Locally recoverable codes from towers of function fields

Francisco Galluccio[1],
joint with Maria Chara[1] and Edgar Martinez-Moro[2]

[1]Universidad Nacional del Litoral
[2]Universidad de Valladolid

Conference **O**n al**G**ebraic varieties over fi**N**ite fields and **A**lgebraic geometry **C**odes
CIRM, February 2023

LRC Codes

LRC Codes

Let q be a prime power. A code $\mathscr{C}$ of length n is a subset of $\mathbb{F}_q^n$.

Dimension $k = \log_q(|\mathscr{C}|)$
Minimum distance $d = \min |\{i \in [n] : x_i \neq y_i\}|$

LRC Codes

Let q be a prime power. A code $\mathscr{C}$ of length n is a subset of $\mathbb{F}_q^n$.

Dimension $k = \log_q(|\mathscr{C}|)$
Minimum distance $d = \min |\{i \in [n] : x_i \neq y_i\}|$

If $\mathscr{C} \subset \mathbb{F}_q^n$ is a subspace, then k is integer and $d = \min |\{i \in [n] : x_i \neq 0\}|$

LRC Codes

Let q be a prime power. A code $\mathscr{C}$ of length n is a subset of $\mathbb{F}_q^n$.

Dimension $k = \log_q(|\mathscr{C}|)$
Minimum distance $d = \min |\{i \in [n] : x_i \neq y_i\}|$

If $\mathscr{C} \subset \mathbb{F}_q^n$ is a subspace, then k is integer and $d = \min |\{i \in [n] : x_i \neq 0\}|$

Clearly, given any $n-d+1$ coordinates of a codeword x, it is posible to recover all the remaining $d-1$ coordinates.

LRC Codes

Let q be a prime power. A code $\mathscr{C}$ of length n is a subset of $\mathbb{F}_q^n$.

Dimension $k = \log_q(|\mathscr{C}|)$
Minimum distance $d = \min |\{i \in [n] : x_i \neq y_i\}|$

If $\mathscr{C} \subset \mathbb{F}_q^n$ is a subspace, then k is integer and $d = \min |\{i \in [n] : x_i \neq 0\}|$

Clearly, given any $n-d+1$ coordinates of a codeword x, it is posible to recover all the remaining $d-1$ coordinates.
¿It is possible to recover any coordinate x_i with fewer than $n-d+1$ other coordinates?

Gopalan gave a first definition of an LRC code, which now state as

Definition (LRC Codes)

A code $\mathscr{C} \subset \mathbb{F}_q^n$ is locally recoverable (LRC) with locality r if the value of every coordinate of the codeword can be found by accessing at most r other coordinates of this codeword. That is, for every $i \in [n]$ exists $A_i \subset [n] \setminus \{i\}$ with $|A_i| \leq r$ and a function $\phi_i : \mathbb{F}_q^{|A_i|} \to \mathbb{F}_q$ s.t. $\forall x \in \mathscr{C}$

$$x_i = \phi_i(x_{j_1}, \ldots, x_{j_{|A_i|}})$$

where $A_i = \{j_1, \ldots, j_{|A_i|}\}$

For $\mathscr{C} \subset \mathbb{F}_q^n$ of length n, dimension k and locality r, we will say $\mathscr{C}$ is a (n, k, r) LRC code.

As an example

$$\mathscr{C} = \{000000, 001111, 111100, 110011\} \subset \mathbb{F}_2^6$$

is a repetition code in which every codeword $x \in \mathscr{C}$ verifies $x_{2j} = x_{2j-1}$ for $j = 1, 2, 3$, so $\mathscr{C}$ is a $(6, 2, 1)$ LRC code with locality 1.

It has enormous *redundancy*, since only two out of the six coordinates (1st and 3rd coordinate) carry information.

LRC RS Codes

LRC RS Codes

Barg and Tamo gave the following construction of LRC codes based on the Reed Solomon codes:

- Consider parameters (n, k, r) with $n \leq q$, $r+1 \mid n$ and $r \mid k$.
- Let $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$ distinct points,
- $\mathscr{A} = \{A_1, \ldots, A_{\frac{n}{r+1}}\}$ a partition of A.
- Suppose exists $g(x) \in \mathbb{F}_q[x]$ of degree $r+1$, constant on each A_i.

LRC RS Codes

Barg and Tamo gave the following construction of LRC codes based on the Reed Solomon codes:

- Consider parameters (n,k,r) with $n \leq q$, $r+1 \mid n$ and $r \mid k$.
- Let $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$ distinct points,
- $\mathscr{A} = \{A_1, \ldots, A_{\frac{n}{r+1}}\}$ a partition of A.
- Suppose exists $g(x) \in \mathbb{F}_q[x]$ of degree $r+1$, constant on each A_i.

The space

$$V = \left\langle g(x)^j x^i : 0 \leq i \leq r-1, 0 \leq j \leq \frac{k}{r} - 1 \right\rangle \subset \mathbb{F}_q[x]$$

is of dimension $r \cdot \frac{k}{r} = k$ with

$$a = (a_{ij}) \in \mathbb{F}_q^k \mapsto f_a = \sum_{i=0}^{r-1} \sum_{j=0}^{k/r-1} a_{ij} g(x)^j x^i.$$

The evaluation map $ev : V \to \mathbb{F}_q^n$ with

$$f_a \mapsto (f_a(P_1), \ldots, f_a(P_n))$$

is injective, so this gives rise to a $(n, k, d \geq n - k - \frac{k}{r} + 2)$ code $\mathscr{C}$.

The evaluation map $ev : V \to \mathbb{F}_q^n$ with

$$f_a \mapsto (f_a(P_1), \ldots, f_a(P_n))$$

is injective, so this gives rise to a $(n, k, d \geq n - k - \frac{k}{r} + 2)$ code $\mathscr{C}$.

It is LRC with locality r: each f_a restricted to A_i can be viewed as a polynomial $\delta_i(x)$ of degree less at most $r - 1$, and thus can be determined by polynomial interpolation in any r elements of A_i.

The evaluation map $ev : V \to \mathbb{F}_q^n$ with

$$f_a \mapsto (f_a(P_1), \ldots, f_a(P_n))$$

is injective, so this gives rise to a $(n, k, d \geq n - k - \frac{k}{r} + 2)$ code $\mathscr{C}$.

It is LRC with locality r: each f_a restricted to A_i can be viewed as a polynomial $\delta_i(x)$ of degree less at most $r-1$, and thus can be determined by polynomial interpolation in any r elements of A_i.

Proposition (Singleton bound)

For $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$ it holds $R < \frac{r}{r+1}(1-\delta) < \frac{r}{r+1}$

The evaluation map $ev : V \to \mathbb{F}_q^n$ with

$$f_a \mapsto (f_a(P_1), \ldots, f_a(P_n))$$

is injective, so this gives rise to a $(n, k, d \geq n - k - \frac{k}{r} + 2)$ code $\mathscr{C}$.

