Teoría de Códigos y Criptografía

Justo Peralta López
Juan Antonio López Ramos

Universidad de Almería
Departamento de Álgebra y Análisis Matemático

Definición

Un código C se dice que es lineal si y solo si la suma de palabras de C pertenece a C.

Definición

Sea $V_n = \{(a_0, a_1, \ldots, a_n) | a_i \in GF(q)\}$ un espacio vectorial. Un subconjunto C de V_n es un código lineal si y solo si es un subespacio de V_n.

Teorema

Sea C un código lineal y $W(C)$ el menor de los pesos de las palabras de C distintas de cero. Entonces

$$d_{min}(C) = W(C)$$

Ventajas

- Si M es el número de palabras del código, ahora, para calcular su mínima distancia sólo hay que hacer $M - 1$ comparaciones. Antes hacia falta $\binom{M}{2}$ comparaciones, es decir, todos con todas de dos en dos.
- Para describir un código no lineal, teníamos que indicar todas sus palabras del código. Ahora al ser un subespacio vectorial solo tenemos que indicar su base.
- Los algoritmos de codificación y decodificación son muy sencillos.

Desventajas

Todo código lineal tiene que ser un q-código, donde q es de la forma p^n con p primo. Esto es debido a que todo código lineal deber ser un K-espacio vectorial, donde K es un cuerpo, y todo cuerpo tiene un tamaño de p^n elementos.

Definición

Una matriz $k \times n$ cuyas filas es la base de un (n, k)-código es llamada *matriz generadora del código*.

Ejemplo

a) $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ genera el código $C = \{000, 011, 101, 110\}$ con parámetros $(3, 2, 2)$

b) $\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$ genera un $(7, 4, 3)$-código lineal.

c) Un q-código de repetición sobre $GF(q)$ es un $(n, 1, n)$-código lineal con matriz generadora $[11 \ldots 1]$.

Definición

Dos códigos son equivalentes si se pueden obtener uno a partir de otro por medio de permutaciones de la posiciones de las palabras del código y multiplicaciones por un escalar no nulo.

Teorema

Sea G la matriz generadora de un $[n, k]$-código lineal. Entonces, realizando operaciones sobre sus filas y columnas, se puede transformar en una matriz estándar

$$G' = [I_k|A]$$

donde I_k es la matriz identidad y A una matriz de dimensión $k \times (n-k)$. Las operaciones que podemos realizar son:

- f1) *Permutación de filas.*
- f2) *Multiplicación de una fila por un escalar distinto de cero.*
- f3) *Adición de un múltiplo de una fila a otra.*
- c1) *Permutación de columnas.*
- c2) *Multiplicación de una columna por un escalar distinto de cero.*

Si las operaciones que realizamos para llegar a G' solo afectan a las filas (operaciones f1,f2 y f3), obtenemos el mismo código. Y en el caso de que afecten a columnas (operaciones c1 y c2), entonces obtenemos el generador de un código equivalente

Algoritmo

Sea $G = [g_{ij}]$ una matriz de dimensión $(k \times n)$, donde i indica la fila y j la columna. Obsérvese, que el número de filas siempre será mayor o igual que el número de columnas, ya que en caso contrario, la matriz G, no será una base. Este algoritmo, para un $1 \leq j \leq k$, realiza las operaciones necesarias para que $g_{jj} = 1$ y la columna C_j tenga ceros por encima y por debajo de g_{jj}

Paso 1
- Si $g_{jj} \neq 0$ ir al Paso 2.
- Si $g_{jj} = 0$ y si existe un $i \geq j$ tal que $g_{ij} \neq 0$ intercambiar la fila i por la fila j (lo notaremos por $f_i \leftrightarrow f_j$).
- Si $g_{jj} = 0$ y $g_{ij} = 0$ para todo $i \geq j$, entonces escoger un $h > j$ tal que $g_{jh} \neq 0$ e intercambiar c_j por c_h $(c_j \leftrightarrow c_h)$.

