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

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos de Reed-Muller e Simplex 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. Seja $\mathcal{R}(m)$ um $\left[2^m; m+1; 2^{m-1}\right]_H$ código binário de Reed-Muller e $\mathcal{S}(m)$ um $\left[2^m-1; m; 2^{m-1}\right]_H$ código binário simplex. Neste trabalho classificaremos as métricas de blocos ordenados, introduzidas por Alves, Panek e Firer em 2008 [1], que tornam os códigos binários de Reed-Muller e simplex códigos 1-perfeitos.

Palavras-chave. Códigos Lineares, Códigos Perfeitos, Métricas de Ordem, Métricas de Blocos, Métricas de Blocos Ordenados, Códigos de Reed-Muller, Códigos Simplex.

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

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

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

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

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

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

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 $\mid X \mid$ 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

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

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 (ver [1]) 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 os códigos binários de Reed-Muller e simplex códigos 1-perfeitos.

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.

DOI: 10.5540/03.2018.006.02.0264

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 [5] estabelecemos o seguinte resultado:

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 $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ torna C um código 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 (ver [5]).

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

$$2^{k_{i_1}} + 2^{k_{i_2}} + \ldots + 2^{k_{i_r}} = 2^{N-k} - 1 + r. \tag{12}$$

3 Códigos Binários de Reed-Muller

Seja $\mathcal{R}(m)$ um $\left[2^m; m+1; 2^{m-1}\right]_H$ código binário de Reed-Muller (para maiores detalhes ver, [4]). Sabe-se que $\mathbf{1} \in \mathcal{R}(m)$ e todos os vetores de $\mathcal{R}(m)$, exceto as palavras-código $\mathbf{0}$ e $\mathbf{1}$, têm peso 2^{m-1}. Aqui $\mathbf{0}$ e $\mathbf{1}$ denotam o vetor nulo e a palavra $(1, 1, \ldots, 1)$ respectivamente.

Começamos descrevendo todas as possíveis estruturas de blocos ordenados que tornam $\mathcal{R}(m)$ um código 1-perfeito. O primeiro passo é estabelecer para quais casos valem a condição de empacotamento:

Lema 3.1. *Sejam $m > 3$ e $1 < r \leq 2^m$. Não existem inteiros positivos $k_1, k_2, \ldots, k_r$ tal que $k_1 + \ldots + k_r \leq 2^m$ e*

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} = 2^{2^m - 1 - m} - 1 + r. \tag{13}$$

Se $r = 1$, então $k = 2^m - 1 - m$ é a única solução para (13).

DOI: 10.5540/03.2018.006.02.0264

Demonstração. Dividiremos a prova da primeira parte do lema em três casos: o caso em que $2^m - 1 - m \leq k_i \leq 2^m$; o caso em que $m + 2 < k_i < 2^m - 1 - m$; e o caso em que $1 \leq k_i \leq m + 2$.

(1^o caso): Se $2^m - 1 - m \leq k_i \leq 2^m - 1$ para algum $1 \leq i \leq r$, então

$$\begin{aligned} 2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} &> 2^{2^m-1-m} + 2^0 + \ldots + 2^0 && (14) \\ &= 2^{2^m-1-m} + r - 1, && (15) \end{aligned}$$

donde segue o resultado.

(2^o caso): Suponha agora que $m + 2 < k_i < 2^m - 1 - m$ para todo $1 \leq i \leq r$. Então $k_1 = 2^m - l - m$ para algum $2 \leq l < 2^m - 2m - 2$, e como $k_1 + \ldots + k_r \leq 2^m$, segue que $k_2 + k_3 \ldots + k_r \leq m + l$. Daí que

$$\begin{aligned} 2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} &< 2^{k_1} + 2^{k_2+\ldots+k_r} && (16) \\ &\leq 2^{2^m-l-m} + 2^{m+l}. && (17) \end{aligned}$$

