XI Bienal de Matemática 2024
Universidade Federal de São Carlos - UFSCar
29 de julho a 02 de agosto de 2024

Códigos e Reticulados

TOLEZANO, Matheus[1]; MARTINS, Victor[2]

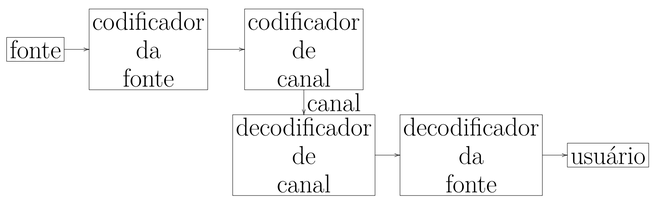
Resumo: *Apresentamos os códigos corretores de erros sob o ponto de vista algébrico, demonstrando os benefícios de se mesclar códigos e estruturas algébricas: melhores e mais sofisticados algoritmos de codificação e decodificação de erros. Visamos estudar elementos geométricos envolvidos na teoria de códigos e assim utilizar toda a base algébrica mesclada a uma visualização geométrica de alguns importantes conceitos. Com isso, nosso objetivo principal é fazer um estudo dos reticulados, que são subgrupos aditivos do espaço euclidiano n – dimensional e tentar compreender sua relação com a teoria de códigos.*

Palavras-chave: *Códigos algébricos, códigos geométricos, reticulados, Teoria da informação.*

1. Introdução

Os códigos participam do nosso cotidiano de inúmeras formas, estando presente sempre que fazemos o uso de informações digitalizadas, por exemplo, ao assistirmos um programa de televisão, falar ao telefone, mandar mensagem para alguém via pager e até mesmo ao navegarmos pela internet. Um código é um modo organizado de transmitir ou armazenar informações, que permita, ao recuperar a informação, detectar e corrigir erros.

Um exemplo clássico de um código corretor de erro é um idioma. Para entendê-lo, vamos analisar a seguinte situação: se uma mensagem de texto é recebida com a palavra **LIÃO**, é possível detectar o erro rapidamente pois a palavra não existe no idioma. Com isso, a palavra é corrigida para **LEÃO**, que é a palavra "mais próxima" e, neste caso, foi possível corrigir o erro. Entretanto, se a mensagem recebida é **ZEIA**, é possível detectar o erro, mas não é possível corrigi-lo, pois existem muitas palavras no idioma que estão próximas dela. E ainda, existe o caso em que não é possível detectar o erro. Se recebermos a palavra **VISTA**, quando na verdade a mensagem original é **MISTA**, é impossível a correção, já que **VISTA** é uma palavra do idioma. A figura abaixo ilustra o processo de detecção e correção de erros.



2. Códigos Lineares

Para a construção de um código corretor de erro, é necessário um conjunto finito A que chamaremos de *alfabeto*. A classe mais utilizada na prática é a chamada classe dos códigos lineares. Neste caso, nosso alfabeto será um corpo finito $\mathbb{K}$. E um código $C \subset \mathbb{K}^n$ será chamado de **código linear** se for um subespaço vetorial próprio de $\mathbb{K}^n$.

Para que seja possível a detecção de erros, precisamos de uma maneira de medir a distância entre essas palavras no alfabeto.

Definição 3.1 *Dados dois elementos $u, v \in \mathbb{K}^n$, a distância de Hamming entre u e v é definida como*

$$d(u,v) = |\{i;\ u_i \neq v_i, 1 \leq i \leq n\}|.$$

Por exemplo, em $\{0,1\}^3$, temos

$$d(001,111) = 2$$
$$d(000,111) = 3$$
$$d(100,110) = 1$$

Se C é um código, a **distância mínima** de C é o número

$$d = min\{d(u,v);\ u,v \in C \text{ e } u \neq v\}.$$

Teorema 3.1 *Seja C um código com distância mínima d. Então C pode corrigir até $\kappa = \left[\frac{d-1}{2}\right]$ erros e detectar até $d-1$ erros.*

Um código C possui três parâmetros fundamentais $[n, M, d]$ sendo eles, respectivamente, seu comprimento, número de elementos e distância mínima.

