Codigo de correxion de errores

→ (definicion): Un codigo de bloque binario es un subconjunto de $\{0,1\}^n$ para algun n fijo. ↳ misma longitud

Una suposicion es que el medio de transmicion puede cambiar bits pero no puede eliminarlos o añadirlos. Tambien suponemos que la probabilidad de cambiar de 0 a 1 es la misma de cambiar de 1 a 0, y es para todos los bits independientemente. Si esta probabilidad es p, suponemos $0 < p < \frac{1}{2}$. La prob. de t errores es p^t.

→ (definicion): la distancia de hamming entre 2 palabras $x, y \in \{0,1\}^n$ es el numero de bits de diferencia entre x e y.

→ (propiedad): d_H es una distancia, es decir:

A) $d_H(x,y) = d_H(y,x)$

B) $d_H(x,y) \geq 0$

C) $d_H(x,y) = 0 \iff x = y$

D) $d_H(x,y) \leq d_H(x,z) + d_H(z,y)$ Desigualdad triangular.

→ (definicion): Sea $S = S(C) = \min\{d_H(x,y) : x,y \in C \mid x \neq y\}$ minima distancia entre 2 palabras de C

→ (definicion): Un codigo C "detecta" r errores si $D_r(x) \cap C = \{x\}\ \forall x \in C$ donde $D_r(x) = \{y : d_H(x,y) \leq r\}$

C corrige t errores si $D_t(x) \cap D_t(y) = \emptyset\ \forall x,y \in C \mid x \neq y$

→ (Teorema): Sea C un codigo tal que R es la mayor capacidad de detectar errores de C, es decir, C detecta R errores pero no R+1. Y a la mayor capacidad de correcciones, es decir, C corrige Q errores pero no comige Q+1. Entonces $R = S - 1$ y $Q = \frac{S-1}{2}$

(R = detecta, Q = comige)

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

$d(00,11) = 2$
$d(00,01) = 1$
$d(10,11) = 1$

$\min = 1 = S \Longrightarrow R = S-1 = 0$ cubre

$Q = \frac{S-1}{2} = \frac{1-1}{2} = 0$ corrige

→ En general si C es un codigo y $rep_r(C) = \{\underbrace{vv\ldots v}_{r} : v \in C\}$ 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 $|C| \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{t}}$

(cant de palabras ↑, long ↑)

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

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

→ (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 $\{0,1\}$

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

↳ basta con ver 2 cosas: $\left.\begin{array}{l} \cdot\ x, y \in C \Longrightarrow x+y \in C \\ \cdot\ 0 \in C \end{array}\right\}$ imp

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

mínima cant de 1's

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

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

→ (definición): una matriz generadora de un código lineal C es una matriz cuyas filas son base de C. Como las filas son base cualquier matriz generadora debe ser $k \times n$.
(k: cant de filas; n: cant de columnas)
Obs: Si $k = \dim(C) \Rightarrow C$ es isomorfo a $\{0,1\}^k \Rightarrow |C| = 2^k$.

→ (definición): Una matriz H es una matriz de chequeo de un código 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 número de columnas de H linealmente dependientes = min $\{r : \exists$ r columnas L.D. de H$\}$
ej: $H^2 = H^1 + H^3 + H^4 \Rightarrow S = 4$ (cant de términos)

→ (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 transformación lineal entonces

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

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

$k = n - \#\text{filas}$ (de H)

falta el razonamiento que llega acá

→ (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 $[A|I]$ y $C = N(H)$, entonces $G = [I|A^t]$ es generadora de C. Viceversa si $G = [I|A^t]$ es generadora, $[A|I]$ es de chequeo.

