Algebraic Geometry C^{2}odes in The sum-rank metric

Elena Berardini and X.Caruso

CNRS, Institut de Mathématiques de Bordeaux

09 June 2023

https://arxiv.org/abs/2303.08903

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 899987

Linear codes and codes in the Hamming metric

k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Linear codes and codes in the Hamming metric

k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Codes in the Hamming metric: k-vector subspaces of k^n endowed with $d(x, y) := \#\{i \mid x_i \neq y_i\}$

Linear codes and codes in the Hamming metric

k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Codes in the Hamming metric: k-vector subspaces of k^n endowed with $d(x, y) := \#\{i \mid x_i \neq y_i\}$

Reed–Solomon (RS) codes:

$$\mathrm{RS}_\delta(\mathbf{x}) := \{(P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\delta}\}$$

Linear codes and codes in the Hamming metric

k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Codes in the Hamming metric: k-vector subspaces of k^n endowed with $d(x,y) := \#\{i \mid x_i \neq y_i\}$

Reed–Solomon (RS) codes:

$$\mathrm{RS}_\delta(\mathbf{x}) := \{(P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\delta}\}$$

✔ **Optimal parameters:** $\delta + d = n + 1$
(Singleton bound: $\delta + d \leq n + 1$)

⚠ **Drawback:** $n \leqslant q$

Linear codes and codes in the Hamming metric

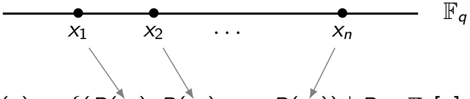
k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Codes in the Hamming metric: k-vector subspaces of k^n endowed with $d(x,y) := \#\{i \mid x_i \neq y_i\}$

Reed–Solomon (RS) codes:

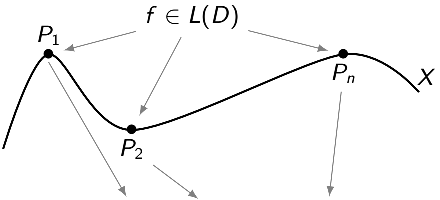


$$\mathrm{RS}_\delta(\mathbf{x}) := \{(P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\delta}\}$$

✔ **Optimal parameters:** $\delta + d = n + 1$
(Singleton bound: $\delta + d \leq n + 1$)

⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes:



$$\mathcal{C}_X(\mathcal{P}, L(D)) := \{(f(P_1), f(P_2), \ldots, f(P_n)) \mid f \in L(D)\}$$

Linear codes and codes in the Hamming metric

k a field (think about $k = \mathbb{F}_q$), $\mathcal{H}$ a k-linear vector space endowed with a metric

Linear code $\mathcal{C}$: k-vector subspace of $\mathcal{H}$

Parameters: length $n = \dim_k \mathcal{H}$, dimension $\delta = \dim_k \mathcal{C}$, minimum distance d (depends on the metric)

Codes in the Hamming metric: k-vector subspaces of k^n endowed with $d(x,y) := \#\{i \mid x_i \neq y_i\}$

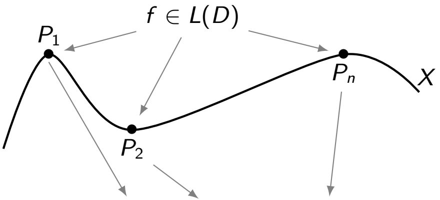
Reed–Solomon (RS) codes:

$$\mathrm{RS}_\delta(\mathbf{x}) := \{(P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\delta}\}$$

✔ **Optimal parameters:** $\delta + d = n + 1$
(Singleton bound: $\delta + d \leq n + 1$)

⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes:



$$\mathcal{C}_X(\mathcal{P}, L(D)) := \{(f(P_1), f(P_2), \dots, f(P_n)) \mid f \in L(D)\}$$

✔ **Good parameters:** $n+1-g \leq \delta + d \leq n+1$

✔ **Longer codes**

General definitions

$\underline{V} = (V_1, \ldots, V_s)$ s-uple of k-vector spaces $(n_i = \dim_k V_i)$

$$\mathcal{H} = \mathrm{End}_k(\underline{V}) := \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s)$$

k-vector space of dimension $\sum_{i=1}^{s} n_i^2$ — k-linear morphisms $V_i \to V_i$

General definitions

$\underline{V} = (V_1, \ldots, V_s)$ s-uple of k-vector spaces $(n_i = \dim_k V_i)$

$$\mathcal{H} = \mathrm{End}_k(\underline{V}) := \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s)$$

k-vector space of dimension $\sum_{i=1}^{s} n_i^2$ — k-linear morphisms $V_i \to V_i$

Definition

Let $\underline{\varphi} = (\varphi_1, \ldots, \varphi_s) \in \mathcal{H}$. The sum-rank weight of $\underline{\varphi}$ is $w_{srk}(\underline{\varphi}) := \sum_{i=1}^{s} rk(\varphi_i)$.
The sum-rank distance between $\underline{\varphi}, \underline{\psi} \in \mathcal{H}$ is

$$d_{srk}(\underline{\varphi}, \underline{\psi}) := w_{srk}(\underline{\varphi} - \underline{\psi}).$$

General definitions

$\underline{V} = (V_1, \ldots, V_s)$ s-uple of k-vector spaces $(n_i = \dim_k V_i)$

$$\mathcal{H} = \mathrm{End}_k(\underline{V}) \quad := \quad \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s)$$

k-vector space of dimension $\sum_{i=1}^{s} n_i^2$ — k-linear morphisms $V_i \to V_i$

Definition

Let $\underline{\varphi} = (\varphi_1, \ldots, \varphi_s) \in \mathcal{H}$. The sum-rank weight of $\underline{\varphi}$ is $w_{srk}(\underline{\varphi}) := \sum_{i=1}^{s} rk(\varphi_i)$.
The sum-rank distance between $\underline{\varphi}, \underline{\psi} \in \mathcal{H}$ is

$$d_{srk}(\underline{\varphi}, \underline{\psi}) := w_{srk}(\underline{\varphi} - \underline{\psi}).$$

A code $\mathcal{C}$ in the sum-rank metric is a k–linear subspace of $\mathcal{H}$ endowed with the sum-rank distance.

