Tópicos Avançados em Ciência da Computação I: Introdução à Teoria de Códigos para Criptografia Pós-quântica

Daniel Panario
School of Mathematics and Statistics
Carleton University

IC - Unicamp, Sala 351 do IC-3
das 13:30 as 18:30 em 16-17 de janeiro de 2020,
das 13:30 as 17:30 em 20-24 de janeiro de 2020

Introdução à Teoria de Códigos: Parte IV

Daniel Panario
School of Mathematics and Statistics
Carleton University

16-24 de janeiro de 2020

Conteúdo da aula

- Códigos cíclicos e de Hamming
- Códigos BCH (que corrigem dois erros)
- Códigos BCH (que corrigem t erros)
- Códigos de Reed-Solomon
- Proposta NIST: Hamming Quasi-Cyclic (HQC)

Códigos cíclicos

Definição

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico, se $(c_0,\ldots,c_{n-1}) \in C$ implica que $(c_{n-1},c_0,\ldots,c_{n-2}) \in C$.

Exemplo: $C = \{000, 110, 101, 011\}$ é um código cíclico.

Exemplo: Seja o código com matriz de paridade:

$$H = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Vemos que $(0,1,0,1,1,0,0)$ é uma palavra de código:

$$H \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Deslocando uma posição temos a palavra $(0, 0, 1, 0, 1, 1, 0)$:

$$H \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Exercício: prove que esse código é cíclico.

Códigos cíclicos e polinômios

Códigos cíclicos podem ser caracterizados com polinômios.

Teorema

Um código linear $C(n, k)$ sobre $\mathbb{F}_q$ é cíclico se e somente se C é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

Retornaremos q esse teorema após ter visto a álgebra de polinômios sobre corpos finitos necessária.

Teorema

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico se e somente se C é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

Demonstração.

Se C é um código cíclico e $c(x) \in C$, temos que $xc(x)$, $x^2c(x)$, $x^3c(x), \ldots$ também pertencem a C. Seja $a(x) = \sum_i a_i x^i \in \mathbb{F}_q[x]/(x^n - 1)$. Como $a(x)c(x) = \sum_i a_i(x^i c(x))$ e C é um subespaço vetorial sobre $\mathbb{F}_q$, temos que C é um ideal.

Reciprocamente, se C é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$ e $c(x) = \sum_{i=0}^{n-1} c_i x^i$ é uma palavra-código, então $xc(x)$ também é uma palavra-código. Logo, C é cíclico. $\square$

Teorema

Um código linear $C(n,k)$ sobre $\mathbb{F}_q$ é cíclico se e somente se C é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$.

Demonstração.

Se C é um código cíclico e $c(x) \in C$, temos que $xc(x)$, $x^2c(x)$, $x^3c(x), \ldots$ também pertencem a C. Seja $a(x) = \sum_i a_i x^i \in \mathbb{F}_q[x]/(x^n - 1)$. Como $a(x)c(x) = \sum_i a_i(x^i c(x))$ e C é um subespaço vetorial sobre $\mathbb{F}_q$, temos que C é um ideal.

Reciprocamente, se C é um ideal de $\mathbb{F}_q[x]/(x^n - 1)$ e $c(x) = \sum_{i=0}^{n-1} c_i x^i$ é uma palavra-código, então $xc(x)$ também é uma palavra-código. Logo, C é cíclico. $\square$

Daniel Panario | Introdução à Teoria de Códigos: Parte IV | 16-24 de janeiro de 2020 | 7 / 46

Códigos e ideais de polinômios

Num domìnio de ideais principais (PID), todo ideal de um anel é gerado por um elemento. Quando $\mathbb{F}$ é um corpo, $\mathbb{F}[x]$ é um PID.

Temos que $\mathbb{F}_q$ é um corpo e, então, $\mathbb{F}_q[x]$ é um PID e cada ideal é gerado por um polinômio.

O seguinte teorema mostra que cada ideal não nulo de $\mathbb{F}_q[x]/(x^n - 1)$ é gerado por um polinômio mônico g de grau mínimo no ideal. Para isto necessitamos da seguinte definição.

Definição

Seja $C = (g)$ um código cíclico. Dizemos que g é o polinômio gerador de C e $h = (x^n - 1)/g$ é o polinômio verificador de C.

Teorema

Seja C um ideal não nulo em $\mathbb{F}_q[x]/(x^n - 1)$, isto é, C é um código cíclico de comprimento n.

