ejemplo: $C = \{00, 11, 10, 01\}$

$$\left.\begin{array}{l} d(00,11) = 2 \\ d(00,01) = 1 \\ d(10,11) = 1 \end{array}\right\} \min = 1 = S \Rightarrow \begin{array}{l} R = S-1 = 0 \\ Q = \frac{S-1}{2} = \frac{1-1}{2} = 0 \end{array}$$

→ En general si C es un codigo y $rep_r(C) = \{\underbrace{vv \dots v}_{r} : v \in C\}$ entonces es trivial ver que $S(rep_r(C)) = r \cdot S(C)$

→ (Teorema): (Cota de hamming): Sea C un codigo de longitud n, $t = \frac{S-1}{2}$ entonces

$$|C| \leq \frac{2^n}{1 + n + \binom{n}{2} + \dots + \binom{n}{t}}$$

cant de palabras ↑ long ↑

ejemplo: $|C_4| = 4$ $S = 3$ $n = 5$. ¿Existe algun codigo tq $|C| = 4$, $n = 4$, $S = 3$?

Si lo ubiera tendriamos $t = \frac{S-1}{2} = 1$ y $|C| = 4 \leq \frac{2^4}{1+4} = 3 \Rightarrow$ abs $\Rightarrow \nexists$

→ (definicion): Un codigo es perfecto si $|C| = \frac{2^n}{\sum_{r=0}^{t} \binom{n}{r}}$ con $t = \frac{S-1}{2}$

Codigos Lineales

→ (definicion): Un codigo es lineal si es un sub-espacio vectorial de $\{0,1\}^n$

→ (subespacio vectorial): C es subespacio vectorial de $\{0,1\}^n$ si

el cuerpo es $\{0,1\}$

- $x, y \in C \Rightarrow x+y \in C$ Cerrado por suma
- $k \in$ cuerpo, $x \in C \Rightarrow kx \in C$ Cerrado por mult
- $C \neq \emptyset$ No sea vacio.

↳ basta con ver 2 cosas:
- $x, y \in C \Rightarrow x+y \in C$
- $0 \in C$

imp

→ (definicion): El peso de haming es $\|x\| = d_H(x, 0) = \boxed{\#\text{cant de 1s de } x}$

minima cant de 1s

→ (propiedad): C es lineal $\Rightarrow S(C) = \min\{\|x\| : x \neq 0, x \in C\}$

- Todo espacio vectorial tiene dimension k y al menos una base
- Una base cumple → genera el espacio
  → linealmente independiente $c_1\alpha_1 + \dots + c_n\alpha_n = 0 \Rightarrow c_1 = \dots = c_n = 0$

→ (definicion): una matriz generadora de un codigo lineal C es una matriz cuyas filas son base de C. Como las filas son base cualquier matriz generadora debe ser $k \times n$.
→ cant de filas
→ cant de columnas

Obs: Si $k = \dim(C) \Rightarrow C$ es isomorfo a $\{0,1\}^k \Rightarrow |C| = 2^k$.

→ (definicion): Una matriz H es una matriz de chequeo de un codigo C si $C = N(H) = \{y \in \{0,1\}^n : Hy^t = 0\}$

→ (Teorema): Si H es una matriz de chequeo de C, entonces S(C) = min numero de columnas de H linealmente dependientes = min {r : ∃ r columnas L.D. de H}
ej: $H^2 = H^1 + H^3 + H^4 \Rightarrow S = 4$ } cant de terminos

→ (corolario): Si H no tiene columna 0 ni columnas repetidas y $C = N(H)$ entonces $S(C) \geq 3$ y corrige al menos un error. $\frac{3-1}{2} = 1$

Sirve para calcular dim(C) a partir de H, suponiendo que las filas de H no son LI.

→ (Teorema): Si $T: V \to W$ es una transformacion lineal entonces

$$\dim(V) = \dim(N(T)) + \dim(\mathrm{Img}(T))$$

$$T(x) = Hx^t \Rightarrow n = k + \dim(\mathrm{Img}(T))$$

$\boxed{k = n - \#\text{filas}}$ → de H

fallo el razonamiento que llega de CD

→ (propiedad): la matriz de chequeo H va a ser una matriz de $(n-k) \times n$

- Si tengo k filas y n columnas la cantidad de combinaciones posibles sin repetir col es de $2^k - 1$
  para sacar el vector nulo

→ (propiedad): Si H es de la forma $[A \mid I]$ y $C = N(H)$, entonces $G = [I \mid A^t]$ es generadora de C. Viseversa si $G = [I \mid A^t]$ es generadora, $[A \mid I]$ es de chequeo.

ejemplo: $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$ $\left.\begin{matrix} n = 7 \\ k = 7 - 3 = 4 \end{matrix}\right\}$ $2^k = 2^4 = 16 = |C|$

Supongamos que llega mensaje $z = 1001010$

$Hz^t = H \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = H^{(1)} + H^{(4)} + H^{(6)} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$ $\Big\{$ es una col H $= H^{(3)}$

Si no estaba era un error

tengo que sumar a la palabra que me llego e_3 para tener la mas probable. Osea que tengo que cambiar el bit i tq me dio la col H_i

el x mas probable es $x = z + e_3 = 1011010$

→ (definicion): Si H tiene todas las columnas no nulas, el codigo se llama "codigo de hamming".

