Trabalho apresentado no XXXIX CNMAC, Uberlândia - MG, 2019.

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Estruturas Algébricas em Teoria de Códigos Corretores de Erros

Lara Nicoletti Sotoma [1]
Instituto de Matemática – Universidade Federal de Mato Grosso do Sul
Marcos Vinicius Pereira Spreafico [2]
Instituto de Matemática – Universidade Federal de Mato Grosso do Sul

1 Resumo

A ideia deste trabalho é apresentar um estudo da Teoria dos Códigos Corretores de Erros, voltado às estruturas algébricas utilizadas na construção e estudo dos códigos de Reed-Solomon.

Numa ligação telefônica, por exemplo, ao falar o número 6, a pessoa que se encontra do outro lado da linha pode entender que foi dito 3, pelo fato da pronúncia das palavras serem um pouco parecidas e da existência de ruídos na linha. Na tentativa de resolver problemas como este é que surgiu a Teoria dos Códigos Corretores de Erros.

Ainda no exemplo anterior, um recurso muito utilizado para garantir que a mensagem foi recebida corretamente é sua repetição. Contudo, dependendo do meio de comunicação e do tamanho da mensagem, repeti-la várias vezes pode gerar um custo muito alto e ser inviável. Uma forma de construir um código mais eficiente é através do uso das estruturas algébricas.

Os códigos de Reed-Solomon, ou códigos RS, inventados por Irving S. Reed e Gustave Solomon, encontram-se entre os códigos mais poderosos no que diz respeito à capacidade de correção de erro. Eles são amplamente utilizados em muitos sistemas digitais, tais como: Comunicações de missões espaciais, CDs, DVDs, aDSL, WiMAX, DVB e QRCode.

Os códigos RS são códigos lineares cíclicos. A seguir, introduzimos os conceitos utilizados na construção de tais códigos, de modo breve e sem o formalismo intrínseco da matemática, mas de forma que seja compreensível no curto espaço possível deste texto.

Seja K um corpo finito com q elementos. Para tornar precisa a ideia de se ter uma palavra parecida com outra utiliza-se a noção de proximidade, usualmente definida pela *distância de Hamming*, dados dois elementos de K^n, a distância de Hamming entre eles é definida como sendo a quantidade de coordenadas distintas. Uma das estruturas algébricas usadas para aumentar a eficiência de transmissão de mensagens é a de espaços vetoriais. Um código $C \subset K^n$ será chamado de *código linear* se for um subespaço vetorial de K^n.

[1] laransotoma@gmail.com
[2] marcos.spreafico@ufms.br

Os parâmetros de um código linear são representados pela terna (n, k, d), onde n é o comprimento das palavras, k é a dimensão de C sobre K e d representa a distância mínima de C, isto é, a menor distância (de Hamming) entre todos os pares de elementos do código.

Um código linear $C \subset K^n$ será chamado de código cíclico se, para todo $c = (c_0, \ldots, c_{n-1})$ pertencente a C, o vetor $(c_{n-1}, c_0, \ldots, c_{n-2})$ pertence a C. Utilizando a identificação $c = (c_0, c_1, \cdots, c_{n-1}) \sim c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$, um código de comprimento n pode ser visto com um subconjunto dos polinômios de grau menor do que ou igual n. Neste sentido, os códigos cíclicos são caracterizados como ideais principais no anel das classes residuais de $K[X]$ módulo $X^n - 1$. Se β é um elemento primitivo em K (isso significa que $\beta^{q-1} = 1$ mas nenhuma potência menor de β é 1) então, podemos fatorar o polinômio $X^{q-1} - 1$ como

$$X^{q-1} - 1 = (X - 1)(X - \beta)(X - \beta^2) \cdots (X - \beta^{q-2}). \tag{1}$$

Para $2 \leq t \leq q - 1$, defina o polinômio de grau $t - 1$

$$g(X) = (X - \beta)(X - \beta^2) \cdots (X - \beta^{t-1}). \tag{2}$$

O código cíclico gerado por g é um código RS, com parâmetros $(n, t, n-t+1)_q$. A ampla utilização desses códigos em sistemas de comunicação digitais deve-se aos parâmetros que estes códigos possuem, uma vez que em um certo sentido, as palavras do código são bem espalhadas (possuem máxima separação) no espaço ambiente.

Referências

[1] P. Garrett. *The Mathematics of Coding: Information, Compression, Error Correction, and Finite Fields*. Minneapolis, University of Minnesota. Disponível em `http://www-users.math.umn.edu/~garrett/coding/CodingNotes.pdf`.

[2] A. Hefez, M. L. T. Villela. *Códigos Corretores de Erros, 2a. edição*. IMPA, Rio de Janeiro, 2008.