

ALGEBRAIC GEOMETRY CODES IN THE SUM-RANK METRIC

Elena Berardini and X.Caruso

CNRS, Institut de Mathématiques de Bordeaux



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

Table of Contents

- 1 Codes in the sum-rank metric
- 2 Riemann–Roch spaces over Ore polynomial rings
- 3 Linearized Algebraic Geometry codes
- 4 Conclusion and further works

Linear codes and codes in the Hamming metric

k a field (keep in mind $k = \mathbb{F}_q$), \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 (keep in mind $k = \mathbb{F}_q$), \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

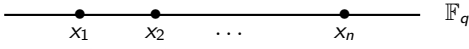
k a field (keep in mind $k = \mathbb{F}_q$), \mathcal{H} a k -linear vector space endowed with a metric

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:



The diagram shows a horizontal line representing the field \mathbb{F}_q . On this line, there are points labeled x_1 , x_2 , an ellipsis \dots , and x_n . Arrows point from each of these points down to the corresponding element in the vector $(P(x_1), P(x_2), \dots, P(x_n))$ within the set definition of $RS_\delta(\mathbf{x})$.

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

Linear codes and codes in the Hamming metric

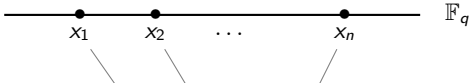
k a field (keep in mind $k = \mathbb{F}_q$), \mathcal{H} a k -linear vector space endowed with a metric

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:



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

✓ **Optimal parameters:** $\delta + d = n + 1$

(Singleton bound: $\delta + d \leq n + 1$)

⚠ **Drawback:** $n \leq q$

Linear codes and codes in the Hamming metric

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

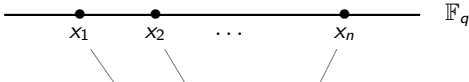
Linear code \mathcal{C} : k -vector subspace of \mathcal{H}

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

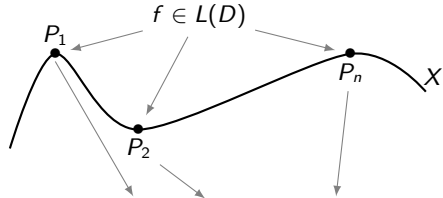
Codes in the Hamming metric: k -vector subspaces of k^n endowed with $d(x, y) := \#\{i \mid x_i \neq y_i\}$

Reed–Solomon (RS) codes:

Algebraic Geometry (AG) codes:



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



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

✓ **Optimal parameters:** $\delta + d = n + 1$

(Singleton bound: $\delta + d \leq n + 1$)

⚠ **Drawback:** $n \leq q$

Linear codes and codes in the Hamming metric

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

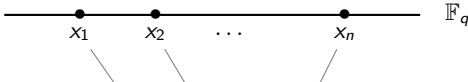
Linear code \mathcal{C} : k -vector subspace of \mathcal{H}

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:

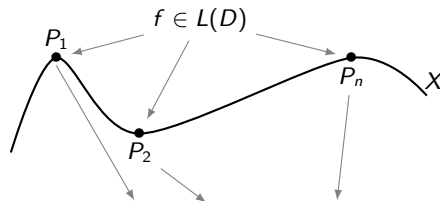
Algebraic Geometry (AG) codes:



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

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

⚠ **Drawback:** $n \leq q$



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

✓ **Good parameters:** $n + 1 - g \leq d + \delta \leq n + 1$
✓ **Longer codes**

General definitions

$\underline{V} = (V_1, \dots, V_s)$ s-uple of k -vector spaces

$(n_i = \dim_k V_i)$

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

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

General definitions

$\underline{V} = (V_1, \dots, V_s)$ s-uple of **k-vector spaces**

$(n_i = \dim_k V_i)$

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

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

Definition

Let $\underline{\varphi} = (\varphi_1, \dots, \varphi_s) \in \mathcal{H}$. 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

$\underline{V} = (V_1, \dots, V_s)$ s-uple of **k-vector spaces**

$(n_i = \dim_k V_i)$

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

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

Definition

Let $\underline{\varphi} = (\varphi_1, \dots, \varphi_s) \in \mathcal{H}$. 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 $\text{End}_k(\underline{V})$ endowed with the sum-rank distance.

