Estructuras Algebraicas para la Computación

Mariam Cobalea

Universidad de Málaga
Dpto. de Matemática Aplicada

Tema 3: Grupos, anillos y cuerpos

- Grupos y subgrupos. Clases laterales y teorema de Lagrange.
- Introducción a la teoría de la codificación.
- Anillos. Elementos inversibles y divisores de cero. Cuerpos.

Introducción a la Teoría de la Codificación

La **teoría de grupos** y **cuerpos finitos** se puede aplicar en el **almacenamiento**, **recuperación** y **comunicación** de información.

Hay muchas situaciones en las que se han de **transmitir** una gran cantidad de **datos** rápidamente y con **fiabilidad**.

El conjunto de datos que se han de transmitir se llama ***mensaje***.

La ***teoría de la codificación*** estudia la representación de este ***mensaje*** mediante secuencias de símbolos de un alfabeto dado.

Introducción a la Teoría de la Codificación

Este alfabeto puede ser:

- $\{0, 1\}$ en un ordenador.
- $\{a, b, ..., y, z, -\}$ formado por las 29 letras y el carácter espacio, para almacenar palabras y oraciones en español.

  En este caso, también podemos hacer corresponder a cada uno de estos 30 símbolos una cadena binaria. De este modo, tendremos la información representada en binario.

  Por ejemplo, podemos usar la equivalencia

000	001	010	011	100	101	110	111
$-$	T	E	D	A	R	N	H

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**.
Por ejemplo, en

- **sistemas de comunicación**: radio, televisión, telégrafo, teléfono, ... los mensajes enviados pueden ser distorionados por fluctuaciones electromagnéticas, interferencias, ...
- **sistemas de almacenamiento de datos**: discos, cintas, películas, ... la información almacenada se puede alterar por cuerpos fuertemente magnéticos,...

El resultado es que **el mensaje recibido o leido puede ser diferente del enviado o almacenado originalmente**.

En este caso decimos que ha habido ***error*** en la transmisión.

Introducción a la Teoría de la Codificación

Es importante saber si ha ocurrido un error en la transmisión. En ese caso, se podría pedir que el mensaje sea repetido. Sin embargo, en algunas circunstancias es imposible o no deseable la repetición. Por eso, el mensaje que se transmite debería traer cierto grado de **redundancia** para que el mensaje original se pueda recuperar con un cierto grado de certidumbre.

La manera de hacer esto es añadir al mensaje un número de símbolos (dígitos) de **control** para que los errores se puedan **detectar** e incluso **corregir**.

La teoría de codificación ha desarrollado técnicas para introducir en los datos transmitidos información redundante que ayude a detectar (e incluso a corregir) los errores.

Algunas de éstas técnicas utilizan la teoría de grupos.

Codificación de la información y detección de errores

Definición

- *Se llama **palabra** a una secuencia de símbolos de un alfabeto.*
- *Un **código** es una colección de palabras que se usan para representar mensajes.*
- *Una palabra de un código se llama también **palabra clave**.*
- *Un **código de bloques** es un código formado por palabras que tienen la misma longitud.*

A partir de ahora, trabajaremos con el alfabeto $\{0, 1\}$.

Cada carácter que se quiera transmitir se representa en forma binaria.

Las palabras de longitud m se pueden considerar como elementos del grupo $(\mathbb{Z}_2^m, \oplus)$ (escritos sin paréntesis ni corchetes).

Por ejemplo, $0010, 0101, 0001$ son palabras de longitud 4.

Codificación de la información y detección de errores

Supongamos que 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). Con esta función cada palabra de $\mathbb{Z}_2^m$ se representa mediante una palabra 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.

Al conjunto $Im\mathcal{C}$ se le denota $\mathcal{W}$ y se le llama también ***código*** o conjunto de ***palabras clave***.

Codificación de la información y detección de errores

Ejemplo

1. Función de codificación de **control de paridad** $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^{m+1}$ definida

$$\mathcal{C}(x) = xc, \text{ donde } c = \begin{cases} 0, & \text{si el nº de } 1'^s \text{ de } x \text{ es par} \\ 1, & \text{si el nº de } 1'^s \text{ de } x \text{ es impar} \end{cases}$$

   - El último dígito es un dígito de **control de paridad:** cualquier palabra transmitida correctamente tiene un número par de $1'^{os}$.

2. Función de codificación de **triple repetición** $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^{3m}$ definida

$$\mathcal{C}(x) = xxx$$

   - Supongamos que xxx es la palabra enviada y abc es la palabra recibida. Si no ha habido errores,

$$a = b = c = x$$

Codificación de la información y detección de errores

Definición

*Se llama **peso** de una palabra x, y se denota $|x|$, al número de $1'^s$ de dicha palabra.*

Ejemplo El peso de la palabra 11001 es 3.

