MATEMATICA DISCRETA II-2007
Códigos (matriz de chequeo)

1.Definición :

H es una matriz de chequeo de un código C si $C = Nu(H) = \{x : Hx^t = 0\}$

2.Teorema :

$[I|A]$ es una matriz de chequeo de un codigo C si y solo si $[A^t|I]$ es una matriz generadora de C, donde si la matriz A es $r \times k$, la primera "I" es $r \times r$ y la segunda "I" es $k \times k$.

Prueba:

Recordemos que H es una matriz de chequeo de C sii $C = Nu(H)$ y G es una matriz generadora de C sii $C = EF(G)$. Por lo tanto, el teorema se reduce a ver que $Nu[I|A] = EF[A^t|I]$.

Veamos primero la inclusiòn $EF[A^t|I] \subseteq Nu[I|A]$: Sea $v \in EF[A^t|I]$. Esto implica que existe un u tal que $v = u[A^t|I]$.

Entonces:

$$\begin{aligned}[I|A]v^t =& [I|A](u[A^t|I])^t \\ =& [I|A]\left[\frac{A}{I}\right]u^t \\ =& (A + A)u^t \\ =& 0\end{aligned}$$

la ultima igualdad pues estamos en $\boldsymbol{Z}_2$. Por lo tanto, $v \in Nu[I|A]$ y hemos probado la inclusion.

Pero entonces tenemos el teorema, pues observemos que la dimensión del espacio fila de una matriz de la forma $[A^t|I]$ es igual al numero de filas, en este caso, k. Por otro lado, el numero de columnas de $[I|A]$ debe ser igual al numero de columnas de I mas el numero de columnas de A, es decir $n = r + k$. Pero entonces, la dimension del nucleo de una matriz de la forma $[I|A]$ es igual a $n - rango[I|A] = n - r = k$. Asi, las dimensiones de estos espacios son iguales, y como uno esta incluido en el otro, deben ser el mismo espacio. QED.

3.Teorema (de la matriz de chequeo) :

Si una matriz de chequeo no tiene la columna cero ni columnas repetidas, entonces el codigo correspondiente a esa matriz corrige un error.

Prueba:

Sea H la matriz de chequeo, C el codigo, y denotemos por $H^{(j)}$ a la columna j-esima de H. Debemos ver que $\delta \geq 3$, pero como el codigo es lineal, basta ver que el menor peso de una palabra no nula del codigo es al menos 3. Supongamos que esto no sea cierto. Entonces, debe haber una palabra en el codigo de peso 1 o peso 2.

Supongamos primero que exista una palabra de peso 1. Entonces, si e_i denota el vector con con un 1 en la posicion i y cero en las demas, tenemos debe existir un j tal que e_j este en el codigo. Pero entonces, com $C = Nu(H)$, tenemos que $0 = He_j^t = H^{(j)}$, y esto dice que H tiene una columna cero, lo que contradice las hipotesis.

Por lo tanto, no have vectores de peso 1. Supongamos que hubiera uno de peso 2. Deberia ser entonces de la forma $e_i + e_j$, para algunos i, j distintos entre si.

Entonces: $0 = H(e_i + e_j)^t = He_i^t + He_j^t = H(i) + H(j)$. Pero como estamos en $\boldsymbol{Z}_2$, el hecho de que $H^{(i)} + H^{(j)} = 0$ implica que $H^{(i)} = H^{(j)}$, lo cual dice que H tiene dos columnas iguales, lo que contradice la hipotesis. QED.

Por lo tanto, construir códigos que corrigan un error, de la longitud que queramos, es facil: simplemente tomamos una matriz con n columnas que no tenga la columna cero ni columnas repetidas, y tendremos un codigo de longitud n que corregira un error.

Por ejemplo, la matriz:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}$$

es un matriz de chequeo cuyo codigo correspondiente tiene longitud 7, corrige un error, y tiene dimension 3. (la dimension sera el numero de columnas de la A en $[I|A]$, como vimos en la prueba del teorema con el cual comenzamos la clase).