General definitions

$\underline{V} = (V_1, \dots, V_s)$ s-uple of **k-vector spaces**

$(n_i = \dim_k V_i)$

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

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

Definition

Let $\underline{\varphi} = (\varphi_1, \dots, \varphi_s) \in \mathcal{H}$. 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 $\text{End}_k(\underline{V})$ 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

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

General definitions

$\underline{V} = (V_1, \dots, V_s)$ s-uple of **k-vector spaces**

$(n_i = \dim_k V_i)$

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

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

Definition

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

The **sum-rank distance** between $\underline{\varphi}, \underline{\psi} \in \mathcal{H}$ is

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

A **code \mathcal{C} in the sum-rank metric** is a k -linear subspace of $\text{End}_k(\underline{V})$ 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

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

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

Particular case and Singleton bound

ℓ = finite extension of k of degree r

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

Particular case and Singleton bound

ℓ = finite extension of k of degree r

$\underline{V} = (V_1, \dots, V_s)$, s -uple of ℓ -vector spaces ($\dim_k V_i = r$) $\rightsquigarrow \mathcal{H} = \text{End}_k(\underline{V})$ 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:

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

Particular case and Singleton bound

ℓ = finite extension of k of degree r

$\underline{V} = (V_1, \dots, V_s)$, s -uple of ℓ -vector spaces ($\dim_k V_i = r$) $\rightsquigarrow \mathcal{H} = \text{End}_k(\underline{V})$ 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:

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

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 (Martínez-Peñas, 2018)

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{array}{ccc} \text{ev} : & \ell[T; \Phi] & \rightarrow \text{End}_k(\ell) \\ & P & \mapsto P(\Phi). \end{array}$$

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

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

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

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

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

$$\begin{aligned} \text{ev}_c : \quad \ell[T; \Phi] &\rightarrow \text{End}_k(\ell) \\ P &\mapsto P(c\Phi). \end{aligned}$$

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

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

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

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

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

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

$$\begin{aligned} \text{ev}_{\underline{c}} : \quad \ell[T; \Phi] &\rightarrow \text{End}_k(\ell)^s \\ P &\mapsto (P(c_1\Phi), \dots, P(c_s\Phi)). \end{aligned}$$

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

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

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

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

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

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

$$\begin{aligned} \text{ev}_{\underline{c}} : \quad \ell[T; \Phi] &\rightarrow \text{End}_k(\ell)^s \\ P &\mapsto (P(c_1\Phi), \dots, P(c_s\Phi)). \end{aligned}$$

Definition (Linearized Reed–Solomon codes)

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

and $\delta \in \mathbb{Z}$

define

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

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

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

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

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

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

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

$$\begin{aligned} \text{ev}_{\underline{c}} : \quad \ell[T; \Phi] &\rightarrow \text{End}_k(\ell)^s \\ P &\mapsto (P(c_1\Phi), \dots, P(c_s\Phi)). \end{aligned}$$

Definition (Linearized Reed–Solomon codes)

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 $\delta \leq rs$ define

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

length = rs dimension = δ minimum distance = $rs - \delta + 1$ \Rightarrow **MSRD** codes

Motivation and idea

Definition (Linearized Reed–Solomon codes)

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 $\mathbb{Z} \ni \delta \leq rs$ define

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

$\Rightarrow s \leq \text{Card}(k)$. Think about $k = \mathbb{F}_q \rightsquigarrow$ same problem as Reed–Solomon codes

Motivation and idea

Definition (Linearized Reed–Solomon codes)

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 $\mathbb{Z} \ni \delta \leq rs$ define

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

$\Rightarrow s \leq \text{Card}(k)$. Think about $k = \mathbb{F}_q \rightsquigarrow$ same problem as Reed–Solomon codes

More in general

Theorem (Byrne, Gluesing–Luerssen, Ravagnani, 2021)

Let $\mathcal{C} \subseteq \text{End}_k(\ell)^s$ be a MSRD code of minimum distance $\leq r + 2$. Then, $s \leq \text{Card}(k)$.

Motivation and idea

Definition (Linearized Reed–Solomon codes)

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 $\mathbb{Z} \ni \delta \leq rs$ define

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

$\Rightarrow s \leq \text{Card}(k)$. Think about $k = \mathbb{F}_q \rightsquigarrow$ same problem as Reed–Solomon codes

More in general

Theorem (Byrne, Gluesing–Luerssen, Ravagnani, 2021)

Let $\mathcal{C} \subseteq \text{End}_k(\ell)^s$ be a MSRD code of minimum distance $\leq r + 2$. Then, $s \leq \text{Card}(k)$.

As in the Hamming case, we can try to overcome the problem using algebraic curves

Motivation and idea

Definition (Linearized Reed–Solomon codes)

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 $\mathbb{Z} \ni \delta \leq rs$ define

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

$\Rightarrow s \leq \text{Card}(k)$. Think about $k = \mathbb{F}_q \rightsquigarrow$ same problem as Reed–Solomon codes

More in general

Theorem (Byrne, Gluesing–Luerssen, Ravagnani, 2021)

Let $\mathcal{C} \subseteq \text{End}_k(\ell)^s$ be a MSRD code of minimum distance $\leq r + 2$. Then, $s \leq \text{Card}(k)$.