Definición

*Sean u y v palabras de la misma longitud. La **distancia** entre u y v, denotada $\delta(u, v)$, es el número de posiciones en que difieren. Este número coincide con el peso de su diferencia.*

$$\delta(u, v) = |u - v| = |u \oplus v|$$

Ejemplo $\delta(11011, 10101) = 3$

Codificación de la información y detección de errores

Teorema (Propiedades de la distancia)

Sean $x, y, z \in \mathbb{Z}_2^m$. Entonces

1. $\delta(x, y) = \delta(y, x)$
2. $\delta(x, y) \geq 0$
3. $\delta(x, y) = 0 \iff x = y$
4. $\delta(x, y) \leq \delta(x, z) + \delta(z, y)$

Demostración: Ejercicio

- 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.
- Por lo tanto, una ***buena*** función de codificación será aquella que ***maximice*** las distancias entre palabras clave.

Codificación de la información y detección de errores

Definición

*Sea $\mathcal{C}$ una función de codificación (m, n). Se dice que la palabra clave $\mathcal{C}(x)$ se ha transmitido con **k errores a lo sumo** si la palabra enviada $\mathcal{C}(x)$ y la palabra recibida v difieren como mínimo en 1 posición y a lo sumo en k posiciones. Es decir, si*

$$1 \leq \delta(\mathcal{C}(x), v) \leq k$$

*Se dice que $\mathcal{C}$ **detecta** a lo sumo k errores si siempre que $\mathcal{C}(x)$ se transmite con k errores a lo sumo, la palabra recibida v no es una palabra clave.*

Codificación de la información y detección de errores

Definición

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

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

Ejercicio Dada la función de codificación

$$\begin{aligned}\mathcal{C}\colon\quad & \mathbb{Z}_2^4 \to \mathbb{Z}_2^9 \\ & \mathcal{C}(x) = xxc\end{aligned} \qquad c = \left\{\begin{array}{ll} 0, & |x| \text{ es par} \\ 1, & |x| \text{ es impar}\end{array}\right\}$$

comprueba que la mínima distancia es 3.

Codificación de la información y detección de errores

Teorema

Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m,n). *Entonces* $\mathcal{C}$ *permite detectar a lo sumo* k *errores si y sólo si la mínima distancia de* $\mathcal{C}$ *es al menos* $k+1$.

Ejemplo La función de codificación

$$\begin{aligned}\mathcal{C}\colon\quad & \mathbb{Z}_2^4 \to \mathbb{Z}_2^9 \\ & \mathcal{C}(x) = xxc\end{aligned} \qquad c = \left\{\begin{array}{ll} 0 & |x| \text{ es par} \\ 1 & |x| \text{ es impar}\end{array}\right\}$$

nos permite detectar 2 errores, ya que la mínima distancia es 3.

Teorema

Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m,n). *Entonces* $\mathcal{C}$ *permite corregir* k *errores a lo sumo si y sólo si la mínima distancia de* $\mathcal{C}$ *es al menos* $2k+1$.

Códigos de grupo

Calcular la mínima distancia de una función de codificación puede ser una tarea tediosa. Sin embargo, se puede evitar usando la teoría de grupos.

Definición

Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m,n). *Se dice que nos da un **código de grupo** si* $\mathrm{Im}\mathcal{C} = \mathcal{W}$ *es un subgrupo de* $\mathbb{Z}_2^n$.
(Estos códigos se llaman también códigos lineales).

Teorema

Sea $\mathcal{C}\colon \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ *una función de codificación* (m,n) *que nos da un código de grupo. Entonces la mínima distancia de* $\mathcal{C}$ *coincide con el mínimo peso de las palabras clave no nulas.*

$$\text{mín.}\{\delta(\mathcal{C}(x),\mathcal{C}(y)),\quad x,y\in\mathbb{Z}_2^m,\quad x\neq y\} = \text{mín.}\{|\mathcal{C}(x)|,\ 0\neq x\in\mathbb{Z}_2^m\}$$

Códigos de grupo

- Aplicando este teorema, se simplifica considerablemente la tarea de encontrar el número de errores que detecta una función de codificación.
- En el ejemplo anterior bastará con calcular los pesos de 15 palabras en vez de hallar todas las distancias entre parejas de palabras clave distintas. Así, es obvio que tener un código de grupo resulta muy útil.
- Ahora se estudiará un procedimiento para generar un código de grupo.
- Teniendo en cuenta que $(\mathbb{Z}_2^m,\oplus)$ y $(\mathbb{Z}_2^n,\oplus)$ son grupos, una manera de asegurarnos un código de grupo es que la función de codificación sea homomorfismo de grupos.
- Veamos cómo conseguirlo.

