Algebraic Geometry codes in the sum-rank metric

Elena Berardini and Xavier Caruso

CNRS, Institut de Mathématiques de Bordeaux

14^{th}–16^{th} February 2024

OPEn problems in the (sum-)**RA**nk metric

To appear in IEEE Transactions on Information Theory

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

Codes in the sum-rank metric: general definitions

Take k a field (think about $k = \mathbb{F}_q$), $\boldsymbol{V} = (V_1, \dots, V_s)$ s-uple of k-vector spaces ($n_i = \dim_k V_i$)

$$\mathrm{End}_k(\boldsymbol{V}) := \mathrm{End}_k(V_1) \times \cdots \times \mathrm{End}_k(V_s) \simeq M_{n_1,n_1}(k) \times \cdots \times M_{n_s,n_s}(k)$$

The sum-rank distance between $\boldsymbol{\varphi} = (\varphi_1, \dots, \varphi_s), \boldsymbol{\psi} = (\psi_1, \dots, \psi_s) \in \mathrm{End}_k(\boldsymbol{V})$ is

$$d_{\mathrm{srk}}(\boldsymbol{\varphi}, \boldsymbol{\psi}) := \sum_{i=1}^{s} \mathrm{rk}(\varphi_i - \psi_i).$$

Definition

A code $\mathcal{C}$ in the sum-rank metric is a k–linear subspace of $\mathrm{End}_k(\boldsymbol{V})$ endowed with the sum-rank distance. Its length n is $\sum_{i=1}^{s} n_i^2$. Its dimension κ is $\dim_k \mathcal{C}$. Its minimum distance is

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

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

$s = 1 \quad \rightsquigarrow \quad$ codes in the rank metric

Particular case and the Singleton bound

$\ell =$ finite extension of k of degree r (think about $\ell = \mathbb{F}_{q^r}$)

$\boldsymbol{V} = (V_1, \ldots, V_s)$, s-uple of ℓ-vector spaces $\rightsquigarrow$ $\mathrm{End}_k(\boldsymbol{V})$ is a ℓ-vector space

$\rightsquigarrow$ ℓ–linear codes in the sum-rank metric: ℓ–linear subspaces $\mathcal{C} \subset \mathrm{End}_k(\boldsymbol{V})$

$\rightsquigarrow$ ℓ–variants of the parameters: (taking $\dim_k V_i = r$)

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

Singleton bound

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

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

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

Particular case and the Singleton bound

ℓ = finite extension of k of degree r (think about $\ell = \mathbb{F}_{q^r}$)

$\boldsymbol{V} = (V_1, \dots, V_s)$, s-uple of ℓ-vector spaces $\rightsquigarrow$ $\mathrm{End}_k(\boldsymbol{V})$ is a ℓ-vector space

$\rightsquigarrow$ ℓ–linear codes in the sum-rank metric: ℓ–linear subspaces $\mathcal{C} \subset \mathrm{End}_k(\boldsymbol{V})$

$\rightsquigarrow$ ℓ–variants of the parameters: (taking $\dim_k V_i = r$)

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

Singleton bound

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

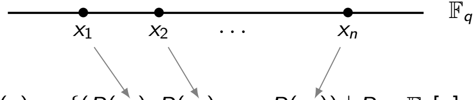
$$d + \kappa_\ell \leq n_\ell + 1.$$

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

$$rd + \kappa \leq n + r.$$

Algebraic and geometric constructions in the Hamming and rank metric

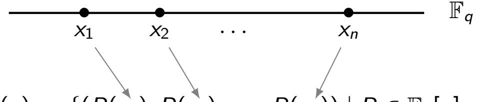
Reed–Solomon (RS) codes:



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

Algebraic and geometric constructions in the Hamming and rank metric

Reed–Solomon (RS) codes:



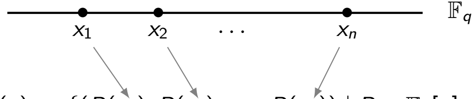
$$\mathrm{RS}(\mathbf{x}) := \{(P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\kappa}\}$$