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

Notations

Consider a smooth projective irreducible algebraic **curve** X of genus g_X defined over k

$K = k(X)$ - **function field** of X

X^* - set of **places** (or, equivalently, closed points) of X

for $\mathfrak{p} \in X^*$, set

$\mathcal{O}_{\mathfrak{p}}$ - the **ring of integers** of \mathfrak{p}

$k_{\mathfrak{p}}$ - the **residue class field** of \mathfrak{p}

$\deg_X(\mathfrak{p})$ - the **degree of \mathfrak{p}** , the degree of the extension $k_{\mathfrak{p}}/k$

$K_{\mathfrak{p}}$ - the **completion** of K at \mathfrak{p} , equipped with the \mathfrak{p} -adic valuation $v_{\mathfrak{p}}$

Divisors and Riemann–Roch spaces: classical theory

Definition

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 $\text{Div}(X)$.

$D \in \text{Div}(X)$ 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

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 $\text{Div}(X)$.

$D \in \text{Div}(X)$ 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

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 $\text{Div}(X)$.

$D \in \text{Div}(X)$ 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 $D \in \text{Div}(X)$ we have

$$\dim_k L_X(D) = \deg_X(D) + 1 - g_X + \dim_k L_X(K_X - D),$$

$= 0$ when $\deg_X(D) > 2g_X - 2$.

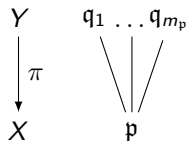
Our setting

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

π a Galois cover with cyclic Galois group of order r

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

Our setting

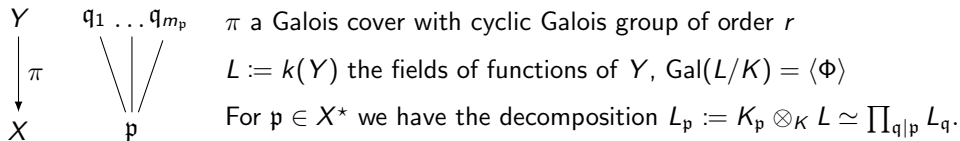


π a Galois cover with cyclic Galois group of order r

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

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

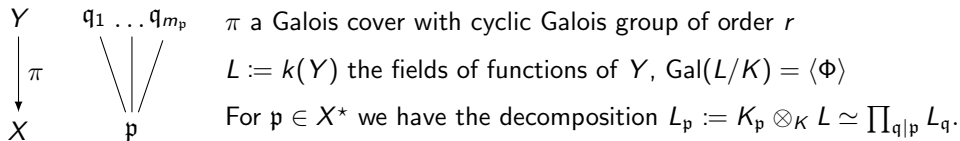


For $x \in K^\times$, consider the algebra

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

and for all $\mathfrak{p} \in X^\star$, 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



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

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

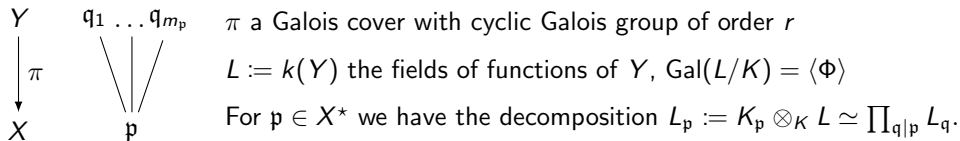
and for all $\mathfrak{p} \in X^*$, the algebras $D_{L_{\mathfrak{p}},x} := K_{\mathfrak{p}} \otimes_K D_{L,x} = L_{\mathfrak{p}}[T; \Phi]/(T^r - x)$.

Define $w_{q_j,x} : D_{L_{\mathfrak{p}},x} \rightarrow \frac{1}{r}\mathbb{Z} \sqcup \{\infty\} (1 \leq j \leq m_{\mathfrak{p}})$: for $f = f_0 + f_1 T + \cdots + f_{r-1} T^{r-1}$,

$$w_{q,x}(f) = \min_{0 \leq i < r} \left(\frac{v_q(f_i)}{e_q} + i \cdot \frac{v_p(x)}{r} \right),$$

where e_q denotes the ramification index of q .

Our setting



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

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

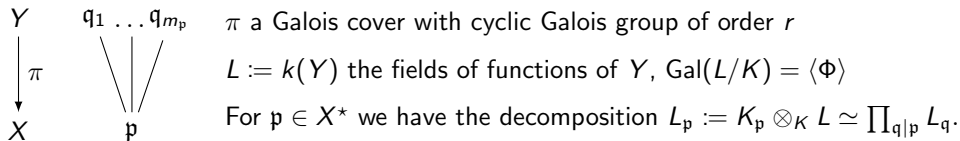
and for all $\mathfrak{p} \in X^*$, the algebras $D_{L_{\mathfrak{p}},x} := K_{\mathfrak{p}} \otimes_K D_{L,x} = L_{\mathfrak{p}}[T; \Phi]/(T^r - x)$.

