Os avanços na Conjectura de Golomb-Welch nos 50 anos desde sua postulação

Roberta Ribeiro[1] & Grasiele Jorge[2]

ICT UNIFESP - São José dos Campos, SP

[1]ranribeiro@unifesp.br, [2]grasiele.jorge@unifesp.br

Resumo

A conjectura de Golomb-Welch lida com a não-existência de códigos perfeitos na métrica de Lee em $\mathbb{Z}^n$ para $n \geq 3$ e raio de empacotamento $r \geq 2$. Postulada há mais de 50 anos e figurando como um dos principais incentivos na área de códigos perfeitos, a conjectura ainda está em aberto.

Introdução

Denotaremos por $S_{n,r}$ a esfera de Lee de raio r centrada na origem, ou seja, $S_{n,r} = \{x; d(0,x) \leq r\}$. Seja V um subconjunto de $\mathbb{Z}^n$, uma cópia de V significa uma translação $V+x = \{v+x, v \in V\}$ de V, onde $x \in \mathbb{Z}^n$. Uma coleção $\mathcal{T} = \{V+l; l \in \mathcal{L}\}, \mathcal{L} \subset \mathbb{Z}^n$, de cópias de V constitui um ladrilhamento de $\mathbb{Z}^n$ por V se $\mathcal{T}$ forma uma partição de $\mathbb{Z}^n$. Um conjunto $\mathcal{L}$ é um código perfeito em $\mathbb{Z}^n$ com capacidade de correção de r erros se, e somente se, $\{S_{n,r} + l; l \in \mathcal{L}\}$ for um ladrilhamento de $\mathbb{Z}^n$ por esferas de Lee $S_{n,r}$. Se $\mathcal{L}$ for um reticulado, então $\mathcal{L}$ será um código linear.

Resultados

Teorema. *[1] Existem códigos perfeitos na métrica de Lee para $n = 2$ e $r > 0$ e $n \geq 2$ e $r = 1$.*

Conjectura (Golomb-Welch [1])**.** *As esferas de Lee $S_{n,r}$ não ladrilham perfeitamente o espaço $\mathbb{Z}^n$, para $n \geq 3$ e $r \geq 2$.*

A conjectura afirma que não existem códigos perfeitos em $\mathbb{Z}^n$ corrigindo r erros, para $n \geq 3$ e $r \geq 2$.

A despeito da literatura prolífica abordando este tópico e da conjectura ser acreditada como verdadeira, ela ainda não foi provada. A seguir listamos alguns resultados importantes obtidos nesses 50 anos:

- Não existem códigos perfeitos para $n > 4$ e $r > r_n$, onde r_n é um parâmetro que depende da eficiência de empacotamento no espaço euclidiano n-dimensional [1];
- A conjectura é verdadeira para $n = 3, 4, 5$ [2];
- Não existem códigos lineares perfeitos com raio $r = 2$ para uma quantidade infinita de dimensões [4].

Estes resultados utilizam diversas ferramentas – como programas computacionais – e abordagens de diferentes áreas da matemática. Uma técnica que tem sido muito relevante nos estudos envolvendo a conjectura utiliza um invariante relacionado com grupos abelianos finitos a partir da existência de homomorfismos especiais de $\mathbb{Z}^n$ a esses grupos, apresentada em [3]. Nesta última abordagem, o teorema a seguir figura como um dos principais resultados utilizados:

Teorema 1. *Seja V um subconjunto de $\mathbb{Z}^n$. Existe então um ladrilhamento reticulado de $\mathbb{Z}^n$ por V 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.*

Demonstração. Suponha $T = \{V + l; l \in L\}$ um ladrilhamento reticulado de $\mathbb{Z}^n$ por V. Sejam o grupo quociente $G = \mathbb{Z}^n/L$ e a aplicação $\phi : \mathbb{Z}^n \to G$, dada por $\phi(x) = [x]$, onde $[x]$ é a classe lateral em $\mathbb{Z}^n/L$ que contém x. Dois elementos $x, y \in \mathbb{Z}^n$ pertencem à mesma classe lateral de $\mathbb{Z}^n/L$ se, e somente se, $x - y \in L$. Para uma contradição, suponha que existem $x, y \in V$, com $x \neq y$, tal que $\phi(x) = \phi(y)$. Como $\phi(x) = \phi(y) \Rightarrow x - y \in L$, x e y pertencem à mesma classe lateral em $\mathbb{Z}^n/L$. Seja $x - y = l \in L, l \neq 0$, então $x \in V + (x - y) = V + l$. Como $l \neq 0$, $V + l \neq V$, assim $x \in V \cap (V + l)$, uma contradição. Suponha agora que existe $[x] \in \mathbb{Z}^n/L$ tal que não existe $[v] \in V$ com $[v] = [x]$. Assim, $v - x \notin L, \forall v \in V$ e $x \notin V + l, \forall l \in L$, então $\exists x \in \mathbb{Z}^n$ tal que $x \notin \bigcup_{l \in L}(V + l)$, uma contradição. Como $\phi : V \to G$ é bijetora, a ordem de G é igual a $|V|$.

