Grupos, anillos y cuerpos

Universidad de Málaga
Dpto. de Matemática Aplicada

30 de marzo de 2017

Introducción a la Teoría de la Codificación

- Nos planteamos la transmisión segura de un mensaje sobre un canal de comunicación que puede estar afectado por *ruido*.
- Para ello, la teoría de codificación ha desarrollado técnicas para introducir en el mensaje que se transmite información *redundante* que ayude a detectar (e incluso a corregir) los errores.
- Algunas de éstas técnicas utilizan la teoría de grupos.

$$\begin{array}{ccccccccc} \text{EMISOR} & & \rightarrow & & \text{CODIFICADOR} & \overset{\text{Ruido=r}}{\Rightarrow} & \text{DECODIFICADOR} & \rightarrow & \text{RECEPTOR} \\ v & & \rightarrow & & u & & y = u + r & & v \end{array}$$

El emisor codifica su mensaje v como u, y lo hace añadiendo a v información redundante, para que, si se introduce el ruido r y el receptor recibe un mensaje alterado $y = u + r$, sea capaz de recuperar el mensaje original v.

Situándonos. Necesidad de introducir Redundancia

Supongamos que tenemos solo dos mensajes posibles, SI y NO, que podríamos codificar y enviar como

$$SI = 1, \qquad NO = 0$$

El ruido puede provocar $1 \Rightarrow 0$, de manera que el receptor entienda NO cuando queríamos decir SI.

Para evitarlo codificamos los mensajes doblándolos; **Códigos**: SI=11, NO=00. Así,

- si se produce un error, por ejemplo si enviamos 11 y se recibe 01, el receptor **detecta el error** porque 01 no forma parte de nuestro código.
- **no se puede corregir el error** porque al recibir 01 es igual de probable que el mensaje original sea 11 o que sea 00.

Sí podemos corregir un error si el código triplica el mensaje: **CÓDIGOS**: SI=111, NO=000; porque si, por ejemplo, recibimos 101, es más probable que el mensaje original sea 111 (con un error) que que fuese 000 (con dos errores) .

Situándonos

Supongamos que tenemos un vehículo de exploración en Marte, que llamaremos Marθ. Lo manejamos a control remoto desde la Tierra por medio de un canal que transmite impulsos eléctricos de dos voltajes distintos: 0 y 1.

El vehículo se mueve un metro en cada movimiento, en una de las cuatro direcciones posibles: norte (N), sur (S), este (E) y oeste (O). Luego, nuestros mensajes son N, S, E y O y los codificamos, por ejemplo, como 00, 11, 01 y 10. Es decir,

$$\textbf{Códigos}: \quad N \to 00; \quad O \to 10; \quad S \to 11; \quad E \to 01$$

Supongamos que el vehículo se encuentra orientado hacia el norte, al borde de un enorme cráter, con el precipicio a su derecha (o sea, hacia el este).

Enviamos el mensaje 00, es decir "avance un metro hacia el norte". Pero si una interferencia en la transmisión hace que Marθ reciba 01, "avance un metro a su derecha". Si no detectamos el error, Marθ caerá en el cráter. Un error aquí es fatal.

Situándonos

El problema está en nuestro código

$$C_1 = \{00, 01, 10, 11\} = \mathbb{Z}_2^2$$

que no detecta errores: Si hay un error en la transmisión, la palabra recibida es otra palabra código. Así, si cometemos un error al enviar 00 recibimos 01 o 10, y como ambas son palabras de C_1, no detectamos ningún error. Igual ocurre con 01, 10 y 11.

Esto se debe a que C_1 consta de todas las palabras de longitud 2 que se pueden formar con ceros y unos.

¿Cómo podemos arreglar esto? La forma más fácil es agregar redundancia mediante un dígito de control de paridad, o sea, agregamos un dígito extra a cada palabra código de modo que la suma de los dígitos de cada palabra código sea par. En nuestro caso, el nuevo código es

$$C_2 = \{000, 011, 101, 110\} \subset \mathbb{Z}_2^3$$

Situándonos

Si ahora transmitimos 000 y se comete un error en la transmisión, entonces recibimos 100, 010 o 001. Como ninguna de estas palabras pertenece al código, detectamos un error. Nuestro vehículo no se mueve.
Lo mismo sucede con las otras palabras del código, es decir, si se comete un único error al enviar cualquier palabra código, la palabra recibida no pertenece al código. Decimos entonces que el código C_2 detecta un error o que es 1-corrector. Ahora bien C_2 no detecta 2 errores. Es decir, si se cometen 2 errores, la palabra recibida estaría en el código cualquiera sea la palabra código enviada.
En nuestro ejemplo, supongamos que enviamos 000 y recibimos 010. Aunque Marθ detecta el error, si quisiera tomar una decisión por sí mismo, no podría.

