Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C| = q^{\kappa} \le q^{n-d+1} \implies \kappa \le n-d+1$  $d \le n-\kappa+1$ . Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C|=q^{\kappa} \leq q^{n-d+1} \implies \kappa \leq n-d+1$  $d \leq n-\kappa+1$ .

Sean oc, ..., xn elementos distintos en IFq. Dado K s n, sea PK el con: sunto de los polinomios en IFq [2] con grado menor a K.

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:

Sean  $x_1, ..., x_n$  elementos distintos en IFq. Dado  $K \leq n$ , sea  $P_K$  el conjunto de los polinomios en IFq[Z] con grado menor a K.

Un código de Reed-Solomon es un código formado de las palajbras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

Sean  $x_1, ..., x_n$  elementos distintos en IFq. Dado  $K \leq n$ , sea  $P_K$  el conjunto de los polinomios en IFq[x] con grado menor a K.

Un código de Reed-Solomon es un código formado de las palaj bras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud queq y lineal.

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C|=q^{\kappa} \leq q^{n-d+1} \implies \kappa \leq n-d+1$  $d \leq n-\kappa+1$ .

Sean  $sc_1,...,x_n$  elementos distintos en IFq. Dado  $\kappa \leq n$ , sea  $P\kappa$  el conjunto de los polinomios en IFq[x] con grado menor a  $\kappa$ .

Un código de Reed-Solomon es un código formado de las palajbras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud queq y lineal. Además:

Prop: La distancia mínima de un código de Reed-Solomon es n-K+1.

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C| = q^{\kappa} \le q^{n-d+1} \implies \kappa \le n-d+1$  $d \le n-\kappa+1$ .

Sean  $x_1, ..., x_n$  elementos distintos en IFq. Dado  $K \leq n$ , sea  $P_K$  el conjunto de los polinomios en IFq[Z] con grado menor a K.

Un código de Reed-Solomon es un código formado de las palajbras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud queq y lineal. Además:

Prop: La distancia mínima de un código de Reed-Solomon es n-K+1.

Dem: touérdese que un polinomio en Fq[x] de grado m tiene al máximo m cercos.

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C|=q^{\kappa} \leq q^{n-d+1} \implies \kappa \leq n-d+1$  $d \leq n-\kappa+1$ 

Sean x,..., xn elementos distintos en IFq. Dado K = n, sea Pk el con: junto de los polinomios en IFq [x] con grado menor a K.
Un código de Reed-Solomon es un código formado de las pala: bras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud q n = q y lineal. Además:

Prop: La distancia mínima de un código de Reed-Solomon es n-K+1.

Dem: Acuérdese que un polinomio en Fq[x] de grado m tiene al máximo m cercos.

Entonces, si f, g e Pk y (f(x1), f(x1), ...f(xn)) = (g(x1), g(x1), ..., g(xn))

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C|=q^{\kappa} \leq q^{n-d+1} \implies \kappa \leq n-d+1$  $d \leq n-\kappa+1$ 

Sean sc1,..., xn elementos distintos en IFq. Dado K = n, sea Pk el con: sunto de los polinomios en IFq [2] con grado menor a K.
Un código de Reed-Solomon es un código formado de las pala: bras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud q n = q y lineal. Además:

Prop: La distancia mínima de un código de Reed-Solomon es n-K+1.

Dem: Acuérdese que un polinomio en Fq[x] de grado m tiene al máximo m cercos.

Entonces, si  $f,g \in P_K$  y  $(f(x_1),f(x_1),...,f(x_n))=(g(x_1),g(x_2),...,g(x_n))$  $f-g \in P_K$ , con  $n > K > \deg(f-g)$ , tiene  $n \in P_K$ 

=> f=g, i.e.: las palabras códigos son todas distintas.

Códigos de Reed-Solomon Hemos mostrado la cota del singulete:  $|C|=q^{\kappa} \leq q^{n-d+1} \implies \kappa \leq n-d+1$  $d \leq n-\kappa+1$ 

Sean oc, ..., xn elementos distintos en IFq. Dado K = n, sea Pk el con: junto de los polinomios en IFq [x] con grado menor a K.
Un código de Reed-Solomon es un código formado de las pala: bras

 $(f(x_1), \ldots, f(x_n))$  con  $f \in P_K$ .

Es un código de longitud queq y lineal. Además:

Prop: La distancia mínima de un código de Reed-Solomon es n-K+1.

Dem: touérdese que un polinomio en Fq[x] de grado m tiene al máximo m cercos.

