Rank-Metric Codes and Combinatorial Theory

Alberto Ravagnani

Eindhoven University of Technology

OPERA 2026, Bordeaux

MDS Codes

q a prime power, $n \geq 2$ an integer

Definition

A **block code** is a non-zero $\mathbb{F}_q$-subspace $C \leq \mathbb{F}_q^n$. Its **minimum (Hamming) distance** is

$$d^{\mathrm{H}}(C) = \min\{\omega^{\mathrm{H}}(x) \mid x \in C, x \neq 0\},$$

where $\omega^{\mathrm{H}}(x) = \#\{i \mid x_i \neq 0\}$ is the **Hamming weight** of $x \in \mathbb{F}_q^n$.

MDS Codes

q a prime power, $n \geq 2$ an integer

Definition

A **block code** is a non-zero $\mathbb{F}_q$-subspace $C \leq \mathbb{F}_q^n$. Its **minimum (Hamming) distance** is

$$d^{\mathrm{H}}(C) = \min\{\omega^{\mathrm{H}}(x) \mid x \in C, x \neq 0\},$$

where $\omega^{\mathrm{H}}(x) = \#\{i \mid x_i \neq 0\}$ is the **Hamming weight** of $x \in \mathbb{F}_q^n$.

Theorem (Singleton Bound)

Let $C \leq \mathbb{F}_q^n$ be k-dimensional and MDS. Then $k \leq n - d^{\mathrm{H}}(C) + 1$.

Trade-off between large dimension and large minimum distance.

Definition

C is **MDS** if the bound is attained with equality.

Most Block Codes are MDS

Theorem (Folklore)

Fix $1 \leq k \leq n$. We have

$$\lim_{q \to +\infty} \frac{\# \text{ of } k\text{-dim MDS codes in } \mathbb{F}_q^n}{\# \text{ of } k\text{-dim block codes in } \mathbb{F}_q^n} = 1.$$

In words: MDS codes are **dense** within the set of k-dimensional block codes in $\mathbb{F}_q^n$.

Most Block Codes are MDS

Theorem (Folklore)

Fix $1 \leq k \leq n$. We have

$$\lim_{q \to +\infty} \frac{\#\text{ of } k\text{-dim MDS codes in } \mathbb{F}_q^n}{\#\text{ of } k\text{-dim block codes in } \mathbb{F}_q^n} = 1.$$

In words: MDS codes are **dense** within the set of k-dimensional block codes in $\mathbb{F}_q^n$.

In the rank-metric world, the analogues of MDS codes are MRD codes.

Rank-Metric Codes

q a prime power, $m \geq n \geq 2$ integers

Definition

A **rank-metric code** is a non-zero subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum (rank) distance** is

$$d^{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(X) \mid X \in \mathscr{C}, X \neq 0\}.$$

Rank-metric codes were studied by Delsarte for combinatorial interest in 1978. They were rediscovered more than once:

- Gabidulin (1985)
- Cooperstein (1998)
- Silva, Koetter, Kschischang (2008)

Rank-Metric Codes

q a prime power, $m \geq n \geq 2$ integers

Definition

A **rank-metric code** is a non-zero subspace $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$. Its **minimum (rank) distance** is

$$d^{\mathrm{rk}}(\mathscr{C}) = \min\{\mathrm{rk}(X) \mid X \in \mathscr{C}, X \neq 0\}.$$

Rank-metric codes were studied by Delsarte for combinatorial interest in 1978. They were rediscovered more than once:

- Gabidulin (1985)
- Cooperstein (1998)
- Silva, Koetter, Kschischang (2008)

Theorem (Singleton-type Bound)

Let $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ be a rank-metric code. We have $\dim(\mathscr{C}) \leq m(n - d^{\mathrm{rk}}(\mathscr{C}) + 1)$.

Definition

$\mathscr{C}$ is **MRD** if it attains the bound with equality.

Proportion of MRD Codes

Notation

For $1 \leq d \leq n$, let $k = m(n-d+1)$ and

$$\delta_q(n \times m, d) = \frac{\#\{\mathscr{C} \leq \mathbb{F}_q^{n \times m} \mid \dim(\mathscr{C}) = k, \mathscr{C} \text{ is MRD}\}}{\#\{\mathscr{C} \leq \mathbb{F}_q^{n \times m} \mid \dim(\mathscr{C}) = k\}}$$

be the proportion of k-dimensional MRD codes within the k-dimensional rank-metric codes.