(a) *Existe um único polinômio mônico g de grau mínimo em C.*

(b) *O código C é gerado por um único polinômio mônico g de grau mínimo em C.*

(c) *O polinômio gerador g de C é um fator de $x^n - 1$.*

(d) *Em $\mathbb{F}_q[x]$, qualquer $c \in C$ pode ser escrito unicamente como $c = fg$, onde $\mathrm{grau}(f) < n - r$ e $\mathrm{grau}(g) = r$. Além disso, a dimensão de C é $n - r$. (Assim, a mensagem f se torna a palavra-código fg.)*

Teorema

(e) *Se* $g(x) = g_0 + g_1 x + \cdots + g_r x^r$*, então* C *é gerado como um subespaço de* $\mathbb{F}_q^n$ *pelas linhas da matriz geradora*

$$G = \begin{bmatrix} g_0 & g_1 & \cdot & \cdot & \cdot & g_r & 0 & 0 & 0 \\ 0 & g_0 & g_1 & \cdot & \cdot & \cdot & g_r & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & 0 & g_0 & g_1 & \cdot & \cdot & \cdot & g_r \end{bmatrix}$$

$$= \begin{bmatrix} g(x) & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ 0 & xg(x) & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & x^{n-r-1}g(x) \end{bmatrix}.$$

Demonstração do teorema

(a) Suponha que existam dois polinômios $f, g \in C$ mônicos de grau mínimo r. Então $f - g \in C$ tem grau menor, uma contradição, a menos que $f - g = 0$, ou $f = g$.

(b) Suponha que $c \in C$ e considere a divisão de c por g. Temos que

$$c = q_0 g + r_0,$$

para polinômios q_0 e r_0 com $\mathrm{grau}(r_0) < \mathrm{grau}(g) = r$. Isto significa que $c - q_0 g \in C$ dado que o código é um ideal, e $c, g \in C$. Então, $r_0 \in C$ com grau menor que $\mathrm{grau}(g)$, uma contradição a menos que $r_0 = 0$. Temos que $c = q_0 g$ e $c \in (g)$.

(c) Em $\mathbb{F}_q[x]$, a divisão de $x^n - 1$ por $g(x)$ da $x^n - 1 = h(x)g(x) + r_1(x)$ onde $\mathrm{grau}(r_1) < \mathrm{grau}(g)$. Em $\mathbb{F}_q[x]/(x^n - 1)$, isto significa que $r_1(x) = -h(x)g(x)$ com $\mathrm{grau}(r_1) < \mathrm{grau}(g)$, uma contradição a menos que $r_1 = 0$. Temos que $g(x)|(x^n - 1)$.

Demonstração do teorema (cont)

(d-e) Seja $c \in C$ com $\mathrm{grau}(c) < n$, e seja $\mathrm{grau}(g) = r$. Pela parte (b), existe um polinômio q_1 tal que $c = q_1 g$ em $\mathbb{F}_q[x]/(x^n - 1)$. Desse modo, em $\mathbb{F}_q[x]$,

$$c(x) = q_1(x)g(x) + l(x)(x^n - 1).$$

Pela parte (c), vamos supor que $x^n - 1 = g(x)h(x)$. Então,

$$c(x) = (q_1(x) + l(x)h(x))g(x) = f(x)g(x).$$

Temos que $c = fg$ onde $\mathrm{grau}(f) \leq n - r - 1$, e o código é formado pelos multiplos de g; esses multiplos são polinômios de grau $n - r - 1$ como máximo.
Há $n - r$ multiplos linearmente independentes de g, ou seja, $g(x), xg(x), x^2g(x), \ldots, x^{(n-r-1)}g(x)$. Os vetores correspondentes são as linhas da matriz geradora G. Assim, o código tem dimensão $n - r$. Finalmente, para codificar f consideramos $fG = c$ dado que

$$(f_0, f_1, \ldots, f_{n-r+1})G = (f_0g_0, f_1g_0 + f_0g_1, \ldots) = fg = c. \qquad \square$$

Check polynomial

Before we consider examples of cyclic codes (like Hamming and 2-error BCH codes), let us define the check polynomial and the parity-check matrix of a cyclic code.

Definição

Let C be a cyclic code with generator polynomial $g(x)$. From the previous theorem, we know that

$$g(x) | (x^n - 1).$$

The polynomial $h(x) = (x^n - 1)/g(x)$ is the check polynomial of C.

We justify the name in the following comments. Let $f(x)$ be a message encoded by multiplication by $g(x)$

$$c(x) = f(x)g(x) = \sum_{i=0}^{n-1} c_i x^i.$$

Then,
$$c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1).$$
Thus, $c(x)h(x) = 0$ in $\mathbb{F}_q[x]/(x^n - 1)$.