Códigos de grupo

Definición (Matriz generadora $\mathcal{G}$)

*Sean m, n enteros, con $m < n$. Una **matriz generadora** $\mathcal{G}$ es una matriz $m \times n$ con entradas en $\mathbb{Z}_2$ de manera que las primeras m columnas forman la matriz identidad $\mathcal{I}_m$.*

$$\mathcal{G} = \begin{pmatrix} \mathcal{I}_m & A \end{pmatrix}, \quad \text{donde } A \text{ es una matriz } m \times (n-m)$$

Ejemplo

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

A partir de una matriz generadora $\mathcal{G}$ podemos definir una función de codificación

$$\begin{array}{rccc} \mathcal{C}_\mathcal{G} & : & \mathbb{Z}_2^m & \to & \mathbb{Z}_2^n \\ & & x & \mapsto & \mathcal{C}_\mathcal{G}(x) = x\mathcal{G} \end{array}$$

Códigos de grupo

A partir de una matriz generadora $\mathcal{G}$ podemos definir una función de codificación

$$\begin{array}{rccc} \mathcal{C}_\mathcal{G} & : & \mathbb{Z}_2^m & \to & \mathbb{Z}_2^n \\ & & x & \mapsto & \mathcal{C}_\mathcal{G}(x) = x\mathcal{G} \end{array}$$

Ejemplo La función de codificación $\mathcal{C}_\mathcal{G} : \mathbb{Z}_2^3 \to \mathbb{Z}_2^4$ dada por la matriz generadora

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \qquad \begin{array}{rcl} \mathcal{C}_\mathcal{G}(000) & = & 0000 \\ \mathcal{C}_\mathcal{G}(001) & = & 0011 \\ \mathcal{C}_\mathcal{G}(010) & = & 0101 \\ \mathcal{C}_\mathcal{G}(010) & = & 0101 \\ \mathcal{C}_\mathcal{G}(011) & = & 0110 \\ \mathcal{C}_\mathcal{G}(100) & = & 1001 \\ \mathcal{C}_\mathcal{G}(101) & = & 1010 \\ \mathcal{C}_\mathcal{G}(110) & = & 1100 \\ \mathcal{C}_\mathcal{G}(111) & = & 1111 \end{array}$$

Códigos de grupo

Teorema

Sea $\mathcal{G}$ una matriz generadora. Entonces $\mathcal{C}_\mathcal{G}$ nos da un código de grupo.

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

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix} \qquad \begin{array}{rcl} \mathcal{C}_\mathcal{G}(00) & = & 0000 \\ \mathcal{C}_\mathcal{G}(01) & = & 0101 \\ \mathcal{C}_\mathcal{G}(10) & = & 1011 \\ \mathcal{C}_\mathcal{G}(11) & = & 1110 \end{array}$$

$$Im\mathcal{C} = \mathcal{W} = \{0000, 0101, 1011, 1110\}$$

La mínima distancia entre palabras clave es 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

$$\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix} \qquad \begin{array}{rcl} \mathcal{C}_\mathcal{G}(00) & = & 00000 \\ \mathcal{C}_\mathcal{G}(01) & = & 01011 \\ \mathcal{C}_\mathcal{G}(10) & = & 10110 \\ \mathcal{C}_\mathcal{G}(11) & = & 11101 \end{array}$$

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

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

Códigos de grupo

Ejemplo Sea la función de codificación $\mathcal{C}_\mathcal{G}: \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ dada por la matriz generadora

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

$$\begin{aligned} \mathcal{C}_\mathcal{G}(000) &= 000000 \\ \mathcal{C}_\mathcal{G}(001) &= 001111 \\ \mathcal{C}_\mathcal{G}(010) &= 010101 \\ \mathcal{C}_\mathcal{G}(011) &= 011010 \\ \mathcal{C}_\mathcal{G}(100) &= 100111 \\ \mathcal{C}_\mathcal{G}(101) &= 101000 \\ \mathcal{C}_\mathcal{G}(110) &= 110010 \\ \mathcal{C}_\mathcal{G}(111) &= 111101 \end{aligned}$$

$$\mathcal{W} = \{000000, 001111, 010101, 011010, 100111, 101000, 110010, 111101\}$$

La mínima distancia entre palabras clave es 2, por eso el código puede detectar 1 error, pero no puede corregir ni siquiera un simple error.

