Locally recoverable codes: Constructions and bounds

Alexander Barg

U. of Maryland

co-authors

Itzhak Tamo, Serge Vlăduţ, Sree Goparaju, Robert Calderbank, Alexey Frolov

Introduction: Big Data

Big Data players: Facebook, Instagram, Google, MSFT, etc.; Dropbox, Box, etc.
Companies marketing coding solutions: CleverSafe (RS codes) and others.

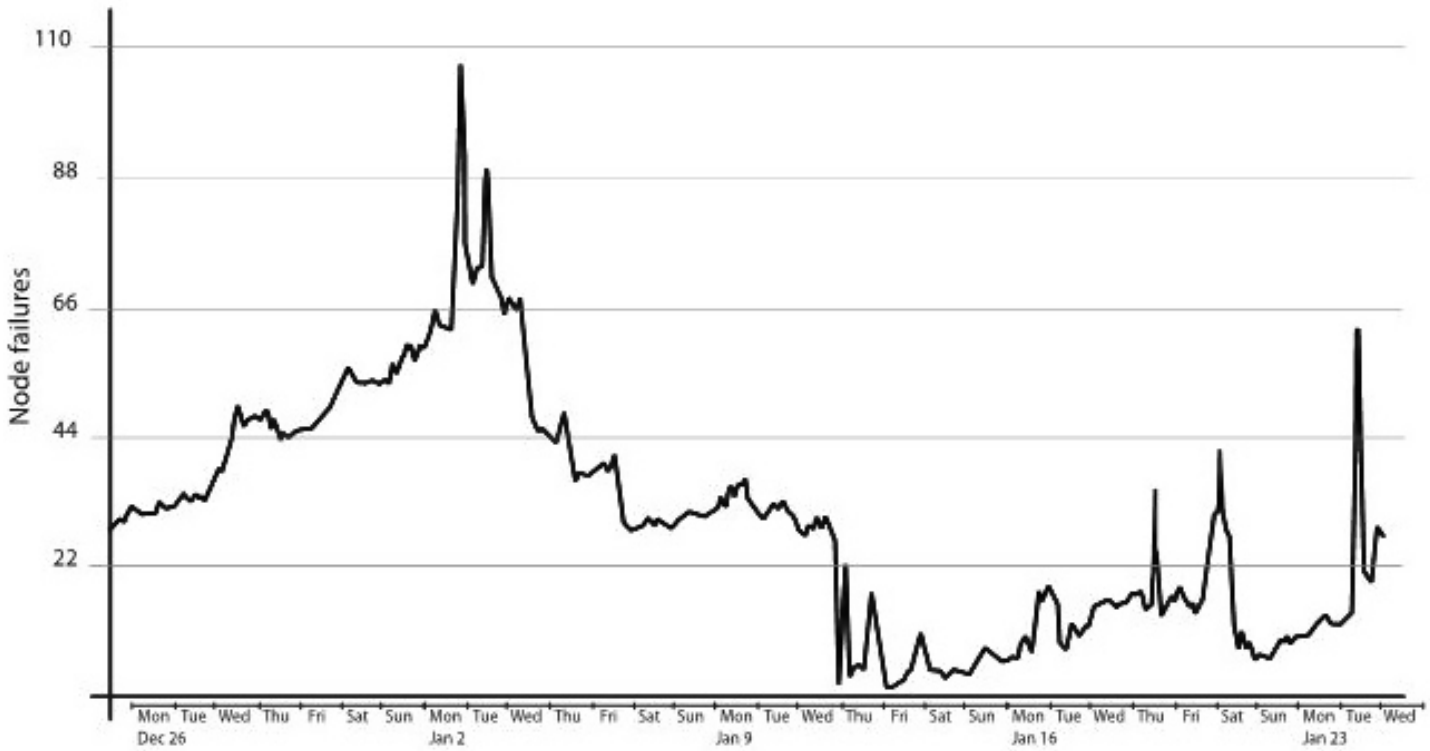
Introduction: Big Data

Big Data players: Facebook, Instagram, Google, MSFT, etc.; Dropbox, Box, etc.
Companies marketing coding solutions: CleverSafe (RS codes) and others.

Cluster of machines running Hadoop at Yahoo!

Node failures are the **norm**

Is repair cost a real issue?



(Average number of failed nodes =20) $\times 15$Tb $= 300$Tb

Locally Recoverable Codes

Code $\mathcal{C} \subset Q^n$, $|Q| = q$; $k = \log_q |\mathcal{C}|$; d - distance of $\mathcal{C}$
Typically $Q = \mathbb{F}_q$

Locally Recoverable Codes

Code $\mathcal{C} \subset Q^n$, $|Q| = q$; $k = \log_q |\mathcal{C}|$; d - distance of $\mathcal{C}$
Typically $Q = \mathbb{F}_q$

Definition (LRC codes)

Code $\mathcal{C}$ has *locality* r if for every $i \in [n]$ there exists a subset $R_i \subset [n] \backslash i$, $|R_i| \leq r$ and a function ϕ_i such that for every codeword $c \in \mathcal{C}$

$$c_i = \phi_i(\{c_j, j \in R_i\})$$

Locally Recoverable Codes

Code $\mathcal{C} \subset Q^n$, $|Q| = q$; $k = \log_q |\mathcal{C}|$; d - distance of $\mathcal{C}$
Typically $Q = \mathbb{F}_q$

Definition (LRC codes)

Code $\mathcal{C}$ has *locality* r if for every $i \in [n]$ there exists a subset $R_i \subset [n] \backslash i$, $|R_i| \leq r$ and a function ϕ_i such that for every codeword $c \in \mathcal{C}$

$$c_i = \phi_i(\{c_j, j \in R_i\})$$

Examples:

Repetition codes, Single parity-check codes
locality $r = k$: $[n, k]$ RS code; locality $r = 1$: $[n/2, k, n/2 - k + 1]$ RS codes

Locally Recoverable Codes

Code $\mathcal{C} \subset Q^n$, $|Q| = q$; $k = \log_q |\mathcal{C}|$; d - distance of $\mathcal{C}$
Typically $Q = \mathbb{F}_q$

Definition (LRC codes)

Code $\mathcal{C}$ has *locality* r if for every $i \in [n]$ there exists a subset $R_i \subset [n] \backslash i$, $|R_i| \leq r$ and a function ϕ_i such that for every codeword $c \in \mathcal{C}$

$$c_i = \phi_i(\{c_j, j \in R_i\})$$

Examples:

Repetition codes, Single parity-check codes
locality $r = k$: $[n, k]$ RS code; locality $r = 1$: $[n/2, k, n/2 - k + 1]$ RS codes

Early constructions:

Prasanth, Kamath, Lalitha, Kumar, ISIT 2012
Silberstein, Rawat, Koyluoglu Vishwanath, ISIT 2013
Tamo, Papailiopoulos, Dimakis, ISIT 2013

Parameters of LRC codes

Parameters of LRC codes

Theorem (Gopalan e.a. (2011) and Papailiopoulos e.a. (2012))

Let $\mathcal{C}$ be an (n,k,r) LRC code of cardinality q^k over an alphabet of size q, then:
The minimum distance of $\mathcal{C}$ satisfies

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \tag{1}$$

The rate of $\mathcal{C}$ satisfies

$$\frac{k}{n} \leq \frac{r}{r+1}. \tag{2}$$

Parameters of LRC codes

Theorem (Gopalan e.a. (2011) and Papailiopoulos e.a. (2012))

Let $\mathcal{C}$ be an (n, k, r) LRC code of cardinality q^k over an alphabet of size q, then:
The minimum distance of $\mathcal{C}$ satisfies

$$d \leq n - k - \left\lceil \frac{k}{r} \right\rceil + 2. \tag{1}$$

The rate of $\mathcal{C}$ satisfies

$$\frac{k}{n} \leq \frac{r}{r+1}. \tag{2}$$

Note that $r = k$ reduces (1) to the Singleton bound

$$d \leq n - k + 1$$

RS codes and Evaluation codes

Given a polynomial $f \in \mathbb{F}_q[x]$ and a set $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$ define the map

$$ev_A : f \mapsto (f(P_i), i = 1, \ldots, n)$$

RS codes and Evaluation codes

Given a polynomial $f \in \mathbb{F}_q[x]$ and a set $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$ define the map

$$ev_A : f \mapsto (f(P_i), i = 1, \ldots, n)$$

Example: Let $q = 8, f(x) = 1 + \alpha x + \alpha x^2$

$$f(x) \mapsto (1, \alpha^4, \alpha^6, \alpha^4, \alpha, \alpha, \alpha^6)$$

RS codes and Evaluation codes

Given a polynomial $f \in \mathbb{F}_q[x]$ and a set $A = \{P_1, \ldots, P_n\} \subset \mathbb{F}_q$ define the map

