Universidade: presente!

UFRGS PROPESQ

XXXI SIC

Salão UFRGS 2019 – Conhecimento, Formação, Inovação

21 . 25 . OUTUBRO . CAMPUS DO VALE

Códigos Lineares com Cota Inferior para sua Distância Mínima

João Pedro Aguinsky
Orientadora: Thaísa Raupp Tamusiunas
Bacharelado em Matemática - Ênfase em Matemática Pura
Universidade Federal do Rio Grande do Sul - UFRGS

Teorema(Bose-Chaudhuri-Hocquenghem):

Seja $K=\mathbb{F}_q$, *n* um inteiro maior do que *1* e primo com *q*, F um corpo onde X^n-1 se decompõe em fatores lineares, $\gamma \in F$ uma raíz *n*-ésima de unidade e *C* um código cíclico com polinômio gerador

$$g=mmc(m_{\gamma^a},\ldots,m_{\gamma^{a+\delta-2}})$$

com $a \geq 0$ e $\delta \leq n$. Então a distância mínima de *C* é, pelo menos, δ e sua dimensão é, pelo menos, $n-m(\delta-1)$, onde m=$dim_K F$.

Introdução:

Um código é dito linear se for um subespaço vetorial do espaço K^n, onde K é um corpo de *q* elementos. Seus parâmetros mais importantes são seu comprimento, sua dimensão e sua distância mínima. O comprimento e a dimensão podem ser facilmente verificados observando sua *matriz geradora*, no entanto, para a distância mínima é necessário olhar para sua *matriz teste de paridade* (imagem).

Se um código, além de ser linear, satisfizer $(a_1,\ldots,a_n)=(a_n,a_1,\ldots,a_{n-1})$ para todos seus vetores, ele será chamado de cíclico. Nós veremos que todo código cíclico de comprimento *n* será isomorfo a algum ideal $I([g])$ de $K[X]_{X^n-1}$, onde g é um polinômio divisor de X^n-1 .

$$G=\begin{pmatrix}1000101\\0100110\\0010011\\0001111\end{pmatrix}$$

É um exemplo de matriz geradora do código binário *C*. Tem 4 linhas e 7 colunas, portanto o comprimento de *C* é 7 e a sua dimensão é 4. O número de elementos em *C* é $2^4=16$ pois F_2 tem 2 elementos elevado na sua dimensão.

$$H=\begin{pmatrix}1101100\\0111010\\1011001\end{pmatrix}$$

É a *matriz teste de paridade* associada a *G*. Quaisquer duas colunas de H são L.I. e existem 3 colunas L.D., o que nos dá que esse código tem distância mínima igual a 3, ou seja, consegue detectar até dois erros e corrigir um erro.

Desenvolvimento:

Para definir um código cíclico, buscamos divisores de X^n-1 em $K[X]$. Isto nos motiva ao estudo das raízes de X^n-1 . Primeiro veremos sob que condição o corpo K possui uma extensão, como ela é um K- espaço vetorial de dimensão finita e como, para cada elemento da extensão, existirá um polinômio minimal em $K[X]$. Após isto, aplicamos este estudo a busca de raízes de unidade. Tomando o divisor que buscamos como o mmc de alguns polinômios minimais destas raízes, vemos de que forma o código gerado será definido em função delas, o que nos dará ferramentas necessárias para provar o Teorema.

Aplicações:

Existem diversas aplicações para códigos corretores de erros, aqui algumas são citadas.

- Permitir que mensagens de satélite, como vídeos, sejam enviadas sem perda de informações.
- Mensagens espaciais são enviadas com menos perdas de informações.
- Em diversas camadas do TCP/IP.

Bibliografia:

Abramo Hefez e Maria Lucia T. Villela, Códigos Corretores de Erros, Série de Computação e Matemática, IMPA (2008).