Introducción a los códigos correctores de errores

Mathematics sin fronteras

María Chara

Universidad Nacional del Litoral

19 de mayo 2021

FIQ UNL. FACULTAD DE INGENIERÍA QUÍMICA

Mariner 9, 1971

Logros de códigos de corrección de errores

Para controlar los errores en la recepción de los datos de imagen en escala de grises enviados por Mariner 9 (causados por una baja relación señal / ruido), los datos tenían que codificarse antes de la transmisión utilizando un llamado código de corrección de errores (FEC). . Sin FEC, el ruido habría constituido aproximadamente una cuarta parte de una imagen recibida, mientras que FEC codificaba los datos de forma redundante, lo que permitía la reconstrucción de la mayoría de los datos de la imagen enviada en la recepción.

Dado que el hardware volado estaba restringido con respecto al peso, el consumo de energía, el almacenamiento y la potencia de cálculo, se tuvieron que tener en cuenta algunas consideraciones al elegir un FEC, y se decidió usar un código Hadamard para Mariner 9. Cada píxel de la imagen se representó como un valor binario de seis bits, que tenía 64 niveles de escala de grises posibles . Debido a las limitaciones del transmisor, la longitud máxima de datos útiles fue de unos 30 bits. En lugar de utilizar un código de repetición , se utilizó un código Hadamard [32, 6, 16], que también es un código Reed-Muller de primer orden . Los errores de hasta siete bits por cada palabra de 32 bits podrían corregirse utilizando este esquema. En comparación con un código de cinco repeticiones, las propiedades de corrección de errores de este código Hadamard eran mucho mejores, pero su velocidad de datos era comparable. El algoritmo de decodificación eficiente fue un factor importante en la decisión de utilizar este código. El circuito utilizado se denominó "Máquina verde", que empleó la transformada rápida de Fourier , aumentando la velocidad de decodificación en un factor de tres.

Figure: https://es.qwe.wiki/wiki/Mariner_9

Codificación y decodificación con la matriz generadora

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k\times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

Codificación y decodificación con la matriz generadora

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k\times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

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

Codificación y decodificación con la matriz generadora

- Dada una base $\mathcal{B} = \{v_1, \ldots, v_k\}$ de un $[n, k]-$código $\mathcal{C}$ definimos la matriz generadora G del código $G_{k\times n}$ como la matriz cuyas filas son los vectores v_i de la base.

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ podemos definir una forma de codificar mensajes usando la matriz generadora G:

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ u & \to & c = uG \end{array}$$

- Ejemplo: Mariner 9

$$u = (a_1, a_2, \ldots, a_6) \longrightarrow c = (c_1, c_2, \ldots, c_{32})$$

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

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), (110110), (011011), (101101), (111000)\}.$$

Codificación y decodificación con la matriz generadora

- Si G está en forma estándar, es decir si $G = (I_k|A)$, entonces decodificar es trivial ya que en esta situación

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

Codificación y decodificación con la matriz generadora

- Si G está en forma estándar, es decir si $G = (I_k|A)$, entonces decodificar es trivial ya que en esta situación

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

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

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), \\ (110110), (011011), (101101), (111000)\}.$$

Codificación y decodificación con la matriz generadora

- Si G está en forma estándar, es decir si $G = (I_k|A)$, entonces decodificar es trivial ya que en esta situación

$$u \in \mathbb{F}_q^k \quad \longrightarrow \quad c = uG = (u|uA) \in \mathbb{F}_q^n \quad \longrightarrow \quad u = c_{|_{\mathbb{F}_q^k}} \in \mathbb{F}_q^k.$$

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

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), \\ (110110), (011011), (101101), (111000)\}.$$

¿Cómo sabemos si una palabra fue transmitida con error?

Matriz de control y código dual

En $\mathbb{F}_q^n$ podemos definir un producto interno como

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ en $\mathbb{F}_q^n$.

Matriz de control y código dual

En $\mathbb{F}_q^n$ podemos definir un producto interno como

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ en $\mathbb{F}_q^n$.

- Si $\mathcal{C}$ es un código sobre $\mathbb{F}_q$, entonces

$$\mathcal{C}^{\perp} = \{u \in \mathbb{F}_q^n : \langle u, c \rangle = 0 \text{ para todo } c \in \mathcal{C}\}$$

se llama código dual de $\mathcal{C}$.

Matriz de control y código dual

En $\mathbb{F}_q^n$ podemos definir un producto interno como

$$\langle a, b \rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ en $\mathbb{F}_q^n$.

- Si $\mathcal{C}$ es un código sobre $\mathbb{F}_q$, entonces

  $$\mathcal{C}^{\perp} = \{u \in \mathbb{F}_q^n : \langle u, c \rangle = 0 \text{ para todo } c \in \mathcal{C}\}$$

  se llama código dual de $\mathcal{C}$.

