

Proposición (Cota de Gilbert-Varshamov) Sean $n, k, d, q \in \mathbb{N}$ donde q es una potencia de un primo. Si

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i$$

entonces existe un $[[n, k, d]]$ código lineal con $d \geq d$.

Demostración

Veremos que si se cumple esa desigualdad entonces se puede definir una matriz H de tamaño $(n-k) \times n$ (que será la matriz de control del código) tal que cualquier conjunto de $d-1$ columnas es l.i.

Como primer columna tomemos cualquier vector no nulo $h_1 \in \mathbb{F}_q^{n-k}$ y como segunda columna cualquier vector no nulo $h_2 \in \mathbb{F}_q^{n-k}$ que no sea múltiplo de h_1 . En general para elegir la i -ésima columna h_i elegimos $h_i \in \mathbb{F}_q^{n-k}$, $h_i \neq 0$ y tal que $h_i \notin \langle h_{i_1}, \dots, h_{i_j} \rangle$

donde $1 \leq i_1 < i_2 < \dots < i_j < i-1$ es decir que h_i no sea combinación lineal de

$j \leq d-2$

cualquier conjunto de columnas previamente elegidas.

Pero el número de combinaciones lineales N_i de $d-2$ columnas o menos, de las existentes

$$a_{i1} h_{i1} + a_{i2} h_{i2} + \dots + a_{i_{d-2}} h_{i_{d-2}}$$

$$N_i = \binom{i-1}{1} (q-1) + \binom{i-1}{2} (q-1)^2 + \binom{i-1}{3} (q-1)^3 + \\ + \dots + \binom{i-1}{d-2} (q-1)^{d-2}$$

$$= \sum_{j=1}^{d-2} \binom{i-1}{j} (q-1)^j$$

Luego hay $q^{n-k} - N_i - 1$ elecciones para

la columna i -ésima, si ese cantidad es positiva.

$$\text{Así } q^{n-k} > N_{n+1} = \sum_{j=0}^{d-2} \binom{n-1}{j} (q-1)^j$$

tenemos que $q^{n-k} - N_{n-1} > 0$ y podemos completar H con n columnas de manera que cualquier conjunto de $d-1$ columnas sea l.i.

Finalmente definiendo

$$C = \{x \in \mathbb{F}_q^n : xH^T = 0\}$$

tenemos que C es un $[n, k, d_k]$ código con $d_k \geq d$, sobre $\mathbb{F}_q$.



Decodificación de códigos lineales

Vamos a ver ahora un algoritmo de decod.
propuesto por Stepien (1860) que aprovecha
la estructura de e.v. del cociente

$$\mathbb{F}_q^n / C$$

donde C es un $[n, k, d]$ -código lineal sobre $\mathbb{F}_q$.

$\mathbb{F}_q^n / C$ está formado por las clases

$$a + C = \{ a + c : c \in C \}$$

para $a \in \mathbb{F}_q^n$ con las operaciones

$$\begin{aligned} \alpha \cdot (a + C) &= \alpha \cdot a + C & \alpha \in \mathbb{F}_q \\ (a + C) + (b + C) &= (a + b) + C & a, b \in \mathbb{F}_q^n. \end{aligned}$$

La cantidad de clases $|\mathbb{F}_q^n / C| = q^{n-k}$ y

cada clase contiene exactamente q^k vectores.

Def. Sea C un $[n, k, d]$ -código sobre $\mathbb{F}_q$ con matriz de chequeos de paridad H . El vector

$$S(y) = y \cdot H^T$$

de longitud $n-k$ se llama el síndrome de y , $y \in \mathbb{F}_q^n$.

Teorema: Si $y, z \in \mathbb{F}_q^n$ entonces

1) $S(y) = 0$ si y sólo si $y \in C$ ← por def. de H .

2) $S(y) = S(z)$ si y sólo si $y + C = z + C$.

Demostación

$$2) \quad S(y) = S(z) \Leftrightarrow yH^T = zH^T \Leftrightarrow yH^T - zH^T = 0$$

$$\Leftrightarrow (y-z)H^T = 0 \Leftrightarrow y-z \in C \Leftrightarrow y-z = c \in C.$$

$$\Leftrightarrow y + C = z + C$$



Luego tenemos que el síndrome es invariante en los elementos de una clase.

Supongamos que se envía una palabra código $c \in C$ y se recibe $y \in \mathbb{F}_q^n$ $y \neq c$. Entonces el error cometido es

$$e = y - c$$

$$y \quad S(e) = S(y - c) = (y - c)H^T = \underbrace{yH^T}_{S(y)} - \underbrace{cH^T}_0 = S(y)$$

es decir, la palabra recibida y el error cometido están en la misma clase, y se puede utilizar el líder de la clase para encontrar ese error.

Def: un elemento de peso mínimo en una clase $a+C$ se llama líder de la clase $a+C$. Si hay varios vectores en $a+C$ de peso mínimo, se elige cualquiera de ellos como líder de la clase.