$$ev_A : f \mapsto (f(P_i), i = 1, \ldots, n)$$

Example: Let $q = 8, f(x) = 1 + \alpha x + \alpha x^2$

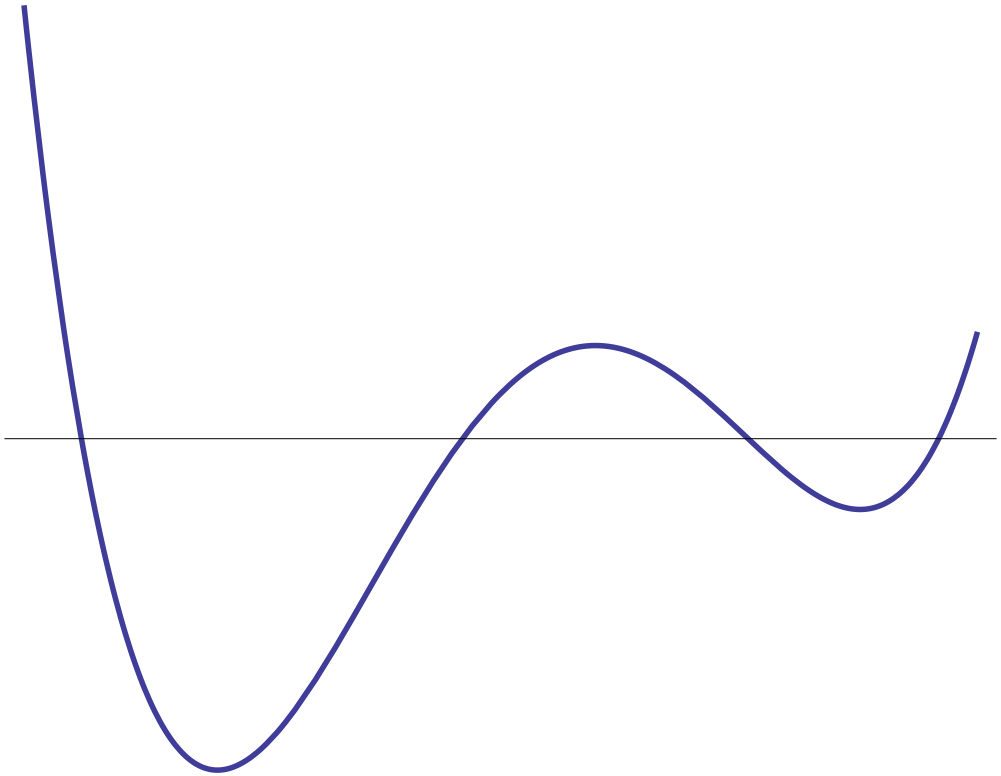
$$f(x) \mapsto (1, \alpha^4, \alpha^6, \alpha^4, \alpha, \alpha, \alpha^6)$$

Evaluation code $\mathcal{C}(A)$

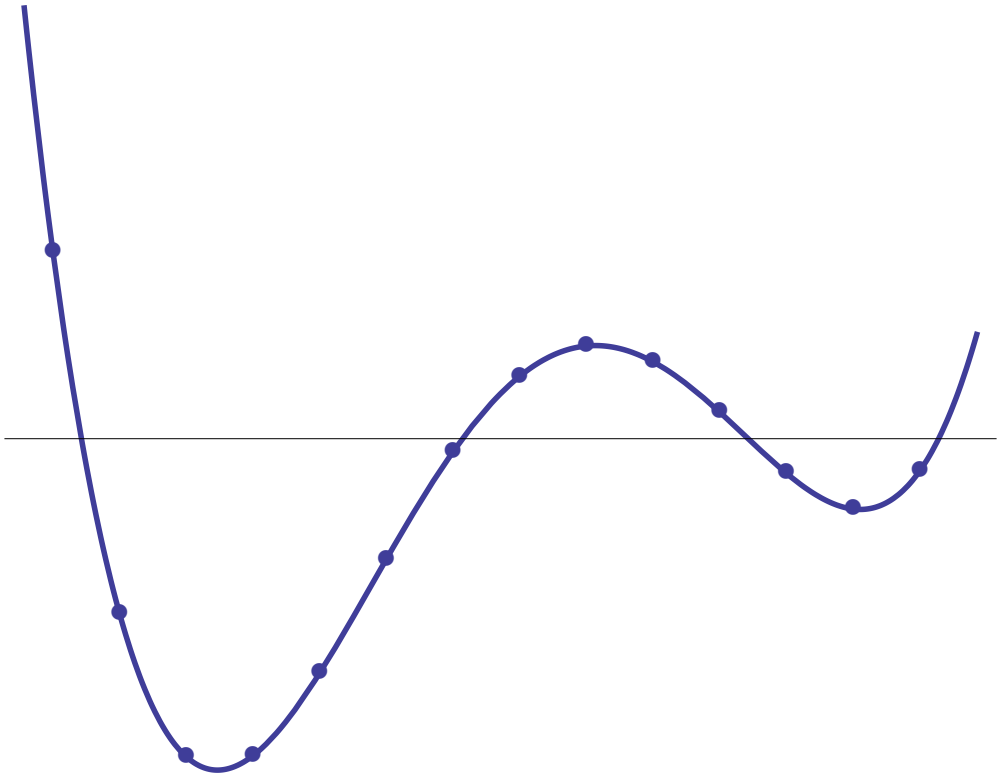
Let $V = \{f \in \mathbb{F}_q[x]\}$ be a set of polynomials, $\dim(V) = k$

$$\begin{aligned} \mathcal{C} : V &\to \mathbb{F}_q^n \\ f &\mapsto ev_A(f) = (f(P_i), i = 1, \ldots, n) \end{aligned}$$