It is natural to try and imitate arguments that prove that MDS are dense, hopefully showing that

$$\lim_{q \to +\infty} \delta_q(n \times m, d) = 1.$$

Unfortunately, this approach fails.

Proportion of MRD Codes

Notation

For $1 \leq d \leq n$, let $k = m(n-d+1)$ and

$$\delta_q(n \times m, d) = \frac{\#\{\mathscr{C} \leq \mathbb{F}_q^{n \times m} \mid \dim(\mathscr{C}) = k, \mathscr{C} \text{ is MRD}\}}{\#\{\mathscr{C} \leq \mathbb{F}_q^{n \times m} \mid \dim(\mathscr{C}) = k\}}$$

be the proportion of k-dimensional MRD codes within the k-dimensional rank-metric codes.

It is natural to try and imitate arguments that prove that MDS are dense, hopefully showing that

$$\lim_{q \to +\infty} \delta_q(n \times m, d) = 1.$$

Unfortunately, this approach fails.

Note: The argument can however be applied to a subclass of rank-metric codes, called "vector rank-metric codes", for $m \to +\infty$. This was done in:
A. Neri, A.-L. Horlemann-Trautmann, T. Randrianarisoa, J. Rosenthal, *On the Genericity of Maximum Rank Distance and Gabidulin Codes*

The density function of MRD codes

Recall:

Notation

For $1 \leq d \leq n$, let $k = m(n-d+1)$ and

$$\delta_q(n \times m, d) = \frac{\#\{\mathscr{C} \leq \mathbb{F}_q^{n\times m} \mid \dim(\mathscr{C}) = k, \mathscr{C} \text{ is MRD}\}}{\#\{\mathscr{C} \leq \mathbb{F}_q^{n\times m} \mid \dim(\mathscr{C}) = k\}}.$$

Problems

1. Compute $\lim_{q\to+\infty} \delta_q(n \times m, d)$
2. Compute $\lim_{m\to+\infty} \delta_q(n \times m, d)$
3. Find upper/lower bounds for $\delta_q(n \times m, d)$

The next part of the talk is about these questions and their (partial) solutions via four different approaches. In particular:

Theorem (Gruica, R.)

MRD codes are "very" sparse as $q \to +\infty$, unless $d = 1$ or $n = d = 2$ (any $m \geq n$).

This is in strong contrast with the behaviour of MDS codes.

Approach 1: Spectrum-Free Matrices

J. Antrobus, H. Gluesing-Luerssen, *Maximal Ferrers Diagram Codes: Constructions and Genericity Considerations*.

Key observation: the m matrices

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_{11} & a_{12} & \cdots & a_{1m} \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2m} \end{pmatrix}, \quad \cdots, \quad \begin{pmatrix} 0 & 0 & \cdots & 1 \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{F}_q^{2 \times m}$$

generate an MRD code if and only if the matrix

$$(a_{ij}) \in \mathbb{F}_q^{m \times m}$$

is **spectrum-free**, i.e., it has no eigenvalues in $\mathbb{F}_q$.

Approach 1: Spectrum-Free Matrices

J. Antrobus, H. Gluesing-Luerssen, *Maximal Ferrers Diagram Codes: Constructions and Genericity Considerations.*

Key observation: the m matrices

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ a_{11} & a_{12} & \cdots & a_{1m} \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & \cdots & 0 \\ a_{21} & a_{22} & \cdots & a_{2m} \end{pmatrix}, \quad \cdots, \quad \begin{pmatrix} 0 & 0 & \cdots & 1 \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{F}_q^{2\times m}$$

generate an MRD code if and only if the matrix

$$(a_{ij}) \in \mathbb{F}_q^{m\times m}$$

is **spectrum-free**, i.e., it has no eigenvalues in $\mathbb{F}_q$. Extending the theory of spectrum-free matrices:

Theorem (Antrobus, Gluesing-Luerssen)

We have

$$\lim_{q\to+\infty} \delta_q(2\times m, 2) = \sum_{i=0}^{m} \frac{(-1)^i}{i!}, \qquad \lim_{m\to+\infty} \delta_q(2\times m, 2) = \prod_{i=1}^{\infty} \left(\frac{q^i-1}{q^i}\right)^{q(n-1)+1}.$$

These numbers are positive and strictly smaller than 1. Therefore these MRD codes are <u>neither sparse, nor dense</u>, both as $q\to+\infty$ and $m\to+\infty$.

