COTAS DE LOS PARÁMETROS DE CÓDIGOS LINEALES

EL OTRO DÍA (15 DE OCTUBRE) VIMOS LA COTA DE SINGLETON QUE NOS DICE QUE LOS PARÁMETROS DE UN CÓDIGO LINEAL $[n, k, d]_q$ VERIFICAN

$$n+1 \geq k+d$$

$[10,6,6]$ NO

$[10,5,5]$ $\Big\}$ IGUAL SI / IGUAL NO

ES DECIR DADO n Y k, LA MAYOR DISTANCIA MÍNIMA QUE SE PODRÍA CONSEGUIR ES $n+1-k$. $(d \leq n+1-k)$

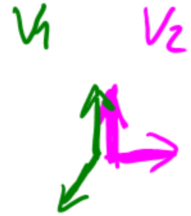
HOY VEMOS MÁS COTAS SUPERIORES (COMO LA DE SINGLETON) Y UNA COTA INFERIOR (NOS VA A ASEGURAR LA EXISTENCIA DE CÓDIGOS CON CIERTOS PARÁMETROS)

DADO n, k $\Bigg\{$
- COTA SUPERIOR: $d \leq$ ALGO
- COTA INFERIOR: $\exists$ CÓDIGO $[n,k,d]$, CON $d \geq$ ALGO

Th: Cota de Plotkin

Sea C un código $[n,k,d]_q$. Entonces

$$d \le \frac{n\, q^{k-1}(q-1)}{q^k-1}$$



DEM

Para dos espacios vectoriales V_1 y V_2 se tiene

$$\underset{k}{\overset{2}{\dim(V_1)}} + \underset{n-1}{\overset{2}{\dim(V_2)}} = \underset{\substack{(*)\ n \\ (**)\ n-1}}{\overset{3}{\dim(V_1+V_2)}} + \underset{\substack{k-1 \\ k}}{\overset{1}{\dim(V_1\cap V_2)}}$$

Nosotros tomamos $V_1 = C$ y $V_2 = \{\vec{x}\in \mathbb{F}_q^n \mid x_i = 0\}$

$$\Rightarrow \dim(V_1\cap V_2) = \begin{cases} k-1 \\ k \end{cases}$$

(*) Si $V_1 = C$ y tiene $\vec{x}\in C \mid x_i \neq 0 \Rightarrow V_2 \subsetneq V_1+V_2$ →

(**) Si $V_1 = C$ y $x_i = 0\ \forall \vec{x}\in C$

↳ $C = \langle (0,1,2,3),\ (0,4,5,6)\rangle$

$i=1 \quad n=4$

$V_2 = \langle \vec{e}_2, \vec{e}_3, \vec{e}_4 \rangle$

$\vec{e}_2 = (0,1,0,0)$

$\vec{e}_3 = (0,0,1,0)$

$\vec{e}_4 = (0,0,0,1)$

$C = \langle (1,*,*,*) \rangle$

ES DECIR, TENEMOS SIEMPRE q^k o q^{k-1} PALABRAS EN EL CÓDIGO CON LA COORDENADA i-ÉSIMA IGUAL A CERO

↳ ($\in$ A $V_1 \cap V_2$)

$$\sum_{\vec{c} \in C} w(\vec{c}) \leq \sum_{i=1}^{n} q^k - q^{k-1} = n(q^k - q^{k-1}) \quad (*)$$

COMO C TIENE DISTANCIA MÍNIMA d, TODAS LAS PALABRAS DEL CÓDIGO TIENEN PESO $\geq d$

$$\sum_{\vec{c} \in C} w(\vec{c}) \geq d(\overbrace{q^k}^{\#C} - \underbrace{1}_{\text{POR EL } \vec{0}}) \quad (**)$$

$(*) + (**)$: $$d(q^k - 1) \leq \sum_{\vec{c} \in C} w(\vec{c}) \leq n(q^k - q^{k-1})$$

$$d(q^k-1) \leq n(q^k-q^{k-1})$$

$$d \leq \frac{n(q^k-q^{k-1})}{q^k-1} = \frac{n q^{k-1}(q-1)}{q^k-1} \qquad \blacksquare$$

EJEMPLO DONDE SE DA IGUALDAD: CÓDIGO DE HAMMING.