It is LRC with locality r: each f_a restricted to A_i can be viewed as a polynomial $\delta_i(x)$ of degree less at most $r-1$, and thus can be determined by polynomial interpolation in any r elements of A_i.

Proposition (Singleton bound)

For $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$ it holds $R < \frac{r}{r+1}(1-\delta) < \frac{r}{r+1}$

Proposition (Barg,Tamo,Vladut bound)

There exist $\mathscr{C} \subset \mathbb{F}_{q^2}$ s.t. its relative parameters verify

$$R \geq \frac{r}{r+1}\left(1 - \delta - \frac{3}{q+1}\right),$$

AG Codes

We now give a brief definition of an AG Codes, based on the RS codes

Definition

Let X be a smooth projective irreducible curve defined over $\mathbb{F}_q$. Set $\mathbb{F}_q(X)$ its function field, and chose a divisor $D = \sum a_i Q_i$ of situable degree $l \geq 1$.

AG Codes

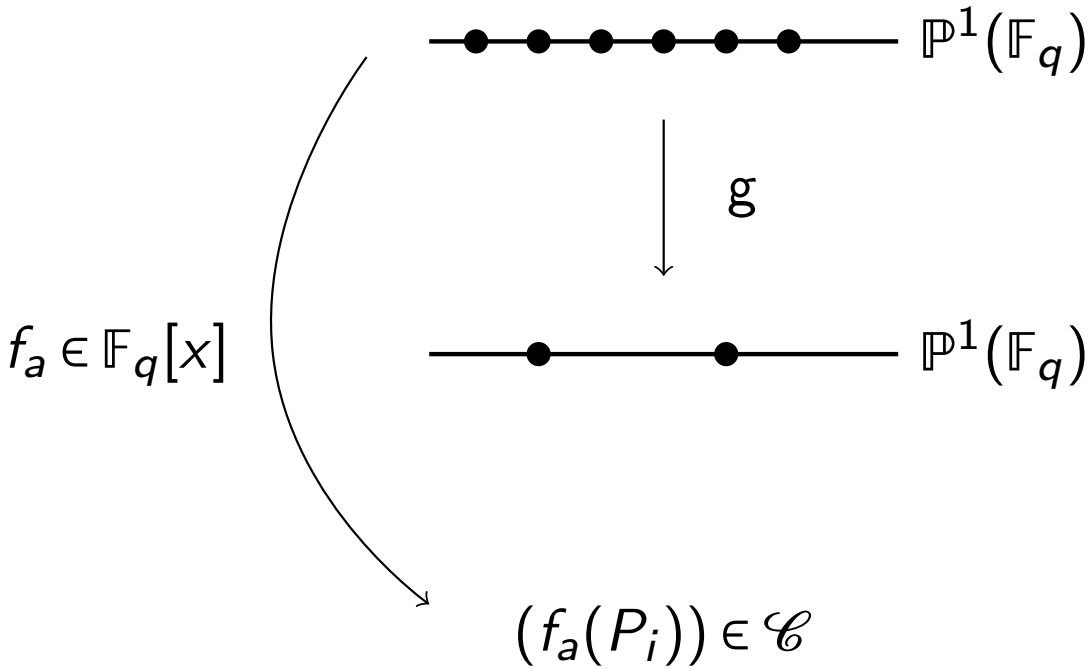
We now give a brief definition of an AG Codes, based on the RS codes

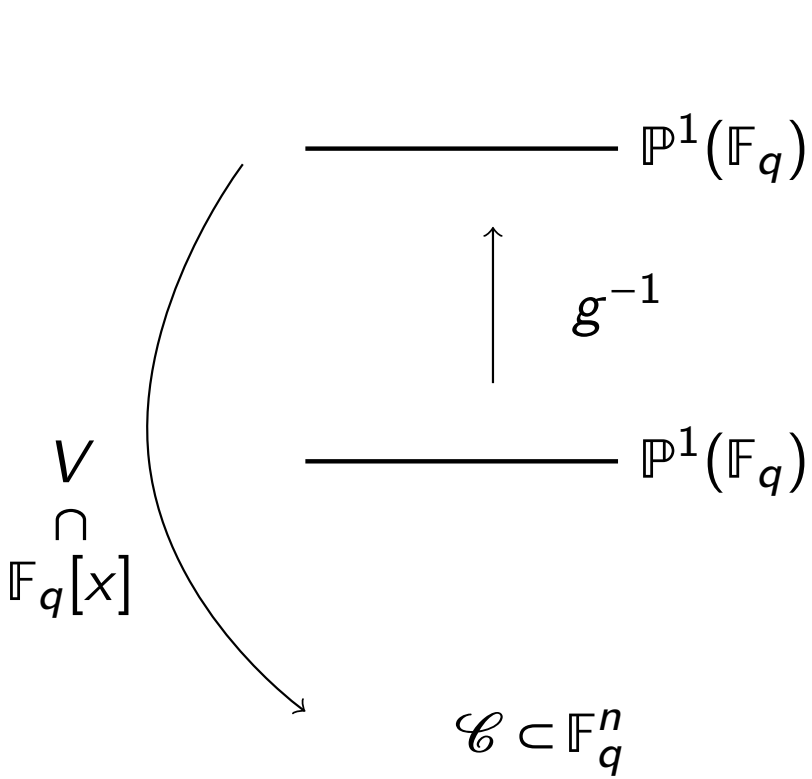
Definition

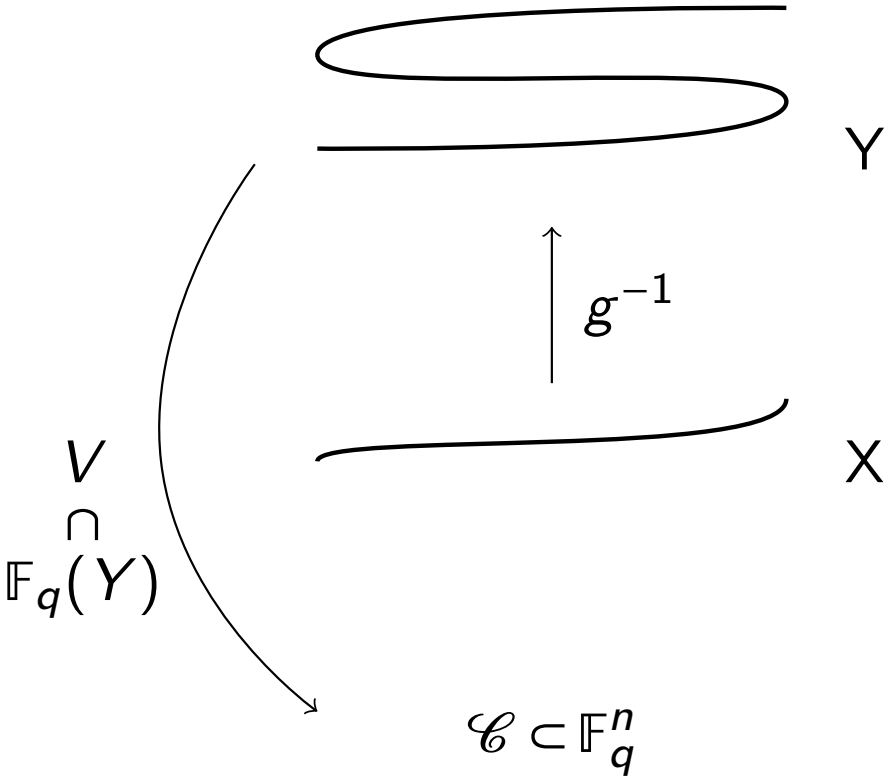
Let X be a smooth projective irreducible curve defined over $\mathbb{F}_q$. Set $\mathbb{F}_q(X)$ its function field, and chose a divisor $D = \sum a_i Q_i$ of situable degree $l \geq 1$.
Suppose $\mathscr{B} \subset X(\mathbb{F}_q)$ is a subset of n $\mathbb{F}_q$-rational points disjoint of $supp(D)$. For $\mathscr{L}(D)$ the Rieman-Roch space associated to D, the code $\mathscr{C} = \mathscr{C}(D, \mathscr{B})$ given by the evaluation map

