Códigos Cíclicos sobre Anéis Comutativos e Anéis de Inteiros Algébricos com Aplicações

Pedro Mendes Odilon*, Reginaldo Palazzo Júnior, Hector Frank de Oliveira

Resumo

A teoria dos Códigos Corretores de Erros se fundamenta na álgebra, principalmente sobre anéis e corpos. Em cima de tal são construídos códigos, como os lineares, BCH e Reed Solomon. Cada um deles tem especificidades e exige um processo de decodificação de acordo. E assim de diferentes algoritmos e ferramentas para recuperar a palavra com erro. A transformada discreta de Fourier pode ajudar no processo e já é utilizada para decodificação em corpos, no entanto o interesse deste presente trabalho é analisar em quais anéis comutativos é possível defini-la.

Palavras-chave: Anéis comutativos, Transformadas discretas, Códigos Corretores de Erro

Introdução

A teoria dos Códigos Corretores de Erro (CCE) tenta resolver o problema de confiabilidade de comunicação. A transmissão de informação em canais reais são sempre acompanhadas de ruído, vindo de interferências eletromagnéticas, curtos, problemas de multiplexação etc. Isso leva a vários erros durante a transmissão e armazenamento de dados.

O objetivo dela é construir códigos tal que quando a informação chegue no destino, mesmo com erros, seja possível detectar e corrigir tais erros. A decodificação é uma das etapas mais importantes do processo, já que nela é que se obtém a palavra reparada, ou ao menos uma detecção de erro. E esse processo pode utilizar a Transformada Discreta de Fourier, por isso é interessante saber sob quais anéis comutativos é possível definir a transformada.

Resultados e Discussão

Seja $\{x_n\}$ uma sequência cujo período é de N amostras, isto é $x(n)=x(n+N)$. Então o k -ésimo coeficiente de Fourier $\theta(k)$ é dado por

$$\theta(k) = \sum_{n=0}^{N-1} x(n) \exp\left(-j \frac{2k\pi n}{N}\right), \quad k = 0, 1, 2, \dots, N-1$$

E sua inversa é dada por:

$$x(n) = \frac{1}{N} \sum_{k=0}^{N-1} \theta(k) \exp\left(j \frac{2k\pi n}{N}\right), \quad n = 0, 1, 2, \dots, N-1$$

Note que $\epsilon = \exp\{-j2\pi n/N\}$ é um elemento primitivo e é uma das N raízes da unidade, isto é, $\epsilon^N = 1$. Com isso, vemos que ϵ pertence ao corpo dos números complexos.

Um código cíclico de comprimento N sobre o corpo finito F , com polinômio gerador $g(x)$, onde $g(x)$ divide $x^N - 1$, é o conjunto de todas as palavras-código b tal que $g(x)$ divide $b(x)$. Isso implica que b é uma palavra-código se, e somente se, $B_i = 0$, onde B_i é a transformada de b .

Denota-se a N -ésima raiz primitiva da unidade por ϵ no anel R . O anel dos inteiros módulo m , Z_m , é um anel comutativo. Este anel é o mais importante dos anéis com interesses em teoria da codificação e criptografia. Quando m é um número primo, R é isomorfo ao corpo de Galois F_m . Com isso, o caso de interesse será quando m for composto, pois teremos um anel.

A equação da transformada de Fourier discreta pode ser escrita, neste caso, como $B=M.b$, onde M é uma matriz transformação $N \times N$. Se ϵ é a N -ésima raiz primitiva da unidade em um anel comutativo R , então

$B=M.b$ define um mapeamento inversível de R^N em R^N cujo mapeamento inverso é dado pela inversa da transformada de Fourier discreta usual se, e somente se, ϵ^{k-1} é uma unidade para $1 \leq k \leq N$.²

Esse resultado implica que não existe a transformada discreta de Fourier em Z_m para qualquer $m \geq 2$, quando m é composto e par. As razões para este resultado são: 1) Por que ϵ deve ser uma unidade e, portanto ímpar. Com isso, $\epsilon-1$ é par, logo não é uma unidade; 2) Para todo número composto ímpar (mod m), $\epsilon=m-1$ é uma segunda raiz primitiva da unidade e gera uma transformada de Fourier discreta de comprimento $N=2$ em Z_m , pois $\epsilon-1=m-2$ e $\text{mdc}(m, m-2)=\text{mdc}(m, 2)=1$ tal que $\epsilon-1$ é uma unidade. Pode-se encontrar uma transformada de Fourier discreta de comprimento $N>2$ em qualquer anel Z_m , para um m composto e, portanto, ímpar? A resposta é sim.

Tabela 1. Valores de m vs N .

M	N
91	2,3,6
169	2,3,4,6,12
121	2,5,10
217	2,3,6

Conforme se vê na **tabela 1**, ilustra alguns valores de m para os quais são possíveis definir a transformada de tamanhos N , e de interesse prático.

Destaca-se a transformada de Fourier discreta com $N=256$ em Z_{257} tem componentes limitadas a resolução de 8 bits, transformada com $N=256$ em Z_{257}^2 tem componentes limitadas a resolução de 16 bits e a com $N=256$ em Z_{257}^3 com resolução de 24 bits.

Conclusões

Definir a transformada discreta sobre anéis comutativos pode ajudar no processo de decodificação. Por isso é interessante sabermos para quais desses anéis é possível defini-la. Para Z_m com m composto e maior que 2 e ímpar, e sempre se encontrará uma transformada de comprimento N no anel comutativo R .

Agradecimentos

Agradeço a FAPESP ao financiamento da pesquisa e ao meu orientador Reginaldo Palazzo pelo apoio.

¹ Blahut Fast, R. E. **Fast Algorithms for Signal Processing**. New York:Cambridge University Press, 2010

² J. L. Massey. **Digital Information Theory**. (Class Notes ETH-Zurich), 1998.

³ Blahut Fast, R. E. **Theory and Practice of Error Control Codes**. Reading, MA:Addison-Wesley Pub. Co, 1983