Proceeding Series of the Brazilian Society of Computational and Applied Mathematics, v. 10, n. 1, 2023.

Trabalho apresentado no XLII CNMAC, Universidade Federal de Mato Grosso do Sul - Bonito - MS, 2023

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Estruturas algébricas aplicadas na codificação de códigos Reed-Solomon

Bianca Lapa Ribeiro[1]
Discente do Programa de Pós-Graduação em Estatística Aplicada e Biometria, UNIFAL-MG
Anderson José de Oliveira[2]
Departamento de Matemática, UNIFAL-MG

Os códigos corretores de erros (CCE's) possuem a capacidade de detectar e corrigir erros que podem surgir durante os processos de transmissão e armazenamento de informações. Existem diversos tipos de CCE's e dentre esses tipos, os códigos BCH são uma importante classe que possuem facilidade nos processos de codificação e decodificação [2].

Os códigos Reed-Solomon (RS) formam uma subclasse dos códigos BCH e são códigos q-ários que possuem forte estrutura algébrica em seu processo de construção tanto na codificação quanto na decodificação [1], [3], sendo particularmente úteis para correção de rajada de erros, possuindo uma notável capacidade de correção de erros e amplamente aplicados em diversos sistemas de armazenamento e transmissão de dados, como HD, CD, DVD e sistemas espaciais [4], [5].

O objetivo deste trabalho é apresentar como as estruturas algébricas são utilizadas no processo de codificação de códigos RS, em particular, na codificação da mensagem $m(X) = 1+\alpha X+\alpha^2 X^2$, para o código RS$(7, 3)$, sobre o corpo $GF(2^3)$.

De acordo com [1], em termos dos parâmetros (n, k, t), para a forma mais comum dos códigos RS, tem-se que: $(n, k) = (2^m - 1, 2^m - 1 - 2t), \quad m > 2$, em que $n - k = 2t$ é o número de símbolos de paridade e t é a capacidade de correção de erro de símbolo do código. O polinômio gerador para um código RS assume a seguinte forma:

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_{2t-1} X^{2t-1} + X^{2t}. \tag{1}$$

O grau do polinômio gerador é igual ao número de símbolos de paridade. Uma vez que o grau do polinômio gerador é igual a $2t$, deve haver precisamente $2t$ potências sucessivas de α, que são raízes do polinômio.

As raízes de $g(X)$ são designadas como: α, α^2, $\cdots$, α^{2t}. Dessa forma, o polinômio gerador $g(X)$ pode ser obtido da seguinte forma:

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

Os códigos Reed-Solomon podem ser codificados na forma sistemática de forma análoga ao procedimento para os códigos binários, uma vez que os códigos RS são códigos cíclicos. Assim,

$$X^{n-k} m(X) = q(X)g(X) + p(X), \tag{3}$$

em que $q(X)$ e $p(X)$ são os polinômios quociente e resto, da divisão da mensagem deslocada de $n - k$ posições, $X^{n-k}m(X)$, pelo polinômio gerador, $g(X)$.

Para o código RS$(7, 3)$ e considerando a mensagem $m(X) = 1 + \alpha X + \alpha^2 X^2$, a mensagem deslocada de $n - k$ posições, $X^{n-k}m(X)$, pode ser obtida fazendo a multiplicação de $m(X) =$

[1]bianca.ribeiro@sou.unifal-mg.edu.br
[2]anderson.oliveira@unifal-mg.edu.br

$1 + \alpha X + \alpha^2 X^2$ por X^4, uma vez que, $X^{n-k} = X^{7-3} = X^4$. Assim: $X^4(1 + \alpha X + \alpha^2 X^2) = X^4 + \alpha X^5 + \alpha^2 X^6$.

