Evaluation codes in the sum-rank metric

Elena Berardini

CNRS, Institut de Mathématiques de Bordeaux

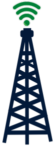
12 June 2025

Arithmetic, **G**eometry, & **C**^{2}oding **T**heory

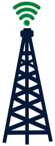
joint works with Xavier Caruso

Data representation and error correction

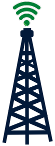
Data representation and error correction



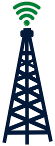
$$(1,1,0,\ldots,1,1)$$



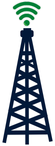
Data representation and error correction



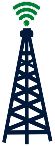
$(1, \underline{0}, 0, \ldots, 1, 1)$



Data representation and error correction



$$(1, 1, 0, \dots, 1, 1, \star, \dots, \star)$$



Codewords are vectors. Errors are vectors with few nonzero entries.

Data representation and error correction

$$(1,1,0,\dots,1,1,\star,\dots,\star)$$

Codewords are vectors. Errors are vectors with few nonzero entries.

$$(1,0,1,\dots,1,1)$$

$$(1,1,1,\dots,0,1)$$

$$(0,0,1,\dots,1,0)$$

Data representation and error correction

$$(1, 1, 0, \ldots, 1, 1, \star, \ldots, \star)$$

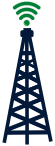
Codewords are vectors. Errors are vectors with few nonzero entries.

$$(1, 0, \underline{1}, \ldots, 1, 1)$$

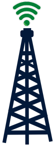
$$(1, 1, \underline{1}, \ldots, 0, 1)$$

$$(0, 0, \underline{1}, \ldots, 1, 0)$$

Data representation and error correction



$$(1,1,0,\ldots,1,1,\star,\ldots,\star)$$



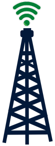
Codewords are vectors. Errors are vectors with few nonzero entries.

$$(1,0,\underline{1},\ldots,1,1)$$

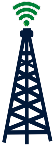
$$(\underline{1,1,1,\ldots,0,1})$$

$$(0,0,\underline{1},\ldots,1,0)$$

Data representation and error correction



$$(1, 1, 0, \ldots, 1, 1, \star, \ldots, \star)$$



Codewords are vectors. Errors are vectors with few nonzero entries.

$$\begin{pmatrix} 1 & 0 & 1 & \ldots & 1 & 1 \\ 1 & 1 & 1 & \ldots & 0 & 1 \\ 0 & 0 & 1 & \ldots & 1 & 0 \end{pmatrix}$$

Codewords are matrices.
Errors are matrices of small rank.

Data representation and error correction

$$\begin{pmatrix} 1 & 0 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 0 & 1 \\ 0 & 1 & 1 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \end{pmatrix}$$

Data representation and error correction

$$\begin{pmatrix} 1 & 0 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & \dots & 0 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 0 & 1 \\ 0 & 1 & 1 & \dots & 0 & 1 \\ 0 & 0 & 0 & \dots & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 & 1 & \dots & 1 & 1 \\ 1 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 1 & \dots & 1 & 0 \end{pmatrix}$$

Linear codes and the Hamming metric

$\mathbb{F}$ a finite field, $\mathscr{H}$ a $\mathbb{F}$-linear vector space endowed with a metric

(Linear) code $\mathscr{C}$: $\mathbb{F}$-vector subspace of $\mathscr{H}$

Parameters: length $n = \dim_{\mathbb{F}} \mathscr{H}$, dimension $k = \dim_{\mathbb{F}} \mathscr{C}$, minimum distance d

(depends on the metric)

$k \leftrightarrow$ information rate, $d \leftrightarrow$ correction capacity: we want k and d "big"

Linear codes and the Hamming metric

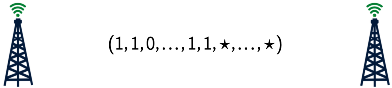
$\mathbb{F}$ a finite field, $\mathscr{H}$ a $\mathbb{F}$-linear vector space endowed with a metric

(Linear) code $\mathscr{C}$: $\mathbb{F}$-vector subspace of $\mathscr{H}$

Parameters: length $n = \dim_{\mathbb{F}} \mathscr{H}$, dimension $k = \dim_{\mathbb{F}} \mathscr{C}$, minimum distance d

(depends on the metric)

$k \leftrightarrow$ information rate, $d \leftrightarrow$ correction capacity: we want k and d "big"



Codes in the Hamming metric: $\mathbb{F}_q$-vector subspaces of $\mathscr{H} = \mathbb{F}_q^n$ endowed with

$$d(\mathbf{x},\mathbf{0}) := \#\{i \mid x_i \neq 0\}.$$

They respect the Singleton bound: $n + 1 \geqslant k + d$.

Very well-studied, many known constructions...

