Slide show test

Petar Hlad Colic

Universitat Politècnica de Catalunya

May 2018

Notation

- $\mathcal{C}$ denotes a code over the finite field $\mathbb{F}_q$.
- The triple of parameters (n, k, r) refers to a code of:
  - length n
  - cardinality q^k
  - locality r
- $[n] := \{1, \ldots, n\}$
- A *restriction* $\mathcal{C}_I$ of the code $\mathcal{C}$ to a subset of coordinates $I \subset [n]$ is the code obtained by removing from each vector the coordinates outside I.

Definition of LRC Codes

Given $a \in \mathbb{F}_q$ consider the sets of codewords of $\mathcal{C}$ with fixed value a at the symbol x_i:

$$\mathcal{C}(i,a) = \{x \in \mathcal{C} : x_i = a\}, \quad i \in [n]$$

Definition

A code $\mathcal{C}$ of length n has **locality r** *if $\forall i \in [n]$ there exists a subset $I_i \subset [n] \setminus i, \quad |I_i| \leq r$ such that the restrictions of the sets $\mathcal{C}(i,a)$ to the coordinates in I_i for different a are disjoint:*

$$\mathcal{C}_{I_i}(i,a) \cap \mathcal{C}_{I_i}(i,a') = \emptyset, \quad a \neq a'.$$

Maximum rate

Let $\mathcal{C}$ be an (n, k, r) LRC code of cardinality q^k over an alphabet of size q. Then:

Theorem (Upper bound on the rate)

The rate of $\mathcal{C}$ satisfies

$$\frac{k}{n} \leq \frac{r}{r+1}$$

Theorem (Generalization of Singleton bound)

The minimum distance of $\mathcal{C}$ satisfies

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

A code that achieves the bound with equality will be called an **optimal LRC code**.

Construction of LRC codes

We want to construct a linear (n, k, r)-LRC code. Assume $r|k$ and $(r+1)|n$.
We need:

- $A_1, \dots, A_{\frac{n}{r+1}}$ disjoint subsets of the field $\mathbb{F}_q$, s.t. $|A_i| = r + 1$
- $g(x) \in \mathbb{F}_q[x]$ a polynomial s.t.
  1. $deg(g) = r + 1$
  2. g is constant on each set A_i: $g(\alpha) = g(\beta)$ for $\alpha, \beta \in A_i$

We will call g a good polynomial.

Construction of LRC codes

Let $A = \bigcup_{i=1}^{\frac{n}{r+1}} A_i \subset \mathbb{F}_q$, $|A| = n$.
We write now message vectors $a \in \mathbb{F}_q^k$ as $r \times \frac{k}{r}$ matrices.

$$a = \begin{pmatrix} a_{0,0} & a_{0,1} & \cdots & a_{0,\frac{k}{r}-1} \\ a_{1,0} & a_{1,1} & \cdots & a_{1,\frac{k}{r}-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r-1,0} & a_{r-1,1} & \cdots & a_{r-1,\frac{k}{r}-1} \end{pmatrix}$$

Construction of LRC codes

Encoding polynomial

Given the message vector $a \in \mathbb{F}_q^k$, define the **encoding polynomial** as:

$$f_a(x) = \sum_{i=0}^{r-1} x^i \cdot f_i(x)$$

where

$$f_i(x) = \sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j$$

$$f_a(x) = \begin{pmatrix} x^0 & \dots & x^{r-1} \end{pmatrix} \begin{pmatrix} a_{0,0} & \cdots & a_{0,\frac{k}{r}-1} \\ \vdots & \ddots & \vdots \\ a_{r-1,0} & \cdots & a_{r-1,\frac{k}{r}-1} \end{pmatrix} \begin{pmatrix} g(x)^0 \\ \vdots \\ g(x)^{\frac{k}{r}-1} \end{pmatrix} =$$

$$= \begin{pmatrix} x^0 & \dots & x^{r-1} \end{pmatrix} \begin{pmatrix} f_0(x) \\ \vdots \\ f_{r-1}(x) \end{pmatrix}$$

The codeword for $a \in \mathbb{F}_q^k$ is found as the evaluation vector of f_a at all the points of A.

