

Códigos Localmente Recuperables

Clase 3: Códigos LR óptimos y algunas generalizaciones

María Chara

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

UMA-RSME 2025
Bariloche, 4 de diciembre

Repaso: 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 $f(x) = a_0 + \dots + a_{k-1}x^{k-1}$

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

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

Repaso: 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 $d = q - k$

Definición de Localidad

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

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 , y decimos que $\mathcal{C}$ es un $[n, k, d; r]$ -código LR.

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.

Construcción Barg-Tamo (2014) (idea central)

Sea $A \subseteq \mathbb{F}_q$, $|A| = n$. Particionamos A en conjuntos disjuntos:

$$A = A_1 \cup A_2 \cup \dots \cup A_{n/r+1}, \quad |A_i| = r + 1$$

Buscamos un subespacio de polinomios $\mathcal{P}$ tal que:

- Evaluar $f \in \mathcal{P}$ en A da un LRC.
- Restricción a cada A_i tiene grado $\leq r - 1$.

Entonces cada símbolo depende de r otros símbolos del mismo bloque.

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 .

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

$$\begin{array}{ccc} \mathbb{F}_q^k & \longrightarrow & \mathbb{F}_q^n \\ \vec{a} = (a_{ij})_{\substack{i=0, \dots, r-1 \\ j=0, \dots, k/r-1}} & \longrightarrow & \vec{c} = (f_{\vec{a}}(\alpha_1), \dots, f_{\vec{a}}(\alpha_n)) \end{array}$$

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

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 $\mathbb{F}_{13}$

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

$$\begin{array}{ccc} \mathbb{F}_{13}^4 & \longrightarrow & \mathbb{F}_{13}^9 \\ \vec{a} & \longrightarrow & (f_{\vec{a}}(1), f_{\vec{a}}(3), \dots, f_{\vec{a}}(12)) \end{array}$$

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

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

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

$$\begin{aligned}\mathbb{F}_{13}^4 &\longrightarrow \mathbb{F}_{13}^9 \\ \vec{a} &\longrightarrow (f_{\vec{a}}(1), f_{\vec{a}}(3), \dots, f_{\vec{a}}(12)) \\ (1, 1, 1, 1) &\longrightarrow (4, 8, 7, 1, 11, 2, 0, 0, 0)\end{aligned}$$

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

Ejemplo

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

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

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

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

Observaciones

- En el caso en que $r = k$ se obtiene la construcción tradicional de códigos de Reed Solomon. En ese caso, no se necesita un polinomio bueno porque el mismo es directamente una constante
- En la construcción se asume que r divide a k , pero esto no es necesario. En el caso en que k/r no sea entero, se define

$$f_i(x) = \sum_{j=0}^{s(r,k,i)} a_{ij}g(x)^j$$

con

$$s(r, k, j) = \begin{cases} \left\lfloor \frac{k}{r} \right\rfloor & i < k \mod r \\ \left\lfloor \frac{k}{r} \right\rfloor - 1 & i \geq k \mod r \end{cases}$$

Códigos AG (Goppa)

Idea: generalizar la construcción de los códigos de Reed-Solomon usando puntos en curvas sobre cuerpos finitos

RS	Goppa
$\mathbb{F}_q$	Curva χ sobre $\mathbb{F}_q$
$\alpha_1, \dots, \alpha_{q-1}$	$P_1, \dots, P_n$ en χ
polinomios en $\mathcal{L}_{k-1}$	funciones en un espacio vectorial adecuado

Códigos AG localmente recuperables

- $F/\mathbb{F}_q$ un cuerpo de funciones con $g > 0$ y $[F : \mathbb{F}_q(x)] = r + 1$
- $P_1, \dots, P_s$ lugares racionales de $\mathbb{F}_q(x)$ que se descomponen completamente en F
- un divisor G de $\mathbb{F}_q$ con soporte disjunto con $D = P_1 + \dots + P_s$
- $\mathcal{L}(G) = \langle f_1, \dots, f_m \rangle$
- $V = \langle f_i x^j : 1 \leq i \leq m; 0 \leq j \leq r - 1 \rangle$

$$\begin{array}{ll} V & \longrightarrow \mathbb{F}_q^{(r+1)s} \\ f & \longrightarrow (f(P_{01}), \dots, f(P_{rs})) \end{array}$$

Recuperación de coordenada

$$(f(P_{01}), \dots, f(P_{r1}), \dots, f(P_{0j}), \dots, \cancel{f(P_{ij})}, \dots, f(P_{rj}), \dots, f(P_{rs}))$$

Idea:

$$f(Q) = \sum_{j=0}^{r-1} \left(\sum_{i=1}^m \alpha_{ij} f_i(Q) \right) x^j(\textcolor{red}{Q}) = \sum_{j=0}^{r-1} c_j x^j(Q)$$

Disponibilidad > 1

Disponibilidad > 1

Definición

Un código localmente recuperable tiene disponibilidad $t > 1$ si cada coordenada tiene t conjuntos de recuperación (disjuntos)

Algunas referencias sobre códigos LR

- A Family of Optimal Locally Recoverable Codes. Barg, Tamo. IEEE Transactions on Information Theory Vol. 60, N 8, 2014.

