Rank metric, when analogies with Hamming metric fail

Alain Couvreur[1,2]

[1]Inria
[2]LIX, École polytechnique

OpeRa 2026, Bordeaux

In this talk...

In this talk...

some rank...

In this talk...

some rank... **no** sum-rank...

In this talk...

some rank... **no** sum-rank... still a lot of *seum*$^{(1)}$

In this talk...

some rank... **no** sum-rank... still a lot of *seum*[(1)]

(1) Don't try to understand this if:

In this talk...

some rank... **no** sum-rank... still a lot of *seum*[(1)]

[(1)] Don't try to understand this if:

- you don't speak french;

In this talk...

some rank... **no** sum-rank... still a lot of *seum*[(1)]

[(1)] Don't try to understand this if:

- you don't speak french;
- you are over 40;

In this talk...

some rank... **no** sum-rank... still a lot of *seum*[(1)]

[(1)] Don't try to understand this if:

- you don't speak french;
- you are over 40;
- both.

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

Rank metric codes

Definition 1

A *rank–metric code* or *matrix code* is an $\mathbb{F}_q$–subspace of $\mathbb{F}_q^{m\times n}$ endowed with the metric

$$\mathrm{dist}(\boldsymbol{A},\boldsymbol{B}) \stackrel{\text{def}}{=} \mathrm{Rk}(\boldsymbol{A}-\boldsymbol{B}).$$

$\mathbb{F}_{q^m}$–linear codes

Choosing an $\mathbb{F}_q$–basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ we have an isomorphism $\Phi_{\mathcal{B}} : \mathbb{F}_{q^m}^n \xrightarrow{\sim} \mathbb{F}_q^{m \times n}$

Definition 2

An $\mathbb{F}_{q^m}$*–linear code* is an $\mathbb{F}_{q^m}$–linear subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank metric (via $\Phi_{\mathcal{B}}$).

$\mathbb{F}_{q^m}$–linear codes

Choosing an $\mathbb{F}_q$–basis $\mathcal{B}$ of $\mathbb{F}_{q^m}$ we have an isomorphism $\Phi_{\mathcal{B}} : \mathbb{F}_{q^m}^n \xrightarrow{\sim} \mathbb{F}_q^{m\times n}$

Definition 2

An $\mathbb{F}_{q^m}$*–linear code* is an $\mathbb{F}_{q^m}$–linear subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank metric (via $\Phi_{\mathcal{B}}$).

In $\mathbb{F}_q^{m\times n}$, these codes correspond to matrix spaces $\mathscr{A}$ satisfying

$$\forall \alpha \in \mathbb{F}_{q^m}, \quad \mathsf{Mul}_{\mathcal{B}}(\alpha)\mathscr{A} = \mathscr{A}.$$

i.e., $\{\mathsf{Mul}_{\mathcal{B}}(\alpha) \ : \ \alpha \in \mathbb{F}_{q^m}\} \simeq_{alg} \mathbb{F}_{q^m}$ is a non-trivial left *stabilizer* of $\mathscr{A}$.

What a wonderful world

Hamming world		**Rank world**
$\mathbb{F}_q^n$ with Hamming distance	$\longleftrightarrow$	$\mathbb{F}_q^{m\times n}$ with Rank distance

What a wonderful world

Hamming world		**Rank world**
$\mathbb{F}_q^n$ with Hamming distance	$\longleftrightarrow$	$\mathbb{F}_q^{m\times n}$ with Rank distance
(Supports) $E \subset \{1, \dots, n\}$	$\longleftrightarrow$	either $V \subseteq \mathbb{F}_q^m$ (Column space) or $W \subseteq \mathbb{F}_q^n$ (Row space)

What a wonderful world

Hamming world		**Rank world**
$\mathbb{F}_q^n$ with Hamming distance	$\longleftrightarrow$	$\mathbb{F}_q^{m\times n}$ with Rank distance
(Supports) $E \subset \{1, \dots, n\}$	$\longleftrightarrow$	either $V \subseteq \mathbb{F}_q^m$ (Column space) or $W \subseteq \mathbb{F}_q^n$ (Row space)
Cardinality	$\longleftrightarrow$	Dimension