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

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

where $e_{\mathfrak{q}}$ denotes the ramification index of \mathfrak{q} . $\triangle!$ $w_{\mathfrak{q},x}(fg) \geq w_{\mathfrak{q},x}(f) + w_{\mathfrak{q},x}(g)$.

Our setting



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

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

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

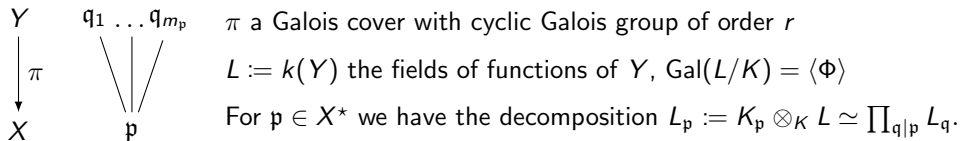
Define $w_{q_j,x} : D_{L_p,x} \rightarrow \frac{1}{r}\mathbb{Z} \sqcup \{\infty\} (1 \leq j \leq m_p)$: for $f = f_0 + f_1 T + \dots + f_{r-1} T^{r-1}$,

$$w_{q,x}(f) = \min_{0 \leq i < r} \left(\frac{v_q(f_i)}{e_q} + i \cdot \frac{v_p(x)}{r} \right),$$

where e_q denotes the ramification index of q . $\triangle! \quad w_{q,x}(fg) \geq w_{q,x}(f) + w_{q,x}(g)$.

$$\Lambda_{L_p,x} := \{f \in D_{L_p,x} \mid w_{q_j,x}(f) \geq 0\}$$

Our setting



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

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

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

Define $w_{q_j,x} : D_{L_p,x} \rightarrow \frac{1}{r}\mathbb{Z} \sqcup \{\infty\} (1 \leq j \leq m_p)$: for $f = f_0 + f_1 T + \dots + f_{r-1} T^{r-1}$,

$$w_{q,x}(f) = \min_{0 \leq i < r} \left(\frac{v_q(f_i)}{e_q} + i \cdot \frac{v_p(x)}{r} \right),$$

where e_q denotes the ramification index of q . $\triangle!$ $w_{q,x}(fg) \geq w_{q,x}(f) + w_{q,x}(g)$.

$$\Lambda_{L_p,x} := \{f \in D_{L_p,x} \mid w_{q_j,x}(f) \geq 0\}$$

For $p \in X^*$, $e_p w_{q,x}(f) \in \frac{1}{b_p}\mathbb{Z}$ where b_p is the denominator of $\rho_p = \frac{e_p \cdot v_p(x)}{r}$ after reduction

Divisors and Riemann–Roch spaces over Ore polynomial rings

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

Let $E = \sum_{\mathfrak{q} \in Y^*} n_{\mathfrak{q}} \mathfrak{q} \in \text{Div}_{\mathbb{Q}}(Y) := \text{Div}(Y) \otimes \mathbb{Q}$ where, for all \mathfrak{q} , the coefficient $n_{\mathfrak{q}}$ is in $\frac{1}{b_{\mathfrak{p}}} \mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$ is the place below \mathfrak{q} . We 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 $E = \sum_{q \in Y^*} n_q q \in \text{Div}_{\mathbb{Q}}(Y) := \text{Div}(Y) \otimes \mathbb{Q}$ where, for all q , the coefficient n_q is in $\frac{1}{b_p} \mathbb{Z}$ where $p = \pi(q)$ is the place below q . We define the *Riemann–Roch space* of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{ f \in D_{L,x} \mid e_q w_{q,x}(f) + n_q \geq 0 \text{ for all } q \in Y^* \}.$$

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

Divisors and Riemann–Roch spaces over Ore polynomial rings

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

Let $E = \sum_{q \in Y^*} n_q q \in \text{Div}_{\mathbb{Q}}(Y) := \text{Div}(Y) \otimes \mathbb{Q}$ where, for all q , the coefficient n_q is in $\frac{1}{b_p} \mathbb{Z}$ where $p = \pi(q)$ is the place below q . We define the **Riemann–Roch space** of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{ f \in D_{L,x} \mid e_q w_{q,x}(f) + n_q \geq 0 \text{ for all } q \in Y^* \}.$$

