OTROS CÓDIGOS LINEALES

LA PRINCIPAL LIMITACIÓN DE LOS CÓDIGOS REED-SOLOMON ES QUE SU LONGITUD ESTÁ LIMITADA POR EL TAMAÑO DEL CUERPO ($n \leq q$)

HAY MÁS FAMILIAS DE CÓDIGOS QUE TRATAN DE APORTAR ALTERNATIVAS PARA TENER CÓDIGOS MÁS LARGOS.

UNA POSIBILIDAD ES CONSIDERAR POLINOMIOS EN MÁS VARIABLES, TENEMOS ASÍ LOS CÓDIGOS REED-MULLER.

RS $\quad f \in \mathbb{F}_q[X] \quad , \mathcal{P} = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q \quad (f(P_1), \ldots, f(P_n))$

CÓDIGOS REED-MULLER

$\mathcal{P} = \{P_1, \ldots, P_n\} = \mathbb{F}_q^m$ $\quad n = q^m$ $\quad P_i = (P_{i1}, \ldots, P_{im})$

EVALUAMOS POLINOMIOS EN VARIAS VARIABLES

$$f = \sum_{i_1, \ldots, i_m} a_{i_1 \ldots i_m} X_1^{i_1} \cdots X_m^{i_m}$$

$f \in \mathbb{F}_q[X_1, \ldots, X_m]$

$$(f(P_1), \ldots, f(P_n))$$ ← ASÍ CODIFICAMOS

CONSIDERAMOS LOS POLINOMIOS DE GRADO $\leq r$

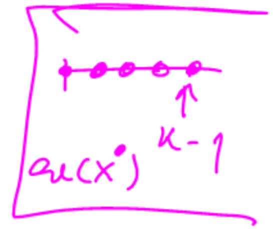
$$\mathbb{F}_q[X_1, \ldots, X_m]^{(r)} = \{ f \in \mathbb{F}_q[X_1, \ldots, X_m] \;/\; \deg f \leq r \}$$

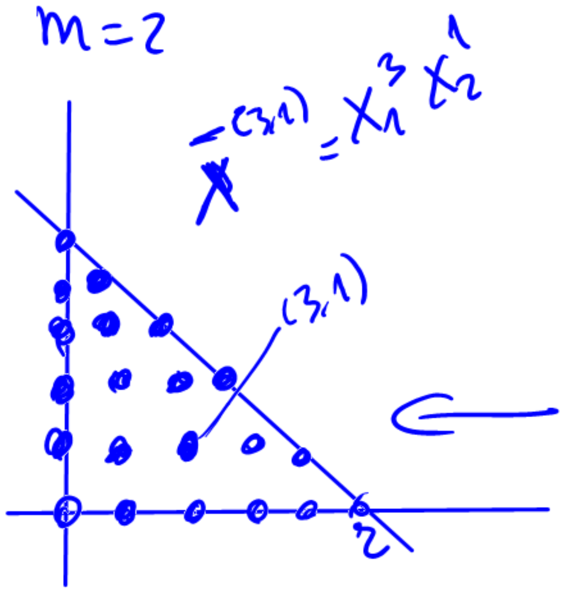
$\deg(X_1^{i_1} \cdots X_m^{i_m}) = i_1 + \cdots + i_m$ $\qquad \deg(X_1^2 X_2^3) = 5$