What a wonderful world

Hamming world		**Rank world**
$\mathbb{F}_q^n$ with Hamming distance	$\longleftrightarrow$	$\mathbb{F}_q^{m\times n}$ with Rank distance
(Supports) $E \subset \{1, \dots, n\}$	$\longleftrightarrow$	either $V \subseteq \mathbb{F}_q^m$ (Column space) or $W \subseteq \mathbb{F}_q^n$ (Row space)
Cardinality	$\longleftrightarrow$	Dimension
(Isometries) $\mathfrak{S}_n \rtimes \mathbb{F}_q^\times$	$\longleftrightarrow$	$\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$ [(2)]

[(2)] $\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q) \rtimes \mathbb{Z}/2\mathbb{Z}$ when $m = n$

What a wonderful world

Hamming world		**Rank world**
$\mathbb{F}_q^n$ with Hamming distance	$\longleftrightarrow$	$\mathbb{F}_q^{m\times n}$ with Rank distance
(Supports) $E \subset \{1,\dots,n\}$	$\longleftrightarrow$	either $V \subseteq \mathbb{F}_q^m$ (Column space) or $W \subseteq \mathbb{F}_q^n$ (Row space)
Cardinality	$\longleftrightarrow$	Dimension
(Isometries) $\mathfrak{S}_n \rtimes \mathbb{F}_q^\times$	$\longleftrightarrow$	$\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q)$ [(2)]
Schur product	$\longleftrightarrow$	Matrix product

(2) $\mathrm{GL}_m(\mathbb{F}_q) \times \mathrm{GL}_n(\mathbb{F}_q) \rtimes \mathbb{Z}/2\mathbb{Z}$ when $m = n$

Even better the $\mathbb{F}_{q^m}$–linear wonderful world

$\mathbb{F}_{q^m}$–linear codes come with:

Even better the $\mathbb{F}_{q^m}$–linear wonderful world

$\mathbb{F}_{q^m}$–linear codes come with:

- a releaving vector structure;

Even better the $\mathbb{F}_{q^m}$–linear wonderful world

$\mathbb{F}_{q^m}$–linear codes come with:

- a releaving vector structure;
- representations with generator and parity–check matrices;

Even better the $\mathbb{F}_{q^m}$–linear wonderful world

$\mathbb{F}_{q^m}$–linear codes come with:

- a releaving vector structure;
- representations with generator and parity–check matrices;
- a duality over $\mathbb{F}_{q^m}$ with the canonical Euclidean product;

Even better the $\mathbb{F}_{q^m}$–linear wonderful world

$\mathbb{F}_{q^m}$–linear codes come with:

- a releaving vector structure;
- representations with generator and parity–check matrices;
- a duality over $\mathbb{F}_{q^m}$ with the canonical Euclidean product;
- etc.

What a wonderful world II

Hamming world
Reed–Solomon codes

Rank metric world
Gabidulin codes

What a wonderful world II

Hamming world
Reed–Solomon codes

$x_1, \dots, x_n \in \mathbb{F}_q$ are distinct

Rank metric world
Gabidulin codes

$g_1, \dots, g_n \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$–independent

What a wonderful world II

Hamming world	**Rank metric world**
Reed–Solomon codes	*Gabidulin codes*
$x_1, \dots, x_n \in \mathbb{F}_q$ are distinct	$g_1, \dots, g_n \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$–independent
$\{(f(x_i))_{i=1}^n \ : \ f \in \mathbb{F}_q[x],\ \deg f < k\}$	$\{(P(g_i))_{i=1}^n \ : \ P \in \mathcal{L}_q,\ \deg_q P < k\}$

What a wonderful world II

Hamming world
Reed–Solomon codes

$x_1, \dots, x_n \in \mathbb{F}_q$ are distinct

$\{(f(x_i))_{i=1}^n \ : \ f \in \mathbb{F}_q[x],\ \deg f < k\}$

MDS code

Rank metric world
Gabidulin codes

$g_1, \dots, g_n \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$–independent

$\{(P(g_i))_{i=1}^n \ : \ P \in \mathcal{L}_q,\ \deg_q P < k\}$

MRD code

What a wonderful world II

Hamming world
Reed–Solomon codes

$x_1, \dots, x_n \in \mathbb{F}_q$ are distinct

$\{(f(x_i))_{i=1}^n \ : \ f \in \mathbb{F}_q[x],\ \deg f < k\}$

MDS code

Welch–Berlekamp :

corrects $\lfloor \frac{n-k}{2} \rfloor$ errors

Rank metric world
Gabidulin codes

$g_1, \dots, g_n \in \mathbb{F}_{q^m}$ are $\mathbb{F}_q$–independent

$\{(P(g_i))_{i=1}^n \ : \ P \in \mathcal{L}_q,\ \deg_q P < k\}$

MRD code

Loidreau:

corrects $\lfloor \frac{n-k}{2} \rfloor$ errors

Looks like...