En efecto, suponiendo un error, la palabra 010 puede ser decodificada como 110, como 000 o como 011, todas palabras códigos. Luego, Marθ no se mueve y solicita la **retransmisión** del mensaje.

De nuevo podemos mejorar nuestra situación. Una solución fácil es agregar mayor redundancia. Formamos el código

$$C_3 = \{000000, 000111, 111000, 111111\}$$

repitiendo tres veces cada dígito del código original C_1. Ahora, si mandamos nuestro mensaje 000000 y se comete un error, cualquier palabra que nos llegue puede ser corregida.

Por ejemplo, 00 se codifica a 000000 y, si cometemos un error, recibimos uno de los mensajes

$$100000,\ 010000,\ 001000,\ 000100,\ 000100,\ 000010,\ 000001$$

sabemos que cualquiera de ellos es erróneo y lo corregimos a 000000 y lo decodificamos a 00. Así que no sólo detectamos el error sino que podemos corregirlo. Intuitivamente, 000100 está "más cerca" de 000000 que de 000111, 111000 o 111111. Luego, corregimos 000100 como 000000 y no como 000111 ya que es más probable cometer un error que cometer tres. Luego, hemos mejorado las propiedades detectoras y correctoras del código original C_1 y de C_2.

Definiciones Básicas

Definición

- *Se llama* **palabra** *a una cadena de símbolos de un alfabeto.*
- *Un* **código** *es una colección de palabras usadas para representar mensajes. Una palabra de un código se llama también* **palabra clave**.
- *Un* **código de bloque** *está formado por palabras con la misma longitud. En estos nos centraremos.*

1. Trabajaremos en binario, con el alfabeto $\{0, 1\}$.
2. Las palabras de longitud m se pueden considerar como elementos del grupo $(\mathbb{Z}_2^m, +)$ (m-tuplas de 0's y 1's), escritos sin paréntesis ni corchetes.

Definiciones

- Se llama **peso** de una palabra $x \in \mathbb{Z}_2^m$, y se denota $ps(x)$, al número de unos de x. Así, $ps(10010) = 2$

Recordando

Si en el conjunto $\mathbb{Z}_2 = \{0, 1\}$ de las clases de los restos módulo 2, defines las operaciones de suma y producto de clases, se tiene que.

- $(\mathbb{Z}_2, +)$ es un grupo abeliano
- $(\mathbb{Z}_2, \cdot)$ es un grupo abeliano
- ¿Cuál es el opuesto de 1 respecto de la suma?: Es 1 , es decir, -1=1. Y el opuesto de 0 es 0. Por tanto, en $\mathbb{Z}_2$, la RESTA se define igual que la suma:

$$0 - 1 = 0 + 1 = 1 - 0 = 1 + 0 = 1; \qquad 1 - 1 = 1 + 1 = 0; \qquad 0 - 0 = 0$$

Recordando

En el conjunto $\mathbb{Z}_2^n$

$$(1,1,0,1)+(0,1,0,0)=(1,0,0,1)=(1,1,0,1)-(0,1,0,0)$$

- $(\mathbb{Z}_2^n,+)$ es un grupo abeliano
- el opuesto de x es el propio x

Función de Codificación: Introduciendo redundancia

Definiciones

- Si nuestro mensaje original está compuesto por palabras de longitud m, entonces se elige un entero $n > m$ y una función **INYECTIVA** $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ que se llama **función de codificación** (m, n).
- Cada palabra de $\mathbb{Z}_2^m$ se representa mediante una palabra (codificada) de $\mathbb{Z}_2^n$.
- De esta forma, si $x \in \mathbb{Z}_2^m$, entonces $\mathcal{C}(x)$ es la **palabra codificada** que representa a x. Los ceros y unos adicionales que aporta $\mathcal{C}$ serán el medio para detectar o corregir los errores producidos por el ruido en el canal de transmisión.

