

Códigos Localmente Recuperables

Clase 2: Códigos de Reed-Solomon e introducción a los códigos LR

María Chara

Profesora en Universidad de la República, Uruguay
Investigadora de CONICET, Argentina

UMA-RSME 2025

Bariloche, 3 de diciembre

Repaso: Códigos Lineales

Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

- Parámetros: $[n, k]_q$
 - n : longitud
 - k : dimensión

Repaso: Códigos Lineales

Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

- Parámetros: $[n, k]_q$
 - n : longitud
 - k : dimensión
- Codifica k símbolos en n

Repaso: Códigos Lineales

Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

- Parámetros: $[n, k]_q$
 - n : longitud
 - k : dimensión
- Codifica k símbolos en n
- Parámetros: $[n, k, d]_q$
 - n : longitud
 - k : dimensión
 - d : distancia mínima de Hamming

Repaso: Códigos Lineales

Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

- Parámetros: $[n, k]_q$
 - n : longitud
 - k : dimensión
- Codifica k símbolos en n
- Parámetros: $[n, k, d]_q$
 - n : longitud
 - k : dimensión
 - d : distancia mínima de Hamming
- Permite detectar hasta $d - 1$ errores y corregir hasta $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores

Repaso: Códigos Lineales

Un código lineal sobre $\mathbb{F}_q$ es un subespacio vectorial $C \subseteq \mathbb{F}_q^n$.

- Parámetros: $[n, k]_q$
 - n : longitud
 - k : dimensión
- Codifica k símbolos en n
- Parámetros: $[n, k, d]_q$
 - n : longitud
 - k : dimensión
 - d : distancia mínima de Hamming
- Permite detectar hasta $d - 1$ errores y corregir hasta $\left\lfloor \frac{d-1}{2} \right\rfloor$ errores
- Cota de Singleton: $k + d \leq n + 1$

Códigos de Reed-Solomon

Códigos de Reed-Solomon (MDS)

- $q = p^r$, p primo
- $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$
- $1 \leq k \leq q-1$ $\mathcal{L}_{k-1} = \{g(x) \in \mathbb{F}_q[x] : \deg g(x) \leq k-1\}$
- $\vec{a} = (a_0, \dots, a_{k-1})$ definimos $f(x) = a_0 + \dots + a_{k-1}x^{k-1}$

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^{q-1} \\ (a_0, \dots, a_{k-1}) & \rightarrow & (f(\alpha_1), \dots, f(\alpha_{q-1})) \end{array}$$

$$RS(k, q) = \{(f(\alpha_1), \dots, f(\alpha_{q-1})) : f \in \mathcal{L}_{k-1}\}$$

Códigos de Reed-Solomon (MDS)

- $q = p^r$, p primo
- $\mathbb{F}_q^* = \{\alpha_1, \dots, \alpha_{q-1}\}$
- $1 \leq k \leq q-1$ $\mathcal{L}_{k-1} = \{g(x) \in \mathbb{F}_q[x] : \deg g(x) \leq k-1\}$
- $\vec{a} = (a_0, \dots, a_{k-1})$ definimos $f(x) = a_0 + \dots + a_{k-1}x^{k-1}$

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^{q-1} \\ (a_0, \dots, a_{k-1}) & \rightarrow & (f(\alpha_1), \dots, f(\alpha_{q-1})) \end{array}$$

$$RS(k, q) = \{(f(\alpha_1), \dots, f(\alpha_{q-1})) : f \in \mathcal{L}_{k-1}\}$$

- longitud $n = q - 1$
- dimensión k
- distancia mínima $d = q - k$

Motivación de localidad

En códigos clásicos, para recuperar un símbolo perdido puede ser necesario usar **todos los otros símbolos**.

Queremos recuperar localmente un símbolo usando un subconjunto de los otros.

Localidad

Reducir el número de accesos en la recuperación.

Definición de Localidad

Sea C un código lineal y $c = (c_1, \dots, c_n) \in C$.

Decimos que el símbolo c_i tiene localidad r si existe un conjunto $R_i \subseteq \{1, \dots, n\} \setminus \{i\}$ tal que:

- $|R_i| \leq r$
- c_i se puede obtener de $\{c_j : j \in R_i\}$

Si **todos** los símbolos la tienen, el código tiene localidad r .

Ejemplo pequeño

Código binario de longitud 5:

$$c_4 = c_1 + c_2, \quad c_5 = c_1 + c_3$$

- c_4 depende de c_1, c_2 : localidad $r = 2$
- c_5 depende de c_1, c_3 : localidad $r = 2$

Ejercicio: ¿Podemos recuperar c_1, c_2 y c_3 localmente?

Códigos localmente recuperables

Definición

$\mathcal{C}$ es un $[n, k, d; r]$ -código si cualquier coordenada “borrada” puede ser recuperada accediendo a, como máximo, r otros símbolos, $1 \leq r < k$.

$$(c_1, c_2, \dots, c_{i-1}, c_i, c_{i+1}, \dots, c_{n-1}, c_n)$$

Observación

ERROR vs. BORRÓN

Teorema

Si $\mathcal{C}$ es un $[n, k, d; r]$ -código entonces

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

Teorema

Si $\mathcal{C}$ es un $[n, k, d; r]$ -código entonces

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

- Notar que si $r = k$ se obtiene la Cota de Singleton

Teorema

Si $\mathcal{C}$ es un $[n, k, d; r]$ -código entonces

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2.$$

- Notar que si $r = k$ se obtiene la Cota de Singleton

Definición

Un código LR que satisface $d = n - k - \left\lceil \frac{k}{r} \right\rceil + 2$ se dice óptimo.

- Para el caso $r = k$ los códigos LR óptimos son los MDS.