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

⚠ **Drawback:** $n \leqslant q$

Algebraic and geometric constructions in the Hamming and rank metric

Reed–Solomon (RS) codes:



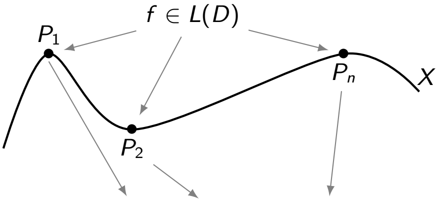
$$\mathrm{RS}(\mathbf{x}) := \{(P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\kappa}\}$$

✔ **Optimal parameters:** $\kappa + d = n + 1$

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

⚠ **Drawback:** $n \leqslant q$

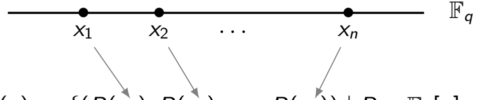
Algebraic Geometry (AG) codes:



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

Algebraic and geometric constructions in the Hamming and rank metric

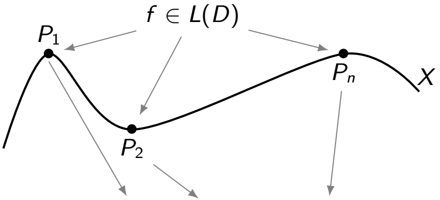
Reed–Solomon (RS) codes:



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

- ✔ **Optimal parameters:** $\kappa + d = n + 1$
  (Singleton bound: $\kappa + d \leq n + 1$)
- ⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes:

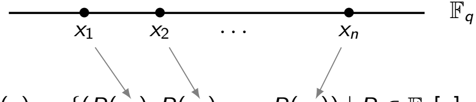


$$\mathcal{C}_X(\mathcal{P}, L(D)) := \{(f(P_1), f(P_2), \dots, f(P_n)) \mid f \in L(D)\}$$

- ✔ **Good parameters:** $n+1-g \leq \kappa+d \leq n+1$
- ✔ **Longer codes**

Algebraic and geometric constructions in the Hamming and rank metric

Reed–Solomon (RS) codes:



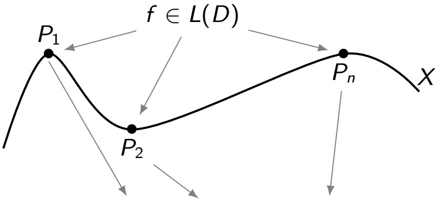
$$\mathrm{RS}(\mathbf{x}) := \{(P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[x]_{<\kappa}\}$$

- ✔ **Optimal parameters:** $\kappa + d = n + 1$
  (Singleton bound: $\kappa + d \leq n + 1$)
- ⚠ **Drawback:** $n \leqslant q$

Gabidulin codes:

- ✔ **Optimal parameters:** MRD codes
- ⚠ **Drawback: ??**

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:** $n+1-g \leq \kappa+d \leq n+1$
- ✔ **Longer codes**

AG codes in the rank metric:

404 Error : Not Found

Algebraic and geometric constructions in the Hamming and rank metric

Reed–Solomon (RS) codes:

RS(x) := …

✔ Op…
(Si…

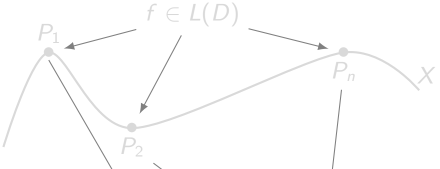
⚠ Dr…

Gabidul… codes:

✔ **Optimal parameters:** MRD codes

⚠ **Drawback:** ??