Como $l < 2^m - 2m - 2$, então $2^m - m - 1 > m + 1 + l$, o que implica que $2^m - m - 1 + l - 2 > m + 1 + 2l - 2$. Daí que $2^{l-2}2^{2^m-m-1} > 2^{m+2l-1}$, donde segue que $(2^{l-1} - 1)2^{2^m-m-1} > 2^{m+2l-1}$. Esta última desigualdade assegura que

$$\frac{(2^{l-1} - 1)}{2^{l-1}} 2^{2^m-m-1} > 2^{m+l}. \tag{18}$$

Consequentemente,

$$\frac{2^{2^m-m-1}}{2^{l-1}} + 2^{m+l} < 2^{2^m-m-1}, \tag{19}$$

ou seja,

$$2^{2^m-m-l} + 2^{m+l} < 2^{2^m-m-1}. \tag{20}$$

De (17) concluímos que

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} < 2^{2^m-l-m} + 2^{m+l} < 2^{2^m-m-1} + r - 1. \tag{21}$$

(3^o caso): Assuma agora que $1 \leq k_i \leq m + 2$. Então

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} \leq 2^{m+2} r \leq 2^{m+2} 2^m = 2^{2m+2}. \tag{22}$$

Note agora que $2m + 2 < 2^m - m - 1$, já que $2^m > 3m + 3$ se $m > 3$. Logo $2^{2m+2} < 2^{2^m-m-1}$, e portanto

$$2^{k_1} + 2^{k_2} + \ldots + 2^{k_r} \leq 2^{2m+2} < 2^{2^m-m-1} + r - 1. \tag{23}$$

É claro que se $r = 1$, então $k = 2^m - 1 - m$ é a única solução de (13). □

Teorema 3.1. *Seja $m \geq 3$, π um rótulo sobre $[n]$ tal que*

$$\pi(1) + \pi(2) + \ldots + \pi(n) = 2^m \tag{24}$$

e $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ com V_j isomorfo a $\mathbb{F}_2^{\pi(j)}$ para todo $j \in [n]$. Então uma ordem $P = ([n], \leq)$ torna o código binário de Reed-Muller $\mathcal{R}(m)$ um código 1-perfeito se, e somente se,

DOI: 10.5540/03.2018.006.02.0264

(i) $I^1_{(P,\pi)}(P) = \{\{i\}\}$;

(ii) $\pi(i) = 2^m - 1 - m$;

(iii) $\widehat{V} = V_1 \oplus \ldots \oplus V_{i-1} \oplus \widehat{V}_i \oplus V_{i+1} \oplus \ldots \oplus V_n$ *é um conjunto de informações para* $\mathcal{R}(m)$.

Demonstração. ($\Leftarrow$) Seja V_i como acima e suponha que $\widehat{V}$ é um conjunto de informações para $\mathcal{R}(m)$. A Proposição 2.1 assegura que $i < j$ para todo $j \in [n] \setminus \{i\}$, já que $I^1_{(P,\pi)} = \{\{i\}\}$. Segue agora do Teorema 2.1 que $\mathcal{R}(m)$ é um código 1-perfeito.

($\Rightarrow$) Assuma que (P, π) é uma estrutura de blocos ponderados que tornam $\mathcal{R}(m)$ um código 1-perfeito. Se existe um ideal minimal $\{i\} \in I^1_{(P,\pi)}$ tal que o correspondente bloco é de dimensão $k_i > 2^m - 1 - m$, então

$$\left|B_{(P,\pi)}(\mathbf{0}; 1)\right| \geq 1 + \left(2^{k_i} - 1\right) = 2^{k_i} > 2^{2^m - 1 - m} \tag{25}$$

e, consequentemente, $\mathcal{R}(m)$ não pode ser 1-perfeito, já que $\mathcal{R}(m)$ contém 2^{m+1} palavras-código comprimento 2^m e $2^{k_i} \cdot 2^{m+1} > 2^{2^m}$.

