Códigos especiales

En el caso en que trabajemos con códigos lineales grandes, se vuelve muy costoso encontrar todos los líderes de las clases con pesos mínimos. Por lo tanto es conveniente construir códigos especiales con mejores algoritmos de decodificación.

Antes de hacerlo observemos lo siguiente:

Teorema: En un código lineal binario con parámetros n y k y con matriz de control H el síndrome de una palabra recibida con error es la suma de las columnas de H que corresponden a las posiciones en donde ocurrieron errores.

Demostración

Sea $c \in C$ que se envía por un canal y se recibe $y = c + e \quad e \neq 0$. Entonces

$$S(y) = S(c+e) = S(e) = e \cdot H^T.$$

Si $i_1, i_2, \ldots, i_j \quad 1 \leq j \leq n$ son las posiciones en donde

$H_{(n-k)\times n}$

se cometieran los errores, es decir

$$e = (0 \dots 0 \underset{i_1}{1} \dots \underset{i_2}{1} \dots \underset{i_3}{1} \dots 0 \dots 0)_n$$

entonces si $H = (h_1\ h_2 \dots h_n)$

$$S(y) = S(e) = eH^T = (0 \dots 0 \underset{i_1}{1} \dots \underset{i_2}{1} \dots) \begin{pmatrix} h_1^T \\ h_2^T \\ \vdots \\ h_n^T \end{pmatrix}$$

$$= h_{i_1}^T + h_{i_2}^T + \dots + h_{i_j}^T$$

Si todas las columnas de H son distintas y el canal puede cometer como máximo un único error entonces si ese error se comete en la i-ésima posición entonces $S(y) = h_i$ y se puede corregir cambiando el símbolo de la posición i.

Para simplificar el proceso de localización de errores, se introducen los siguientes códigos.

Def: Un código binario C_m de longitud $n = 2^m - 1$ $m \geq 2$ con matriz de cheques de paridad H de $m \times (2^m - 1)$ se llama código binario de Hamming si las columnas de H son las representaciones binarias de los enteros $1, 2, \ldots, 2^m - 1$.

(m: $n-k$; 2^m-1: n)

Lema: El código de Hamming C_m es un

$$[2^m - 1,\ 2^m - 1 - m,\ 3]$$

Código binario, $m \geq 2$.

Demostración

$n = 2^m - 1$ y $k = \underbrace{2^m - 1 - m}_{n-(n-k)}$ por la definición de H.

Además dos columnas cualquiera son l.i, pero la suma de dos columnas cualesquiera es otra columna de H, y por un resultado anterior esto implica que $d = 3$.

Ejemplo: Consideremos el código binario de Hamming C_3. En este caso $m=3$, $n=2^m-1=2^3-1=7$ y la dimensión es $k=7-3=4$.

$1=0.2^2+0.2+1.2^0 \rightarrow \begin{pmatrix}0\\0\\1\end{pmatrix}$ $\quad 7=\begin{pmatrix}1\\1\\1\end{pmatrix}$

$2=0.2^2+1.2+0.2^0 \rightarrow \begin{pmatrix}0\\1\\0\end{pmatrix}$

$3=\begin{pmatrix}0\\1\\1\end{pmatrix}$ $\quad 4=\begin{pmatrix}1\\0\\0\end{pmatrix}$ $\quad 5=\begin{pmatrix}1\\0\\1\end{pmatrix}$ $\quad 6=\begin{pmatrix}1\\1\\0\end{pmatrix}$

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

Si por ejemplo recibimos la palabra

$$y=(0\,1\,1\,0\,\underline{1}\,1\,1)$$

$$S(y)=y.H^T=(1\;0\;1)\rightarrow 1.2^2+0.2+1.2^1=5$$

y provino de la palabra código

$$c=(0\,1\,1\,0\,0\,1\,1)$$

Se detectó 1 error cometido en la 5ª posición.

Ejercicio: Calcular la matriz generadora del código C_m, y encontrar el mensaje original enviado. (decodificar c).

Observar que en el ejemplo anterior, como C_m tiene distancia mínima 3, es capaz de detectar hasta 2 errores pero la corrección se realiza correctamente hasta 1 cometido.

Por ejemplo: supongamos que $c = (0\,1\,1\,0\,0\,1\,1)$ es enviada y

$$z = (\underline{1}\,1\,1\,\underline{1}\,0\,1\,1) \quad \text{es recibida.}$$

En este caso $S(z) = zH^T = (1\,0\,1)$ y el código se decodifica usando

$$\tilde{c} = (1\,1\,1\,1\,\underline{1}\,1\,1)$$

Si miramos las columnas de H vemos que la quinta columna $\begin{pmatrix}1\\0\\1\end{pmatrix}$ es la suma de las columnas 1 y 4.

