Códigos Reed-Solomon

Raquel Souza **Fábio Borges**
Coordenação de Sistemas e Redes, LNCC,
25651-075, Petrópolis, RJ
E-mail: rasouza@lncc.br, borges@lncc.br

RESUMO

Os códigos Reed-Solomon, criados em 1960 por Irving S. Reed e Gustave Solomon [2], são cíclicos e podem ser construídos de forma a corrigir erros múltiplos. São usados em telecomunicações [1], tanto em meios de armazenamento, como *compact disc* (CD), assim como em transmissões distantes, como no caso do satélite Voyager 2. Esse tipo de código não é recomendado para a transmissão de grande quantidade de dados, entretanto, sua vantagem é a possibilidade de corrigir um elevado número de erros dentro da mesma palavra. Neste resumo, apresentamos um estudo teórico sobre estes códigos. Durante o estudo do tema, os autores conseguiram constatar, através de testes em casos particulares, a eficácia do algoritmo de correção de erros exposto no trabalho.

Definição. Um código BCH sobre $GF(q)$ onde o comprimento n é igual a $q-1$ é chamado de código *Reed-Solomon*, e representado por $RS(n,t)$. Os parâmetros k, d e t representam a dimensão, a distância mínima e o número de erros corrigíveis do código, respectivamente.

Um código Reed-Solomon é construído a partir de um corpo finito $R = GF(q)$. O polinômio $g(x)$ gerador de um código Reed-Solomon C, corretor de t erros, é dado por:

$$g(x) = (x-a)(x-a^2)\cdots(x-a^{2t}),$$

onde a é um elemento primitivo de $R = GF(q)$.

Temos que $C = \{c(x) = b(x)g(x) : b(x) \in R[x],\ grau(c(x)) < q-1\}$. A seguir, é apresentado um modelo de correção de erros para códigos Reed-Solomon de comprimento 2^m-1, que são muito utilizados devido à possibilidade de representação binária.

Correção de erros em $RS(2^m-1,t)$

Suponhamos que nos é transmitido o polinômio $c(x) \in C$ e recebemos o polinômio $r(x) \neq c(x)$, tal que $r(x) = c(x) + e(x)$, sendo $e(x)$ um polinômio não-nulo de grau menor que 2^m+1. Primeiramente, calculamos $S_i = r(a^i)$, com $i \in \{1,2,\ldots,2t\}$, e formamos o polinômio

$$S(z) = S_1 + S_2 z + S_3 z^2 + \ldots + S_{2t} z^{2t-1},$$

o qual chamamos de *polinômio localizador de erros*. Depois, construímos a tabela do algoritmo de Euclides estendido para polinômios, como em [1], sendo $a(z) = z^{2t}$ e $b(z) = S(z)$. O algoritmo deve terminar na primeira linha j para a qual $grau(R(j)) < t$. A coluna U da tabela pode ser suprimida. Consideraremos $R(z) = R_j$ e $V(z) = V_j$. Temos que, se $a^{i_1}, a^{i_2}, \ldots, a^{i_k}$ são as raízes de $V(z)$, as posições dos erros em $r(x)$ são $x^{-i_1}, x^{-i_2}, \ldots, x^{-i_k}$. Os coeficientes e_{-i} dos termos x^{-i} em $e(x)$ são dados por:

$$e_{-i} = \frac{R(a^i)}{V'(a^i)},$$

onde $V'(a^i)$ é a derivada de $V(z)$ em $z = a^i$.

Referências

[1] Richard E. Klima, Neil Sigmon, and Ernest Stitzinger, *Applications of abstract algebra with Maple*, 2000.

[2] Irving Reed and Solomon Golomb, *Polynomial codes over certain finite fields*, Joint Society of Industrial and Applied Mathematics Journal **8** (1960), no. 2, 300–304.