- Un código $\mathcal{C}$ se llama auto dual si $\mathcal{C}^{\perp} = \mathcal{C}$.

Matriz de control y código dual

En $\mathbb{F}_q^n$ podemos definir un producto interno como

$$\langle a, b\rangle = \sum_{i=1}^{n} a_i b_i,$$

para $a = (a_1, \ldots, a_n)$ y $b = (b_1, \ldots, b_n)$ en $\mathbb{F}_q^n$.

- Si $\mathcal{C}$ es un código sobre $\mathbb{F}_q$, entonces

  $$\mathcal{C}^{\perp} = \{u \in \mathbb{F}_q^n : \langle u, c\rangle = 0 \text{ para todo } c \in \mathcal{C}\}$$

  se llama código dual de $\mathcal{C}$.

- Un código $\mathcal{C}$ se llama auto dual si $\mathcal{C}^{\perp} = \mathcal{C}$.

Proposición

Si $\mathcal{C}$ es un $[n, k]-$código sobre $\mathbb{F}_q$ entonces $\mathcal{C}^{\perp}$ es un $[n, n-k]-$código sobre $\mathbb{F}_q$.

Matriz de control y código dual

Una matriz H de $(n-k) \times n$ que es una matriz generadora de $\mathcal{C}^{\perp}$ se llama matriz de control o matriz de chequeo de paridad del código C.

Matriz de control y código dual

Una matriz H de $(n-k) \times n$ que es una matriz generadora de $\mathcal{C}^{\perp}$ se llama matriz de control o matriz de chequeo de paridad del código C.

- Esta matriz H permite decidir (o controlar) si una palabra está en el código o no, ya que

$$x \in \mathcal{C} \iff Hx^T = 0.$$

Matriz de control y código dual

Una matriz H de $(n-k) \times n$ que es una matriz generadora de $\mathcal{C}^{\perp}$ se llama matriz de control o matriz de chequeo de paridad del código C.

- Esta matriz H permite decidir (o controlar) si una palabra está en el código o no, ya que
$$x \in \mathcal{C} \iff Hx^T = 0.$$
- Si la matriz generadora G de un código $\mathcal{C}$ se encuentre en forma estándar, es decir
$$G = (I_k|A)$$
entonces una matriz de control para $\mathcal{C}$ es
$$H = (-A^T|I_{n-k})$$
donde I_{n-k} es la matriz identidad de tamaño $n-k$.

Matriz de control y código dual

Una matriz H de $(n-k) \times n$ que es una matriz generadora de $\mathcal{C}^{\perp}$ se llama matriz de control o matriz de chequeo de paridad del código C.

- Esta matriz H permite decidir (o controlar) si una palabra está en el código o no, ya que
$$x \in \mathcal{C} \iff Hx^T = 0.$$
- Si la matriz generadora G de un código $\mathcal{C}$ se encuentre en forma estándar, es decir
$$G = (I_k|A)$$
entonces una matriz de control para $\mathcal{C}$ es
$$H = (-A^T|I_{n-k})$$
donde I_{n-k} es la matriz identidad de tamaño $n-k$.
- Una matriz H de esta forma se dice que está en forma estándar como matriz de paridad (aunque no está en forma estándar como matriz generadora de $\mathcal{C}^{\perp}$).

Ejemplo

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

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), \\ (110110), (011011), (101101), (111000)\}.$$

Definición

Si $\mathcal{C}$ es un $[n,k]-$código sobre $\mathbb{F}_q$ y H es una matriz de paridad para $\mathcal{C}$, entonces para cualquier vector $y \in \mathbb{F}_q^n$ definimos el *síndrome* de y como $S(y) = yH^T$.

- $y \in \mathcal{C}$ si y sólo si $S(y) = 0$.
- Si $y \notin \mathcal{C}$ entonces corregimos a y como $y - e$ donde $S(y) = S(e)$.

Definición

Si $\mathcal{C}$ es un $[n, k]-$código sobre $\mathbb{F}_q$ y $a \in \mathbb{F}_q^n$, definimos la *clase lateral izquierda* $a + \mathcal{C}$ como $a + \mathcal{C} = \{a + x : x \in \mathcal{C}\}$.

Definición

Si $\mathcal{C}$ es un $[n,k]-$código sobre $\mathbb{F}_q$ y $a \in \mathbb{F}_q^n$, definimos la *clase lateral izquierda* $a+\mathcal{C}$ como $a+\mathcal{C} = \{a+x : x \in \mathcal{C}\}$.

