

$[n, k, d]$ - código $\mathcal{C}$

$\mathbb{F}_q$

k : dimensión

n : longitud

d : distancia mínima

$$\mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$$

Ejemplo: Consideremos el código binario ($\mathbb{F}_2$) dado por la siguiente matriz: (generadora)

$$G = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}_{k \times n}$$

$$\mathbb{F}_2^2 \rightarrow \mathbb{F}_2^4$$

$$\mathcal{C} = \{c_1, c_2, c_3, c_4\}$$

$$(0,0) \rightarrow c_1 = (0 \ 0 \ 0 \ 0)$$

$$(0,1) \rightarrow c_2 = (0 \ 1 \ 0 \ 1) \rightarrow w(c_2) = 2$$

$$(1,0) \rightarrow c_3 = (1 \ 0 \ 1 \ 1) \rightarrow w(c_3) = 3$$

$$(1,1) \rightarrow c_4 = (1 \ 1 \ 1 \ 0) \rightarrow w(c_4) = 3$$

$\mathcal{C}$ es un $[4, 2, 2]$ - código binario. $\leadsto$ detecta hasta 1 error.

$$(0 \ 0 \ 0 \ 0) \leadsto (1 \ 0 \ 1 \ 0)$$

$$(0,0) \rightarrow (0 \ 0 \ 0 \ 0) \leadsto (0 \ 0 \ 1 \ 0) = y$$

$$d(y, c_1) = 1$$

$$d(y, c_2) = 3$$

$$d(y, c_3) = d(y, c_4) = 2$$

$$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$$

este código no puede corregir errores

$$c_2 = (0 \underset{\uparrow}{1} 0 1) \rightsquigarrow y = (0 0 0 1)$$

$$\begin{aligned} d(y, c_1) &= 1 \nearrow \\ d(y, c_2) &= 1 \searrow \end{aligned}$$

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

$$G = \left(\begin{array}{cc|cc} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right)_{k \times n} \rightarrow H = \left(\begin{array}{cc} -B^T & I_{22} \end{array} \right)$$

$\underbrace{\quad}_{I_{2 \times 2}} \quad \underbrace{\quad}_B$

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

$$y H^T = 0 \iff y \in C$$

$$c_2 H^T = (0 1 0 1) \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = (0, 2) = (0, 0)$$

$$(0 0 0 1) H^T = (0 1) \neq (0 0) \Rightarrow (0 0 0 1) \notin C.$$

$$(d-1)$$

Ejercicio 1: Considerando $H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}_{3 \times 6}$

encontrar la generadora G del código binario asociado a H como matriz de paridad. Listar las palabras de C y determinar los parámetros de C . $[n, k, d]$.

El siguiente resultado es útil para determinar la distancia mínima de un código.

Teorema: Sea C un $[n, k, d]$ -código y sea H es una matriz de control para C entonces

$$d = \min \{ r : \text{hay } d \text{ columnas de } H \text{ que L.D.} \}$$

Es decir, H tiene d columnas L.D pero cualquier conjunto de $d-1$ columnas es L.I.

Demostración

$$H = \begin{pmatrix} H_1 & H_2 & \dots & H_n \end{pmatrix}_{(n-k) \times n} \quad \text{donde } H_i \text{ es la columna } i\text{-ésima de } H$$

Entonces si $c = (c_1, c_2, \dots, c_n)$ es una palabra código $c \in C$ entonces

$$c H^T = \vec{0}$$

$$0 = c H^T = (c_1 \ c_2 \ \dots \ c_n) \begin{pmatrix} H_1^T \\ H_2^T \\ \vdots \\ H_n^T \end{pmatrix} = c_1 H_1^T + c_2 H_2^T + \dots + c_n H_n^T$$

Supongamos que H tiene t columnas l.d. con $t < d$

entonces existe una combinación lineal de esas t columnas con coeficientes no nulos.

$$a_1 H_{i_1} + \dots + a_t H_{i_t} = 0 \quad a_1, \dots, a_t \text{ no todos nulos.}$$

Usando esos coeficientes podríamos

armar una palabra $(c_1, \dots, c_n)$ que será una palabra código pero cuyo peso es menor o igual a $t < d$

y esto no es posible.

$c_i = a_i$ para las posiciones i_j $j=1, \dots, t$.

Luego debe haber d o más columnas l.d.

Por otro lado, si c es una palabra de peso mínimo, hay d columnas l.d. (usando los coef. no nulos de c).



El resultado anterior puede usarse para construir códigos lineales con distancia mínima el prefijo de.

Veremos ahora 2 cotos muy importantes y conocidos que relacionan los parámetros n, k, d de un código lineal.

Proposición (Cote de Singleton) Si C es un $[n, k, d]$ -código entonces

$$k + d \leq n + 1.$$

Demostración

Si consideramos el subespacio vectorial $E \subset \mathbb{F}_q^n$ dado por

$$E = \{ (a_1, \dots, a_n) \in \mathbb{F}_q^n : a_i = 0 \ \forall i \geq d \}$$

entonces $w(a) \leq d-1$ para cualquier palabra $a \in E$.

Como $w(c) \geq d$ para todo $c \in C$, $c \neq 0$ entonces

$$C \cap E = \{0\} \quad \rightarrow \quad \dim(E+C) = \overbrace{\dim E}^{d-1} + \dim C$$

$$k + d - 1 = \dim C + \dim E = \dim(E+C) \leq \dim(\mathbb{F}_q^n) = n$$

$$\therefore k + d \leq n + 1.$$



Los códigos cuyos parámetros alcanzan la igualdad en la cota de Singleton se llaman MDS (por "maximum distance separables") ya que tienen la mayor distancia posible dada una longitud y una dimensión fijos.

El próximo resultado es un resultado de existencia que establece que si n, k, d y q cumplen cierta desigualdad, entonces existe un código con esos parámetros. Mas aún, la demostración da una idea para construirlo.

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 $[n, k, d_q]$ código lineal con $d_q \geq d$.

Observación: En particular para $q=2$ el resultado anterior establece la existencia de un $[n, k, d]$ -código binario si

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

por ejemplo si $n=7$ y $d=3$ $2^{7-k} > \binom{6}{0} + \binom{6}{1} = 7$

$$[n, k, d] = [7, k, 3] \quad 2^{7-k} > 7$$

Luego existen códigos binarios de long. 7 y dist. mínima 3 por los dimensiones 1, 2, 3 y 4.

Simplificar
↓
 $k=5$

??

$S+3 = 8 = 7+1$