El proceso de decodificación se realiza utilizando el llamado arreglo estándar o arreglo síndromo por C .

$$\begin{array}{rcll}
 & 0 & \tilde{c}_1 G & \tilde{c}_2 G \dots \tilde{c}_r G & C \in [n, k, d] \\
 \text{clase de } 0 \leftarrow & 0 & c_1 & c_2 \dots c_r & |C| = q^k \\
 \text{clase de } a_1 \leftarrow & a_1 & a_1 + c_1 & a_1 + c_2 \dots a_1 + c_r & \\
 & a_2 & a_2 + c_1 & a_2 + c_2 \dots a_2 + c_r & \\
 & \vdots & & & \\
 & a_s & a_s + c_1 & a_s + c_2 \dots a_s + c_r &
 \end{array}$$

donde $r = q^k - 1$ $s = q^{n-k} - 1$.

En el arreglo anterior la primera fila tiene todas las palabras del código (clase de 0).

Para la segunda fila elegimos una palabra a_1 de peso mínimo que no esté en la primera fila y armamos la clase de a_1 .

En general para la i -ésima fila tomamos a_i de peso mínimo que no esté en las anteriores $i-1$ filas. El proceso va a terminar en la fila $s = q^{n-k} - 1$ pues

$$\mathbb{F}_q^n = (0 + C) + (a_1 + C) + \dots + (a_s + C)$$

Notar que en ese arreglo todas las palabras de una misma fila tienen el mismo síndrome.

Entonces si se recibe un vector $y \in \mathbb{F}_2^n$, calculamos $S(y)$ y buscamos el líder de clase con el mismo síndrome, digamos e . Luego sabemos que la palabra enviada era $c = y - e$.

Ejemplo: Consideremos el código binario $[4, 2, 2]$ cuyas matrices generadora y de control son

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

$$C = \{ x \cdot G : x \in \mathbb{F}_2^2 \} =$$

$$= \left\{ \begin{matrix} (0,0) \\ (0,0,0,0) \end{matrix}, \begin{matrix} (0,1) \\ (0,1,1,1) \end{matrix}, \begin{matrix} (1,0) \\ (1,0,1,0) \end{matrix}, \begin{matrix} (1,1) \\ (1,1,0,1) \end{matrix} \right\}$$

$(0,0,0,0)$	$(0,1,1,1)$	$(1,0,1,0)$	$(1,1,0,1)$
$(1,0,0,0)$	$(1,1,1,1)$	$(0,0,1,0)$	$(0,1,0,1)$
$(0,1,0,0)$	$(0,0,1,1)$	$(1,1,1,0)$	$(1,0,0,1)$
$(0,0,0,1)$	$(0,1,1,0)$	$(1,0,1,1)$	$(1,1,0,0)$

$e_0 = (0 \ 0 \ 0 \ 0)$	$(0 \ 1 \ 1 \ 1)$	$(1 \ 0 \ 1 \ 0)$	$(1 \ 1 \ 0 \ 1)$
$e_1 = (1 \ 0 \ 0 \ 0)$	$(1 \ 1 \ 1 \ 1)$	$(0 \ 0 \ 1 \ 0)$	$(0 \ 1 \ 0 \ 1)$
$e_2 = (0 \ 1 \ 0 \ 0)$	$(0 \ 0 \ 1 \ 1)$	$(1 \ 1 \ 1 \ 0)$	$(1 \ 0 \ 0 \ 1)$
$e_3 = (0 \ 0 \ 0 \ 1)$	$(0 \ 1 \ 1 \ 0)$	$(1 \ 0 \ 1 \ 1)$	$(1 \ 1 \ 0 \ 0)$

Supongamos que recibimos $y = (1 \ 1 \ 1 \ 0)$

$$S(y) = (1 \ 1 \ 1 \ 0) \begin{pmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (1 \ 1)$$

$$S(e_0) = (0 \ 0) \quad S(e_1) = (1, 0)$$

$$S(e_2) = (1 \ 1) \quad S(e_3) = (0, 1)$$

y proviene $(1 \ 0 \ 1 \ 0)$ palabra

código y por lo tanto

se decodifica como $\underbrace{(1, 0)}$
mensaje original.

Notar que no es necesario almacenar la tabla completa, sino solamente necesitamos guardar los líderes de las clases y sus correspondientes síndromes

Líderes	Síndromes
$e_0 = (0000)$	(00)
$e_1 = (1000)$	$(1,0)$
$e_2 = (0100)$	$(1,1)$
$e_3 = (0001)$	$(0,1)$

$$y \rightarrow S(y) \rightarrow c = y - e_i$$

$$\vec{x} \cdot \vec{y} = (x_1, \dots, x_n) \cdot (y_1, \dots, y_n)$$

$$= x_1 y_1 + x_2 y_2 + \dots + x_n y_n.$$

$$C^\perp = \left\{ y \in \mathbb{F}_2^n : y \cdot c = 0 \quad \forall c \in C \right\}$$

Subspaces

$$C = C^\perp$$

$$\{x : x \cdot H^T = 0\}.$$

$$(G, H^T)^T = 0^T$$

$$H^T \cdot G^T = 0$$

$$H \cdot G^T = 0.$$