Now,
$$c(x)h(x) = \left(\sum_{i=0}^{n-1} c_i x^i\right)\left(\sum_{\ell=0}^{k} h_\ell x^\ell\right),$$
where $h_k \neq 0$. For $j = 0, 1, \ldots, n-1$, the coefficient of x^j in this product is (observe that $i + \ell = j$)
$$\sum_{i=0}^{n-1} c_i h_{j-i} = 0, \tag{1}$$
where the subscripts are taken modulo n, and we have $h_{n-1} = h_{n-2} = \cdots = h_{k+1} = 0$. So, if $c \in C$, then Equation (1) implies that $Hc^T = 0$, where the parity-check matrix H is given by

$$H = \begin{bmatrix} 0 & \cdot & \cdot & \cdot & 0 & h_k & h_{k-1} & \cdot & \cdot & \cdot & h_1 & h_0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ h_k & h_{k-1} & \cdot & \cdot & \cdot & h_1 & h_0 & 0 & \cdot & \cdot & \cdot & 0 \end{bmatrix},$$

or with the polynomial notation we used for G:

$$H = \begin{bmatrix} 0 & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & h(x) \\ 0 & 0 & 0 & \cdot & \cdot & \cdot & 0 & xh(x) & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ x^{n-k-1}h(x) & 0 & 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 \end{bmatrix}.$$

The dimension of the code is:

$$\dim\ C = n - \deg(g) = n - r = \deg(h) = k.$$

(We recall that if the parity-check matrix has dimension $(n-k) \times n$, n is the length of the code and k is the dimension of the code.)

In the following we show classical examples of generator matrix and parity-check matrix for cyclic codes.

Códigos de Hamming

Definição

Seja m um inteiro maior ou igual a 2. Um código binário C_m, de comprimento $n = 2^m - 1$, com uma matriz de paridade H de ordem $m \times (2^m - 1)$ é chamado de código binário de Hamming, se as colunas de H correspondem às representações binárias dos inteiros $1, 2, \ldots, 2^m - 1$.

Exemplo: C_3 tem matriz de paridade

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A dimensão de C_m é $2^m - 1 - m$. Quaisquer duas colunas são linearmente independentes, já que nenhuma coluna é múltipla da outra.

Por outro lado, há três colunas que são linearmente dependentes. Por exemplo,

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} + \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 1 \end{pmatrix}.$$

Concluímos que a distância mínima de C_m é $2 + 1 = 3$ e assim C_m corrige um erro.

Seja α um elemento primitivo de $\mathbb{F}_{2^m}$. Podemos escrever a matriz de paridade do código de Hamming de comprimento $n = 2^m - 1$ como

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \end{pmatrix}.$$

Então um vetor $c = (c_0, c_1, \ldots, c_{n-1})$ pertence ao código de Hamming se e somente se $Hc^T = 0$. Temos que

$$\begin{aligned} (c_0, c_1, \ldots, c_{n-1}) \in C &\Leftrightarrow HC^T = 0 \\ &\Leftrightarrow \textstyle\sum_{i=0}^{n-1} c_i\alpha^i = 0 \\ &\Leftrightarrow c(\alpha) = 0, \end{aligned}$$

onde usamos a correspondência

$$(c_0, c_1, \ldots, c_{n-1}) \longleftrightarrow c_0 + \cdots + c_{n-1}x^{n-1}.$$

Como $c(x)$ tem raiz α, o polinômio minimal de α deve dividir $c(x)$, ou seja, $M^{(1)}(x)|c(x)$. Com isso, mostramos que $c \in C$ se e somente se $M^{(1)}|c(x)$.

Em outras palavras, um código de Hamming é formado pelos múltiplos de $M^{(1)}(x)$. Podemos concluir que $M^{(1)}(x)$ é um polinômio gerador do código de Hamming.

Também temos que $\mathrm{grau}(M_1) = m$ e

$$M^{(1)}(x) = (x - \alpha)(x - \alpha^2) \cdots (x - \alpha^{2^{m-1}}).$$

Teorema

O código de Hamming com parâmetros $n = 2^m - 1$, $k = n - m$ e $d = 3$ é um código com matriz geradora

$$G = \begin{pmatrix} M^{(1)} & 0 & \cdot & \cdot & \cdot & 0 \\ 0 & xM^{(1)} & \cdot & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & x^{n-m-1}M^{(1)} \end{pmatrix},$$

onde o polinômio $M^{(1)} = g$ (o polinômio gerador do código), é o polinômio minimal dos elementos na classe lateral ciclotômica $C_1 = \{1, 2, 4, \dots\}$ módulo $n = 2^m - 1$.

