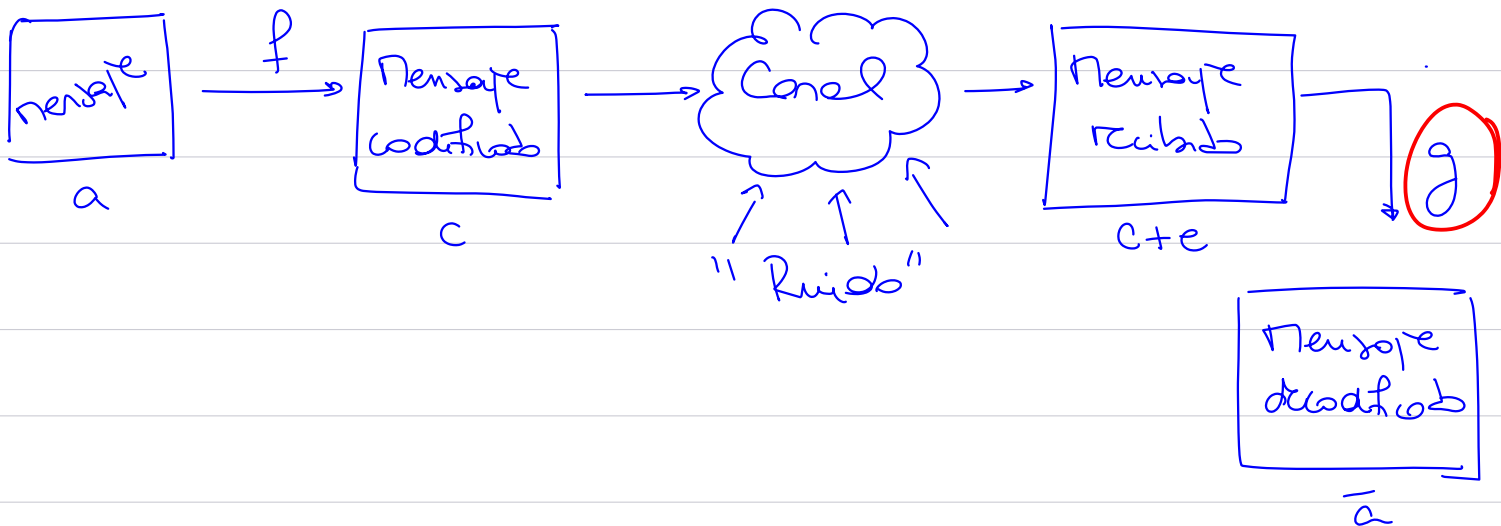


Aplicaciones 1: Teoría de códigos

Un modelo sencillo de un sistema de comunicación



Vamos a suponer que los símbolos del mensaje original y del mensaje codificado son elementos de un mismo cuerpo finito $\mathbb{F}_q$. Codificar significa transformar un bloque de k símbolos del mensaje original $(a_1, a_2, \dots, a_k) \in \mathbb{F}_q^k$ en una palabra código $(c_1, \dots, c_n) \in \mathbb{F}_q^n$ de n símbolos donde $n > k$.

En el gráfico anterior

$$\left. \begin{array}{l} f: \mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n \\ a \longmapsto c = f(a) \end{array} \right\} \begin{array}{l} \text{Esquema} \\ \text{de} \\ \text{codificación} \end{array}$$

Un esquema de codificación sencillo se obtiene cuando un bloque $(a_1, \dots, a_k)$ que corresponde a un mensaje original se codifica en una palabra código de la forma

$$(a_1, a_2, \dots, a_k, c_{n+1}, c_{n+2}, \dots, c_n)$$

donde los primeros k símbolos corresponden al mensaje original y los restantes $n-k$ símbolos son símbolos de control.

Ejemplo: $\mathbb{F}_2 = \{0, 1\}$

$$k=1$$

$$\mathbb{F}_2 \rightarrow \mathbb{F}_2^2$$

$$0 \rightarrow (0, 0)$$

$$\rightsquigarrow (0, 1)$$

$$1 \rightarrow (1, 1)$$

$$\mathbb{F}_2 \rightarrow \mathbb{F}_2^3$$

$$0 \rightarrow (0, 0, 0)$$

$$1 \rightarrow (1, 1, 1)$$

$$\rightsquigarrow (0, 1, 0) \rightsquigarrow (0, 0, 0) \rightsquigarrow 0.$$

Para este tipo de esquemas en donde tenemos k símbolos de información y $n-k$ símbolos de control podemos pensar en lo siguiente:

Sea H una matriz de $(n-k) \times n$ con coeficientes en $\mathbb{F}_q$ de la forma $H = (A | I_{n-k})$ donde

A es una matriz cuadrada de $(n-k) \times (n-k)$ y I_{n-k} es la identidad de tamaño $(n-k)$.