Algebraic Geometry (AG) codes:



… $L(D)\}$

… $n+1$

404 Error : Not Found

On today's menu

Equivalent constructions in the **sum-rank metric** of

- Reed–Solomon codes
  $\rightsquigarrow$ linearized Reed-Solomon codes (Martínez-Peñas, 2018)
- Algebraic Geometry codes
  $\rightsquigarrow$ linearized Algebraic Geometry codes (B. & Caruso, 2023)

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

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

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

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

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

for $c \in \ell$

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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

$\ell = \mathbb{F}_{q^r},\ k = \mathbb{F}_q,\ \mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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 $\kappa \in \mathbb{Z}$

consider

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

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

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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 $\kappa \in \mathbb{Z}$ such that $\kappa \leq rs$ consider

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

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

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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 $\kappa \in \mathbb{Z}$ such that $\kappa \leq rs$ consider

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

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

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

Ore polynomials and Linearized Reed–Solomon codes

$\ell = \mathbb{F}_{q^r}$, $k = \mathbb{F}_q$, $\mathrm{Gal}(\ell/k) = \langle \Phi \rangle$ ($\Phi : \ell \to \ell$ is the q-Frobenius)

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

The ring of Ore polynomials $\ell[T;\Phi]$ is the ring of 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 $\kappa \in \mathbb{Z}$ such that $\kappa \leq rs$ consider

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

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

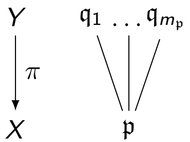
Our setting

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

π a cover with cyclic Galois group of order r

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

Our setting

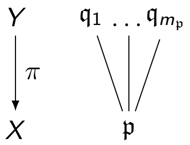


π a cover with cyclic Galois group of order r

$K := k(X), L := k(Y)$ the field of functions of X and 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



π a cover with cyclic Galois group of order r

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

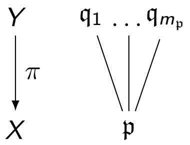
For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.

For $x \in K^\times$, consider the algebra of Ore polynomials with coefficient in L

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

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



π a cover with cyclic Galois group of order r

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

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

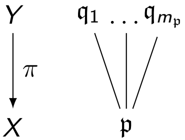
For $x \in K^\times$, consider the algebra of Ore polynomials with coefficient in L

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

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

- ☐ Riemann–Roch spaces of $D_{L,x}$
  $\rightsquigarrow$ need to define a valuation for $f \in D_{L,x}$
- ☐ a Riemann's inequality
- ☐ equivalent of "evaluate at a rational point"

Our setting



π a cover with cyclic Galois group of order r

$K := k(X), L := k(Y)$ the field of functions of X and 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 of Ore polynomials with coefficient in L

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

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

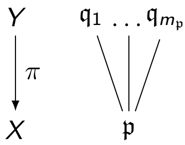
The valuation

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

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

$e_\mathfrak{q}$ =ramification index of $\mathfrak{q}$

Our setting



π a cover with cyclic Galois group of order r

$K := k(X), L := k(Y)$ the field of functions of X and 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 of Ore polynomials with coefficient in L

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

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

The valuation

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

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

$e_\mathfrak{q}$ =ramification index of $\mathfrak{q}$

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

Let $E = \sum_{\mathfrak{q} \in Y} n_{\mathfrak{q}} \mathfrak{q} \in \mathrm{Div}\,(Y) \otimes \mathbb{Q}$, with $n_{\mathfrak{q}} \in \frac{1}{b_{\mathfrak{p}}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$.

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

The Riemann–Roch space of $D_{L,x}$ associated with E is

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

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

Divisors and Riemann–Roch spaces over Ore polynomial rings

Let $E = \sum_{\mathfrak{q} \in Y} n_\mathfrak{q} \mathfrak{q} \in \mathrm{Div}\,(Y) \otimes \mathbb{Q}$, with $n_\mathfrak{q} \in \frac{1}{b_\mathfrak{p}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$.

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

The Riemann–Roch space of $D_{L,x}$ associated with E is

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

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

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

Let $E = \sum_{\mathfrak{q} \in Y} n_{\mathfrak{q}} \mathfrak{q} \in \mathrm{Div}\,(Y) \otimes \mathbb{Q}$, with $n_{\mathfrak{q}} \in \frac{1}{b_{\mathfrak{p}}}\mathbb{Z}$ where $\mathfrak{p} = \pi(\mathfrak{q})$.