Exemplo

Para $n = 2^3 - 1 = 7$ e $m = 3$, temos que $M^{(1)}(x) = 1 + x + x^3$ é o polinômio minimal dos elementos na classe lateral ciclotômica $C_1 = \{1, 2, 4\}$ módulo 7 e, então, a matriz geradora é

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

Se não conhecermos a matriz de paridade H, podemos usar que $h(x) = (x^7 - 1)/(x^3 + x + 1) = x^4 + x^2 + x + 1$ e, assim, temos que

$$H = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Códigos BCH que corrigem dois erros

Idéia (Bose-Chaudhuri-Hocquenghem): considerar uma matriz de paridade com $2m$ linhas, de tal maneira que as primeiras m linhas sejam iguais às da matriz do código de Hamming, ao passo que as m linhas restantes tenham o propósito de corrigir dois erros.

Definição

Seja m um inteiro maior ou igual a 2. Definimos o código binário BCH que corrige dois erros, como sendo o código C de comprimento $n = 2^m - 1$, com matriz de paridade de ordem $2m \times (2^m - 1)$, dada por

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)} \end{pmatrix},$$

onde α é um elemento primitivo de $\mathbb{F}_{2^m}$.

Porque não funciona se as m linhas restantes forem $(1\ \alpha^2\ \alpha^4 \cdots)$?

Códigos BCH que corrigem dois erros

Idéia (Bose-Chaudhuri-Hocquenghem): considerar uma matriz de paridade com $2m$ linhas, de tal maneira que as primeiras m linhas sejam iguais às da matriz do código de Hamming, ao passo que as m linhas restantes tenham o propósito de corrigir dois erros.

Definição

Seja m um inteiro maior ou igual a 2. Definimos o código binário BCH que corrige dois erros, como sendo o código C de comprimento $n = 2^m - 1$, com matriz de paridade de ordem $2m \times (2^m - 1)$, dada por

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)} \end{pmatrix},$$

onde α é um elemento primitivo de $\mathbb{F}_{2^m}$.

Porque não funciona se as m linhas restantes forem $(1\ \alpha^2\ \alpha^4 \cdots)$?

Códigos BCH que corrigem dois erros

Idéia (Bose-Chaudhuri-Hocquenghem): considerar uma matriz de paridade com $2m$ linhas, de tal maneira que as primeiras m linhas sejam iguais às da matriz do código de Hamming, ao passo que as m linhas restantes tenham o propósito de corrigir dois erros.

Definição

Seja m um inteiro maior ou igual a 2. Definimos o código binário BCH que corrige dois erros, como sendo o código C de comprimento $n = 2^m - 1$, com matriz de paridade de ordem $2m \times (2^m - 1)$, dada por

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)} \end{pmatrix},$$

onde α é um elemento primitivo de $\mathbb{F}_{2^m}$.

Porque não funciona se as m linhas restantes forem $(1\ \alpha^2\ \alpha^4 \cdots)$?

Introdução aos códigos BCH que corrigem dois erros

Consider, as an example, the Hamming code with $m = 4, n = 15$:

$$H' = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

If we denote each column by the number they represent from 1 to 15, and we denote by $f(i)$, $i = 1, \ldots, 15$, the 4-tuple in the last four rows of column i, then the parity-check matrix becomes

$$H = \begin{pmatrix} 1 & 2 & \cdots & 14 & 15 \\ f(1) & f(2) & \cdots & f(14) & f(15) \end{pmatrix},$$

where the column i is an 8-tuple, $i = 1, \ldots, 15$,

$$H_i = \begin{pmatrix} i \\ f(i) \end{pmatrix}.$$

Códigos BCH que corrigem dois erros

Now, the question is how do we choose f such that we can correct up to 2 errors? This means

$$S(y) = H_i + H_j = \begin{pmatrix} i \\ f(i) \end{pmatrix} + \begin{pmatrix} j \\ f(j) \end{pmatrix} = \begin{pmatrix} i+j \\ f(i)+f(j) \end{pmatrix} = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}.$$

The question is, then, how do we find i and j given z_1 and z_2?
We have to solve the following system for i, j given z_1 and z_2:

$$\begin{array}{rcl} i+j & = & z_1 \\ f(i)+f(j) & = & z_2. \end{array}$$

In order to solve this system, we have to add, subtract, multiply and divide 4-tuples. That is the 4-tuples have to form a field.