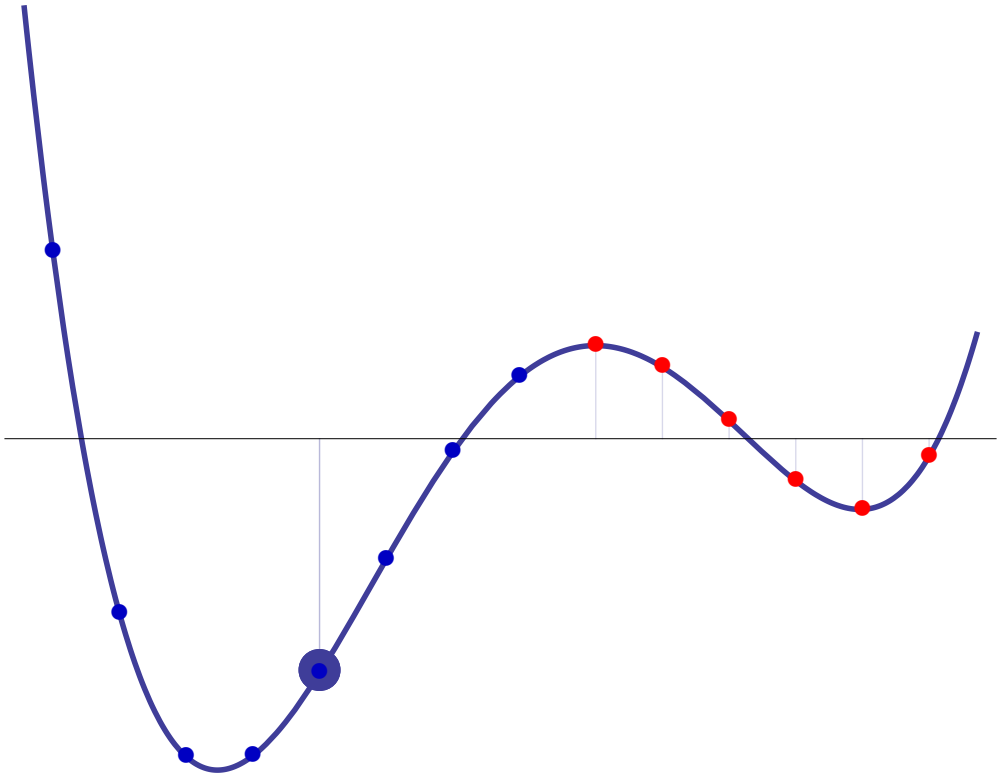
Reed-Solomon codes



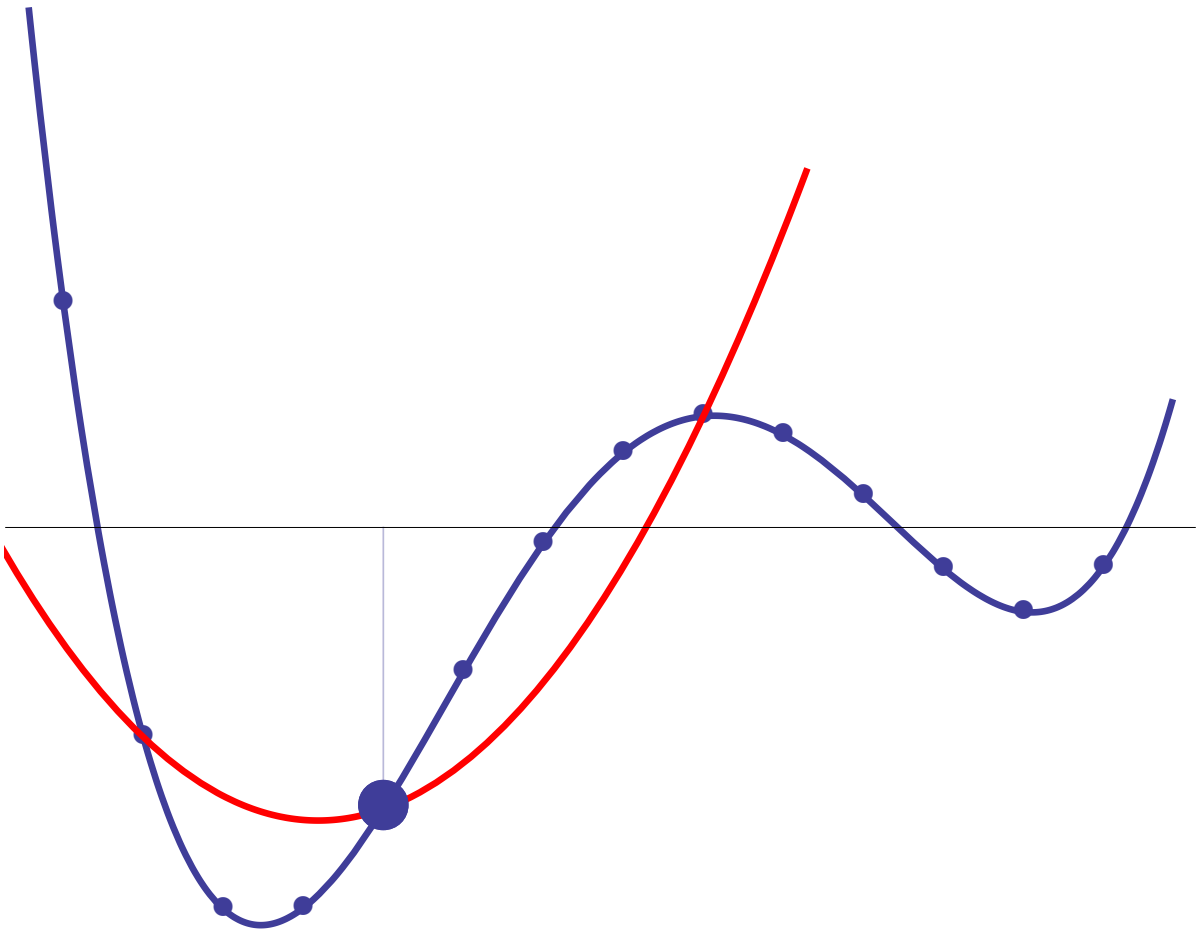
Reed-Solomon codes



Reed-Solomon codes



Evaluation codes with locality



Construction of (n, k, r) LRC codes: Example

Parameters: $n = 9, k = 4, r = 2, q = 13$;

Set of points: $A = \{P_1, \ldots, P_9\} \subset \mathbb{F}_{13}$

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

Set of functions: $V = \{f_a(x) = a_0 + a_1 x + a_3 x^3 + a_4 x^4\}$

Code construction:

$$ev_A : f_a \mapsto (f(P_i), i = 1, \ldots 9)$$

Construction of (n, k, r) LRC codes: Example

Parameters: $n = 9, k = 4, r = 2, q = 13$;

Set of points: $A = \{P_1, \ldots, P_9\} \subset \mathbb{F}_{13}$

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

Set of functions: $V = \{f_a(x) = a_0 + a_1 x + a_3 x^3 + a_4 x^4\}$

Code construction:

$$ev_A : f_a \mapsto (f(P_i), i = 1, \ldots 9)$$

E.g., $a = (1111)$ then $f_a(x) = 1 + x + x^3 + x^4$

$$c := ev_A(f_a) = (\underbrace{4, 8, 7}_{A_1} | \underbrace{1, 11, 2}_{A_2} | \underbrace{0, 0, 0}_{A_3})$$

$$f_a(x)|_{A_1} = a_0 + a_3 + (a_1 + a_4)x$$

Construction of (n, k, r) LRC codes: Example

Parameters: $n = 9, k = 4, r = 2, q = 13$;

Set of points: $A = \{P_1, \ldots, P_9\} \subset \mathbb{F}_{13}$

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

Set of functions: $V = \{f_a(x) = a_0 + a_1 x + a_3 x^3 + a_4 x^4\}$

Code construction:

$$ev_A : f_a \mapsto (f(P_i), i = 1, \ldots 9)$$

E.g., $a = (1111)$ then $f_a(x) = 1 + x + x^3 + x^4$

$$c := ev_A(f_a) = (\underbrace{4, 8, 7}_{A_1} | \underbrace{1, 11, 2}_{A_2} | \underbrace{0, 0, 0}_{A_3})$$

$$f_a(x)|_{A_1} = a_0 + a_3 + (a_1 + a_4)x = 2 + 2x$$

Construction of (n, k, r) LRC codes: Example

Parameters: $n = 9, k = 4, r = 2, q = 13$;

Set of points: $A = \{P_1, \ldots, P_9\} \subset \mathbb{F}_{13}$

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

Set of functions: $V = \{f_a(x) = a_0 + a_1 x + a_3 x^3 + a_4 x^4\}$

Code construction:

$$ev_A : f_a \mapsto (f(P_i), i = 1, \ldots 9)$$

E.g., $a = (1111)$ then $f_a(x) = 1 + x + x^3 + x^4$

$$c := ev_A(f_a) = (\underbrace{4, 8, 7}_{A_1} | \underbrace{1, 11, 2}_{A_2} | \underbrace{0, 0, 0}_{A_3})$$

$$f_a(x)|_{A_1} = a_0 + a_3 + (a_1 + a_4)x = 2 + 2x$$
$$f_a(x)|_{A_2} = a_0 + 8a_3 + (a_1 + 8a_4)x$$

Construction of (n, k, r) LRC codes

$$A = (P_1, \ldots, P_n) \subset \mathbb{F}_q$$

$$A = A_1 \cup A_2 \cup \cdots \cup A_{\frac{n}{r+1}}$$

Basis of functions: Take $g(x)$ constant on A_i, $i = 1, \ldots, \frac{n}{r+1}$, $\deg(g) = r + 1$

$$V = \left\langle g(x)^j x^i, i = 0, \ldots, r-1; j = 0, \ldots, \frac{k}{r} - 1 \right\rangle; \ \dim(V) = k$$

$$V = \left\{ f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j x^i \right\}$$

Construction of (n, k, r) LRC codes

$$A = (P_1, \ldots, P_n) \subset \mathbb{F}_q$$

$$A = A_1 \cup A_2 \cup \cdots \cup A_{\frac{n}{r+1}}$$

Basis of functions: Take $g(x)$ constant on A_i, $i = 1, \ldots, \frac{n}{r+1}$, $\deg(g) = r + 1$

$$V = \left\langle g(x)^j x^i, i = 0, \ldots, r-1; j = 0, \ldots, \frac{k}{r} - 1 \right\rangle;\ \dim(V) = k$$

$$V = \left\{ f_a(x) = \sum_{i=0}^{r-1} \sum_{j=0}^{\frac{k}{r}-1} a_{ij} g(x)^j x^i \right\}$$

We obtain a family of optimal r-LRC codes: $d = n - \deg(g(x)^j x^i) \geq n - k\frac{r+1}{r} + 2$

Erasure recovery by polynomial interpolation over r points.

Piecewise constant polynomials?

Take $H < G := \mathbb{F}^*$ (or $G := \mathbb{F}^+$) and let

$$g(x) = \prod_{h \in H} (x - h)$$

Then g is constant on every coset aH of H in G:

$$g(a\bar{h}) = \prod_{h \in H} (a\bar{h} - h) = \bar{h}^{-1} \prod_{h \in H} (a - h\bar{h}^{-1}) = g(a)$$

(work with *I. Tamo*, *IEEE Trans. Inf. Theory,* Aug. 2014)

Extensions

- Codes with multiple disjoint recovery sets for every coordinate

Extensions

- Codes with multiple disjoint recovery sets for every coordinate
- Codes that recover locally from $\rho \geq 2$ erasures: The local codes are $[r + \rho - 1, r, \rho]$ MDS

Extensions

- Codes with multiple disjoint recovery sets for every coordinate
- Codes that recover locally from $\rho \geq 2$ erasures: The local codes are $[r + \rho - 1, r, \rho]$ MDS
- Systematic encoding

Geometric view of LRC codes

$$A = \{1, \ldots, 9\} \subset \mathbb{F}_{13}$$

$$A = A_1 \cup A_2 \cup A_3$$

$$A_1 = (1, 3, 9)$$
$$A_2 = (2, 6, 5)$$
$$A_3 = (4, 12, 10)$$

Geometric view of LRC codes

$$A = \{1, \ldots, 9\} \subset \mathbb{F}_{13}$$

$$A = A_1 \cup A_2 \cup A_3$$

$$A_1 = (1, 3, 9)$$
$$A_2 = (2, 6, 5)$$
$$A_3 = (4, 12, 10)$$

$$g : A \to \mathbb{F}_{13}$$
$$x \mapsto x^3 - 1$$

Geometric view of LRC codes

$$A = \{1, \ldots, 9\} \subset \mathbb{F}_{13}$$

$$A = A_1 \cup A_2 \cup A_3$$

$$A_1 = (1, 3, 9)$$
$$A_2 = (2, 6, 5)$$
$$A_3 = (4, 12, 10)$$

$$g : A \to \mathbb{F}_{13}$$
$$x \mapsto x^3 - 1$$

$$g : \mathbb{F}_{13} \to \{0, 7, 8\} \subset \mathbb{F}_{13}$$
$$|g^{-1}(y)| = r + 1$$

