Journées Codage et Cryptographie
Najac, 17/10/2023.

Introducing locality in some generalized AG codes

Bastien Pacifico
ECo, LIRMM, Montpellier.

Plan

1. Background
   - Linear codes
   - Locally Recoverable Codes
   - Reed-Solomon Codes
   - AG Codes
   - Generalized AG Codes
2. Locality in generalized AG code
   - Proposition
   - An optimal example
   - More examples

Linear codes

A linear code $\mathcal{C} \subset \mathbb{F}_q^n$ is a linear subspace.

We denote by $[n, k, d]$ a code if

- n is its length,
- k is its dimension,
- d is its minimum distance.

Theorem (Singleton Bound)

$$d \leqslant n - k + 1.$$

Such a code can be defined by the image of an injective map $\mathbb{F}_q^k \longrightarrow \mathbb{F}_q^n$.

Locally Recoverable Codes (LRC)

Definition

Let $\mathcal{C} \subset \mathbb{F}_q^n$ be a $\mathbb{F}_q-$linear code. The code $\mathcal{C}$ is locally recoverable with locality r if every symbol of a codeword $c = (c_1, \ldots, c_n) \in \mathcal{C}$ can be recovered using a subset of at most r other symbols. The smallest such r is called the locality of the code.

$$(c_1, \cdots, c_{i-1}, \cancel{c_i}, c_{i+1}, \ldots, c_{n-1}, c_n)$$

Theorem (Singleton Bound for LRC)

Let $\mathcal{C}$ be a $q-$ary linear code with parameters $[n, k, d]$ with locality r. The minimum distance d of $\mathcal{C}$ verifies

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

Reed-Solomon codes

A Reed-Solomon code $RS(n, k)$ of length n and dimension k is defined by the image of an application

$$RS(n,k): \begin{array}{ccc} \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(\alpha_1), \ldots, f(\alpha_n)), \end{array}$$

where $\alpha_1, \ldots, \alpha_n$ are distinct elements of $\mathbb{F}_q$.

The minimum distance of $RS(n, k)$ veririfes

$$d = n - k + 1.$$

Reed-Solomon codes

A Reed-Solomon code $RS(n,k)$ of length n and dimension k is defined by the image of an application

$$RS(n,k): \begin{array}{lcl} \mathbb{F}_q[x]_{<k} & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(\alpha_1),\dots,f(\alpha_n)), \end{array}$$

where $\alpha_1,\dots,\alpha_n$ are distinct elements of $\mathbb{F}_q$.

The minimum distance of $RS(n,k)$ veririfes

$$d = n - k + 1.$$

This gives codes of length at most q, we need more evaluation points !

More evaluation points

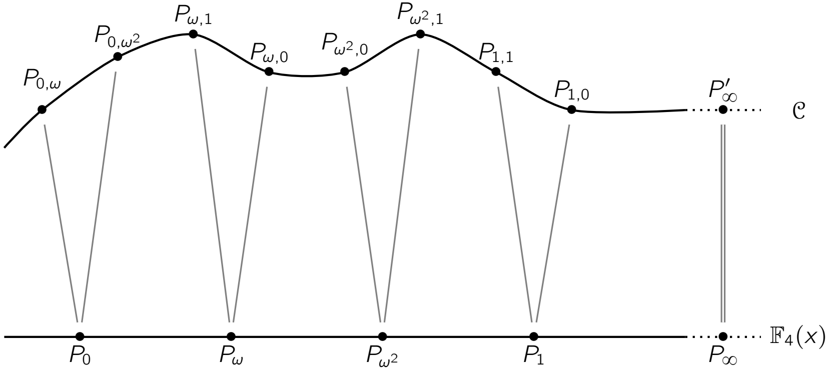


Figure: Decomposition of the rational places of $\mathbb{F}_4(x)$ in the Hermitian function field, associated to the curve defined by the equation $y^2 + y = x^3 + 1$.

Algebraic-Geometric (AG) codes

Let $F/\mathbb{F}_q$ be a function field of genus g.
Let $\mathcal{D}$ and G be divisors of F, with $\mathcal{D} = P_1 + \cdots + P_n$, where $P_i, \dots, P_n$ are distinct rational places of F.
An AG code $\mathcal{C}(\mathcal{D}, G)$ is defined by the image of an application

$$\mathcal{C}(\mathcal{D}, G) : \begin{array}{ccc} \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (f(P_1), \dots, f(P_n)) . \end{array}$$

If $2g - 2 < \deg G < n$, the code $\mathcal{C}(\mathcal{D}, G)$ has dimension

$$k = \deg(G) - g + 1$$

and minimum distance

$$d \geqslant n - \deg(G).$$

Examples : RS codes are AG codes

Let $\mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$.