Códigos BCH que corrigem dois erros

The next step is to choose the function f for the BCH code due to Bose, Ray-Chaudhuri and Hocquenghem (1959-1960). Remember that we want that the previous system has a solution, so we can correct two errors.

1st try: Let us consider a linear function $f(i) = ci$ where c is a constant. We have

$$\begin{array}{rcl} i+j & = & z_1 \\ ci+cj & = & z_2, \end{array}$$

that is, the second equation is a multiple of the first one. Thus, these equations are redundant and cannot solve the system.

Códigos BCH que corrigem dois erros

2nd try: Next, let us consider a quadratic function $f(i) = i^2$. The system becomes

$$\begin{aligned} i + j &= z_1 \\ i^2 + j^2 &= z_2. \end{aligned}$$

This may look promising but it is not since over $\mathbb{F}_2$

$$(i+j)^2 = i^2 + j^2,$$

and thus, again, the equations are redundant. The problem with the function $f(i) = i^2$ is that we are working over $\mathbb{F}_2$.

Códigos BCH que corrigem dois erros

3rd try: Let us consider $f(i) = i^3$. The system is now

$$\begin{aligned} i + j &= z_1 \\ i^3 + j^3 &= z_2. \end{aligned}$$

In this case,

$$\begin{aligned} z_2 &= i^3 + j^3 = (i+j)(i^2 + ij + j^2) \\ &= z_1(i^2 + j^2 + ij) = z_1(z_1^2 + ij). \end{aligned}$$

So, if $z_1 \neq 0$, the system is

$$\begin{aligned} i + j &= z_1 \\ ij &= \frac{z_2}{z_1} + z_1^2. \end{aligned}$$

This provides a system that we can solve for i, j.

Códigos BCH que corrigem dois erros

If $z_1 \neq 0$, the system is

$$\begin{aligned} i + j &= z_1 \\ ij &= \frac{z_2}{z_1} + z_1^2, \end{aligned}$$

and with $i + j$ and ij we can write the equation:

$$x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2 \right) = 0 \qquad (z_1 \neq 0).$$

Bad news: over finite fields, we cannot apply the formula for the roots of an equation of degree two, as we normally do over $\mathbb{R}$. We have to try pairs i, j but the method above gives a straightforward algorithm for BCH 2-error decoding.

Códigos BCH que corrigem dois erros

If $z_1 \neq 0$, the system is

$$\begin{aligned} i + j &= z_1 \\ ij &= \frac{z_2}{z_1} + z_1^2, \end{aligned}$$

and with $i + j$ and ij we can write the equation:

$$x^2 + z_1 x + \left(\frac{z_2}{z_1} + z_1^2 \right) = 0 \qquad (z_1 \neq 0).$$

Bad news: over finite fields, we cannot apply the formula for the roots of an equation of degree two, as we normally do over $\mathbb{R}$. We have to try pairs i, j but the method above gives a straightforward algorithm for BCH 2-error decoding.

Códigos BCH que corrigem dois erros (de novo)

Idéia (Bose-Chaudhuri-Hocquenghem): considerar uma matriz de paridade com $2m$ linhas de tal maneira que as primeiras m linhas sejam iguais às da matriz do código de Hamming, ao passo que as m linhas restantes tenham o propósito de corrigir dois erros.

Definição

Seja m um inteiro maior ou igual a 2. Definimos o código binário BCH que corrige dois erros, como sendo o código C de comprimento $n = 2^m - 1$, com matriz de paridade de ordem $2m \times (2^m - 1)$, dada por

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{2^m-2} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(2^m-2)} \end{pmatrix},$$

onde α é um elemento primitivo de $\mathbb{F}_{2^m}$.

$$\begin{aligned} c \in C &\iff Hc^T = 0 \\ &\iff \textstyle\sum_{i=0}^{n-1} c_i\alpha^i = 0 \text{ e } \sum_{i=0}^{n-1} c_i\alpha^{3i} = 0 \\ &\iff c(\alpha) = 0 \text{ e } c(\alpha^3) = 0 \\ &\iff M^{(1)} \mid c \text{ e } M^{(3)} \mid c, \end{aligned}$$

onde $M^{(3)}$ é o polinômio minimal de α^3. Como $M^{(1)}$ e $M^{(3)}$ são irredutíveis e distintos, temos que $c \in C$ se e somente se $M^{(1)}M^{(3)}$ divide c. Assim $M^{(1)}M^{(3)}$ é um gerador do código binário BCH que corrige dois erros. Não é difícil demonstrar que, quando $p = 2$ e $n = 2^m - 1$ com $m \geq 3$, temos $\mathrm{grau}(M^{(1)}) = \mathrm{grau}(M^{(3)}) = m$. Logo, $\mathrm{grau}(g) = 2m$ e $k = n - 2m$.