Codes in the sum-rank metric: definition 1/2

$\mathbb{F}_{q^r}$ = finite extension of $\mathbb{F}_q$ of degree r, $s \in \mathbb{N}$

Codes in the sum-rank metric: definition 1/2

$\mathbb{F}_{q^r}$ = finite extension of $\mathbb{F}_q$ of degree r, $s \in \mathbb{N}$

$$\mathscr{H} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s \quad := \quad \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \times \cdots \times \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \quad \simeq M_{r,r}(\mathbb{F}_q) \times \cdots \times M_{r,r}(\mathbb{F}_q)$$

$\mathbb{F}_{q^r}$-vector space — linear morphisms $\mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$

Codes in the sum-rank metric: definition 1/2

$\mathbb{F}_{q^r}$ = finite extension of $\mathbb{F}_q$ of degree r, $s \in \mathbb{N}$

$$\mathscr{H} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s \quad := \quad \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \times \cdots \times \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \quad \simeq M_{r,r}(\mathbb{F}_q) \times \cdots \times M_{r,r}(\mathbb{F}_q)$$

$\mathbb{F}_{q^r}$-vector space — linear morphisms $\mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$

Definition

The sum-rank distance between $\underline{\varphi} = (\varphi_1, \dots, \varphi_s)$ *and* $\underline{\psi} = (\psi_1, \dots, \psi_s) \in End_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s$ *is*

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

Codes in the sum-rank metric: definition 2/2

Definition

A code $\mathscr{C}$ in the sum-rank metric is a $\mathbb{F}_{q^r}$–linear subspace of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s$ endowed with the sum-rank distance.

Codes in the sum-rank metric: definition 2/2

Definition

A code $\mathscr{C}$ in the sum-rank metric is a $\mathbb{F}_{q^r}$–linear subspace of $End_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s$ endowed with the sum-rank distance. Its length n is sr. Its dimension k is $\dim_{\mathbb{F}_{q^r}} \mathscr{C}$. Its minimum distance is $d := \min\left\{ d_{srk}(\underline{\varphi}, \underline{0}) \mid \underline{\varphi} \in \mathscr{C}, \underline{\varphi} \neq \underline{0} \right\}$.

Codes in the sum-rank metric: definition 2/2

Definition

A code $\mathscr{C}$ in the sum-rank metric is a $\mathbb{F}_{q^r}$–linear subspace of $\mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s$ endowed with the sum-rank distance. Its length n is sr. Its dimension k is $\dim_{\mathbb{F}_{q^r}} \mathscr{C}$. Its minimum distance is $d := \min\left\{ d_{srk}(\underline{\varphi}, \underline{0}) \mid \underline{\varphi} \in \mathscr{C}, \underline{\varphi} \neq \underline{0} \right\}$.

$r = 1 \quad \rightsquigarrow$ codes of length s in the Hamming metric

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

Codes in the sum-rank metric: definition 2/2

Definition

A code $\mathscr{C}$ in the sum-rank metric is a $\mathbb{F}_{q^r}$–linear subspace of $End_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s$ endowed with the sum-rank distance. Its length n is sr. Its dimension k is $\dim_{\mathbb{F}_{q^r}} \mathscr{C}$. Its minimum distance is $d := \min\left\{ d_{srk}(\underline{\varphi}, \underline{0}) \mid \underline{\varphi} \in \mathscr{C}, \underline{\varphi} \neq \underline{0} \right\}$.

$r = 1 \quad \rightsquigarrow \quad$ codes of length s in the Hamming metric

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

Singleton bound

The $\mathbb{F}_{q^r}$-parameters of $\mathscr{C}$ satisfy

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

Slogan & Roadmap

We aim at reproducing in the sum-rank metric existing constructions of linear codes in the Hamming metric, known as evaluation codes.

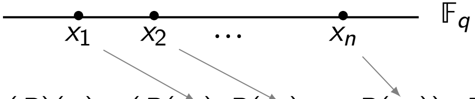
Slogan & Roadmap

We aim at reproducing in the sum-rank metric existing constructions of linear codes in the Hamming metric, known as evaluation codes.

Evaluating...	**Getting...**	**with properties...**
univariate polynomials	Reed–Solomon (RS) codes	optimal parameters, somewhat "short"
multivariate polynomials	Reed–Muller (RM) codes	longer than RS codes
rational functions	Algebraic Geometry (AG) codes	longer than RS codes, (asymptotically) good parameters, featuring nice algebraic geometry

Reed–Solomon codes in the Hamming metric

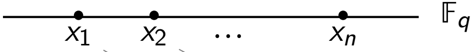
Reed–Solomon (RS) codes: take $k < n$



$$\mathrm{RS}_k(\boldsymbol{x}) := \{\mathrm{ev}(P)(\boldsymbol{x}) = (P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

Reed–Solomon codes in the Hamming metric

Reed–Solomon (RS) codes: take $k < n$

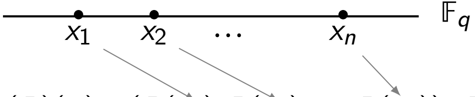


$$\mathrm{RS}_k(\boldsymbol{x}) := \{\mathrm{ev}(P)(\boldsymbol{x}) = (P(x_1), P(x_2), \dots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

The length n is $\leq q$: we can choose up to q distinct elements in $\mathbb{F}_q$.

Reed–Solomon codes in the Hamming metric

Reed–Solomon (RS) codes: take $k < n$



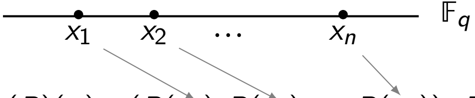
$$\mathrm{RS}_k(\boldsymbol{x}) := \{\mathrm{ev}(P)(\boldsymbol{x}) = (P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

The length n is $\leq q$: we can choose up to q distinct elements in $\mathbb{F}_q$.

The dimension is k: a basis of $\mathbb{F}_q[T]_{<k}$ is given by $\{1, T, \ldots, T^{k-1}\}$.

Reed–Solomon codes in the Hamming metric

Reed–Solomon (RS) codes: take $k < n$



$$\mathrm{RS}_k(\boldsymbol{x}) := \{\mathrm{ev}(P)(\boldsymbol{x}) = (P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

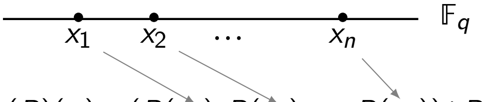
The length n is $\leq q$: we can choose up to q distinct elements in $\mathbb{F}_q$.