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

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

Divisors and Riemann–Roch spaces over Ore polynomial rings

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

Let $E = \sum_{q \in Y^*} n_q q \in \text{Div}_{\mathbb{Q}}(Y) := \text{Div}(Y) \otimes \mathbb{Q}$ where, for all q , the coefficient n_q is in $\frac{1}{b_p} \mathbb{Z}$ where $p = \pi(q)$ is the place below q . We define the **Riemann–Roch space** of $D_{L,x}$ associated with E as

$$\Lambda_{L,x}(E) := \{ f \in D_{L,x} \mid e_q w_{q,x}(f) + n_q \geq 0 \text{ for all } q \in Y^* \}.$$

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

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

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

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

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

Code's construction

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

Code's construction

Let $p \in X^*$ rational, t_p a uniformizer ($K_p \simeq k((t))$), $x \in K^\times$

if x is a nonzero norm in L_p/K_p , more precisely $\exists u_p = (u_q)_{q|p} \in L_p^\times$ s.t. $x = \prod_{q|p} N_{L_q/K_p}(u_q)$, then

$$\varepsilon_p : \begin{array}{ccc} D_{L_p, x} & \xrightarrow{\simeq} & \text{End}_{K_p}(L_p) \\ f & \mapsto & f(u_p \Phi). \end{array}$$

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 $\exists u_{\mathfrak{p}} = (u_q)_{q|\mathfrak{p}} \in L_{\mathfrak{p}}^{\times}$ s.t. $x = \prod_{q|\mathfrak{p}} N_{L_q/K_{\mathfrak{p}}}(u_q)$ and $\forall q, v_{\mathfrak{p}}(u_q) = v$, then

$$\varepsilon_{\mathfrak{p}} : \begin{array}{ccc} D_{L_{\mathfrak{p}}, x} & \xrightarrow{\simeq} & \text{End}_{K_{\mathfrak{p}}}(L_{\mathfrak{p}}) \\ f & \mapsto & f(u_{\mathfrak{p}} \Phi). \end{array}$$

Code's construction

Let $p \in X^*$ rational, t_p a uniformizer ($K_p \simeq k((t))$), $x \in K^\times$

if x is a nonzero norm in L_p/K_p , more precisely $\exists u_p = (u_q)_{q|p} \in L_p^\times$ s.t. $x = \prod_{q|p} N_{L_q/K_p}(u_q)$ and $\forall q, v_p(u_q) = v$, then

$$\varepsilon_p : \begin{array}{ccc} \Lambda_{L_p, x} & \xrightarrow{\simeq} & \text{End}_{\mathcal{O}_{K_p}}(\mathcal{O}_{L_p}) \\ f & \mapsto & f(u_p \Phi). \end{array}$$

Code's construction

Let $p \in X^*$ rational, t_p a uniformizer ($K_p \simeq k((t))$), $x \in K^\times$

if x is a nonzero norm in L_p/K_p , more precisely $\exists u_p = (u_q)_{q|p} \in L_p^\times$ s.t. $x = \prod_{q|p} N_{L_q/K_p}(u_q)$ and $\forall q, v_p(u_q) = v$, then

$$\begin{array}{ccccc} \bar{\varepsilon}_p : & \Lambda_{L_p, x} & \xrightarrow{\simeq} & \text{End}_{\mathcal{O}_{K_p}}(\mathcal{O}_{L_p}) & \xrightarrow{\text{red}} & \text{End}_k(\mathcal{O}_{L_p}/t_p \mathcal{O}_{L_p}) \\ & f & \mapsto & f(u_p \Phi) & \mapsto & f(u_p \Phi) \pmod{t_p}. \end{array}$$

Code's construction

Let $p \in X^*$ rational, t_p a uniformizer ($K_p \simeq k((t))$), $x \in K^\times$

if x is a nonzero norm in L_p/K_p , more precisely $\exists u_p = (u_q)_{q|p} \in L_p^\times$ s.t. $x = \prod_{q|p} N_{L_q/K_p}(u_q)$ and $\forall q, v_p(u_q) = v$, then

$$\begin{array}{ccccc} \bar{\varepsilon}_p : & \Lambda_{L_p, x} & \xrightarrow{\simeq} & \text{End}_{\mathcal{O}_{K_p}}(\mathcal{O}_{L_p}) & \xrightarrow{\text{red}} & \text{End}_k(\mathcal{O}_{L_p}/t_p \mathcal{O}_{L_p}) \\ & f & \mapsto & f(u_p \Phi) & \mapsto & f(u_p \Phi) \pmod{t_p}. \end{array}$$

if $p \notin \pi(\text{supp}(E)) \rightsquigarrow \Lambda_{L_p, x}(E) \subseteq \Lambda_{L_p, x}$