Paso 2 Sustituir la fila f_j por $f_j.g_{jj}^{-1}$

Paso 3 Ahora, $g_{jj} = 1$. Para cada $i = 1, 2, \ldots, k$, con $i \neq j$, reemplazar f_i por $f_i - g_{ij} f_j$

Ejemplo

Apliquemos el algoritmo a la siguiente matriz generadora y discutamos sobre los parámetros del código que ésta genera.

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \text{ y } \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 2 \\ 1 & 0 & 2 & 0 & 1 & 1 \end{bmatrix}$$

Codificación

Sea C un $[n,k]$-código lineal sobre $GF(q)$, con matriz generadora G. C contiene q^k palabras y por lo tanto se puede utilizar para transmitir q^k mensajes distintos. Identificamos cada mensaje por una k-tupla del espacio vectorial $V(k,q)$. Si denotamos a las filas de G por $r_1, ..., r_k$, codificamos cada mensaje $u = u_1 u_2 ... u_k$ por

$$uG = \sum_{i=1}^{k} u_i r_i$$

Es decir, a cada mensaje le hacemos corresponder una combinación lineal de los elementos de la base del subespacio vectorial C.

Ejemplo

$G_1 = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \end{bmatrix}$ y $G_2 = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 2 \end{bmatrix}$ son dos matrices que generan el mismo código.

Supongamos que G es de la forma

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & P_{0,0} & P_{0,1} & \dots & P_{0,n-k-1} \\ 0 & 1 & 0 & \dots & 0 & P_{1,0} & P_{1,1} & \dots & P_{1,n-k-1} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 00 & \dots & 1 & P_{k-1,0} & P_{k-1,1} & \dots & P_{k-1,n-k-1} \end{bmatrix}$$

Sea $d = (d_0, d_1, \dots, d_{k-1})$ el mensaje o dato a codificar. Entonces codificamos por $c = uG$ donde $G = [I_k P]$. Luego la palabra codificada será

$$u = d_0, d_1, \dots, d_{k-1}, P_k, P_{k+1}, \dots, P_{n-1}$$

donde

$$\begin{aligned} P_k &= d_0 P_{0,0} + d_1 P_{1,0} + \cdots + d_{k-1} P_{k-1,0} \\ P_{k+1} &= d_0 P_{0,1} + d_1 P_{1,1} + \cdots + d_{k-1} P_{k-1,1} \\ &\vdots \\ P_k &= d_0 P_{0,n-k-1} + d_1 P_{1,n-k-1} + \cdots + d_{k-1} P_{k-1,n-k-1} \end{aligned}$$

Ejemplo

Sea $G_1 = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 2 & 2 \end{bmatrix}$ y $G_2 = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 2 \end{bmatrix}$ los dos matrices generadores del mismo código. La siguiente tabla nos muestra como se realiza la decodificación en ambos casos.

d_0	d_1	u_0	u_1	u_2	u_3	u_0	u_1	u_2	u_3
0	0	0	0	0	0	0	0	0	0
1	0	1	0	2	1	1	0	2	1
2	0	2	0	1	2	2	0	1	2
0	1	0	1	2	2	1	2	0	2
0	2	0	2	1	1	2	1	0	1
1	1	1	1	1	0	0	2	1	1
2	1	2	1	0	1	0	2	1	1
1	2	1	2	0	2	0	1	2	2
2	2	2	2	2	0	1	1	1	0