Explicitamente, tomando este código es:

$$\begin{aligned} C =& \{w = w_1w_2...w_7 : Hw^t = 0\} \\ =& \{w = w_1w_2...w_7 : \begin{cases} w_1 = w_5 \oplus w_7 \\ w_2 = w_6 \oplus w_7 \\ w_3 = w_5 \oplus w_6 \oplus w_7 \\ w_4 = w_5 \oplus w_6 \end{cases} \} \end{aligned}$$

Como vemos, en vez de una sola ecuacion de paridad, aca tenemos 4 ecuaciones de paridad. LAs variables dependientes son w_1, w_2, w_3, w_4, y las indepenendientes son w_5, w_6, w_7, por lo que la dimension del codigo es 3, como dijimos antes. El codigo tiene entonces 8 palabras. Ellas son:

$$C = \left\{ \begin{matrix} 0000000 & 1110001 & 0111010 & 1001011 \\ 1011100 & 0101101 & 1100110 & 0010111 \end{matrix} \right\}$$

Observar que el codigo no es lo mas eficiente posible, porque la taza de transmisión es de $\frac{3}{7}$, mientras que podriamos haber construido un codigo que tambien tenga dimension 3 y corriga un error, pero con taza de transmisión $\frac{1}{2}$, simplemente tomando como H una matriz 3×6 sin la columna cero ni columnas repetidas. Por ejemplo, podriamos haber tomado la matriz:

$$\tilde{H} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

la cual da el codigo

$$\tilde{C} = \left\{ \begin{matrix} 000000 & 111001 & 011010 & 100011 \\ 110100 & 001101 & 101110 & 010111 \end{matrix} \right\}$$

Un detalle sin emabrgo, es que si bien $\tilde{C}$ y C corrigen ambos un error, es claro mirando sus palabaras que $\delta(\tilde{C}) = 3$ pero $\delta(C) = 4$. Con lo cual C detecta hasta tres errores, mientras que $\tilde{C}$ solo detecta dos. Dependiendo de la aplicacion,me sto puede o no ser relevante.

Obviamente no podemos hacer un codigo mas chico, porque si queremos que en $[I|A]$ A tenga k columnas, tales que no se repitan, no sean cero, y no sean iguales a ninguna de las columnas de la I (que es $r \times r$), entonces como las columnas seran $r \times 1$, y hay a lo sumo 2^r tales columnas, pero no puede estar la cero ni las r columnas de la identidad, tenemos que debemos tener un r tal que $k \leq 2^r - 1 - r$. En el caso de $k = 3$, esto dice que el r no puede ser 2, y por lo tanto el tamaño minimo de la matriz debe ser $3 \times (3 + 3) = 3 \times 6$. Por ejemplo, si quisieramos un codigo de dimension 5, deberiamos tener un r tal que $5 \leq 2^r - 1 - r$. El minimo tal r es $r = 4$, por lo tanto el tamaño minimo de la matriz debe ser $4 \times (4 + 5) = 4 \times 9$. Por ejemplo, la matriz:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Este codigo tiene entonces $2^5 = 32$ palabras, de longitud 9.

Una posibilidad es, por ejemplo, elejir un r, y luego tomar la matriz H formada por TODAS las columnas $r \times 1$ distintas de cero. Estos códigos se llaman **códigos de Hamming**, y los denotaremos por $\mathcal{H}_r$. Por supuesto, dependiendo de el orden en que ordenemos las columnas, tendremos distintos códigos, pero en general le llamaremos a todos "códigos de Hamming", aunque por convencion "el" codigo de Hamming suele ser el que tiene como columna i-esima la representacion binaria del numero i.

Por ejemplo, las matrices para $\mathcal{H}_r$ con $r = 2, 3, 4$ ordenando las columnas de esta forma, son:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Observar que el codigo de Hamming $\mathcal{H}_r$ tiene: $n = 2^r - 1$ columnas, dimension $k = 2^r - 1 - r$ y $\delta = 3$.(sabemos por el teorema que es al menos 3. Es exactamente 3 pues por ejemplo la palabra que tiene un uno en las posiciones 1,2,3 y cero en las demas, es una palabra del codigo siempre, si ordenamos las columnas como dijimos antes). Los codigso de Hamming tienen una propiedad muy improtante:

4.Propiedad :

Los códigos de Hamming son perfectos.