LEMA: EXISTEN $\binom{n}{r}(q-1)^r$ VECTORES EN $\mathbb{F}_q^n$ DE PESO EXACTAMENTE r.

$\binom{n}{r}(q-1)^r$ EN r POSICIONES

ESCOGEMOS r POSICIONES

POSIBLES VALORES $\neq 0$

DEM:

$\binom{n}{r}$ FORMAS ESCOGER r ELEMENTOS DE UN CONJUNTO DE n ELEMENTOS

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

QUEREMOS VECTORES DE PESO r: $\overbrace{(*, 0, 0, *, \ldots, *, 0)}^{n}$

r - POSICIONES $\neq 0$ $\neq 0$ $\neq 0$

ESCOGEMOS r POSICIONES ¿DE CUANTAS MANERAS? $\binom{n}{r}$

EN CADA UNA DE ESAS r POSICIONES ESCOGEMOS UN VALOR $\neq 0$ ¿DE CUANTAS MANERAS? $(q-1)$

PERO AL HABER r-POSICIONES: $(q-1)\cdots(q-1) = (q-1)^r$

DEF: LLAMAMOS $V_q(n,t)$ A LA BOLA DE CENTRO $\vec{0}$ Y RADIO $t \geq 0$ EN $\mathbb{F}_q^n$

$V_q(n,t) = \{\vec{x} \in \mathbb{F}_q^n \mid \underbrace{d(\vec{0},\vec{x})}_{w(\vec{x})} \leq t\}$

LEMA:

$$\#V_q(n,t) = \overset{\text{PESO } 0}{1} + \overbrace{\binom{n}{1}(q-1)}^{\text{PALABRAS PESO } 1} + \cdots + \overbrace{\binom{n}{t}(q-1)^t}^{\text{PALABRAS PESO } t}$$

PALABRAS

$$= \sum_{i=0}^{t} \binom{n}{i}(q-1)^i$$

DEM: APLICAR EL LEMA ANTERIOR PARA LOS PESOS $0, 1, 2, \ldots, t$ QUE NOS DA LAS PALABRAS QUE ESTÁN A DISTANCIA MENOR O IGUAL QUE t.

NOTA: CUALQUIER OTRA BOLA CENTRADA EN CUALQUIER PALABRA DE $\mathbb{F}_q^n$ CONTIENE EL MISMO NÚMERO DE ELEMENTOS (C CÓDIGO LINEAL , w NORMA)

Th: COTA DE HAMMING

SEA C UN CÓDIGO DE LONGITUD n Y CAPACIDAD CORRECTORA $t\left(=\left\lfloor\frac{d-1}{2}\right\rfloor\right)$. ENTONCES

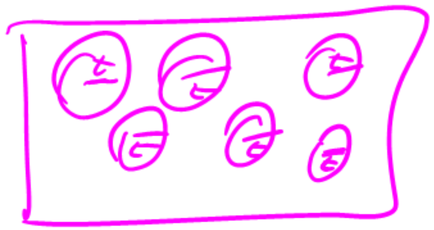
$$\#V_q(n,t) \le q^{n-k}$$

$q^k \# V_q(n,t) \le q^n$

(PARA CÓDIGOS NO LINEALES $\underbrace{(\#C)}_{q^k}\cdot V_q(n,t) \le q^n$)

DEM: PARA QUE UN CÓDIGO TENGA CAPACIDAD CORRECTORA t, LAS BOLAS CON RADIO t Y CENTRO LAS PALABRAS DEL CÓDIGO DEBEN SER DISJUNTAS

$$\underbrace{q^k}_{\text{PALABRAS EN } C}\ \underbrace{V_q(n,t)}_{\#\text{BOLA RADIO } t} \le \underbrace{q^n}_{\text{PALABRAS EN } \mathbb{F}_q^n}$$



LOS CÓDIGOS QUE VERIFICAN LA COTA DE HAMMING SE LLAMAN CÓDIGOS PERFECTOS.