Teorema

O código binário BCH que corrige dois erros com parâmetros $n = 2^m - 1$, $k = n - 2m$, $d \geq 5$ e $m \geq 3$ tem polinômio gerador $g = M^{(1)}M^{(3)}$, onde $\mathrm{grau}(M^{(1)}) = \mathrm{grau}(M^{(3)}) = m$.

Exemplo

Consideremos o código binário BCH que corrige dois erros com comprimento $n = 15$, $m = 4$ e

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^i & \cdots & \alpha^{14} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3i} & \cdots & \alpha^{3(14)} \end{pmatrix}.$$

Sejam $\mathbb{F}_{2^4} \cong \mathbb{F}_2[x]/(x^4 + x + 1)$ e α um elemento primitivo de $\mathbb{F}_{2^4}$. As classes laterais ciclotômicas módulo 15 são

$$C_0 = \{0\},\ C_1 = \{1, 2, 4, 8\},\ C_3 = \{3, 6, 12, 9\},$$
$$C_5 = \{5, 10\},\ C_7 = \{7, 14, 13, 11\}.$$

Como α é primitivo, o polinômio minimal de α é $x^4 + x + 1$.
O polinômio minimal de α^3 é $x^4 + x^3 + x^2 + x + 1$; então,

$$g(x) = (x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1).$$

A matriz de paridade H é obtida com o polinômio

$$h(x) = (x^{15} - 1)/g(x) = x^7 + x^6 + x^4 + 1.$$

Códigos BCH que corrigem t erros

So far we have not commented much on the distance of the code. In general, it is very difficult to find d. Next, we show a lower bound on d if the zeros of the generator polynomial g are known.

Let C be a cyclic code with generator polynomial g. We know that $g(x)|(x^n - 1)$. Let

$$g(x) = \prod_{j \in K} (x - \alpha^j),$$

where K is the union of some cyclotomic cosets. Then, α^i is a zero of the code if and only if $i \in K$. Otherwise, α^i is a nonzero of the code (we have that the nonzeros of the code are the zeros of h).

BCH bound

Teorema (BCH Bound)

Let C be a cyclic code with generator polynomial g such that for some integers $b \geq 0$ and $\delta \geq 1$, we have

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0.$$

That is, the code has a string of $\delta - 1$ consecutive powers of α zeros. Then, the minimum distance d of the code satisfies $d \geq \delta$.

Demonstração. If $c = (c_0, c_1, \ldots, c_{n-1}) \in C$, $c(x)$ is such that

$$c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+\delta-2}) = 0,$$

since the generator polynomial is zero in $\alpha^b, \ldots, \alpha^{b+\delta-2}$.
Let us consider the matrix H':

BCH bound (cont)

$$H' = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & \alpha^{2(b+\delta-2)} & \cdots & \alpha^{(n-1)(b+\delta-2)} \end{pmatrix}.$$

Then, $H'c^T = 0$. We observe that H' does not need to be the full parity check matrix H of the code.

Let us prove that any $\delta - 1$ columns are linearly independent, and then using a theorem that we proved $d \geq \delta$; if, in addition, we can prove that there exist δ columns that are linearly dependent, then the minimum distance d would be exactly δ.

BCH bound (cont)

Consider any $\delta - 1$ distinct columns of H'. Taking the determinant we obtain

$$\begin{vmatrix} \alpha^{a_1 b} & \alpha^{a_2 b} & \dots & \alpha^{a_{\delta-1} b} \\ \alpha^{a_1(b+1)} & \alpha^{a_2(b+1)} & \dots & \alpha^{a_{\delta-1}(b+1)} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{a_1(b+\delta-2)} & \alpha^{a_2(b+\delta-2)} & \dots & \alpha^{a_{\delta-1}(b+\delta-2)} \end{vmatrix}$$

$$= \alpha^{a_1 b + a_2 b + \cdots + a_{\delta-1} b} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{a_1} & \alpha^{a_2} & \dots & \alpha^{a_{\delta-1}} \\ \alpha^{2a_1} & \alpha^{2a_2} & \dots & \alpha^{2a_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \end{vmatrix} \neq 0.$$

This is a Vandermonde determinant. Hence, the determinant is the product of $\alpha^{a_i} - \alpha^{a_j}$, for all i, j, and thus, the product is different from zero. The homogeneous system of equations has the unique null solution, and so the columns are linearly independent. □

Exemplos

Example 1: The binary Hamming code has generator polynomial $M^{(1)}(x)$. We have $M^{(1)}(\alpha) = 0$. Now, the minimum polynomial of α and $\alpha^p = \alpha^2$ is the same. Hence $M^{(1)}(\alpha^2) = 0$, and we have two consecutive powers of α that are zero. By the previous theorem, the minimum distance $d \geq 3$.