General definitions

$\underline{V} = (V_1, \ldots, V_s)$ s-uple of k-vector spaces $(n_i = \dim_k V_i)$

$$\mathcal{H} = \mathrm{End}_k(\underline{V}) := \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s)$$

k-vector space of dimension $\sum_{i=1}^{s} n_i^2$ — k-linear morphisms $V_i \to V_i$

Definition

Let $\underline{\varphi} = (\varphi_1, \ldots, \varphi_s) \in \mathcal{H}$. The sum-rank weight of $\underline{\varphi}$ is $w_{srk}(\underline{\varphi}) := \sum_{i=1}^{s} rk(\varphi_i)$.
The sum-rank distance between $\underline{\varphi}, \underline{\psi} \in \mathcal{H}$ is

$$d_{srk}(\underline{\varphi}, \underline{\psi}) := w_{srk}(\underline{\varphi} - \underline{\psi}).$$

A code $\mathcal{C}$ in the sum-rank metric is a k–linear subspace of $\mathcal{H}$ endowed with the sum-rank distance. Its length n is $\sum_{i=1}^{s} n_i^2$. Its dimension δ is $\dim_k \mathcal{C}$. Its minimum distance is

$$d := \min\left\{ w_{srk}(\underline{\varphi}) \mid \underline{\varphi} \in \mathcal{C}, \underline{\varphi} \neq \underline{0} \right\}.$$

General definitions

$\underline{V} = (V_1, \ldots, V_s)$ s-uple of k-vector spaces $(n_i = \dim_k V_i)$

$$\mathcal{H} = \mathrm{End}_k(\underline{V}) := \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s)$$

k-vector space of dimension $\sum_{i=1}^s n_i^2$ — k-linear morphisms $V_i \to V_i$

Definition

Let $\underline{\varphi} = (\varphi_1, \ldots, \varphi_s) \in \mathcal{H}$. The sum-rank weight of $\underline{\varphi}$ is $w_{srk}(\underline{\varphi}) := \sum_{i=1}^s rk(\varphi_i)$. The sum-rank distance between $\underline{\varphi}, \underline{\psi} \in \mathcal{H}$ is

$$d_{srk}(\underline{\varphi}, \underline{\psi}) := w_{srk}(\underline{\varphi} - \underline{\psi}).$$

A code $\mathcal{C}$ in the sum-rank metric is a k–linear subspace of $\mathcal{H}$ endowed with the sum-rank distance. Its length n is $\sum_{i=1}^s n_i^2$. Its dimension δ is $\dim_k \mathcal{C}$. Its minimum distance is

$$d := \min \left\{ w_{srk}(\underline{\varphi}) \mid \underline{\varphi} \in \mathcal{C}, \underline{\varphi} \neq \underline{0} \right\}.$$

$n_i = 1 \ \forall i \quad \rightsquigarrow \quad$ codes of length s in the Hamming metric

Particular case and Singleton bound

$\ell =$ finite extension of k of degree r

$\underline{V} = (V_1, \ldots, V_s)$, s-uple of ℓ-vector spaces $(\dim_k V_i = r)$ $\rightsquigarrow$ $\mathcal{H} = \mathrm{End}_k(\underline{V})$ is a ℓ-vector space

Particular case and Singleton bound

$\ell =$ finite extension of k of degree r

$\underline{V} = (V_1, \ldots, V_s)$, s-uple of ℓ-vector spaces ($\dim_k V_i = r$) $\rightsquigarrow \mathcal{H} = \mathrm{End}_k(\underline{V})$ is a ℓ-vector space

$\rightsquigarrow$ ℓ–linear codes in the sum-rank metric: ℓ–linear subspaces $\mathcal{C} \subset \mathcal{H}$

$\rightsquigarrow$ ℓ–variants of the parameters:

$$\begin{cases} n_\ell := sr & \ell\text{–length} \\ \delta_\ell := \dim_\ell \mathcal{C} & \ell\text{–dimension} \\ \text{the minimum distance stays unchanged} \end{cases}$$

Particular case and Singleton bound

$\ell =$ finite extension of k of degree r

$\underline{V} = (V_1, \ldots, V_s)$, s-uple of ℓ-vector spaces ($\dim_k V_i = r$) $\rightsquigarrow \mathcal{H} = \mathrm{End}_k(\underline{V})$ is a ℓ-vector space

$\rightsquigarrow$ ℓ–linear codes in the sum-rank metric: ℓ–linear subspaces $\mathcal{C} \subset \mathcal{H}$

$\rightsquigarrow$ ℓ–variants of the parameters:

$$\begin{cases} n_\ell := sr & \ell\text{–length} \\ \delta_\ell := \dim_\ell \mathcal{C} & \ell\text{–dimension} \\ \text{the minimum distance stays unchanged} & \end{cases}$$

Singleton bound

The ℓ-parameters of $\mathcal{C}$ satisfy

$$d + \delta_\ell \leq n_\ell + 1.$$

Codes with parameters attaining this bound are called Maximum Sum-Rank Distance (MSRD).