- Rational places are given by the elements of $\mathbb{F}_q$ $(+P_\infty)$.
- Set $G = (k-1)P_\infty$. Then $\mathcal{L}(G) = \mathbb{F}_q[x]_{\leqslant k-1}$.

Examples : RS codes are AG codes

Let $\mathbb{F}_q(x)$ be the rational function field over $\mathbb{F}_q$.

- Rational places are given by the elements of $\mathbb{F}_q$ $(+P_\infty)$.
- Set $G = (k-1)P_\infty$. Then $\mathcal{L}(G) = \mathbb{F}_q[x]_{\leqslant k-1}$.

Useful example : Let $\mathbb{F}_3(x)$ be the rational function field over $\mathbb{F}_3$.
Let $G = P_\infty$ and $\mathcal{D} = P_0 + P_1 + P_2$.

$$\mathcal{C}(\mathcal{D}, G) : \begin{array}{lcl} \mathcal{L}(P_\infty) & \longrightarrow & \mathbb{F}_3^3 \\ f & \longmapsto & (f(P_0), f(P_1), f(P_2)) \,. \end{array}$$

$$=$$

$$RS(3,2) : \begin{array}{lcl} \mathbb{F}_3[x]_{<2} & \longrightarrow & \mathbb{F}_3^3 \\ f & \longmapsto & (f(0), f(1), f(2)) \,. \end{array}$$

Places of higher degrees of $\mathbb{F}_q(x)$ / Irreducible polynomials

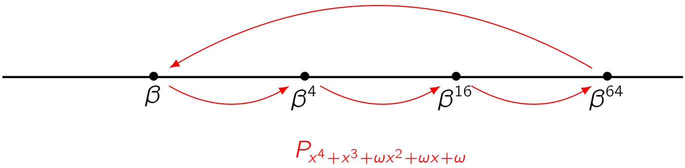


Figure: $P_{x^4+x^3+\omega x^2+\omega x+\omega}$ is a degree 4 place of $\mathbb{F}_4(x)$

Places of higher degrees

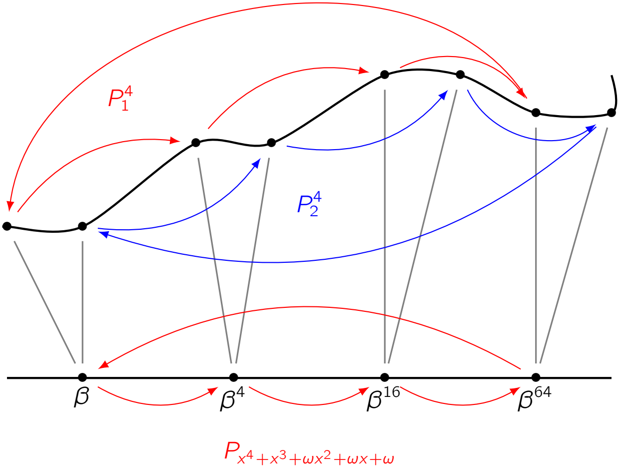


Figure: $P_{x^4+x^3+\omega x^2+\omega x+\omega}$ is totally decomposed in $F/\mathbb{F}_4$

Generalized AG codes[1]

Let $F/\mathbb{F}_q$ be an algebraic function field defined over $\mathbb{F}_q$ of genus g, and

- $P_1, \ldots, P_s$ are s distinct places of F,
- G is a divisor of F such that $Supp(G) \bigcap \{P_1, \ldots, P_s\} = \emptyset$,

and for $1 \leqslant i \leqslant s$:

- $k_i = \deg(P_i)$ the degree of P_i,
- C_i is a $[n_i, k_i, d_i]_q$ linear code,
- π_i is a fixed $\mathbb{F}_q-$linear isomorphism mapping $\mathbb{F}_{q^{k_i}}$ to C_i.

Consider the application

$$\alpha \ : \ \begin{array}{lcl} \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n \\ f & \longmapsto & (\pi_1(f(P_1)), \ldots, \pi_s(f(P_s))) \,. \end{array} \,.$$

Definition

The image of α is called a generalized algebraic-geometric code, denoted by $C(P_1, \ldots, P_s : G : C_1, \ldots, C_s)$.

[1] Xing, Niederreiter and Lam, *A Generalization of Algebraic-Geometric Codes*, 1999.