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

$$h_1 + h_4 \qquad h_5.$$

Códigos cíclicos

Def. Un código lineal $C \subset \mathbb{F}_q^n$ es cíclico si cada vez que

$$c = (c_0 c_1 \dots c_{n-1}) \in C$$

entonces

$$\tilde{c} = (c_{n-1} c_0 c_1 \dots c_{n-2})$$

también esté en C.

Ejemplo: 1) $\mathbb{F}_2$ $\quad C = \{(000), (111)\}$ $\quad [3,1,3]$ código binario cíclico.

2) $C = \{(000), (110), (011), (101)\}$ es un $[3,2,2]$-código binario cíclico.

Notar que por la definición un código lineal es cíclico si es cerrado por cualquier desplazamiento cíclico

$$c_0 c_1 \dots c_{n-2} c_{n-1} \longrightarrow c_{n-1} c_0 c_1 \dots c_{n-2} \longrightarrow c_{n-2} c_{n-1} c_0 c_1 \dots c_{n-3}$$
$$\in C \qquad\qquad \in C \qquad\qquad \in C$$

$$\dots \longrightarrow c_k c_{k+1} \dots c_n c_0 c_1 \dots c_{k-1}$$
$$\in C.$$

A partir de ahora vamos a suponer que n y q son coprimos ($\text{mcd}(q,n)=1$).

En particular, si $q=2$ (es decir $\mathbb{F}_2$ binarios) entonces la longitud n deberá ser impar.

Si $C \subset \mathbb{F}_q^n$ es un código lineal q-ario, entonces a cada palabra código c podemos asignarle un polinomio de la siguiente manera:

$$c = (c_0\, c_1 \dots c_{n-1}) \longrightarrow p_c(x) = c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$$

entonces podemos definir un isomorfismo de espacios vectoriales

$$\begin{aligned} \phi : C &\longrightarrow \mathbb{F}_q[x] \\ c &\longrightarrow p_c(x) \end{aligned}$$

Entonces podemos pensar a las palabras código directamente como polinomios de grado menor a n en $\mathbb{F}_q[x]$.

El cociente $R_n = \mathbb{F}_q[x] / \langle x^n - 1 \rangle$ donde $\langle x^n-1 \rangle$ es el ideal generado por el polinomio $x^n - 1$; es el álgebra de polinomios de grado menor a

R_n con la suma usual de polinomios y el producto de polinomios módulo x^n-1.

Observar que en este caso

$$x \cdot p_c(x) = x\left(c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}\right)$$

$$= c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1}x^n$$

$$\text{mod } x^n-1 \quad \equiv c_{n-1} + c_0 x + c_1 x^2 + \cdots + c_{n-2}x^{n-1}$$

Teorema: Un código C es cíclico si y sólo si $I = \phi(C)$ es un ideal en R_n.

Demostración

$\Rightarrow$) Recordemos que todo ideal de $R_n = \mathbb{F}_2[x]/\langle x^n-1\rangle$ es un ideal principal, es decir si $I \neq \{0\}$ entonces está generado por un polinomio $I = \langle p(x)\rangle$.

Si $C = \{(c_0, \ldots, c_{n-1}) : p_c(x) \in I\}$

Como I es un ideal y $x \in R_n$ entonces $x \cdot p_c(x) \in I$, pero ya vimos que $x \cdot p_c(x) = c_{n-1} + c_0 x + \cdots + c_{n-2}x^{n-1}$

Luego si $c=(c_0,\dots,c_{n-1}) \in C \Rightarrow (c_{n-1},c_0,\dots,c_{n-2}) \in C$
y por lo tanto C es cíclico.

$\Rightarrow$) Recíprocamente supongamos que C es un código cíclico y sea $c \in C$, $c=(c_0 c_1,\dots,c_{n-1})$

Entonces $p_c(x) \in \phi(C) \subset R_n$.

Como $c \in C$ y C es cíclico entonces $(c_{n-1} c_0 \dots c_{n-2}) \in C$
$\Rightarrow$ $x \cdot p_c(x) \in \phi(C)$
De manera análoga obtenemos que $(c_{n-2} c_{n-1} c_0,\dots c_{n-3}) \in C$
y por lo tanto
$$x^2 p_c(x) = x(x p_c(x)) \in \phi(C)$$
$$\vdots$$
En general $x^j p_c(x) \in \phi(C)$

Luego $b(x) \cdot p_c(x) \in \phi(C)$ para cualquier $b(x) \in R_n$
y por lo tanto $\phi(C)$ es un ideal.

Observar que como en $R_n = \mathbb{F}_2[x]/\langle x^n-1\rangle$ todos los ideales son principales, entonces todo ideal no nulo C está generado por

un polinomio mónico de menor grado en el ideal, digamos $g(x)$ donde $g(x)$ divide a $x^n - 1$.