Introducción a los códigos correctores de errores

Mathematics sin fronteras

María Chara

Universidad Nacional del Litoral

26 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

Matriz de control y código dual

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ y matriz generadora G:

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

Matriz de control y código dual

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ y matriz generadora G:

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

- 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

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ y matriz generadora G:

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

- 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.

- H permite decidir (o controlar) si una palabra está en $\mathcal{C}$:

$$y \in \mathcal{C} \iff yH^T = 0 \iff S(y) = 0$$

Matriz de control y código dual

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ y matriz generadora G:

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

- 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.

- H permite decidir (o controlar) si una palabra está en $\mathcal{C}$:

$$y \in \mathcal{C} \iff yH^T = 0 \iff S(y) = 0$$

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

Matriz de control y código dual

- Para un $[n, k]-$código $\mathcal{C}$ sobre $\mathbb{F}_q$ y matriz generadora G:

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

- 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.

- H permite decidir (o controlar) si una palabra está en $\mathcal{C}$:

$$y \in \mathcal{C} \iff yH^T = 0 \iff S(y) = 0$$

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

- 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: $x = (110110) \rightarrow y = (110101)$

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 para $i = 0, \ldots, 2^r - 1$.

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 para $i = 0, \ldots, 2^r - 1$.

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

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 para $i = 0, \ldots, 2^r - 1$.

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

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

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

Recuperación de coordenadas

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ g_0 & g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \end{pmatrix}$$

$\vec{x}$ $\quad$ $\vec{c} = \vec{x} \cdot G$ $\quad$ $g_7 = g_1 + g_6$

$000 \rightarrow (00000000)$
$001 \rightarrow (01010101)$
$010 \rightarrow (00110011)$
$100 \rightarrow (00001111)$
$101 \rightarrow (01011010)$
$011 \rightarrow (01100110)$
$110 \rightarrow (00111100)$
$111 \rightarrow (01101001)$

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 de primer orden

Los códigos Reed-Muller se encuentran entre los códigos más antiguos conocidos (1954).

Definición (Recursiva)

Los códigos de Reed-Muller (de primer orden) $\mathcal{R}(1, m)$ son códigos binarios definidos recursivamente para cualquier $m \geq 1$ como:

- $\mathcal{R}(1, 1) = \{00, 01, 10, 11\} = \mathbb{Z}_2^2$;
- para $m \geq 1$,

$$\mathcal{R}(1, m) = \{(u, u), (u, u+\mathbf{1}) : u \in \mathcal{R}(1, m-1) \text{ y } \mathbf{1} = \text{ vector con todos 1}\}$$

Proposición

Para $m \geq 1$ el código de Reed-Muller $\mathcal{R}(1, m)$ es un $[2^m, m+1, 2^{m-1}]$-código binario donde todas las palabras, excepto las palabras con todos 0 y con todos 1, tienen peso 2^{m-1}.

Tenemos que:

- Como la distancia mínima es $d = 2^{m-1}$, el código puede corregir hasta $2^{m-2} - 1$ errores.
- La palabra con todos ceros está en el código y la palabra con todos 1 (de peso 2^m) también.
- Todas las otras palabras tienen la mitad de sus coordenadas 0 y la otra mitad 1.

Corrección de errores

- Convertir todas las palabras código (y las palabras recibidas) en vectores con componentes ± 1 cambiando los 0 por -1.
- Realizar el producto escalar de la palabra recibida con todas las palabras código.
- Corregir la palabra recibida como la palabra código que tenga producto mayor o igual a $2^{m-1} + 2$.

Corrección de errores

$$\mathcal{R}(1,3) = \{(00000000), (00001111), (01010101), (01011010),$$
$$(10101010), (10100101), (11111111), (11110000)$$
$$(00110011), (00111100), (01100110), (01101001)$$
$$(10011001), (10010110), (11001100), (11000011)\}$$

$$d(c_i, c_j) = w(c_i - c_j) = \begin{cases} 0 & \text{si } i = j, \\ 8 & \text{si todas las coordenadas son diferentes,} \\ 4 & \text{en otro caso.} \end{cases}$$

$$c_i \cdot c_j = \begin{cases} 8 & \text{si } i = j, \\ -8 & \text{si todas las coordenadas son diferentes,} \\ 0 & \text{en otro caso.} \end{cases}$$

$$c \quad \rightarrow \quad y = c + e \quad \rightarrow \quad y \cdot c_i = \begin{cases} \geq 6 & \text{si } c_i = c, \\ \leq 2 & \text{en otro caso.} \end{cases}$$

Código 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

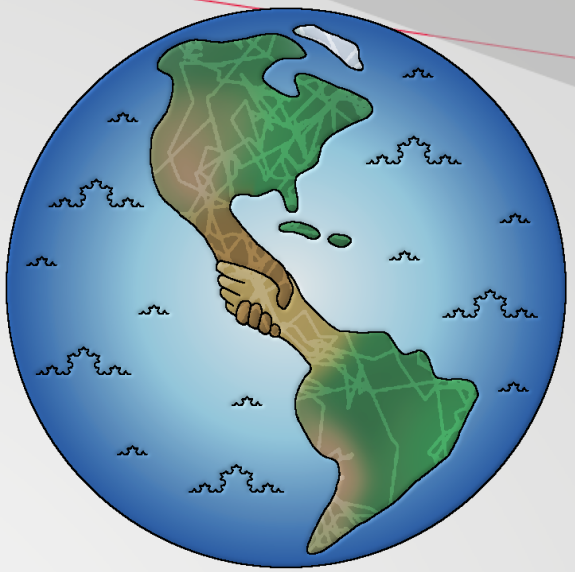
$[32, 6, 16]$ – código

que usó el Mariner 9.

¿Preguntas?

María Chara
charamaria@gmail.com

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



FIQ

UNL . FACULTAD DE
INGENIERÍA QUÍMICA