Definiciones

viernes, 27 de mayo de 2022 17:08

Rotaciones:

Sea:

$w \in \{0,1\}^n$

$w = w_0 w_1 \dots w_{n-1}$

$\mathrm{rot} : \{0,1\}^n \to \{0,1\}^n$

$\mathrm{rot}(w) = w_{n-1} w_0 w_1 \dots w_{n-2}$

$\mathrm{rot}^0(w) = w$

$\mathrm{rot}^{i+1}(w) = \mathrm{rot}\left(\mathrm{rot}^i(w)\right)$

Códigos cíclicos:

Sea:

$C \subseteq \{0,1\}^n$

$$C \text{ es un código cíclico} \Leftrightarrow C \text{ es un código lineal} \wedge \forall w \in C : \mathrm{rot}(w) \in C$$

Multiplicación de palabras:

Sea:

$w \in \{0,1\}^n$

Se define el polinomio de w:

$$w(x) = \sum_{i=0}^{n-1} w_i x^i$$

Sean:

$v, w \in \{0,1\}^n$

$v \odot w = v(x)w(x) \bmod (1 + x^n)$

Grado:
Sea
$w \in \{0,1\}^n$

$$\mathrm{gr}(w) = \max\{i \in \{0,1,\dots,n-1\} : w_i = 1\}$$
$$\mathrm{grmin}(w) = \min\{i \in \{0,1,\dots,n-1\} : w_i = 1\}$$

Polinomio generador:
Sea:
C un código lineal
$g \in C$

$$g \text{ es polinomio generador de } C$$
$$\Leftrightarrow g \neq 0 \wedge \nexists p \in C - \{0\} : \mathrm{gr}(p) < \mathrm{gr}(g)$$

Polinomio chequeador:
Sea:
C un código lineal
g un polinomio generador de C

$$\frac{1 + x^n}{g(x)} \text{ es el polinomio de chequeo de } C$$

Teoremas

viernes, 27 de mayo de 2022 17:20

rot es lineal:

rot es una transformación lineal lineal

Propiedades de la multiplicación de palabras:

Sea:

$v \in \{0,1\}^n$

C un código ciclico de logitud n

$w \in C$

$$\mathrm{rot}(w) = e_1 \odot w \qquad (e_1 = 0100 \cdots \text{(base canoncia)})$$

$$\mathrm{rot}^i(w) = e_i \odot w$$

$$v \odot w \in C$$

Propiedades del polinomio generador para códigos lineales:

Sea:

C un código lineal

El polinomio generador es único

Propiedades del polinomio generador para códigos cíclicos:

Sea:

C un código cíclico de longitud n

g el polinomio generador de C

$$C = \{p : \mathrm{gr}(p) < n \wedge g(x) | p(x)\}$$

$$C = \{v \odot g : v \in \{0,1\}^*\}$$

$$\mathrm{gr}(g) = n - \dim(C)$$
$$g(x) | (1 + x^n)$$
$$g_0 = 1$$

Matrices generadoras de un código ciclico:

Sea:

C un código cíclico de longitud n

$k = \dim(C)$

g el polinomio generador de C

$G, G' \in \{0,1\}^{k \times n}$

$$G = \begin{bmatrix} g \\ \mathrm{rot}(g) \\ \vdots \\ \mathrm{rot}^{k-1}(g) \end{bmatrix}$$

$$G' = \begin{bmatrix} \left(x^{n-k} \bmod g(x)\right) + x^{n-k} \\ \left(x^{n-k+1} \bmod g(x)\right) + x^{n-k+1} \\ \vdots \\ x\left(^{n-1} \bmod g(x)\right) + x^{n-1} \end{bmatrix}$$

G y G' generan a C (métodos 1 y 2 respectivamente)

Polinomio chequeador:

Sea:

C un código lineal de logitud n

h un polinomio de chequeo de C

$w \in \{0,1\}^n$

$$w \in C \Leftrightarrow h \odot w = 0$$

Codificación:
Sea:
C un código cilcio de logitud n
$k = \dim(C)$
g un polinomio generador de C

$u \in \{0,1\}^k$ una palabra a codificar

Las formas de codificar son:

$$g \odot u$$
$$\left(u(x)x^{n-k} \bmod g(x)\right) + u(x)x^{n-k}$$

Y se corresponden a cada una de los tipos de matriz generadora

Decodificación: 🛠️
Sea:
C un código cilcio de logitud n
$k = \dim(C)$
t la cantidad de errores que corrige C
g un polinomio generador de C
$v \in \{0,1\}^k$
$e \in \{0,1\}^n$ con $|e| \leq t$
$w = g \odot v + e$
(w es la palabra a decodificar)

$S_i(x) = x^{n-1}w(x) \bmod g(x)$

$$\forall i : |S_i| \leq t : \; e(x) = x^{n-j}S_i(x) \bmod (x^n + 1)$$

Demostraciones

viernes, 27 de mayo de 2022 19:06

rot es lineal:

rot es una transformación lineal lineal

Demostración:

rot es una transformación lineal lineal

$\Leftrightarrow$

$\forall \alpha, \beta \in \{0,1\}^n : \mathrm{rot}(\alpha + \beta) = \mathrm{rot}(\alpha) + \mathrm{rot}(\beta)$

Trabajo sin el $\forall$:

$\mathrm{rot}(\alpha + \beta)$

$=$

$\mathrm{rot}\big((\alpha_0 + \beta_0)(\alpha_1 + \beta_1) \cdots (\alpha_{n-1} + \beta_{n-1})\big)$

$=$

$(\alpha_{n-1} + \beta_{n-1})(\alpha_0 + \beta_0)(\alpha_1 + \beta_1) \cdots (\alpha_{n-2} + \beta_{n-2})$

$=$

$(\alpha_{n-1}\alpha_0\alpha_1 \cdots \alpha_{n-2}) + (\beta_{n-1}\beta_0\beta_1 \cdots \beta_{n-2})$

$=$

$\mathrm{rot}(\alpha) + \mathrm{rot}(\beta)$

Propiedades de la multiplicación de palabras:

Sea:

$w \in \{0,1\}^n$

$\mathrm{rot}^i(w) = e_i \odot w$

Demostración por inducción en i:

Caso base:

$\mathrm{rot}(w) = e_1 \odot w$

$\Leftrightarrow$

$$w_{n-1}x^0 + \sum_{i=0}^{n-2} w_i x^{i+1} = e_1(x) \cdot w(x) \bmod (1 + x^n)$$

Demuestro esto:

$e_1(x) \cdot w(x) \bmod (1 + x^n)$

$=$

$x \cdot w(x) \bmod (1 + x^n)$

$$=$$

$$x \cdot \sum_{i=0}^{n-1} w_i x^i \mod (1 + x^n)$$

$$=$$

$$x \cdot \sum_{i=0}^{n-1} w_i x^i \mod (1 + x^n)$$

$$=$$

$$\sum_{i=0}^{n-1} w_i x^{i+1} \mod (1 + x^n)$$

$$=$$

$$\sum_{i=0}^{n-2} w_i x^{i+1} + w_{n-1} x^n \mod (1 + x^n)$$

$$=$$

$$\left(\sum_{i=0}^{n-2} w_i x^{i+1} \mod (1 + x^n)\right) + \left(w_{n-1} x^n \mod (1 + x^n)\right)$$

$$= \{\left(\textstyle\sum_{i=0}^{n-2} w_i x^{i+1} \mod (1 + x^n)\right) = \textstyle\sum_{i=0}^{n-2} w_i x^{i+1}\}$$

$$\sum_{i=0}^{n-2} w_i x^{i+1} + \left(w_{n-1} x^n \mod (1 + x^n)\right)$$

$$= \{w_{n-1} x^n \mod (1 + x^n) = w_{n-1}\}$$

$$\sum_{i=0}^{n-2} w_i x^{i+1} + w_{n-1}$$

$$=$$

$$w_{n-1} x^0 + \sum_{i=0}^{n-2} w_i x^{i+1}$$

Caso inductivo para $i + 1$ suponiendo que vale para i:

$$\mathrm{rot}^{i+1}(w)$$

$$=$$

$$\mathrm{rot}\left(\mathrm{rot}^i(w)\right)$$

$$= \{\text{Caso base}\}$$

$$e_1 \odot \mathrm{rot}^i(w)$$

$$= \{\text{Caso inductivo}\}$$

$$e_1 \odot e_i \odot w$$

$$= \{e_1 \odot e_i = e_{i+1}\}$$

$$e_{i+1} \odot w$$

Sea:
$v \in \{0,1\}^n$
C un código ciclico de logitud n
$w \in C$

$$v \odot w \in C$$

Demostración:

$$v \odot w \in C$$
$\Leftrightarrow \{v_i$ es un número, e_i un vector$\}$
$$\left(\sum_{i=0}^{n-1} v_i e_i\right) \odot w \in C$$
$\Leftrightarrow$
$$\sum_{i=0}^{n-1} v_i (e_i \odot w) \in C$$
$\Leftarrow \{C$ es lineal, por lo tanto, si los elementos están, la combinación lineal está$\}$
$$\forall i \in \{0,1,\dots,n-1\} : \ e_i \odot w \in C$$
$\Leftrightarrow$
$$\forall i \in \{0,1,\dots,n-1\} : \mathrm{rot}^i(w) \in C$$
$\Leftrightarrow \{C$ es cilico, $w \in C\}$
True

Propiedades del polinomio generador para códigos lineales:
Sea:
C un código lineal

El polinomio generador es único

Demostración, mostrando que si hay dos son iguales:
Sean g, q polinomios generadores de C distintos

Pruebo que su suma es 0, lo cuál significa que son iguales

$$g + q$$
$= \{g$ y q son polinomios generadores de $C \Rightarrow \mathrm{gr}(g) = \mathrm{gr}(q)$
Sea $t = \mathrm{gr}(g)$
$\}$
$$g(x) + x^t - x^t + q(x) + x^t - x^t$$
$=$

$g(x) - x^t + q(x) - x^t + x^t + x^t$
$= \{x^t + x^t = 0\}$
$g(x) - x^t + q(x) - x^t$
$= \{\mathrm{gr}(g(x) - x^t) < t, \mathrm{gr}(q(x) - x^t) < t$
$\Rightarrow \mathrm{gr}(g(x) - x^t + q(x) - x^t) < t$
$\Rightarrow g(x) - x^t + q(x) - x^t = 0$ (Ya que t es el grado mínimo de C, y $g + q \in C$)
$\}$
0

Propiedades del polinomio generador para códigos cíclicos: 🛠️
Sea:
C un código cíclico de longitud n
g el polinomio generador de C

Ⓐ $C = \{p : \mathrm{gr}(p) < n \wedge g(x)|p(x)\}$
Ⓑ $C = \{v \odot g : v \in \{0,1\}^*\}$

Ⓒ $\mathrm{gr}(g) = n - \dim(C)$
Ⓓ $g(x)|(1 + x^n)$
Ⓔ $g_0 = 1$

Demostraciones:

Ⓐ y Ⓑ
Sea:
$C_1 = \{p : \mathrm{gr}(p) < n \wedge g(x)|p(x)\}$
$C_2 = \{v \odot g : v \in \{0,1\}^*\}$

Pruebo $C \subseteq C_1 \subseteq C_2 \subseteq C$

$C \subseteq C_1$:
Sea $p \in C$, pruebo que satisface la condición de C_1

$\mathrm{gr}(p) < n$ es si o si cierto porque $C \subseteq \{0,1\}^n$

$g(x)|p(x)$:

Para probar esto, pruebo que el resto en la división es 0:
Sean q el resultado y r el resto de dividir p en g:

O sea:
$p(x) = q(x) * g(x) + r(x)$
$\Leftrightarrow$

$$r(x) = p(x) + q(x) * g(x)$$

$\Rightarrow$ {Por ser r el resto de dividir en g: $\mathrm{gr}(r) < \mathrm{gr}(g) \Rightarrow \mathrm{gr}(r) < n$}

$$r(x) = (p(x) + q(x) * g(x)) \bmod (1 + x^n)$$

$\Leftrightarrow$

$$r(x) = p(x) \bmod (1 + x^n) + q(x) * g(x) \bmod (1 + x^n)$$

$\Leftrightarrow$ {$\mathrm{gr}(p) < n$, definición $\odot$}

$$r(x) = p(x) + q(x) \odot g(x)$$

$\Rightarrow$ {$p \in C, q \odot g \in C$}

$$r \in C$$

$\Rightarrow$ {g es el no nulo de menor grado}

$$r = 0$$

$C_1 \subseteq C_2$

Sea $p \in C_1$

Pruebo $p \in C_2$ encontrando v tal que $p = v \odot g$

Sea $v(x) = \frac{p(x)}{g(x)}$ (existe porque $g(x)|p(x)$)

$$p = v \odot g$$

$\Leftrightarrow$

$$p(x) = v(x) * g(x) \bmod (1 + x^n)$$

$\Leftrightarrow$

$$p(x) = \frac{p(x)}{g(x)} * g(x) \bmod (1 + x^n)$$

$\Leftrightarrow$

$$p(x) = p(x) \bmod (1 + x^n)$$

$\Leftrightarrow$ {$p \in C_1 \Rightarrow \mathrm{gr}(p) < n$}

True

$C_2 \subseteq C$

Sea $v \odot g \in C_2$, pruebo que está en C

$$v \odot g$$

$=$

$$v(x) * g(x) \bmod (1 + x^n)$$

$=$ {Re-escribo el producto por v}

$$\left(\sum_{i=0}^{\mathrm{gr}(v)} v_i x^i g(x)\right) \bmod (1 + x^n)$$

$=$ {$x^i * p(x) = \mathrm{rot}^i(p(x))$}

$$\left(\sum_{i=0}^{\mathrm{gr}(v)} v_i \mathrm{rot}^i(g(x))\right) \bmod (1 + x^n)$$

