ETIQUETAS: MD2::(05)Codigosciclicos

¿Cuando un código es ciclico?

Cuando es lineal y la rotación de cualquiera de sus palabras es otra palabra del código

¿Cómo se define $rot(w)$ dada una palabra $w = w_0 w_1 \dots w_{n-1}$?

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

¿Como que polinomio se puede pensar la palabra $w = w_0 w_1 \dots w_{n-1}$?

$w_0 + w_1 x + \dots + w_{n-1} x^{n-1}$

¿Que denota $p(x) \mod m(x)$ siendo $p(x)$ y $m(x)$ polinomios?

El resto de la división de $p(x)$ por $m(x)$

¿Cómo se define $v \odot w$ dadas dos palabras v y w de longitud n?

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

$x^n \mod (1 + x^n) =$ {{c1::1}}

$x^{n+1} \mod (1 + x^n) =$ {{c2::x}}

$x^{n+2} \mod (1 + x^n) =$ {{c2::x^2}}

$rot(w) =$ {{c1::$x \odot w(x)$}}

Sea C un código cíclico, {{c1::$w \in C$ y v una palabra cualquiera}}.
Entonces {{c2::$v \odot w \in C$}}

Si C es {{c2::lineal}}, entonces existe un único {{c1::polinomio no nulo en C de grado mínimo}}

¿Que es el polinomio generador de C código ciclico?

Es el único polinomio no nulo de grado mínimo en C

¿Cómo se lo denota al polinomio generador de C?

$g(x)$

¿Que dice el teorema fundamental de códigos cíclicos?

Sea $g(x)$ el polinomio generador de un código cíclico C de longitud n.
Entonces:

1. $C = \{p(x) : gr(p) < n \ \& \ g(x) | p(x)\}$ (C esta formado por los multiplos de $g(x)$ de grado menor que n)
2. $C = \{v(x) \odot g(x) : v \text{ es un polinomio cualquiera } \}$
3. $gr(g(x)) = n - k$
4. $g(x)$ divide a $1 + x^n$
5. $g_0 = 1$

¿Cómo calcular la dimensión de un código cíclico?

Usando que $gr(g(x)) = n - k$

¿Cual es el polinomio chequeador de C?

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

¿Cómo se lo denota al polinomio chequeador de C?

$h(x)$

¿Cómo es el primer método de codificación de códigos ciclicos?

Se agarra el mensaje m y se lo multiplica por $g(x)$

¿Cómo queda la matriz generadora formada con el primer método de codificación de códigos ciclicos?

$$G = \begin{bmatrix} g \\ xg \\ x^2 g \\ \vdots \\ x^{k-1} g \end{bmatrix}$$

¿Que desventaja tiene el primer método de codificación de códigos ciclicos?

Es dificil decodificar la palabra

¿Porque es dificil decodificar la palabra en el primer método de codificación de códigos ciclicos?

Porque la matriz de chequeo no contiene a la identidad

¿Que ventaja tiene el primer método de codificacion de códigos ciclicos?

Es facil codificar la palabra/es intuitivo

¿Cómo es el segundo método de codificación de códigos ciclicos?

Se agarra el mensaje m y se calcula $mx^{n-k} + (mx^{n-k} \mod g)$

¿Cómo se calcula $x^{n-k} \mod g$?

Despejando x^{n-k} de $g(x) \mod g(x) = 0$

¿Cómo se calcula $x^{n-k+i} \mod g$?

Utilizando valores previamente calculados

¿Cómo recuperar el mensaje en el segundo método de codificación de códigos ciclicos?

Son los últimos k bits de la palabra codificada

¿Cómo chequear que $g(x)$ divide a $1 + x^n$?

Se calcula $x^n \mod g(x)$ y si da 1 entonces $g(x)$ divide a $1 + x^n$

¿Cómo chequear que no me equivoque en alguna cuenta al hacer todas las congruencias?

Deberia cumplirse que $x^n \mod g(x) = 1$

¿Cómo queda la matriz generadora formada con el segundo método de codificación de códigos ciclicos?

$$G = \begin{bmatrix} x^{n-k} & \mod\ g(x) + x^{n-k} \\ x^{n-k+1} & \mod\ g(x) + x^{n-k+1} \\ x^{n-k+2} & \mod\ g(x) + x^{n-k+2} \\ & \vdots \\ x^{n-1} & \mod\ g(x) + x^{n-1} \end{bmatrix}$$

¿Son los códigos de Hamming códigos ciclicos?

Sí

Extra: En algún orden de las columnas

¿Cómo obtener la matriz de chequeo con la identidad a la izquierda de un código ciclico? (Método 2)

La columna j-ésima es $x^j \mod\ g(x)$

¿Que satisface el polinomio chequeador de un código ciclico?

$h(x) \odot p(x) = 0$ para toda palabra $p(x)$ del código

¿Cómo obtener el polinomio chequeador de un código ciclico?

Dividiendo $1 + x^n$ por $g(x)$

¿Para que sirve error trapping?

Para detectar errores que suecedieron en rafaga

¿El método de error trapping siempre funciona?

No

¿Cómo es el método de error trapping?

1. Calculo los S_i hasta que $||S_i|| \leq t$ siendo t la cantidad de errores máximos que puedo corregir
2. Obtener la palabra sin errores

¿Cómo se define el error en el método de error trapping?

$$\tilde{e} = x^{n-i} S_i \mod\ (x^n + 1)$$

¿Cómo se define S_0 en el método de error trapping?

$S_0 = w(x) \mod g(x)$ siendo $w(x)$ la palabra recibida

¿Cómo se define S_i en el método de error trapping?

$S_i = xS_{i-1} \mod g(x)$

¿Cómo se obtiene la palabra sin errores en el método de error trapping?

$w(x) + \tilde{e}$

¿De que tamaño es la ventana en la cual deben estar los errores para que el método de error trapping funcione?

$n - k = gr(g)$

¿Cuantos códigos binarios de longitud n hay? (Con al menos 2 palabras)

$$2^{2^n} - (n+1)$$

Extra: $2^{\text{cant de elementos del codigo}} - \text{conjunto vacio y codigos con 1 elemento}$

¿Cuantos códigos binarios de longitud n y z cantidad de elementos hay?

$$\frac{n!}{z!(n-z)!}$$

¿Cuando existen códigos lineales de longitud n y z cantidad de elementos?

Cuando $z = 2^k$ para algún k

¿Cuantos códigos lineales de longitud 3 y 4 palabras hay? (dar la forma generalizada)

$$\frac{\binom{2^3-1}{2}}{3} = \frac{\binom{2^n - |\text{la palabra } 0|}{k}}{n}$$

¿Cómo calcular cuantos códigos cíclicos de longitud n y 2^k palabras hay?

Por fuerza bruta verificando que palabras de las 2^n palabras pueden pertenecer al código ciclico