Example 2: The 2-error-correcting BCH code has generator polynomial $M^{(1)}(x)M^{(3)}(x)$.

$$M^{(1)}(\alpha) = M^{(1)}(\alpha^2) = M^{(1)}(\alpha^4) = 0$$

$$M^{(3)}(\alpha^3) = M^{(3)}(\alpha^6) = 0$$

We have four consecutive powers of α that are zeros of $g(x) = M^{(1)}(x)M^{(3)}(x)$, and so, the minimum distance $d \geq 5$.

Códigos BCH que corrigem t erros

Definição

Um código cíclico de comprimento n sobre $\mathbb{F}_q$ é um código BCH de distância de projeto D se, para certos inteiros $b \geq 0$ e $D \geq 1$, temos que

$$g(x) = \operatorname{lcm}(M^{(b)}, M^{(b+1)}, \dots, M^{(b+D-2)}).$$

Em outras palavras, g é o polinômio minimal de menor grau sobre $\mathbb{F}_q$ que possui $\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+D-2}$ como zeros, e temos

$$c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+D-2}) = 0,$$

se e somente se $c = (c_0, c_1, \dots, c_{n-1}) \in C$.

O teorema anterior implica que $d \geq D$. Se $D \geq 2t+1$, podemos corrigir t erros. Logo, isto nos permite obter códigos com distância de projeto D e capacidade de corrigir t erros.

Vamos estudar a matriz de paridade H. Temos que $c \in C$ se e somente se $c(\alpha^b) = c(\alpha^{b+1}) = \cdots = c(\alpha^{b+D-2}) = 0$, ou seja,

$$H = \begin{pmatrix} 1 & \alpha^b & \alpha^{2b} & \dots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \dots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+D-2} & \alpha^{2(b+D-2)} & \dots & \alpha^{(n-1)(b+D-2)} \end{pmatrix},$$

onde cada entrada é substituída pela coluna correspondente de m elementos em $\mathbb{F}_q$. Temos que $\operatorname{grau}(g) = n - \dim(C)$. Como

$$g = \operatorname{lcm}(M^{(b)}, M^{(b+1)}, \dots, M^{(b+D-2)})$$

e $\operatorname{grau}(M^{(i)}) \leq m$, temos que $\operatorname{grau}(g) \leq m(D-1)$ e, assim, $\dim(C) \geq n - m(D-1)$. Provamos assim o seguinte teorema.

Teorema

Um código BCH sobre $\mathbb{F}_q$ de comprimento n e distância de projeto D tem distância mínima $d \geq D$ e dimensão $\geq n - m(D-1)$.

Em certos casos particulares, os códigos BCH tem nomes especiais.

1. Se $b = 1$, o código é chamado BCH no sentido estrito.
2. Se $n = q^m - 1$, o código BCH é chamado primitivo.
   Neste caso, α é um elemento primitivo.
3. Se $n = q - 1$, o código BCH é chamado o código de Reed-Solomon.

Códigos de Reed-Solomon tem comprimento $n = q - 1$. Então, não consideramos $q = 2$, porém o corpo pode ser uma extensão de $\mathbb{F}_2$.

Códigos BCH que corrigem t erros são usados no sistema criptográfico Hamming Quasi-Cyclic (HQC).

Exemplos

Examples: (1) A lista de todos os códigos BCH (binários, sentido estrito, primitivo) de comprimento 15:

distância planejada	polinômio gerador	expoentes das raizes de $g(x)$	dimensão $n - \deg(g(x))$	distância
1	1	-	15	1
3	$M^{(1)}(x)$	1, 2, 4, 8	11	3
5	$M^{(1)}M^{(3)}$	1-4, 6, 8, 9, 12	7	5
7	$M^{(1)}M^{(3)}M^{(5)}$	1-6, 8-10, 12	5	7
9, 11, 13, 15	$M^{(1)}M^{(3)}M^{(5)}M^{(7)}$	1-14	1	15

Exemplos (cont)