El circuito que realzaría la codificación del código sistemático sería

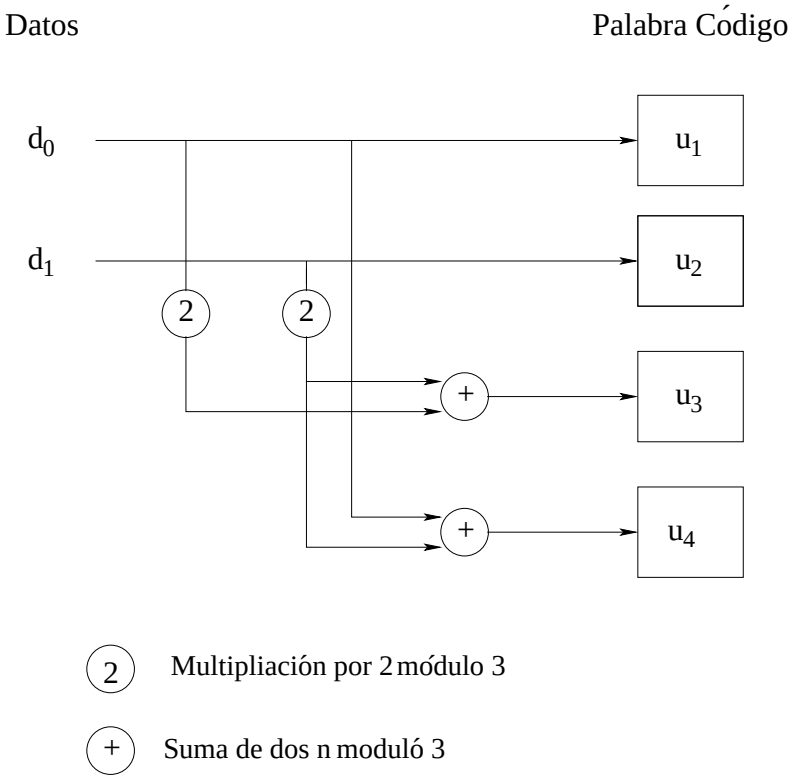

Figura: Circuito de un $(4, 2)$-código sistemático sobre $GF(3)$

El circuito para un código sistemático cualquiera viene dado por

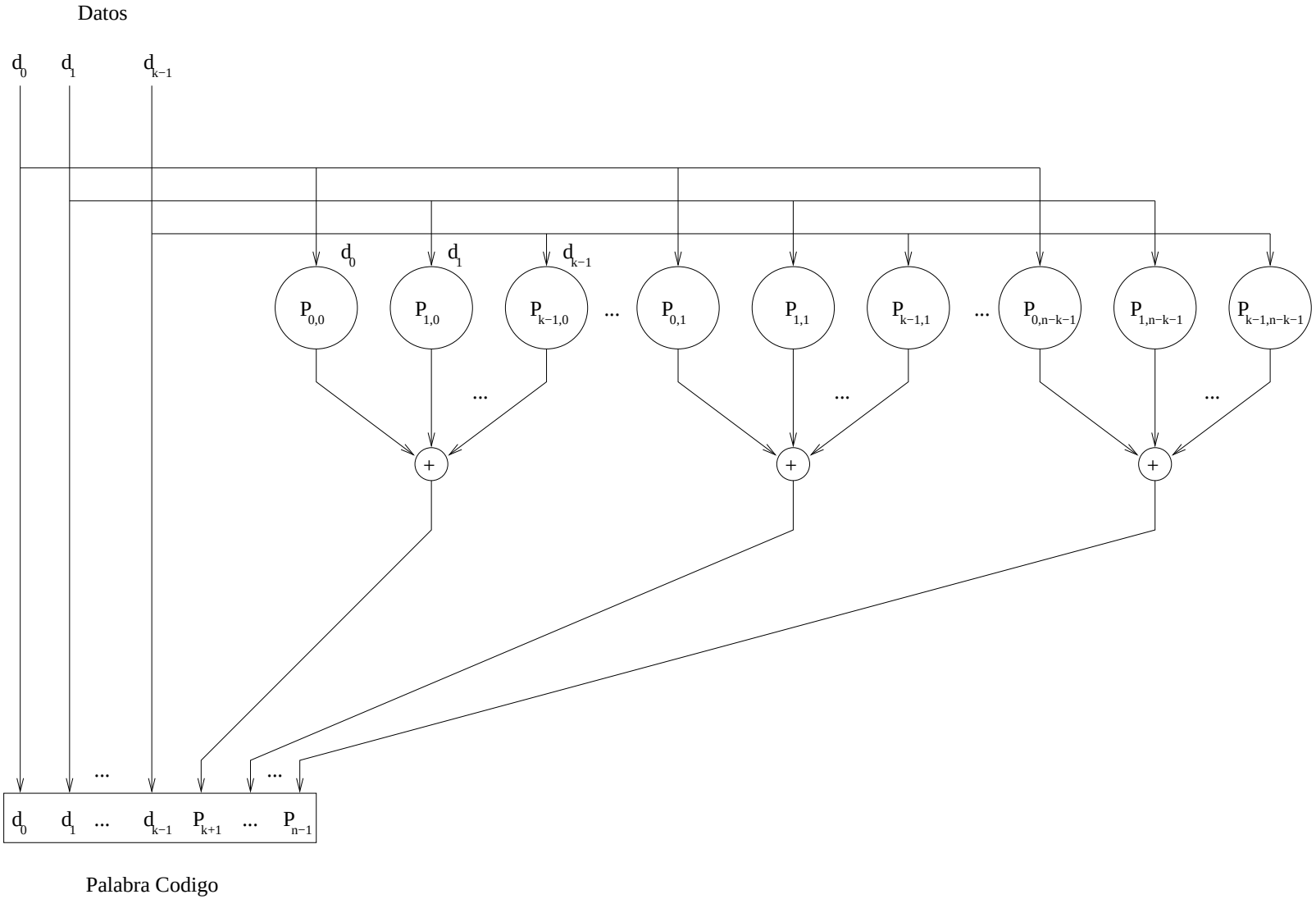

Figura: Circuito de un (n, k)-código sistemático sobre $GF(q)$

Sea C un $[n,k]$-código lineal , $x = (x_1, x_2, ..., x_n) \in C$ la palabra código enviada, $y = (y_1, y_2, ..., y_n)$ la palabra código recibida y $e = x - y = (e_1, e_2, ..., e_n)$ el error cometido durante la transmisión. C tiene estructura de subespacio vectorial de $V(n,q)$, por lo tanto tiene estructura de grupo respecto a la suma de la misma forma que ocurre con $V(n,q)$. Ya que C es un subgrupo de $V(n,q)$, podemos definir la siguiente relación de equivalencia: $x \sim y$ si y solo si $x - y \in C$. Definimos el conjunto cociente V/C y tomamos como representante de cada clase el vector de esa clase de mínimo peso y lo llamamos líder de la clase.

Definición

Llamamos array estándar de decodificación al array cuyas filas son las clases de V/C.

El siguiente algoritmo de decodificación fue introducido por Slepian(1960)

Definición

Supongamos que C es un $[n,k]$-código lineal sobre $GF(q)$ (cuerpo de Galois de q elementos) y que x es cualquier vector o palabra en $V(n,q)$. Entonces los conjuntos de la forma $x + C = \{x + y | y \in C\}$ son las clases o coclases de C.