Códigos de grupo

Ejercicio

Sea $\mathcal{C} \subseteq \mathbb{Z}_2^5$ un código de grupo de cuatro elementos.

Sabiendo que 10101 y 11010 son elementos de $\mathcal{C}$, determina:

1. los restantes elementos de $\mathcal{C}$.
2. una matriz $\mathcal{G}$ generadora del código.

Códigos de grupo

¿Cómo detectar y corregir errores en un mensaje recibido?

- Sea $\mathcal{C}: \mathbb{Z}_2^m \to \mathbb{Z}_2^n$ un código de grupo y sea $\mathcal{W}$ el conjunto de palabras clave (que es un subgrupo de $\mathbb{Z}_2^n$).
- Se envía la palabra $\mathcal{C}(x) = w$, pero ocurre algún error y se recibe v.

Nuestro problema es identificar la palabra $\mathcal{C}(x) = w$ del mensaje original.

- Si al enviar la palabra w ocurre un error en el último dígito, por ejemplo, y se recibe la palabra v, entonces v coincide con w en todos los dígitos excepto en el último:

$$v = e_n \oplus w, \text{ donde } e_n = 0\ldots01$$

- Así pues, el conjunto de palabras que se pueden recibir como resultado de un simple error en el último dígito es $e_n \oplus \mathcal{W}$.

$$e_n \oplus \mathcal{W}: \text{ clase lateral de } e_n \text{ respecto del subgrupo } \mathcal{W}$$

Códigos de grupo

¿Cómo detectar y corregir errores en un mensaje recibido?

- Análogamente, para un error en el dígito j, obtendremos una palabra de la clase lateral $e_j \oplus \mathcal{W}$ del elemento e_j respecto al subgrupo $\mathcal{W}$.
- Si se recibe una palabra que no es una palabra clave, sabemos que ha ocurrido algún error.
- Buscaremos recuperar la palabra que haya sido enviada más probablemente: **criterio de máxima verosimilitud**
- Lo que hacemos es 'corregir' el mensaje reemplazando la palabra recibida v por la palabra clave w que sea 'más cercana'.
- Para ello, calculamos la distancia entre la palabra recibida v y cada una de las palabras clave $w \in \mathcal{W}$, buscando la mínima distancia $\delta(v, w)$ y reemplazamos la palabra recibida v por la palabra clave w_0 tal que $\delta(v, w_0)$ es mínima.

Códigos de grupo
¿Cómo detectar y corregir errores en un mensaje recibido?

En vez de hacer los cálculos anteriores para cada palabra errónea recibida, se hacen de una vez y se prepara una tabla que muestra los resultados. Esta tabla se llama **tabla de decodificación**y se construye siguiendo los pasos:

1. Se escriben los elementos de $\mathcal{W}$ en la primera fila.
2. Se busca una palabra de peso mínimo e que no esté en $\mathcal{W}$.
3. Se escribe la palabra $e \oplus w$ bajo cada palabra clave.
4. Se busca una palabra de peso mínimo e' que todavía no esté escrita y se escribe la clase lateral $e' \oplus \mathcal{W}$ en la siguiente línea.

Se repite este procedimiento hasta que todos los elementos de $\mathbb{Z}_2^n$ se hayan escrito.

Códigos de grupo
¿Cómo detectar y corregir errores en un mensaje recibido?

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

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

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

La tabla de decodificación es

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

Códigos de grupo
¿Cómo detectar y corregir errores en un mensaje recibido?

Al recibir una palabra v, buscamos dónde está situada en la tabla.

Una vez encontrada, la reemplazamos por la palabra clave que está en la primera fila de su columna:

$$v = e \oplus w \implies (-e) \oplus v = (-e) \oplus e \oplus w \implies w = -e \oplus v = e \oplus v$$

Este procedimiento se resumen en:

1. Se determinan todas las clases laterales respecto de $\mathcal{W}$.
2. En cada clase se elige una palabra de peso mínimo (**representante** de la clase).
3. Para una palabra recibida v, la palabra transmitida (con mayor probabilidad) es $e \oplus v$, donde e es el representante de la clase a la que pertenece v.

Códigos de grupo
¿Cómo detectar y corregir errores en un mensaje recibido?

Ejemplo Se quiere enviar el mensaje

00 01 10 11 11 01 00

Se codifica usando la matriz $\mathcal{G}$ del ejemplo anterior y queda

00000 01011 10110 11101 11101 01011 00000

se envía, pero se recibe

00000 00011 11100 11101 10101 11101 01000

Se corrige a

00000 01010 11101 11101 11101 11101 00000

Se recupera lo que esperamos es el mensaje enviado.
Por último, extrayendo los dos primeros dígitos de cada palabra, nos queda

00 01 11 11 11 11 00

Hemos corregido los errores simples, pero no los dobles ni los triples.