$=$ {Por ser rotación de n, el grado de eso es menor que n}

$$\sum_{i=0}^{\mathrm{gr}(v)} v_i \mathrm{rot}^i_g((x))$$

$\in$ {Por ser C cilico, la convinación lineal de rotaciones de un elemento está}

$$C$$

© $\mathrm{gr}(g) = n - \dim(C)$

$$\mathrm{gr}(g) = n - \dim(C)$$

$\Leftrightarrow$

$$\dim(C) = n - \mathrm{gr}(g)$$

$\Leftarrow$

$$\exists \mathcal{B} \subseteq C : \mathcal{B} \text{ genera a } C : \#\mathcal{B} = n - \mathrm{gr}(g)$$

Doy un conjunto que satisface esto:

$\mathcal{B} = \left\{\mathrm{rot}^i(g) : i \in \{0, \dots, n - \mathrm{gr}(g) - 1\}\right\}$

$\mathcal{B} \subseteq C$ porque C es cliclo (y por ende tiene las rotaciones de cualquier elemento)

$\mathcal{B}$ es LI ya que cada elemento tiene un grado mas que el anterior (llengando hasta grado $n - 1$)

Por eso mismo, todos los $\mathrm{rot}^i(g)$ son distintos, y por ende $\#\mathcal{B} = n - \mathrm{gr}(g)$

Pruebo ahora que $\mathcal{B}$ genera a C

Sea $p \in C$:

$$p(x)$$

$= \{Ⓐ \Rightarrow g(x)|p(x), \text{ sea } q(x) = \frac{p(x)}{g(x)}\}$

$$q(x)g(x)$$

$= \{$Re-escribo el producto de polinomios, ① $\Rightarrow \mathrm{gr}(p) < n \Rightarrow \mathrm{gr}(q) < n - \mathrm{gr}(g)\}$

$$\sum_{i=0}^{n-\mathrm{gr}(g)-1} q_i x^i g(x)$$

$= \{$Multiplicar por x^i es como rotar i veces$\}$

$$\sum_{i=0}^{n-\mathrm{gr}(g)-1} q_i \mathrm{rot}^i_g((x))$$

Esto es una combinación lineal de elementos de $\mathcal{B}$, por ende $\mathcal{B}$ genera a C

Ⓓ $g(x)|(1 + x^n)$

Sea q el resultado y r el resto de dividir $(1 + x^n)$ en $g(x)$

Pruebo que $r = 0$

$$1 + x^n = g(x)q(x) + r(x)$$
$\Leftrightarrow$
$$r(x) = g(x)q(x) + 1 + x^n$$
$\Rightarrow$
$$r(x) \bmod (1 - x^n) = (g(x)q(x) + 1 + x^n) \bmod (1 - x^n)$$
$\Leftrightarrow \{\mathrm{gr}(r) < \mathrm{gr}(g) \leq n\}$
$$r(x) = g(x)q(x) \bmod (1 - x^n)$$
$\Leftrightarrow$ {Definición $\odot$}
$$r(x) = g(x) \odot q(x)$$
$\Leftrightarrow$
$$r = q \odot g$$
$\Rightarrow$ {Ⓑ}
$$r \in C$$
$\Rightarrow \{\mathrm{gr}(r) < \mathrm{gr}(g)$ y g es el no nulo de menor grado$\}$
$$r = 0$$

Ⓔ $g_0 = 1$

Demostración por contradición: (o sea, supongo $g_0 = 0$)

Sea:
$g' = \mathrm{rot}^{n-1}(g)$

① $g' \in C$
Ya que al ser C cilico, todas las rotciones de un elemento están

② $\mathrm{gr}(g') = \mathrm{gr}(g) - 1$
Ya que rotar $n - 1$ veces hacia la derecha es como rotar 1 vez hacia la izquierda y al ser $g_0 = 0$, no pasa nada a g'_{n-1}

③ $g' \neq 0$
Ya que $g \neq 0$ por ser g generador

Esto contradice que g sea el no nulo de grado mínimo

Queda probado $g_0 = 1$

Decodificación: 🛠️
Sea:
C un código cilcio de logitud n
$k = \dim(C)$
t la cantidad de errores que corrige C
g un polinomio generador de C
$v \in \{0,1\}^k$

$e \in \{0,1\}^n$ con $|e| \leq t$
$w = g \odot v + e$
(w es la palabra a decodificar y e es el error)

$S_i(x) = x^i w(x) \bmod g(x)$

$j = \min_{i\,:\,|S_i| \leq t} i$

$$e(x) = x^{n-j} S_j(x) \bmod (x^n + 1)$$

Demostración:
Llamemos $\tilde{e}(x) = x^{n-j} S_j(x) \bmod (x^n + 1)$

$$\tilde{e}(x) \equiv x^{n-j} S_j(x) \mod (x^n + 1)$$
$\Rightarrow \{g(x) | (x^n + 1)\}$
$$\tilde{e}(x) \equiv x^{n-j} S_j(x) \mod g(x)$$
$\Leftrightarrow$
$$\tilde{e}(x) \equiv x^{n-j} \left(x^j w(x) \bmod g(x)\right) \bmod g(x)$$
$\Leftrightarrow$
$$\tilde{e}(x) \equiv x^{n-j} x^j w(x) \mod g(x)$$
$\Leftrightarrow$
$$\tilde{e}(x) \equiv x^n w(x) \mod g(x)$$
$\Leftrightarrow \{x^n \equiv 1 \text{ mop } g\}$
$$\tilde{e}(x) \equiv w(x) \mod g(x)$$
$\Leftrightarrow \{e \equiv w \mod g\}$
$$\tilde{e}(x) \equiv e(x) \mod g(x)$$
$\Rightarrow \{$Sean $u(x)$ y $k(x)$ tal que $e(x) = u(x)g(x) + k(x)\}$
$$\tilde{e}(x) = u(x)g(x) + k(x)$$

Parto de lo que quiero probar:
$$e(x) = x^{n-j} S_j(x) \bmod (x^n + 1)$$
$\Leftrightarrow$
$$e(x) = x^{n-j} \left(x^j w(x) \bmod g(x)\right) \bmod (x^n + 1)$$
$\Leftrightarrow$
$$e(x) = x^{n-j} \left(x^j \left(g(x)v(x) + e(x)\right) \bmod g(x)\right) \bmod (x^n + 1)$$
$\Leftrightarrow$
$$e(x) = x^{n-j} \left(x^j e(x) \bmod g(x)\right) \bmod (x^n + 1)$$
$\Leftrightarrow$
$$x^j e(x) \bmod (x^n + 1) = x^j e(x) \bmod g(x)$$

$$w(x) = g(x)v(x) + e(x)$$

$\Leftrightarrow$

$$x^j w(x) \bmod (x^n + 1) = x^j\big(g(x)v(x) + e(x)\big) \bmod (x^n + 1)$$

$\Leftrightarrow$

$$x^j w(x) \bmod (x^n + 1) = x^j g(x)v(x) \bmod (x^n + 1) + x^j e(x) \bmod (x^n + 1)$$