Entonces, si f, g e Px y (f(x1), f(x1),...f(xn)) = (g(x1), g(x1),...,g(xn))

f-g Elk, con n>k> deg (fig), Tiene n ceros!

=> f=g, i.e.: las palabras cúdigos son todas distintas.

Finalmente, f tiene al máximo  $\kappa-1$  cercos, por eso  $wt(f(x_1),...,f(x_n)) > n-\kappa+1$  si los  $x_i$  no son todos cerco.  $\square$ 

Usualmente se escogen los xi en la signiente manera.

Usualmente se escogen los  $x_i$  en la signiente manera. Sea  $\alpha \in \mathbb{F}_q$  de orden q-1, Llamamos  $x_i = \alpha^{i-1}$ , i = 1, ..., q-1. multiplicativo Isualmente se escogen los xi en la signiente manera.

Sea « « IFq de orden q-1, Llamamos » ci = «i-1, i=1,..., q-1.

miltiplicativo

Notése que no con ci 11000

Notese que  $x_i^n = x_i^{q-1} = \alpha^{(i-1)(q-1)} = 1$ , i = 1, ..., q-1.

Usualmento se escogen los  $x_i$  en la signiente manera.

Sea  $\kappa \in \mathbb{F}_q$  de orden q.1, Llamamos  $sc_i = \kappa^{i-1}$ ,  $i=1,\ldots,q-1$ .

miltiplicativo

Notése que  $x_i^n = x_i^{q-1} = \alpha^{(i-1)(q-1)} = 1$ ,  $i=1,\ldots,q-1$ .

La codificación de  $a_0 \cdots a_{\kappa-1}$ corresponde a la palabra  $(i(x_1), \ldots, i(x_n))$ , donde  $i(\kappa) = a_0 + a_1 \times \cdots + a_{n-1} \times \cdots + a_{n-1}$ 

```
Isualmente se escogen los x_i en la signiente manera.

Sea \alpha el f_q de orden q-1, le mamos x_i = \alpha^{i-1}, i=1,...,q-1.

miltiplicativo

Noté se que x_i^n = x_i^{q-1} = \alpha^{(i-1)(q-1)} = 1, i=1,...,q-1.

La codificación de a_0 \cdots a_{K-1}

corrnesponde a la palabra (i(x_1), ..., i(x_n)), donde i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^n

Ejemplo:
```

F=1F11 , K=5

Isualmente se escogen los xi en la signiente manera. Sea « « lfq de orden q.1, Llamamos » ci = «i-1, i=1,..., q-1. multiplicativo Notése que  $x_{i}^{n} = x_{i}^{q-1} = \alpha^{(i-1)(q-1)} = 1$  i = 1, ..., q-1. La codificación de a ... a K-1 corrresponde a la palabra  $(i(x_1),...,i(x_n)),$  donde  $i(x) = a_0 + a_1 x + ... + a_n x^n$ Ejemplo: F=1, K=5