Como o polinômio paridade, $p(X)$, é o resto da divisão do polinômio deslocado, $X^{n-k}m(X)$, por $g(X)$, segue que:

$$p(X) = X^{n-k}m(X) \mod g(X). \tag{4}$$

Realizando a divisão polinomial do polinômio $X^{n-k}m(X) = \alpha^2 X^6 + \alpha X^5 + \alpha^0 X^4$ pelo polinômio $g(X) = \alpha^0 X^4 + \alpha^3 X^3 + \alpha^0 X^2 + \alpha^1 X + \alpha^3$, obtém-se o quociente $q(X) = \alpha^2 X^2 + \alpha^6 X + \alpha^0$ e resto $p(X) = \alpha^6 X^3 + \alpha^5 X^2 + \alpha^4 X + \alpha^3$.

A palavra-código na forma polinomial resulta em:

$$c(X) = p(X) + X^{n-k}m(X), \tag{5}$$

ou seja: $c(X) = \alpha^3 + \alpha^4 X + \alpha^5 X^2 + \alpha^6 X^3 + \alpha^0 X^4 + \alpha^1 X^5 + \alpha^2 X^6$.

É possível realizar a codificação na forma sistemática com registradores de deslocamento de $(n - k)$ estágios, conforme esquema apresentado na Tabela 1.

Tabela 1: Codificação Reed-Solomon.

Fila de entrada	Ciclos *clock*	Registradores	Realimentação	Fila de saída
$\alpha^0 \quad \alpha^1 \quad \alpha^2$	0	$0 \quad 0 \quad 0 \quad 0$	α^2	α^2
$\alpha^0 \quad \alpha^1$	1	$\alpha^5 \quad \alpha^3 \quad \alpha^2 \quad \alpha^5$	α^6	$\alpha^1\alpha^2$
α^0	2	$\alpha^2 \quad \alpha^4 \quad \alpha^4 \quad 0$	α^0	$\alpha^0\alpha^1\alpha^2$
$-$	3	$\alpha^3 \quad \alpha^4 \quad \alpha^5 \quad \alpha^6$	0	$\alpha^6\alpha^0\alpha^1\alpha^2$
$-$	4	$0 \quad \alpha^3 \quad \alpha^4 \quad \alpha^5$	0	$\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
$-$	5	$0 \quad 0 \quad \alpha^3 \quad \alpha^4$	0	$\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
$-$	6	$0 \quad 0 \quad 0 \quad \alpha^3$	0	$\alpha^3\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$
$-$	7	$0 \quad 0 \quad 0 \quad 0$	0	$-\alpha^3\alpha^4\alpha^5\alpha^6\alpha^0\alpha^1\alpha^2$

Na forma polinomial a fila de saída pode ser escrita como: $c(X) = \alpha^3 + \alpha^4 X + \alpha^5 X^2 + \alpha^6 X^3 + \alpha^0 X^4 + \alpha^1 X^5 + \alpha^2 X^6$.

Pode-se notar a importância da álgebra no processo de codificação dos códigos Reed-Solomon, em particular no código RS$(7, 3)$, utilizando entre outros as operações envolvendo a extensão do corpo $GF(2^3)$, além das estruturas de grupos, anéis e aritmética modular.

Referências

[1] G. Iezzi e H. Domingues. **Álgebra Moderna**. São Paulo: Atual, 2003.

[2] S. Lin e D. J. Costello. **Error Control Coding.** 2 ed. Prentice Hall, 2004.

[3] P. Shrivastava e U. P. Singh. Detecção e correção de erros usando códigos Reed Solomon. **Jornal Internacional de Pesquisa Avançada em Ciência da Computação e Engenharia de Software**, v.3, n.8, 2013.

[4] A. H. L. Silva e T. A. Rodolfo. 67f. **Implementação de uma Arquitetura Reed-Solomon para uso em Redes OTN 10.7 Gbps**. Trabalho de Conclusão de Curso (Bacharelado em Engenharia de Computação). Porto Alegre, 2007.

[5] D. B. C. Zanitti e C. W. O. Benedito. Códigos Reed-Solomon para Correção de Erros em Rajada. **Proceeding Series of the Brazilian Society of Computational and Applied Mathematics**, v. 7, n. 1, 2020.