanto $\dim(V_i) = 1$ para todo $i \in I$. □

DOI: 10.5540/03.2018.006.02.0263

Agora estamos prontos para descrever todas as estruturas de blocos ordenados que tornam um código de codimensão m um código m-perfeito.

Teorema 3.2. *Seja C um $[N; N-m]$ código linear de codimensão m. Então C é m-perfeito se, e somente se:*

(i) $I^m_{(P,\pi)} = \{I\}$;

(ii) $\dim(V_i) = 1$ *para todo* $i \in I$;

(iii) $[N]\setminus I$ *é um conjunto de informações de* C.

Demonstração. ($\Leftarrow$) Suponha que $I^m_{(P,\pi)} = \{I\}$, $\dim(V_i) = 1$ para todo $i \in I$ e $[N]\setminus I$ é um conjunto de informações de C. A Proposição 2.1 assegura que $i < j$ para todo $i \in I$ e para todo $j \in P\setminus I$. O resultado segue do Teorema 2.1.

($\Rightarrow$) Suponha agora que C é m-perfeito. Então $R_{d_{(P,\pi)}}(C) = m$ e, como consequência do Teorema 3.1, $I^m_{(P,\pi)} = \{I\}$ e $\dim(V_i) = 1$ para todo $i \in I$. Se existirem palavras-código $c_1, c_2 \in C$ com $c_1 \neq c_2$ tal que $\mathrm{supp}_H(c_1 - c_2) \subseteq I$, então $d_{(P,\pi)}(c_1, c_2) \leq |I| = m$, o que implica que

$$B_{(P,\pi)}(c_1; m) \cap B_{(P,\pi)}(c_2; m) \neq \varnothing, \tag{15}$$

ou seja, C não é m-perfeito, uma contradição. Logo $[N]\setminus I$ é um conjunto de informações de C. □

4 Códigos Fortemente Perfeitos

Dois códigos são ditos *equivalentes* se um deles difere do outro por uma permutação de coordenadas. Duas estruturas de blocos ordenados (P, π) e (P', π') são ditas *equivalentes* se existir uma bijeção entre P e P' que preserva as dimensões dos blocos.

Se C é $R_{d_H}(C)$-perfeito e C' é equivalente a C, então é verdade que C' é também $R_{d_H}(C)$-perfeito. Em geral não é verdade que se C é $R_{d_{(P,\pi)}}(C)$-perfeito e C' é equivalente a C, então C' é também $R_{d_{(P,\pi)}}(C')$-perfeito. Diremos que C é $R_{d_{(P,\pi)}}(C)$-*fortemente perfeito* se todo código C' equivalente a C é também $R_{d_{(P,\pi)}}(C')$-perfeito. De forma equivalente, C será $R_{d_{(P,\pi)}}(C)$-fortemente perfeito se for $R_{d_{(P',\pi')}}(C)$-perfeito para toda estrutura de bloco (P', π') equivalente a (P, π). A noção de código fortemente perfeito foi introduzida inicialemnte em [4] com as métricas poset.

Um $[N, k]$ código C é dito MDS (em relação à métrica de Hamming d_H) se

$$d_H(C) = N - k + 1. \tag{16}$$

É bem conhecido na literatura especializada que um $[N; k]$ código C é MDS se, e somente se, todo conjunto de k coordenadas é um conjunto de informações de C (Corollary 3, Chapter 11, [6]). Este fato permite que classifiquemos os códigos fortemente perfeitos em relação a estrutura de blocos ordenados (P, Π) dada em (11):

Teorema 4.1. *Seja V munido com a métrica $d_{(P,\Pi)}$. Um código C é r-fortemente perfeito em V se, e somente se, C é um código MDS.*

DOI: 10.5540/03.2018.006.02.0263

Demonstração. Suponha que C é r-fortemente perfeito com a estrutura de blocos ordenados (P, Π) e C' é um código equivalente a C. Não podem existir $c'_1, c'_2 \in C'$ com $c'_1 \neq c'_2$ tal que $\mathrm{supp}_H(c'_1 - c'_2) \subseteq A$, pois caso contrário $d_{(P,\pi)}(c'_1, c'_2) \leq r$ e C' não seria r-perfeito. Isto implica todo conjunto de k coordenadas é um conjunto de informações de C, e daí que C é um código MDS.

Agora se C é MDS, então B será um conjunto de informações para todo código C' equivalente a C. O Teorema 2.1 assegura que C é r-fortemente perfeito. □

Se C é um $[N; k]$ código MDS, então $N - k = d_H(C) - 1$. Segue dos Teoremas 3.2 e 4.1 que:

Corolário 4.1. *Seja C um $[N; k]$ código MDS. Então C é $(d_H(C) - 1)$-fortemente perfeito se, e somente se, $I_{(P,\pi)}^{d_H(C)-1} = \{I\}$ e $\dim(V_i) = 1$ para todo $i \in I$.*

Como os códigos de Reed-Solomon são exemplos de códigos MDS:

Corolário 4.2. *Um $[q - 1; k]$ código de Reed-Solomon é $(q - k - 1)$-fortemente perfeito se, e somente se, $I_{(P,\pi)}^{q-k-1} = \{I\}$ e $\dim(V_i) = 1$ para todo $i \in I$.*

5 Conclusões

Se C é um $[N; k]$ código linear, então

$$0 \leq R_{d_{(P,\pi)}}(C) \leq N - k. \tag{17}$$

É conhecido na teoria dos códigos sobre as estruturas métricas de ordem (ou seja, quando a estrutura de blocos ordenados satisfaz a condição $\pi(i) = 1$ para todo i) que existem códigos nos quais nenhuma ordem parcial os torna r-perfeitos se $R_{d_H}(C) \leq r \leq N - k$: se C é o $[24; 12; 8]_H$ código binário de Golay, então C não admite uma estrutura métrica de ordem que torne C 5-perfeito (ver [5]).

Diferentemente do que acontece com as estruturas métricas de ordem, dado um $[N; k]$ código C e um inteiro $1 \leq r \leq N - k$, sempre existe uma estrutura de blocos ordenados que torna C r-perfeito (Terema 2.1). O Teorema 3.2 descreve todas as estruturas de blocos ordenados que tornam um código de codimensão m em m-perfeito. Considerando essa classificação e os resultados em [8], obtemos uma descrição completa das estruturas de blocos ordenados que tornam os códigos de Reed-Muller e simplex códigos 1-perfeitos e $(N - k)$-perfeitos. Restam ainda as classificações para os demais raios de empacotamento r com $1 < r < N - k$.

Referências

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

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

DOI: 10.5540/03.2018.006.02.0263

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

[4] J. Y. Hyun, H. K. Kim, The poset structures admitting the extended binary Hamming code to be a perfect code, *Discrete Mathematics*, 288:37-47, 2004.

[5] C. Jang, H. K. Kim, D. Y. Oh, Y. Rho, The poset structures admitting the extended binary Golay code to be a perfect code, *Discrete Mathematics*, 308:4057-4068, 2008.

[6] F. J. MacWilliams, N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland Mathematical Library, 1977.

[7] L. Panek, N. M. P. Panek, Códigos de Hamming Estendidos como Códigos Perfeitos, *Proceeding Series of the Brazilian Society of Applied and Computational Mathematics*, volume 6, número 1, 2018. DOI: 10.5540/03.2018.006.01.0347.

[8] L. Panek, N. M. P. Panek, Códigos de Reed-Muller e Simplex como Códigos Perfeitos, to appear.

