Códigos de Reed-Solomon

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \dots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \dots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Un <u>código de Reed-Solomon</u> es un código formado de las palabras

$$(f(x_1), \dots, f(x_n)) \qquad \text{con } f \in P_k.$$

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \ldots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Un <u>código de Reed-Solomon</u> es un código formado de las palabras

$$(f(x_1), \ldots, f(x_n)) \qquad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \Rightarrow \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \dots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Un <u>código de Reed-Solomon</u> es un código formado de las palabras

$$(f(x_1), \dots, f(x_n)) \qquad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Además:

<u>Prop:</u> La distancia mínima de un código de Reed-Solomon es $n-k+1$.

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \dots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Un <u>código de Reed-Solomon</u> es un código formado de las palabras

$$(f(x_1), \dots, f(x_n)) \qquad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Además:

<u>Prop:</u> La distancia mínima de un código de Reed-Solomon es $n-k+1$.

<u>Dem:</u> Acuérdese que un polinomio en $\mathbb{F}_q[x]$ de grado m tiene al máximo m ceros.

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \Rightarrow k \leq n-d+1$$
$$d \leq n-k+1.$$

Sean $x_1, \dots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

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

$$(f(x_1), \dots, f(x_n)) \quad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Además:

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

Dem: Acuérdese que un polinomio en $\mathbb{F}_q[x]$ de grado m tiene al máximo m ceros.

Entonces, si $f, g \in P_k$ y $(f(x_1), f(x_2), \dots f(x_n)) = (g(x_1), g(x_2), \dots, g(x_n))$

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \ldots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

Un <u>código de Reed-Solomon</u> es un código formado de las palabras

$$(f(x_1), \ldots, f(x_n)) \qquad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Además:

<u>Prop</u>: La distancia mínima de un código de Reed-Solomon es $n-k+1$.

<u>Dem</u>: Acuérdese que un polinomio en $\mathbb{F}_q[x]$ de grado m tiene al máximo m ceros.

Entonces, si $f, g \in P_k$ y $(f(x_1), f(x_2), \ldots f(x_n)) = (g(x_1), g(x_2), \ldots, g(x_n))$

$$f-g \in P_k, \text{ con } n \geq k > \deg(f-g), \text{ tiene } n \text{ ceros!}$$

$\implies f = g$, i.e.: las palabras códigos son todas distintas.

Códigos de Reed-Solomon

Hemos mostrado la cota del singulete:

$$|C| = q^k \leq q^{n-d+1} \implies \begin{array}{l} k \leq n-d+1 \\ d \leq n-k+1. \end{array}$$

Sean $x_1, \ldots, x_n$ elementos distintos en $\mathbb{F}_q$. Dado $k \leq n$, sea P_k el conjunto de los polinomios en $\mathbb{F}_q[x]$ con grado menor a k.

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

$$(f(x_1), \ldots, f(x_n)) \qquad \text{con } f \in P_k.$$

Es un código de longitud $n \leq q$ y lineal.

Además:

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

Dem: Acuérdese que un polinomio en $\mathbb{F}_q[x]$ de grado m tiene al máximo m ceros.

Entonces, si $f, g \in P_k$ y $(f(x_1), f(x_2), \ldots f(x_n)) = (g(x_1), g(x_2), \ldots, g(x_n))$

$$f - g \in P_k, \text{ con } n \geq k > \deg(f-g), \text{ tiene } n \text{ ceros!}$$

$\Rightarrow f = g$, i.e.: las palabras códigos son todas distintas.

Finalmente, f tiene al máximo $k-1$ ceros, por eso $wt(f(x_1), \ldots, f(x_n)) \geq n-k+1$ si los x_i no son todos ceros. $\square$

Usualmente se escogen los x_i en la siguiente manera.

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

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

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

Usualmente se escogen los x_i en la siguiente manera.

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

multiplicativo

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \ldots, i(x_n)), \quad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-}$$

Usualmente se escogen los x_i en la siguiente manera.

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

(orden ↑ multiplicativo)

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \ldots, i(x_n)), \quad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n}$$

<u>Ejemplo</u>:

$F = \mathbb{F}_{11}$, $k = 5$

Usualmente se escogen los x_i en la siguiente manera.

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

multiplicativo

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \ldots, i(x_n)), \qquad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

Ejemplo:

$F = \mathbb{F}_{11}$, $k = 5$

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

Usualmente se escogen los x_i en la siguiente manera.

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

multiplicativo

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \ldots, i(x_n)), \qquad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n}$$

Ejemplo:

$F = \mathbb{F}_{11}$, $k=5$

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

$a = (1,0,0,0,0) \rightsquigarrow i(x) = 1 \rightsquigarrow (1,1,1,1,1,1,1,1,1,1) = (i(x_1), \ldots, i(x_{10}))$

Usualmente se escogen los x_i en la siguiente manera.