$$\begin{aligned} ev : \mathscr{L}(D) &\to \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

is a (n, k, d) code where $k = \ell(D) = \dim \mathscr{L}(D)$ and $d \geq n - l$.


$\mathbb{P}^1(\mathbb{F}_q)$
g
$f_a \in \mathbb{F}_q[x]$
$\mathbb{P}^1(\mathbb{F}_q)$
$(f_a(P_i)) \in \mathscr{C}$


$\mathbb{P}^1(\mathbb{F}_q)$
g^{-1}
$\mathbb{P}^1(\mathbb{F}_q)$
V
$\cap$
$\mathbb{F}_q[x]$
$\mathscr{C} \subset \mathbb{F}_q^n$


Y
g^{-1}
X
V
$\cap$
$\mathbb{F}_q(Y)$
$\mathscr{C} \subset \mathbb{F}_q^n$

LRC AG Codes

LRC AG Codes

More precisely, we have a construction of LRC AG codes

Theorem (Barg, Tamo, Vladut)

For $S = \{P_1, \ldots, P_s\} \subset X(\mathbb{F}_q)$ a set of rational points,
$\mathscr{B} = g^{-1}(S) = \{P_{ij}\} \subset Y$ a set of rs rational points,
$\mathscr{L}(D) = \langle f_1, \ldots, f_m \rangle$ for a suitable divisor, and $y \in \mathbb{F}_q(Y)$ such that $\mathbb{F}_q(Y) = \mathbb{F}_q(X)(y)$, then for

$$V = \left\langle f_l x^i : 1 \leq l \leq m, 0 \leq i \leq r-1 \right\rangle$$

one obtain a LRC code $\mathscr{C}$ of locality $r = deg(g)$ and parameters

$$n = (r+1)s, \quad k = r\ell(D) \geq r(deg(D) - g_X + 1),$$

$$d \geq n - deg(D)(r+1) - (r-1)deg(x)$$

provided d is a positive integer.

For the case of more than one recovery set, there also is another important construction

Theorem (Haymaker, Malmskog, Matthews)

For $S = \{P_1, \ldots, P_s\} \subset X$ a set of rational points, $Y_1, \ldots, Y_t$ curves such that $\mathbb{F}_q(Y_j) = \mathbb{F}_q(X)(x_j)$, $Y = Y_1 \times_X \ldots \times_X Y_t$ the fiber product, $\mathscr{L}(D) = \langle f_1, \ldots, f_m \rangle$ for a suitable divisor of X, then for

$$V = \left\langle f_l x_1^{e_1} \cdots x_t^{e_t} : 1 \leq l \leq m, 0 \leq e_i \leq d_i - 2 \right\rangle$$

one obtain a LRC code $\mathscr{C}$ of locality $d_i - 1$ and parameters

$$n = rs, \quad k = \ell(D)(d_1 - 1) \cdots (d_t - 1),$$

$$d \geq n - deg(D)r - \sum (d_i - 1) deg(x_i)[\mathbb{F}_q(Y) : \mathbb{F}_q(Y_j)]$$

provided d is a positive integer.

Construction on Function Fields

Construction on Function Fields

Theorem

$F/\mathbb{F}_q$ function field, and let E/F function field extension of degree m. $S \subset \mathbb{P}(F)$ set of s places that split completely in E/F s.t.

$$\{Q \in \mathbb{P}(E) : Q \cap F \in S\} \cap \{Q \in \mathbb{P}(E) : v_Q(x) < 0\} = \emptyset$$

and let $\mathscr{B} = \{Q \in \mathbb{P}(E) : Q = P \cap F$ for some P in $S\}$, so $|\mathscr{B}| = sm$.

Construction on Function Fields

Theorem

$F/\mathbb{F}_q$ function field, and let E/F function field extension of degree m. $S \subset \mathbb{P}(F)$ set of s places that split completely in E/F s.t.

$$\{Q \in \mathbb{P}(E) : Q \cap F \in S\} \cap \{Q \in \mathbb{P}(E) : \nu_Q(x) < 0\} = \emptyset$$

and let $\mathscr{B} = \{Q \in \mathbb{P}(E) : Q = P \cap F$ for some P in $S\}$, so $|\mathscr{B}| = sm$. For a divisor D of F of degree l and $supp(D) \cap S = \emptyset$, let $\{f_1, \ldots, f_\ell\}$ a basis for $\mathscr{L}(D)$.

Construction on Function Fields

Theorem

$F/\mathbb{F}_q$ function field, and let E/F function field extension of degree m. $S \subset \mathbb{P}(F)$ set of s places that split completely in E/F s.t.

$$\{Q \in \mathbb{P}(E) : Q \cap F \in S\} \cap \{Q \in \mathbb{P}(E) : \nu_Q(x) < 0\} = \emptyset$$

and let $\mathscr{B} = \{Q \in \mathbb{P}(E) : Q = P \cap F \text{ for some } P \text{ in } S\}$, so $|\mathscr{B}| = sm$. For a divisor D of F of degree l and $supp(D) \cap S = \emptyset$, let $\{f_1, \ldots, f_\ell\}$ a basis for $\mathscr{L}(D)$. Then for $r = m-1$, consider the space $V = \langle f_w x^e : w = 1, \ldots, \ell; e = 0, \ldots, r-1 \rangle$,

$$\begin{array}{rccc} ev: & V & \longrightarrow & \mathbb{F}_q^{(r+1)s} \\ & f & \to & (f(P_{11}), \ldots, f(P_{ms})) \end{array}$$

is well defined and gives a LRC code $\mathscr{C} = C(S, D)$ with locality r. The code coordinates are naturally partitioned into s subsets $A_j = \{P_{ij}\}_{i=1,\ldots,r+1}$.

Denoting by $g(F)$ the genus of F and $h = [E : \mathbb{F}_q(x)]$, we have that the parameters of the code satisfy

$$\begin{aligned} n &= (r+1)s \\ k &= r\ell \geq r(l+1-g(F)) \\ d &\geq n - l(r+1) - (r-1)h \end{aligned}$$

provided that the right-hand side of the inequality for d is a positive integer.