Algunas referencias sobre códigos LR

- A Family of Optimal Locally Recoverable Codes. Barg, Tamo. IEEE Transactions on Information Theory Vol. 60, N 8, 2014.
- Locally recoverable codes on algebraic curves. Barg, Tamo and Vlăduț. IEEE International Symposium on Information Theory (ISIT), 1252-1256, 2015.

Algunas referencias sobre códigos LR

- A Family of Optimal Locally Recoverable Codes. Barg, Tamo. IEEE Transactions on Information Theory Vol. 60, N 8, 2014.
- Locally recoverable codes on algebraic curves. Barg, Tamo and Vlăduț. IEEE International Symposium on Information Theory (ISIT), 1252-1256, 2015.
- Locally recoverable codes with availability $t \geq 2$ from fiber products of curves. Haymaker, Malmskog, Matthews. Vol. 12, N 2: 317-336, 2018.

Algunas referencias sobre códigos LR

- A Family of Optimal Locally Recoverable Codes. Barg, Tamo. IEEE Transactions on Information Theory Vol. 60, N 8, 2014.
- Locally recoverable codes on algebraic curves. Barg, Tamo and Vlăduț. IEEE International Symposium on Information Theory (ISIT), 1252-1256, 2015.
- Locally recoverable codes with availability $t \geq 2$ from fiber products of curves. Haymaker, Malmskog, Matthews. Vol. 12, N 2: 317-336, 2018.
- Minimum Distance and Parameter Ranges of Locally Recoverable Codes with Availability from Fiber Products of Curves. Chara, Kottler, Malmskog, et al. Des. Codes Cryptogr. Vol. 91, 2077–2105, 2023.

Algunas referencias sobre códigos LR

- A Family of Optimal Locally Recoverable Codes. Barg, Tamo. IEEE Transactions on Information Theory Vol. 60, N 8, 2014.
- Locally recoverable codes on algebraic curves. Barg, Tamo and Vlăduț. IEEE International Symposium on Information Theory (ISIT), 1252-1256, 2015.
- Locally recoverable codes with availability $t \geq 2$ from fiber products of curves. Haymaker, Malmskog, Matthews. Vol. 12, N 2: 317-336, 2018.
- Minimum Distance and Parameter Ranges of Locally Recoverable Codes with Availability from Fiber Products of Curves. Chara, Kottler, Malmskog, et al. Des. Codes Cryptogr. Vol. 91, 2077–2105, 2023.
- Locally recoverable codes from towers of function field. Chara, Galluccio, Martinez-Moro. Finite Fields and Their Applications Vol. 94, 102359, 2024.

Algunas referencias generales sobre códigos

- Libro: Coding Theory. van Lint. Lecture Notes in Mathematics. Springer-Verlag Berlin. 1973

Algunas referencias generales sobre códigos

- Libro: Coding Theory. van Lint. Lecture Notes in Mathematics. Springer-Verlag Berlin. 1973
- Libro: Fundamentals of error correcting codes. Huffman and Pless. Cambridge University Press. 2003.

Algunas referencias generales sobre códigos

- Libro: Coding Theory. van Lint. Lecture Notes in Mathematics. Springer-Verlag Berlin. 1973
- Libro: Fundamentals of error correcting codes. Huffman and Pless. Cambridge University Press. 2003.
- Libro: Introduction to finite fields and their applications. R. Lidl and H. Niederreiter. Cambridge University Press. Revised edition. 1994.

Algunas referencias generales sobre códigos

- Libro: Coding Theory. van Lint. Lecture Notes in Mathematics. Springer-Verlag Berlin. 1973
- Libro: Fundamentals of error correcting codes. Huffman and Pless. Cambridge University Press. 2003.
- Libro: Introduction to finite fields and their applications. R. Lidl and H. Niederreiter. Cambridge University Press. Revised edition. 1994.
- Notas: Cuerpos finitos y códigos correctores de errores. Chara, 2019
<https://sites.google.com/view/maria-chara/publications>

Algunas referencias generales sobre códigos

- Libro: Coding Theory. van Lint. Lecture Notes in Mathematics. Springer-Verlag Berlin. 1973
- Libro: Fundamentals of error correcting codes. Huffman and Pless. Cambridge University Press. 2003.
- Libro: Introduction to finite fields and their applications. R. Lidl and H. Niederreiter. Cambridge University Press. Revised edition. 1994.
- Notas: Cuerpos finitos y códigos correctores de errores. Chara, 2019
<https://sites.google.com/view/maria-chara/publications>
- Notas: Introducción a la teoría de códigos autocorrectores. Podestá, 2006
<https://www.famaf.unc.edu.ar/documents/940/CMat35-3.pdf>

¡ GRACIAS !