Los símbolos de control $c_{k+1}, \dots, c_n$ ^{para un polinomio $C = (c_1, \dots, c_k, c_{k+1}, \dots, c_n)$} pueden calcularse entonces del sistema

$$H C^T = 0 = C \cdot H^T$$

$$H_{(n-k) \times n} C_{n \times 1}^T = 0$$

Las ecuaciones en este sistema se llaman ecuaciones de chequeo de paridad o de control y la matriz H se llama matriz de control o matriz de chequeo de paridad.

Ejemplo: H de 3×7 sobre $\mathbb{F}_2$. $n=7$ $k=4$

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & : & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & : & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & : & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ c_5 \\ c_6 \\ c_7 \end{pmatrix} \xrightarrow{f: \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^7} (a_1, a_2, a_3, a_4) \rightarrow$$

$$H C^T = 0$$

$$\left. \begin{aligned} a_1 + a_3 + a_4 + c_5 &= 0 \\ a_1 + a_2 + a_4 + c_6 &= 0 \\ a_1 + a_2 + a_3 + c_7 &= 0 \end{aligned} \right\} \rightarrow$$

$$(a_1, a_2, a_3, a_4, c_5, c_6, c_7)$$

$$\mathbb{F}_2^4 \rightarrow \mathbb{F}_2^7$$

$$(a_1, a_2, a_3, a_4) \rightarrow (a_1, a_2, a_3, a_4, a_1 + a_3 + a_4, a_1 + a_2 + a_4, a_1 + a_2 + a_3)$$

Ejemplo: (Codigo de chequeo de paridad)

$$\begin{aligned}\mathbb{F}_2^k &\longrightarrow \mathbb{F}_2^{k+1} \\ (a_1, \dots, a_k) &\longrightarrow (a_1, \dots, a_k, a_1 + a_2 + \dots + a_k)\end{aligned}$$

En este caso si la suma de todas las coordenadas de la palabra recibida no da cero, se detecta que se ha cometido un error en la transmisi3n.

Def: Un c3digo (bloque) lineal q-ario de longitud n y dimensi3n k es un subespacio vectorial C de $\mathbb{F}_q^n$ de dimensi3n k . Los elementos de C se llaman palabras c3digo.

Si $B = \{v_1, \dots, v_k\}$ es una base de C sobre $\mathbb{F}_q^n$ definimos la matriz generadora G del c3digo C como la matriz cuyas filas son los vectores v_i de la base

$$C \subseteq \mathbb{F}_q^n$$

$$\begin{aligned}C: \mathbb{F}_q^k &\longrightarrow \mathbb{F}_q^n \\ \vec{a} = (a_1, \dots, a_k) &\longrightarrow \vec{c} = \vec{a} \cdot G\end{aligned}$$

$$G_{k \times n}$$

$$\text{donde } G_{k \times n} = \begin{pmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_k \end{pmatrix} = \begin{pmatrix} v_{11} & v_{12} & \dots & v_{1n} \\ v_{21} & v_{22} & \dots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{k1} & v_{k2} & \dots & v_{kn} \end{pmatrix}$$

Si $G_{k \times n}$ es una matriz generadora y $H_{(n-k) \times n}$ que satisface

$$HG^T = \vec{0}$$

entonces decimos que H es una matriz de control o de chequeo de paridad para C .

Decimos que una matriz G generadora para C esté en forma estándar si

$$G = (I_k | B)$$

donde I_k es la identidad de tamaño k y B es una matriz de $k \times (n-k)$

En este caso, $H = (-B^T | I_{n-k})$ satisface $H \cdot G^T = 0$ y decimos que H está en forma estándar como matriz de control.

Si G está en forma estándar en el esquema de codificación

$$\mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$$

$$a \rightarrow \vec{c} = a \cdot G.$$

Modificación es trivial ya que corresponde a reasignar la palabra código a los primeros k símbolos.

Ejemplo (Código de repetición) En un código de repetición cada palabra código está formada por un símbolo de información (o mensaje original) a_1 y $n-1$ símbolos de control $c_2 = \dots = c_n = a_1$

La long. de este código es n , la dimensión es 1, y la matriz generadora es

$$G = (1 | \overbrace{1 \dots 1}^{B_{1 \times (n-1)}})_{1 \times n}$$

$$\mathbb{F}_q^1 \rightarrow \mathbb{F}_q^n$$

$$a \mapsto a \cdot G$$

y la matriz de chequeo de paridad.

$$H = \left(\begin{array}{cccc} -1 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \dots & 1 \end{array} \right)_{(n-1) \times (n)} = (-B^T | I_{n-1})$$

Def: Si c es una palabra código y recibimos una palabra y luego de la transmisión por un canal "ruidoso" entonces

$$e = y - c$$

se llama vector error.