"Tonight, Santa will come down the chimney and fill your boots with rank metric analogues of all Hamming metric statements, because analogy always holds"

Wrong!

Bazinga!!!

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

Yesterday's talk

Genericity of MDS property: For fixed n, k, $q \to \infty$ the density of MDS codes $\to 1$;

Yesterday's talk

Genericity of MDS property: For fixed n, k, $q \to \infty$ the density of MDS codes $\to 1$;

Genericity of the MRD property:

- **General matrix codes:** (Byrne, Ravagnani 2020)
  - For fixed m, n, k, the density for $q \to \infty$ of MRD codes is $< 1/2$.
  - For fixed q, n, k the density for $m \to \infty$ of MRD codes is $< 1/2$.

Yesterday's talk

Genericity of MDS property: For fixed n, k, $q \to \infty$ the density of MDS codes $\to 1$;

Genericity of the MRD property:

- **General matrix codes:** (Byrne, Ravagnani 2020)
  - For fixed m, n, k, the density for $q \to \infty$ of MRD codes is $< 1/2$.
  - For fixed q, n, k the density for $m \to \infty$ of MRD codes is $< 1/2$.
- $\mathbb{F}_{q^m}$**–linear codes:** (Neri, Horlemann–Trautmann, Randrianariosa, Rosenthal, 2018.)
  - For fixed q, n, k the density of $\mathbb{F}_{q^m}$–linear MRD codes for $m \to \infty$ is 1.

Finding words of weight one

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^n$ find (if exists) $\boldsymbol{c} \in \mathscr{C}$ of weight 1

Finding words of weight one

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^n$ find (if exists) $\boldsymbol{c} \in \mathscr{C}$ of weight 1

Easy! Take $\boldsymbol{H} \in \mathbb{F}_q^{(n-k)\times n}$ a parity–check matrix of $\mathscr{C}$ and solve:

$$\boldsymbol{H}\begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} = 0, \qquad \text{then,} \qquad \boldsymbol{H}\begin{pmatrix} 0 \\ x \\ \vdots \\ 0 \end{pmatrix} = 0, \qquad \cdots \qquad , \boldsymbol{H}\begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \end{pmatrix} = 0.$$

n **linear systems with one variable to solve.** (Actually just search zero columns of $\boldsymbol{H}$).

In rank metric

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^{m \times n}$ find if exists matrices $\boldsymbol{C} \in \mathscr{C}$ of rank 1.

Easy!

In rank metric

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^{m \times n}$ find if exists matrices $\boldsymbol{C} \in \mathscr{C}$ of rank 1.

~~**Easy!**~~... the problem is NP-hard.

In rank metric

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^{m \times n}$ find if exists matrices $\boldsymbol{C} \in \mathscr{C}$ of rank 1.

~~**Easy!**~~... the problem is NP-hard.

Problem

Let $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$–linear code. Find if exists $\boldsymbol{c} \in \mathscr{C}$ of rank 1.

In rank metric

Problem

Given $\mathscr{C} \subset \mathbb{F}_q^{m \times n}$ find if exists matrices $\boldsymbol{C} \in \mathscr{C}$ of rank 1.

~~**Easy!**~~... the problem is NP-hard.

Problem

Let $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$–linear code. Find if exists $\boldsymbol{c} \in \mathscr{C}$ of rank 1.

Easy! compute the subfield subcode.

Summary

	Hamming ($\dim_{\mathbb{F}_q} \mathscr{C} = k$)	**Matrix codes** ($\dim_{\mathbb{F}_q} \mathscr{C} = mk$)	$\mathbb{F}_{q^m}$**–linear codes** ($\dim_{\mathbb{F}_{q^m}} \mathscr{C} = k$)
Finding $\boldsymbol{c}$ of weight 1	Easy	Hard	Easy
Finding $\boldsymbol{c}$ of weight $t > 1$ $t = O(1)$, $n \to \infty$	$O(n^{t+\omega})$	$\widetilde{O}(q^{kt})$	$\widetilde{O}(q^{(k+1)(t-1)})$

See:

- Ourivski, Johansson 2002;
- Gaborit, Ruatta, Schrek 2013;
- Aragon, Gaborit, Hauteville, Tillich 2018.