The dimension is k: a basis of $\mathbb{F}_q[T]_{<k}$ is given by $\{1, T, \ldots, T^{k-1}\}$.

The minimum distance is $n-k+1$: a polynomial of degree $k-1$ has at most $k-1$ zeros.

Reed–Solomon codes in the Hamming metric

Reed–Solomon (RS) codes: take $k < n$



$$\mathrm{RS}_k(\boldsymbol{x}) := \{\mathrm{ev}(P)(\boldsymbol{x}) = (P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

⚠ **The length n is $\leq q$** $\rightsquigarrow$ to construct long RS codes we need big finite fields!

(the bigger the q, the less efficient the arithmetic)

The dimension is k: a basis of $\mathbb{F}_q[T]_{<k}$ is given by $\{1, T, \ldots, T^{k-1}\}$.

The minimum distance is $n-k+1$: a polynomial of degree $k-1$ has at most $k-1$ zeros.

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

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

$$\begin{array}{c} \mathbb{F}_{q^r} \\ \Big\downarrow \Phi \\ \mathbb{F}_q \end{array}$$

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\ \Phi\ } \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\ \Phi\ } \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

⚠ Evaluation of Ore polynomials at elements of $\mathbb{F}_{q^r}$ is not a ring homomorphism

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\ \Phi\ } \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

$$\begin{array}{rccc} \mathrm{ev}: & \mathbb{F}_{q^r}[T;\Phi] & \longrightarrow & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & P & \longmapsto & P(\Phi). \end{array}$$

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\ \Phi\ } \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

for $c \in \mathbb{F}_{q^r}$

$$\mathrm{ev}_c : \begin{array}{ccc} \mathbb{F}_{q^r}[T;\Phi] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ P & \mapsto & P(c\Phi). \end{array}$$

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\ \Phi\ } \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

for $\underline{c} = (c_1, \ldots, c_s) \in \mathbb{F}_{q^r}^s$

$$\mathrm{ev}_{\underline{c}} : \begin{array}{ccc} \mathbb{F}_{q^r}[T;\Phi] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s \\ P & \mapsto & (P(c_1\Phi), \ldots, P(c_s\Phi)). \end{array}$$

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

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

$$\mathbb{F}_{q^r} \xrightarrow{\Phi} \mathbb{F}_q$$

Ring of Ore polynomials $\mathbb{F}_{q^r}[T;\Phi]$: polynomials with coefficients in $\mathbb{F}_{q^r}$, with usual sum and multiplication

$$T \cdot a = \Phi(a) \cdot T \quad \forall a \in \mathbb{F}_{q^r}.$$

for $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s$

$$\begin{array}{rccc} \mathrm{ev}_{\underline{c}} : & \mathbb{F}_{q^r}[T;\Phi] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})^s \\ & P & \mapsto & (P(c_1\Phi), \dots, P(c_s\Phi)). \end{array}$$

Definition (Linearized Reed–Solomon codes)

For $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s$ and $k \in \mathbb{Z}$ define

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T;\Phi]_{<k}).$$

Different metrics, same problem

Proposition (Parameters of LRS codes)

For $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s \setminus \{\underline{0}\}$ *with* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_i) \neq N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_j)\ \forall i \neq j$ *and* $k \leq rs$

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T; \Phi]_{<k})$$

has parameters

$$\textit{length} = rs \quad \textit{dimension} = k \quad \textit{minimum distance} = rs - k + 1 \quad (\Rightarrow \textbf{\textit{optimal}})$$

Different metrics, same problem

Proposition (Parameters of LRS codes)

For $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s \setminus \{\underline{0}\}$ *with* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_i) \neq N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_j)\ \forall i \neq j$ *and* $k \leq rs$

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T;\Phi]_{<k})$$

has parameters

length $= rs$ *dimension* $= k$ *minimum distance* $= rs - k + 1$ ($\Rightarrow$ ***optimal***)

Main ingredients:

1. $\text{rk}(\text{ev}_{c_i}(P)) = \dim_{\mathbb{F}_q} \mathbb{F}_{q^r} - \dim_{\mathbb{F}_q} \ker(\text{ev}_{c_i}(P))$

Different metrics, same problem

Proposition (Parameters of LRS codes)

For $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s \setminus \{\underline{0}\}$ *with* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_i) \neq N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_j)\ \forall i \neq j$ *and* $k \leq rs$

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T;\Phi]_{<k})$$

has parameters

$$\textit{length} = rs \quad \textit{dimension} = k \quad \textit{minimum distance} = rs - k + 1 \quad (\Rightarrow \textbf{\textit{optimal}})$$

Main ingredients:

1. $\mathrm{rk}(\mathrm{ev}_{c_i}(P)) = \dim_{\mathbb{F}_q} \mathbb{F}_{q^r} - \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P))$
2. for $P \in \mathbb{F}_{q^r}[T;\Phi]_{<k}$, $\sum_{i=1}^{s} \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P)) \leqslant \deg P < k$

Different metrics, same problem

Proposition (Parameters of LRS codes)

For $\underline{c} = (c_1, \ldots, c_s) \in \mathbb{F}_{q^r}^s \setminus \{\underline{0}\}$ *with* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_i) \neq N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_j)\ \forall i \neq j$ *and* $k \leq rs$