Denoting by $g(F)$ the genus of F and $h = [E : \mathbb{F}_q(x)]$, we have that the parameters of the code satisfy

$$\begin{aligned} n &= (r+1)s \\ k &= r\ell \geq r(l+1-g(F)) \\ d &\geq n - l(r+1) - (r-1)h \end{aligned}$$

provided that the right-hand side of the inequality for d is a positive integer.

Local recovery of an erased symbol $c_{ij} = f(P_{ij})$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A_j \setminus \{P_{ij}\}$.

Towers of Function Fields

Towers of Function Fields

We consider a sequence $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ of function fields such that

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots$
- F_{i+1}/F_i is finite separable for any $i \geq 0$,
- $\mathbb{F}_q \subset F_i$ is algebraically closed for any $i \geq 0$

We say $\mathscr{F}$ is a *tower* if the genus $g(F_i)$ grows to infinity as $i \to \infty$.

Towers of Function Fields

We consider a sequence $\mathscr{F} = (F_0, F_1, F_2, \ldots)$ of function fields such that

- $F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \ldots$
- F_{i+1}/F_i is finite separable for any $i \geq 0$,
- $\mathbb{F}_q \subset F_i$ is algebraically closed for any $i \geq 0$

We say $\mathscr{F}$ is a *tower* if the genus $g(F_i)$ grows to infinity as $i \to \infty$.

Although is not needed, we may suppose that exist some polynomial $f(x, y)$ such that $F_0 = \mathbb{F}_q(x_0)$ and $F_{i+1} = F_i(x_{i1})$ where $f(x_i, x_{i+1}) = 0$ and

$$[F_{i+1} : F_i] = \deg f.$$

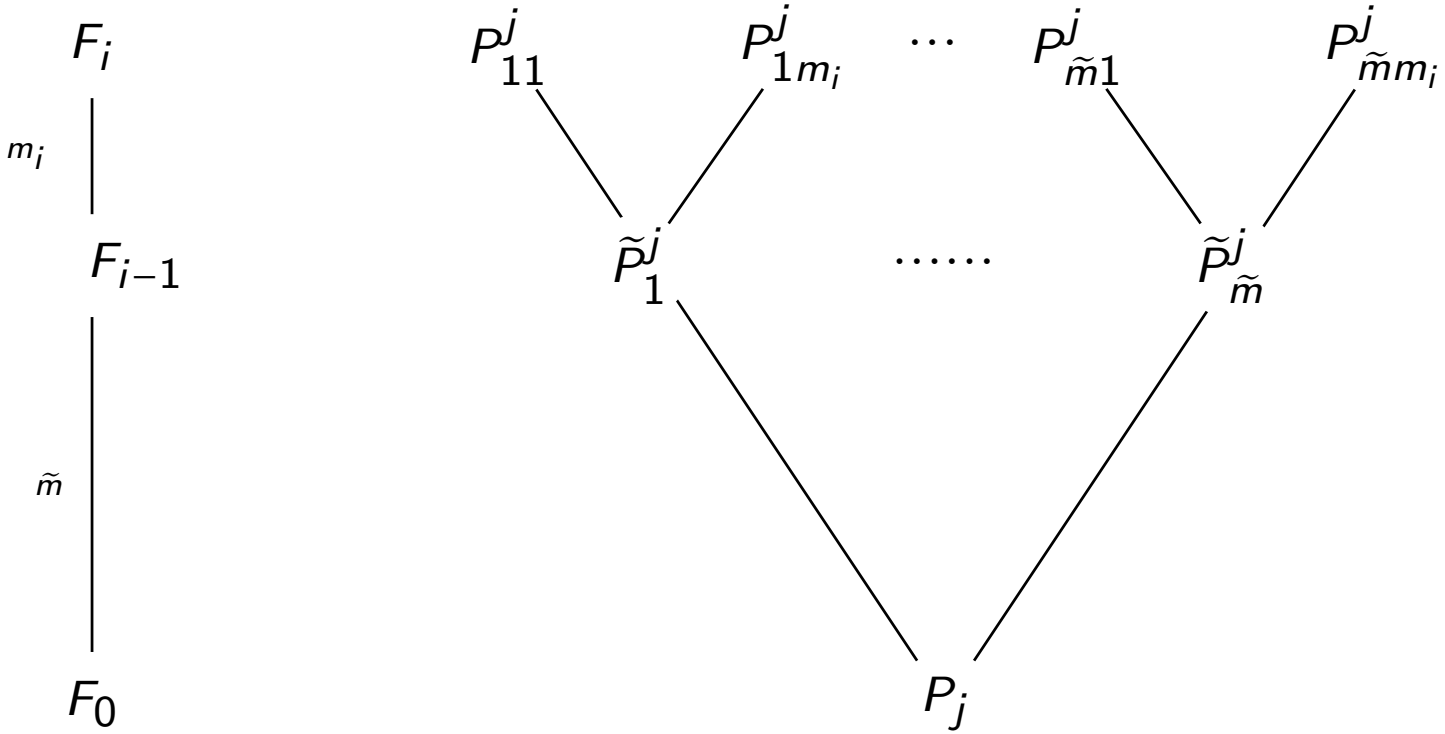


Figure: Diagram of an splitting place P_j of F_0 in F_i

A Tower by Garcia Stichtenoth

A Tower by Garcia Stichtenoth

For simplicity, we will suppose q is odd.

A Tower by Garcia Stichtenoth

For simplicity, we will suppose q is odd.
Consider the function field $E/\mathbb{F}_{q^2}$ defined by

$$y^q + y = \frac{x^q}{x^{q-1}+1},$$

so that $F = \mathbb{F}_{q^2}(x)$. Set $S = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha \neq 0\}$.

A Tower by Garcia Stichtenoth

For simplicity, we will suppose q is odd.
Consider the function field $E/\mathbb{F}_{q^2}$ defined by

$$y^q + y = \frac{x^q}{x^{q-1}+1},$$

so that $F = \mathbb{F}_{q^2}(x)$. Set $S = \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha \neq 0\}$.

It can be shown that

1. $[E : F] = [E : \mathbb{F}_{q^2}(y)] = q$,
2. x has exactly one pole in E (namely, Q_∞) totally ramified in E/F,
3. If P_α is the only zero of $x - \alpha$ for $\alpha \in S$, then P_α splits completely.
   Otherwise, it is totally ramified if $\alpha \neq 0$.