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\begin{array}{c} \ell \\ \Big\downarrow \Phi \\ k \end{array}$$

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

The ring of Ore polynomials $\ell[T; \Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\begin{array}{c} \ell \\ \Big\downarrow \Phi \\ k \end{array}$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a) T \quad \forall a \in \ell.$$

$$\begin{array}{rccc} \mathrm{ev} : & \ell[T;\Phi] & \to & \mathrm{End}_k(\ell) \\ & P & \mapsto & P(\Phi). \end{array}$$

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

for $c \in \ell$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

$$\begin{array}{rccc} \mathrm{ev}_c : & \ell[T;\Phi] & \to & \mathrm{End}_k(\ell) \\ & P & \mapsto & P(c\Phi). \end{array}$$

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\begin{array}{c} \ell \\ \big\downarrow \Phi \\ k \end{array}$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a) T \quad \forall a \in \ell.$$

for $\underline{c} = (c_1, \ldots, c_s) \in \ell^s$

$$\begin{array}{rrcl} \mathrm{ev}_{\underline{c}} : & \ell[T;\Phi] & \to & \mathrm{End}_k(\ell)^s \\ & P & \mapsto & (P(c_1\Phi), \ldots, P(c_s\Phi)). \end{array}$$

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

Linearized Reed–Solomon codes (Martínez-Peñas, 2018)

for $\underline{c} = (c_1, \dots, c_s) \in \ell^s$ and $\delta \in \mathbb{Z}$ consider

$$\begin{array}{rrcl} \mathrm{ev}_{\underline{c}} : & \ell[T;\Phi]_{<\delta} & \to & \mathrm{End}_k(\ell)^s \\ & P & \mapsto & (P(c_1\Phi), \dots, P(c_s\Phi)). \end{array}$$

We define $\mathrm{LRS}(\delta, \underline{c}) = \mathrm{ev}_{\underline{c}}(\ell[T;\Phi]_{<\delta})$.

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

Linearized Reed–Solomon codes (Martínez-Peñas, 2018)

for $\underline{c} = (c_1, \dots, c_s) \in \ell^s$ such that $N_{\ell/k}(c_i) \neq N_{\ell/k}(c_j)\ \forall i \neq j$ and $\delta \in \mathbb{Z}$ such that $\delta \leq rs$ consider

$$\begin{array}{rrcl} \mathrm{ev}_{\underline{c}}: & \ell[T;\Phi]_{<\delta} & \to & \mathrm{End}_k(\ell)^s \\ & P & \mapsto & (P(c_1\Phi), \dots, P(c_s\Phi)). \end{array}$$

We define $\mathrm{LRS}(\delta, \underline{c}) = \mathrm{ev}_{\underline{c}}(\ell[T;\Phi]_{<\delta})$. MSRD codes!

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

Linearized Reed–Solomon codes (Martínez-Peñas, 2018)

for $\underline{c} = (c_1, \ldots, c_s) \in \ell^s$ such that $N_{\ell/k}(c_i) \neq N_{\ell/k}(c_j)\ \forall i \neq j$ and $\delta \in \mathbb{Z}$ such that $\delta \leq rs$ consider

$$\begin{array}{rrcl} \mathrm{ev}_{\underline{c}} : & \ell[T;\Phi]_{<\delta} & \to & \mathrm{End}_k(\ell)^s \\ & P & \mapsto & (P(c_1\Phi), \ldots, P(c_s\Phi)). \end{array}$$

We define $\mathrm{LRS}(\delta, \underline{c}) = \mathrm{ev}_{\underline{c}}(\ell[T;\Phi]_{<\delta})$. MSRD codes!

$\Rightarrow s \leq \mathrm{Card}(k) \rightsquigarrow$ same problem as Reed–Solomon codes

Ore polynomials and Linearized Reed–Solomon codes

ℓ field, $\Phi : \ell \to \ell$ a ring homomorphism, $\ell^{\Phi=1} = k$, $[\ell : k] = r$,

$$\ell \xrightarrow{\Phi} k$$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring whose elements are polynomials with coefficients in ℓ, with usual $+$ and

$$T \times a = \Phi(a)T \quad \forall a \in \ell.$$

Linearized Reed–Solomon codes (Martínez-Peñas, 2018)

for $\underline{c} = (c_1, \dots, c_s) \in \ell^s$ such that $N_{\ell/k}(c_i) \neq N_{\ell/k}(c_j)\ \forall i \neq j$ and $\delta \in \mathbb{Z}$ such that $\delta \leq rs$ consider

$$\begin{array}{rccc} \mathrm{ev}_{\underline{c}} : & \ell[T;\Phi]_{<\delta} & \to & \mathrm{End}_k(\ell)^s \\ & P & \mapsto & (P(c_1\Phi), \dots, P(c_s\Phi)). \end{array}$$

We define $\mathrm{LRS}(\delta, \underline{c}) = \mathrm{ev}_{\underline{c}}(\ell[T;\Phi]_{<\delta})$. MSRD codes!

$\Rightarrow s \leq \mathrm{Card}(k) \rightsquigarrow$ same problem as Reed–Solomon codes

As in the Hamming case, we can **try to overcome the problem using algebraic curves**
Main idea: consider Ore polynomials with coefficients in the function field of a curve

Divisors and Riemann–Roch spaces: classical theory

Definition

Let X be a nice curve, K its function field. A divisor on X is a formal finite sum

$$D = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \mathfrak{p} \quad \text{with } n_{\mathfrak{p}} \in \mathbb{Z} \text{ almost all zero.}$$

The group of divisors on X is denoted by $Div(X)$.
$D \in Div(X)$ is positive, $D \geq 0$, if $n_{\mathfrak{p}} \geq 0\ \forall \mathfrak{p}$. The degree of D is $\deg_X(D) = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \deg_X(\mathfrak{p})$.

