ETIQUETAS: MD2::(04)CodigosLineales

¿Que permite realizar un código de corrección de errores cuando ocurren errores de transmisión?

- Detectar errores
- Corregir errores

¿Que es más facil, detectar un error o corregirlo?

Detectar un error

¿Que es un código?

Es un conjunto no vacio de palabras sobre un alfabeto A

¿Que es un código de bloque?

Es un código en el que todas las palabras tienen la misma longitud

Un código de bloque sobre el alfabeto A es un subconjunto de {{c1::A^n para algún $n \in \mathbb{N}$}}

¿Que es un código binario?

Es un código sobre el alfabeto $\{0, 1\}$

¿A que códigos nos referimos cuando hablamos de códigos?

Códigos binarios de bloque

¿Que suposiciones hacemos sobre el canal de transmisión al usar códigos?

1. El canal no pierde ni añade bits, solo los transforma.
2. La probabilidad de un cambio de 1 a 0 es la misma que la de un cambio de 0 a 1.
3. La probabilidad de un cambio en el bit i es independiente de la probabilidad de un cambio en el bit j
4. Esa probabilidad es independiente de i, es decir, es la misma para todos los bits (la llamaremos p).
5. $0 < p < \frac{1}{2}$

¿A cual palabra corregimos al recibir un mensaje con errores?

A la palabra del código que es más probable que haya sido enviada

¿Que significa que una palabra sea más probable que otra de haber sido enviada?

Que necesito cambiar menos bits para pasar de esa palabra a la recibida

¿Que es la distancia de Hamming entre dos palabras $v, w \in \{0,1\}^n$?

$$|\{\text{Bits diferentes entre v y w}\}|$$

¿Cómo se denota la distancia de Hamming entre dos palabras $v, w \in \{0,1\}^n$?

$$d_H(v,w)$$

¿Cómo se define $\delta(C)$ dado un código C?

$$\delta(C) = \min\{d_H(v,w) : v,w \in C, v \neq w\}$$

$d_H(v,w) = d_H(${{c1::w,v}}$)$

$d_H(v,w) \geq$ {{c1::0}}

$d_H(v.w) = 0 \Leftrightarrow$ {{c1::$v = w$}}

$d_H(v \cdot w) \leq$ {{c1::$d_H(v \cdot u) + d_H(u,w)$}}
Extra: Desigualdad triangular

¿Cómo se define el disco de radio r alrededor de v dado $r \geq 0$ y $v \in \{0,1\}^n$?

$$\{w \in \{0,1\}^n : d_H(v,w) \leq r\}$$

¿Cómo se denota el disco de radio r alrededor de v dado $r \geq 0$ y $v \in \{0,1\}^n$?

$$D_r(v)$$

¿Cuando un código C detecta r errores?

Si $D_r(v) \cap C = \{v\}$ para todo $v \in C$

¿Cuando un código C corrige r errores?

Si $D_r(v) \cap D_r(w) = \emptyset$ para todo $v, w \in C$ con $v \neq w$

¿Que dice el teorema de δ para códigos?

Sea C un código y $\delta = \delta(C)$. Entonces:

1. C detecta $\delta - 1$ errores, pero no detecta δ errores.
2. C corrige $\lfloor \frac{\delta-1}{2} \rfloor$ errores, pero no corrige $\lfloor \frac{\delta-1}{2} \rfloor + 1$ errores.

¿Que dice el teorema de la cota de Hamming?

Sea C un código de longitud n, $\delta = \delta(C)$ y $t = \lfloor \frac{\delta-1}{2} \rfloor$. Entonces:

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

La cota de Hamming sirve para probar {{c1::imposibilidad de que un código exista}}

La cota de Hamming no sirve para probar {{c1::existencia de un código}}

¿Que es un código perfecto?

Un código C es perfecto si cumple la cota de Hamming con igualdad

¿Que es un código lineal de longitud n?

Es un subespacio vectorial de $\{0,1\}^n$

¿Que propiedades debe cumplir W subespacio vectorial de V?

1. $W \neq \emptyset$
2. $u, v \in W \Rightarrow u + v \in W$
3. $u \in W, \lambda \in \mathbb{K} \Rightarrow \lambda u \in W$

Un código C es lineal $\Leftrightarrow$ es un subconjunto {{c1::que contiene al vector nulo y es invariante por la suma}}

¿Que requisitos debo pedir para que el código C sea lineal?

- Respeta la suma
- Contiene al vector nulo

¿Que es el peso de Hamming de una palabra v de un código?

Es la cantidad de unos que tiene la palabra
Extra: $d_H(v, 0)$

$d_H(x, y) = |${{c1::$x + y$}}$|$

¿Cómo se denota el peso de Hamming de una palabra v de un código?

$$||v||$$

Si C es lineal, entonces $\delta(C) =$ {{c1::$\min\{||v|| : v \in C, v \neq 0\}$}}

¿Que es la dimensión de un espacio vectorial?

La cardinalidad de cualquier base del espacio

¿Que es una base de un espacio vectorial?

Un conjunto de vectores linealmente independientes que generan el espacio

¿Cuando se cumple que $\{u_1, \ldots, u_k\}$ es base de V?

- Genera V
- Es linealmente independiente

¿Cómo se denota la dimesión de un código lineal?

$$k$$

¿Cuantos elementos tiene un código lineal de dimensión k?

$$2^k$$

¿Cual es la dimensión de un código lineal con n palabras?

$$log_2(n)$$

¿Que representa la dimensión de un código lineal?

Cuantos bits del código son de información

¿Que representa $n-k$ de un código lineal, siendo n la longitud de las palabras y k la dimensión?