Proposition

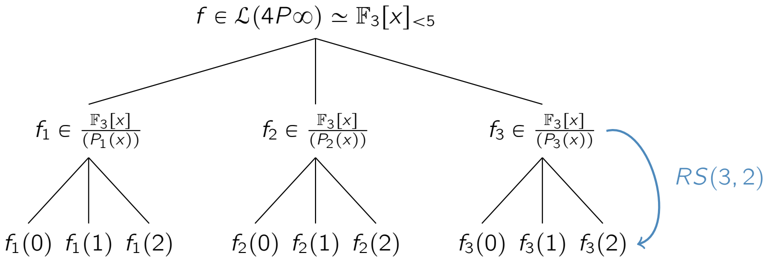
Observation : if $k_1 = \ldots = k_s =: k$, the code defined above has locality k. More formally,

Proposition

Let $\mathcal{C} = C(P_1, \ldots, P_s : G : C_1, \ldots, C_s)$ be a generalized AG-code as in the previous slide.
If there exists $r \in \mathbb{N}$ such that for all $1 \leqslant i \leqslant s$, we have $1 < k_i \leqslant r$, $n_i > \deg(P_i)$, and C_i has locality k_i, then $\mathcal{C}$ has locality r.

An optimal example

Let $\mathbb{F}_3(x)$ be the rational function field. Set $G = 4P_\infty$.
Let $P_1(x) = x^2 + 2x + 2$, $P_2(x) = x^2 + 1$, and $P_3(x) = x^2 + x + 2$,
and the Reed-Solomon code $RS(3,2)$: $\begin{array}{ccc} \mathbb{F}_3[x]_{<2} & \longrightarrow & \mathbb{F}_q^3 \\ f & \longmapsto & (f(0), f(1), f(2)) \end{array}$.



The code $C(P_1, P_2, P_3 : 4P_\infty : RS(3,2), RS(3,2), RS(3,2))$ is a $[9,5,3]$ linear code with locality 2, reaching the Singleton Bound for LRC .

More examples : set-up

We constructed several codes over $\mathbb{F}_3$ using evaluation at (random) places of degree 2, then encoding the evaluations with $RS(3,2)$ as previously.

We use the following curves.

- The rational function field $\mathbb{F}_3(x)$, of genus 0, that contains 3 places of degree 2. Then one can construct codes of length at most 9.
- The elliptic curve defined by the equation $y^2 = x^3 + x$ of genus 1, that contains 6 places of degree 2. Then one can construct codes of length at most 18.
- The Klein quartic defined by the equation $x^4 + y^4 + 1 = 0$ of genus 3, that contains 12 places of degree 2. Then one can construct codes of length at most 36.

This gives $[3s, k, d]$ linear code with locality 2, where s is the number of places of degree 2 used in the construction.

More examples : results

		$\mathbb{F}_3(x)$		$y^2 = x^3 + x$		$x^4 + y^4 + 1$	
n	k	d	defect	d	defect	d	defect
9	3	4	2	4	2	4	2
	4	4	1	4	1	4	1
	5	3	0	3	0	3	0
12	4	-	-	5	3	6	2
	5	-	-	4	2	4	2
	6	-	-	3	2	4	1
15	5	-	-	6	3	6	3
	6	-	-	4	4	5	3
	7	-	-	4	2	4	2
	8	-	-	3	2	4	1
18	6	-	-	6	5	6	5
	7	-	-	6	3	6	3
	8	-	-	4	4	4	4
	9	-	-	4	2	4	2
	10	-	-	2	3	3	2
21	7	-	-	-	-	8	4
	8	-	-	-	-	6	5
	9	-	-	-	-	5	4
	10	-	-	-	-	4	4
	11	-	-	-	-	4	2
	12	-	-	-	-	4	1
24	8	-	-	-	-	8	6
	9	-	-	-	-	7	5
	10	-	-	-	-	6	5
	11	-	-	-	-	6	3
	12	-	-	-	-	4	4
	13	-	-	-	-	4	2
	14	-	-	-	-	3	2
	15	-	-	-	-	3	1
27	9	-	-	-	-	8	7
	10	-	-	-	-	8	6
	11	-	-	-	-	7	5

		$x^4 + y^4 + 1$	
n	k	d	defect
27	12	6	5
	13	6	3
	14	4	4
	15	4	2
	16	3	2
30	10	10	7
	11	8	7
	12	7	7
	13	7	5
	14	6	5
	15	6	3
	16	4	4
	17	4	2
	18	3	2
33	11	10	8
	12	10	7
	13	8	7
	14	8	6
	15	6	6
	16	6	5
	17	5	4
	18	4	4
	19	4	2
36	12	10	10
	13	10	8
	14	8	9
	15	8	7
	16	6	8
	17	6	6
	18	5	6
	19	4	5
	20	4	4

Table: Parameters of obtained linear codes over $\mathbb{F}_3$ with locality 2.

Thanks for your attention!