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

McWilliams extension theorem

Theorem 1 (McWilliams, 1962)

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$. Suppose there exists a linear map $f : \mathscr{C} \to \mathscr{D}$ which preserves weights. Then f is the restriction to $\mathscr{C}$ of an isometry of $\mathbb{F}_q^n$.

McWilliams extension theorem

Theorem 1 (McWilliams, 1962)

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$. Suppose there exists a linear map $f : \mathscr{C} \to \mathscr{D}$ which preserves weights. Then f is the restriction to $\mathscr{C}$ of an isometry of $\mathbb{F}_q^n$.

- Counter examples exist for rank metric codes
  - Barra, Gluesing-Luerssen 2015;
  - Cruz, Kiermaier, Wassermann, Willems, 2016;
  - Gorla, Salizzoni, 2024.

McWilliams extension theorem

Theorem 1 (McWilliams, 1962)

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$. Suppose there exists a linear map $f : \mathscr{C} \to \mathscr{D}$ which preserves weights. Then f is the restriction to $\mathscr{C}$ of an isometry of $\mathbb{F}_q^n$.

- Counter examples exist for rank metric codes
  - Barra, Gluesing-Luerssen 2015;
  - Cruz, Kiermaier, Wassermann, Willems, 2016;
  - Gorla, Salizzoni, 2024.
- **Question:** What about $\mathbb{F}_{q^m}$–linear codes?

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

Decoding random codes

Theorem 2 (Gaborit, Ruatta, Schrek, 2013 (informal))

Let $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ be a random code of dimension k. Then, there is a polynomial–time decoder correcting $t \approx \frac{n}{k}$ errors w.h.p.

Decoding random codes

Theorem 2 (Gaborit, Ruatta, Schrek, 2013 (informal))

Let $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ be a random code of dimension k. Then, there is a polynomial–time decoder correcting $t \approx \frac{n}{k}$ errors w.h.p.

Remark

For $\mathbb{F}_q$–linear matrix codes of $\mathbb{F}_q$–dimension $K = km$, combinatorial solvers run in $\widetilde{O}(q^{kt})$.

Decoding random codes

Theorem 2 (Gaborit, Ruatta, Schrek, 2013 (informal))

Let $\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$ be a random code of dimension k. Then, there is a polynomial–time decoder correcting $t \approx \frac{n}{k}$ errors w.h.p.

Remark

For $\mathbb{F}_q$–linear matrix codes of $\mathbb{F}_q$–dimension $K = km$, combinatorial solvers run in $\widetilde{O}(q^{kt})$.

What about Hamming metric? No analog but for $kt \leqslant n$, Prange (1962) runs in $O(n^\omega)$.

Tensor products

Theorem 3

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$ with minimum distances $d_{\mathscr{C}}$ and $d_{\mathscr{D}}$, then $\mathscr{C} \otimes \mathscr{D} \subset \mathbb{F}_q^{n^2}$ has distance $d_{\mathscr{C}} d_{\mathscr{D}}$.

Tensor products

Theorem 3

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$ with minimum distances $d_{\mathscr{C}}$ and $d_{\mathscr{D}}$, then $\mathscr{C} \otimes \mathscr{D} \subset \mathbb{F}_q^{n^2}$ has distance $d_{\mathscr{C}} d_{\mathscr{D}}$.

In rank metric?

Tensor products

Theorem 3

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$ with minimum distances $d_{\mathscr{C}}$ and $d_{\mathscr{D}}$, then $\mathscr{C} \otimes \mathscr{D} \subset \mathbb{F}_q^{n^2}$ has distance $d_{\mathscr{C}} d_{\mathscr{D}}$.

In rank metric?

Take $\mathscr{C} = \mathscr{D} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then, $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes \mathscr{C}) = 2$.

Tensor products

Theorem 3

Let $\mathscr{C}, \mathscr{D} \subset \mathbb{F}_q^n$ with minimum distances $d_{\mathscr{C}}$ and $d_{\mathscr{D}}$, then $\mathscr{C} \otimes \mathscr{D} \subset \mathbb{F}_q^{n^2}$ has distance $d_{\mathscr{C}} d_{\mathscr{D}}$.

In rank metric?

Take $\mathscr{C} = \mathscr{D} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then, $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes \mathscr{C}) = 2$.

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 & -1 & 0 \\ 1 & 0 & 0 & -1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

In rank metric?

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

In rank metric?

$\mathscr{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes_{\mathbb{R}} \mathbb{C}) = 1$:

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

In rank metric?