Los bits agregados para poder corregir y detectar errores

¿Cómo se define $REP_r(C)$ siendo C un código y $r \geq 0$?

$$REP_r(C) = \{vvvv\ldots v : v \in C\}$$

Extra: v se repite r veces

¿Cual es el valor de $\delta(REP_r(C))$?

$$r \cdot \delta(C)$$

¿Que es una matriz generadora de un código lineal C?

Una matriz cuyas filas son una base de C

¿Que tamaño tiene la matriz generadora de un código lineal C?

$$(k \times n)$$

¿Que es una matriz de chequeo de un código lineal C?

Una matriz que satisface que $C = Nu(H)$

¿Cómo se define $Nu(H)$ siendo H una matriz de chequeo?

$$Nu(H) = \{v \in \{0,1\}^n : Hv^t = 0\}$$

¿Cómo saber $\delta(C)$ a partir de la matriz de chequeo H?

$$\delta(C) = \min\{r : \text{ Existen r columnas de H linealmente dependientes}\}$$

¿Cómo calcular la dimensión de un código lineal a partir de la matriz de chequeo?

$$k = \text{Cant columnas} - \text{Cant filas}$$

Si H es una matriz que {{c2::no tiene la columna cero ni tiene columnas repetidas}}, entonces $C = Nu(H)$ {{c1::corrije al menos un error}}
Extra: $\delta \geq 3$

¿Cuando sucede que la matriz H corrije exactamente un error?

Cuando H no tiene la columnna cero, no tiene columnas repetidas y alguna columna es suma de otras dos u otras tres columnas
Extra: Las filas deben ser LI

{{c1::$H = [Id|A]$ matriz de chequeo}} $\Leftrightarrow$ {{c2::$G = [A^t|Id]$ matriz generadora}}

{{c1::$G = [Id|A]$ matriz generadora}} $\Leftrightarrow$ {{c2::$H = [A^t|Id]$ matriz de chequeo}}

¿Cuando un código es de Hamming? (Basado en la matriz de chequeo)

Cuando H es una matriz con todas las $2^r - 1$ columnas no nulas posibles.

¿Que caracteristica tienen los códigos de Hamming?

Son perfectos

¿Cómo es el algoritmo de corrección de un error?

1. Se recibe la palabra w
2. Se calcula Hw^t
3. Si $Hw^t = 0$, entonces w no tiene errores
4. Si $Hw^t \neq 0$, entonces $w + e_i$ es la palabra recibida, donde i es la posición del vector w en las columnas de H

¿Cómo construir un código que corrija un error?

Crear una matriz H de las dimensiones adecuadas que no tenga columnas nulas y que no tenga columnas repetidas

¿Que característica tiene la matriz H de los códigos de Hamming?

Contiene todas las columnas no nulas y no repetidas

¿Que forma tiene la matriz que decodifica 2^k palabras?

$$(r \times (r + k))$$

¿Que cota tiene el valor de r para que la matriz H decodifique 2^k palabras y corrija un error?

$$r + k \leq 2^r - 1$$

¿Que "variable/parametro" es la que debo saber para conocer cuantos errores detecta y corrige un código?

δ

¿Que es la longitud de un código?

La cantidad de bits que tiene cada palabra del código

¿Que es la dimensión de un código lineal en cantidad de bits?

La cantidad de bits que tiene cada mensaje que permite transmitir el código

¿Cómo obtener la longitud de un código lineal a partir de la matriz generadora?

La cantidad de columnas de la matriz generadora

¿Cómo obtener la dimensión de un código lineal a partir de la matriz generadora?

La cantidad de filas de la matriz generadora

¿Que permite verificar facilmente una matriz que tiene la Id como submatriz?

Que sus filas son linealmente independientes

¿Que relación hay entre la posición de la Id en la matriz generadora y el mensaje real que se transmite?

La posición de la Id en la matriz generadora indica los bits de la palabra recibida que corresponden al mensaje real

¿Cómo obtener δ a partir de la matriz generadora?

1. Construir la matriz de chequeo
2. Obtenerlo a partir de la matriz de chequeo

¿Que dimensiones tiene la matriz de chequeo?

$$((n-k) \times n)$$

¿Cómo obtener δ a partir de la matriz de chequeo? (Pasos)

1. Verificar si tiene columna 0 -> $\delta = 1$

2. Verificar si tiene columnas repetidas -> $\delta = 2$
3. Verificar si hay 3 columnas LD -> $\delta = 3$
4. Calcular por fuerza bruta

¿Que cosas SI se pueden concluir al recibir una palabra?

Que tuvo una cierta cantidad de errores

¿Que cosas NO se pueden concluir al recibir una palabra?

Cual fue la palabra originalmente enviada
Extra: Solo se puede decir cual es la palabra mas probable que se haya enviado

Los códigos de Hamming son {{c1::perfectos}}

¿Cuantas filas tiene un código de Hamming?

r

¿Cual es la dimensión de un código de Hamming?

$k = 2^r - r - 1$

¿Cuantas palabras tiene un código de Hamming?

$2^{2^r - r - 1}$

¿Cual es el δ de un código de Hamming?

3

¿Cuantos errores corrige un código de Hamming?

Exactamente 1

¿Cuales es el orden más comun de los códigos de Hamming para las columnas de la matriz de chequeo?

Es el que tiene como columna i-esima la representacion binaria del numero i

¿Cual es la ventaja de los códigos de Hamming para la corrección de errores en su orden más comun de las columnas de la matriz de chequeo?

Se obtiene la posición del error al calcular Hw^t

¿Cómo verificar/construir una palabra del código a partir de la matriz de chequeo?

Se calcula Hw^t y se verifica que sea 0

¿Que restricción tiene la matriz de chequeo para que su tamaño sea $((n-k) \times n)$?

Sus filas deben ser LI

¿Cómo se define r? (para códigos de hamming por ejemplo)

$$r = n - k$$