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 $\exists u_{\mathfrak{p}} = (u_q)_{q|\mathfrak{p}} \in L_{\mathfrak{p}}^\times$ s.t. $x = \prod_{q|\mathfrak{p}} N_{L_q/K_{\mathfrak{p}}}(u_q)$ and $\forall q, v_{\mathfrak{p}}(u_q) = v$, then

$$\begin{array}{ccccc} \bar{\varepsilon}_{\mathfrak{p}} : & \Lambda_{L_{\mathfrak{p}},x} & \xrightarrow{\simeq} & \text{End}_{\mathcal{O}_{K_{\mathfrak{p}}}}(\mathcal{O}_{L_{\mathfrak{p}}}) & \xrightarrow{\text{red}} & \text{End}_k(\mathcal{O}_{L_{\mathfrak{p}}}/t_{\mathfrak{p}}\mathcal{O}_{L_{\mathfrak{p}}}) \\ & f & \mapsto & f(u_{\mathfrak{p}}\Phi) & \mapsto & f(u_{\mathfrak{p}}\Phi) \bmod t_{\mathfrak{p}}. \end{array}$$

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

Definition (Linearized Algebraic Geometry codes)

Let $E = \sum_{q \in Y^*} n_q q \in \text{Div}_{\mathbb{Q}}(Y)$. Chose $x \in K$ and $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ rational places on X such that the hypotheses hold. Set $V_{\mathfrak{p}_i} := \mathcal{O}_{L_{\mathfrak{p}_i}}/t_{\mathfrak{p}_i}\mathcal{O}_{L_{\mathfrak{p}_i}}$. Consider

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

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

Code's parameters

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

Code's parameters

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

Its **length** n is the k -dimension of the ambient space : $\dim_k V_{\mathfrak{p}_i} = r \Rightarrow n = sr^2$

Code's parameters

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

Its **length** n is the k -dimension of the ambient space : $\dim_k V_{p_i} = r \Rightarrow n = sr^2$

Theorem (B., Caruso)

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 $\mathcal{C}(x; E; p_1, \dots, p_s)$ satisfy

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

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

Code's parameters

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

Its **length** n is the k -dimension of the ambient space : $\dim_k V_{p_i} = r \Rightarrow n = sr^2$

Theorem (B., Caruso)

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 $\mathcal{C}(x; E; p_1, \dots, p_s)$ satisfy

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

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

Singleton bound:

$$rd + \delta \leq n + r$$

We have:

$$rd + \delta \geq n + r - \left(r \cdot g_Y + \frac{r^2}{2} \sum_{p \in X^*} \frac{b_p - 1}{b_p e_p} \deg_X(p) \right)$$

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,x}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{\varepsilon}_{\mathfrak{p}_i}(f)$.

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{\varepsilon}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{\varepsilon}_i(f)$ for $i \in \{1, \dots, s\}$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{\varepsilon}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{\varepsilon}_i(f)$ for $i \in \{1, \dots, s\}$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

We have $\text{Nrd}(f) \in L_X(E')$ where $\text{Nrd}(f) \in K$ and is defined as the determinant of $g \xrightarrow{\mu_f} gf$

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{e}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{e}_i(f)$ for $i \in \{1, \dots, s\} \Rightarrow \sum_{i=1}^s d_i = \sum_{i=1}^s \dim_k V_{\mathfrak{p}_i} - \text{rk } \bar{e}_{\mathfrak{p}_i}(f) = sr - \omega$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

We have $\text{Nrd}(f) \in L_X(E')$ where $\text{Nrd}(f) \in K$ and is defined as the determinant of $g \xrightarrow{\mu_f} gf$

$$\deg_Y(E') \leq -\sum_{i=1}^s d_i + \sum_{\mathfrak{q} \in Y^*} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \deg_X(\pi(\mathfrak{q})) = \omega - sr + \deg_Y(E).$$

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{e}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{e}_i(f)$ for $i \in \{1, \dots, s\} \Rightarrow \sum_{i=1}^s d_i = \sum_{i=1}^s \dim_k V_{\mathfrak{p}_i} - \text{rk } \bar{e}_{\mathfrak{p}_i}(f) = sr - \omega$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

We have $\text{Nrd}(f) \in L_X(E')$ where $\text{Nrd}(f) \in K$ and is defined as the determinant of $g \xrightarrow{\mu_f} gf$

$$\deg_Y(E') \leq -\sum_{i=1}^s d_i + \sum_{\mathfrak{q} \in Y^*} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \deg_X(\pi(\mathfrak{q})) = \omega - sr + \deg_Y(E).$$

If $\omega < sr - \deg_Y(E) \Rightarrow \text{Nrd}(f) = 0 \Rightarrow \mu_f$ is not injective $\Rightarrow f$ is a nonzero zero divisor in $D_{L,X}$