Suponha agora que $\left|I^1_{(P,\pi)}\right| = r$. Sejam $k_1, k_2, \ldots, k_r$ as correspondentes dimensões dos blocos rotulados pelos elementos do conjunto $I^1_{(P,\pi)}$. Como o código é 1-perfeito, temos da Proposição 2.2 que

$$2^{k_1} + \ldots + 2^{k_r} = 2^{2^m - 1 - m} - 1 + r. \tag{26}$$

Se $m > 3$, segue do Lema 3.1 que a equação em (26) só admitirá solução se $r = 1$. Para $r = 1$ a única solução é $k_i = 2^m - 1 - m$. O caso $m = 3$ é descartado em [1] (Theorem 3.3).

Como $k_i = 2^m - 1 - m$, concluímos que V_i não pode conter nenhuma palavra-código $c \in \mathcal{R}(m)$, caso contrário $d_{(P,\pi)}(\mathbf{0}, c) = 1$. Portanto $\widehat{V}$ é um conjunto de informações para $\mathcal{R}(m)$. □

Agora seja $\mathcal{S}(m)$ um $\left[2^m - 1; m; 2^{m-1}\right]_H$ código binário simplex (para maiores detalhes ver, [4]). Sabe-se que todos os vetores não nulos de $\mathcal{R}(m)$ têm peso constante igual a 2^{m-1}.

Considerando o fato de que $N - k$ é igual para ambos os códigos $\mathcal{R}(m)$ e $\mathcal{S}(m)$,

$$N - k = 2^m - 1 - m, \tag{27}$$

e que os argumentos do Lema 3.1 e do Teorema 3.1 dependem somente de $N - k$ e do fato de que $k_1 + \ldots + k_r \leq 2^m$, obtemos que:

Corolário 3.1. *Seja* $m > 3$, π *um rótulo sobre* $[n]$ *tal que*

$$\pi(1) + \pi(2) + \ldots + \pi(n) = 2^m - 1 \tag{28}$$

e $V = V_1 \oplus V_2 \oplus \ldots \oplus V_n$ *com* V_j *isomorfo a* $\mathbb{F}_2^{\pi(j)}$ *para todo* $j \in [n]$. *Então uma ordem* $P = ([n], \leq)$ *torna o código binário simplex* $\mathcal{S}(m)$ *um código* 1*-perfeito se, e somente se, as condições* (i), (ii) *e* (iii) *do Teorema 3.1 são satisfeitas.*

DOI: 10.5540/03.2018.006.02.0264

4 Conclusões

Em [5] os autores apresentam uma classificação parcial das estruturas de blocos ordenados que tornam o código binário de Hamming estendido $\mathcal{H}(m)$ um código 1-perfeito: são classificadas apenas as estruturas de blocos ordenados tal que se

$$I^1_{(P,\pi)} = \{\{1\}, \{2\}, \ldots, \{s\}\}, \tag{29}$$

então

$$\sum_{i=i_0}^{s} \binom{k_i}{3} > 2^m - \left(\sum_{i=1}^{s} k_i\right) \tag{30}$$

onde

$$i_0 = \min\{i : 1 \leq i \leq s \text{ e } k_i = \pi(i) \geq 3\}. \tag{31}$$

Neste trabalho descrevemos *todas* as estruturas de blocos ordenados que tornam o código binário de Reed-Muller 1-perfeito. Como é bem conhecido na literatura especializada que o código binário de Reed-Muller é o dual do código binário de Hamming estendido $\mathcal{H}(m)$, podemos considerar o seguinte problema: é possível descrever todas as estruturas de blocos ordenados que tornam $\mathcal{H}(m)$ perfeito a apartir das estruturas de blocos ordenados que tornam $\mathcal{R}(m)$ perfeito? Ou de forma mais geral: existe uma relação entre as estruturas de blocos ordenados que tornam um código perfeito com as que tornam o seu dual perfeito?

Uma resposta positiva para a questão acima implicará na classificação completa das estruturas de blocos ordenados que tornam o código binário de Hamming estendido 1-perfeito, já que neste trabalho descrevemos todas as possíveis estruturas que tornam o seu dual 1-perfeito.

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, 1977.

[5] L. Panek and 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.