Una función de codificación (m, n) asigna a cada una de las posibles m-tuplas de entrada una n-tupla de las 2^n disponibles.

Codificación de la información y detección de errores

Definiciones (Detección de Errores)

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ una función de codificación (m, n). Se dice que $\mathcal{C}$ detecta a lo sumo k errores, si nos permite rechazar todas las palabras $\mathcal{C}(x)$ con k o menos errores.

Distancia de Hamming entre palabras

Definiciones

- Dadas dos palabras de la misma longitud, u y v, se define $\delta(u, v)$, la **distancia de Hamming** entre u y v, como el número de posiciones (bits) en que difieren. Este número coincide con el peso de su diferencia (= peso de su suma), esto es, $\delta(u, v) = ps(u + v) = ps(u - v)$.

- Si w es una palabra clave transmitida y se recibe como v, el número de errores ocurridos en la transmisión es la distancia entre w y v.

Definición

La **mínima distancia** *de una función de codificación* $\mathcal{C} : \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *es*

$$\delta_{min}^{\mathcal{C}} = \text{mín}\{\delta(\mathcal{C}(x), \mathcal{C}(y)) \mid x, y \in \mathbb{Z}_2^m, \quad x \neq y\}$$

es decir la mínima de todas las distancias entre todas las distintas parejas de palabras codificadas

Distancia de Hamming

Ejemplos

1. $\delta(1001, 0111) = ps(1001 + 0111) = ps(1110) = 3$
2. $\delta(01001, 11101) = ps(101001 + 11101) = ps(01100) = 2$
3. $\delta(11010, 10101) = ps(11010 + 10101) = ps(01111) = 4$

Ejemplo: Si $\mathcal{C}(\mathbb{Z}_2) = \{100, 111, 011\}$, tenemos que

$$\delta^{\mathcal{C}}_{min} = min\{\delta(100, 111), \delta(100, 011), \delta(111, 011)\} = min\{2, 3, 1\} = 1$$

Ejemplos

Consideremos $\mathbb{Z}^2 = \{00, 01, 10, 11\}$ y la función de codificación (2,5)

$$\mathcal{C} : \mathbb{Z}^2 \longrightarrow \mathbb{Z}^5$$

definida por la tabla

x	$\mathcal{C}(x)$
00	00000
01	00111
10	01110
11	11111

$\delta^{\mathcal{C}}_{min} = 2$ (obtenido después de hacer 6 cálculos)

Codificación de la información y detección de errores

Definiciones

Sea $\mathcal{C}$ una función de codificación (m, n).

- Se dice que $\mathcal{C}$ **detecta** a lo sumo k errores si siempre que $\mathcal{C}(x)$ se transmite con a lo sumo k errores (es decir, recibimos "y" en lugar de $\mathcal{C}(x)$, con $1 \leq \delta(\mathcal{C}(x), y) \leq k$, sabemos que y no es una palabra clave.

Información de $\delta^{\mathcal{C}}_{min}$

Teorema

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m, n), *entonces:*

1. *Si* $\delta^{\mathcal{C}}_{min} = d$, *se pueden detectar* $d - 1$ *errores*
2. *Si* $\delta^{\mathcal{C}}_{min} = d$, *se pueden corregir* $\frac{d-1}{2}$ *errores*

Ejemplo

Dada la función de codificación $\mathcal{C}: \mathbb{Z}_2^4 \to \mathbb{Z}_2^9$ definida como $\mathcal{C}(x) = xxc$, donde

$$c = \begin{cases} 0, & si \text{ ps(x) es par} \\ 1, & si \text{ ps(x) es impar} \end{cases},$$

después de $\begin{pmatrix} 16 \\ 2 \end{pmatrix} = \frac{16 \cdot 15}{2} = 120$ cálculos, obtenemos que $\delta^{\mathcal{C}}_{min} = 3$

Según el teorema anterior, con $\mathcal{C}$ se pueden detectar hasta 2 errores (3-1), pero solo se podrá corregir 1 error ($\frac{3-1}{2}$).