We can consider $D = lP_\infty$ and

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\},$$

We can consider $D = lP_\infty$ and

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\},$$

obtaining $n = [E : F] \cdot |S| = q(q^2 - q)$,

We can consider $D = lP_\infty$ and

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\},$$

obtaining $n = [E : F] \cdot |S| = q(q^2 - q)$,

$$V = \left\langle x^j y^i : 0 \leq j \leq l, 0 \leq i \leq q-2 \right\rangle,$$

We can consider $D = lP_\infty$ and

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\},$$

obtaining $n = [E : F] \cdot |S| = q(q^2 - q)$,

$$V = \left\langle x^j y^i : 0 \leq j \leq l, 0 \leq i \leq q-2 \right\rangle,$$

and thus a

$$(n = q(q^2 - q), k = l(q-1), r = q-1) \text{ LRC code.}$$

The main Theorem

The main Theorem

Using a Tower of Function Fields, we can extend the construction and obtain codes with higher dimension and moderate locality

Theorem (Chara, G., Martinez-Moro)

Let $\mathscr{F} = \{F_j\}_{j=0}^{\infty}$ be a sequence of function fields such that $F_0 = \mathbb{F}_q(x_0)$ and $F_j = F_{j-1}(x_j)$ for $j > 0$. Let $m_j = [F_j : F_{j-1}]$ and $E = F_i$, for some $i \geq 2$.

The main Theorem

Using a Tower of Function Fields, we can extend the construction and obtain codes with higher dimension and moderate locality

Theorem (Chara, G., Martinez-Moro)

Let $\mathscr{F} = \{F_j\}_{j=0}^{\infty}$ be a sequence of function fields such that $F_0 = \mathbb{F}_q(x_0)$ and $F_j = F_{j-1}(x_j)$ for $j > 0$. Let $m_j = [F_j : F_{j-1}]$ and $E = F_i$, for some $i \geq 2$.
Let S be a set of places of F_0 that split completely in E/F_0 and such that

$$\{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\} \cap \left(\bigcup_{j=1}^{i} \{Q \in \mathbb{P}(E) : v_Q(x_j) < 0\} \right) = \emptyset$$

and let $\mathscr{B} = \{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\}$.

The main Theorem

Using a Tower of Function Fields, we can extend the construction and obtain codes with higher dimension and moderate locality

Theorem (Chara, G., Martinez-Moro)

Let $\mathscr{F} = \{F_j\}_{j=0}^{\infty}$ be a sequence of function fields such that $F_0 = \mathbb{F}_q(x_0)$ and $F_j = F_{j-1}(x_j)$ for $j > 0$. Let $m_j = [F_j : F_{j-1}]$ and $E = F_i$, for some $i \geq 2$.
Let S be a set of places of F_0 that split completely in E/F_0 and such that

$$\{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\} \cap \left(\bigcup_{j=1}^{i} \{Q \in \mathbb{P}(E) : v_Q(x_j) < 0\} \right) = \emptyset$$

and let $\mathscr{B} = \{Q \in \mathbb{P}(E) : Q \cap F_0 \in S\}$. Then, if $s = |S| > 0$ we have that $|\mathscr{B}| = sm$ where $m = m_i \dots m_1$. For a divisor D of F_0 of degree l such that $supp(D) \cap S = \emptyset$, let $\{f_1, \dots, f_\ell\}$ a basis for $\mathscr{L}(D)$.

The main Theorem

Theorem

Consider the space V generated by

$$\{f_w x_1^{e_1} \cdots x_i^{e_i} : 1 \leq w \leq \ell; 0 \leq e_i \leq m_i - 2 \text{ and } 0 \leq e_j \leq m_j - 1 \text{ for } j = 1, \ldots, i-1\}.$$

Then $ev : V \to \mathbb{F}_q^{ms}$

$$f \to (f(P_{11}), \ldots, f(P_{ms}))$$

is well defined.

The main Theorem

Theorem

Consider the space V generated by

$$\{f_w x_1^{e_1} \cdots x_i^{e_i} : 1 \leq w \leq \ell; 0 \leq e_i \leq m_i - 2 \text{ and } 0 \leq e_j \leq m_j - 1 \text{ for } j = 1, \ldots, i-1\}.$$

Then $ev : V \to \mathbb{F}_q^{ms}$

$$f \to (f(P_{11}), \ldots, f(P_{ms}))$$

is well defined. The image of V is a LRC code, with locality $m_i - 1$, which we denote by $C_i(S, D)$.

The main Theorem

Theorem

Consider the space V generated by

$$\{f_w x_1^{e_1} \cdots x_i^{e_i} : 1 \le w \le \ell; 0 \le e_i \le m_i - 2 \text{ and } 0 \le e_j \le m_j - 1 \text{ for } j = 1, \ldots, i-1\}.$$

Then $ev : V \to \mathbb{F}_q^{ms}$

$$f \to (f(P_{11}), \ldots, f(P_{ms}))$$

is well defined. The image of V is a LRC code, with locality $m_i - 1$, which we denote by $C_i(S, D)$. The code coordinates are naturally partitioned into $\tilde{m}s$ subsets of size m_i each:

$$A_t^j = \{P_{tu}^j : 1 \le u \le m_i\} = \{Q \in \mathbb{P}(F_i) : Q \cap F_{i-1} = P_{t1}^j \cap F_{i-1} = \widetilde{P_t}^j\}$$

where $1 \le j \le s$; $1 \le t \le \tilde{m}$ and $\tilde{m} = m_{i-1} \ldots m_1 = m/m_i$.

Denoting by $h_j = [F_i : \mathbb{F}_q(x_j)]$, we have that the parameters of the code satisfy

$$
\begin{aligned}
&n = ms = m_i \dots m_1 s \\
&k = \ell(m_i - 1)m_{i-1} \cdots m_1 \geq (l+1)(m_i - 1)m_{i-1} \cdots m_1 \\
&d \geq n - lm - (m_1 - 1)h_1 - \cdots - (m_{i-1} - 1)h_{i-1} - (m_i - 2)h_i
\end{aligned}
$$

provided that the right-hand side of the inequality for d is a positive integer.

Local recovery of an erased symbol $f(P^j_{tu})$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A^j_t \setminus \{P^j_{tu}\}$.

Denoting by $h_j = [F_i : \mathbb{F}_q(x_j)]$, we have that the parameters of the code satisfy

$$
\begin{aligned}
&n = ms = m_i \dots m_1 s \\
&k = \ell(m_i - 1)m_{i-1} \cdots m_1 \geq (l+1)(m_i - 1)m_{i-1} \cdots m_1 \\
&d \geq n - lm - (m_1 - 1)h_1 - \cdots - (m_{i-1} - 1)h_{i-1} - (m_i - 2)h_i
\end{aligned}
$$

provided that the right-hand side of the inequality for d is a positive integer.

Local recovery of an erased symbol $f(P^j_{tu})$ can be performed by polynomial interpolation through the positions of the points in the recovery set $A^j_t \setminus \{P^j_{tu}\}$.

The Garcia Stichtenoth Tower

The Garcia Stichtenoth Tower

We recall the Garcia-Stichtenoth Tower, defined recursively for $i \geq 0$ as

$$F_0 = \mathbb{F}_{q^2}(x_0), \quad F_{i+1} = F_i(x_{i+1}),$$

where

$$x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}.$$

Garcia-Stichtenoth showed that $N(F_j) \geq q^j(q^2 - q) + 1$ and moreover

$$S = \{P_\alpha \in \mathbb{P}(F_0) : \alpha \in \mathbb{F}_{q^2} \text{ and } \alpha^q + \alpha \neq 0\}$$

is a set of places that splits completely on $\mathscr{F}$.

