Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 8, n. 1, 2021.

Trabalho apresentado no XL CNMAC, Evento Virtual - Co-organizado pela Universidade do Mato Grosso do Sul (UFMS).

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos Perfeitos e Raio de Empacotamento

Raphael C. S. Souza[1]
DM-ICE-UFJF, Juiz de Fora, MG
Beatriz C. M. Ribeiro[2]
DM-ICE-UFJF, Juiz de Fora, MG

Fixado um corpo finito $\mathbb{F}_q$, um $(n; M)$ código $\mathcal{C}$ sobre $\mathbb{F}_q$ é um subconjunto de $\mathbb{F}_q^n$ com M elementos. Dizemos que $\mathcal{C} \subset \mathbb{F}_q^n$ é um $[n; k]$ código linear sobre $\mathbb{F}_q$ se $\mathcal{C}$ for um subespaço vetorial de dimensão k de $\mathbb{F}_q^n$. Os vetores em C são ditos as palavras do código.

Um importante conceito da teoria de códigos é o do raio de empacotamento $R_e(C)$, que é o raio máximo que permite cobrir o espaço em que o código está contido com bolas $B(v; R_e(C))$ disjuntas centradas nas palavras do código. Formalmente, o raio de empacotamento é

$$R_e(\mathcal{C}) = \max\{r \in \mathbb{N} \ : \ B(v; r) \cap B(w; r) = \emptyset \, , \forall v, w \in \mathcal{C}, \, v \neq w\} \, .$$

Definimos a distância de Hamming entre duas palavras $x, y \in \mathbb{F}_q^n$ com $x = (x_1, x_2, \ldots, x_n)$ e $y = (y_1, y_2, \ldots, y_n)$, como sendo

$$d_H(x, y) = \#\{i \ : \ x_i - y_i \neq 0, \ i = 1, 2, \ldots, n\} \, .$$

Definimos, ainda, o peso de Hamming de x como

$$\omega_H(x) = d_H(x, 0) \, .$$

Quando utilizamos a métrica de Hamming, o conceito de raio de empacotamento é ofuscado pelo conceito de distância mínima pois tal raio pode ser totalmente determinado por ela. Isto é, dado um código $\mathcal{C}$ e sua distância mínima $d_H(\mathcal{C})$ sob a métrica de Hamming, sabemos que o raio de empacotamento de $\mathcal{C}$ é

$$R_e(\mathcal{C}) = \left\lfloor \frac{d_H(\mathcal{C}) - 1}{2} \right\rfloor .$$

Dizemos que um código linear $\mathcal{C} \subset \mathbb{F}_p^n$ é um código perfeito se

$$\bigcup_{u \in \mathcal{C}} B(u; R_e(\mathcal{C})) = \mathbb{F}_p^n \quad \text{e} \quad B(u; R_e(\mathcal{C})) \cap B(v; R_e(\mathcal{C})) = \emptyset$$

quaisquer que sejam $u, v \in \mathcal{C}$ com $u \neq v$.

Notamos que a definição de código perfeito implica que o empacotamento em esferas centradas nas palavras do código é máximo no sentido que cobre todo o espaço. Isto é, códigos perfeitos são mais eficientes: os erros sempre produzem palavras que não se distanciam demais das palavras do código, possibilitando a identificação e correção, propiciando mais confidencialidade, integridade e autenticidade à mensagem.

[1] raphaelcascelli@hotmail.com
[2] beatriz@ice.ufjf.br

Agora, definimos os chamados códigos de Hamming como a seguir. Sejam $n = 2^r - 1$, com $r \geq 2$, e H_r a matriz de ordem $r \times (2^r - 1)$ cujas colunas são todos os vetores não nulos de $\mathbb{F}_2^r$.

O código linear

$$\mathcal{H}_r = \{x \in \mathbb{F}_2^{2^r-1} \ : \ H_r \cdot x^t = 0\}$$

que tem H_r como matriz de verificação de paridade, é chamado de Código de Hamming. Uma matriz de verificação de paridade de um dado código $\mathcal{C}$ é a representação matricial dos coeficientes do sistema linear tal que a solução é o próprio código $\mathcal{C}$. Assim, temos que $\mathcal{H}_r$ é um $[2^r-1; 2^r-r-1]$ código linear.

No decorrer do trabalho, mostramos que um código de Hamming $\mathcal{H}_r$ tem distância mínima igual a 3. Dessa forma, $R_e(\mathcal{H}_r) = 1$. Além disso, o código de Hamming $\mathcal{H}_r$ é um código perfeito considerando a métrica de Hamming. Para demonstrar esse resultado basta mostrar que as bolas unitárias em torno dos elementos do código contemplam todos os pontos de $\mathbb{F}_2^{2^r-1}$.

Além disso, buscamos encontrar o raio de empacotamento de códigos em que as métricas utilizadas são regidas por ordens parciais, as quais chamamos de métricas ponderadas (*posets*). Dada uma ordem parcial P no conjunto $[n] = \{1, 2, \ldots, n\}$ definimos o P-peso ponderado de x como sendo a cardinalidade do ideal gerado pelo suporte de x

$$\omega_P(x) = \#(\langle \text{supp}(x) \rangle) \, ,$$

onde o suporte de x é o conjunto de coordenadas não nulas de x.

Uma propriedade interessante dessas métricas é que o raio de empacotamento não é necessariamente determinado pela distância mínima. E ainda, a distância ponderada por esta ordem P, em alguns casos, é mais eficiente que a métrica de Hamming. Desta maneira, podemos utilizar essas métricas para nos fornecer uma vasta gama de códigos perfeitos. Exemplificando, considerando o conjunto $[n]$ totalmente ordenado, se $\mathcal{C} \subset \mathbb{F}_q^n$ é um código com distância mínima $d_P(\mathcal{C})$, então $\mathcal{C}$ tem a capacidade de corrigir $d_P - 1$ erros.

Por fim, podemos nos perguntar: será que dado qualquer código existe uma métrica de forma que o código seja perfeito? Essa pergunta, dentre outras, indica que ainda há campo para continuar o estudo aqui proposto. O autor, sob orientação da autora, desenvolveu este trabalho como pesquisa de iniciação cientifica o qual foi apresentado no Seminário de Iniciação Científica (SEMIC) da UFJF e em seguida como Trabalho de Conclusão do Curso de Matemática, ambos no ano de 2019.

Referências

[1] D'Oliveira, R. G. L. Raio de Empacotamento de Códigos Poset, Dissertação de Mestrado, Unicamp, 2012.

[2] Firer, M. Códigos Corretores de Erros - Notas de Aula. Disponível em: https://www.ime.unicamp.br/ mfirer/3NotasFoz2006.pdf. Acesso em: 29 de março de 2019.

[3] Hefez, A., Villela, M. L. T. *Códigos Corretores de Erros, 2a. edição*. IMPA, Rio de Janeiro, 2008.

[4] Huffman, W. C., Pless, V. *Fundamentals of Error-Correcting Codes*. Cambridge University Press, Cambridge, 2003.

[5] Miles, C. P. Breve Introdução à Teoria dos Códigos Corretores de Erros, *Colóquio de Matemática da Região Centro-Oeste*, 2009. Disponível em: https://www.sbm.org.br/docs/coloquios/CO-1-09.pdf. Acesso em: 29 de março de 2019.

[6] Moura, A. Dualidade em Espaços Poset, Tese de Doutorado, Unicamp, 2010.