Geometric view of LRC codes

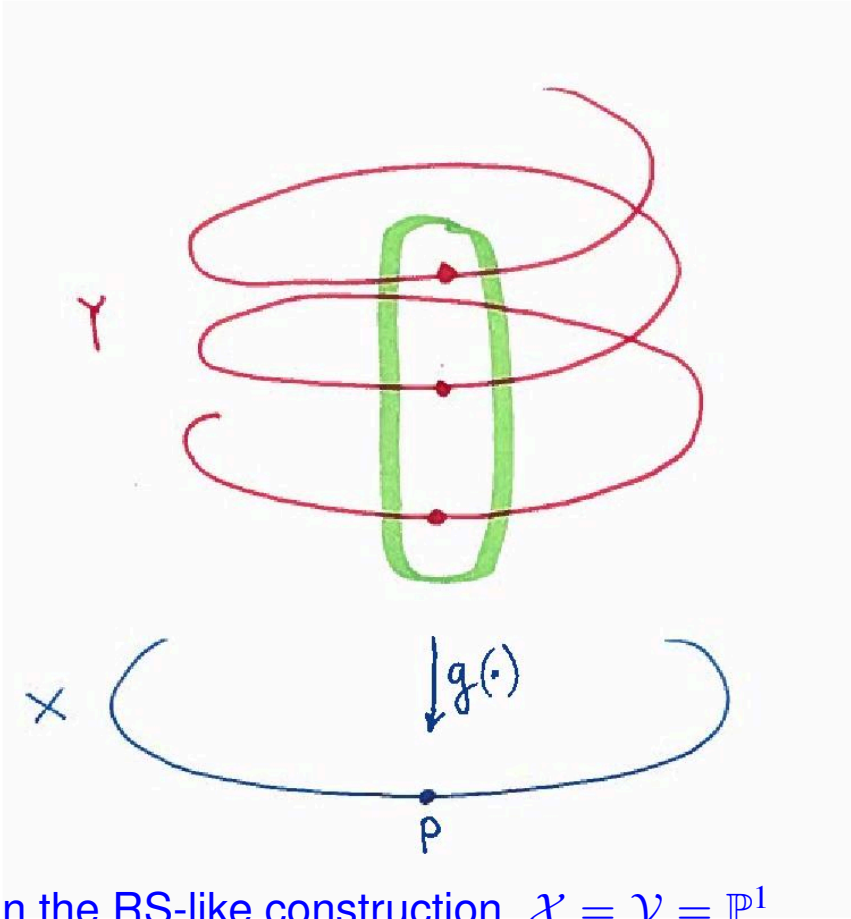
$$A = \{1, \ldots, 9\} \subset \mathbb{F}_{13}$$

$$A = A_1 \cup A_2 \cup A_3$$

$$A_1 = (1, 3, 9)$$
$$A_2 = (2, 6, 5)$$
$$A_3 = (4, 12, 10)$$

$$g : A \to \mathbb{F}_{13}$$
$$x \mapsto x^3 - 1$$

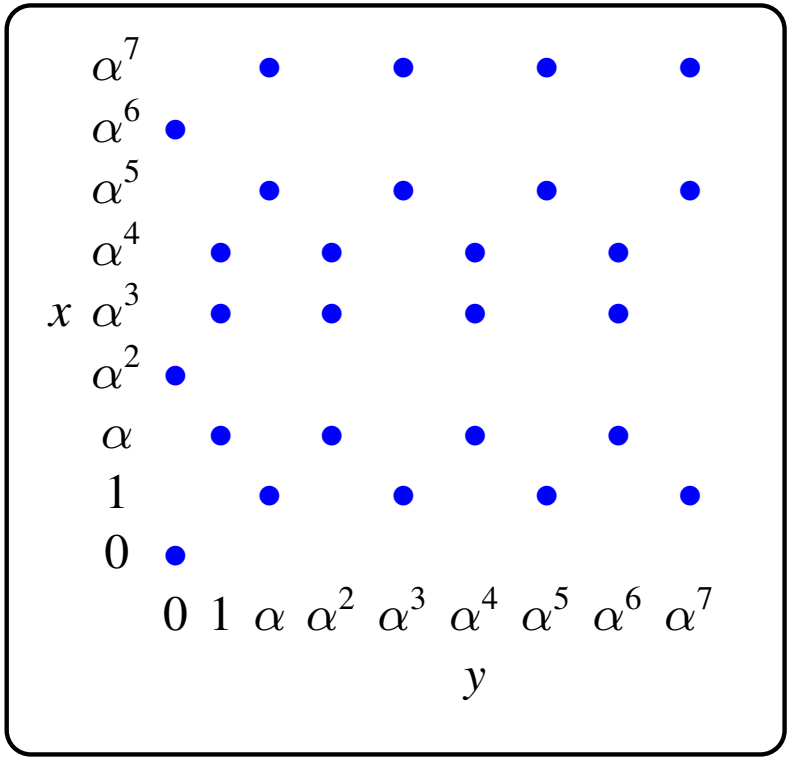
$$g : \mathbb{F}_{13} \to \{0, 7, 8\} \subset \mathbb{F}_{13}$$
$$|g^{-1}(y)| = r + 1$$



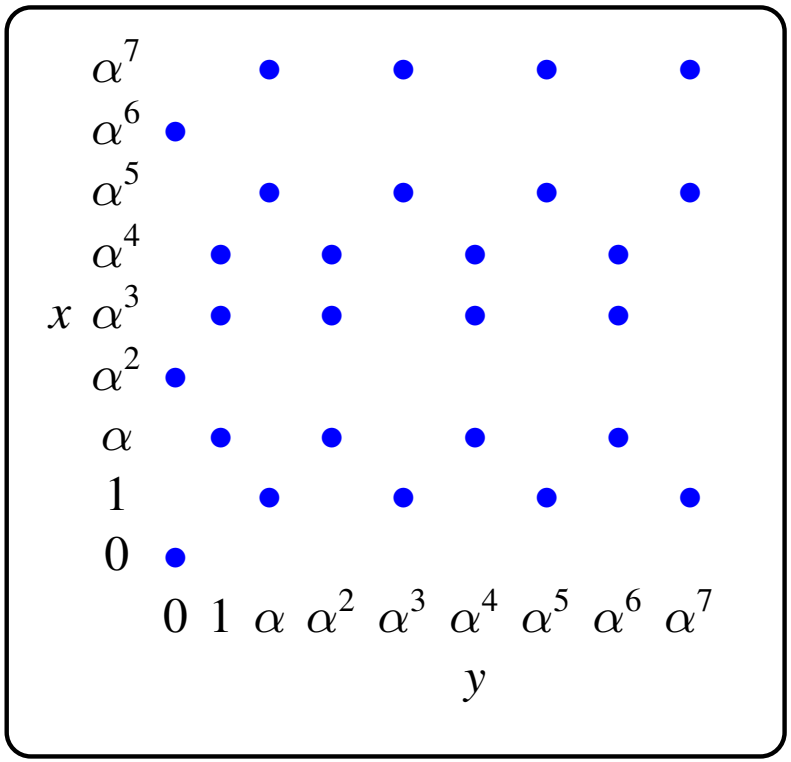
In the RS-like construction, $\mathcal{X} = \mathcal{Y} = \mathbb{P}^1$

LRC codes on curves

Consider the set of pairs $(x, y) \in \mathbb{F}_9$ that satisfy the equation $x^3 + x = y^4$



Consider the set of pairs $(x, y) \in \mathbb{F}_9$ that satisfy the equation $x^3 + x = y^4$



Affine points of the Hermitian curve $\mathcal{X}$ over $\mathbb{F}_9$; $\alpha^2 = \alpha + 1$

Hermitian codes

$$\begin{array}{rccc} g: & \mathcal{X} & \to & \mathbb{P}^1 \\ & (x,y) & \mapsto & y \end{array}$$

Space of functions $V := \langle 1, y, y^2, x, xy, xy^2 \rangle$

A=$\{$Affine points of the Hermitian curve over $\mathbb{F}_9\}$; $n = 27, k = 6$

$$\mathcal{C} : V \to \mathbb{F}_9^n$$

Hermitian codes

$$\begin{array}{rccc} g: & \mathcal{X} & \to & \mathbb{P}^1 \\ & (x,y) & \mapsto & y \end{array}$$