2 tiene orden 10: {1,2,4,8,5,10,9,7,3,6}

```
Isualmente se escogen los x_i en la signiente manera.

Sea x \in \mathbb{F}_q de orden q \in \mathbb{F}_q, l'amamos x_i = x^{i-1}, i = 1, ..., q-1.

multiplicativo

Notése que x_i^n = x_i^{q-1} = \alpha^{(i-1)(q-1)} = 1, i = 1, ..., q-1.

La codificación de a_0 \cdots a_{K-1}

corresponde a la palabra (i(x_1), ..., i(x_m)), donde i(x) = a_0 + a_1 x + \cdots + a_{m-1} x^m

E_j \in \mathbb{F}_{11}, K = 5

2 tiene orden 10 : \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}

a = (1, 0, 0, 0, 0) \longrightarrow i(x) = 1 \longrightarrow (1313131, 1, 1, 1) = (i(x_1), ..., i(x_m))
```

```
Isualmente se escogen los xi en la signiente manera.
Sea « « lfq de orden q1, Llamamos » ci = «i-1, i=1,..., q-1.
              multiplicativo
Notése que
              x_{i}^{n} = x_{i}^{q-1} = \alpha^{(i-1)(q-1)} = 1  i = 1, ..., q-1.
La codificación de
       a ... a K-1
corrresponde a la palabra
            (i(x_1), ..., i(x_n)), donde i(x) = a_0 + a_1 x + ... + a_n x^n
Ejemplo:
F=F1, K=5
2 tiene orden 10: {1,2,4,8,5,10,9,7,3,6}
  a = (1, 0, 0, 0, 0) m > i(x) = 1 m > (1,1,1,1,1,1,1) = (i(x,1), ..., i(x,0))
     (0,1,0,0,0) ~> i(x)=x ~> (1,2,4,8,5,10,9,7,3,6)
    (0,0,1,0,0) ~> i (>c)=x2 ~~ (1,4,5,9,3,1,4,5,9,3)
    (0,0,0,1,0) m> i(x)=x3 m> (1,8,9,6,4,10,3,2,5,7)
    (0,0,0,0,1) ~ i(x)=x4 ~ (1,5,3,4,9,1,5,3,4,9)
```

```
Isualmente se escogen los xi en la signiente manera.
Sea « cifq de orden q1, Llamamos » ci = «i-1, i=1,..., q-1.
               multiplicativo
Notése que
               x_{i}^{n} = x_{i}^{q-1} = \alpha^{(i-1)(q-1)} = 1  i = 1, ..., q-1.
La codificación de
        a ... a K-1
corrresponde a la palabra
            (i(x_1), ..., i(x_n)), donde i(x) = a_0 + a_1 x + ... + a_n x^n
Ejemplo:
F=1F11 , K=5
2 tiene orden 10: {1,2,4,8,5,10,9,7,3,6}
  a = (1, 0, 0, 0, 0) \longrightarrow i(x) = 1 \longrightarrow (1,11,11,1,1,1) = (i(x_1), ..., i(x_{10}))
     (0,1,0,0,0) ~> i(x)=x ~> (1,2,4,8,5,10,9,7,3,6)
     (0,0,1,0,0) ~> i (x)=x2 ~~ (1,4,5,9,3,1,4,5,9,3)
    (0,0,0,1,0) m> i(x)=x3 m> (1,8,9,6,4,10,3,2,5,7)
    (0,0,0,0,1) ~ i(x)=x4 ~ (1,5,3,4,9,1,5,3,4,9)
con estas palabras formamos una matriz generadora. Se
puede verificar que el peso minimo es 6=10-5+1 (sel cochigo
 es MOS).
```

Usualmente se escogen los  $x_i$  en la signiente manera. Sea  $\alpha \in \mathbb{F}_q$  de orden  $q_1$ , Llamamos  $sc_i = \alpha^{i-1}$ , i = 1, ..., q-1. multiplicativo

Notese que  $x_i^n = x_i^{q-1} = \alpha^{(i-1)(q-1)} = 1$ , i = 1, ..., q-1.

La codificación de ao...a<sub>K-1</sub>

corrresponde a la palabra

 $(i(x_1), ..., i(x_n)),$  donde  $i(x) = a_0 + a_1 x + ... + a_{n-1} x^n$ 

Ejemplo:

F=F11, K=5

2 tiene orden 10: {1,2,4,8,5,10,9,7,3,6}

 $a = (1, 0, 0, 0, 0) \quad \text{if} \quad x = 1 \quad \text{if} \quad (1,1,1,1,1,1,1,1) = (i(x_1), ..., i(x_{10}))$   $(0,1,0,0,0) \quad \text{if} \quad (x) = x \quad \text{if} \quad (1,2,4,8,5,10,9,7,3,6)$   $(0,0,1,0,0) \quad \text{if} \quad (x) = x^2 \quad \text{if} \quad (1,4,5,9,3,1,4,5,3,3)$   $(0,0,0,1,0) \quad \text{if} \quad (x) = x^3 \quad \text{if} \quad (1,8,9,6,4,10,3,2,5,7)$   $(0,0,0,0,1) \quad \text{if} \quad (x) = x^4 \quad \text{if} \quad (1,5,3,4,9,1,5,3,4,9)$ 

con estas palabras formamos una matriz generadora. Se puede verificar que el peso mínimo es 6=10-5+1 (sel cochigo es MOS).

 $G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \vdots \\ x_1^K & x_2^K & \cdots & x_n^K \end{pmatrix}$  <-- si K = N-1 esta se llama matriz de Vandermonde.

Lema: Sea pelly un elements de orden n. Llamamos  $x_j = \beta^{j-1}$ , j=1,...,n.

Sean  $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ x_1 x_2 & \cdots & x_n \end{pmatrix}$   $B = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \end{pmatrix}$   $\begin{cases} x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & \ddots & \vdots \\ x_1^2 & x_2^2 & \cdots & x_n^2 \end{cases}$ con  $s+a+1 \le n$ . Luego  $BA^T = 0 = AB^T$ .

Lema: Sea pelle un elemento de orden n. Llamamos x; = Bi-1, j=1,...,n.
Sean

con statism. Luego BAT=0=ABT.

El lema se puede utilizar para buscar una matriz de conted H.  $(a=\kappa,j, j=n-\kappa, a+s+1=n).$