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T;\Phi]_{<k})$$

has parameters

length $= rs$ *dimension* $= k$ *minimum distance* $= rs - k + 1$ ($\Rightarrow$ ***optimal***)

Main ingredients:

1. $\mathrm{rk}(\mathrm{ev}_{c_i}(P)) = \dim_{\mathbb{F}_q} \mathbb{F}_{q^r} - \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P))$
2. for $P \in \mathbb{F}_{q^r}[T;\Phi]_{<k}$, $\sum_{i=1}^s \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P)) \leqslant \deg P < k$

⚠ $s < \mathrm{Card}(\mathbb{F}_q) = q \rightsquigarrow$ similar problem as for Reed–Solomon codes

Different metrics, same problem

Proposition (Parameters of LRS codes)

For $\underline{c} = (c_1, \dots, c_s) \in \mathbb{F}_{q^r}^s \setminus \{\underline{0}\}$ *with* $N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_i) \neq N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(c_j)\ \forall i \neq j$ *and* $k \leq rs$

$$LRS(k, \underline{c}) = ev_{\underline{c}}(\mathbb{F}_{q^r}[T;\Phi]_{<k})$$

has parameters

$$\textit{length} = rs \quad \textit{dimension} = k \quad \textit{minimum distance} = rs - k + 1 \quad (\Rightarrow \textbf{\textit{optimal}})$$

Main ingredients:

1. $\mathrm{rk}(\mathrm{ev}_{c_i}(P)) = \dim_{\mathbb{F}_q} \mathbb{F}_{q^r} - \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P))$
2. for $P \in \mathbb{F}_{q^r}[T;\Phi]_{<k}$, $\sum_{i=1}^{s} \dim_{\mathbb{F}_q} \ker(\mathrm{ev}_{c_i}(P)) \leqslant \deg P < k$

⚠ $s < \mathrm{Card}(\mathbb{F}_q) = q \rightsquigarrow$ similar problem as for Reed–Solomon codes

How do we solve the problem in the Hamming metric?

From univariate to multivariate

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

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

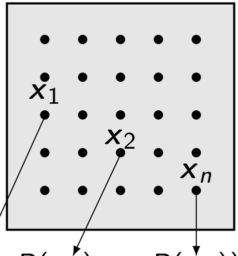
From univariate to multivariate

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

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

Reed–Muller (RM) codes:



- Use multivariate polynomials $P \in \mathbb{F}_q[X_1, \ldots, X_m]$
- Evaluate at points in $\mathbb{F}_q^m$
- ✔ **Length:** q^m

($m = 2$ in the picture)

$$\mathrm{RM}_k(2) := \{(P(\boldsymbol{x}_1), P(\boldsymbol{x}_2), \ldots, P(\boldsymbol{x}_n)) \mid P \in \mathbb{F}_q[X_1, X_2]_{\leq k}\}$$

Multivariate polynomials

Setting: $\mathbb{F}_{q^r}/\mathbb{F}_q$, $\Phi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ is the q-Frobenius, $(e_1, \ldots, e_m) \in \mathbb{Z}^m$

The ring of multivariate Ore polynomials $\mathbb{F}_{q^r}[X_1, \ldots, X_m; \Phi^{e_1}, \ldots, \Phi^{e_m}]$: multivariate polynomials with usual sum and multiplication given by

$$X_i \cdot X_j = X_j \cdot X_i, \text{ and } X_i \cdot a = \Phi^{e_i}(a) \cdot X_i, \quad \forall a \in \mathbb{F}_{q^r}.$$

Multivariate polynomials

Setting: $\mathbb{F}_{q^r}/\mathbb{F}_q$, $\Phi : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ is the q-Frobenius, $(e_1, \ldots, e_m) \in \mathbb{Z}^m$

The ring of multivariate Ore polynomials $\mathbb{F}_{q^r}[X_1, \ldots, X_m; \Phi^{e_1}, \ldots, \Phi^{e_m}]$: multivariate polynomials with usual sum and multiplication given by

$$X_i \cdot X_j = X_j \cdot X_i, \text{ and } X_i \cdot a = \Phi^{e_i}(a) \cdot X_i, \quad \forall a \in \mathbb{F}_{q^r}.$$

- ☐ an evaluation morphism

$$\epsilon : \mathbb{F}_{q^r}[X_1, \ldots, X_m; \Phi^{e_1}, \ldots, \Phi^{e_m}] \to \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})$$

- ☐ for $P \in \mathbb{F}_{q^r}[X_1, \ldots, X_m; \Phi^{e_1}, \ldots, \Phi^{e_m}]$ a bound on

$$\dim_{\mathbb{F}_q} \ker \epsilon(P)$$

Reed–Muller codes in the sum-rank metric — B. & Caruso, 2025

☑ Evaluation: take $\gamma : \mathbb{Z}^m \to \mathbb{F}_{q^r}^{\times}$ such that $\gamma(\boldsymbol{u}+\boldsymbol{v}) = \gamma(\boldsymbol{u}) \cdot \Phi^{e_1 u_1 + \cdots + e_m u_m}(\gamma(\boldsymbol{v}))$

$$\begin{array}{rrcl} \epsilon_\gamma : & \mathbb{F}_{q^r}[X_1, \ldots, X_m; \Phi^{e_1}, \ldots, \Phi^{e_m}] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & P = \sum_{\boldsymbol{u} \in \mathbb{Z}^m} a_{\boldsymbol{u}} X_1^{u_1} \cdots X_m^{u_m} & \mapsto & \sum_{\boldsymbol{u} \in \mathbb{Z}^m} a_{\boldsymbol{u}} \gamma(\boldsymbol{u}) \Phi^{e_1 u_1 + \cdots + e_m u_m} \end{array}$$