Space of functions $V := \langle 1, y, y^2, x, xy, xy^2 \rangle$

A=$\{$Affine points of the Hermitian curve over $\mathbb{F}_9\}$; $n = 27, k = 6$

$$\mathcal{C} : V \to \mathbb{F}_9^n$$

E.g., message $(1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$

$$F(x,y) = 1 + \alpha y + \alpha^2 y^2 + \alpha^3 x + \alpha^4 xy + \alpha^5 xy^2$$

$$F(0,0) = 1 \text{ etc.}$$

LRC codes on curves

$$
\begin{array}{cccccccccc}
 & \alpha^7 & & & \alpha & & \alpha^7 & & \alpha^5 & & 0 \\
 & \alpha^6 & \alpha^2 & & & & & & & & \\
 & \alpha^5 & & & \alpha^6 & & \alpha^4 & & \alpha^2 & & 0 \\
 & \alpha^4 & & \alpha^7 & & \alpha^3 & & \alpha^5 & & \alpha^5 & \\
x & \alpha^3 & & \alpha^3 & & \alpha^7 & & \alpha & & \alpha & \\
 & \alpha^2 & \alpha^3 & & & & & & & & \\
 & \alpha & & 0 & & 0 & & 0 & & 0 & \\
 & 1 & & & 1 & & \alpha^6 & & \alpha^4 & & 0 \\
 & 0 & 1 & & & & & & & & \\
 & & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\
 & & & & & & & y & & &
\end{array}
$$

Hermitian LRC codes

$$
\begin{array}{cccccccccc}
 & \alpha^7 & & & \alpha & & \alpha^7 & & \alpha^5 & & 0 \\
 & \alpha^6 & \alpha^2 & & & & & & & & \\
 & \alpha^5 & & & \alpha^6 & & \alpha^4 & & \alpha^2 & & 0 \\
 & \alpha^4 & & \alpha^7 & & \alpha^3 & & \alpha^5 & & \alpha^5 & \\
x & \alpha^3 & & \alpha^3 & & \alpha^7 & & \alpha & & \alpha & \\
 & \alpha^2 & \alpha^3 & & & & & & & & \\
 & \alpha & & 0 & & 0 & & 0 & & 0 & \\
 & 1 & & & 1 & & \alpha^6 & & \alpha^4 & & 0 \\
 & 0 & 1 & & & & & & & & \\
 & & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\
 & & & & & & & y & & &
\end{array}
$$

Let $P = (\alpha, 1)$ be the erased location.

Local recovery with Hermitian codes

$$
\begin{array}{cccccccccc}
 & \alpha^7 & & & \alpha & & \alpha^7 & & \alpha^5 & & 0 \\
 & \alpha^6 & \alpha^2 & & & & & & & & \\
 & \alpha^5 & & & \alpha^6 & & \alpha^4 & & \alpha^2 & & 0 \\
 & \alpha^4 & & \alpha^7 & & \alpha^3 & & \alpha^5 & & \alpha^5 & \\
x & \alpha^3 & & \alpha^3 & & \alpha^7 & & \alpha & & \alpha & \\
 & \alpha^2 & \alpha^3 & & & & & & & & \\
 & \alpha & & ? & & 0 & & 0 & & 0 & \\
 & 1 & & & 1 & & \alpha^6 & & \alpha^4 & & 0 \\
 & 0 & 1 & & & & & & & & \\
 & & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\
 & & & & & & & y & & &
\end{array}
$$

Let $P = (\alpha, 1)$ be the erased location. Recovery set $I_P = \{(\alpha^4, 1), (\alpha^3, 1)\}$
Find $f(x) : f(\alpha^4) = \alpha^7, f(\alpha^3) = \alpha^3$

$$\Rightarrow \quad f(x) = \alpha x - \alpha^2$$

Local recovery with Hermitian codes

$$
\begin{array}{cccccccccc}
 & \alpha^7 & & & \alpha & & \alpha^7 & & \alpha^5 & & 0 \\
 & \alpha^6 & \alpha^2 & & & & & & & & \\
 & \alpha^5 & & & \alpha^6 & & \alpha^4 & & \alpha^2 & & 0 \\
 & \alpha^4 & & \alpha^7 & & \alpha^3 & & \alpha^5 & & \alpha^5 & \\
x & \alpha^3 & & \alpha^3 & & \alpha^7 & & \alpha & & \alpha & \\
 & \alpha^2 & \alpha^3 & & & & & & & & \\
 & \alpha & & ? & & 0 & & 0 & & 0 & \\
 & 1 & & & 1 & & \alpha^6 & & \alpha^4 & & 0 \\
 & 0 & 1 & & & & & & & & \\
 & & 0 & 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\
 & & & & & & & y & & &
\end{array}
$$

Let $P = (\alpha, 1)$ be the erased location. Recovery set $I_P = \{(\alpha^4, 1), (\alpha^3, 1)\}$
Find $f(x) : f(\alpha^4) = \alpha^7, f(\alpha^3) = \alpha^3$

$$\Rightarrow \quad f(x) = \alpha x - \alpha^2$$

$$f(\alpha) = 0 = F(P)$$

Hermitian codes

$q = q_0^2$, q_0 prime power

Hermitian codes

$q = q_0^2$, q_0 prime power

$$\mathcal{X} : x^{q_0} + x = y^{q_0+1}$$

Hermitian codes

$q = q_0^2$, q_0 prime power

$$\mathcal{X} : x^{q_0} + x = y^{q_0+1}$$

$\mathcal{X}$ has $q_0^3 = q^{3/2}$ points in $\mathbb{F}_q$

Hermitian codes

$q = q_0^2$, q_0 prime power

$$\mathcal{X} : x^{q_0} + x = y^{q_0+1}$$

$\mathcal{X}$ has $q_0^3 = q^{3/2}$ points in $\mathbb{F}_q$

Let $g : \mathcal{X} \to \mathcal{Y} = \mathbb{P}^1$, $g(P) = g(x, y) := y$

Hermitian codes

$q = q_0^2$, q_0 prime power

$$\mathcal{X} : x^{q_0} + x = y^{q_0+1}$$

$\mathcal{X}$ has $q_0^3 = q^{3/2}$ points in $\mathbb{F}_q$

Let $g : \mathcal{X} \to \mathcal{Y} = \mathbb{P}^1$, $g(P) = g(x, y) := y$

We obtain a family of q-ary codes of length $n = q_0^3$,

$$k = (t+1)(q_0 - 1), d \geq n - tq_0 - (q_0 - 2)(q_0 + 1)$$

with locality $r = q_0 - 1$.

Hermitian codes

$q = q_0^2$, q_0 prime power

$$\mathcal{X} : x^{q_0} + x = y^{q_0+1}$$

$\mathcal{X}$ has $q_0^3 = q^{3/2}$ points in $\mathbb{F}_q$

Let $g : \mathcal{X} \to \mathcal{Y} = \mathbb{P}^1$, $g(P) = g(x, y) := y$

We obtain a family of q-ary codes of length $n = q_0^3$,

$$k = (t+1)(q_0 - 1), d \geq n - tq_0 - (q_0 - 2)(q_0 + 1)$$

with locality $r = q_0 - 1$.

It is also possible to take $g(P) = x$ (projection on x); we obtain LRC codes with locality q_0

General construction

Map of curves

X, Y smooth projective absolutely irreducible curves over $\mathbb{k}$

$$g : X \to Y$$

rational separable map of degree $r + 1$

General construction

Map of curves

X, Y smooth projective absolutely irreducible curves over $\mathbb{k}$

$$g : X \to Y$$

rational separable map of degree $r+1$

Lift the points of Y

$S = \{P_1, \ldots, P_s\} \subset Y(\mathbb{k})$. Partition of points:

$$A := g^{-1}(S) = \{P_{ij}, i = 0, \ldots, r, j = 1, \ldots, s\} \subseteq X(\mathbb{k})$$

such that $g(P_{ij}) = P_j$ for all i, j

General construction

Map of curves

X, Y smooth projective absolutely irreducible curves over $\mathbb{k}$

$$g : X \to Y$$

rational separable map of degree $r+1$

Lift the points of Y

$S = \{P_1, \ldots, P_s\} \subset Y(\mathbb{k})$. Partition of points:

$$A := g^{-1}(S) = \{P_{ij}, i = 0, \ldots, r, j = 1, \ldots, s\} \subseteq X(\mathbb{k})$$

such that $g(P_{ij}) = P_j$ for all i, j

Let $x \in \mathbb{k}(X)$ be such that $\mathbb{k}(X) = \mathbb{k}(Y)(x)$, and let $\deg x = h$ as a projection $x : X \to \mathbb{P}^1_{\mathbb{k}}$

General construction, II

Let $Q_\infty \subset \pi^{-1}(\infty), \deg Q_\infty = \ell \geq 1$

Let $\mathcal{L}(Q_\infty) = \langle f_1, \ldots, f_m \rangle, m \geq \ell - g_Y + 1$

Function space

$$V := \left\langle f_j x^i, i = 0, \ldots, r-1; j = 1, \ldots, m \right\rangle$$

General construction, II

Let $Q_\infty \subset \pi^{-1}(\infty), \deg Q_\infty = \ell \geq 1$

Let $\mathcal{L}(Q_\infty) = \langle f_1, \ldots, f_m \rangle, m \geq \ell - g_Y + 1$