Códigos de grupo

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

Se puede simplificar la tarea de decodificación realizada anteriormente.

Definición

Dada una matriz generadora $\mathcal{G} = (I_m \; A)$, *la* **matriz de verificación de paridad** *asociada es la matriz* $\mathcal{H}$ *dada por*

$$\mathcal{H} = \begin{pmatrix} A \\ I_{n-m} \end{pmatrix}$$

Ejemplo

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

$$m = 2, \qquad n = 5, \qquad n - m = 3$$

Códigos de grupo

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

Definición

Dada una palabra $v \in \mathbb{Z}_2^n$, *el* **síndrome** *de* v *es* $v\mathcal{H}$

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* $w\mathcal{H}$ *es el elemento neutro de* $\mathbb{Z}_2^{n-m}$.

$$w \in \mathcal{W} \iff w\mathcal{H} = 0\ldots0 \in \mathbb{Z}_2^{n-m}$$

Corolario

Dos palabras están en la misma fila de la tabla de decodificación si y sólo si tienen el mismo síndrome.

Códigos de grupo

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

Ejercicio Sea el código generado por la matriz $\mathcal{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}$

Comprueba el teorema y el corolario anterior para

$$w = 01011, \quad e_3 = 00100, \quad v_1 = 01111 \;\text{ y }\; v_2 = 11001$$

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

Códigos de grupo

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

Ejercicio Sea $\mathcal{C}$ un código con matriz de verificación de paridad

$$\mathcal{H} = \begin{pmatrix} a & 0 & c & 1 \\ 1 & b & 0 & d \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

1. Calcula los valores a, b, c, d para que $\mathcal{H}$ reconozca las palabras 101011 y 110110 como pertenecientes al código.
2. Encuentra las restantes palabras del código y determina hasta cuántos errores se pueden corregir.

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?

Solución: Usamos la matriz de verificación de paridad $\mathcal{H}$, correspondiente a la matriz generadora $\mathcal{G}$, para hallar los síndromes de cada uno de los representantes (**líderes**) de cada clase lateral

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

Síndromes	Líderes
000	000000
001	000001
010	000010
100	000100
110	001000
011	010000
101	100000
111	100010

Solución:(cont.)

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

101 100 000 011 000 011 000 100

(2) Hallamos los correspondientes líderes de las clases laterales:

$$e \mid e\mathcal{H} = v\mathcal{H}$$

100000 000100 000000 010000 000000 010000 000000 000100

(3) Se corrige el mensaje: $w = e \oplus v$

001110 100101 101011 101011 010011 001110 111000 100101

(4) Se obtiene el mensaje inicial

$\underbrace{001}_{C}110$ $\underbrace{100}_{O}101$ $\underbrace{101}_{R}011$ $\underbrace{101}_{R}011$ $\underbrace{010}_{E}011$ $\underbrace{001}_{C}110$ $\underbrace{111}_{T}000$ $\underbrace{100}_{O}101$

Teoría de la Codificación

Ejercicio Sea la función de codificación $\mathcal{C}_{\mathcal{G}} : \mathbb{Z}_2^3 \to \mathbb{Z}_2^6$ dada por la matriz generadora

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

1. Escribe la tabla de decodificación para $\mathcal{C}_{\mathcal{G}}$.
2. Decodifica y traduce el mensaje

011011 110000 010110 100000 110110 110111 011111.

usando la equivalencia

000 blanco 100 A 010 E 001 T 110 N 101 R 011 D 111 H

Teoría de la Codificación

Ejercicio Se sabe que la matriz generadora de un cierto código es

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

y se recibe el mensaje

000111 011100 000000 101101 001010 010011

1. Determina qué palabras pertenecen o no al código calculando su síndrome.
2. Decodifica y traduce el mensaje recibido usando la equivalencia
   111 A 110 N 101 T 100 S 011 E 010 R 001 O 000 C

Bibliografía

Matemáticas discreta y combinatoria R.P. Grimaldi (Ed. Addison Wesley)

Estructuras de Matemáticas Discretas para la Computación
B. Kolman y R.C. Busby (Ed. Prentice Hall)

Estructuras de Matemáticas Discretas para la Computación
B. Kolman, R.C. Busby y S. Ross (Ed. Prentice Hall)

Algebra lineal con aplicaciones y Mathlab
B. Kolman y D. Hill (Ed. Prentice Hall)

Elementos de Matemáticas Discretas C.L. Liu (Ed. McGraw Hill)