$$ev : \mathbb{F}_q[X_1, \dots, X_m]^{(r)} \longrightarrow \mathbb{F}_q^{\,n}$$

$$f \longmapsto (f(P_1), \dots, f(P_m))$$

$$RM_q(r,m) = \mathrm{Im}(ev) \qquad n = q^m$$



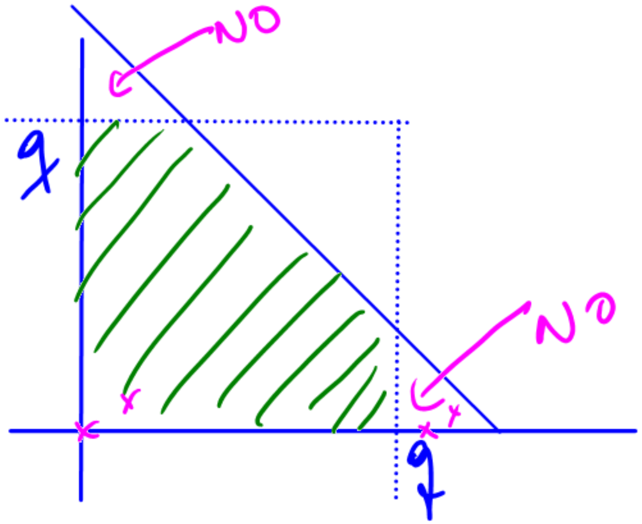


$\dim RM_q(r,m) = \#\{\bullet$ PUNTOS EN $\blacktriangle\}$

$\Leftarrow$ $ev(\bar{X}^{\bullet})$ ES UNA BASE

LEMA: SI $r \geq m(q-1) \Rightarrow RM_q(r,m) = \mathbb{F}_q^{\,n}$

$a^q = a$ en $\mathbb{F}_q$



$X \neq X^q$

$a(X) = a(X^q)$

EJ: $\mathbb{F}_2$ $m=3$ $n=2^3=8$

GRADO 0: 1 $RM_2(0,3) = \langle ev(1) \rangle$

GRADO 1: X_1, X_2, X_3

GRADO 2: X_1X_2, X_1X_3, X_2X_3, $\cancel{X_1^2, X_2^2, X_3^2}$

GRADO 3: $X_1X_2X_3$

$$RM_2(2,3) = \langle ev(1), ev(X_1), ev(X_2), ev(X_3), ev(X_1X_2), ev(X_1X_3), ev(X_2X_3) \rangle$$

$$\dim RM_2(2,3) = 7$$

$$G = \begin{pmatrix} ev(1) \\ ev(X_1) \\ \vdots \\ ev(X_2X_3) \end{pmatrix}$$

$ev(X_1X_2) = (0,0,0,0,0,0,1,1)$

FILA 5

$$\left\{ \begin{matrix} (000) & (100) \\ (001) & (101) \\ (010) & (110) \\ (011) & (111) \end{matrix} \right\} = P$$

FÓRMULA PARA LA DIMENSIÓN:

$$\dim(RM_q(r,m)) = \sum_{t=0}^{r}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\binom{t-iq+m+1}{t-iq}$$

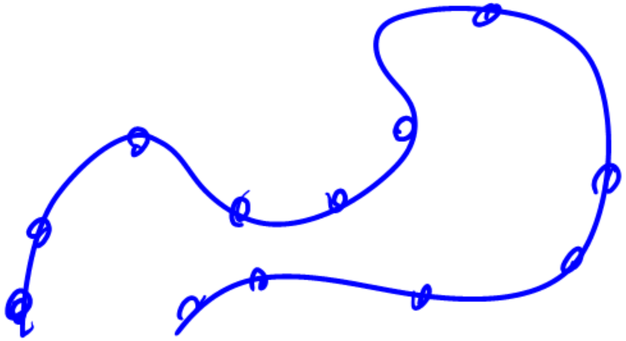
SI $q=2 \Rightarrow K = \sum_{t=0}^{r}\binom{m}{t}$

FÓRMULA PARA LA DISTANCIA MÍNIMA:

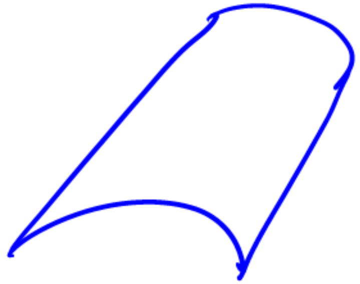
SI $r = v(q-1)+s$, CON $0 \leq s < q-1$

$$d(RM_q(r,m)) = (q-s)\,q^{m-v-1}$$

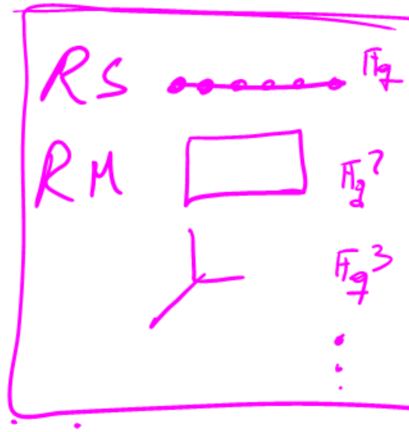
CÓDIGOS ALGEBRO-GEOMETRICOS



CURVAS ,



SUPERFICIES , ...



SE EVALUAN FUNCIONES $\left(\frac{F(x)}{G(x)}\right)$ CON CEROS Y POLOS ACOTADOS POR UNOS CIERTOS VALORES EN UNOS PUNTOS, Y SE EVALUAN EN OTROS PUNTOS DE UNA CURVA, SUPERFICIE, ...