$\mathscr{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes_{\mathbb{R}} \mathbb{C}) = 1$:

$$\mathrm{Rk} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} = 1$$

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

In rank metric?

$\mathscr{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes_{\mathbb{R}} \mathbb{C}) = 1$:

$$\mathrm{Rk} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} = 1$$

$\mathbb{F}_{q^m}$–linear codes?

Tensor product — Ground field extension

Theorem 3

Let $\mathscr{C} \subseteq \mathbb{F}_q^n$ be a code of minimum distance d. Then $\mathscr{C} \otimes \mathbb{F}_{q^\ell}$ has minimum distance d.

In rank metric?

$\mathscr{C} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ : \ a, b \in \mathbb{R} \right\}$. Then $d_{min}(\mathscr{C}) = 2$ and $d_{min}(\mathscr{C} \otimes_{\mathbb{R}} \mathbb{C}) = 1$:

$$\mathrm{Rk} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} = 1$$

$\mathbb{F}_{q^m}$–linear codes?

Given $\mathscr{C} \subset \mathbb{F}_{q^m}^n$ of distance d; $\mathscr{C}^{mat}$ its matrix version. Then, $\mathscr{C}^{mat} \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}$ has distance 1!

Explanation

In Hamming metric, $d_{min} \geqslant d$ means, $\forall I \subset \{1, \dots, n\}$, $|I| = d - 1$, the puncturing map

$$p_I : \left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ \boldsymbol{c} = (c_i)_{i=1}^n & \longmapsto & (c_i)_{i \in \{1,\dots,n\} \setminus I} \end{array} \right. \quad \text{is injective.}$$

Flatness $\implies$ $p \otimes \mathrm{Id}_{\mathbb{F}_{q^\ell}}$ is injective.

Explanation

In Hamming metric, $d_{min} \geqslant d$ means, $\forall I \subset \{1, \dots, n\}$, $|I| = d-1$, the puncturing map

$$p_I : \left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ \boldsymbol{c} = (c_i)_{i=1}^n & \longmapsto & (c_i)_{i \in \{1,\dots,n\} \setminus I} \end{array} \right. \quad \text{is injective.}$$

Flatness $\implies$ $p \otimes \mathrm{Id}_{\mathbb{F}_{q^\ell}}$ is injective.

In Rank metric, consider all the $W \subset \mathbb{F}_q^m$ s.t. $\dim W = d-1$ and the puncturing maps

$$\left\{ \begin{array}{ccc} \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m) & \longrightarrow & \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m / W) \\ f & \longmapsto & \pi \circ f \end{array} \right. , \quad \text{where} \quad \pi : \mathbb{F}_q^m \to \mathbb{F}_q^m / W$$

Explanation

In Hamming metric, $d_{min} \geqslant d$ means, $\forall I \subset \{1, \dots, n\}$, $|I| = d-1$, the puncturing map

$$p_I : \left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ \boldsymbol{c} = (c_i)_{i=1}^n & \longmapsto & (c_i)_{i \in \{1,\dots,n\} \setminus I} \end{array} \right. \quad \text{is injective.}$$

Flatness $\implies$ $p \otimes \mathrm{Id}_{\mathbb{F}_{q^\ell}}$ is injective.

In Rank metric, consider all the $W \subset \mathbb{F}_q^m$ s.t. $\dim W = d-1$ and the puncturing maps

$$\left\{ \begin{array}{ccc} \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m) & \longrightarrow & \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m/W) \\ f & \longmapsto & \pi \circ f \end{array} \right. , \quad \text{where} \quad \pi : \mathbb{F}_q^m \to \mathbb{F}_q^m/W$$

The set W's to enumerate depend on the ground field!

Explanation

In Hamming metric, $d_{min} \geqslant d$ means, $\forall I \subset \{1, \dots, n\}$, $|I| = d-1$, the puncturing map

$$p_I : \left\{ \begin{array}{ccc} \mathscr{C} & \longrightarrow & \mathbb{F}_q^{n-d+1} \\ \boldsymbol{c} = (c_i)_{i=1}^n & \longmapsto & (c_i)_{i \in \{1,\dots,n\} \setminus I} \end{array} \right. \quad \text{is injective.}$$

Flatness $\implies$ $p \otimes \mathrm{Id}_{\mathbb{F}_{q^\ell}}$ is injective. The I's do not depend on the field!