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{e}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{e}_i(f)$ for $i \in \{1, \dots, s\} \Rightarrow \sum_{i=1}^s d_i = \sum_{i=1}^s \dim_k V_{\mathfrak{p}_i} - \text{rk } \bar{e}_{\mathfrak{p}_i}(f) = sr - \omega$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

We have $\text{Nrd}(f) \in L_X(E')$ where $\text{Nrd}(f) \in K$ and is defined as the determinant of $g \xrightarrow{\mu_f} gf$

$$\deg_Y(E') \leq -\sum_{i=1}^s d_i + \sum_{\mathfrak{q} \in Y^*} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \deg_X(\pi(\mathfrak{q})) = \omega - sr + \deg_Y(E).$$

If $\omega < sr - \deg_Y(E) \Rightarrow \text{Nrd}(f) = 0 \Rightarrow \mu_f$ is not injective $\Rightarrow f$ is a nonzero zero divisor in $D_{L,X}$

In conclusion: $\omega \geq sr - \deg_Y(E)$ ✓

Sketch of the proof

Want: $d \geq sr - \deg_Y(E) + \text{bound on the dimension } \delta$

Let $0 \neq f \in \Lambda_{L,X}(E)$, with $\omega = w_{\text{rk}}(\alpha(f)) = \sum_{i=1}^s \text{rk } \bar{e}_{\mathfrak{p}_i}(f)$.

Let $d_i := \dim_k \ker \bar{e}_i(f)$ for $i \in \{1, \dots, s\} \Rightarrow \sum_{i=1}^s d_i = \sum_{i=1}^s \dim_k V_{\mathfrak{p}_i} - \text{rk } \bar{e}_{\mathfrak{p}_i}(f) = sr - \omega$

and define the divisor $E' := -\sum_{i=1}^s d_i \mathfrak{p}_i + \sum_{\mathfrak{p} \in X^*} \left\lfloor \sum_{\mathfrak{q}|\mathfrak{p}} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \right\rfloor \mathfrak{p} \in \text{Div}(X)$.

We have $\text{Nrd}(f) \in L_X(E')$ where $\text{Nrd}(f) \in K$ and is defined as the determinant of $g \xrightarrow{\mu_f} gf$

$$\deg_Y(E') \leq -\sum_{i=1}^s d_i + \sum_{\mathfrak{q} \in Y^*} \frac{r \cdot n_{\mathfrak{q}}}{e_{\mathfrak{p}} m_{\mathfrak{p}}} \deg_X(\pi(\mathfrak{q})) = \omega - sr + \deg_Y(E).$$

If $\omega < sr - \deg_Y(E) \Rightarrow \text{Nrd}(f) = 0 \Rightarrow \mu_f$ is not injective $\Rightarrow f$ is a nonzero zero divisor in $D_{L,X}$

In conclusion: $\omega \geq sr - \deg_Y(E)$ ✓

Injectivity of the map $\alpha \Rightarrow \delta = \dim_k \Lambda_{L,X}(E) \rightsquigarrow$ lower bound on δ via Riemann's inequality ✓

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 .

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 $Y = \operatorname{Spec} \ell \times_{\operatorname{Spec} k} X$ (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 $Y = \operatorname{Spec} \ell \times_{\operatorname{Spec} k} X$ (cyclic Galois cover of X of degree r)

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

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 $\mathcal{C}(x; E; p_1, \dots, p_s)$ is ℓ -linear

ℓ -parameters of the code

For the code $\mathcal{C}(x; E; p_1, \dots, p_s)$ with x, p_1, \dots, p_s, E satisfying the hypotheses, we have

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

Linearized AG codes over \mathbb{P}^1 are Linearized Reed–Solomon codes

$X = \mathbb{P}_k^1$ and $Y = \mathbb{P}_\ell^1$, both viewed as curves over $\text{Spec } k$, $t =$ the coordinate on X and Y

Linearized AG codes over \mathbb{P}^1 are Linearized Reed–Solomon codes

$X = \mathbb{P}_k^1$ and $Y = \mathbb{P}_\ell^1$, both viewed as curves over $\text{Spec } k$, $t =$ the coordinate on X and Y

Choose the function $x = t \in K^\times = k(t)^\times$. Then

$$b_{\mathfrak{p}} = \begin{cases} r & \text{for } \mathfrak{p} = 0, \infty, \\ 1 & \text{for all other } \mathfrak{p} \in X^\star, \end{cases}$$

$$D_{L,x} = \ell(t)[T; \Phi]/(T^r - t) \simeq \text{Frac}(\ell[T; \Phi])$$

Linearized AG codes over \mathbb{P}^1 are Linearized Reed–Solomon codes

$X = \mathbb{P}_k^1$ and $Y = \mathbb{P}_\ell^1$, both viewed as curves over $\text{Spec } k$, $t =$ the coordinate on X and Y