LRC code

The (n, k, r) LRC code $\mathcal{C}$ is defined as the set of n-dimensional vectors

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

Remark

$$x \in A_i \Rightarrow \quad g(x) \ constant$$

$$\Rightarrow f_\ell(x) = \sum_{j=0}^{\frac{k}{r}-1} a_{\ell j} g(x)^j \ constant \ in \ A_i$$

$$\Rightarrow deg(f_a(x)) = deg(\sum_{j=0}^{r-1} x^j \cdot f_j(x)) \leq r-1 \ in \ A_i$$

Recovery of the erased symbol

Suppose erased symbol: $\alpha \in A_j$.
Let $(c_\beta,\ \beta \in A_j \setminus \alpha)$ denote the remaining r symbols of the recovering set.
To find the value $c_\alpha = f_a(\alpha)$, find the unique polynomial $\delta(x)$ s.t.

- $\deg(\delta(x)) \leq r$
- $\delta(\beta) = c_\beta \quad \forall \beta \in A_j \setminus \alpha$

This polynomial is:

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

Finally, set $c_\alpha = \delta(\alpha)$.

Theorem

The linear code $\mathcal{C}$ defined has dimension k and is an optimal (n, k, r) LRC code.

Proof of dimension.

For $i \in \{0, \ldots, r-1\}$; $j \in \{0, \ldots, \frac{k}{r-1}\}$ the k polynomials $g(x)^j x^i$ all are of distinct degrees, i.e. linearly independent over $\mathbb{F}$.
$\Rightarrow$ The mapping $a \mapsto f_a$ is injective.

$$\deg(f_a(x)) \leq \deg(x^{r-1}) + \deg(g(x)^{\frac{k}{r}-1}) = r - 1 + (r+1)(\frac{k}{r} - 1)$$

$$= k + \frac{k}{r} - 2 \leq n - 2$$

This means that two distinct encoding polynomials give rise to two distinct codevectors. $\Rightarrow$ The dimension of the code is k. $\square$

Proof of optimality.

Since the encoding is linear:

$$d(\mathcal{C}) \geq n - \max_{f_a, a \in \mathbb{F}_q^k} \deg(f_a) = n - k - \frac{k}{r} + 2 \geq n - k - \left\lceil \frac{k}{r} \right\rceil + 2$$

But we have that $d(\mathcal{C}) \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2$. Therefore, we have equality and thus it is an optimal LRC Code. □

Example: (9,4,2) LRC code

We will now construct a $(n = 9, k = 4, r = 2)$ LRC code over the field $\mathbb{F}_q$.

$$q = |\mathbb{F}_q| \geq n \quad \Rightarrow \quad q \geq 9$$

Choose $q = 13$

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

.

$$g(x) = x^3 = \begin{cases} 1 & \text{if } x \in A_1 \\ 8 & \text{if } x \in A_2 \\ 12 & \text{if } x \in A_3 \end{cases}$$

For $a = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \in \mathbb{F}_{13}^4$ define the encoding polynomial:

$$f_a(x) = \begin{pmatrix} 1 & x \end{pmatrix} \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} 1 \\ x^3 \end{pmatrix} = a_{00} + a_{10}x + a_{01}x^3 + a_{11}x^4$$

E.g. $a = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. $f_a(x) = 1 + x + x^3 + x^4$

$$c = (f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$= (4, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(4, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(\cancel{f_a(1)}, f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(\cancel{4}, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(\cancel{f_a(1)}, f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(\cancel{4}, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$1 \in A_1 = \{1, 3, 9\}$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(\cancel{f_a(1)}, f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(\cancel{4}, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$1 \in A_1 = \{1, 3, 9\}$$

$$\Rightarrow \delta(x) = c_3 \frac{x - 9}{3 - 9} + c_9 \frac{x - 3}{9 - 3} = 2x + 2$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(\cancel{f_a(1)}, f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(\cancel{4}, 8, 7, 1, 11, 2, 0, 0, 0)$$

$$1 \in A_1 = \{1, 3, 9\}$$

$$\Rightarrow \delta(x) = c_3 \frac{x - 9}{3 - 9} + c_9 \frac{x - 3}{9 - 3} = 2x + 2$$

$$\delta(1) = 4$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), \cancel{f_a(2)}, f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(4, 8, 7, \cancel{1}, 11, 2, 0, 0, 0)$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), \xcancel{f_a(2)}, f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(4, 8, 7, \xcancel{1}, 11, 2, 0, 0, 0)$$