Reed–Muller codes in the sum-rank metric

B. & Caruso, 2025

☑ Evaluation: take $\gamma : \mathbb{Z}^m \to \mathbb{F}_{q^r}^\times$ such that $\gamma(\boldsymbol{u}+\boldsymbol{v}) = \gamma(\boldsymbol{u}) \cdot \Phi^{e_1 u_1 + \cdots + e_m u_m}(\gamma(\boldsymbol{v}))$

$$\begin{array}{rccc} \epsilon_\gamma : & \mathbb{F}_{q^r}[X_1,\ldots,X_m;\Phi^{e_1},\ldots,\Phi^{e_m}] & \to & \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & P = \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}} X_1^{u_1}\cdots X_m^{u_m} & \mapsto & \sum_{\boldsymbol{u}\in\mathbb{Z}^m} a_{\boldsymbol{u}} \gamma(\boldsymbol{u}) \Phi^{e_1 u_1 + \cdots + e_m u_m} \end{array}$$

Let H be the set of "convenient" γ, and define

$$\begin{array}{rccc} \epsilon : & \mathbb{F}_{q^r}[X_1,\ldots,X_m;\Phi^{e_1},\ldots,\Phi^{e_m}] & \to & \prod_{\gamma\in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r}) \\ & P & \mapsto & (\epsilon_\gamma(P))_{\gamma\in H} \end{array}.$$

Linearized Reed–Muller code

The *linearized Reed-Muller code* associated to $(e_1,\ldots,e_m) \in \mathbb{Z}^m$ and $c \in \mathbb{Z}_{>0}$ is

$$\mathrm{LRM}((e_1,\ldots,e_m);c) = \epsilon\left(\mathbb{F}_{q^r}[X_1,\ldots,X_m;\Phi^{e_1},\ldots,\Phi^{e_m}]_{\leq c}\right).$$

Parameters

B. & Caruso, 2025

☑ Bound: let $P \in \mathbb{F}_{q^r}[X_1,\ldots,X_m;\Phi^{e_1},\ldots,\Phi^{e_m}]_{\leqslant c}$. Then

$$\sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \epsilon_\gamma(P) \leq rc \cdot (q-1)^{m-1}.$$

Parameters

B. & Caruso, 2025

☑ Bound: let $P \in \mathbb{F}_{q^r}[X_1, \dots, X_m; \Phi^{e_1}, \dots, \Phi^{e_m}]_{\leqslant c}$. Then

$$\sum_{\gamma \in H} \dim_{\mathbb{F}_q} \ker \epsilon_\gamma(P) \leq rc \cdot (q-1)^{m-1}.$$

Main ingredients:

- $\dim_{\mathbb{F}_q} \ker \epsilon_\gamma(P) \leq \mathrm{ord}_\gamma(\mathrm{Nrd}(P))$
- for $P \in \mathbb{F}_q[X_1, \dots, X_m]_{\leq c}$, $\sum_{\mathrm{a} \in (\mathbb{F}_q^\times)^m} \mathrm{ord}_{\mathrm{a}}(P) \leq c \cdot (q-1)^{m-1}$

Parameters

B. & Caruso, 2025

☑ Bound: let $P \in \mathbb{F}_{q^r}[X_1,\dots,X_m;\Phi^{e_1},\dots,\Phi^{e_m}]_{\leqslant c}$. Then

$$\sum_{\gamma\in H} \dim_{\mathbb{F}_q} \ker \epsilon_\gamma(P) \le rc\cdot(q-1)^{m-1}.$$

Main ingredients:

- $\dim_{\mathbb{F}_q} \ker \epsilon_\gamma(P) \le \mathrm{ord}_\gamma(\mathrm{Nrd}(P))$
- for $P \in \mathbb{F}_q[X_1,\dots,X_m]_{\le c}$, $\sum_{a\in(\mathbb{F}_q^\times)^m} \mathrm{ord}_a(P) \le c\cdot(q-1)^{m-1}$

Theorem

Let $1 \le c \le q-2$. The code $\mathrm{LRM}((e_1,\dots,e_m);c) \subseteq \prod_{\gamma\in H} \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^r})$ has parameter

$$n = r\cdot(q-1)^m \qquad k = \binom{c+m}{c} \qquad \text{and} \qquad d \ge r\cdot(q-1)^{m-1}\cdot(q-1-c).$$

Main ingredients: the bound above + $\mathrm{Card}(H) = (q-1)^m$.

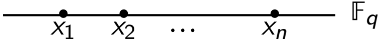
From polynomials to rational functions

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

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

From polynomials to rational functions

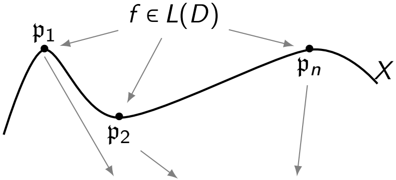


$$\mathrm{RS}_k(\boldsymbol{x}) := \{(P(x_1), P(x_2), \ldots, P(x_n)) \mid P \in \mathbb{F}_q[T]_{<k}\}$$

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes: X a nice curve, $\mathscr{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq X(\mathbb{F}_q)$



$$\mathrm{AG}_X(\mathscr{P}, D) := \{(f(\mathfrak{p}_1), f(\mathfrak{p}_2), \ldots, f(\mathfrak{p}_n)) \mid f \in L(D)\}$$