We can consider, then, for each $j \geq 1$ the following subspace of F_j

$$V = \left\langle x_0^{e_0} x_1^{e_1} \cdots x_j^{e_j} : 0 \leq e_0 \leq l, 0 \leq e_i \leq q-1; 1 \leq i \leq j \right\rangle.$$

for suitable bound l.

We can consider, then, for each $j \geq 1$ the following subspace of F_j

$$V = \left\langle x_0^{e_0} x_1^{e_1} \cdots x_j^{e_j} : 0 \leq e_0 \leq l, 0 \leq e_i \leq q-1; 1 \leq i \leq j \right\rangle.$$

for suitable bound l.

This gives a k dimensional linear subspace, with $k = (l+1)q^{j-1}(q-1)$, and considering $\mathscr{B} = \{Q \in \mathbb{P}(F_j) : Q|P \text{ for some } P \in S\}$ we can define an (n, k, r) code $\mathscr{C} = C_j(S, D)$ with

$$n = q^j(q^2 - q),\ k = (l+1)q^{j-1}(q-1),\ r = q-1$$

$$d \geq n - lq^j - \sum_{t=1}^{j}(q-1)q^j = (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$$

We can consider, then, for each $j \geq 1$ the following subspace of F_j

$$V = \left\langle x_0^{e_0} x_1^{e_1} \cdots x_j^{e_j} : 0 \leq e_0 \leq l, 0 \leq e_i \leq q-1; 1 \leq i \leq j \right\rangle.$$

for suitable bound l.

This gives a k dimensional linear subspace, with $k = (l+1)q^{j-1}(q-1)$, and considering $\mathscr{B} = \{Q \in \mathbb{P}(F_j) : Q|P \text{ for some } P \in S\}$ we can define an (n, k, r) code $\mathscr{C} = C_j(S, D)$ with

$$n = q^j(q^2 - q),\ k = (l+1)q^{j-1}(q-1),\ r = q-1$$

$$d \geq n - lq^j - \sum_{t=1}^{j}(q-1)q^j = (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$$

Note that the lower bound is negative for fixed q and j large enough!

An example: the bound for d is sharp

An example: the bound for d is sharp

We will show the bound

$$d \geq (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$$

might not be improved for small steps. That is, for j small enough there exists codes $C_j(S, D)$ with $d = (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$

An example: the bound for d is sharp

We will show the bound

$$d \geq (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$$

might not be improved for small steps. That is, for j small enough there exists codes $C_j(S, D)$ with $d = (q^2 - 2q + 2 - l - (q-1)(j-1))q^j$

Proposition

For $q \geq 5$, the code $C_2(S, D)$ over the Garcia-Stichtenoth Tower, with $D = qP_\infty$, is a locally recoverable code over $\mathbb{F}_{q^2}$, with locality $r = q - 1$, whose parameters are

$$n = q^2(q^2 - q),$$
$$k = (q+1)q(q-1) = q^3 - q,$$
$$d = q^2(q^2 - 2q + 2 - q - (q-1)) = q^2(q^2 - 4q + 3).$$

Proof of shaprness:

Proof of shaprness:

We must show that exist some $f \in V$ such that f has at least $q^2(3q-3)$ zeroes, so the minimum distance of the evaluation code $C_2(S,D)$ is at most

$$q^2(q^2-q)-q^2(3q-3)=q^2(q^2-4q+3)$$

and thus the bound of the theorem is attained

Proof of shaprness:

We must show that exist some $f \in V$ such that f has at least $q^2(3q-3)$ zeroes, so the minimum distance of the evaluation code $C_2(S,D)$ is at most

$$q^2(q^2-q)-q^2(3q-3)=q^2(q^2-4q+3)$$

and thus the bound of the theorem is attained
Consider the set $S_0=\{\alpha \in \mathbb{F}_{q^2} : \alpha^q+\alpha \neq 0\}$. This set is naturally partitioned into $q-1$ disjoints subsets $S_1,\ldots,S_{q-1}$ of size q where

$$S_i=\{\alpha \in \mathbb{F}_{q^2} : \frac{\alpha^q}{\alpha^{q-1}+1}=\frac{\alpha^{q+1}}{\alpha^q+\alpha}=\beta_i\}, \quad \beta_i \in \mathbb{F}_q^*$$

For a rational place $P \in \mathbb{P}(F_j)$ we denote

$$N(P) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^{q+1},$$

$$Tr(P) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^q + x_j(P),$$

where $x_j \in F_j$ is the transcendental element defining the Tower.

For a rational place $P \in \mathbb{P}(F_j)$ we denote

$$N(P) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^{q+1},$$

$$Tr(P) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^q + x_j(P),$$

where $x_j \in F_j$ is the transcendental element defining the Tower. Now, if $Q|P$ for $Q \in \mathbb{P}(F_j)$, $P \in \mathbb{P}(F_{j-1})$ and $x_{j-1}(P) \in S_i$, then

$$Tr(Q) = \frac{x_{j-1}(Q)^{q+1}}{x_{j-1}(Q)^q + x_{j-1}(Q)} = \frac{N(P)}{Tr(P)} = \beta_i,$$

For a rational place $P \in \mathbb{P}(F_j)$ we denote

$$N(P) = N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^{q+1},$$

$$Tr(P) = Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x_j(P)) = x_j(P)^q + x_j(P),$$

where $x_j \in F_j$ is the transcendental element defining the Tower. Now, if $Q|P$ for $Q \in \mathbb{P}(F_j)$, $P \in \mathbb{P}(F_{j-1})$ and $x_{j-1}(P) \in S_i$, then

$$Tr(Q) = \frac{x_{j-1}(Q)^{q+1}}{x_{j-1}(Q)^q + x_{j-1}(Q)} = \frac{N(P)}{Tr(P)} = \beta_i,$$

so in particular we see that for each $P \in \mathscr{B} \cap F_{j-1}$ there are at most two places $Q_1, Q_2 \in \mathscr{B}$ such that

