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

Proceeding Series of the Brazilian Society of Computational and Applied Mathematics

Códigos Reed-Solomon para Correção de Erros em Rajada

Débora Beatriz Claro Zanitti [1]
Universidade Estadual Paulista (UNESP), Campus de São João da Boa Vista, SP
Cintya Wink de Oliveira Benedito [2]
Universidade Estadual Paulista (UNESP), Campus de São João da Boa Vista, SP

1 Introdução

A utilização dos códigos corretores de erros provém da necessidade de se armazenar e transmitir grande número de dados, muitos dos quais são sensíveis a erros. Este processo requer cada vez mais sistemas eficientes e seguros. Devido a isto e a grandes avanços tecnológicos, a teoria de códigos corretores de erros continua sendo uma área de forte interesse de estudo atualmente.

Códigos de bloco com símbolos em $GF(q)$, onde q é uma potência de primo, são chamados de códigos de bloco q-ário. Uma mensagem para um código de bloco q-ário (n, k) consiste em k símbolos de informação em $GF(q)$. Os códigos de Reed-Solomon (RS) são códigos q-ários que constituem uma sub-classe dos códigos BCH e são os códigos mais amplamente utilizados na prática, [3]. Esses códigos são usados em uma vasta aplicações em comunicações digitais e também em sistemas de armazenamento em massa para corrigir erros de rajada associados a defeitos de mídia, podendo detectar qualquer combinação de até t erros, ou corrigir até $\frac{t}{2}$ erros, [2]. Neste trabalho, apresentamos a codificação e decodificação dos códigos RS, exemplificando para um código $(15, 9)$. Além disso, apresentamos os parâmetros e a eficiência de correção de erros em rajada de códigos RS utilizados em aplicações práticas de telecomunicações, [3].

2 Codificação e Decodificação de Códigos RS

Na codificação dos códigos RS, o polinômio gerador destes códigos é especificado em termos das suas raízes do corpo de Galois $GF(q^m)$. Seja α um elemento primitivo de $GF(q^m)$ e $\phi_i(X)$ o polinômio minimal de α^i para $1 \leq i \leq 2t$, então, $g(X)$ deve ser o mínimo múltiplo comum (MMC) dos polinômios minimais, ou seja

$$g(X) = MMC\{\phi_1(X), \phi_3(X), ..., \phi_{2t}(X)\}. \quad (1)$$

A decodificação dos códigos de Reed-Solomon ocorre através do seguinte algoritmo, [1]:

[1] bia.zanitti@hotmail.com
[2] cintya.benedito@unesp.br

1. Substituir as raízes do polinômio gerador no polinômio recebido, encontrar as síndromes $S_1, S_2, \cdots, S_{2t}$ e o polinômio síndrome $S(X) = S_1 + S_2X + ... + S_{2t}X^{2t-1}$.
2. Para cada $i = 1, \cdots, 2t$, divide-se $Z_0^{(i-2)}(X)$ por $Z_0^{(i-1)}(X)$ para obter o quociente $q_i(X)$ e o resto $Z_0^{(i)}(X)$. Neste passo adota-se as condições iniciais sendo $Z_0^{(-1)}(X) = X^{2t}$, $Z_0^{(0)}(X) = S(X)$, $\sigma^{(-1)}(X) = 0$ e $\sigma^{(0)}(X) = 1$. A iteração acaba quando $grau[Z_0^{(p)}(X)] < grau[\sigma^{(p)}(X)] \leq t$.
3. Adote $\sigma(X) = \sigma^{(p)}(X)$ e $Z_0(X) = Z_0^{(p)}(X)$, onde p é a última iteração.
4. Encontre as raízes de $\sigma(X)$ e tome o inverso de cada uma das raízes, do qual o expoente fornece as localizações dos erros no padrão de erro $e(X)$.
5. Seja $\sigma'(X)$ a derivada de $\sigma(X)$, os valores dos erros na localização j_i são dados por $e_{j_i} = \frac{-Z_0(\alpha^{-j_i})}{\sigma'(\alpha^{-j_i})}$.
6. Corrigir o polinômio recebido através de $V(X) = r(X) - e(X)$.

Exemplo 2.1. *Considerando o código RS corretor de erro triplo (15,9) gerado por* $g(X) = (X+\alpha)(X+\alpha^2)(X+\alpha^3)(X+\alpha^4)(X+\alpha^5)(X+\alpha^6)$. *Supondo que um código polinomial* $v(X)$ *é transmitido e* $r(X) = \alpha^7X^3 + \alpha^{11}X^{10}$ *é recebido, através do* ***Passo 1*** *encontra-se a síndrome* $S(X) = \alpha^7 + \alpha^{12}X + \alpha^6X^2 + \alpha^{12}X^3 + \alpha^{14}X^4$. *Na divisões realizadas no* ***Passo 2****, até a sua última iteração, obtêm-se* $\sigma(X) = \alpha^{11} + \alpha^8X + \alpha^9X^2$ *e* $Z_0(X) = \alpha^3 + \alpha^2X$, *onde as raízes de* $\sigma(X)$ *são* α^5 *e* α^{12} *e seus inversos são* α^{10} *e* α^3. *Através do* ***Passo 5****, encontra-se* α^7 *e* α^{11}, *logo têm-se* $e(X) = \alpha^7X^3 + \alpha^{11}X^{10}$. *Logo,* $V(X) = r(X) - e(X) = (\alpha^7X^3 + \alpha^{11}X^{10}) - (\alpha^7X^3 + \alpha^{11}X^{10}) = 0$.

Devido a sua capacidade de corrigir erros em rajada (*burst errors*), os códigos RS são utilizados em muitas aplicações práticas tais como a gravação de discos compactos com parâmetros RS$(255, 223)$ e capacidade de correção $t = 16$, WiMAX com RS$(255, 239)$ e capacidade de correção $t = 8$, transmissão de vídeo digital RS$(204, 188)$ e $t = 8$, [1, 3].

Agradecimentos

Os autores agradecem o apoio financeiro da FAPESP Processo 2017/17948-8.

Referências

[1] W. C. Huffman and V. Pless. *Fundamentals of Error Correting Codes*, Cambridge University Press, 2003.

[2] W. E. Ryan and S. Lin. *Channel codes: Classical and modern*, Cambridge University Press, 2009.

[3] P. Shrivastava1 and U. P. Singh. Error Detection and Correction Using Reed Solomon Codes, *International Journal of Advanced Research in Computer Science and Software Engineering*, volume 3(8), pp. 965-969, 2013.