Approach 1: Spectrum-Free Matrices

More generally,

Theorem (Antrobus, Gluesing-Luerssen)

For all $d \geq 2$,

$$\limsup_{q \to +\infty} \delta_q(n \times m, d) \leq \left(\sum_{i=0}^{m} \frac{(-1)^i}{i!} \right)^{(d-1)(n-d+1)}.$$

The number on the RHS is always positive and smaller than 1. This shows that MRD codes for $d \geq 2$ are never dense for $q \to +\infty$.

Theorem (Antrobus, Gluesing-Luerssen)

For all $d \geq 2$,

$$\limsup_{m \to +\infty} \delta_q(n \times m, d) \leq \prod_{i=1}^{\infty} \left(\frac{q^i - 1}{q^i} \right)^{q(d-1)(n-d+1)+1}.$$

Again, the number on the RHS is always positive and smaller than 1. This shows that MRD codes for $d \geq 2$ are never dense for $m \to +\infty$.

Approach 2: Partition-Balanced Families of Codes

E. Byrne, A. R., *Partition-Balanced Families of Codes and Asymptotic Enumeration in Coding Theory*.

Machinery to study asymptotic enumeration problems in coding theory, in relation to:

- maximality,
- extremality with respect to bounds,
- covering radius,
- average parameters of codes,
- ...

Approach 2: Partition-Balanced Families of Codes

E. Byrne, A. R., *Partition-Balanced Families of Codes and Asymptotic Enumeration in Coding Theory.*

Machinery to study asymptotic enumeration problems in coding theory, in relation to:

- maximality,
- extremality with respect to bounds,
- covering radius,
- average parameters of codes,
- ...

We apply this to estimate the number of MRD codes:

Theorem (Byrne, R.)

Let $2 \leq d \leq n$ and $k = m(n-d+1)$. There are at least

$$q\left(\sum_{h=1}^{m(n-k)} \begin{bmatrix} t \\ h \end{bmatrix} \sum_{s=h}^{m(n-k)} \begin{bmatrix} m(n-k)-h \\ s-h \end{bmatrix} \begin{bmatrix} mn-s \\ mn-k \end{bmatrix} (-1)^{s-h} q^{\binom{s-h}{2}}\right)\left(1 - \frac{(q^k-1)(q^{mn-k}-1)}{2(q^{mn}-q^{mn-k})}\right)$$

k-dimensional non-MRD codes in $\mathbb{F}_q^{n\times m}$.

The asymptotics of this formula can be explicitly computed.

Approach 2: Partition-Balanced Families of Codes

Corollary (Byrne, R.)

Let $2 \leq d \leq n$. Then

$$\limsup_{q \to +\infty} \delta_q(n \times m, d) \leq \frac{1}{2}.$$

This also shows that MRD codes are never dense for $q \to +\infty$ if $d \geq 2$.

Corollary (Byrne, R.)

Let $2 \leq d \leq n$. Then

$$\limsup_{m \to +\infty} \delta_q(n \times m, d) \leq \frac{(q-1)(q-2)+1}{2(q-1)^2}.$$

Same story: MRD codes are never dense for $m \to +\infty$ if $d \geq 2$.

Corollary (Byrne, R.)

Let $2 \leq d \leq n$. Then

$$\limsup_{q \to +\infty} \delta_q(n \times m, d) \leq \frac{1}{2}.$$

This also shows that MRD codes are never dense for $q \to +\infty$ if $d \geq 2$.

Corollary (Byrne, R.)

Let $2 \leq d \leq n$. Then

$$\limsup_{m \to +\infty} \delta_q(n \times m, d) \leq \frac{(q-1)(q-2)+1}{2(q-1)^2}.$$

Same story: MRD codes are never dense for $m \to +\infty$ if $d \geq 2$.

Summary so far

- MRD codes are never dense, unless $d = 1$, both for $q \to +\infty$ and $m \to +\infty$.
- For $d = n = 2$, MRD codes are neither sparse, nor dense (both for q and m large).