$$x_{j-1}(Q_1) = x_{j-1}(Q_2) = x_{j-1}(P) \in S_i.$$

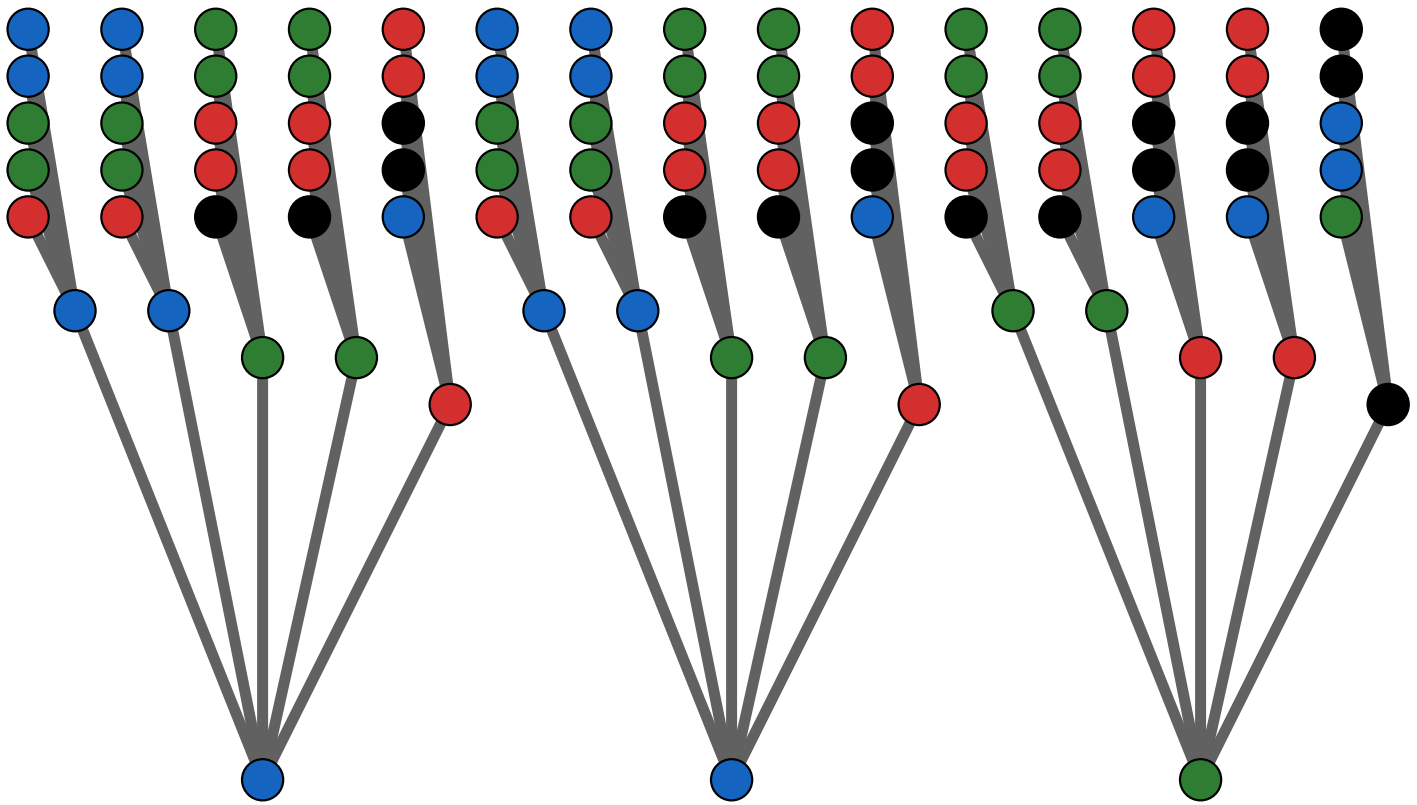


Diagram of three splitting places P_j of F_0 in F_2/F_0, for $q = 5$. Each colour, in each function field, represent a set S_i, for $1 \leq i \leq 4 = q - 1$

Moreover, if σ is the only nontrivial automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ then $x_j(Q_1) = \sigma(x_j(Q_2))$ so that, since q is odd, there is exactly one place $Q|P$ such that $x_{j-1}(Q) = x_{j-1}(P) \in S_i$ and $\sigma(x_j(Q)) = x_j(Q)$.

Moreover, if σ is the only nontrivial automorphism of $\mathbb{F}_{q^2}/\mathbb{F}_q$ then $x_j(Q_1) = \sigma(x_j(Q_2))$ so that, since q is odd, there is exactly one place $Q|P$ such that $x_{j-1}(Q) = x_{j-1}(P) \in S_i$ and $\sigma(x_j(Q)) = x_j(Q)$.
In other words, we can define $q-1$ disjoint subsets

$$B_i = \{\alpha \in \mathbb{F}_{q^2} : Tr(\alpha) = \beta_i\}, \beta_i \in \mathbb{F}_q^*$$

such that for any indexes $1 \leq i, k \leq q-1$ we have

$$|S_i \cap B_k| = |\{Q \in \mathbb{P}(F_j) : x_j(Q) \in S_i \text{ and } x_j(Q) \in B_k\}| \leq 2$$

with

$$|\{Q \in \mathbb{P}(F_j) : x_j(Q) \in S_i \text{ and } x_j(Q) \in B_k\}| = 1 \iff x_j(Q) \in \mathbb{F}_q$$

Now, in the notation of the theorem, we can consider $i = 2$, $l = q$, and $D = qP_\infty$ so that

$$V = \left\langle x_0^{e_0} x_1^{e_1} x_2^{e_2} : 0 \leq e_0 \leq l, 0 \leq e_1 \leq q-1, 0 \leq e_2 \leq q-2 \right\rangle.$$

Now, in the notation of the theorem, we can consider $i = 2$, $l = q$, and $D = qP_\infty$ so that

$$V = \left\langle x_0^{e_0} x_1^{e_1} x_2^{e_2} : 0 \le e_0 \le l, 0 \le e_1 \le q-1, 0 \le e_2 \le q-2 \right\rangle.$$

Chose some $\beta_1 \in \mathbb{F}_q^*$ and set

$$h_0 = \prod_{\alpha \in S_1} (x_0 - \alpha),$$

so that h_0 is a function with exactly $q^3 = |S_1|[F_2 : F_0]$ zeroes $Q \in \mathscr{B}$. These places verify $x_0(Q) \in S_1$ and thus $x_1(Q) \in B_1$ by the recursive definition of the Tower.

Now, since q is odd, chose β_i such that $|S_i \cap B_1| = 1$, and set

$$h_1 = \prod_{\alpha \in S_i \setminus B_1} (x_1 - \alpha),$$

so we have $(q-1)q^2 = (|S_i|-1)[F_2 : F_1]|\{Q \in \mathbb{P}(F_1) : x_1(Q) = \alpha\}$ new places $Q \in \mathscr{B}$ that are zeroes of h_1.

Now, since q is odd, chose β_i such that $|S_i \cap B_1| = 1$, and set

$$h_1 = \prod_{\alpha \in S_i \setminus B_1} (x_1 - \alpha),$$

so we have $(q-1)q^2 = (|S_i|-1)[F_2 : F_1]|\{Q \in \mathbb{P}(F_1) : x_1(Q) = \alpha\}$ new places $Q \in \mathscr{B}$ that are zeroes of h_1.
Since $|B_1| = q$, we can write B_1 as a disjoint union of $(q+1)/2$ subsets

$$B_1 = \bigcup_{k=1}^{(q+1)/2} B_1 \cap S_{i_k}$$

and therefore if $Q \in \mathscr{B}$ is such that $x_0(Q) \in S_1$ or $x_1(Q) \in S_i$, then $x_2(Q)$ is among $q(q+1)/2$ different values of $\mathbb{F}_{q^2}$.