In Rank metric, consider all the $W \subset \mathbb{F}_q^m$ s.t. $\dim W = d-1$ and the puncturing maps

$$\left\{ \begin{array}{ccc} \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m) & \longrightarrow & \mathrm{Hom}(\mathbb{F}_q^n, \mathbb{F}_q^m/W) \\ f & \longmapsto & \pi \circ f \end{array} \right. , \quad \text{where} \quad \pi : \mathbb{F}_q^m \to \mathbb{F}_q^m/W$$

The set W's to enumerate depend on the ground field!

Working in groups

Question

Let $\mathscr{C} \subseteq K^{m \times n}$ a code of minimum distance d.

- *Does there exist an infinite extension L/K such that $\mathscr{C} \otimes L$ has minimum distance d?*
- *Does there exist an inifinte sequence of finite extensions L_i/K such that $[L_i : K] \to \infty$ such that $\mathscr{C} \otimes L_i$ all have minimum distance d?*

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

Preserve your mental health : don't reproduce this at home

Hamming Metric **Reed–Solomon codes** (rate R)	**Rank metric** **Gabidulin codes** (rate R)
Welch–Berlekamp $\tau = t/n = (1-R)/2$	Loidreau $\tau = t/n = (1-R)/2$
Sudan $1-\sqrt{2R}$	??
Guruswami–Sudan $1-\sqrt{R}$	??

Preserve your mental health : don't reproduce this at home

Hamming Metric **Reed–Solomon codes** (rate R)	**Rank metric** **Gabidulin codes** (rate R)
Welch–Berlekamp $\tau = t/n = (1-R)/2$	Loidreau $\tau = t/n = (1-R)/2$
Sudan $1-\sqrt{2R}$	??
Guruswami–Sudan $1-\sqrt{R}$	??

Theorem 4 (Raviv, Wachter–Zeh, 2016, informal)

There exist an $[n,k]_{q^m}$ Gabidulin code $\mathscr{C}$ and $\boldsymbol{y} \in \mathbb{F}_{q^m}^n$ at distance $t = \lfloor \frac{d-1}{2} \rfloor + 1$ from $\mathscr{C}$ such that $B(\boldsymbol{y}, t)$ contains exponentially many codewords of $\mathscr{C}$.

1. The amazing analogies with Hamming metric

2. When $\mathbb{F}_{q^m}$–linearity (seems to) save analogies
   - Is MRD structure generic?
   - Finding constant weight codewords
   - McWilliams extension Theorem

3. When there is nothing to save
   - A mysterious generic decoder
   - Tensor product
   - Preserve your mental health: no list decoding
   - Analog constructions?

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin

1

2

3

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin
Alternant, Goppa	??

1

2

3

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin
Alternant, Goppa	??
AG	??

1

2

3

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin
Alternant, Goppa	??
AG	??
Reed-Muller	Only over infinite fields[1]

[1] Augot, C., Lavauzelle, Neri, 2021

2

3

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin
Alternant, Goppa	??
AG	??
Reed-Muller	Only over infinite fields[1]
LDPC	LRPC[2]?

[1] Augot, C., Lavauzelle, Neri, 2021
[2] Gaborit, Murat, Ruatta, Zémor, 2013
[3]

Is there always an analog construction?

Hamming metric	Rank metric
Reed–Solomon	Gabidulin
Alternant, Goppa	??
AG	??
Reed-Muller	Only over infinite fields[1]
LDPC	LRPC[2]?
??	Silva-Kschischang-Kötter[3] "Simple codes"

[1] Augot, C., Lavauzelle, Neri, 2021
[2] Gaborit, Murat, Ruatta, Zémor, 2013
[3] Silva, Kschischang, Kötter, 2010

Conclusion

- Take your favorite statement/construction in Hamming metric;

Conclusion

- Take your favorite statement/construction in Hamming metric;
- Consider its adaptation to the rank metric setting (which is unknown);

Conclusion

- Take your favorite statement/construction in Hamming metric;
- Consider its adaptation to the rank metric setting (which is unknown);
- some colleague claims the analogy to be "blabla" where:

$$\text{blabla} \in \{\texttt{straightforward}, \texttt{obvious}, \texttt{trivial}\};$$

Conclusion

- Take your favorite statement/construction in Hamming metric;
- Consider its adaptation to the rank metric setting (which is unknown);
- some colleague claims the analogy to be "blabla" where:

$$\text{blabla} \in \{\texttt{straightforward}, \texttt{obvious}, \texttt{trivial}\};$$

- search for another colleague.