$$\tilde{e}(x) - x^{n-j} S_j(x) \equiv 0 \mod (x^n + 1)$$
$$\tilde{e}(x) + x^{n-j} S_j(x) \equiv 0 \mod (x^n + 1)$$

$$p(x)(x^n + 1) = \tilde{e}(x) + x^{n-j} S_j(x)$$
$$\tilde{e}(x) + p(x)(x^n + 1) = x^{n-j} S_j(x)$$
$$\tilde{e}(x) + p(x)(x^n + 1) = x^{n-j}\left(x^i w(x) \bmod g(x)\right)$$
$$\frac{\tilde{e}(x) + p(x)(x^n + 1)}{x^{n-j}} = x^i w(x) \bmod g(x)$$
$$\frac{\tilde{e}(x) + p(x)(x^n + 1)}{x^{n-j}} + x^i w(x) = q(x)g(x)$$
$$\frac{\tilde{e}(x) + p(x)(x^n + 1)}{x^{n-j}} = q(x)g(x) + x^i w(x)$$
$$\tilde{e}(x) + p(x)(x^n + 1) = x^{n-j} q(x)g(x) + x^{n-j} x^i w(x)$$
$$\tilde{e}(x) + p(x)(x^n + 1) = x^{n-j} q(x)g(x) + x^n w(x)$$

$$\tilde{e}(x) + p(x)(x^n + 1) = x^n w(x) \bmod g(x)$$

$\Leftrightarrow \{g(x) | (x^n + 1)\}$

$$\tilde{e}(x) = x^n w(x) \bmod g(x)$$

$$x^{n-i} S_i(x) \bmod (x^n + 1)$$

$= \{$Notar que $S_i(x) = x^i e(x) \bmod g(x)$

Entonces, como $|S_i| \leq t$ tenemos que $\left|x^i e(x) \bmod g(x)\right| \leq t$

$\}$

$$x^{n-i}\left(x^i e(x) \bmod g(x)\right) \bmod (x^n + 1)$$

$= \{$Notar que $S_i(x) = x^i e(x) \bmod g(x)$

$\}$

$= \{\text{Definición } w\}$

$$x^{n-i}\left(x^{i}\left(g(x)v(x) + e(x)\right) \bmod g(x)\right) \bmod (x^n + 1)$$

$=$

$= \{x^{n-1}g(x)v(x) \bmod g(x) = 0, \text{ por ser un multiplo de } g\}$

$$x^{n-i}\left(e(x) \bmod g(x)\right) \bmod (x^n + 1)$$

1i) ❌

miércoles, 1 de junio de 2022 16:29

(1) Dados los siguientes polinomios $g(x)$, junto con la longitud n, sea C el código de longitud n generado por $g(x)$. Hacer en cada caso los siguientes items. Para el codigo iv), solo hacer los 2 primeros items, pero para el segundo, codificar 3 palabras no nulas en vez de 2. Para el codigo iii), no hace falta hacer el ultimo item.

(a) Dar la dimension de C.

(b) Elejir dos palabras no nulas de la dimension adecuada, y codificarlas, usando ambos metodos enseñados en clase.

(c) Dar la matriz generadora de C correspondiente a g(x) correspondiente al "metodo 1"de codificacin dado en clase.

(d) Dar una matriz generadora de C con la identidad a derecha (correspondiente al "metodo 2"dado en clase).

(e) Dar una matriz de chequeo de C con la identidad a izquierda.

(f) Probar que $g(x)$ divide a $x^n + 1$.

(g) Hallar el polinomio chequeador.

i) $g(x) = 1 + x + x^3$; $n = 7$. ii) $g(x) = 1 + x + x^4$; $n = 15$

(los anteriores generan códigos de Hamming)

iii) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$; $n = 15$.

(este genera un código que corrige 2 errores)

iv) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$; $n = 23$.

(nota: este ultimo genera el código **Golay**. Corrige 3 errores, pues tiene $\delta = 7$. (no hace falta que pruebe esto)).

a) $g = 1011000$

$n = 7$

$k = n - gr(g) = 7 - 3 = 4$

b)

Codifico las palabras $u_1 = 0101$ y $u_2 = 1100$

Metodo 1:

$u_1 \odot g = 01011000 + 0001011$

$= 0100111$

$$U_2 \odot g = 1011000 + 0101100$$
$$= 1110100$$

Metodo 2:

$$(U_1(x) \cdot x^3 \mod g(x)) + U_1(x) \cdot x^3$$
$$= (x^4 + x^6 \mod x^3 + x^2 + 1) + x^4 + x^6$$
$$= 1 + x + x^2 + x + x^2 + x^4 + x^6$$
$$= 1 + x^4 + x^6$$
$$= 1000101$$

$$(U_2(x) \cdot x^3 \mod g(x)) + U_2(x) \cdot x^3$$
$$= (x^3 + x^4 \mod x^3 + x^2 + 1) + x^3 + x^4$$
$$= 1 + x^2 + 1 + x + x^2 + x^3 + x^4$$
$$= x + x^3 + x^4$$
$$= 0101100$$

c) En el método 1 la matriz generadora es

$$G = \begin{bmatrix} g \\ rot(g) \\ \vdots \\ rot^{k-1}(g) \end{bmatrix}$$

$$g = 1011000$$

$$= \begin{bmatrix} 1 & 0 & 1 & 1 & & & 0 \\ & 1 & 0 & 1 & 1 & & \\ & & 1 & 0 & 1 & 1 & \\ 0 & & & 1 & 0 & 1 & 1 \end{bmatrix}$$

d) $g(x) = 1 + x^2 + x^3$

$x^3 \equiv 1 + x^2$ (sean mod g todos los $\equiv$)

$\Rightarrow$

$x^4 \equiv x + x^3 \equiv 1 + x + x^2$

$x^5 \equiv x + x^2 + x^3 \equiv 1 + x$

$x^6 \equiv x + x^2$

$x^7 \equiv x^2 + x^3 \equiv 1$ $\Rightarrow$ $g(x)$ divide a $x^7 + 1$ (f)

Por teorema, una matriz generadora es:

$$G = \begin{bmatrix} (x^{n-k} \bmod g) + x^{n-k} \\ (x^{n-k+1} \bmod g) + x^{n-k+1} \\ \vdots \\ (x^{n-1} \bmod g) + x^{n-1} \end{bmatrix}$$

$$G = \begin{bmatrix} 1 & 0 & 1 & & \\ 1 & 1 & 1 & & \\ 1 & 1 & 0 & & Id_4 \\ 0 & 1 & 1 & & \end{bmatrix}$$

g) El polinomío de chequeo es:

$$h(x) = \frac{x^7+1}{g(x)}$$

Hago la división:

$$\begin{array}{l|l}
x^7+1 & x^3+x^2+1 \\ \cline{2-2}
-\ x^7+x^6+x^4 & x^4+x^3+x^2+1 \\ \cline{1-1}
x^6+x^4+1 & \\
-\ x^6+x^5+x^3 & \\ \cline{1-1}
x^5+x^4+x^3+1 & \\
-\ x^5+x^4+x^2 & \\ \cline{1-1}
x^3+x^2+1 & \\
-\ x^3+x^2+1 & \\ \cline{1-1}
0 &
\end{array}$$

Queda:

$h = 1011100$

1ii) 🛠️ ❌

viernes, 3 de junio de 2022 17:14

(1) Dados los siguientes polinomios $g(x)$, junto con la longitud n, sea C el código de longitud n generado por $g(x)$. Hacer en cada caso los siguientes items. Para el codigo iv), solo hacer los 2 primeros items, pero para el segundo, codificar 3 palabras no nulas en vez de 2. Para el codigo iii), no hace falta hacer el ultimo item.