HAY MUY POCOS: LOS DE HAMMING Y GOLAY

TIENEN LA PROPIEDAD DE QUE EN LA DECODIFICACIÓN POR SÍNDROME, TODA CLASE TIENE LIDER.

(DADO QUE HEMOS LLENADO EL ESPACIO DE BOLAS)

AHORA VEMOS UNA COTA INFERIOR QUE GARANTIZA LA EXISTENCIA DE UN CÓDIGO CON CIERTOS PARÁMETROS.

Th: COTA DE GILBERT-VARSHAMOV

SI $q^{n-(k-1)} > \# V_q(n, d-1)$ ENTONCES EXISTE UN CÓDIGO DE PARÁMETROS $[n, k, \geq d]_q$

DEM: CONSTRUIMOS INDUCTIVAMENTE UNA BASE, Y POR TANTO, UNA MATRIZ GENERADORA

$\vec{c}_1 :=$ CUALQUIER VECTOR DE PESO $\geq d$ (DE $\mathbb{F}_q^n$)

$\vec{c}_2 :=$ CUALQUIER VECTOR DE PESO $\geq d$ TAL QUE

$\{\vec{c}_1, \vec{c}_2\}$ LIN. INDEPENDIENTES

$d(\underbrace{\langle \vec{c}_1, \vec{c}_2 \rangle}_{C_2}) \geq d$

⋮

$\vec{C}_{j-1} :=$ CUALQUIER VECTOR DE PESO $\geq d$ TAL QUE

$\{\vec{C}_1, \ldots, \vec{C}_{j-1}\}$ LIN. INDEPENDIENTES

$d(\underbrace{<\vec{C}_1, \ldots, \vec{C}_{j-1}>}_{C_{j-1}}) \geq d$

SI HACEMOS ESTO, TENEMOS UN CÓDIGO $[n, j-1, \geq d]$

PERO, ¿HASTA CUANDO PODEMOS HACER ESTO?

SI $j-1 = k$ HEMOS GANADO, PERO SI $j-1 < k$ ENTONCES

$$q^{j-1} V_q(n, d-1) < q^n$$

COMO

POR LA HIPÓTESIS DEL RESULTADO $\left(q^{k-1} V_q(n, d-1) < q^n \right)$

POR LO QUE EXISTE UN VECTOR DE $\mathbb{F}_q^n$ A DISTANCIA

AL MENOS d DE TODAS LAS PALABRAS DE C_{j-1}

LLAMAMOS $\vec{c}_j$ A CUALQUIER VECTOR FUERA DE LAS BOLAS DE CENTRO UNA PALABRA C_{j-1} Y RADIO $d-1$

LLAMAMOS $C_j = \langle \vec{c}_1, \dots, \vec{c}_{j-1}, \vec{c}_j \rangle$

C_j ES UN CÓDIGO $[n, j, d]$ PORQUE

SI $\vec{x} \in C_j \setminus C_{j-1}$, $\vec{x} = \underset{\neq 0}{\lambda} \vec{c}_j + \vec{y}$, CON $\vec{y} \in C_{j-1}$

$$w(\vec{x}) = w(\underset{\neq 0}{\lambda^{-1}} \vec{x}) = w(\vec{c}_j + \lambda^{-1}\vec{y}) = d(\vec{c}_j, \underbrace{-\lambda^{-1}\vec{y}}_{\in C_{j-1}}) \geq d$$

$w(\vec{a} - \vec{b}) = d(\vec{a}, \vec{b})$

$\vec{c}_j$ FUERA BOLAS

$\square$

EJERCICIO: USA LA COTA DE GILBERT-VARSHAMOV PARA DETERMINAR K TAL QUE EXISTA UN CÓDIGO BINARIO CON PARÁMETROS [15, K, 5]