UMA INTRODUÇÃO AOS CÓDIGOS BCH

Pedro Leonardo Pinto de Souza [38]
Edney Augusto Jesus de Oliveira [39]
Vinícius Vivaldino Pires de Almeida [40]

Resumo: Nesse trabalho introduziremos os códigos corretores de erros e abordaremos a classe desses códigos que é mais utilizada na prática: os códigos lineares. Além disso, apresentaremos os códigos cíclicos e BCH, sendo este último uma subclasse dos códigos cíclicos. Veremos que os códigos cíclicos são uma classe específica de códigos lineares e, por consequência, os códigos BCH também são. Nosso objetivo é apresentarmos esses códigos através de um ponto de vista matemático, evidenciando a estrutura sobre a qual cada um deles é construído, bem como algumas semelhanças e diferenças entre eles.

Os códigos corretores de erros são códigos criados para garantir a integridade de uma informação, que ao ser transmitida por um canal de comunicação imperfeito, como o telefone, canais via rádio, wi-fi, entre outros, pode chegar danificada ao destinatário. Esses códigos buscam detectar e, se possível, corrigir eventuais erros que possam ter ocorrido durante a transmissão de uma mensagem, através de um processo denominado decodificação. Tal processo é baseado em três parâmetros principais, o comprimento das palavras de um código, a quantidade de palavras e a distância mínima entre essas palavras, sendo a determinação deste último um dos grandes desafios na construção de um código corretor de erros.

Denotando por K um corpo finito com q elementos, e K^n o espaço vetorial n-dimensional sobre K, definimos um código linear da seguinte maneira:

Definição 1 *Um código $\mathcal{C} \subset \mathbb{K}^n$ é chamado de código linear se $\mathcal{C}$ for um subespaço vetorial de $\mathbb{K}^n$.*

A partir da definição de códigos lineares, vemos que eles possuem a estrutura de um espaço vetorial, o que possibilita descrevermos um código linear $\mathcal{C}$ ou como imagem, ou como núcleo de uma transformação linear $T : K^k \to K^n$, em que k é a dimensão do código linear $\mathcal{C}$. Além disso, obtemos que a matriz da transformação T com relação a uma base β de $\mathcal{C}$ é uma matriz geradora do código linear $\mathcal{C}$ e através dela determinamos uma outra matriz H, a qual chamamos de matriz teste de paridade, geradora do complemento ortogonal de $\mathcal{C}$, $\mathcal{C}^{\perp}$, que também é um código linear. A partir desses conceitos obtemos um resultado que possibilita determinarmos de maneira eficiente a distância mínima de um código linear e, consequentemente, estabelecermos um algoritmo de decodificação.

[38]Universidade Federal de Ouro Preto, pedro.leonardo@aluno.ufop.edu.br
[39]Universidade Federal de Ouro Preto, edney@ufop.edu.br
[40]Universidade Federal de Ouro Preto, viniciusalmeida@ufop.edu.br

Por serem uma classe de códigos lineares, os códigos cíclicos também possuem estrutura de subespaço vetorial. Com isso, definimos os códigos cíclicos da seguinte maneira:

Definição 2 *Seja K um corpo e K^n um espaço vetorial sobre K. Dizemos que o subespaço vetorial $\mathcal{C} \subset K^n$ é um código cíclico quando para todo $\mathbf{c} = (c_0, ..., c_{n-1}) \in \mathcal{C}$ temos $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$*

Por outro lado, podemos enxergar os códigos cíclicos como o ideal $I([g(X)])$ do anel quociente $R_n = K[X]/I(X^n - 1)$, em que $I([g(X)])$ e $I(X^n - 1)$ são os ideais gerados, respectivamente, pela classe do polinômio $g(X) \in K[X]$, divisor de $X^n - 1$, e pelo polinômio $X^n - 1 \in K[X]$. Vemos que esse ideal é principal e que através do seu polinômio gerador, estabeleceremos de maneira mais simples que os códigos lineares em geral, do ponto de vista matemático, a matriz geradora e matriz teste de paridade de um código cíclico. No entanto, não há uma maneira prática de encontrar sua distância mínima, o que torna a quantidade de cálculos realizados no algoritmo da decodificação muito maior quando aplicado aos códigos cíclicos. Por essa razão, estudamos os códigos BCH, pois eles nos fornecem uma maneira prática de estimarmos sua distância mínima por meio de uma cota.

Os códigos BCH, por se tratarem de um código cíclico particular, também são vistos como o ideal $I([g(X)])$ de R_n, com $g(X) = mmc(m_{\gamma^a}(X), \ldots, m_{\gamma^{a+\delta-2}}(X))$, em que γ é uma raiz n-ésima primitiva da unidade e $m_{\gamma^a}(X), \ldots, m_{\gamma^{a+\delta-2}}(X)$ são os polinômios minimais de $\gamma^a, \ldots, \gamma^{a+\delta-2}$ tal que $a \geq 0$ e $0 \leq \delta \leq n$. Consequentemente, o polinômio gerador $g(X)$ é um polinômio minimal de raízes n-ésimas da unidade. Essa restrição nos permite estabelecer uma cota para a distância mínima de um código BCH. Deste modo, conseguimos aplicar o algoritmo da decodificação para códigos lineares com uma quantidade consideravelmente menor de cálculos do que para os códigos cíclicos e, mais ainda, diferentemente dos códigos lineares em geral, é possível construir códigos BCH capazes de corrigir múltiplos erros.

Referências

[1] BERLEKAMP, E. *Algebraic coding theory, revised edition.* Singapore: World Scientific, 2015.

[2] HEFEZ, A. *Curso de álgebra, volume 1.* 3. ed. Rio de Janeiro/RJ: Impa, 2002. (Coleção Matemática Universitária).

[3] HEFEZ, A.; VILLELA, M. L. T. *Códigos corretores de erros.* 2. ed. Rio de Janeiro/RJ: IMPA, 2008.