Correção de Erros em Códigos BCH Binários

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

RESUMO

Neste resumo apresentamos um trabalho teórico sobre os códigos BCH, que foram propostos em meados de 1960 por Bose, Chaudhuri e Hocquenghem. São uma classe de códigos cíclicos que podem ser construídos de forma a corrigir até t erros múltiplos [2].

Definição. O *polinômio mínimo* sobre $GF(p)$ de $\alpha^i \in GF(p^m)$ é o polinômio mônico $M_i(x)$ de menor grau possível, com coeficientes em $GF(p)$, tal que $M_i(\alpha^i) = 0$.

Definição. Um código cíclico C de comprimento n sobre $GF(p^m)$ é um *código BCH* se o seu polinômio gerador é dado por

$$g(x) = \text{MMC}(M(x), M_2(x), \ldots, M_{2t}(x)).$$

Para se construir um código BCH binário de comprimento n é necessário encontrarmos polinômios $f(x) = x^n - 1$, com $n \in \mathbb{Z}_+^*$, e $g(x)$ tal que $g(x)|f(x)$. Para encontrar $g(x)$ nessas condições, podemos escolher $n = 2^m - 1$, onde m é o grau de um polinômio primitivo $p(x)$. Construímos, então, o corpo $\mathbb{Z}_2[x]/(p(x))$, considerando $x = \alpha$. Temos que toda potência α^i, com $i \in \{1, 2, \ldots, s\}$ e $s < n$, é raiz de $f(x)$. Para corrigir até t erros, devemos utilizar $2t$ potências de α. Pela definição anterior, para encontrar $g(x)$ basta encontrar os polinômios mínimos de $\alpha, \alpha^2, \ldots, \alpha^{2t}$. O código C gerado por $g(x)$ será o conjunto de todos os múltiplos de $g(x)$ em $\mathbb{Z}_2[x]$ de grau menor que n. Por ser um espaço vetorial em $\mathbb{Z}_2[x]/(f(x))$, com dimensão $k = n - grau(g(x))$, C é um código linear $[n, k]$, que contém 2^k palavras.

O polinômio verificação de paridade é dado por $h(x) = f(x)/g(x)$.

Suponhamos que um polinômio $c(x) \in C$ nos é transmitido e recebemos um polinômio $r(x) \neq c(x) \in \mathbb{Z}_2[x]$, de grau menor que n. Sabe-se que $c(x) = r(x) + e(x)$, para algum polinômio não-nulo $e(x)$ de grau menor que n em $\mathbb{Z}_2[x]$. Seja $e(x) = x^{m_1} + x^{m_2} + \ldots + x^{m_q}$, com $q \leqslant t$ e $m_q < n$. Observe que q é o número de erros da palavra recebida. Temos que as raízes do polinômio

$$\begin{aligned} E(z) &= (z - \alpha^{m_1})(z - \alpha^{m_2}) \ldots (z - \alpha^{m_q}) \\ &= z^q + \delta_1 z^{q-1} + \ldots + \delta_q, \end{aligned}$$

nos dão as posições dos erros em $r(x)$ [1].

Para encontrar δ_i, com $i \in \{1, \ldots, q\}$, usamos

$$\begin{bmatrix} r_1 & \ldots & r_q \\ \vdots & & \vdots \\ r_q & \ldots & r_{2q-1} \end{bmatrix} \begin{bmatrix} \delta_q \\ \vdots \\ \delta_1 \end{bmatrix} = \begin{bmatrix} r_{q+1} \\ \vdots \\ r_{2q} \end{bmatrix},$$

onde $r_i = r(\alpha^i) = e(\alpha^i)$, com $i \in \{1, 2, \ldots, 2q\}$ e $q = t$, inicialmente.

Seja A a matriz $q \times q$ dos coeficientes, o sistema é possível e determinado somente se $\text{Det}A \neq 0$. Caso contrário, $r(x)$ não possui exatamente t erros e devemos reduzir q até que tenhamos $\text{Det}A \neq 0$. Se $\text{Det}A = 0$ para qualquer $q \leqslant t$, $r(x)$ não é corretível.

Referências

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

[2] FJ Williams and NJA Sloane, *The theory of error-correcting codes*, North-Holland, 1977.