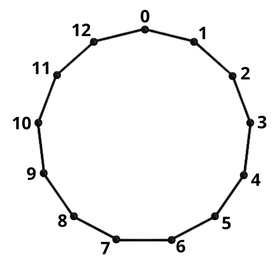
3. Códigos q-ários: A distância de Lee

Chamamos códigos q-ários os que têm por alfabeto o anel $\mathbb{Z}_q$ dos inteiros módulo q. Em função da tecnologia computacional atualmente, os códigos em uso são os binários. Outros códigos são usados em etapas intermediárias e posteriormente convertidos em binários.

A distância de Lee, ou métrica de Lee é uma outra noção de distância que pode ser definida em $\mathbb{Z}_q$ e $\mathbb{Z}_q^n$. Dados $\overline{a}$ e $\overline{b} \in \mathbb{Z}_q$, definimos:

$$d_{Lee}(\overline{a}, \overline{b}) = min\{|a-b|, q-|a-b|\}$$

Assim, por exemplo, em $\mathbb{Z}_{13}$, $d_{Lee}(\overline{1}, \overline{4}) = 3$. A figura abaixo ilustra uma representação geométrica de $\mathbb{Z}_{13}$ com a distância de Lee.



A distância de Lee em $\mathbb{Z}_q^n$ é definida como a soma das distâncias nas coordenadas:

$$d_{Lee}((\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}), (\overline{b_1}, \overline{b_2}, \ldots, \overline{b_n})) = \sum_{i=1}^{n} d_{Lee}(\overline{a_i}, \overline{b_i})$$

4. Reticulados

Quando estudamos reticulados, o que estamos buscando é, encontrar o melhor reticulado possível em $\mathbb{Z}^n$, onde n é a dimensão, em relação à uma certa propriedade. O problema de encontrar o melhor código possível em $\mathbb{Z}^n$ corresponde, em $\mathbb{R}^n$, ao problema do *empacotamento esférico*. Ou seja, queremos distribuir esferas de raio r em $\mathbb{R}^n$, de modo que

i) Duas esferas quaisquer apenas se toquem em um ponto da "casca", ou não possuam intersecção nenhuma;

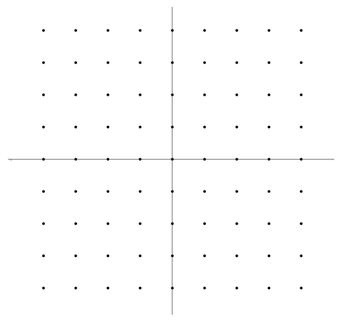
ii) Este arranjo de esferas ocupe o "maior espaço possível".

Este problema torna-se um pouco menos complicado quando se tem alguma estrutura algébrica no código, ou seja, nos centros das esferas. O mesmo vale para o empacotamento esférico em $\mathbb{R}^n$ e, neste caso, a estrutura algébrica é a de *reticulado*.

Definição 5.1 *Dado $B = \{v_1, v_2, ..., v_m\}$ um conjunto de vetores linearmente independentes em $\mathbb{R}^n$, definimos por* ***reticulado*** *de* ***base*** *B o conjunto*

$$\Lambda = \left\{ \sum_{i=1}^{m} \lambda_i v_i, \lambda_i \in \mathbb{Z} \text{ para todo } i = 1, 2, ..., m \right\}.$$

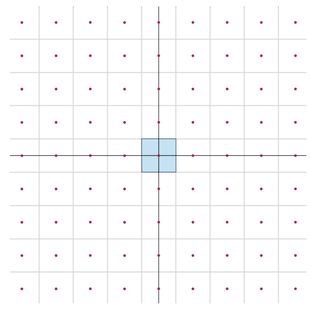
Considere o reticulado $\mathbb{Z}^2$ da figura abaixo.



Um empacotamento esférico é feito colocando-se um disco D, de raio $\frac{1}{2}$, centrado em cada ponto $\mathbf{v}$ do reticulado. Note que, se tomarmos discos de raio maior do que $\frac{1}{2}$, haverá sobreposição; portanto, $\frac{1}{2}$ é o maior raio possível para um empacotamento de discos com centro em pontos de $\mathbb{Z}^2$. Este maior raio é chamado de *raio de empacotamento* ρ do reticulado.