Funciones de Codificación especiales: Códigos de grupo

Definiciones

Una función de codificación $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ es un **código de grupo** si Im $\mathcal{C}$ es un subgrupo de $(\mathbb{Z}_2^n, +)$, así pues, es un subgrupo normal

Si $\mathcal{C}$ es un **código de grupo**

- $\mathbf{0} \in Im(\mathcal{C})$
- La suma de dos palabras de $Im(\mathcal{C})$ es una palabra de $Im(\mathcal{C})$

Los Códigos de grupo facilitan el cálculo de δ_{min}

Teorema

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *un código de grupo, entonces*

$$\delta_{min}^{\mathcal{C}} = min\{ps(\mathcal{C}(x) \mid x \in \mathbb{Z}_2^m;\ \mathcal{C}(x) \neq 0\}$$

En el último ejemplo bastará con calcular los pesos de 7 palabras en vez de hallar las 28 distancias entre parejas de palabras clave distintas.

x	$\mathcal{C}(x)$	$ps(\mathcal{C}(x))$
000	000000	0
001	001100	2
010	010011	3
011	011111	5
100	100101	3
101	101001	3
110	110110	4
111	111010	4

$\delta_{min}^{\mathcal{C}} = 2$

Matriz generadora para obtener códigos de grupo

Definición

Sean $m, n \in \mathbb{N}^+$, con $m < n$. Una **matriz generadora** *$\mathcal{G}$ es una matriz booleana $m \times n$ tal que las primeras m columnas forman la matriz identidad Id_m. Es decir, se tiene que $\mathcal{G} = \left(Id_m \mid A\right)$ donde A es una matriz $m \times (n-m)$.*

Teorema

Sea $\mathcal{G}$ una matriz generadora. Entonces la función de codificación $\mathcal{C}_\mathcal{G}$:

$$\begin{array}{ccc} \mathbb{Z}_2^m & \longrightarrow & \mathbb{Z}_2^n \\ (x_1 \dots x_m) & & (x_1 \dots x_m) \cdot \mathcal{G} = (y_1 \dots y_n) \end{array}$$

es un código de grupo.

Como $\mathcal{G} = \left(Id_m \mid A\right)$, el teorema dice que los m primeros símbolos de $(y_1 \dots y_n)$ coinciden con los de $(x_1 \dots x_m)$. Así, para obtener y solo es preciso calcular los $n-m$ símbolos de redundancia $y_{m+1}, \dots y_n$: $y_{m+j} = \Sigma_1^m x_i a_{ij} \quad j = 1, \dots n-m$

El código es el subgrupo generado por las filas de $\mathcal{G}$

Matriz Generadora

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^4$ dada por la matriz generadora

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

$$\begin{aligned}
\mathcal{C}_\mathcal{G}(00) &= \begin{pmatrix} 0 & 0 \end{pmatrix} \cdot \left(\begin{array}{cc||cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right) = 0000; \\
\mathcal{C}_\mathcal{G}(01) &= \begin{pmatrix} 0 & 1 \end{pmatrix} \cdot \left(\begin{array}{cc||cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right) = 0101; \quad 2^a \text{ fila de } \mathcal{G} \\
\mathcal{C}_\mathcal{G}(10) &= \begin{pmatrix} 1 & 0 \end{pmatrix} \cdot \left(\begin{array}{cc||cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right) = 1011; \quad 1^a \text{ fila de } \mathcal{G} \\
\mathcal{C}_\mathcal{G}(11) &= \begin{pmatrix} 1 & 1 \end{pmatrix} \cdot \left(\begin{array}{cc||cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right) = 1110; \quad 1^a + 2^a \text{ fila de } \mathcal{G}
\end{aligned}$$

$\delta_{min} = min\{2, 3\} = 2$, por eso el código puede detectar un error, pero no puede corregir errores.

Códigos de grupo

Ejemplo

Sea la función de codificación $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$ dada por la matriz generadora

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

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 00000 \\ \mathcal{C}_\mathcal{G}(10) &= 10110 \\ \mathcal{C}_\mathcal{G}(01) &= 01011 \\ \mathcal{C}_\mathcal{G}(11) &= 11101 \end{aligned}$$

$$\text{Im } \mathcal{C} = \{00000, 01011, 10110, 11101\}$$

La mínima distancia es 3, por eso el código puede detectar 2 errores y corregir 1.

Ejercicio

Sea $\mathcal{C} \subseteq \mathbb{Z}_2^5$ un código de grupo de cuatro elementos. Sabiendo que 10101 y 11010 son elementos de $\mathcal{C}$, determine los restantes elementos de $\mathcal{C}$ y una matriz generadora del código.