Barg-Tamo (2014), $n \leq q$

Barg-Tamo (2014), $n \leq q$

- $A \subset \mathbb{F}_q$ tal que $|A| = n$ y $A = A_1 \cup A_2 \cup \dots \cup A_{n/r+1}$
- Polinomio $g(x) \in \mathbb{F}_q[x]$ bueno para A :
 - $\deg g(x) = r + 1$,
 - g es constante en cada A_i para todo i .

$$\mathcal{C} = \{(f_{\vec{a}}(\vec{\alpha})) : \vec{\alpha} \in A, \vec{a} \in \mathbb{F}_q^k\}$$

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ \vec{a} & \rightarrow & \vec{c} = (f_{\vec{a}}(\alpha_1), \dots, f_{\vec{a}}(\alpha_n)) \end{array}$$

$$f_{\vec{a}}(x) = \sum_{i=0}^{r-1} f_i(x) x^i = \sum_{i=0}^{r-1} \left(\sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j \right) x^i$$

Recuperación de una coordenada

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ \vec{a} & \longrightarrow & (f_{\vec{a}}(\alpha_1), \dots, \cancel{f_{\vec{a}}(\alpha_i)}, \dots, f_{\vec{a}}(\alpha_n)) \end{array}$$

$$\alpha_i \in A_s, \quad |A_s| = r + 1 \rightsquigarrow \{(\beta, f_{\vec{a}}(\beta)) : \beta \in A_s \setminus \alpha_i\}$$

$$f_{\vec{a}}(x) = \sum_{i=0}^{r-1} f_i(x) x^i = \sum_{i=0}^{r-1} \left(\sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j \right) x^i$$

Interpolación

$$\delta(x) = \sum_{\beta \in A_s \setminus \{\alpha_i\}} f_{\vec{a}}(\beta) \prod_{\gamma \in A_s \setminus \{\alpha_i, \beta\}} \frac{x - \gamma}{\beta - \gamma} \implies f_{\vec{a}}(\alpha_i) = \delta(\alpha_i)$$

Ejemplo: $[9,4,5;2]$ -código sobre $\mathbb{F}_{13}$

- $A_1 = \{1, 3, 9\}$, $A_2 = \{2, 6, 5\}$, $A_3 = \{4, 12, 10\}$
- $A = A_1 \cup A_2 \cup A_3 = \{1, 3, 9, 2, 6, 5, 4, 12, 10\}$
- $g(x) = x^3$ ($1 = 1^3 = 3^3 = 9^3$, $8 = 2^3 = 6^3 = 5^3$, $12 = 4^3 = 12^3 = 10^3$)

$$\begin{array}{ccc} \mathbb{F}_{13}^4 & \longrightarrow & \mathbb{F}_{13}^9 \\ \vec{a} & \longrightarrow & (f_{\vec{a}}(1), f_{\vec{a}}(3), \dots, f_{\vec{a}}(10)) \end{array}$$

$$\begin{aligned} \vec{a} = (a_{00}, a_{01}, a_{10}, a_{11}) \rightsquigarrow f_{\vec{a}}(x) &= \sum_{i=0}^{r-1} \left(\sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j \right) x^i \\ &= \sum_{i=0}^1 \left(\sum_{j=0}^1 a_{ij} x^{3j} \right) x^i \\ &= f_0(x) + f_1(x) x \end{aligned}$$

Ejemplo: [9,4,5;2]-código sobre $\mathbb{F}_{13}$

- $A_1 = \{1, 3, 9\}$, $A_2 = \{2, 6, 5\}$, $A_3 = \{4, 12, 10\}$
- $A = A_1 \cup A_2 \cup A_3 = \{1, 3, 9, 2, 6, 5, 4, 12, 10\}$
- $g(x) = x^3$ ($1 = 1^3 = 3^3 = 9^3$, $8 = 2^3 = 6^3 = 5^3$, $12 = 4^3 = 12^3 = 10^3$)

$$\begin{aligned}\mathbb{F}_{13}^4 &\longrightarrow \mathbb{F}_{13}^9 \\ \vec{a} &\longrightarrow (f_{\vec{a}}(1), f_{\vec{a}}(3), \dots, f_{\vec{a}}(10)) \\ (1, 1, 1, 1) &\longrightarrow (4, 8, 7, 1, 11, 2, 0, 0, 0)\end{aligned}$$

$$\begin{aligned}\vec{a} = (a_{00}, a_{01}, a_{10}, a_{11}) \rightsquigarrow f_{\vec{a}}(x) &= \sum_{i=0}^{r-1} \left(\sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j \right) x^i \\ &= \sum_{i=0}^1 \left(\sum_{j=0}^1 a_{ij} x^{3j} \right) x^i \\ &= f_0(x) + f_1(x) x\end{aligned}$$

Ejemplo

- $A_1 = \{1, 3, 9\}$, $A_2 = \{2, 6, 5\}$, $A_3 = \{4, 12, 10\}$
- $A = A_1 \cup A_2 \cup A_3 = \{1, 3, 9, 2, 6, 5, 4, 12, 10\}$

$$\begin{array}{ccc} \mathbb{F}_{13}^4 & \longrightarrow & \mathbb{F}_{13}^9 \\ (1, 1, 1, 1) & \rightarrow & (\cancel{4}, 8, 7, 1, 11, 2, 0, 0, 0) \end{array}$$

$$(1, f_{\vec{a}}(1) = ?), (3, f_{\vec{a}}(3) = 8), (9, f_{\vec{a}}(9) = 7)$$

$$\delta(x) = 2x + 2 \rightsquigarrow f_{\vec{a}}(1) = \delta(1) = 2 \cdot 1 + 2 = 4$$