Para provar a recíproca, seja G um grupo abeliano de ordem $|V|$ e seja $\phi : \mathbb{Z}^n \to G$ um homomorfismo tal que a restrição de ϕ a V seja uma bijeção. Sendo $\text{Ker}(\phi) = L, \mathbb{Z}^n/L \cong G$. Suponha que existe $x \in \mathbb{Z}^n$ tal que $x \notin \bigcup_{l \in L}(V + l)$. Seja $\phi(x) = g$. Existe $y \in V$ tal que $\phi(y) = g$. Assim, $\phi(x) = \phi(y) \Rightarrow x - y = l \in L$, ou seja, x e y pertencem à mesma classe lateral em $\mathbb{Z}^n/L$. Como $y \in V$, então $x \in V + l, l \in L$, uma contradição. Portanto, $\bigcup_{l \in L}(V + l) = \mathbb{Z}^n$. Suponha agora que existem $l, l_0 \in L; l \neq l_0$ e $x \in \mathbb{Z}^n$ tal que $x \in (V+l) \cap (V+l_0)$. Assim, $x = y + l$ e $x = y_0 + l_0$ para $y, y_0 \in V$ com $y \neq y_0$. Assim, $y + l = y_0 + l_0 \Rightarrow y - y_0 = l_0 - l \in L$. No entanto, $y - y_0 \in L$ implica que $\phi(y - y_0) = 0$, ou seja, $\phi(y) = \phi(y_0)$, o que contradiz ϕ ser bijeção em V. Logo, $(V + l) \cap (V + l_0) = \emptyset$, para quaisquer $l, l_0 \in L$ com $l \neq l_0$. Portanto $T = \{V + l; l \in L\}$ é um ladrilhamento reticulado de $\mathbb{Z}^n$ por V. □

O invariante mencionado relaciona as distâncias de Lee mínimas da origem até os elementos de dado grupo abeliano sob a ação de todos os possíveis homomorfismos, e é invariante quanto a grupos isomorfos. A partir disso, [3] utilizou o resultado acima para mapear homomorfismos de ordem igual ao número de pontos contidos em esferas de Lee, relacionando-o com a Conjectura de Golomb-Welch e provando o seguinte teorema:

Teorema. *[3] Não existe código linear perfeito na métrica de Lee em $\mathbb{Z}^n$ com $r = 2$ e $7 \leq n \leq 12$.*

Conclusão

Apesar desses resultados em direção à veracidade da conjectura, ela ainda está longe de ser provada. Em uma tentativa de abordar o problema de formas que possibilitem novas ideias e recursos para sua resolução, pesquisadores têm ampliado as áreas de pesquisa. Algumas das alternativas abrangem o estudo dos códigos *quasi*-perfeitos e dos códigos perfeitos em outras métricas. Nesse sentido, destacamos os resultados:

- Para cada $n \geq 3$ existem infinitos valores de r que garantem a existência de códigos *quasi*-perfeitos na métrica de Lee em $\mathbb{Z}^n$ [3];
- Não existem códigos lineares perfeitos na métrica ℓ_p para $1 \leq p \leq \infty$ com $r = 2^{\frac{1}{p}}, 3^{\frac{1}{p}}$ [5].

Referências

[1] S. W. Golomb, L. R. Welch, *Perfect codes in the Lee metric and the packing of polyominoes*, *IEEE Transactions on Information Theory*, 18(2), 302-317, 1970.

[2] P. Horak, *Tilings in Lee Metric*, *European Journal of Combinatorics*, 30, 480-489, 2009.

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

[4] C. Qureshi, A. Campello and S. I. R. Costa, *Non-Existence of Linear Perfect Lee Codes With Radius 2 for Infinitely Many Dimensions*, *IEEE Transactions on Information Theory*, 64(4), 3042-3047, 2018.

[5] T. Zhang, G. Ge, *Perfect and Quasi-Perfect Codes under the l_p Metric*, *SIAM Journal on Applied Mathematics*, 63(7), 4325-4331, 2017.

Agradecimentos

Agradecemos à CAPES e ao Comitê Organizador do 34º Colóquio Brasileiro de Matemática pelo auxílio financeiro.