Def: Sean $x, y \in \mathbb{F}_2^n$ entonces

(1) La distancia de Hamming $d(x, y)$ entre x e y se define como la cantidad de coordenados distintas en las que x e y difieren, es decir

$$d(x, y) = \# \{ i : x_i \neq y_i \quad 1 \leq i \leq n \}$$

(2) El peso (de Hamming) $w(x)$ de x es la cantidad de coordenados no nulos de x ,

$$w(x) = \# \{ i : x_i \neq 0 \quad 1 \leq i \leq n \}.$$

Con esta definición si x es transmitida y se recibe y entonces $d(x, y)$ cuenta la cantidad de errores cometidos en la comunicación.

Por supuesto, $w(x) = d(x, 0)$ ya que

$$d(x, y) = w(x - y).$$

Proposición: La distancia de Hamming es una métrica en $\mathbb{F}_2^n$, es decir

1) $d(x, y) \geq 0$ y $d(x, y) = 0$ si y sólo si $x = y$

2) $d(x, y) = d(y, x)$

3) $d(x, z) \leq d(x, y) + d(y, z) \quad x, y, z \in \mathbb{F}_2^n.$

Permutación: EJERCICIO.

Def. El número

$$\begin{aligned} d &= \min \{ d(u,v) : u,v \in C, u \neq v \} \\ &= \min \{ w(x) : x \in C, x \neq 0 \} \end{aligned}$$

se llama distancia mínima del código.

Notación: Un código C con longitud n y dimensión k va a ser denotado como $[n,k]$ -código, y si se quiere hacer mención a la distancia mínima vamos a decir que es un $[n,k,d]$ -código.

Supongamos que un vector y es recibido al ser enviada una palabra código x de $\mathbb{F}_q^n$ usando un $[n,k,d]$ -código C . Si y no es una palabra código, es razonable decodificar usando la palabra código $z \in C$ tal que $d(y,z)$ sea lo más pequeño posible. Esto se denomina "decodificación por el vecino más cercano" y funcionará mejor cuando estemos suponiendo que

- 1) Cada símbolo transmitido tiene la misma probabilidad $p < 1/2$ de ser recibido con error

2) Si un símbolo es recibido con error, cada uno de los $q-1$ símbolos restantes tienen la misma probabilidad de aparecer.

Teorema: Un $[n, k, d]$ -código C puede

1) detectar hasta $d-1$ errores

2) corregir hasta $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores, donde $L(x)$ denota el peso x

Demostración

1) Supongamos x se envía ($x \in C$) y se recibe el vector y con a lo sumo $d-1$ errores.

$$d(x, y) \leq d-1 < d.$$

Pero entonces $y \notin C$, pues ningún par de palabras código puede tener distancia menor a la distancia mínima d .

2) Supongamos x se envía ($x \in C$) y se recibe el vector y que difiere de x en a lo sumo $\left\lfloor \frac{d-1}{2} \right\rfloor$ coordenadas.

$$d(x, y) \leq \left\lfloor \frac{d-1}{2} \right\rfloor$$

Sea $z \in C$. Como

$$d(x, y) \leq \frac{d-1}{2}$$

$$d(x, z) \leq d(x, y) + d(y, z)$$

$$\Rightarrow d(y, z) \geq \underbrace{d(x, z)}_{\geq d} - \underbrace{d(x, y)}_{\geq \frac{d-1}{2}} \geq d - \frac{d-1}{2}$$

$$= \frac{2d - d + 1}{2} = \frac{d+1}{2} > \frac{d-1}{2} \geq d(x, y)$$

Luego x es la más cercana a y , y por lo tanto se corrigen los errores.

$$0, 1 \rightarrow \begin{pmatrix} 0, 0 \\ 1, 1 \end{pmatrix}$$

$$C = \{ (0, 0), (1, 1) \}$$

$$C_2 = \{ (0, 0, 0), (1, 1, 1) \}$$

$$n=2 \quad G=(1, 1)$$

$$k=1$$

$$d=2$$

$$n=3 \quad k=1 \quad d=3$$

$$d-1=1 \rightarrow \text{detecta 1 error}$$

$$d-1=2 \rightarrow \text{detecta hasta 2 errores}$$

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0.$$

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor 1 \right\rfloor = 1 \rightarrow \text{corregir hasta 1 error.}$$

$$(0, 1, 0) \rightarrow (0, 0, 0) \rightarrow 0$$