Divisors and Riemann–Roch spaces: classical theory

Definition

Let X be a nice curve, K its function field. A divisor on X is a formal finite sum

$$D = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \mathfrak{p} \quad \text{with } n_{\mathfrak{p}} \in \mathbb{Z} \text{ almost all zero.}$$

The group of divisors on X is denoted by $Div(X)$.
$D \in Div(X)$ is positive, $D \geq 0$, if $n_{\mathfrak{p}} \geq 0 \ \forall \mathfrak{p}$. The degree of D is $\deg_X(D) = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \deg_X(\mathfrak{p})$.
The Riemann–Roch space associated with D is

$$L_X(D) := \{x \in K^\times \mid (x) + D \geq 0\} \cup \{0\},$$

where $(x) = \sum_{\mathfrak{p} \in X} v_{\mathfrak{p}}(x)\, \mathfrak{p}$ is the principal divisor associated to a nonzero function $x \in K$.

Divisors and Riemann–Roch spaces: classical theory

Definition

Let X be a nice curve, K its function field. A divisor on X is a formal finite sum

$$D = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \mathfrak{p} \quad \text{with } n_{\mathfrak{p}} \in \mathbb{Z} \text{ almost all zero.}$$

The group of divisors on X is denoted by $Div(X)$.
$D \in Div(X)$ is positive, $D \geq 0$, if $n_{\mathfrak{p}} \geq 0\ \forall \mathfrak{p}$. The degree of D is $\deg_X(D) = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \deg_X(\mathfrak{p})$.
The Riemann–Roch space associated with D is

$$L_X(D) := \{x \in K^\times \mid (x) + D \geq 0\} \cup \{0\},$$

where $(x) = \sum_{\mathfrak{p} \in X} v_{\mathfrak{p}}(x)\, \mathfrak{p}$ is the principal divisor associated to a nonzero function $x \in K$.

Riemann–Roch theorem

Let K_X denotes a canonical divisor on X. For any divisor $D \in \mathrm{Div}(X)$ we have

$$\dim_k L_X(D) = \deg_X(D) + 1 - g_X + \underbrace{\dim_k L_X(K_X - D)}_{=0 \text{ when } \deg_X(D) > 2g_X - 2.},$$

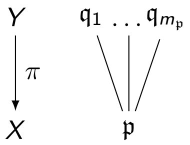
Our setting

$$\begin{array}{c} Y \\ \downarrow \pi \\ X \end{array}$$

π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

Our setting



π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

Our setting

$$\begin{array}{ccc} Y & & \mathfrak{q}_1 \ldots \mathfrak{q}_{m_\mathfrak{p}} \\ \downarrow \pi & & \diagdown \mid \diagup \\ X & & \mathfrak{p} \end{array}$$

π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

For $x \in K^\times$, consider the algebra

$$D_{L,x} := L[T;\Phi]/(T^r - x)$$

and for all $\mathfrak{p} \in X$, the algebras $D_{L_\mathfrak{p},x} := K_\mathfrak{p} \otimes_K D_{L,x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$.

Our setting

$$\begin{array}{ccc} Y & & \mathfrak{q}_1 \dots \mathfrak{q}_{m_\mathfrak{p}} \\ \downarrow \pi & & \diagdown \mid \diagup \\ X & & \mathfrak{p} \end{array}$$

π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

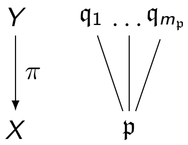
For $x \in K^\times$, consider the algebra

$$D_{L,x} := L[T;\Phi]/(T^r - x)$$

and for all $\mathfrak{p} \in X$, the algebras $D_{L_\mathfrak{p},x} := K_\mathfrak{p} \otimes_K D_{L,x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$.

- ☐ principal divisors associated to $f \in D_{L,x}$
  $\rightsquigarrow$ need to define a valuation
- ☐ Riemann–Roch spaces of $D_{L,x}$
- ☐ a Riemann–Roch theorem
- ☐ equivalent of "evaluate at a rational point"

Our setting



π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

For $x \in K^\times$, consider the algebra

$$D_{L,x} := L[T;\Phi]/(T^r - x)$$

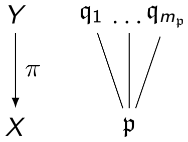
and for all $\mathfrak{p} \in X$, the algebras $D_{L_\mathfrak{p},x} := K_\mathfrak{p} \otimes_K D_{L,x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$.

Define the valuation map $w_{\mathfrak{q}_j,x} : D_{L_\mathfrak{p},x} \to \frac{1}{r}\mathbb{Z} \sqcup \{\infty\}_{(1 \le j \le m_\mathfrak{p})}$: for $f = f_0 + f_1 T + \cdots + f_{r-1} T^{r-1}$,

$$w_{\mathfrak{q},x}(f) = \min_{0 \le i < r} \left(\frac{v_\mathfrak{q}(f_i)}{e_\mathfrak{q}} + i \cdot \frac{v_\mathfrak{p}(x)}{r} \right),$$

where $e_\mathfrak{q}$ denotes the ramification index of $\mathfrak{q}$.