→ (propiedad): Los codigos de hamming son perfectos.

- Una palabra esta en el codigo si cuando la multiplico por H da 0

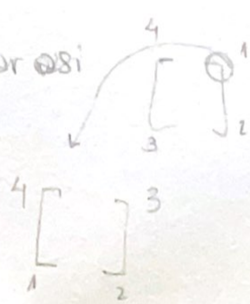
los codigos de hamming son lineales

Codigos ciclicos.

→ cambio de notacion: a la palabra $w_1, \ldots, w_n$ la denotaremos $w_0, \ldots, w_{n-1}$ pues identificaremos la palabra $w = w_0, \ldots, w_{n-1}$ con el polinomio $w(x) = w_0 + w_1 x + \ldots + w_{n-1} x^{n-1}$ en $\mathbb{Z}_2[x]$. No confundir con funciones, $1+x \neq 1+x^2$ como pol., pero como funciones como estamos en $\mathbb{Z}_2[x]$ son iguales.

- Queremos multiplicar palabras de longitud n, podriamos multiplicar los polinomios asociados, pero queremos que el resultado tenga grado $< n$. Lo que se hace es tomar la multiplicacion modulo algun polinomio de grado n. Tomaremos el pol. $1+x^n$.

para transponer basta con hacer así



→ (definicion): $v(x) \odot w(x) = v(x) \cdot w(x) \bmod (1+x^n)$

ej: $(1011) \odot (0110) = (1+x^2+x^3) \cdot (x+x^2) \bmod 1+x^4 = x^2+x^3 = 0011$

obs: $(1+x^n) \bmod (1+x^n) = 0$
$x^n \bmod (1+x^n) = 1$

→ (definicion): $rot(w) = rot(w_0, \ldots, w_{n-1}) = w_{n-1}, w_0, \ldots, w_{n-2}$

→ (propiedad) "Obvia": $rot(w) = x \odot w(x)$

→ (definicion): Un codigo C es ciclico si es lineal e invariante por rotaciones:

$rot(w) \in C : \forall w \in C$ lo roto y vuelve a caer en C.

→ (propiedad): Si C es ciclico entonces existe un unico polinomio no nulo en C de grado minimo. (que tenga la menor cantidad de $1s \neq y$)

→ (definicion): al unico pol. no nulo de grado minimo de un codigo ciclico C, se lo llama polinomio generador y se denota $g(x)$.

→ (corolario de "prop obvia"): Sea C ciclico, $w(x)$ cualquier palabra en C y $v(x)$ cualquier polinomio de cualquier grado. Entonces $w(x) \odot v(x) \in C$ [illegible]
Trae palabras de cualquier longitud a la longitud de C.

→ (Teorema Fundamental de codigos ciclicos): Sea C un codigo ciclico de longitud n, con generador $g(x)$. Entonces:

(1) $C = \{ p(x) \in \mathbb{Z}_2[x] : gr(p(x)) < n \wedge g(x) \mid p(x) \}$

(2) $C = \{ v(x) \odot g(x) : v \in \mathbb{Z}_2[x] \}$

(3) Si $k = \dim(C) \Rightarrow gr(g(x)) = n-k \longrightarrow \boxed{k = n - gr(g(x))}$

(4) $g(x) \mid (1+x^n)$

(5) Si $g(x) = g_0 + g_1 x + \ldots + g_{n-1} x^{n-1} \Rightarrow g_0 = 1$

Metodo 1 de codificacion (ciclicos)

ejemplo metodo 1:

$g(x) = 1 + x^2 + x^3$ ($n = 7$ → longitud)

$k = \dim(C) = 7 - gr(g(x)) = 7 - 3 = 4$ (dimension)

$|C| = 2^4 = 16$ (cant de palabras)

Si quiero codificar $\{0,1\}^4 \longrightarrow \{0,1\}^7$
basta hacer ⟶ $g(x) \longrightarrow (g(x) \cdot q(x))$

codificar 1001

$1001 = (1 + x^3) \cdot (1 + x^2 + x^3)$
$= 1 + x^2 + x^3 + x^3 + x^5 + x^6$
$= 1 + x^2 + x^5 + x^6$
$= (1010011)$

(ciclicos)

→ (Idea metodo 2 codificacion): $\forall p$. $[(p \bmod g) + p]$ es multiplo de g
pues

$$((p \bmod g) + p) \bmod g = p \bmod g + p \bmod g = 0$$

Usaremos este truco pero con cuidado pues $\{0,1\}^k \longrightarrow \{0,1\}^n$
porque esta funcion no es inyectiva $\quad q \longrightarrow q \cdot (q \bmod g)$ no funciona

ej: $1 \to 1+1 = 0$
$0 \to 0$

lo que se tiene que hacer es: $q \longrightarrow (x^{n-k} q \bmod g) + x^{n-k} q$ (*)

ej: $g(x) = 1 + x^2 + x^3 \quad n = 7 \quad q(x) = 1100 = 1 + x \quad k = 4$

$x^{n-k} \cdot q(x) = x^3 + x^4 \longrightarrow x^3 + x^4 \bmod g = 1 + x^2 + 1 + x + x^2 = x$