For $q \geq 5$ we have

$$q(q+1)/2 < (q^2 - q) - (q-2)$$

so we can chose $q-2$ values $\gamma_1, \ldots, \gamma_{q-2}$ in S_0 and form

$$h_2 = \prod_{i=1}^{q-2} (x_2 - \gamma_i)$$

with exactly $q^2(q-2)$ new different zeroes in $\mathscr{B}$

For $q \geq 5$ we have

$$q(q+1)/2 < (q^2 - q) - (q-2)$$

so we can chose $q-2$ values $\gamma_1, \ldots, \gamma_{q-2}$ in S_0 and form

$$h_2 = \prod_{i=1}^{q-2} (x_2 - \gamma_i)$$

with exactly $q^2(q-2)$ new different zeroes in $\mathscr{B}$
Therefore, $f = h_0 h_1 h_2 \in V$ has exactly

$$q^3 + q^2(q-1) + q^2(q-2) = q^2(3q-3)$$

different zeroes, attaining the bound provided by the theorem. $\square$

Nevertheless, we obtain good parameters

Nevertheless, we obtain good parameters

Remark

The ideas used in the previous proposition can be used to show that exist a LRC code $C_2(S,D)$ *with* $D = \frac{q(q-1)}{2}P_\infty$ *with locality* $r = q-1$ *and parameters*

$$n = q^2(q^2-q),$$

$$k = \left(\frac{q(q-1)}{2}+1\right)q(q-1)$$

$$d = \frac{1}{2}q^2(q^2-3q+6) = q^2(q^2-4q+3).$$

Extending the construction for $j \geq 3$

Extending the construction for $j \geq 3$

The construction attain the bound of the distance for $j = 2$, that is, for two steps in the tower. For $j \geq 3$ it can be shown that

$$d > (q^2 - 2q + 2 - l - (q-1)(j-1))q^j,$$

in the case x_0 and x_3 have a common zero, which is the case of the García-Stichtenoth Tower. Thus, the bound can be slightly improved.

Extending the construction for $j \geq 3$

The construction attain the bound of the distance for $j = 2$, that is, for two steps in the tower. For $j \geq 3$ it can be shown that

$$d > (q^2 - 2q + 2 - l - (q-1)(j-1))q^j,$$

in the case x_0 and x_3 have a common zero, which is the case of the García-Stichtenoth Tower. Thus, the bound can be slightly improved.

Proposition

For odd $q \geq 5$, $2 \leq i \leq q-1$ and $1 \leq l \leq (q-1)(q-i)$ the parameters $R = \frac{k}{n}$ and $\delta = \frac{d}{n}$ of $C_i(S, D)$ verify

$$R + \frac{q-1}{q}\delta > \frac{q-1}{q}\left(\frac{q-i}{q}\right)$$

However, for the general case of an arbitrary tower $\mathscr{F}$ we don't know how to improve the bound, if possible.

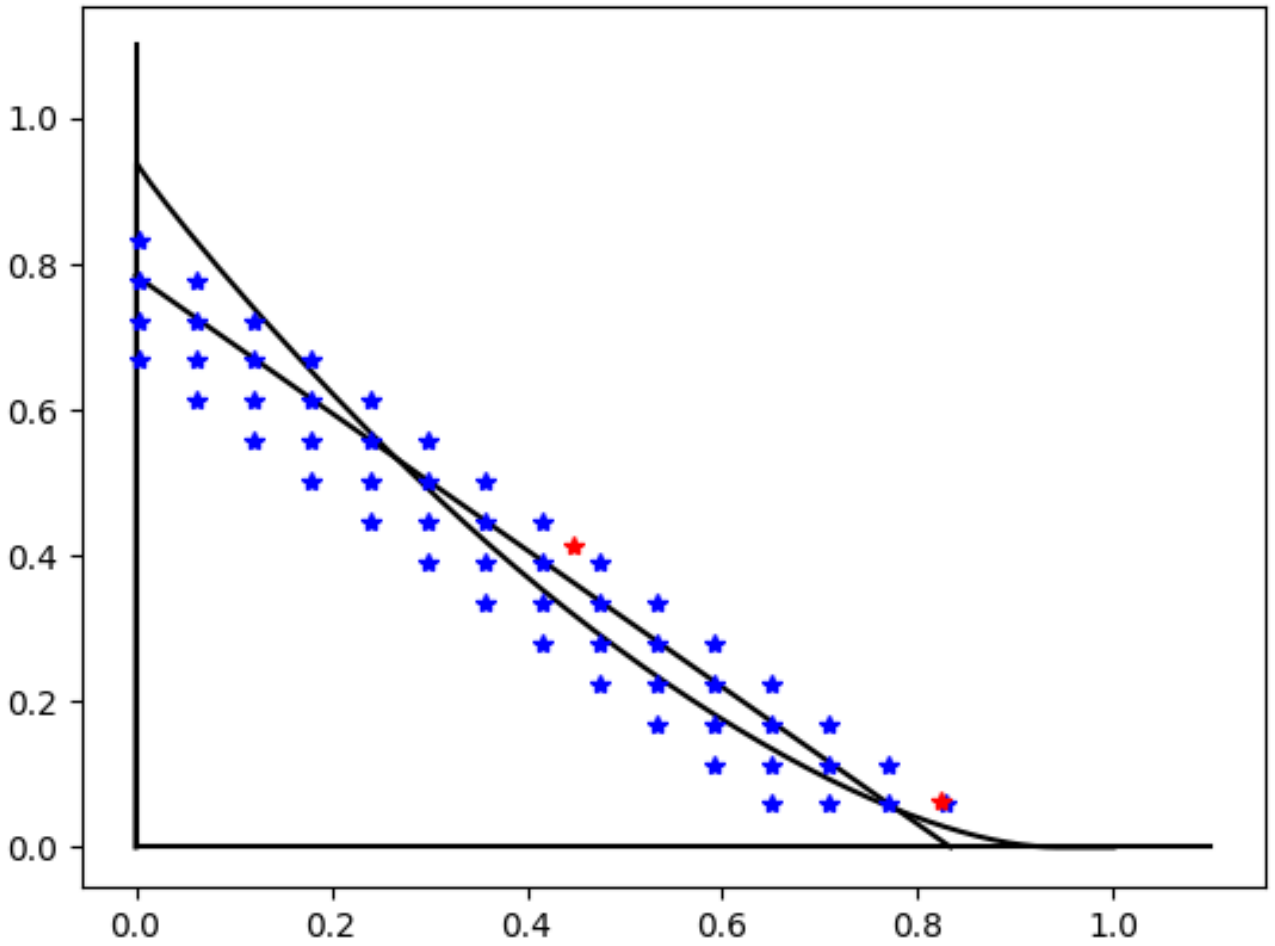


Figure: BTV and GV bounds (shown in black) are improved. For $2 \leq i \leq 5$, lower bounds for $C_i(S, D)$ are shown in blue. Parameters of $C_2(S, D)$ are shown in red.

Tanks for your attention :)