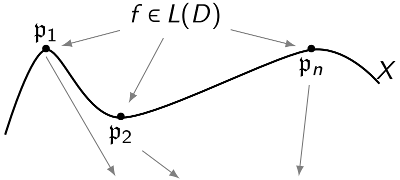
From polynomials to rational functions

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

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes: X a nice curve, $\mathscr{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq X(\mathbb{F}_q)$



$$\mathrm{AG}_X(\mathscr{P}, D) := \{(f(\mathfrak{p}_1), f(\mathfrak{p}_2), \ldots, f(\mathfrak{p}_n)) \mid f \in L(D)\}$$

Definition

A divisor is a formal sum of points on X

$$D = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \mathfrak{p},\ n_{\mathfrak{p}} \in \mathbb{Z}.$$

*The Riemann–Roch space $L(D)$ is a vector space of functions with **zeros and poles** controlled by D.*

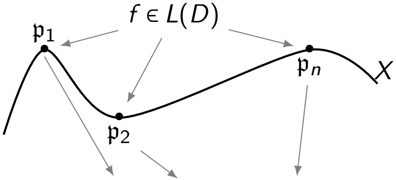
From polynomials to rational functions

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

✔ **Optimal:** $k + d = n + 1$

⚠ **Drawback:** $n \leqslant q$

Algebraic Geometry (AG) codes: X a nice curve, $\mathscr{P} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq X(\mathbb{F}_q)$



$$\mathrm{AG}_X(\mathscr{P}, D) := \{(f(\mathfrak{p}_1), f(\mathfrak{p}_2), \ldots, f(\mathfrak{p}_n)) \mid f \in L(D)\}$$

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

✔ **Length** $\sim \#X(\mathbb{F}_q) \leq q + 1 + 2g\sqrt{q}$

Definition

A divisor is a formal sum of points on X

$$D = \sum_{\mathfrak{p} \in X} n_{\mathfrak{p}} \mathfrak{p},\ n_{\mathfrak{p}} \in \mathbb{Z}.$$

The Riemann–Roch space $L(D)$ is a vector space of functions with ***zeros and poles*** *controlled by D.*

AG codes: classical ingredients

X a nice curve over $\mathbb{F}_q$ of genus g_X, $K = \mathbb{F}_q(X)$ the function field of X.

To any point $\mathfrak{p} \in X$ corresponds a valuation $v_{\mathfrak{p}}$: for $f \in K$ we have

$$v_{\mathfrak{p}}(f) = \begin{cases} m > 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{zero} \text{ of } f \text{ of multiplicity } m, \\ -m < 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{pole} \text{ of } f \text{ of multiplicity } m. \end{cases}$$

AG codes: classical ingredients

X a nice curve over $\mathbb{F}_q$ of genus g_X, $K = \mathbb{F}_q(X)$ the function field of X.

To any point $\mathfrak{p} \in X$ corresponds a valuation $v_{\mathfrak{p}}$: for $f \in K$ we have

$$v_{\mathfrak{p}}(f) = \begin{cases} m > 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{zero} \text{ of } f \text{ of multiplicity } m, \\ -m < 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{pole} \text{ of } f \text{ of multiplicity } m. \end{cases}$$

The Riemann–Roch space associated with $D = \sum n_{\mathfrak{p}} \mathfrak{p}$ is

$$L_X(D) := \{f \in K^{\times} \mid v_{\mathfrak{p}}(f) + n_{\mathfrak{p}} \geq 0 \, \forall \mathfrak{p} \in X\} \cup \{0\}.$$

AG codes: classical ingredients

X a nice curve over $\mathbb{F}_q$ of genus g_X, $K = \mathbb{F}_q(X)$ the function field of X.

To any point $\mathfrak{p} \in X$ corresponds a valuation $v_\mathfrak{p}$: for $f \in K$ we have

$$v_\mathfrak{p}(f) = \begin{cases} m > 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{zero} \text{ of } f \text{ of multiplicity } m, \\ -m < 0 \text{ if } \mathfrak{p} \text{ is a } \textbf{pole} \text{ of } f \text{ of multiplicity } m. \end{cases}$$

The Riemann–Roch space associated with $D = \sum n_\mathfrak{p} \mathfrak{p}$ is

$$L_X(D) := \left\{ f \in K^\times \mid v_\mathfrak{p}(f) + n_\mathfrak{p} \geq 0 \, \forall \mathfrak{p} \in X \right\} \cup \{0\}.$$

Riemann's inequality

Let $\deg(D) = \sum_{\mathfrak{p} \in X} n_\mathfrak{p} \deg \mathfrak{p}$. We have

$$\dim_{\mathbb{F}_q} L_X(D) \geq \deg(D) + 1 - g_X.$$

Our setting

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

π a Galois cover with cyclic Galois group of order r

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

Our setting

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

π a Galois cover with cyclic Galois group of order r

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

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

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

π a Galois cover with cyclic Galois group of order r

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

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

Today: $Y = \mathrm{Spec}\,\mathbb{F}_{q^r} \times_{\mathrm{Spec}\,\mathbb{F}_q} X$. So, π is unramified.

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

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

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

Today: $Y = \mathrm{Spec}\, \mathbb{F}_{q^r} \times_{\mathrm{Spec}\, \mathbb{F}_q} X$. So, π is unramified.