SOLUCIÓN

$\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^? \to \mathbb{Z}_2^5$, pero puesto que $\mathcal{C}_\mathcal{G}$ es inyectiva, si $|Im(\mathcal{C}_\mathcal{G}| = 4$ sabemos que $|\mathbb{Z}_2^?| = 4$, es decir, $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^2 \to \mathbb{Z}_2^5$

- Los restantes elementos, puesto que $Im(\mathcal{C}_\mathcal{G})$ es un subgrupo, son 00000 y $10101 + 11010 = 01111$
- Por lo tanto, la matriz generadora es

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

$$\begin{aligned} \mathcal{C}_\mathcal{G}(00) &= 00000 \\ \mathcal{C}_\mathcal{G}(10) &= 10101 \\ \mathcal{C}_\mathcal{G}(01) &= 01111 \\ \mathcal{C}_\mathcal{G}(11) &= 11011 \end{aligned}$$

Supongamos que tenemos $\mathcal{C}_{\mathcal{G}} : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$, dado por

$$\mathcal{C}_{\mathcal{G}} = (a_1 a_2 a_3) \cdot \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = a_1 a_2 a_3 (a_1 + a_3)(a_1 + a_2)(a_2 + a_3) = a_1 a_2 a_3 a_4 a_5 a_6$$

Obtenemos las ecuaciones

$$\begin{aligned} a_4 &= a_1 + a_3 \\ a_5 &= a_1 + a_2 \\ a_6 &= a_2 + a_3 \end{aligned}$$

Y como $-a_i = a_i$, podemos reescribir estas ecuaciones, llamadas de de verificación de paridad) como sigue:

$$\begin{array}{ccccccccccccc} a_1 & & & & a_3 & + & a_4 & & & & & = & 0 \\ a_1 & + & a_2 & & & & & + & a_5 & & & = & 0 \\ & & a_2 & + & a_3 & & & & & + & a_6 & = & 0 \end{array}$$

Es decir

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \end{pmatrix} = H \cdot \mathcal{C}(a)^{tr} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

El ejemplo anterior nos dice que

Si $y = (y_1y_2y_3y_4y_5y_6) \in \mathbb{Z}_2^6$, *podemos identificar* y *como una palabra codificada si y solo si*

$$H \cdot y^{tr} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Ahora vemos que la matriz H, *a la que llamaremos matriz de verificación de paridad, es de la forma* $H = (B \mid Id_3)$ *y que* $B = A^{tr}$

Teorema

Si H *es una matriz de verificación de paridad sin ninguna columna de ceros y sin columnas iguales, el código* $\mathcal{C} = \{w \mid H \cdot w^T = 0 \in \mathbb{Z}_2^m\}$ *corrige errores simples.*

Teorema

- *si* $G = (Id_m \mid A)$ *es una matriz generatriz de código* (m, n), *entonces la matriz* $H = (A^T \mid Id_{n-m})$ *es una matriz de verificación de paridad que reconoce el código generado por* G.
- *si* $H = (A \mid Id_{n-m})$ *es una matriz de verificación de paridad, entonces* $G = (Id_m \mid A^T)$ *es su correspondiente función generadora de código.*

Ejemplo

Si $\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$ es una matriz generadora de código, su matriz de verificación de paridad asociada es

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

Si una matriz de r filas no contiene una columna de ceros y ningún par de columnas iguales y tiene el número máximo de columnas posibles ($m = 2^r - 1$), entonces se le llama matriz de Hamming. Estas matrices tienen la propiedad de ser las que tienen mayor número de palabras en el código.

Decodificando con la matriz $\mathcal{H}$

Cuando se transmite un código x por un canal con ruido, la tupla de $\mathbb{Z}_2^n$ recibido, y no siempre coincide con el transmitido. Es decir

$$x + r = y; \qquad \text{con } r \neq 0$$

La tupla r se denomina **error**

A la salida del canal, el decodificador ignora el valor de x y de r. Dispone solo de la tupla y para inferir la palabra del código x.