(a) Dar la dimension de C.

(b) Elejir dos palabras no nulas de la dimension adecuada, y codificarlas, usando ambos metodos enseñados en clase.

(c) Dar la matriz generadora de C correspondiente a g(x) correspondiente al "metodo 1"de codificacin dado en clase.

(d) Dar una matriz generadora de C con la identidad a derecha (correspondiente al "metodo 2"dado en clase).

(e) Dar una matriz de chequeo de C con la identidad a izquierda.

(f) Probar que $g(x)$ divide a $x^n + 1$.

(g) Hallar el polinomio chequeador.

i) $g(x) = 1 + x + x^3$; $n = 7$. ii) $g(x) = 1 + x + x^4$; $n = 15$

(los anteriores generan códigos de Hamming)

iii) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$; $n = 15$.

(este genera un código que corrige 2 errores)

iv) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$; $n = 23$.

(nota: este ultimo genera el código **Golay**. Corrige 3 errores, pues tiene $\delta = 7$. (no hace falta que pruebe esto)).

b)

$g = 110010000000000$

$$
\begin{aligned}
k &= \dim(C) \\
&= n - \mathrm{gr}(g) \\
&= 15 - 5 \\
&= 10
\end{aligned}
$$

$$G = \begin{bmatrix} \left(x^{n-k} \bmod g(x)\right) + x^{n-k} \\ \left(x^{n-k+1} \bmod g(x)\right) + x^{n-k+1} \\ \vdots \\ x\left(^{n-1} \bmod g(x)\right) + x^{n-1} \end{bmatrix}$$

$$g(x) = 1 + x + x^4$$

$$1 + x + x^4 \equiv 0$$

$$x^4 \equiv 1 + x$$

$$x^5 \equiv x + x^2$$
$$x^6 \equiv x^2 + x^3$$
$$x^7 \equiv x^3 + x^4 \equiv x^3 + 1 + x \equiv 1 + x + x^3$$
$$x^8 \equiv x + x^2 + x^4 \equiv x + x^2 + 1 + x \equiv 1 + x^2$$
$$x^9 \equiv x + x^3$$
$$x^{10} \equiv x^2 + x^4 \equiv x^2 + 1 + x \equiv 1 + x + x^2$$
$$x^{11} \equiv x + x^2 + x^3$$
$$x^{12} \equiv x^2 + x^3 + x^4 \equiv x^2 + x^3 + 1 + x \equiv 1 + x + x^2 + x^3$$
$$x^{13} \equiv x + x^2 + x^3 + x^4 \equiv x + x^2 + x^3 + 1 + x \equiv 1 + x^2 + x^3$$
$$x^{14} \equiv x + x^3 + x^4 \equiv x + x^3 + 1 + x \equiv 1 + x^3$$
$$x^{15} \equiv x + x^4 \equiv x + 1 + x \equiv 1$$

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 & \\ 0 & 1 & 1 & 0 & \\ 0 & 0 & 1 & 1 & \\ 1 & 1 & 0 & 1 & \\ 1 & 0 & 1 & 0 & \\ 0 & 1 & 0 & 1 & \mathrm{Id}_{11} \\ 1 & 1 & 1 & 0 & \\ 0 & 1 & 1 & 1 & \\ 1 & 1 & 1 & 1 & \\ 1 & 0 & 1 & 1 & \\ 1 & 0 & 0 & 1 & \end{bmatrix}$$

$$h = \frac{1 + x^{15}}{g(x)}$$

Hago la división:

$$
\begin{array}{r|l}
 & 1 + x + x^4 \\
\hline
1 + x + x^2 + x^3 + x^5 + x^7 + x^8 + x^{11} & 1 + x^{15} \\
 & - \; x^{11} + x^{12} + x^{15} \\
 & 1 + x^{11} + x^{12} \\
 & - \; x^8 + x^9 + x^{12} \\
 & 1 + x^8 + x^9 + x^{11} \\
 & - \; x^7 + x^8 + x^{11} \\
 & 1 + x^7 + x^9 \\
 & - \; x^5 + x^6 + x^9 \\
 & 1 + x^5 + x^6 + x^7 \\
 & - \; x^3 + x^4 + x^7 \\
 & 1 + x^3 + x^4 + x^5 + x^6 \\
 & - \; x^2 + x^3 + x^6 \\
 & 1 + x^2 + x^4 + x^5 \\
 & - \; x + x^2 + x^5 \\
 & 1 + x + x^4 \\
 & - \; 1 + x + x^4 \\
 & 0
\end{array}
$$

$h = 1\,1\,1\,1\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,0$

1iii) 🛠️

sábado, 4 de junio de 2022 17:24

iii) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$; $n = 15$.
(este genera un código que corrige 2 errores)

$g = 100010111000000$

$n = 15$

$k = \dim(c)$

$= n - gr(g)$

$= 15 - 8 = 7$

$g(x) = 1 + x^4 + x^6 + x^7 + x^8$

$x^8 \equiv 1 + x^4 + x^6 + x^7$ (sean todos los $\equiv$ mod g)

$x^9 \equiv x + x^5 + x^7 + x^8$

$\equiv 1 + x + x^4 + x^5 + x^6$

$x^{10} \equiv x + x^2 + x^5 + x^6 + x^7$

$x^{11} \equiv x^2 + x^3 + x^6 + x^7 + x^8$

$\equiv 1 + x^2 + x^3 + x^4$

$x^{12} \equiv x + x^3 + x^4 + x^5$

$x^{13} \equiv x^2 + x^4 + x^5 + x^6$

$$x^{13} \equiv x^2 + x^4 + x^5 + x^6$$

$$x^{14} \equiv x^3 + x^5 + x^6 + x^7$$

$$x^{15} \equiv x^4 + x^6 + x^7 + x^8$$

$$\equiv 1$$

Por teorema, una matriz generadora es:

$$G = \begin{bmatrix} (x^{n-k} \bmod g) + x^{n-k} \\ (x^{n-k+1} \bmod g) + x^{n-k+1} \\ \vdots \\ (x^{n-1} \bmod g) + x^{n-1} \end{bmatrix}$$

$$G = [A \quad Id_7]$$

con:

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$\Rightarrow$ La matriz de chequeo es:

$$H = [Id_8 \quad A^t]$$

El polinomio de chequeo es:

$$h(x) = \frac{1+x^{15}}{g(x)}$$

$$\begin{array}{r|l} 1+x^4+x^6+x^7+x^8 & 1+x^{15} \\ \cline{2-2} 1+x^4+x^6+x^7 & -\ x^7+x^{11}+x^{13}+x^{14}+x^{15} \\ \cline{2-2} & 1+x^7+x^{11}+x^{13}+x^{14} \\ & -\ x^6+x^{10}+x^{12}+x^{13}+x^{14} \\ \cline{2-2} & 1+x^6+x^7+x^{10}+x^{11}+x^{12} \\ & -\ x^4+x^8+x^{10}+x^{11}+x^{12} \\ \cline{2-2} & 1+x^4+x^6+x^7+x^8 \\ & -\ 1+x^4+x^6+x^7+x^8 \\ \cline{2-2} & 0 \end{array}$$

$$h(x) = 1+x^4+x^6+x^7$$

Código 2 palabras:

$\alpha_1 = 1000000$

Método 1:

$g \cdot \alpha_1 = 1000101111000000$

Método 2:

$$\left(\alpha_1(x)\cdot x^{n-k} \mod g(x)\right) + \alpha_1(x)\cdot x^{n-k}$$

$$\left|\begin{array}{l} \alpha_1(x)\cdot x^8 \equiv x^8 \\ \qquad\qquad \equiv 1+x^4+x^6+x^7 \end{array}\right.$$ calculado al calcular G

$$= 1+x^4+x^6+x^7+x^8$$

$$= 100010111000000$$

$\alpha_2 = 1100000$

Método 1:

$$g\cdot\alpha_2 = \begin{array}{r} 100010111000000 \\ +\ 010001011100000 \end{array}$$

$$= 110011100100000$$

Método 2:

$$\left(\alpha_2(x)\cdot x^{n-k} \mod g(x)\right) + \alpha_2(x)\cdot x^{n-k}$$

$$\left|\begin{array}{l} \alpha_2(x)\cdot x^8 \equiv x^8+x^9 \\ \qquad\qquad \equiv 1+x^4+x^6+x^7+1+x+x^4+x^5+x^6 \\ \qquad\qquad \equiv x^7 \end{array}\right.$$ calculado al calcular G

$$= x^7+x^8+x^9$$

$= 0000001110000 0$

1iv) 🛠️

sábado, 4 de junio de 2022 19:46

iv) $g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$; $n = 23$.

(nota: este ultimo genera el código **Golay**. Corrige 3 errores, pues tiene $\delta = 7$. (no hace falta que pruebe esto)).

$g = 11000111010100000000000$

$n = 23$

$k = \dim(C) = n - gr(g)$

$= 23 - 11$

$= 12$

Por teorema, una matriz generadora es:

$$G = \begin{bmatrix} (x^{11} \bmod g) + x^{11} \\ (x^{12} \bmod g) + x^{12} \\ \vdots \\ (x^{22} \bmod g) + x^{22} \end{bmatrix}$$

Calculo las filas:

$g(x) = 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11}$

$x^{11} \equiv 1 + x + x^5 + x^6 + x^7 + x^9$ (Sean todos los $\equiv$ mod g)

$\vdots$

$x^{13} \equiv x^2 + x^3 + x^7 + x^8 + x^9 + x^{11}$

$\equiv 1 + x + x^2 + x^3 + x^5 + x^6 + x^8$

$x^{14} \equiv x + x^2 + x^3 + x^4 + x^6 + x^7 + x^9$

$$x^{14} \equiv x + x^2 + x^3 + x^4 + x^6 + x^7 + x^9$$

$$\vdots$$

$$x^{16} \equiv x^3 + x^4 + x^5 + x^6 + x^8 + x^9 + x^{11}$$

$$\equiv 1 + x + x^3 + x^4 + x^7 + x^8$$

$$x^{17} \equiv x + x^2 + x^4 + x^5 + x^8 + x^9$$

$$\vdots$$

$$x^{19} \equiv x^3 + x^4 + x^6 + x^7 + x^{10} + x^{11}$$

$$\equiv 1 + x + x^3 + x^4 + x^5 + x^9 + x^{10}$$

$$x^{20} \equiv x + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$$

$$\equiv 1 + x^2 + x^4 + x^7 + x^9 + x^{10}$$

$$x^{21} \equiv x + x^3 + x^5 + x^8 + x^{10} + x^{11}$$

$$\equiv 1 + x^3 + x^6 + x^7 + x^8 + x^9 + x^{10}$$

$$x^{22} \equiv x + x^4 + x^7 + x^8 + x^9 + x^{10} + x^{11}$$

$$\equiv 1 + x^4 + x^5 + x^6 + x^8 + x^{10}$$

$$x^{23} \equiv x + x^5 + x^6 + x^7 + x^9 + x^{11}$$

$$\equiv 1$$

$$G = [A \;\; Id_{12}]$$

con:

$$A = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Matriz de chequeo:

$$H = [Id_{11} \quad A^t]$$

El polinomio de chequeo es:

$$h = \frac{1 + x^{23}}{g(x)}$$

Hago la división:

$$\begin{array}{r|l} & 1 + x^{23} \\ \hline 1 + x + x^5 + x^6 + x^7 + x^9 + x^{11} & \\ x + x^2 + x^3 + x^4 + x^7 + x^{10} + x^{12} & \\ \hline - & x^{12} + x^{13} + x^{17} + x^{18} + x^{19} + x^{21} + x^{23} \\ & 1 + x^{12} + x^{13} + x^{17} + x^{18} + x^{19} + x^{21} \\ \hline - & x^{10} + x^{11} + x^{15} + x^{16} + x^{17} + x^{19} + x^{21} \\ & 1 + x^{10} + x^{11} + x^{12} + x^{13} + x^{15} + x^{16} + x^{18} \\ \hline - & x^7 + x^8 + x^{12} + x^{13} + x^{14} + x^{16} + x^{18} \\ & 1 + x^7 + x^8 + x^{10} + x^{11} + x^{14} + x^{15} \\ \hline - & x^4 + x^5 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} \end{array}$$

$$
\begin{array}{rl}
 & 1+x^7+x^8+x^{10}+x^{11}+x^{14}+x^{15} \\
- & x^4+x^5+x^9+x^{10}+x^{11}+x^{13}+x^{15} \\
\hline
 & 1+x^4+x^5+x^7+x^8+x^9+x^{13}+x^{14} \\
- & x^3+x^4+x^8+x^9+x^{10}+x^{12}+x^{14} \\
\hline
 & 1+x^3+x^5+x^7+x^{10}+x^{12}+x^{13} \\
- & x^2+x^3+x^7+x^8+x^9+x^{11}+x^{13} \\
\hline
 & 1+x^2+x^5+x^8+x^9+x^{10}+x^{11}+x^{12} \\
- & x+x^2+x^6+x^7+x^8+x^{10}+x^{12} \\
\hline
 & 1+x+x^5+x^6+x^7+x^9+x^{11} \\
- & 1+x+x^5+x^6+x^7+x^9+x^{11} \\
\hline
 & 0
\end{array}
$$