Teorema

Sea C un $[n, k]$-código sobre $GF(q)$. Entonces

1. *Todo vector de $V(n, q)$ está en alguna clase de C.*
2. *Toda clase tiene exactamente q^k vectores.*
3. *Dos clases o son disjuntos o coinciden.*

Ejemplo

Sea $C = \{0000, 1011, 0101, 1110\}$, entonces sus clases vienen dadas por la tabla 1

$$\begin{array}{lcllll} 0000 + C & = & 0000 & 1011 & 0101 & 1110 \\ 0001 + C & = & 0001 & 1010 & 0100 & 1111 \\ 0010 + C & = & 0010 & 1001 & 0111 & 1100 \\ 1000 + C & = & 1000 & 0011 & 1101 & 0110 \end{array}$$

Cuadro: Array de decodificación de C

Algoritmo

1. Buscamos la palabra recibida y, e identificamos la clases a la que pertenece.
2. Tomamos como error cometido e=líder de la clase.
3. Decodificamos por x=y-e

Realmente estamos decodificando la palabra recibida y, por la palabra del código C que más se le parece, es decir, por aquella de C cuya distancia mínima con y es menor. Ya que la probabilidad de error es $p << 1/2$ la palabra de C más parecida con y, será la que tenga mayor probabilidad de haber sido enviada. Este es el motivo por el cual como representante de cada clase se tome el de menor peso, ya que éste indicará el error cometido si la palabra y pertenece a esa clase; y los errores más probables son los de menor peso.