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

$$\begin{array}{ccc} Y & & \mathfrak{q}_1 \ldots \mathfrak{q}_{m_\mathfrak{p}} \\ \downarrow \pi & & \backslash \; | \; / \\ X & & \mathfrak{p} \end{array}$$

π a Galois cover with cyclic Galois group of order r

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

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

Today: $Y = \mathrm{Spec}\,\mathbb{F}_{q^r} \times_{\mathrm{Spec}\,\mathbb{F}_q} X$. So, π is unramified.

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 a valuation for $f \in D_{L,x}$
- ☐ a Riemann's inequality
- ☐ equivalent of "evaluate at a rational point"

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

$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$

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

Today: $Y = \mathrm{Spec}\,\mathbb{F}_{q^r} \times_{\mathrm{Spec}\,\mathbb{F}_q} X$. So, π is unramified.

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: Consider the 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 $f = f_0 + f_1 T + \cdots + f_{r-1} T^{r-1}$,

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

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
$K := \mathbb{F}_q(X), L := \mathbb{F}_q(Y)$, $\mathrm{Gal}(L/K) = \langle \Phi \rangle$
For $\mathfrak{p} \in X$ we have the decomposition $L_\mathfrak{p} := K_\mathfrak{p} \otimes_K L \simeq \prod_{\mathfrak{q}|\mathfrak{p}} L_\mathfrak{q}$.
Today: $Y = \mathrm{Spec}\,\mathbb{F}_{q^r} \times_{\mathrm{Spec}\,\mathbb{F}_q} X$. So, π is unramified.

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: Consider the 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 $f = f_0 + f_1 T + \cdots + f_{r-1} T^{r-1}$,

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

!! $w_{\mathfrak{q}_j,x}(f) \in \frac{1}{b_\mathfrak{p}}\mathbb{Z}$.

Divisors and Riemann–Roch spaces over Ore polynomial rings

☑ The Riemann–Roch space: 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 $\mathfrak{p} = \pi(\mathfrak{q})$. The Riemann–Roch space of $D_{L,x}$ associated to E is

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

Divisors and Riemann–Roch spaces over Ore polynomial rings

☑ The Riemann–Roch space: 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 $\mathfrak{p} = \pi(\mathfrak{q})$. The Riemann–Roch space of $D_{L,x}$ associated to E is

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

!! $\Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i)\cdot T^i$, for some explicit $E_i \in \mathrm{Div}(Y)$.

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

Divisors and Riemann–Roch spaces over Ore polynomial rings

☑ The Riemann–Roch space: 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 $\mathfrak{p} = \pi(\mathfrak{q})$. The Riemann–Roch space of $D_{L,x}$ associated to E is

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

!! $\Lambda_{L,x}(E) = \bigoplus_{i=0}^{r-1} L_Y(E_i) \cdot T^i$, for some explicit $E_i \in \mathrm{Div}(Y)$.

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

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

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

Code's construction

B. & Caruso, 2024

Let $\mathfrak{p} \in X(\mathbb{F}_q)$ such that $\mathfrak{p} \notin \pi(\mathrm{Supp}(E))$, and $t_\mathfrak{p}$ a uniformizer.
Let $x \in K^\times$ and $u_\mathfrak{p} = (u_\mathfrak{q})_{\mathfrak{q}|\mathfrak{p}} \in L_\mathfrak{p}^\times$ such that $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_\mathfrak{q}/K_\mathfrak{p}}(u_\mathfrak{q})$. Then

$$\begin{array}{rcccccl} \varepsilon_\mathfrak{p} : & \Lambda_{L_\mathfrak{p},x}(E) & \xrightarrow{\simeq} & \mathrm{End}_{\mathcal{O}_{K_\mathfrak{p}}}(\mathcal{O}_{L_\mathfrak{p}}) & \xrightarrow{red} & \mathrm{End}_{\mathbb{F}_q}(\mathcal{O}_{L_\mathfrak{p}}/t_\mathfrak{p}\mathcal{O}_{L_\mathfrak{p}}) =: \mathrm{End}_{\mathbb{F}_q}(V_\mathfrak{p}) \\ & f & \longmapsto & f(u_\mathfrak{p}\Phi) & \longmapsto & f(u_\mathfrak{p}\Phi) \mod t_\mathfrak{p} \end{array}.$$

Code's construction

B. & Caruso, 2024

Let $\mathfrak{p} \in X(\mathbb{F}_q)$ such that $\mathfrak{p} \notin \pi(\mathrm{Supp}(E))$, and $t_{\mathfrak{p}}$ a uniformizer.
Let $x \in K^\times$ and $u_{\mathfrak{p}} = (u_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in L_{\mathfrak{p}}^\times$ such that $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(u_{\mathfrak{q}})$. Then

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

Whence, for $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ rational places on X, we define

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

Code's construction — B. & Caruso, 2024

Let $\mathfrak{p} \in X(\mathbb{F}_q)$ such that $\mathfrak{p} \notin \pi(\mathrm{Supp}(E))$, and $t_{\mathfrak{p}}$ a uniformizer.
Let $x \in K^\times$ and $u_{\mathfrak{p}} = (u_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in L_{\mathfrak{p}}^\times$ such that $x = \prod_{\mathfrak{q}|\mathfrak{p}} N_{L_{\mathfrak{q}}/K_{\mathfrak{p}}}(u_{\mathfrak{q}})$. Then

$$\begin{array}{rcccccl} \varepsilon_{\mathfrak{p}} : & \Lambda_{L_{\mathfrak{p}},x}(E) & \xrightarrow{\simeq} & \mathrm{End}_{\mathscr{O}_{K_{\mathfrak{p}}}}(\mathscr{O}_{L_{\mathfrak{p}}}) & \xrightarrow{red} & \mathrm{End}_{\mathbb{F}_q}(\mathscr{O}_{L_{\mathfrak{p}}}/t_{\mathfrak{p}}\mathscr{O}_{L_{\mathfrak{p}}}) =: \mathrm{End}_{\mathbb{F}_q}(V_{\mathfrak{p}}) \\ & f & \mapsto & f(u_{\mathfrak{p}}\Phi) & \mapsto & f(u_{\mathfrak{p}}\Phi) \mod t_{\mathfrak{p}} \end{array}.$$