- $\mathcal{C} \subset \mathbb{F}_q^n$ es un espacio vectorial
- El cociente

$$\mathbb{F}_q^n/\mathcal{C} = \{a+\mathcal{C} : a \in \mathbb{F}_q^n\}$$

también es un espacio vectorial

$$\alpha(a+\mathcal{C}) = \alpha a + \mathcal{C} \qquad (a+\mathcal{C})+(b+\mathcal{C}) = (a+b)+\mathcal{C}$$

con $\alpha \in \mathbb{F}_q$ y $a, b \in \mathbb{F}_q^n$, y además

Definición

Si $\mathcal{C}$ es un $[n,k]-$código sobre $\mathbb{F}_q$ y $a \in \mathbb{F}_q^n$, definimos la *clase lateral izquierda* $a+\mathcal{C}$ como $a+\mathcal{C} = \{a+x : x \in \mathcal{C}\}$.

- $\mathcal{C} \subset \mathbb{F}_q^n$ es un espacio vectorial
- El cociente

$$\mathbb{F}_q^n/\mathcal{C} = \{a+\mathcal{C} : a \in \mathbb{F}_q^n\}$$

también es un espacio vectorial

$$\alpha(a+\mathcal{C}) = \alpha a + \mathcal{C} \qquad (a+\mathcal{C})+(b+\mathcal{C}) = (a+b)+\mathcal{C}$$

con $\alpha \in \mathbb{F}_q$ y $a, b \in \mathbb{F}_q^n$, y además

- $|\mathbb{F}_q^n/\mathcal{C}| = |\mathbb{F}_q^n|/|\mathcal{C}| = q^n/q^k = q^{n-k}$.

Teorema

Cada palabra de $\mathbb{F}_q^n$ pertenece a una sola clase lateral de $\mathcal{C}$. Dos clases laterales o son disjuntas o son iguales.

- Hay q^{n-k} clases disjuntas con q^k palabras cada una.
- El *líder* de cada clase es una palabra de peso mínimo, y si hay más de una, cualquiera de ellas.
- Para corregir errores necesitamos una tabla con los líderes de cada clase y sus síndromes.

Ejemplo

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

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), \\ (110110), (011011), (101101), (111000)\}.$$

Ejemplo

$$\mathcal{C} = \{(000000), (100011), (010101), (001110), (110110), (011011), (101101), (111000)\}.$$

$e_0 = (000000)\ S(e_0) = (000)$	$e_4 = (000100)\ S(e_4) = (100)$
$e_1 = (100000)\ S(e_1) = (011)$	$e_5 = (000010)\ S(e_5) = (010)$
$e_2 = (010000)\ S(e_2) = (101)$	$e_6 = (000001)\ S(e_6) = (001)$
$e_3 = (001000)\ S(e_3) = (110)$	$e_7 = (100100)\ S(e_7) = (111)$

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

- $x = (010101) \rightarrow y = (010001)$
- $x = (010101) \rightarrow y = (011101)$
- $x = (011011) \rightarrow y = (011111)$
- $x = (110110) \rightarrow y = (110010)$
- 2 errores: $x = (110110) \rightarrow y = (110101)$

Teorema

Sea $\mathcal{C}$ un $[n, k, d]$-código y sea H una matriz de control para $\mathcal{C}$. Entonces

$$d = \min\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Teorema

Sea $\mathcal{C}$ un $[n, k, d]$-código y sea H una matriz de control para $\mathcal{C}$. Entonces

$$d = \min\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Demostración

Teorema

Sea $\mathcal{C}$ un $[n, k, d]$-código y sea H una matriz de control para $\mathcal{C}$. Entonces

$$d = \min\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Demostración Sean H^1, H^2, ..., H^n las columnas de H. Entonces

$$c = (c_1, \ldots, c_n) \in \mathcal{C} \iff Hc^T = 0 \iff cH^T = 0 \iff c_1 H^1 + \cdots + c_n H^n = 0.$$

Teorema

Sea $\mathcal{C}$ un $[n, k, d]$-código y sea H una matriz de control para $\mathcal{C}$. Entonces

$$d = \min\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Demostración Sean H^1, H^2, ..., H^n las columnas de H. Entonces

$$c = (c_1, \ldots, c_n) \in \mathcal{C} \iff Hc^T = 0 \iff cH^T = 0 \iff c_1 H^1 + \cdots + c_n H^n = 0.$$

Si $c \in \mathcal{C}$ es una palabra de peso mínimo d tenemos que H tiene d columnas linealmente dependientes en H, y no puede haber ninguna cantidad menor de columnas linealmente dependientes porque en ese caso habría palabras no nulas en $\mathcal{C}$ con peso menor a d.

Teorema

Sea $\mathcal{C}$ un $[n, k, d]$-código y sea H una matriz de control para $\mathcal{C}$. Entonces

$$d = \min\{r : \text{ hay } r \text{ columnas linealmente dependientes en } H\}.$$

Es decir, H tiene d columnas linealmente dependientes pero cualquier conjunto de $d-1$ columnas son linealmente independientes.