5. Regiões fundamentais e matriz de Gram

Seja Λ um reticulado em $\mathbb{R}^n$. Uma *região fundamental* F de Λ é um subconjunto fechado de $\mathbb{R}^n$ que ladrilha $\mathbb{R}^n$, ou seja, tomando os transladados $F + \mathbf{v}$, com $\mathbf{v} \in \Lambda$, conseguimos cobrir todo o $\mathbb{R}^n$ de modo que dois ladrilhos ou não têm interseção ou se interceptam apenas nos bordos. A seguir, um exemplo de uma região fundamental de $\mathbb{Z}_2$.



Definição 6.1 *Se $\mathbf{v} \in \Lambda$, a* ***região de Voronoi*** *de $\mathbf{v}$ é o conjunto*

$$R(\mathbf{v}) = \{\mathbf{x} \in \mathbb{R}^n; ||\mathbf{v}-\mathbf{x}|| \leq ||\mathbf{v}-\mathbf{u}||, \forall \mathbf{u} \in \Lambda\}.$$

Tendo construído uma região, todas as outras são obtidas por translações, já que cada translação é uma isometria. Assim, todas essas regiões possuem as mesmas propriedades geométricas. Estas regiões constituem um ladrilhamento perfeito no plano e se sobrepõem apenas nos pontos de fronteira. Com isso, define-se a **densidade do reticulado**, fornecendo o quanto do plano foi preenchido pelos discos.

$$\Delta = \frac{\text{área}(D)}{\text{área}(R(\mathbf{0}))}.$$

Seja $\beta = \{\mathbf{u_1}, \mathbf{u_2}, ..., \mathbf{u_n}\}$, uma base do reticulado Λ, e seja $x = k_1\mathbf{u_1} + ... + k_n\mathbf{u_n}$ um elemento de Λ. Escrevendo os vetores na forma de colunas, com as coordenadas na base canônica, temos

$$\mathbf{x} = \underbrace{\begin{bmatrix} u_{11} & \cdots & u_{1n} \\ \vdots & & \vdots \\ u_{n1} & \cdots & u_{nn} \end{bmatrix}}_{A} \cdot \begin{bmatrix} k_1 \\ \vdots \\ k_n \end{bmatrix} = \begin{bmatrix} u_{11}k_1 + & \cdots & + u_{1n}k_n \\ \vdots & & \vdots \\ u_{n1}k_1 + & \cdots & + u_{nn}k_n \end{bmatrix}$$

Isso nos mostra que Λ é a imagem de $\mathbb{Z}^n$ pela matriz $A = (u_{ij})$, ou seja, todo $\mathbf{x} \in \Lambda$ é da forma $A\mathbf{v}^t$, para algum $\mathbf{v} = \{k_1, ..., k_n\}$ em $\mathbb{Z}^n$. A matriz A é chamada de **matriz geradora** de Λ. E ainda, se A é uma matriz geradora de Λ, a matriz de **Gram** associada é $G = A^tA$.

6. Considerações finais

Os códigos apresentam diversas aplicabilidades em nosso cotidiano, principalmente por vivermos em uma era onde a comunicação digital se faz presente. O tempo todo estamos lidando com troca de informações e sobretudo com a segurança dessas informações. Em virtude disso, esse é um assunto bastante estudado em grandes áreas. Nos estudos da teoria, estamos procurando códigos que sejam o mais eficiente possível. Ao introduzirmos os reticulados, estamos procurando o melhor código que satisfaça uma determinada propriedade. A partir disso, o projeto tem como objetivo futuro relacionar esses dois conceitos e analisar a chamada "Construção A", que envolve a construção de reticulados a partir da teoria de códigos.

Referências

[1] HEFEZ, A.; VILLELA, M. L. T. **Códigos corretores de erros**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2008.

[2] LAVOR, C. C.; ALVEZ, M. M. et all. **Uma introdução à teoria de códigos**. Notas em Matemática Aplicada. Vol. 21. SBMAC, 2012.

Apoios:

[1]Universidade Federal do Espírito Santo
[2]Universidade Federal do Espírito Santo