Our setting



π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

For $x \in K^\times$, consider the algebra

$$D_{L,x} := L[T;\Phi]/(T^r - x)$$

and for all $\mathfrak{p} \in X$, the algebras $D_{L_\mathfrak{p},x} := K_\mathfrak{p} \otimes_K D_{L,x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$.

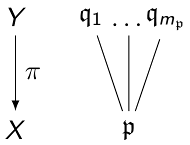
Define the valuation map $w_{\mathfrak{q}_j,x} : D_{L_\mathfrak{p},x} \to \frac{1}{r}\mathbb{Z} \sqcup \{\infty\}_{(1 \le j \le m_\mathfrak{p})}$: for $f = f_0 + f_1 T + \cdots + f_{r-1} T^{r-1}$,

$$w_{\mathfrak{q},x}(f) = \min_{0 \le i < r} \left(\frac{v_\mathfrak{q}(f_i)}{e_\mathfrak{q}} + i \cdot \frac{v_\mathfrak{p}(x)}{r} \right),$$

where $e_\mathfrak{q}$ denotes the ramification index of $\mathfrak{q}$.

$$\Lambda_{L_\mathfrak{p},x} := \{ f \in D_{L_\mathfrak{p},x} \mid w_{\mathfrak{q}_j,x}(f) \ge 0 \}$$

Our setting



π a Galois cover with cyclic Galois group of order r

$L := k(Y)$ the fields of functions of Y, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

For $x \in K^\times$, consider the algebra

$$D_{L,x} := L[T;\Phi]/(T^r - x)$$

and for all $\mathfrak{p} \in X$, the algebras $D_{L_\mathfrak{p},x} := K_\mathfrak{p} \otimes_K D_{L,x} = L_\mathfrak{p}[T;\Phi]/(T^r - x)$.

Define the valuation map $w_{\mathfrak{q}_j,x} : D_{L_\mathfrak{p},x} \to \frac{1}{r}\mathbb{Z} \sqcup \{\infty\}_{(1 \le j \le m_\mathfrak{p})}$: for $f = f_0 + f_1 T + \cdots + f_{r-1}T^{r-1}$,

$$w_{\mathfrak{q},x}(f) = \min_{0 \le i < r} \left(\frac{v_\mathfrak{q}(f_i)}{e_\mathfrak{q}} + i \cdot \frac{v_\mathfrak{p}(x)}{r} \right),$$

where $e_\mathfrak{q}$ denotes the ramification index of $\mathfrak{q}$.

$$\Lambda_{L_\mathfrak{p},x} := \{ f \in D_{L_\mathfrak{p},x} \mid w_{\mathfrak{q}_j,x}(f) \ge 0 \}$$

For $\mathfrak{p} \in X$, $e_\mathfrak{p} w_{\mathfrak{q},x}(f) \in \frac{1}{b_\mathfrak{p}}\mathbb{Z}$ where $b_\mathfrak{p}$ is the denominator of $\rho_\mathfrak{p} = \frac{e_\mathfrak{p} \cdot v_\mathfrak{p}(x)}{r}$ after reduction

Divisors and Riemann–Roch spaces over Ore polynomial rings

Definition (Riemann–Roch spaces of $D_{L,x}$)

Let $E = \sum_{\mathfrak{q} \in Y} n_{\mathfrak{q}} \mathfrak{q} \in Div_{\mathbb{Q}}(Y) := Div\,(Y) \otimes \mathbb{Q}$, *with* $n_{\mathfrak{q}} \in \frac{1}{b_{\mathfrak{p}}}\mathbb{Z}$ *where* $\mathfrak{p} = \pi(\mathfrak{q})$.
Define the Riemann–Roch space of $D_{L,x}$ *associated with* E *as*

$$\Lambda_{L,x}(E) := \{\, f \in D_{L,x} \mid e_{\mathfrak{q}} w_{\mathfrak{q},x}(f) + n_{\mathfrak{q}} \geq 0 \text{ for all } \mathfrak{q} \in Y \,\}.$$

Divisors and Riemann–Roch spaces over Ore polynomial rings

Definition (Riemann–Roch spaces of $D_{L,x}$)

Let $E = \sum_{\mathfrak{q}\in Y} n_{\mathfrak{q}}\mathfrak{q} \in Div_{\mathbb{Q}}(Y) := Div\,(Y) \otimes \mathbb{Q}$, *with* $n_{\mathfrak{q}} \in \frac{1}{b_{\mathfrak{p}}}\mathbb{Z}$ *where* $\mathfrak{p} = \pi(\mathfrak{q})$.
Define the Riemann–Roch space of $D_{L,x}$ *associated with* E *as*

$$\Lambda_{L,x}(E) := \{\, f \in D_{L,x} \mid e_{\mathfrak{q}} w_{\mathfrak{q},x}(f) + n_{\mathfrak{q}} \geq 0 \text{ for all } \mathfrak{q} \in Y \,\}.$$

$\Rightarrow \Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i)\cdot T^i$, where $E_i := \sum_{\mathfrak{q}\in Y} \lfloor n_{\mathfrak{q}} + i\cdot\rho_{\pi(\mathfrak{q})}\rfloor \mathfrak{q} \in \mathrm{Div}(Y) \qquad (0 \leq i < r)$.