Prueba:

Debemos ver que $|C| = \frac{2^n}{1+n+\binom{n}{2}+...+\binom{n}{t}}$, donce t es la cantidad de errores que corrige. En nuestro caso, $t = 1$, $n = 2^r - 1$ y $|C| = 2^k = 2^{2^r-r-1}$, asi que es cuestion simplemente de colocar los numeros y verificarlos:

$$\begin{aligned} \frac{2^n}{1+n+\binom{n}{2}+...+\binom{n}{t}} &= \frac{2^n}{1+n} && (t=1) \\ &= \frac{2^n}{1+2^r-1} && (n = 2^r - 1) \\ &= 2^{n-r} \\ &= 2^{2^r-1-r} && (n = 2^r - 1) \\ &= |C| && (k = 2^r - r - 1) \end{aligned}$$

QED.

Ok, todo bien hasta ahora, sabemos como crear códigos que corrijan un error, y tenemos incluso toda una familia que son lo mas eficientes posibles. Pero, ¿como correjimos ese error?. En este caso, el algoritmo tambien es muy facil:

5.Algoritmo para correjir un error con códigos con matrices de chequeo :

Recibido un vector w que suponemos ha tenido a lo sumo un error de transmisión, realizar el producto Hw^t. Si ese producto es cero, aceptar w. Si ese producto es la columna j-esima de H, cambiarle el bit j a w. Si ese producto no es ninguna columna de H ni es cero, entonces la suposicion esta mal y ha habido al menos dos errores de transmisión. Pedir retransmisión.

Prueba:

Veamos que este algoritmo es correcto: supongamos que se manda v y llega w, con a lo sumo un solo error de transmisión.

Si no hubo errores, entonces $v = w$, y como v esta en el codigo, entonces $Hw^t = Hv^t = 0$.

Supongamos ahora que hay un error. Esto quiere decir que existe un j tal que $w = v \oplus e_j$. Por lo tanto, $Hw^t = Hv^t + He_j^t = 0 + H^{(j)} = H^{(j)}$. Es decir, hemos probado que, si hay a lo sumo un error, entonces, si no hay errores $Hw^t = 0$ y si hay un error $Hw^t = H^{(j)}$ donde j es el bit donde se produjo el error. Con lo cual, razonando hacia atras, si $Hw^t = 0$, (y suponemos a lo sumo un error), entonces, NO HUBO errores, pues si lo hubiera habido deberia haber dado una columna de H y H no tiene la columna 0. Por otro lado, si Hw^t es la columna j-esima de H, entonces sabemos que hubo un error, y en ese caso sabemos que el error estuvo en el bit j. Por lo tanto el algoritmo es correcto. QED.

6.Observacion :

Esto NO quiere decir que si $Hw^t = 0$ entonces no hubo errores, o que si $Hw^t = H^{(j)}$ entonces solo hubo un error, y en el bit j-esimo. Lo que dice el algoritmo es que SI HUBO a lo sumo un error, ENTONCES, esto que acabamos de decir es cierto. Pero pueda haber habido tres errores y tener $Hw^t = 0$, o puede haber habido dos errores, y tener $Hw^t = H^{(j)}$,etc.

Ejemplo:

sea H la matriz de chequeo:

$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Supongamos que se reciben las palabras $w = 100111100, x = 101001111, y = 110011001$. ¿Que hace el receptor en cada caso?

En el primer caso, $Hw^t = 0$, por lo tanto se acepta w. En el segundo caso:

$$Hx^t = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

que es la sexta columna de H, por lo tanto el recpetor aceptara la palabra $\tilde{x} = 101000111$ que se obtiene de x cambiandole el sexto bit. En el tercer caso:

$$Hy^t = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

que no es ningna columna de H, asi que el receptor pide retransmisión.