Choose the function $x = t \in K^\times = k(t)^\times$. Then

$$b_{\mathfrak{p}} = \begin{cases} r & \text{for } \mathfrak{p} = 0, \infty, \\ 1 & \text{for all other } \mathfrak{p} \in X^\star, \end{cases}$$

$$D_{L,x} = \ell(t)[T; \Phi]/(T^r - t) \simeq \text{Frac}(\ell[T; \Phi])$$

Consider the divisor $E = \frac{\delta}{r} \cdot \infty \in \text{Div}_{\mathbb{Q}}(Y)$, $\delta \in \mathbb{N} \rightsquigarrow \Lambda_{L,t}(E) = \ell[T; \Phi]_{\leq \delta}$

Linearized AG codes over \mathbb{P}^1 are Linearized Reed–Solomon codes

$X = \mathbb{P}_k^1$ and $Y = \mathbb{P}_\ell^1$, both viewed as curves over $\text{Spec } k$, $t =$ the coordinate on X and Y

Choose the function $x = t \in K^\times = k(t)^\times$. Then

$$b_{\mathfrak{p}} = \begin{cases} r & \text{for } \mathfrak{p} = 0, \infty, \\ 1 & \text{for all other } \mathfrak{p} \in X^*, \end{cases}$$

$$D_{L,x} = \ell(t)[T; \Phi]/(T^r - t) \simeq \text{Frac}(\ell[T; \Phi])$$

Consider the divisor $E = \frac{\delta}{r} \cdot \infty \in \text{Div}_{\mathbb{Q}}(Y)$, $\delta \in \mathbb{N} \rightsquigarrow \Lambda_{L,t}(E) = \ell[T; \Phi]_{\leq \delta}$

Fix rational places $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ corresponding to elements $c_1, \dots, c_s \in k \sqcup \{\infty\}$. They satisfy **the hypothesis** if and only if $c_i \in N_{\ell/k}(\ell^\times) \ \forall i$. For $c_i = N_{\ell/k}(u_i)$ we have

$$\begin{aligned} \alpha : \quad \ell[T; \Phi]_{\leq \delta} &\longrightarrow \text{End}_k(\ell)^s \\ f &\mapsto (f(u_i \Phi))_{1 \leq i \leq s}, \end{aligned}$$

\rightsquigarrow construction of linearized Reed–Solomon!

Linearized AG codes over \mathbb{P}^1 are Linearized Reed–Solomon codes

$X = \mathbb{P}_k^1$ and $Y = \mathbb{P}_\ell^1$, both viewed as curves over $\text{Spec } k$, $t =$ the coordinate on X and Y

Choose the function $x = t \in K^\times = k(t)^\times$. Then

$$b_{\mathfrak{p}} = \begin{cases} r & \text{for } \mathfrak{p} = 0, \infty, \\ 1 & \text{for all other } \mathfrak{p} \in X^*, \end{cases}$$

$$D_{L,x} = \ell(t)[T; \Phi]/(T^r - t) \simeq \text{Frac}(\ell[T; \Phi])$$

Consider the divisor $E = \frac{\delta}{r} \cdot \infty \in \text{Div}_{\mathbb{Q}}(Y)$, $\delta \in \mathbb{N} \rightsquigarrow \Lambda_{L,t}(E) = \ell[T; \Phi]_{\leq \delta}$

Fix rational places $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ corresponding to elements $c_1, \dots, c_s \in k \sqcup \{\infty\}$. They satisfy **the hypothesis** if and only if $c_i \in N_{\ell/k}(\ell^\times) \ \forall i$. For $c_i = N_{\ell/k}(u_i)$ we have

$$\begin{aligned} \alpha : \quad \ell[T; \Phi]_{\leq \delta} &\longrightarrow \text{End}_k(\ell)^s \\ f &\mapsto (f(u_i \Phi))_{1 \leq i \leq s}, \end{aligned}$$

\rightsquigarrow construction of linearized Reed–Solomon!

Our lower bounds: $\delta_\ell \geq m + 1$ and $d \geq sr - m = n_\ell - m \Rightarrow$ **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 $\mathcal{C}(x; E; \mathfrak{p}_1, \dots, \mathfrak{p}_s)$
(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 $\mathcal{C}(x; E; \mathfrak{p}_1, \dots, \mathfrak{p}_s)$
(require to develop the theory of differential forms and residues in our framework)

Merci de votre attention !

Questions?

elena.berardini@math.u-bordeaux.fr