Si estamos trabajando con un código de grupo, ya hemos visto que, para saber si y es una palabra de código nos basta comprobar si $H \cdot y^{tr} = 0$. El resultado de este cálculo se denomina síndrome

Usando la matriz de verificación de paridad para Decodificar

Teorema

Sea una matriz generadora $\mathcal{G} = \left(I_m \mid A_{m\times(n-m)}\right)$, *y su matriz de verificación de paridad asociada,* $\mathcal{H} = \left(A^{tr} \mid I_{n-m}\right)$. *Si* w_1 *y* w_2 *pertenecen a la misma clase lateral, entonces* $H \cdot w_1^{tr} = H \cdot w_2^{tr}$. *A este valor (cadena de longitud* $n-m$*) se le llama* **síndrome** *de la clase.*

Ejemplo

Tenemos $m = 2, n = 5, n - m = 3$

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \mathcal{H} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

El síndrome de 01100 es $\mathcal{H} \cdot 01100^{tr} = 111$ (la suma de la 2^a y 3^a columna de $\mathcal{H}$

El síndrome de 11101 es $\mathcal{H} \cdot 11101^{tr} = 000$. (suma de las columnas 1^a, 2^a, 3^a y 5^a). Así pues 11101 es una palabra de código (la suma de las dos filas de $\mathcal{G}$).

Usando la matriz de verificación para Decodificar

Teorema

Sea $\mathcal{H}$ una matriz de verificación de paridad asociada a una matriz $\mathcal{G}$ generadora de un código de grupo. Entonces w es una palabra clave si y sólo si su síndrome $\mathcal{H} \cdot w^{tr}$ es el elemento neutro de $\mathbb{Z}_2^{n-m}$.

Así pues:

El síndrome, s, de una tupla recibida y satisface:

$$s = \mathcal{H} \cdot y^{tr} = \mathcal{H} \cdot (x + r)^{tr} = \mathcal{H} \cdot x^{tr} + \mathcal{H} \cdot r^{tr} = 0 + \mathcal{H} \cdot r^{tr} = \mathcal{H} \cdot r^{tr}$$

Pero OJO : si $s = 0$ puede ser debido a que r es una palabra del código, y esto no lo podremos detectar.

¿Qué haremos si $s \neq 0$?. Tendremos que intentar resolver la ecuación

$$\mathcal{H} \cdot r^{tr} = s$$

en la que conocemos s y $\mathcal{H}$ son conocidos y r es la incógnita. De entre todas las soluciones de esta ecuación nos decidimos a favor de aquellas con menor peso (la más probable).

Decodificando

Haciendo uso de los síndromes, podemos pues decodificar una palabra y mediante el siguiente procedimiento:

1. Calculamos el síndrome de y, es decir, $s = \mathcal{H} \cdot y^{tr}$ (que no será 0). Ahora, si s es la i-ésima columna de $\mathcal{H}$, sabemos que x e y difieren únicamente en la i-ésima componente de y y procedemos a cambiarla, es decir, si, por ejemplo difieren en la 2^a columna, $y = x + (0, 1, 0 \ldots 0)$
2. Si s no es una columna de $\mathcal{H}$, pero sí la suma de la i-ésima columna y la j-ésima columna de $\mathcal{H}$, sabemos que x e y difieren en la i-ésima y en la j-ésima componente de y y procedemos a cambiarlas.
3. Sumamos $x + y$ y obtenemos c

Usando la matriz $\mathcal{C}$ para Decodificar

Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ un código de grupo. Sabemos que su imagen es un subgrupo normal de $\mathbb{Z}_2^n$. Veamos como obtener sus clases laterales

Tabla de decodificación

Se construye siguiendo los pasos:

1. Se escriben los elementos del código en la primera fila, es decir la clase $0 + \mathcal{C}$.
2. Para formar la segunda fila, se busca una palabra de peso mínimo $a_1 \in \mathbb{Z}_2^n$ que no esté en $\mathcal{C}$, y obtenemos la clase $a_1 + W$
3. En general, para formar la i-ésima fila tomamos a_i de peso mínimo que no se encuentre en las $i-1$ filas y obtenemos $a_i + \mathcal{C}$
4. El proceso termina cuando obtenemos una partición de $\mathbb{Z}_2^n$

Ejemplo

Consideremos la función codificadora generada por la matriz

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

da la siguiente tabla de corrección de errores:

$\mathcal{C}_G$	00000	01011	10101	11110
$00001 + \mathcal{C}_G$	00001	01010	10100	11111
$00010 + \mathcal{C}_G$	00010	01001	10111	11100
$00100 + \mathcal{C}_G$	00100	01111	10001	11010
$01000 + \mathcal{C}_G$	01000	00011	11101	10110
$10000 + \mathcal{C}_G$	10000	11011	00101	01110
$11000 + \mathcal{C}_G$	11000	10011	01101	00110
$01100 + \mathcal{C}_G$	01100	00111	11001	10010