Demostración Sean H^1, H^2, ..., H^n las columnas de H. Entonces

$$c = (c_1, \ldots, c_n) \in \mathcal{C} \iff Hc^T = 0 \iff cH^T = 0 \iff c_1 H^1 + \cdots + c_n H^n = 0.$$

Si $c \in \mathcal{C}$ es una palabra de peso mínimo d tenemos que H tiene d columnas linealmente dependientes en H, y no puede haber ninguna cantidad menor de columnas linealmente dependientes porque en ese caso habría palabras no nulas en $\mathcal{C}$ con peso menor a d. Recíprocamente, si hay r columnas linealmente dependientes entonces hay palabras de peso r y la distancia mínima es el menor de esos pesos.

Código de Hadamard

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 23 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = (11 \cdot 2 + 1) \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 11 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = (5 \cdot 2 + 1) \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 5 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = (2 \cdot 2 + 1) \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 2 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = (1 \cdot 2 + 0)2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

Código de Hadamard

El código Hadamard es un $[2^r, r, 2^{r-1}]$-código lineal binario que es capaz de corregir muchos errores. La matriz generadora de un código Hadamard puede ser construida columna por columna: la i^{th} columna son los bits de la representación binaria del número entero i.

$$23 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$

- Ejemplo: el $[8, 3, 4]-$código de Hadamard tiene matriz generadora:

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

Código de Hadamard perforado

Código de Hadamard perforado

El código Hadamard perforado binario es un $[2^{r-1}, r, 2^{r-2}]$-código lineal que se obtiene quitando de la matriz generadora de un código de Hadamard todas las columnas que empiezan con 0.

Código de Hadamard perforado

El código Hadamard perforado binario es un $[2^{r-1}, r, 2^{r-2}]$-código lineal que se obtiene quitando de la matriz generadora de un código de Hadamard todas las columnas que empiezan con 0.

- Ejemplo: $r = 3$:

$$G_{[8,3,4]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \quad G_{[4,3,2]} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

Código de Hadamard perforado

El código Hadamard perforado binario es un $[2^{r-1}, r, 2^{r-2}]$-código lineal que se obtiene quitando de la matriz generadora de un código de Hadamard todas las columnas que empiezan con 0.

- Ejemplo: $r = 3$:

$$G_{[8,3,4]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} \quad \rightarrow \quad G_{[4,3,2]} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$\mathcal{C} = \{(0000), (0101), (0011), (1111), (0110), (1010), (1100), (1001)\}$$

Código de de Reed-Muller

- Para $0 \leq r \leq m$ el código de Reed-Muller denotado $\mathcal{R}(r,m)$ es un $[n,k,d]$-código binario con

$$n = 2^m, \qquad k = \sum_{i=0}^{r} \binom{m}{i}, \qquad d = 2^{m-r}.$$

- $\mathcal{R}(r,m)$ tiene matriz generadora

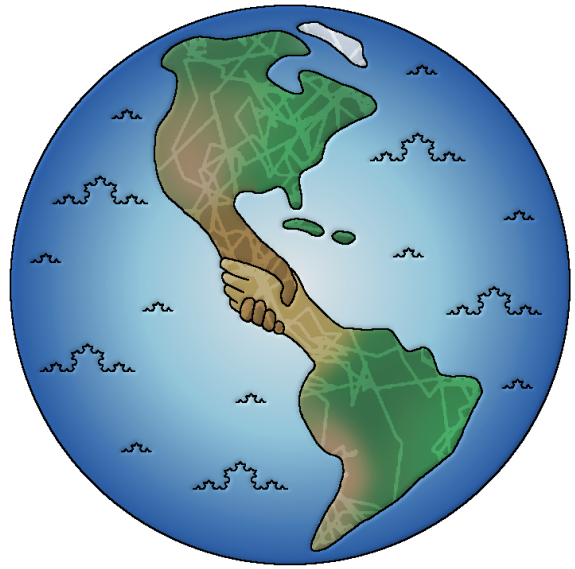
$$G_{r,m} = \begin{pmatrix} G_{r,m-1} & G_{r,m-1} \\ 0 & G_{r-1,m-1} \end{pmatrix} \qquad \text{si } 0 < r < m$$

$$G_{0,m} = \underbrace{(1\ 1\ \cdots 1)}_{m+1} \qquad G_{m,m} = \begin{pmatrix} G_{m-1,m} \\ 0 \cdots 0\ 1 \end{pmatrix}$$

Desafío

Escribir la matriz generadora del $[32, 6, 16]$ – código de Hadamard perforado que usó el Mariner 9.

¿Preguntas?



María Chara
charamaria@gmail.com

Saraí Hernández-Torres
sarai.h@campus.technion.ac.il