$h = 1 + x + x^2 + x^3 + x^4 + x^7 + x^{10} + x^{12}$

Codifico las palabras $U_1 = 101000000000$ y $U_2 = 001101000000$

Método 1:

$$
\begin{aligned}
g \odot U_1 = \; & 110001110101000000000000 + \\
& 001100011101010000000000
\end{aligned}
$$

$$= 111100110100010000000$$

$$
\begin{aligned}
g \odot U_2 = \; & 001100011101010000000000 + \\
& 000110001110101000000000 + \\
& 000001100011101010000000
\end{aligned}
$$

$$= 0010111100001001000000$$

Método 2:

$$\left(u_1(x)\,x^{11} \bmod g(x)\right) + u_1(x)\,x^{11}$$

$$u_1(x)\,x^{11}$$

$$\equiv x^{11} + x^{13}$$

$$\equiv 1 + x + x^5 + x^6 + x^7 + x^9 + 1 + x + x^2 + x^3 + x^5 + x^6 + x^8$$

calculos de G

$$\equiv x^2 + x^3 + x^7 + x^8 + x^9$$

$$= x^2 + x^3 + x^7 + x^8 + x^9 + x^{11} + x^{13}$$

$$= 0011000111010100000000$$

$$\left(u_2(x)\,x^{11} \bmod g(x)\right) + u_2(x)\,x^{11}$$

$$u_2(x)\,x^{11}$$

$$\equiv x^{13} + x^{14} + x^{16}$$

$$\equiv 1 + x + x^2 + x^3 + x^5 + x^6 + x^8 + x + x^2 + x^3 + x^6 + x^7 + x^9 + 1 + x + x^3 + x^4 + x^7 + x^8$$

calculos de G

$$\equiv x + x^3 + x^4 + x^5 + x^9$$

$$= x + x^3 + x^4 + x^5 + x^9 + x^{13} + x^{14} + x^{16}$$

$$= 0101110001000110100000$$

2)

domingo, 5 de junio de 2022 10:12

(2) Probar que el código Golay dado en el ejercicio anterior es perfecto.

C es perfecto

$\Leftrightarrow$

$$\#C = \frac{2^n}{\sum_{r=0}^{\left\lfloor \frac{\delta(C)-1}{2} \right\rfloor} \binom{n}{r}}$$

$\Leftrightarrow \{\#C = 2^k,\ k = 12,\ n = 23\}$

$$2^{12} = \frac{2^{23}}{\sum_{r=0}^{\left\lfloor \frac{\delta(C)-1}{2} \right\rfloor} \binom{23}{r}}$$

$\Leftrightarrow$

$$\sum_{r=0}^{\left\lfloor \frac{\delta(C)-1}{2} \right\rfloor} \binom{23}{r} = 2^{11}$$

$\Leftrightarrow$ {Según el enunciado: $\delta(C) = 7$}

$$\sum_{r=0}^{\left\lfloor \frac{7-1}{2} \right\rfloor} \binom{23}{r} = 2048$$

$\Leftrightarrow$

$$\sum_{r=0}^{3} \binom{23}{r} = 2048$$

$\Leftrightarrow$

$$\binom{23}{0} + \binom{23}{1} + \binom{23}{2} + \binom{23}{3} = 2048$$

$\Leftrightarrow$

$$1 + 23 + \frac{23 \cdot 22}{2} + \frac{23 \cdot 22 \cdot 21}{3 \cdot 2} = 2048$$

$\Leftrightarrow$

$$2048 = 2048$$

$\Leftrightarrow$

True

3)

domingo, 5 de junio de 2022 10:22

(3) a) ¿Cuántos códigos binarios de longitud n hay? (con al menos 2 palabras)

b) ¿Cuántos códigos binarios de longitud 3 con exactamente 5 palabras hay?

c) ¿Cuántos de esos códigos son lineales?

d) ¿Cuántos códigos binarios de longitud 3 con exactamente 4 palabras hay?

e) ¿Cuántos de esos códigos son lineales?

f) ¿Cuántos de esos códigos son cíclicos?

a)
Hay 2^n palabras, y cada palabra puedo elegirla o no (ademas resto el código vacio y los códigos de 1 palabra)

$2^{2^n} - 1 - 2^n c)$

b)
Formas de elegir 5 elementos de 2^3

$$\binom{2^3}{5} = \frac{8!}{(8-5)! \cdot 5!} = \frac{8 \cdot 7 \cdot 6}{3 \cdot 2} = 8 \cdot 7 = 56$$

c)
Ninguno, porque los códigos lineales tienen que tener una potencia de 2 de cantidad de elementos

d)
Formas de elegir 4 elementos de 2^3

$$\binom{2^3}{4} = \frac{8!}{(8-4)! \cdot 4!} = \frac{8 \cdot 7 \cdot 6 \cdot 5}{4 \cdot 3 \cdot 2} = 2 \cdot 7 \cdot 5 = 70$$

e)
$\{0,1\}^3 = \{000,001,010,011,100,101,110,111\}$

Formas de elegir una base de 2 elementos
Cualquieras 2 elementos que no sean el 0 que se elijan, van a ser LI, y por ende formar una base, así que las formas de elegir 2 elementos de $2^3 - 1$

$$\binom{2^3 - 1}{2} = \binom{7}{2} = \frac{7 \cdot 6}{2} = 21$$

f)

Averiguo la cantidad de polinomios generadores g

La dimensión del código tiene que ser 2

$$\Rightarrow \mathrm{gr}(g) = 3 - 2$$
$$\Rightarrow \mathrm{gr}(g) = 1$$

Esto significa que el primer bit tiene que ser 1, el segundo 1, y el tercero 0
Eso solo deja a 110

Por ende hay un solo código ciclico de longitud 3 con 4 elementos

4) 🛠️

viernes, 2 de junio de 2023 10:52

(4) $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ con $n = 15$ genera un código de longitud 15 que corrije 2 errores. Use el algoritmo de "error trapping" para corregir los errores de las siguientes palabras:

a) 001000001110110 b) 110010011110111
c) 001111101001001 d) 001000000110000
e) 110001101000101 f) 001001000100110

$$g(x) = 1 + x^4 + x^6 + x^7 + x^8$$

$$n = 15$$

$$k = 15 - 8 = 7$$

$$A = \begin{bmatrix} 1 & & & & 1 & & 1 & 1 \\ 1 & 1 & & & 1 & 1 & 1 & \\ & 1 & 1 & & & 1 & 1 & 1 \\ 1 & & 1 & 1 & 1 & & & \\ & 1 & & 1 & 1 & 1 & & \\ & & 1 & & 1 & 1 & 1 & \\ & & & 1 & & 1 & 1 & 1 \end{bmatrix}$$

$$G = [A \quad Id_7]$$

$$\Rightarrow H = [Id_8 \quad A^t]$$

1 — * — *'

a) $r = 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0$

$H r^t = 0\ 1\ 1\ 1\ 0\ 0\ 0\ 0$

	1				1		1	1
s_0	0	1	1	1	0	0	0	0
s_1			1	1	1			
s_2				1	1	1		
s_3					1	1	1	
s_4						1	1	1
s_5	1			1				