$$2 \in A_2 = \{2, 6, 5\}$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), \cancel{f_a(2)}, f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(4, 8, 7, \cancel{1}, 11, 2, 0, 0, 0)$$

$$2 \in A_2 = \{2, 6, 5\}$$

$$\Rightarrow \delta(x) = c_6 \frac{x-5}{6-5} + c_5 \frac{x-6}{5-6} = 9x + 9$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), \cancel{f_a(2)}, f_a(6), f_a(5), f_a(4), f_a(12), f_a(10))$$

$$(4, 8, 7, \cancel{1}, 11, 2, 0, 0, 0)$$

$$2 \in A_2 = \{2, 6, 5\}$$

$$\Rightarrow \delta(x) = c_6 \frac{x-5}{6-5} + c_5 \frac{x-6}{5-6} = 9x + 9$$

$$\delta(2) = 1$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), \xcancel{f_a(4)}, f_a(12), f_a(10))$$

$$(4, 8, 7, 1, 11, 2, \xcancel{0}, 0, 0)$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), \cancel{f_a(4)}, f_a(12), f_a(10))$$

$$(4, 8, 7, 1, 11, 2, \cancel{0}, 0, 0)$$

$$4 \in A_3 = \{4, 12, 10\}$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), \cancel{f_a(4)}, f_a(12), f_a(10))$$

$$(4, 8, 7, 1, 11, 2, \cancel{0}, 0, 0)$$

$$4 \in A_3 = \{4, 12, 10\}$$

$$\Rightarrow \delta(x) = c_{12} \frac{x - 10}{12 - 10} + c_{10} \frac{x - 12}{10 - 12} = 0$$

$$\delta(x) = \sum_{\beta \in A_j \setminus \alpha} c_\beta \prod_{\beta' \in A_j \setminus \{\alpha, \beta\}} \frac{x - \beta'}{\beta - \beta'}$$

$$(f_a(1), f_a(3), f_a(9), f_a(2), f_a(6), f_a(5), \cancel{f_a(4)}, f_a(12), f_a(10))$$

$$(4, 8, 7, 1, 11, 2, \cancel{0}, 0, 0)$$

$$4 \in A_3 = \{4, 12, 10\}$$

$$\Rightarrow \delta(x) = c_{12} \frac{x - 10}{12 - 10} + c_{10} \frac{x - 12}{10 - 12} = 0$$

$$\delta(4) = 0$$

Example of LRC-2 code

Let $\mathbb{F} = \mathbb{F}_{13}$, $A = \mathbb{F} \setminus \{0\}$
$\mathcal{A} = \{\{1,5,12,8\},\{2,10,11,3\},\{4,7,9,6\}\}$
$\mathcal{A}' = \{\{1,3,9\},\{2,6,5\},\{4,12,10\},\{7,8,11\}\}$
$f_a(x) = a_0 + a_1 x + a_2 x^4 + a_3 x^6$
$a = (1,1,1,1)$
$c = (4,8,7,5,2,6,2,2,2,3,9,1)$
As already seen: $\delta(x) = 2x+2$; $\delta(1) = 4$.

$$\delta'(x) = c_5 \frac{x-12}{5-12}\frac{x-8}{5-8} + c_{12}\frac{x-5}{12-5}\frac{x-8}{12-8} + c_8 \frac{x-5}{8-5}\frac{x-12}{8-12}$$

$$= 6\cdot 5\cdot (x^2+6x+5) + 2\cdot 7\cdot (x^2+1) + 9\cdot 1\cdot (x^2+9x+8)$$

$$= x^2 + x + 2 \quad \longrightarrow \quad \delta'(1) = 4$$

Every coordinate i has t disjoint recovering sets $R_1^i, \ldots, R_j^i$, each of size r, where $R_j^i \subset [n] \setminus i$.

Definition

The **recovering graph** of a (n, k, r, t) LRC code $\mathcal{C}$ is an directed graph $G = (V, E)$ where:

- $V = [n]$. The set of vertices corresponds the set of n coordinates of $\mathcal{C}$.
- $(i, j) \in E \iff j \in R_l^i$ for some $l \in [t]$.
  There is an edge $i \to j$ if j is in a recovering set of i.
  Note that $N(i) = \bigcup_{l=1}^{t} R_l^i$