Function space

$$V := \left\langle f_j x^i, i = 0, \ldots, r-1; j = 1, \ldots, m \right\rangle$$

The code $\mathcal{C}$ is an image of the map

$$\begin{aligned} e := ev_A : V &\longrightarrow \mathbb{k}^{(r+1)s} \\ F &\mapsto (F(P_{ij}), i = 0, \ldots, r, j = 1, \ldots, s) \end{aligned}$$

General construction, II

Let $Q_\infty \subset \pi^{-1}(\infty), \deg Q_\infty = \ell \geq 1$

Let $\mathcal{L}(Q_\infty) = \langle f_1, \ldots, f_m \rangle, m \geq \ell - g_Y + 1$

Function space

$$V := \left\langle f_j x^i, i = 0, \ldots, r-1; j = 1, \ldots, m \right\rangle$$

The code $\mathcal{C}$ is an image of the map

$$\begin{aligned} e := ev_A : V &\longrightarrow \mathbb{k}^{(r+1)s} \\ F &\mapsto (F(P_{ij}), i = 0, \ldots, r, j = 1, \ldots, s) \end{aligned}$$

Theorem: (with I.Tamo and S.Vlăduţ, '15) The subspace $\mathcal{C}(D, g) \subset \mathbb{F}_q$ forms an (n, k, r) linear LRC code with the parameters

$$\left.\begin{array}{c} n = (r+1)s \\ k = rm \geq r(\ell - g_Y + 1) \\ d \geq n - \ell(r+1) - (r-1)h \end{array}\right\}$$

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

Asymptotically good sequences of codes

Let $q = q_0^2$, where q_0 is a prime power. Take Garcia-Stichtenoth towers of curves:

$$x_0 := 1;\ X_1 := \mathbb{P}^1, \Bbbk(X_1) = \Bbbk(x_1);$$

$$X_l : z_l^{q_0} + z_l = x_{l-1}^{q_0+1}, x_{l-1} := \frac{z_{l-1}}{x_{l-2}} \in \Bbbk(X_{l-1}) \text{ (if } l \geq 3)$$

Asymptotically good sequences of codes

Let $q = q_0^2$, where q_0 is a prime power. Take Garcia-Stichtenoth towers of curves:

$$x_0 := 1;\ X_1 := \mathbb{P}^1, \Bbbk(X_1) = \Bbbk(x_1);$$

$$X_l : z_l^{q_0} + z_l = x_{l-1}^{q_0+1}, x_{l-1} := \frac{z_{l-1}}{x_{l-2}} \in \Bbbk(X_{l-1}) \text{ (if } l \geq 3)$$

There exist families of q-ary LRC codes with locality r whose *rate and relative distance* satisfy

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

$$R \geq \frac{r}{r+1}\left(1 - \delta - \frac{2\sqrt{q}}{q-1}\right), \qquad r = \sqrt{q}$$

Asymptotically good sequences of codes

Let $q = q_0^2$, where q_0 is a prime power. Take Garcia-Stichtenoth towers of curves:

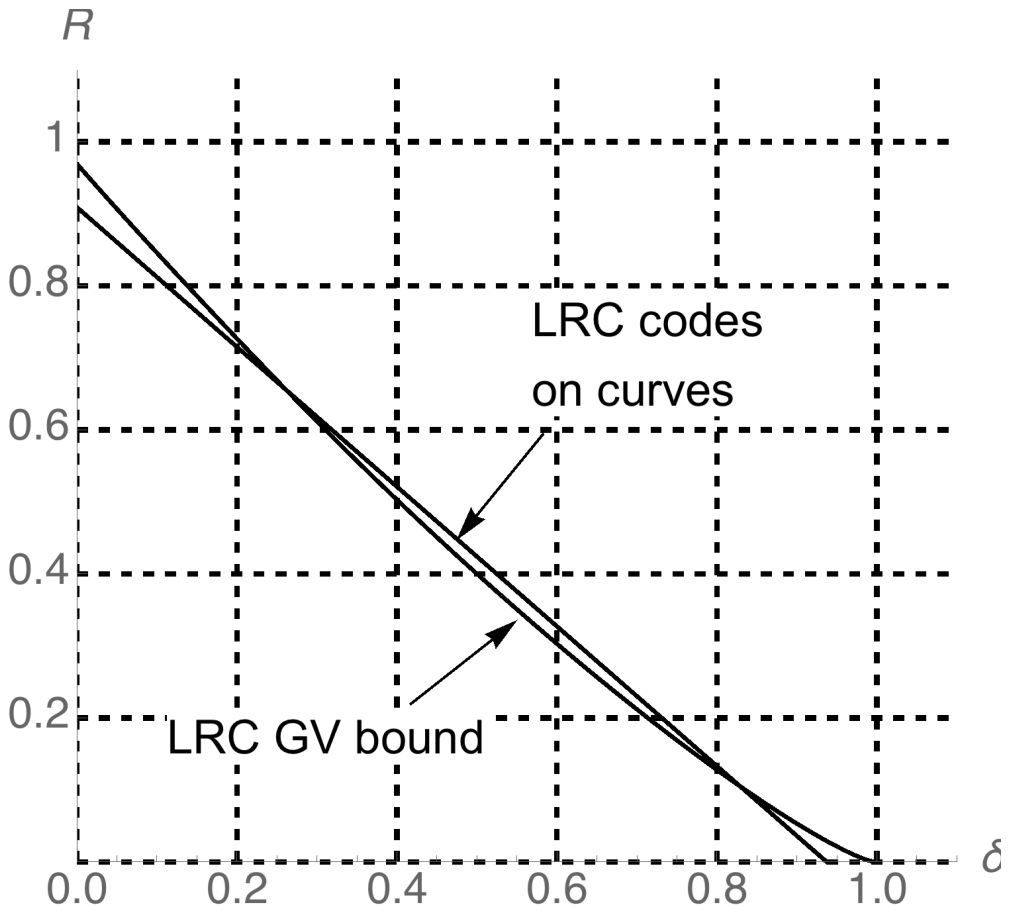
$$x_0 := 1;\ X_1 := \mathbb{P}^1, \Bbbk(X_1) = \Bbbk(x_1);$$
$$X_l : z_l^{q_0} + z_l = x_{l-1}^{q_0+1}, x_{l-1} := \frac{z_{l-1}}{x_{l-2}} \in \Bbbk(X_{l-1}) \text{ (if } l \geq 3)$$

There exist families of q-ary LRC codes with locality r whose *rate and relative distance* satisfy

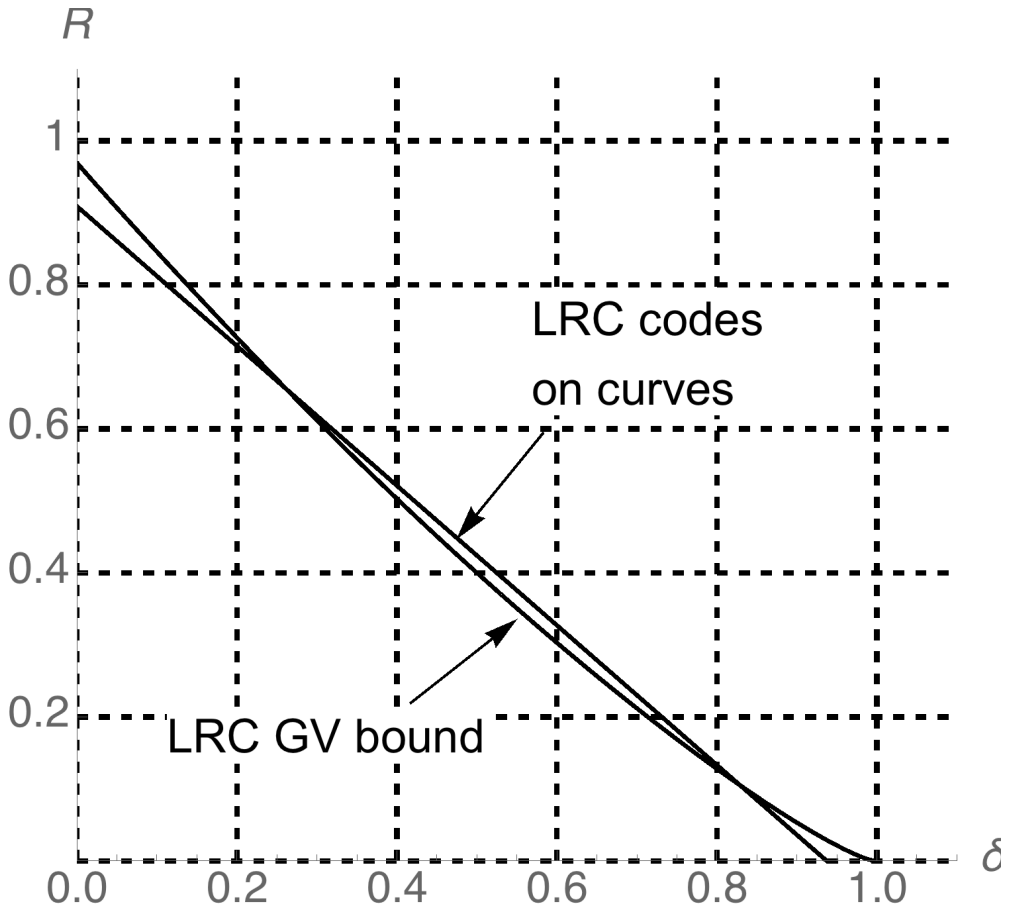
$$R \geq \frac{r}{r+1}\left(1 - \delta - \frac{3}{\sqrt{q}+1}\right), \qquad r = \sqrt{q} - 1$$
$$R \geq \frac{r}{r+1}\left(1 - \delta - \frac{2\sqrt{q}}{q-1}\right), \qquad r = \sqrt{q}$$

*) Recall the TVZ '81 bound without locality: $R \geq 1 - \delta - \frac{1}{\sqrt{q}-1}$

LRC codes on curves better than the GV bound



LRC codes on curves better than the GV bound



The asymptotic GV bound can be improved for any given (constant) r for all q greater than some value.