Example (2) A lista de todos os códigos BCH (binários, sentido estrito, primitivo) de comprimento 31:

distância planejada	polinômio gerador	dimensão $n - \deg(g(x))$	distância
1	1	31	1
3	$M^{(1)}(x)$	26	3
5	$M^{(1)}M^{(3)}$	21	5
7	$M^{(1)}M^{(3)}M^{(5)}$	16	7
9 or 11	$M^{(1)}M^{(3)}M^{(5)}M^{(7)}$	11	11
13 or 15	$M^{(1)}M^{(3)}M^{(5)}M^{(7)}M^{(11)}$	6	15
17, 19, ..., 31	$M^{(1)}M^{(3)}M^{(5)}M^{(7)}M^{(11)}M^{(15)}$	1	31

Códigos de Reed-Solomon (breve)

Os códigos Reed-Solomon são usados na prática em muitos problemas. Por exemplo, ele são usados na comunicação pela NASA e pela Agência Espacial Européia. Em algumas aplicações, os códigos Reed-Solomon são usados em combinação com outros códigos, tais como os códigos convolucionais, por exemplo. São também usados para recuperar erros em CDs.

Como $n = q - 1$, temos que $x^n - 1 = x^{q-1} - 1 = \prod_{\beta \in \mathbb{F}_q^*} (x - \beta)$. Isto implica que o polinômio minimal de α^i seja $M^{(i)}(x) = x - \alpha^i$.

Portanto, um código Reed-Solomon de comprimento $n = q - 1$ e distância de projeto D tem polinômio gerador

$$g(x) = (x - \alpha^b)(x - \alpha^{b+1}) \cdots (x - \alpha^{b+D-2}),$$

onde é usual tomar $b = 1$, ou seja, no sentido estrito.

Exemplo

Sejam $q = 5$ *e* $n = q - 1 = 4$. *Queremos distância de projeto* $D = 3$. *Um elemento primitivo em* $\mathbb{F}_5$ *é* $\alpha = 2$. *Então* $g(x) = (x - \alpha)(x - \alpha^2) = (x - 2)(x - 4) = x^2 + 4x + 3$.
Como $k = n - \mathrm{grau}(g) = 4 - 2 = 2$, *a dimensão do código é* 2. *Assim, temos* $q^k = 5^2 = 25$ *palavras-código. A matriz geradora é*

$$G = \begin{pmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{pmatrix}.$$

Alguns exemplos de palavras-código são:

$$\begin{aligned} (0\ 0)G &= (0\ 0\ 0\ 0), \quad (1\ 0)G = (3\ 4\ 1\ 0), \\ (2\ 0)G &= (1\ 3\ 2\ 0), \quad (3\ 0)G = (4\ 2\ 3\ 0), \\ (4\ 0)G &= (2\ 1\ 4\ 0). \end{aligned}$$

Exemplo

Sejam $q = 4$ *e* $n = q - 1 = 3$. *Queremos distância de projeto* $D = 2$ *e* $b = 2$ *(não no sentido estrito). Se considerarmos* $x^2 + x + 1 \in \mathbb{F}_2[x]$ *como o polinômio irredutível definindo* $\mathbb{F}_{2^2}$, *temos* $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\}$, *onde* α *é uma raiz de* $x^2 + x + 1$ *(neste caso,* $\beta = \alpha + 1 = \alpha^2$*). Então o polinômio gerador é* $g(x) = x - \alpha^2 = x - \beta$ *e a matriz geradora é*
$$G = \begin{pmatrix} \beta & 1 & 0 \\ 0 & \beta & 1 \end{pmatrix}.$$

Códigos MDS

A dimensão de um código Reed-Solomon é sempre

$$k = n - \mathrm{grau}(g) = n - D + 1.$$

A distância mínima d é, pela cota BCH é, pelo menos, D:

$$d \geq D = n - k + 1.$$

Pela cota de Singleton tem-se que $d \leq n - k + 1$; logo,
para códigos Reed-Solomon sempre temos $d = n - k + 1$.

Em geral, códigos com $d = n - k + 1$ são chamados MDS (distância máxima separável). Esses códigos conseguem atingir a distância mínima mais alta possível para os parâmetros dados.

Assim, os códigos de Reed-Solomon são códigos MDS.

Proposta NIST: Hamming Quasi-Cyclic (HQC)

A proposta de NIST Hamming Quasi-Cyclic (HQC) usa fortemente códigos BCH, incluindo a decodificação por síndrome desses códigos, e boa parte da informação que acabamos de ver.

Por mais informação ver
`http://pqc-hqc.org/doc/hqc-specification_2019-08-24.pdf`

No arquivo de slides da rodada 2 da competição, ler o material das seções 1.1 (especificação do sistema) e 1.5 ("coding theory components and decoding, with error analysis").