Whence, for $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ rational places on X, we define

$$\begin{array}{rccl} \epsilon : & \Lambda_{L,x}(E) & \longrightarrow & \prod_{i=1}^{s} \mathrm{End}_{\mathbb{F}_q}(V_{\mathfrak{p}_i}) \\ & f & \mapsto & (\varepsilon_{\mathfrak{p}_1}(f), \ldots, \varepsilon_{\mathfrak{p}_s}(f)). \end{array}$$

Linearized Algebraic Geometry codes

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

$$\mathrm{LAG}(x; E; \mathfrak{p}_1, \ldots, \mathfrak{p}_s) = \varepsilon(\Lambda_{L,x}(E)).$$

Code's parameters B. & Caruso, 2024

Theorem

Assume $\deg_Y(E) < sr$, the previous hypotheses and $D_{L,x}$ has no nonzero divisors. The code $\mathrm{LAG}(x;E;\mathfrak{p}_1,\dots,\mathfrak{p}_s) \subseteq \prod_{i=1}^{s} \mathrm{End}_{\mathbb{F}_q}(V_{\mathfrak{p}_i})$ has parameters

$$n = sr,$$

$$k \geq \deg_Y(E) - r\cdot(g_X - 1) - \frac{r}{2}\sum_{\mathfrak{p}\in X} \frac{b_{\mathfrak{p}}-1}{b_{\mathfrak{p}}} \deg_X(\mathfrak{p}),$$

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

Main ingredients:

- For the dimension: Riemann's inequality
- For the minimum distance: $\dim_{\mathbb{F}_q} \ker \epsilon_{\mathfrak{p}}(f) \leq v_{\mathfrak{p}}(\mathrm{Nrd}(f))$

Retrieving the classical behavior of AG codes

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

Our lower bounds $\Rightarrow$ optimal codes

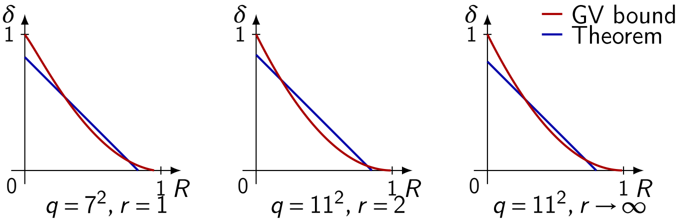
Retrieving the classical behavior of AG codes

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

Our lower bounds $\Rightarrow$ optimal codes

Theorem

For $q \geqslant 11^2$ square we beat the sum-rank version of the Gilbert–Varshamov bound.



Take away and further questions

- ✔ We have RS, RM and AG codes in the sum-rank metric
- ✔ They respect similar bounds as in the Hamming metric

Take away and further questions

- ✔ We have RS, RM and AG codes in the sum-rank metric
- ✔ They respect similar bounds as in the Hamming metric

?? decoding problem:

- for LRS codes: done by U. Martínez–Peñas
- for LAG codes: in progress with X. Caruso and F. Drain
- for LRM codes: LRM codes can be embedded in LAG codes

Take away and further questions

- ✔ We have RS, RM and AG codes in the sum-rank metric
- ✔ They respect similar bounds as in the Hamming metric

?? decoding problem:

- for LRS codes: done by U. Martínez–Peñas
- for LAG codes: in progress with X. Caruso and F. Drain
- for LRM codes: LRM codes can be embedded in LAG codes

?? explicit constructions: ongoing with P. Beelen, A. Gruica and M. Montanucci

Take away and further questions

- ✔ We have RS, RM and AG codes in the sum-rank metric
- ✔ They respect similar bounds as in the Hamming metric

?? decoding problem:
- for LRS codes: done by U. Martínez–Peñas
- for LAG codes: in progress with X. Caruso and F. Drain
- for LRM codes: LRM codes can be embedded in LAG codes

?? explicit constructions: ongoing with P. Beelen, A. Gruica and M. Montanucci

?? Goppa codes in the (sum-)rank metric: in progress with P. Trivedi

Take away and further questions

- ✔ We have RS, RM and AG codes in the sum-rank metric
- ✔ They respect similar bounds as in the Hamming metric

?? decoding problem:

- for LRS codes: done by U. Martínez–Peñas
- for LAG codes: in progress with X. Caruso and F. Drain
- for LRM codes: LRM codes can be embedded in LAG codes

?? explicit constructions: ongoing with P. Beelen, A. Gruica and M. Montanucci

?? Goppa codes in the (sum-)rank metric: in progress with P. Trivedi

Thank you for your attention!

This is an historical edition of AGC^{2}T!

We are at the 20^{th} edition (it has been around since 1987...) and

- the first edition with a woman in the organization committee was: 2019
- the first edition with 50% of plenary speakers being women: 2021 probably
- the first all-women plenary speakers edition was: **this one!**

Increased visibility of women on stage encourages women attendees to pursue career and speaking opportunities, which is key to closing the gender gap for future generations.

If this will become the norm, then we will fortunately see the effects being echoed in plenty of other events!