Divisors and Riemann–Roch spaces over Ore polynomial rings

Definition (Riemann–Roch spaces of $D_{L,x}$)

Let $E = \sum_{\mathfrak{q}\in Y} n_\mathfrak{q} \mathfrak{q} \in Div_\mathbb{Q}(Y) := Div\,(Y) \otimes \mathbb{Q}$, with $n_\mathfrak{q} \in \frac{1}{b_\mathfrak{p}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$.
Define the Riemann–Roch space of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{\, f \in D_{L,x} \mid e_\mathfrak{q} w_{\mathfrak{q},x}(f) + n_\mathfrak{q} \geq 0 \text{ for all } \mathfrak{q} \in Y \,\}.$$

$\Rightarrow \Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i) \cdot T^i$, where $E_i := \sum_{\mathfrak{q}\in Y} \lfloor n_\mathfrak{q} + i \cdot \rho_{\pi(\mathfrak{q})} \rfloor \mathfrak{q} \in \mathrm{Div}(Y) \qquad (0 \leq i < r)$.

Lemma: We have $\sum_{i=0}^{r-1} \deg_Y(E_i) = r \cdot \deg_Y(E) - \frac{r^2}{2} \sum_{\mathfrak{p}\in X} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p}\, e_\mathfrak{p}} \deg_X(\mathfrak{p})$.

Divisors and Riemann–Roch spaces over Ore polynomial rings

Definition (Riemann–Roch spaces of $D_{L,x}$)

Let $E = \sum_{\mathfrak{q}\in Y} n_\mathfrak{q}\mathfrak{q} \in Div_{\mathbb{Q}}(Y) := Div\,(Y)\otimes\mathbb{Q}$, with $n_\mathfrak{q} \in \frac{1}{b_\mathfrak{p}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$.
Define the Riemann–Roch space of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{\, f \in D_{L,x} \mid e_\mathfrak{q} w_{\mathfrak{q},x}(f) + n_\mathfrak{q} \geq 0 \text{ for all } \mathfrak{q}\in Y \,\}.$$

$\Rightarrow \Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i)\cdot T^i$, where $E_i := \sum_{\mathfrak{q}\in Y} \lfloor n_\mathfrak{q} + i\cdot\rho_{\pi(\mathfrak{q})}\rfloor \mathfrak{q} \in \mathrm{Div}(Y)$ $\quad (0\leq i<r)$.

Lemma: We have $\sum_{i=0}^{r-1} \deg_Y(E_i) = r\cdot\deg_Y(E) - \frac{r^2}{2}\sum_{\mathfrak{p}\in X}\frac{b_\mathfrak{p}-1}{b_\mathfrak{p} e_\mathfrak{p}}\deg_X(\mathfrak{p})$.

Riemann's inequality for $\Lambda_{L,x}(E)$

For a divisor $E = \sum_{\mathfrak{q}\in Y} n_\mathfrak{q}\mathfrak{q} \in \mathrm{Div}_{\mathbb{Q}}(Y)$ the space $\Lambda_{L,x}(E)$ is finite dimensional over k and

$$\dim_k \Lambda_{L,x}(E) \geq r\cdot\deg_Y(E) - r\cdot(g_Y-1) - \frac{r^2}{2}\sum_{\mathfrak{p}\in X}\frac{b_\mathfrak{p}-1}{b_\mathfrak{p} e_\mathfrak{p}}\deg_X(\mathfrak{p}).$$

Code's construction

Let $\mathfrak{p} \in X$ rational, $t_\mathfrak{p}$ a uniformizer $(K_\mathfrak{p} \simeq k((t)))$, $x \in K^\times$

Code's construction

Let $\mathfrak{p} \in X$ rational, $t_{\mathfrak{p}}$ a uniformizer $(K_{\mathfrak{p}} \simeq k((t)))$, $x \in K^{\times}$

if x is a nonzero norm in $L_{\mathfrak{p}}/K_{\mathfrak{p}}$, more precisely $\exists u_{\mathfrak{p}} = (u_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in L_{\mathfrak{p}}^{\times}$ s.t. $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(u_{\mathfrak{q}})$ and $\forall \mathfrak{q},\ v_{\mathfrak{p}}(u_{\mathfrak{q}}) = v$, then

$$\begin{array}{rccc} \varepsilon_{\mathfrak{p}}: & \Lambda_{L_{\mathfrak{p}},x} & \xrightarrow{\simeq} & \mathrm{End}_{\mathcal{O}_{K_{\mathfrak{p}}}}(\mathcal{O}_{L_{\mathfrak{p}}}) \\ & f & \mapsto & f(u_{\mathfrak{p}}\Phi). \end{array}$$

Code's construction

Let $\mathfrak{p} \in X$ rational, $t_{\mathfrak{p}}$ a uniformizer $(K_{\mathfrak{p}} \simeq k((t)))$, $x \in K^{\times}$

if x is a nonzero norm in $L_{\mathfrak{p}}/K_{\mathfrak{p}}$, more precisely $\exists u_{\mathfrak{p}} = (u_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in L_{\mathfrak{p}}^{\times}$ s.t. $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(u_{\mathfrak{q}})$ and $\forall \mathfrak{q}$, $v_{\mathfrak{p}}(u_{\mathfrak{q}}) = v$, then

$$\begin{array}{rcccccl} \overline{\varepsilon}_{\mathfrak{p}} : & \Lambda_{L_{\mathfrak{p}},x} & \xrightarrow{\simeq} & \mathrm{End}_{\mathcal{O}_{K_{\mathfrak{p}}}}(\mathcal{O}_{L_{\mathfrak{p}}}) & \xrightarrow{red} & \mathrm{End}_k(\mathcal{O}_{L_{\mathfrak{p}}}/t_{\mathfrak{p}}\mathcal{O}_{L_{\mathfrak{p}}}) =: \mathrm{End}_k(V_{\mathfrak{p}}) \\ & f & \mapsto & f(u_{\mathfrak{p}}\Phi) & \mapsto & f(u_{\mathfrak{p}}\Phi) \mod t_{\mathfrak{p}} \end{array}$$