Sea $\alpha \in \mathbb{F}_q$ de orden $q-1$, Llamamos $x_i = \alpha^{i-1}$, $i = 1, \dots, q-1$.

$\underset{\text{multiplicativo}}{\uparrow}$

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \dots, i(x_n)), \qquad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

<u>Ejemplo</u>:

$F = \mathbb{F}_{11}$, $k = 5$

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

$a = (1,0,0,0,0) \rightsquigarrow i(x) = 1 \rightsquigarrow (1,1,1,1,1,1,1,1,1,1) = (i(x_1), \dots, i(x_{10}))$

$(0,1,0,0,0) \rightsquigarrow i(x) = x \rightsquigarrow (1,2,4,8,5,10,9,7,3,6)$

$(0,0,1,0,0) \rightsquigarrow i(x) = x^2 \rightsquigarrow (1,4,5,9,3,1,4,5,9,3)$

$(0,0,0,1,0) \rightsquigarrow i(x) = x^3 \rightsquigarrow (1,8,9,6,4,10,3,2,5,7)$

$(0,0,0,0,1) \rightsquigarrow i(x) = x^4 \rightsquigarrow (1,5,3,4,9,1,5,3,4,9)$

Usualmente se escogen los x_i en la siguiente manera.

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

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

$$(i(x_1), \ldots, i(x_n)), \qquad \text{donde } i(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$$

<u>Ejemplo</u>:

$F = \mathbb{F}_{11}$, $k = 5$

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

$a = (1,0,0,0,0) \rightsquigarrow i(x) = 1 \rightsquigarrow (1,1,1,1,1,1,1,1,1,1) = (i(x_1), \ldots, i(x_{10}))$

$(0,1,0,0,0) \rightsquigarrow i(x) = x \rightsquigarrow (1,2,4,8,5,10,9,7,3,6)$

$(0,0,1,0,0) \rightsquigarrow i(x) = x^2 \rightsquigarrow (1,4,5,9,3,1,4,5,9,3)$

$(0,0,0,1,0) \rightsquigarrow i(x) = x^3 \rightsquigarrow (1,8,9,6,4,10,3,2,5,7)$

$(0,0,0,0,1) \rightsquigarrow i(x) = x^4 \rightsquigarrow (1,5,3,4,9,1,5,3,4,9)$

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

Usualmente se escogen los x_i en la siguiente manera.

Sea $\alpha \in \mathbb{F}_q$ de orden $q-1$, Llamamos $x_i = \alpha^{i-1}$, $i = 1, \dots, q-1$.

multiplicativo

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

La codificación de

$$a_0 \cdots a_{k-1}$$

corresponde a la palabra

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

Ejemplo:

$F = \mathbb{F}_{11}$, $k=5$

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

$a = (1,0,0,0,0) \rightsquigarrow i(x) = 1 \rightsquigarrow (1,1,1,1,1,1,1,1,1,1) = (i(x_1), \dots, i(x_{10}))$

$(0,1,0,0,0) \rightsquigarrow i(x) = x \rightsquigarrow (1,2,4,8,5,10,9,7,3,6)$

$(0,0,1,0,0) \rightsquigarrow i(x) = x^2 \rightsquigarrow (1,4,5,9,3,1,4,5,9,3)$

$(0,0,0,1,0) \rightsquigarrow i(x) = x^3 \rightsquigarrow (1,8,9,6,4,10,3,2,5,7)$

$(0,0,0,0,1) \rightsquigarrow i(x) = x^4 \rightsquigarrow (1,5,3,4,9,1,5,3,4,9)$

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

$$G = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & & x_n \\ \vdots & \vdots & & \vdots \\ x_1^k & x_2^k & \cdots & x_n^k \end{pmatrix} \longleftarrow \text{si } k=n-1 \text{ esta se llama matriz de Vandermonde.}$$

Lema: Sea $\beta \in \mathbb{F}_q$ un elemento de orden n. Llamamos $x_j = \beta^{j-1}$, $j = 1, \dots, n$.
Sean

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \\ x_1^a & x_2^a & \cdots & x_n^a \end{pmatrix} \quad , \quad B = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^s & x_2^s & \cdots & x_n^s \end{pmatrix}$$

con $s + a + 1 \leq n$. Luego $BA^T = 0 = AB^T$.

Lema: Sea $\beta \in \mathbb{F}_q$ un elemento de orden n. Llamamos $x_j = \beta^{j-1}$, $j=1,\dots,n$.
Sean

$$A = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ x_1 & x_2 & \cdots & x_n \\ \vdots & \vdots & & \\ x_1^a & x_2^a & \cdots & x_n^a \end{pmatrix} , \qquad B = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & & \vdots \\ x_1^s & x_2^s & \cdots & x_n^s \end{pmatrix}$$

con $s+a+1 \leq n$. Luego $BA^T = 0 = AB^T$.

El lema se puede utilizar para buscar una matriz de control H. ($a = k-1$, $s = n-k$, $a+s+1 = n$).