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

The Riemann–Roch space of $D_{L,x}$ associated with E is

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

$\Rightarrow \Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i) \cdot T^i$, 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 $\sum_{i=0}^{r-1} \deg_Y(E_i) = r \cdot \deg_Y(E) - \frac{r^2}{2} \sum_{\mathfrak{p} \in X} \frac{b_{\mathfrak{p}} - 1}{b_{\mathfrak{p}} e_{\mathfrak{p}}} \deg_X(\mathfrak{p})$.

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

The space $\Lambda_{L,x}(E)$ is finite dimensional over k and

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

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 $(K_\mathfrak{p} \simeq k((t)))$, $x \in K^\times$

under some hypotheses on x get

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

Code's construction

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

under some hypotheses on x get

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

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

$$\begin{array}{rccc} \alpha: & \Lambda_{L,x}(E) & \longrightarrow & \prod_{i=1}^s \mathrm{End}_k(V_{\mathfrak{p}_i}) \\ & f & \mapsto & (\bar{\varepsilon}_{\mathfrak{p}_1}(f), \ldots, \bar{\varepsilon}_{\mathfrak{p}_s}(f)). \end{array}$$

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 $\prod_{i=1}^{s} \mathrm{End}_k(V_{\mathfrak{p}_i})$.

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 κ and the minimum distance d of $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ satisfy

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

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

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

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

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 κ and the minimum distance d of $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$ satisfy

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

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

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

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

$X = \mathbb{P}^1_k$, $Y = \mathbb{P}^1_\ell$, $E = \frac{\kappa}{r} \cdot \infty \in \mathrm{Div}_{\mathbb{Q}}(Y) \rightsquigarrow$ linearized Reed–Solomon codes!

Our lower bounds $\Rightarrow$ MSRD codes

Asymptotic behaviour: better than the Gilbert–Varshamov bound

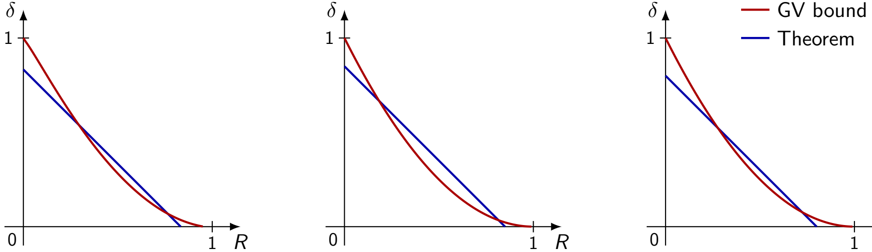
Theorem (B. & Caruso, 2023)

We assume that q is a square. For all real numbers $R, \delta \in (0,1)$ such that

$$R < 1 - \delta - \frac{2}{\sqrt{q}-1} + \frac{1}{r(\sqrt{q}-1)}$$

there exists a ℓ-linear LAG code with rate at least R and relative minimum distance at least δ.

We compare to the sum-rank version of the Gilbert–Varshamov bound :



$q = 7^2$, $r = 1$ $\quad$ $q = 11^2$, $r = 2$ $\quad$ $q = 11^2$, $r \to \infty$

Take away and further questions

- ✔ We have Algebraic Geometry codes in the sum-rank metric, of length sr^2
- ✔ The s in the length is the number of rational places $\rightsquigarrow$ can take $s > q$
- ✔ We beat the sum-rank metric version of the Gilbert-Varshamov bound

Take away and further questions

- ✓ We have Algebraic Geometry codes in the sum-rank metric, of length sr^2
- ✓ The s in the length is the number of rational places $\rightsquigarrow$ can take $s > q$
- ✓ We beat the sum-rank metric version of the Gilbert-Varshamov bound

- decoding problem: work in progress with X. Caruso and F. Drain (our Ph.D student) (decoding algorithm for linearized Reed–Solomon codes ✓)
- duality theorem for the codes $\mathcal{C}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s)$: work in progress with X. Caruso (require to develop the theory of differential forms and residues in our framework)

Grazie per l'attenzione!