- SE USAN TÉCNICAS DE GEOMETRÍA ALGEBRAICA
- PRODUCEN MUY BUENOS CÓDIGOS: SUPERANDO LA COTA ASINTÓTICA DE GILBERT-VARSHAMOV

CÓDIGOS CÍCLICOS

$$(c_0, \_\_, c_{n-1}) \in C \Rightarrow (c_{n-1}, c_0, c_1, \_\_, c_{n-1}) \in C$$

$$(1,2,3,4) \in C \Rightarrow (4,1,2,3) \in C \Rightarrow (3,4,1,2) \in C \Rightarrow$$

$$\Rightarrow (2,3,4,1) \in C$$

$$X(c_0 + c_1 X + \_\_ + c_{n-1} X^{n-1}) = c_0 X + c_1 X^2 + \_\_ + c_{n-2} X^{n-1}$$

$$+ c_{n-1} \cancel{X^n}$$

$$1$$

$$= c_{n-1} + c_0 X + \cdots + c_{n-2} X^{n-1}$$

$$\boxed{\mathbb{F}[X] / \langle X^n - 1 \rangle}$$

CODIGOS CICLICOS $\longleftrightarrow$ IDEAL EN ESTE ANILLO

CÓDIGOS SUBCUERPO

$C \subset \mathbb{F}_{2^m}^n$ $\qquad (\alpha, 1, 0, \alpha, \ldots\ldots) \in C$

$C \cap \mathbb{F}_2^n$ $\qquad C \quad [n, k, d]_{2^m}$

$C \cap \mathbb{F}_2^n \quad [n, k', \geq d]_2$

$\boxed{k' < n}$

CONTROLAR k'

$\boxed{BCH}$

CÓDIGOS "FOLDED"

$\mathbb{F}_{16}$ $\qquad (a, b, c, d) \in \mathbb{F}_2^4$

$C \quad [3, k, d]_{16}$ $\qquad c(\underset{\mathbb{F}_{16}}{\underset{\cap}{c_1}}, \underset{\mathbb{F}_{16}}{\underset{\cap}{c_2}}, \underset{\mathbb{F}_{16}}{\underset{\cap}{c_3}}) \overset{\in C}{\in} \mathbb{F}_{16}^3$

$$c(c_1, c_2, c_3) = \left(\boxed{\ \ }\boxed{\ \ }\boxed{\ \ }\boxed{\ \ },\ \boxed{\ \ }\boxed{\ \ }\boxed{\ \ }\boxed{\ \ },\ \boxed{\ \ }\boxed{\ \ }\boxed{\ \ }\boxed{\ \ } \right) \in \mathbb{F}_2^{4\cdot 3 = 12}$$

$C' \quad [3\cdot 4, \circledast, \circledast]$

CAPACIDAD DE UN CANAL

$1 \to 1$ CON PROBABILIDAD $1-p$

$1 \to 0$ " " p

$0 \to 0$ " " $1-p$

$0 \to 1$ " " p

$p < 1/2$

UN CANAL SIMÉTRICO BINARIO TIENE CAPACIDAD:

$$1 - H(p) = 1 + p\log(p) + (1-p)\log(1-p)$$

ENTROPIA

Th DE SHANNON PARA CANALES CON RUIDO

EN UN CANAL SIMÉTRICO BINARIO DE CAPACIDAD $C>0$, PARA TODO NÚMERO REAL $\varepsilon>0$, EXISTE UN CÓDIGO DE BLOQUE $\mathcal{C}_n$ DE LONGITUD n (QUE DEPENDE DE ε) TAL QUE

- PROBABILIDAD ERROR COMUNICACIÓN $< \varepsilon$
- TASA TRANSMISIÓN $\geq C-\varepsilon$ $\left(R(\mathcal{C}) = \frac{\log_q \# \mathcal{C}}{n} = \frac{k}{n}\right)$

EN PARTICULAR EXISTE UNA SUCESIÓN DE CÓDIGOS $(\mathcal{C}_n)_{n=1}^{\infty}$ TAL QUE

$$\lim_{n\to\infty} \mathrm{Prob}_{\mathrm{ERROR}}(\mathcal{C}_n) = 0, \quad \lim_{n\to\infty} R(\mathcal{C}_n) = C$$