Reducing the locality

For Hermitian or GS curves we had $r = q_0 = \sqrt{q}$ (rather large)

Reducing the locality

For Hermitian or GS curves we had $r = q_0 = \sqrt{q}$ (rather large)
It is possible to reduce locality by taking r such that $(r+1)|(q_0+1)$
Take $X = X_l$, $Y := Y_{l,r}$ be such that

$$\Bbbk(Y_{l,r}) = \Bbbk(x_1^{r+1}, z_2, \ldots, z_l)$$

Reducing the locality

For Hermitian or GS curves we had $r = q_0 = \sqrt{q}$ (rather large)
It is possible to reduce locality by taking r such that $(r+1)|(q_0+1)$
Take $X = X_l$, $Y := Y_{l,r}$ be such that

$$\Bbbk(Y_{l,r}) = \Bbbk(x_1^{r+1}, z_2, \ldots, z_l)$$

Proposition

Let $(r+1)|(q_0+1)$. There exists a family of q-ary (n,k,r) LRC codes on the curve $X_l, l \geq 2$ with the parameters

$$\left.\begin{aligned} n = n_l &= q_0^{l-1}(q_0^2-1) \\ k &\geq r\left(\ell - q_0^{l-1}\frac{q_0+1}{r+1} + 1\right) \\ d &\geq n_l - \ell(r+1) - (r-1)q_0^{l-1} \end{aligned}\right\} \quad (3)$$

where ℓ is any integer such that $g_Y \leq \ell \leq n_{l-1}$.

Reducing the locality

For Hermitian or GS curves we had $r = q_0 = \sqrt{q}$ (rather large)
It is possible to reduce locality by taking r such that $(r+1)|(q_0+1)$
Take $X = X_l$, $Y := Y_{l,r}$ be such that

$$\Bbbk(Y_{l,r}) = \Bbbk(x_1^{r+1}, z_2, \ldots, z_l)$$

Proposition

Let $(r+1)|(q_0+1)$. There exists a family of q-ary (n,k,r) LRC codes on the curve $X_l, l \geq 2$ with the parameters

$$\left.\begin{aligned} n = n_l &= q_0^{l-1}(q_0^2-1) \\ k &\geq r\left(\ell - q_0^{l-1}\frac{q_0+1}{r+1} + 1\right) \\ d &\geq n_l - \ell(r+1) - (r-1)q_0^{l-1} \end{aligned}\right\} \quad (3)$$

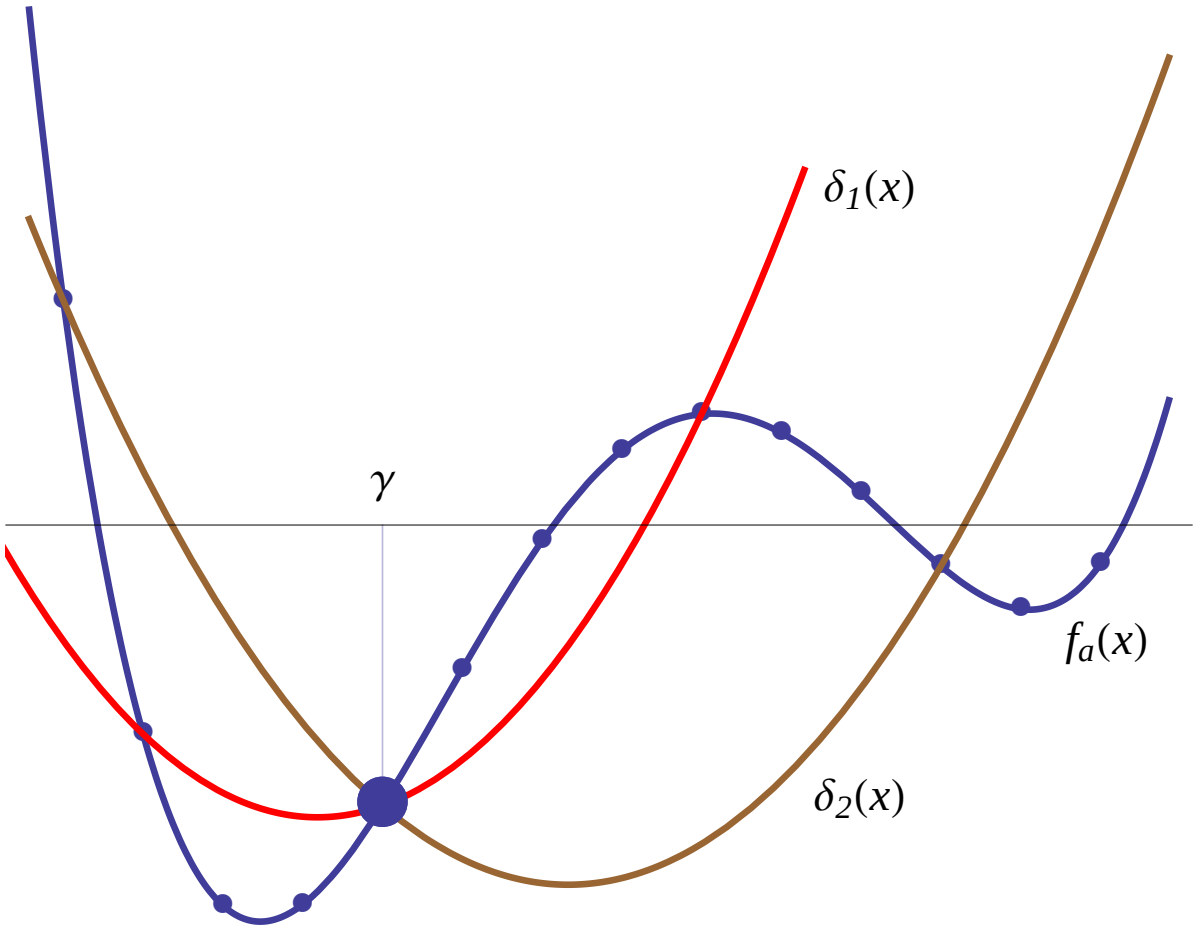
where ℓ is any integer such that $g_Y \leq \ell \leq n_{l-1}$.

(asymptotic improvement of the GV bound for $r = 2$, $q = 32$)

Availability

A code $\mathcal{C}$ is called an $LRC(2)$ code if every coordinate has 2 disjoint recovery sets $R_{1,i}, |R_{1,i}| \leq r_1$; $R_{2,i}, |R_{2,i}| \leq r_2$

Multiple recovery sets: Idea of construction



$f_a(\gamma)$ can be found by interpolating $\delta_1(x)$ as well as $\delta_2(x)$

Multiple recovery sets: Example

Take $\mathbb{F} = \mathbb{F}_{13}$; $G, H \leq \mathbb{F}^*$; $G = \langle 5 \rangle, H = \langle 3 \rangle$

$$\mathcal{A}_G = \{\{1, 5, 12, 8\}, \{2, 10, 11, 3\}, \{4, 7, 9, 6\}\}$$
$$\mathcal{A}_H = \{\{1, 3, 9\}, \{2, 6, 5\}, \{4, 12, 10\}, \{7, 8, 11\}\}$$

Let

$$\mathbb{F}_{\mathcal{A}_G}[x] = \{f \in \mathbb{F}[x] : f \text{ is constant on } A_i, i = 1, 2, 3;\ \deg f < |\mathbb{F}^*|\}$$
$$\mathbb{F}_{\mathcal{A}_G}[x] = \langle 1, x^4, x^8 \rangle, \quad \mathbb{F}_{\mathcal{A}_H}[x] = \langle 1, x^3, x^6, x^9 \rangle$$

Multiple recovery sets: Example

Take $\mathbb{F} = \mathbb{F}_{13}$; $G, H \leq \mathbb{F}^*$; $G = \langle 5 \rangle, H = \langle 3 \rangle$

$$\mathcal{A}_G = \{\{1,5,12,8\},\{2,10,11,3\},\{4,7,9,6\}\}$$
$$\mathcal{A}_H = \{\{1,3,9\},\{2,6,5\},\{4,12,10\},\{7,8,11\}\}$$