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

Supongamos que llega mensaje $z = 1001010$

$Hz^t = H\begin{bmatrix} 1\\0\\0\\1\\0\\1\\0 \end{bmatrix} = H^{(1)} + H^{(4)} + H^{(6)} = \begin{bmatrix}1\\0\\0\end{bmatrix} + \begin{bmatrix}1\\1\\0\end{bmatrix} + \begin{bmatrix}0\\1\\1\end{bmatrix} = \begin{bmatrix}0\\0\\1\end{bmatrix}$ es una col H = He_3

Si no estaba el 3 en error

tengo que sumar a la palabra que me llego e3 para tener la mas probable. O sea que tengo q el cambiar el bit 3 y me da la col H3

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

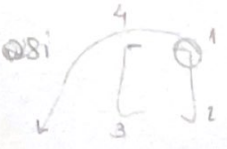
los codigos de hamming son lineales

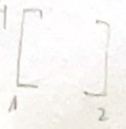
Codigos ciclicos.

→ cambio de notacion: a la palabra $w_1, \dots, w_n$ la denotaremos $w_0, \dots, w_{n-1}$ pues identificaremos la palabra $w = w_0, \dots, w_{n-1}$ con el polinomio $w(x) = w_0 + w_1 x + \dots + w_{n-1} x^{n-1}$ 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 asi





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

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

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

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

→ (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 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 $w(x) \odot v(x) \in C$
Trae palabras de cualquier longitud a la longitud de C.

(contiene todos los polinomios)

→ (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 $g(x) = g_0 + g_1 x + \dots + g_{n-1} x^{n-1} \Rightarrow g_0 = 1$

Metodo 1 de codificacion

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 $\longrightarrow$ $q(x) \longrightarrow (q(x) \cdot g(x))$

codificar 1001

$1001 = (1 + x^3) \cdot (1 + x^2 + x^3)$
$= 1 + x^2 + x^3 + x^3 + x^5 + x^6$
$= 1 + x^2 + x^5 + x^6$
$= (1\,0\,1\,0\,0\,1\,1)$ //

(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 ej: $q \longrightarrow q \cdot (q \bmod g)$ no funciona

$1 \to 1+1=0$
$0 \to 0$

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

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

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

$g \bmod g = 0$

$(1 + x^2 + x^3) \bmod g = 0$

$(1 + x^2) \bmod g + x^3 \bmod g = 0$

$1 + x^2$

$\Rightarrow x^3 \bmod g = 1 + x^2$

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

usando (*)

$(x^3 + x^4) \bmod g + x^3 + x^4 = x + x^3 + x^4$
$= 0\,1\,0\,1\,1\,0\,0$
q

Ahora nos construyamos la matriz generadora

$100 \longrightarrow 0 \to 1 \longrightarrow (x^{n-k} \bmod g) + x^{n-k} \longrightarrow x^3 \bmod g + x^3$

$010 \longrightarrow 0 \to x \longrightarrow (x^{n-k+1} \bmod g) + x^{n-k+1} \longrightarrow x^4 \bmod g + x^4$ → traspuesta

$G = \begin{bmatrix} & & & \\ & & & \\ & & & \\ & & & \end{bmatrix}$

---

matriz generadora

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

- $h(x) = \frac{1+x^n}{g(x)}$ Suponpamos que $p \in C \Rightarrow p = q \cdot g$ 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: $G = [A \mid Id] \Rightarrow H = [Id \mid A^t]$

$x^n \bmod g = 1 \Rightarrow g \mid x^n + 1$ ¿imp?

Error de Trapping

• Suponpamos que C es ciclico de lonpitud n con pol generador $g(x)$ y conge 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

- $rot^i(w) = rot^i(v) + rot^i(e)$ ~~$rot^i(w) \bmod g$~~ $rot^i(e) = \|e\| = t$
- $rot^i(w) \bmod g = \underbrace{rot^i(v) \bmod g}_{=0} + rot^i(e) \bmod g = rot^i(e) \bmod g$

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

En terminos de polinomios, el algoritmo queda:

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

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

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 $g \mid (1+x^n)$, tiene que cumplir ⟶ $(1+x^n) \bmod g = 0$

$x^n \bmod g = 1$