Code's construction

Let $\mathfrak{p} \in X$ rational, $t_\mathfrak{p}$ a uniformizer $(K_\mathfrak{p} \simeq k((t)))$, $x \in K^\times$

if x is a nonzero norm in $L_\mathfrak{p}/K_\mathfrak{p}$, more precisely $\exists u_\mathfrak{p} = (u_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}} \in L_\mathfrak{p}^\times$ s.t. $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q})$ and $\forall \mathfrak{q},\ v_\mathfrak{p}(u_\mathfrak{q}) = v$, then

$$\begin{array}{rcccccl} \overline{\varepsilon}_\mathfrak{p} : & \Lambda_{L_\mathfrak{p},x} & \xrightarrow{\simeq} & \mathrm{End}_{\mathcal{O}_{K_\mathfrak{p}}}(\mathcal{O}_{L_\mathfrak{p}}) & \xrightarrow{red} & \mathrm{End}_k(\mathcal{O}_{L_\mathfrak{p}}/t_\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}}) =: \mathrm{End}_k(V_\mathfrak{p}) \\ & f & \mapsto & f(u_\mathfrak{p}\Phi) & \mapsto & f(u_\mathfrak{p}\Phi) \mod t_\mathfrak{p} \end{array}$$

if $\mathfrak{p} \notin \pi(\mathrm{supp}(E)) \Rightarrow \Lambda_{L_\mathfrak{p},x}(E) \subseteq \Lambda_{L_\mathfrak{p},x}$

Code's construction

Let $\mathfrak{p} \in X$ rational, $t_\mathfrak{p}$ a uniformizer $(K_\mathfrak{p} \simeq k((t)))$, $x \in K^\times$

if x is a nonzero norm in $L_\mathfrak{p}/K_\mathfrak{p}$, more precisely $\exists u_\mathfrak{p} = (u_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}} \in L_\mathfrak{p}^\times$ s.t. $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q})$ and $\forall \mathfrak{q},\ v_\mathfrak{p}(u_\mathfrak{q}) = v$, then

$$\begin{array}{rcccccl} \bar{\varepsilon}_\mathfrak{p} : & \Lambda_{L_\mathfrak{p},x} & \xrightarrow{\simeq} & \mathrm{End}_{\mathcal{O}_{K_\mathfrak{p}}}(\mathcal{O}_{L_\mathfrak{p}}) & \xrightarrow{red} & \mathrm{End}_k(\mathcal{O}_{L_\mathfrak{p}}/t_\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}}) =: \mathrm{End}_k(V_\mathfrak{p}) \\ & f & \mapsto & f(u_\mathfrak{p}\Phi) & \mapsto & f(u_\mathfrak{p}\Phi) \mod t_\mathfrak{p} \end{array}$$

if $\mathfrak{p} \notin \pi(\mathrm{supp}(E)) \Rightarrow \Lambda_{L_\mathfrak{p},x}(E) \subseteq \Lambda_{L_\mathfrak{p},x}$

Linearized Algebraic Geometry codes (B., Caruso, 2023)

Let $E = \sum_{\mathfrak{q}\in Y} n_\mathfrak{q}\mathfrak{q} \in \mathrm{Div}_\mathbb{Q}(Y)$. Chose $x \in K$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ rational places on X such that the hypotheses hold. Consider

$$\begin{array}{rcccl} \alpha : & \Lambda_{L,x}(E) & \longrightarrow & \prod_{i=1}^s \mathrm{End}_k(V_{\mathfrak{p}_i}) \\ & f & \mapsto & \left(\bar{\varepsilon}_{\mathfrak{p}_i}(f)\right)_{1\le i\le s}. \end{array}$$

The code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ is defined as the image of α.

Code's parameters

We study the parameters of the k-linear code $\mathcal{C}$ in $\prod_{i=1}^{s} \mathrm{End}_k(V_{\mathfrak{p}_i})$.

Code's parameters

We study the parameters of the k-linear code $\mathcal{C}$ in $\prod_{i=1}^{s} \mathrm{End}_k(V_{\mathfrak{p}_i})$.

The length is $n = sr^2$ $(\dim_k V_{\mathfrak{p}_i} = r)$

Code's parameters

We study the parameters of the k-linear code $\mathcal{C}$ in $\prod_{i=1}^{s} \mathrm{End}_k(V_{\mathfrak{p}_i})$.

The length is $n = sr^2$ $(\dim_k V_{\mathfrak{p}_i} = r)$

Theorem (B., Caruso, 2023)

Assume $\deg_Y(E) < sr$. Assume the previous hypotheses and that $D_{L,x}$ contains no nonzero divisors. Then, the dimension δ and the minimum distance d of $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ satisfy

$$\delta \geq r \cdot \deg_Y(E) - r \cdot (g_Y - 1) - \frac{r^2}{2} \sum_{\mathfrak{p} \in X} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}} e_{\mathfrak{p}}} \deg_X(\mathfrak{p}),$$

$$d \geq sr - \deg_Y(E).$$

Code's parameters

We study the parameters of the k-linear code $\mathcal{C}$ in $\prod_{i=1}^{s} \mathrm{End}_k(V_{\mathfrak{p}_i})$.