Let

$$\mathbb{F}_{\mathcal{A}_G}[x] = \{f \in \mathbb{F}[x] : f \text{ is constant on } A_i, i = 1,2,3;\ \deg f < |\mathbb{F}^*|\}$$
$$\mathbb{F}_{\mathcal{A}_G}[x] = \langle 1, x^4, x^8 \rangle, \quad \mathbb{F}_{\mathcal{A}_H}[x] = \langle 1, x^3, x^6, x^9 \rangle$$

We construct an LRC $(12, 4, \{2,3\})$, distance ≥ 6, code $\mathcal{C} : \mathbb{F}^4 \to \mathbb{F}^{12}$

$$a = (a_0, a_1, a_2, a_3) \mapsto f_a(x) = a_0 + a_1 x + a_2 x^4 + a_3 x^6$$

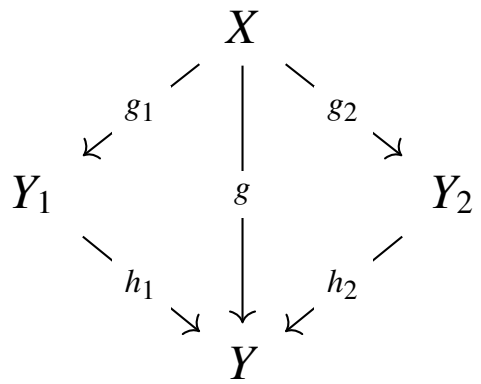
$$f_a(x) = \sum_{i=0}^{2} f_i(x) x^i, \text{ where } f_0(x) = a_0 + a_2 x^4,\ f_1(x) = a_1,\ f_2(x) = a_3 x^4; f_i \in \mathbb{F}_{\mathcal{A}}[x]$$

$$f_a(x) = \sum_{j=0}^{1} g_j(x) x^j \text{ where } g_0(x) = a_0 + a_3 x^6, g_1(x) = a_1 + a_2 x^3; g_j \in \mathbb{F}_{\mathcal{A}_H}[x]$$

E.g., $f_a(1)$ can be recovered by computing $\delta_1(x), x \in \{5,12,8\}$ OR $\delta_2(x), x \in \{3,9\}$

Availability and codes on curves

Codes on Hermitian curves naturally provide 2 recovery sets. Generally:



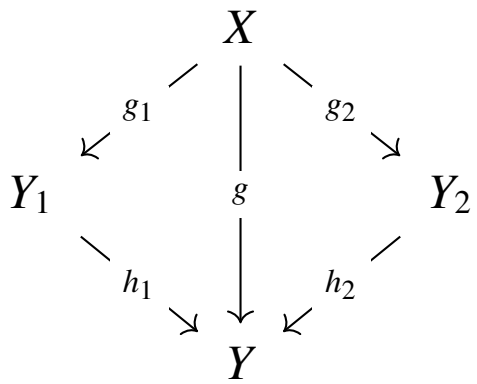
$$\deg g = d_g; \deg g_1 = \deg h_2 = d_{1,g}; \deg g_2 = \deg h_1 = d_{2,g}$$

Fiber product $X = Y_1 \times_Y Y_2$

$$g^*(\Bbbk(Y)) = g_1^*(\Bbbk(Y_1)) \cap g_2^*(\Bbbk(Y_2))$$

Availability and codes on curves

Codes on Hermitian curves naturally provide 2 recovery sets. Generally:



$$\deg g = d_g; \deg g_1 = \deg h_2 = d_{1,g}; \deg g_2 = \deg h_1 = d_{2,g}$$

Fiber product $X = Y_1 \times_Y Y_2$

$$g^*(\Bbbk(Y)) = g_1^*(\Bbbk(Y_1)) \cap g_2^*(\Bbbk(Y_2))$$

Data for constructing the code: Let $D \in \mathcal{D}(Y), D \geq 0, \deg D = \ell, \mathrm{supp}(D) \subset \pi^{-1}(\infty)$ $\{f_1, \ldots, f_m\}$ a basis of $L(D) \subset \Bbbk(Y)$.
Consider the following polynomial space of dimension md_g:

$$L := \text{span}\,\{x_1^i x_2^j f_k, i = 0, 1, \ldots, d_{1,g} - 2, j = 0, 1, \ldots, d_{2,g} - 2, k = 1, \ldots, m\} \subset \Bbbk(X).$$

Hermitian codes with two recovery sets

X Hermitian curve over $\mathbb{k} = \mathbb{F}_q, q = q_0^2$.

Hermitian codes with two recovery sets

X Hermitian curve over $\Bbbk = \mathbb{F}_q, q = q_0^2$.

Take $e_1 | (q_0 + 1)$; consider the map $g_1 : X \to Y_1$

$$g_1(x, y) := (x, y^{d_1}); \quad d_1 = \frac{q_0 + 1}{e_1}; r_1 = d_1 - 1$$

Then

$$Y_1 : x^{q_0} + x = u^{e_1}; \quad \Bbbk(Y_1) = \Bbbk(x, u := y^{d_1})$$

Hermitian codes with two recovery sets

X Hermitian curve over $\Bbbk = \mathbb{F}_q, q = q_0^2$.

Take $e_1 | (q_0 + 1)$; consider the map $g_1 : X \to Y_1$

$$g_1(x, y) := (x, y^{d_1}); \quad d_1 = \frac{q_0 + 1}{e_1}; r_1 = d_1 - 1$$

Then

$$Y_1 : x^{q_0} + x = u^{e_1}; \quad \Bbbk(Y_1) = \Bbbk(x, u := y^{d_1})$$

Take $d_2 | q_0$ such that $q_0 = d_2^a$ for some $a \geq 1$; consider the projection $g_2 : X \to Y_2$

$$g_2(x, y) := (v := x^{d_2} + x, y), \text{where} \quad \Bbbk(Y_2) = \Bbbk(v, y).$$

Let $r_2 = d_2 - 1$.

Hermitian codes with two recovery sets

X Hermitian curve over $\Bbbk = \mathbb{F}_q, q = q_0^2$.

Take $e_1 | (q_0 + 1)$; consider the map $g_1 : X \to Y_1$

$$g_1(x, y) := (x, y^{d_1}); \quad d_1 = \frac{q_0 + 1}{e_1}; r_1 = d_1 - 1$$

Then

$$Y_1 : x^{q_0} + x = u^{e_1}; \quad \Bbbk(Y_1) = \Bbbk(x, u := y^{d_1})$$

Take $d_2 | q_0$ such that $q_0 = d_2^a$ for some $a \geq 1$; consider the projection $g_2 : X \to Y_2$

$$g_2(x, y) := (v := x^{d_2} + x, y), \text{where} \quad \Bbbk(Y_2) = \Bbbk(v, y).$$

Let $r_2 = d_2 - 1$. Finally, define the curve Y by $\Bbbk(Y) := \Bbbk(Y_1) \cap \Bbbk(Y_2) \subset \Bbbk(X)$.

Hermitian codes with two recovery sets

X Hermitian curve over $\Bbbk = \mathbb{F}_q, q = q_0^2$.

Take $e_1 | (q_0 + 1)$; consider the map $g_1 : X \to Y_1$

$$g_1(x, y) := (x, y^{d_1}); \quad d_1 = \frac{q_0 + 1}{e_1}; r_1 = d_1 - 1$$

Then

$$Y_1 : x^{q_0} + x = u^{e_1}; \quad \Bbbk(Y_1) = \Bbbk(x, u := y^{d_1})$$

Take $d_2 | q_0$ such that $q_0 = d_2^a$ for some $a \geq 1$; consider the projection $g_2 : X \to Y_2$

$$g_2(x, y) := (v := x^{d_2} + x, y), \text{where} \quad \Bbbk(Y_2) = \Bbbk(v, y).$$

Let $r_2 = d_2 - 1$. Finally, define the curve Y by $\Bbbk(Y) := \Bbbk(Y_1) \cap \Bbbk(Y_2) \subset \Bbbk(X)$.

This approach can be also implemented for GS curves

References

- with Itzhak Tamo, A family of optimal locally recoverable codes, IT Trans, Aug. 2014
- with Itzhak Tamo and Alexey Frolov, Bounds on the parameters of LRC codes, IT Trans., June 2016
- with Itzhak Tamo, S. Goparaju, and R. Calderbank, Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes, preprint arXiv:1603.08878
- with Itzhak Tamo and Serge Vlăduţ, LRC codes on algebraic curves preprint arXiv:1603.08876

References

- with Itzhak Tamo, A family of optimal locally recoverable codes, IT Trans, Aug. 2014
- with Itzhak Tamo and Alexey Frolov, Bounds on the parameters of LRC codes, IT Trans., June 2016
- with Itzhak Tamo, S. Goparaju, and R. Calderbank, Cyclic LRC codes, binary LRC codes, and upper bounds on the distance of cyclic codes, preprint arXiv:1603.08878
- with Itzhak Tamo and Serge Vlăduţ, LRC codes on algebraic curves preprint arXiv:1603.08876

Thank you!