Definición

Dado un código lineal C, llamamos código dual de C, y lo notamos por $C^{\perp}$, al conjunto de los vectores del espacio vectorial $V(n,q)$ que son ortogonales a toda palabra de C, y notamos por $u.v$ al producto escalar de dos vectores.

$$C^{\perp} = \{v \in V(n,q) | v.u = 0 \ \forall u \in C\}$$

$C^{\perp}$ es un subespacio vectorial de $V(n,q)$ de dimensión $n-k$, luego será un $[n, n-k]$-código.

Ejemplo

- $C = \{0000, 1100, 0011, 1111\}$, $C^{\perp} = C$
- $C = \{000, 110, 011, 101\}$, $C^{\perp} = \{000, 111\}$

La matriz de paridad H para un $[n, k]$-código C es el generador de $C^{\perp}$, lo cual nos permite definir un código de la siguiente forma

$$C = \{x \in V(n, q) | xH^t = 0\}$$

Ejemplo

Si $H = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ entonces

$$C = \{(x_1, x_2, x_3, x_4) \in V(4, 2) | x_1 + x_2 = 0, x_3 + x_4 = 0\}$$

Lema

Sea C un $[n, k]$-código lineal con matriz generadora G. Entonces un vector $u \in V(n, q)$ pertenece a $C^{\perp}$ si y sólo si es ortogonal a todas las filas de G. Es decir,

$$u \in C^{\perp} \leftrightarrow vG^t = 0$$

Teorema

Para todo $[n, k]$-código lineal C, $(C^{\perp})^{\perp} = C$.

Teorema

Sea C un $[n,k]$-código lineal sobre $GF(q)$. Entonces el dual de C es un $[n, n-k]$-código lineal. Además, si H es la matriz generadora de $C^{\perp}$, a la cual llamaremos matriz de paridad, entonces $GH^t = 0$

Teorema

Si $G = [I_k|A]$ es la matriz generadora de un $[n,k]$-código, entonces la matriz de paridad de C es $H = [-A^t|I_{n-k}]$

Ejemplo

Sea $G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right]$
la matriz generadora de C. Su matriz de paridad o matriz generadora de su dual será

$$H = \left[\begin{array}{cccc|ccc} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{array}\right]$$

Definición

Sea H una matriz de paridad de un $[n, k]$-código C. Entonces para cualquier vector $y \in V(n, q)$, se define el síndrome de y como sigue

$$S(y) = yH^t$$

- Si las filas de H son $h_1, h_2, \ldots, h_{n-k}$, entonces

$$S(y) = (y_1 h_1, y_2 h_2, \ldots, y_n h_n)$$

- $S(y) = 0 \Leftrightarrow y \in C$

Lema

Dos vectores u y v de $V(n, q)$ están en la misma clase de C si y solo si tienen el mismo síndrome.

Decodificación

Enviamos x y recibimos y.

1. Calculamos $S(y) = yH^t$
2. Si $S(y) = 0$ no se ha producido ningún error.
3. Si $S(y) \neq 0$ se ha producido algún error. Buscamos un líder con el mismo síndrome y decodificamos por y-líder.

Ejemplo

Sea C un código lineal generado por $G = \begin{bmatrix} 1011 \\ 0101 \end{bmatrix}$.

Líder	Síndrome
0000	00
1000	11
0100	01
0010	10

Entonces la palabra $y = 1001$ tiene síndrome 10 y decodificamos por 1011.

Ejemplo

Sea C un $[6, 2, 3]$ código lineal generado por $G = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix}$

El array de decodificación vendrá dado por

Líder			
00000	10110	01011	11101
10000	00110	11011	01101
01000	11110	00011	10101
00100	10010	01111	11001
00010	10100	01001	11111
00001	10111	01010	11100
11000	01110	10011	00101
10001	00111	11010	01100

Si recibimos 10011 podemos decir que se han producido 2 errores, pero sabemos como corregirlo, ya que la palabra enviada podría ser 01011 o 10110.

Teorema

Para cualquier palabra $u \in C$ de pesos d, d columnas de H son linealmente dependientes.

Teorema

Un código lineal C tiene distancia mínima como mínimo d si y sólo si cualquier $d-1$ o menos columnas de H son linealmente independientes.