Observamos que cuando obtenemos la fila $10000 + \mathcal{C}_G$, podemos elegir entre las palabras de peso 2: 11000, 10010, 01100 y 00110. Después de obtener la fila $11000 + \mathcal{C}_G$, podemos elegir entre 10010 y 01100

En el ejemplo anterior, $\delta_{min} = 3$ por lo que solo podemos corregir errores simples. Esto es debido a que las palabras de peso 1 son todas líderes de clase (las 5 primeras filas), pero no podemos corregir todos los errores dobles, ya que solo dos palabras de peso 2 son líderes de clase.
La matriz $\mathcal{H}$ asociada es

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

en la tabla anterior, vamos a añadir los síndromes de los líderes de clase

Ejemplo

000	$\mathcal{C}_G$	00000	01011	10101	11110
001	$00001 + \mathcal{C}_G$	00001	01010	10100	11111
010	$00010 + \mathcal{C}_G$	00010	01001	10111	11100
100	$00100 + \mathcal{C}_G$	00100	01111	10001	11010
011	$01000 + \mathcal{C}_G$	01000	00011	11101	10110
101	$10000 + \mathcal{C}_G$	10000	11011	00101	01110
110	$11000 + \mathcal{C}_G$	11000	10011	01101	00110
111	$01100 + \mathcal{C}_G$	01100	00111	11001	10010

Ahora, usando las dos primeras columnas de esta tabla, podemos decodificar una palabra recibida y como sigue

1. Calculamos el síndrome $s = \mathcal{H} \cdot y^{tr}$
2. elegimos el lider l de la clase a su derecha de la tabla
3. Sumamos $l + y$ para obtener la palabra x

Ejemplo

Volviendo a nuestro ejemplo

000	$\mathcal{C}_G$
001	$00001 + \mathcal{C}_G$
010	$00010 + \mathcal{C}_G$
100	$00100 + \mathcal{C}_G$
011	$01000 + \mathcal{C}_G$
101	$10000 + \mathcal{C}_G$
110	$11000 + \mathcal{C}_G$
111	$01100 + \mathcal{C}_G$

Así si la palabra recibida es $y = 10001$, su síndrome es $s = \mathcal{H} \cdot y^{tr} = 100$ y el lider de la clase a la derecha es 00100. Por lo tanto, corregimos y a $x = 10001$ de clase es $x = 00100$ por lo que, observando la tabla se tiene que encabeza su columna $x = l + y = 00100 + 10001 = 10101$, por tanto $D(10101) = 10$ (los dos 1^{os} dígitos de c).

Ejemplo

Sea un código de grupo dado por

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

Usando la equivalencia

000	001	010	011	100	101	110	111
A	C	E	N	O	R	S	T

se codifica y envía un mensaje que se recibe

101110 100001 101011 111011 010011 011110 111000 100001

¿Qué información se quiere transmitir?

Códigos de grupo

Matriz $\mathcal{H}$ de verificación de paridad

Solución

1. Calculamos el síndrome $v\mathcal{H}$ de cada palabra v recibida:

$$101 \quad 100 \quad 000 \quad 011 \quad 000 \quad 011 \quad 000 \quad 100$$

2. Hallamos los líderes e asociados usando la biyección:

$$100000 \quad 000100 \quad 000000 \quad 010000 \quad 000000 \quad 010000 \quad 000000 \quad 000100$$

3. Se corrige el mensaje haciendo $w = e + v$

$$\mathbf{0}01110 \quad 100\mathbf{1}01 \quad 101011 \quad 1\mathbf{0}1011 \quad 010011 \quad 0\mathbf{0}1110 \quad 111000 \quad 100\mathbf{1}01$$

4. Ignorando la información redundante, se obtiene el mensaje inicial

$$\underbrace{001}_{\mathbf{C}}\ \underbrace{100}_{\mathbf{O}}\ \underbrace{101}_{\mathbf{R}}\ \underbrace{101}_{\mathbf{R}}\ \underbrace{010}_{\mathbf{E}}\ \underbrace{001}_{\mathbf{C}}\ \underbrace{111}_{\mathbf{T}}\ \underbrace{100}_{\mathbf{O}}$$