$\tilde{e} = x^{11} s_5(x) \mod (x^n + 1)$

$s_5(x)$	1	0	0	0	1	0	0	0	0	0	0	0	0	0
$x^{10} s_5(x)$											1			1

$r = 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ \underline{0}\ 0\ 1\ 1\ \underline{1}$

$$
A = \begin{array}{cc}
\begin{bmatrix}
1 & & & & 1 & & 1 & 1 \\
1 & 1 & & & 1 & 1 & 1 & \\
 & 1 & 1 & & & 1 & 1 & 1 \\
1 & & 1 & 1 & 1 & & & \\
 & 1 & & 1 & 1 & 1 & & \\
 & & 1 & & 1 & 1 & 1 & \\
 & & & 1 & & 1 & 1 & 1
\end{bmatrix} & \begin{matrix} * \\ * \\ \\ \\ * \\ * \\ * \end{matrix} \\
\begin{matrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix} &
\end{array}
$$

5)

domingo, 5 de junio de 2022 10:44

(5) Sean C_1, C_2 códigos cíclicos con generadores g_1, g_2. Probar que $C_1 + C_2$ tambien es cíclico y tiene generador $\mathrm{mcd}(g_1, g_2)$.

Sean:
C_1, C_2 códigos cíclicos de lognitud n con generadores g_1 y g_2

$C_1 + C_2$ es cilico
$\mathrm{mcd}(g_1, g_2)$ es generador de $C_1 + C_2$

Demostraciones:
$C_1 + C_2$ es cilico

Sea
$\tilde{u} \in C_1 + C_2$
Y sea $u_1 \in C_1$ y $u_2 \in C_2$ tal que $\tilde{u} = u_1 + u_2$
Pruebo que una rotación de $\tilde{u}$ está en $C_1 + C_2$

$\mathrm{rot}(\tilde{u}) \in C_1 + C_2$
$\Leftrightarrow$
$\mathrm{rot}(u_1 + u_2) \in C_1 + C_2$
$\Leftrightarrow$
$\mathrm{rot}(u_1) + \mathrm{rot}(u_2) \in C_1 + C_2$
$\Leftarrow$
$\mathrm{rot}(u_1) \in C_1 \wedge \mathrm{rot}(u_2) \in C_2$
$\Leftrightarrow \{C_1$ y C_2 son cíclicos$\}$
True

$\mathrm{mcd}(g_1, g_2)$ es generador de $C_1 + C_2$:

$\mathrm{mcd}(g_1, g_2)$ es generador de $C_1 + C_2$
$\Leftrightarrow$
$C_1 + C_2 = \{v \odot \mathrm{mcd}(g_1, g_2) : v \in \{0,1\}^*\}$
$\Leftrightarrow$
$\forall \alpha : \alpha \in C_1 + C_2 \Leftrightarrow \alpha \in \{v \odot \mathrm{mcd}(g_1, g_2) : v \in \{0,1\}^*\}$

Pruebo esto por doble inducción:

Ida ($\Rightarrow$) suponiendo al antecedente:

Tengo que probar $\alpha \in \{v \odot \operatorname{mcd}(g_1, g_2) : v \in \{0,1\}^*\}$, trabajo con α:

$$\begin{aligned}
&\alpha \\
&= \{\alpha \text{ es suma de elementos de } C_1 \text{ y } C_2\text{, sean } \beta_1 \in C_1 \text{ y } \beta_2 \in C_2\} \\
&\quad \beta_1 + \beta_2 \\
&= \{g_1 \text{ genera a } C_1 \text{ y } g_2 \text{ genera a } C_2\text{, sea } \beta_1 = v_1 \odot g_1,\ \beta_2 = v_2 \odot g_2\} \\
&\quad v_1 \odot g_1 + v_2 \odot g_2 \\
&= \{\text{Saco factor común } \operatorname{mcd}(g_1, g_2)\} \\
&\quad \left(v_1 \odot \frac{g_1}{\operatorname{mcd}(g_1, g_2)} + v_2 \odot \frac{g_2}{\operatorname{mcd}(g_1, g_2)}\right) \odot \operatorname{mcd}(g_1, g_2)
\end{aligned}$$

Esta claro que esto está en $\{v \odot \operatorname{mcd}(g_1, g_2) : v \in \{0,1\}^n\}$

Vuelta ($\Leftarrow$) suponiendo el antecedente:

Tengo que probar $\alpha \in C_1 + C_2$, trabajo con α:

$$\begin{aligned}
&\alpha \\
&= \{\text{Por antecedente, sea } \alpha = v \odot \operatorname{mcd}(g_1, g_2)\} \\
&\quad v \odot \operatorname{mcd}(g_1, g_2) \\
&= \{\text{Por teorema, el mcd se puede escribir como combinación lineal de los elementos,} \\
&\qquad \text{así que sea } \operatorname{mcd}(g_1, g_2) = k_1 \cdot g_1 + k_2 \cdot g_2 \text{ con } k_1, k_2 \in \{0,1\}^* \\
&\qquad \text{(Notar que se usa el producto normal, no el } \odot\text{)} \\
&\} \\
&\quad v \odot (k_1 \cdot g_1 + k_2 \cdot g_2) \\
&= \\
&\quad v \odot (k_1 \cdot g_1) + v \odot (k_2 \cdot g_2) \\
&= \{(p \cdot q) \odot r = (p \cdot q) \cdot r \bmod g = p \cdot (q \cdot r) \bmod g = p \odot (q \cdot r)\} \\
&\quad (v \cdot k_1) \odot g_1 + (v \cdot k_2) \odot g_2
\end{aligned}$$

Esta claro que esto está en $C_1 + C_2$, porque $(v \cdot k_1) \odot g_1 \in C_1$ y $(v \cdot k_2) \odot g_2 \in C_2$

Error trapping

miércoles, 7 de junio de 2023 12:23

Sean:
C un código cilcio de logitud n
$k = \dim(C)$
t la cantidad de errores que corrige C
g un polinomio generador de C
$v \in \{0,1\}^k$
$e \in \{0,1\}^n$ con $|e| \leq t$
$w = g \odot v + e$

w sería la palabra a decodificar, la cual tiene e como error

El algoritmo (que puede no lograrlo) para decodificar sería así:

Definir $S_i(x) = x^i w(x) \bmod g(x)$

Buscar el mínimo i tal que $|S_i| \leq t$

Si el i no existe, en algún momento se llega a un S_i igual a alguno anterior y significa que en ese caso no se va a poder decodificar el error

Si el i existe, el error se calcula así: $e(x) = x^{n-i} S_i(x) \bmod (x^n + 1)$