Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 7, n. 1, 2020.

Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Uma prova da Conjectura de Golomb-Welch para códigos lineares em $\mathbb{Z}^n$ com $7 \leq n \leq 12$ e raio 2

Lucas Eduardo Nogueira Gonçalves[1]
Instituto de Ciência e Tecnologia, Unifesp, São José dos Campos, SP
Grasiele Cristiane Jorge[2]
Instituto de Ciência e Tecnologia, Unifesp, São José dos Campos, SP

1 Introdução

Dados um alfabeto A (finito ou infinito) e $n \in \mathbb{N}$, um código é um subconjunto de A^n. Fixada uma métrica em A^n, o raio de empacotamento de um código é o maior raio k tal que ao traçarmos esferas com este raio ao redor de todas as palavras do código, estas esferas não se intersectam. Um código é dito perfeito se a união das esferas centradas nas palavras do código e com raio igual ao raio de empacotamento resultar no espaço todo.

A teoria dos códigos corretores de erros, propriamente dita, surgiu na década de 40 com os trabalhos de Golay, Hamming e Shannon, onde os autores consideraram códigos na então denominada métrica de Hamming [3]. A métrica de Lee foi introduzida 1958 em [7] considerando o alfabeto A como o anel de inteiros módulo p, $\mathbb{Z}_p$, com p primo. Depois, em 1968 ela foi generalizada para $\mathbb{Z}_q$, com $q \geq 2$ natural [2]. Em certos canais tal métrica mostrou-se mais adequada do que a de Hamming [1].

Códigos lineares em $\mathbb{Z}_q^n$, ou seja, subgrupos aditivos de $\mathbb{Z}_q^n$, podem ser "levantados" para códigos lineares em $\mathbb{Z}^n$ via a imagem inversa da aplicação projeção $\phi : \mathbb{Z}^n \longrightarrow \mathbb{Z}_q^n$ tal que $\phi(x_1, \ldots, x_n) = (\overline{x_1}, \ldots, \overline{x_n})$. Por conta desta relação, temos que para q suficientemente grande códigos lineares perfeitos em $\mathbb{Z}_q^n$ na métrica de Lee estão associados a códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica da soma [6, Proposição 1].

Em [2] foi enunciada a famosa Conjectura de Golomb-Welch, que afirma que não existem códigos perfeitos em $\mathbb{Z}_q^n$ na métrica de Lee para qualquer dimensão $n \geq 3$, qualquer raio $r > 1$ e q grande. Na Seção 7 de [2], a conjectura foi reformulada para $\mathbb{Z}^n$ e diz que não existem códigos perfeitos em $\mathbb{Z}^n$ na métrica da soma para qualquer dimensão $n \geq 3$ e qualquer raio $r > 1$. Esta conjectura completou 50 anos do seu enunciado em 2018 e embora existam vários resultados parciais relacionados a ela, acredita-se que ela ainda está longe de ser demonstrada [6]. Os resultados parciais obtidos foram provenientes de diferentes técnicas e devido às limitações computacionais não puderam ser estendidos para outros casos.

[1]lucasedng@gmail.com
[2]grasiele.jorge@unifesp.br

2 Códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica da soma para raio 2

Sejam V um subconjunto de $\mathbb{Z}^n$ e $\mathcal{T} = \{V + l;\ l \in \mathcal{L}\}$, onde $\mathcal{L} \subset \mathbb{Z}^n$. O conjunto $\mathcal{T}$ é chamado ladrilhamento de $\mathbb{Z}^n$ se $(V + l_1) \cap (V + l_2) = \emptyset$ se $l_1 \neq l_2$ e $\bigcup_{l \in L}(V + l) = \mathbb{Z}^n$. Em [4] é provado que existe um ladrilhamento de $\mathbb{Z}^n$ por V com $\mathcal{L}$ um código linear de $\mathbb{Z}^n$ se, e somente se, existe um grupo abeliano G de ordem $|V|$ e um homomorfismo $\phi : \mathbb{Z}^n \to G$ tal que a restrição de ϕ a V é uma bijeção.

Quando consideramos códigos perfeitos em $\mathbb{Z}^n$ na métrica da soma, tomamos V como a esfera de raio r centrada na origem. Em [5] é apresentado um algoritmo que verifica se existem homomorfismos de $\mathbb{Z}^n$ em grupos abelianos cuja cardinalidade seja a cardinalidade da esfera na métrica da soma centrada na origem com raio 2. Devido à limitações computacionais foi possível demonstrar que não existem tais homomorfismos, ou seja, códigos lineares perfeitos em $\mathbb{Z}^n$ na métrica da soma apenas para $n \leq 12$. Neste trabalho, vamos apresentar a teoria envolvida no detalhamento de tal algoritmo. Em [5] foi considerado apenas $7 \leq n \leq 12$, pois para $3 \leq n < 7$ e raio 2 o resultado já havia sido demonstrado com outra técnica.

Agradecimentos

Agradecemos ao CNPq, processo 432735/2016-0, pelo auxílio financeiro.

Referências

[1] J. C. Chiang. On channels and codes for the Lee metric, *Information and Control*, volume 19, No. 2, p. 159-173, 1971.

[2] S. W. Golomb and L. R. Welch. Perfect codes in the Lee metric and the packing of polyominoes, *SIAM Journal on Applied Mathematics*, volume 18, No. 2, p. 302-317, 1970.

[3] R. W. Hamming. Error detecting and error correcting codes, *Bell System Technical Journal*, volume 29, No. 2, p. 147-160, 1950.

[4] P. Horak, F. Albdaiwi, *Diameter perfect Lee codes*, IEEE Transactions on Information Theory, volume 58, No. 8, p. 5490-5499, 2012.

[5] P. Horak and O. Grosek. A new approach towards the Golomb-Welch conjecture, *European Journal of Combinatorics*, volume 38, p. 12-22, 2014.

[6] P. Horak and D. Kim, 50 Years of the Golomb-Welch Conjecture, *IEEE Transactions on Information Theory*, volume 64, No. 4, p. 3048-3061, 2018.

[7] C. Y. Lee. Some properties of nonbinary error-correcting codes, *IRE Transactions on Information Theory*, volume 4, No. 2, p. 77-82, 1958.