The length is $n = sr^2$ $(\dim_k V_{\mathfrak{p}_i} = r)$

Theorem (B., Caruso, 2023)

Assume $\deg_Y(E) < sr$. Assume the previous hypotheses and that $D_{L,x}$ contains no nonzero divisors. Then, the dimension δ and the minimum distance d of $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ satisfy

$$\delta \geq r \cdot \deg_Y(E) - r \cdot (g_Y - 1) - \frac{r^2}{2} \sum_{\mathfrak{p} \in X} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}} e_{\mathfrak{p}}} \deg_X(\mathfrak{p}),$$

$$d \geq sr - \deg_Y(E).$$

Singleton bound: $rd + \delta \leq n + r$

We have: $rd + \delta \geq n + r - \left(r \cdot g_Y + \frac{r^2}{2} \sum_{\mathfrak{p} \in X} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}} e_{\mathfrak{p}}} \deg_X(\mathfrak{p}) \right)$

The case of isotrivial covers

$$\begin{array}{c} \ell \\ \Big\downarrow \Phi \\ k \end{array}$$

Let ℓ be a finite cyclic extension of k of order r.

The case of isotrivial covers

$$\ell \xrightarrow{\ \Phi\ } k$$

Let ℓ be a finite cyclic extension of k of order r.
Take $Y = \operatorname{Spec} \ell \times_{\operatorname{Spec} k} X$ (cyclic Galois cover of X of degree r)

The case of isotrivial covers

$$\begin{array}{c} \ell \\ \downarrow \Phi \\ k \end{array}$$

Let ℓ be a finite cyclic extension of k of order r.
Take $Y = \text{Spec } \ell \times_{\text{Spec } k} X$ (cyclic Galois cover of X of degree r)

Residue field of any place of Y is a ℓ-algebra $\Rightarrow$ the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ is ℓ-linear

The case of isotrivial covers

$$\begin{array}{c} \ell \\ \big\downarrow \Phi \\ k \end{array}$$

Let ℓ be a finite cyclic extension of k of order r.
Take $Y = \mathrm{Spec}\ \ell \times_{\mathrm{Spec}\ k} X$ (cyclic Galois cover of X of degree r)

Residue field of any place of Y is a ℓ-algebra $\Rightarrow$ the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ is ℓ-linear

ℓ-parameters of the code

For the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ with $x, \mathfrak{p}_1, \ldots, \mathfrak{p}_s, E$ satisfying the hypotheses, we have

- $n_\ell = sr$,
- $\delta_\ell \geq \deg_Y(E) - r{\cdot}(g_X - 1) - \frac{r}{2} \sum_{\mathfrak{p} \in X} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p}} \deg_X(\mathfrak{p})$,
- $d \geq sr - \deg_Y(E)$.

The case of isotrivial covers

$$\ell \xrightarrow{\Phi} k$$

Let ℓ be a finite cyclic extension of k of order r.
Take $Y = \operatorname{Spec} \ell \times_{\operatorname{Spec} k} X$ (cyclic Galois cover of X of degree r)

Residue field of any place of Y is a ℓ-algebra $\Rightarrow$ the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ is ℓ-linear

ℓ-parameters of the code

For the code $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ with $x, \mathfrak{p}_1, \ldots, \mathfrak{p}_s, E$ satisfying the hypotheses, we have

- $n_\ell = sr$,
- $\delta_\ell \geq \deg_Y(E) - r\cdot(g_X - 1) - \frac{r}{2} \sum_{\mathfrak{p} \in X} \frac{b_\mathfrak{p} - 1}{b_\mathfrak{p}} \deg_X(\mathfrak{p})$,
- $d \geq sr - \deg_Y(E)$.

$X = \mathbb{P}^1_k$, $Y = \mathbb{P}^1_\ell$, $E = \frac{\delta}{r} \cdot \infty \in \operatorname{Div}_\mathbb{Q}(Y)$ $\rightsquigarrow$ linearized Reed–Solomon codes!
Our lower bounds $\Rightarrow$ MSRD codes

Further questions

- linearized AG codes in the general framework of central simple algebras

Further questions

- linearized AG codes in the general framework of central simple algebras
- decoding problem
  (decoding algorithm for linearized Reed–Solomon codes ✔)

Further questions

- linearized AG codes in the general framework of central simple algebras
- decoding problem
  (decoding algorithm for linearized Reed–Solomon codes ✔)
- duality theorem for the codes $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$
  (require to develop the theory of differential forms and residues in our framework)

Further questions

- linearized AG codes in the general framework of central simple algebras
- decoding problem
  (decoding algorithm for linearized Reed–Solomon codes ✔)
- duality theorem for the codes $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$
  (require to develop the theory of differential forms and residues in our framework)

AGC²T '17 AGC²T '19

AGC²T '21 AGC²T '23

Merci de votre attention !

Questions?
elena.berardini@math.u-bordeaux.fr

Remarks on the hypotheses

(H1) the algebra $D_{L,x}$ has no nonzero zero divisor

(H2) for all places $\mathfrak{q}$ above $\mathfrak{p}$, there exists $u_{\mathfrak{q}} \in L_{\mathfrak{q}}^{\times}$ such that $v_{\mathfrak{q}}(u_{\mathfrak{q}}) = \frac{e_{\mathfrak{p}}}{r} \cdot v_{\mathfrak{p}}(x)$ and

$$x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(u_{\mathfrak{q}})$$

Lemma

The hypothesis (H1) holds as soon as there exists a place $\mathfrak{p} \in X$ which is inert in Y and at which $v_{\mathfrak{p}}(x)$ is coprime with r.

Lemma

We assume that k is a finite field. Let $\mathfrak{p}$ be a place of X. If $\mathfrak{p}$ is unramified in Y and $v_{\mathfrak{p}}(x)$ is divisible by r, then (H2) holds.