$g \bmod g = 0$
$(1 + x^2 + x^3) \bmod g = 0$
$(1 + x^2) \bmod g + x^3 \bmod g = 0$
$\quad \overset{\shortparallel}{1 + x^2}$
$\Rightarrow x^3 \bmod g = 1 + x^2$

$x^4 \bmod g$
$x \cdot x^3 \bmod g$
$x \cdot (1 + x^2) \bmod g$
$(x + x^3) \bmod g$
$1 + x + x^2$

usando (*)
$(x^3 + x^4) \bmod g + x^3 + x^4 = x + x^3 + x^4$
$= 010\underbrace{1100}_{q}$

Ahora nos construyamos la matriz generadora

$100 — 0 \longrightarrow 1 \longrightarrow (x^{n-k} \bmod g) + x^{n-k} \longrightarrow$
$010 — 0 \longrightarrow x \longrightarrow (x^{n-k+1} \bmod g) + x^{n-k+1} \longrightarrow$

$$\begin{bmatrix} x^3 \bmod g + x^3 \\ x^4 \bmod g + x^4 \\ \\ \end{bmatrix} \xrightarrow{\text{traspuesta}} G = \begin{bmatrix} \\ \\ \end{bmatrix}$$

matriz generadora met 1

multiplicar una base de $\{0,1\}^k$ por $g(x)$

ej: $k = 4 \Rightarrow \{0,1\}^4$

$1000 \longrightarrow 1 \cdot g = g$
$0100 \longrightarrow x \cdot g = gx$
$0010 \longrightarrow x^2 \cdot g = gx^2$
$0001 \longrightarrow x^3 \cdot g = gx^3$

$$G = \begin{bmatrix} g \\ gx \\ gx^2 \\ gx^3 \end{bmatrix}$$

→ (polinomio chequeador): $g \mid 1+x^n \Rightarrow \exists\, h(x) : 1+x^n = g(x)\cdot h(x)$

$h(x) = \dfrac{1+x^n}{g(x)}$ Supongamos que $p \in C \Rightarrow p = qg$ para algun q del grado apropiado.

$ph = qgh = q(1+x^n) \Rightarrow ph \bmod (1+x^n) = 0$ es decir $p(x) \odot h(x) = 0$

Si cumple → la palabra esta en el codigo.

matriz de chequeo: $G = [A \mid Id] \Rightarrow H = [Id \mid A^t]$

$\boxed{x^n \bmod g = 1 \Rightarrow g \mid x^n + 1 \text{ imp}}$

Error de trapping

• Supongamos que C es ciclico de longitud n con pol generador $g(x)$ y corrige t errores. Supongamos que mandamos $v \in C$ y llega $w = v+e$ con $\|e\| \leq t$

Si tomamos mod g: $(w \bmod g) = (v+e) \bmod g = \underbrace{v \bmod g}_{=0 \text{ pues } v \in C} + e \bmod g = e \bmod g$

Pero esto mismo vale para las rotaciones

• $\mathrm{rot}^i(w) = \mathrm{rot}^i(v) + \mathrm{rot}^i(e)$ ~~$\mathrm{rot}^i(w) \bmod g$~~ $\mathrm{rot}^i(e) = \|e\| = t$

• $\mathrm{rot}^i(w) \bmod g = \underbrace{\mathrm{rot}^i(v) \bmod g}_{=0} + \mathrm{rot}^i(e) \bmod g = \mathrm{rot}^i(e) \bmod g$

Si para algun i $\; gr(\mathrm{rot}^i(e)) < gr(g(x)) \Rightarrow \mathrm{rot}^i(e) \bmod g = \mathrm{rot}^i(e)$, equiv. es decir que todos los "1" del error estan en una ventana de longitud $n-k = gr(g(x))$. Si pasa eso: $\mathrm{rot}^i(w) \bmod g = \mathrm{rot}^i(e) \Rightarrow e = \mathrm{rot}^{-i}(\mathrm{rot}^i(w) \bmod g)$

En terminos de polinomios, el algoritmo queda:

$S_0 = w \bmod g$ Sindrome → palabra que llega

$S_i = (x \cdot S_{i-1} \bmod g) \quad i \geq 1$

hasta que $\|S_i\| \leq t \rightarrow$ error $= x^{n-i} S_i \bmod (1+x^n)$

luego la palabra mas probable es $w(x)' = w(x) + \text{error}$

falta ejemplo

Como ver que $g \mid (1+x^n)$. $\quad (1+x^n) \bmod g = 0$

tiene que cumplir → $\boxed{x^n \bmod g = 1}$