Observar que PODRIA haber sucedido que se mandara la palabra $v = 010101100$, la cual esta en el codigo, que hubiera habido tres errores, en los bits 1,2 y 5, y llega w y no nos dimos cuenta. O podria haberse mandado la palabra $z = 000001111$, que esta en el codigo, que hubiera habido dos errores, en los bits 1 y 3, y que llegara x. En este caso, SI nos dimos cuenta que hubo errores, porque no llega una palabra del codigo, pero suponiendo que hubo a lo sumo uno, lo correjimos mal.

En el caso del codigo de Hamming, como tiene todas las columnas, siempre que se produscan dos errores, esto equivaldra a sumar dos columnas, la cual va a dar otra columna, pues Hamming las tiene a todas, por lo tanto Hamming SIEMPRE corrige mal dos errores.

La decodificacion en el caso de Hamming ordenado como habiamos dicho arriba es todavia mas sencilla que el caso general: recibida w, se calcula Hw^t. Si es cero, se acepta w. Si no, es una columna que representa un numero en binario. Se cambia el bit correspondeite a ese numero y listo.

Para evitar el problema de que Hamming siempre corroge mal dos errores, a veces se usa el codigo de Hamming extendido: se agrega un bit extra de paridad. Este codigo ya no es perfecto, porque el n aumento en uno, pero si hay dos errores, no podremos corregirlos, pero sabremos que hubo dos errores y no uno, y se puede pedir retransmisión. Esto es porque agregar un bit extra equivale a tomar una matriz de chequeo ampliada a la cual se le agrega una fila y una columna. La fila es la fila con todos 1 y la ultima columna tiene ceros en las primeras filas y un uno en la ultima. Entonces, si se produce un error en un solo bit, es como antes: llegara la columna correspondiente. Pero si se producen dos errores, llegara la suma de dos columnas. Pero la suma de dos columnas tendra un cero en la ultima fila, y por lo tanto no sera una columna de la matriz, y el receptor sabra que debe pedir retransmisión.

Como dijimos la calse pasada, códigos perfectos hay pocos. Pero hay otra cota, y los códigos que la alcanzan tienen un nombre especial y son numerosos. Primero, geberalizemos el teorema de la matriz de chequeo:

7.Generalizacion del Teorema de la matriz de paridad: :
Si H es matriz de chequeo de C, entonces

$$\delta(C) = Min\{j : \exists \text{ un conjunto de } j \text{ columnas LD de } H\}$$

(esto generaliza el teorema, pues si H no tiene la columna cero ni tiene columnas repetidas, entonces todo conjunto de dos columnas de H es LI, con lo cual el numero minimo de columnas LD es 3).

Prueba:
Sea $\{H^{(j_1)}, H^{(j_2)}, ..., H^{(j_s)}\}$ un conjunto LD de columnas de H. Sea $v = e_{j_1} + e_{j_2} + ... + e_{j_s}$. Entonces, $Hv^t = H^{(j_1)} + H^{(j_2)} + ... + H^{(j_s)} = 0$ por ser LD, por lo tanto, $v \in C$. Como su peso es s, tenemos que $\delta \leq s$. Viceversa, si $v \in C$ tiene peso s, entonces la suma de las columnas correspondientes a los bits no nulos de v sera 0, i.e., esas columnas seran LD.
Por lo tanto, $\delta =$Min$\{s :$ existan s columnas LD de $H\}$. QED.

8.Corolario (Singleton bound) :
Sea C un codigo (n, k, δ). Entonces, $\delta \leq n - k + 1$.

Prueba:
Sea H matriz de chequeo de C. Tenemos que:

$$\begin{aligned}
\text{rango}(H) &= \text{Max}\{j : \text{Existe un conjunto LI de } j \text{ columnas de } H\} \\
&\leq \text{Max}\{j : \text{TODO un conjunto LI de } j \text{ columnas de } H\} \\
&= Min\{j : \exists \text{ un conjunto de } j \text{ columnas LD de } H\} - 1 \\
&= \delta - 1
\end{aligned}$$

Entonces $\delta \leq rango(H) + 1 = n - k + 1$. QED.

9.Definicion :
Códigos (n, k, δ) tales que $\delta = n - k + 1$ se llaman MDS codes (Maximum Distance Separable Codes).