Approach 3: Theory of Semifields

H. Gluesing Luerssen, *On the Sparseness of Certain MRD Codes*

This paper contains a highly specialized machinery for the 3×3 full-rank MRD codes.

- Step 1: identify well-behaved bases for such MRD codes;
- Step 2: count such bases using enumerative results on semifields.

Theorem (Gluesing-Luerssen)

$$\delta_q(3 \times 3, 3) = \frac{(q-1)(q^3-1)(q^3-q)^3(q^3-q^2)^2(q^3-q^2-q-1)}{3(q^7-1)(q^9-1)(q^9-q)}.$$

Since $\delta_q(3 \times 3, 3) \sim \frac{1}{3}q^{-3}$ as $q \to +\infty$, the 3×3 full-rank MRD codes are sparse for q large.

Approach 3: Theory of Semifields

H. Gluesing Luerssen, *On the Sparseness of Certain MRD Codes*

This paper contains a highly specialized machinery for the 3×3 full-rank MRD codes.

- Step 1: identify well-behaved bases for such MRD codes;
- Step 2: count such bases using enumerative results on semifields.

Theorem (Gluesing-Luerssen)

$$\delta_q(3 \times 3, 3) = \frac{(q-1)(q^3-1)(q^3-q)^3(q^3-q^2)^2(q^3-q^2-q-1)}{3(q^7-1)(q^9-1)(q^9-q)}.$$

Since $\delta_q(3 \times 3, 3) \sim \frac{1}{3} q^{-3}$ as $q \to +\infty$, the 3×3 full-rank MRD codes are sparse for q large.

Update

- MRD codes are never dense, unless $d = 1$, both for $q \to +\infty$ and $m \to +\infty$.
- For $d = n = 2$, MRD codes are neither sparse, nor dense.
- **New!** 3×3 full-rank MRD codes are sparse as $q \to +\infty$.
- Arguments don't reveal the difference between $n = d = 2$ and the other cases.

A. Gruica, A. R., *Common Complements of Linear Subspaces and the Sparseness of MRD Codes.*

Refining the methods described so far seems unfeasible $\rightarrow$ look for a different viewpoint.

Recall: Let $\mathscr{X}$ be a linear space and let $\mathscr{C}, \mathscr{D} \leq \mathscr{X}$ be subspaces. Then $\mathscr{D}$ is a **complement** of $\mathscr{C}$ if $\mathscr{C} \cap \mathscr{D} = \{0\}$ and $\mathscr{C} + \mathscr{D} = \mathscr{X}$ (lattice theory).

Approach 4: Extremal Combinatorics

A. Gruica, A. R., *Common Complements of Linear Subspaces and the Sparseness of MRD Codes.*

Refining the methods described so far seems unfeasible $\rightarrow$ look for a different viewpoint.

Recall: Let $\mathscr{X}$ be a linear space and let $\mathscr{C}, \mathscr{D} \leq \mathscr{X}$ be subspaces. Then $\mathscr{D}$ is a **complement** of $\mathscr{C}$ if $\mathscr{C} \cap \mathscr{D} = \{0\}$ and $\mathscr{C} + \mathscr{D} = \mathscr{X}$ (lattice theory).

Remark

- Let $\mathscr{U}$ be the set of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathscr{U}$, denote by $\mathbb{F}_q^{n\times m}(U)$ the set of matrices $X \in \mathbb{F}_q^{n\times m}$ whose column space is contained in U.
  Note: $\mathbb{F}_q^{n\times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathscr{U}$.

Approach 4: Extremal Combinatorics

A. Gruica, A. R., *Common Complements of Linear Subspaces and the Sparseness of MRD Codes.*

Refining the methods described so far seems unfeasible $\rightarrow$ look for a different viewpoint.

Recall: Let $\mathscr{X}$ be a linear space and let $\mathscr{C}, \mathscr{D} \leq \mathscr{X}$ be subspaces. Then $\mathscr{D}$ is a **complement** of $\mathscr{C}$ if $\mathscr{C} \cap \mathscr{D} = \{0\}$ and $\mathscr{C} + \mathscr{D} = \mathscr{X}$ (lattice theory).

Remark

- Let $\mathscr{U}$ be the set of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathscr{U}$, denote by $\mathbb{F}_q^{n\times m}(U)$ the set of matrices $X \in \mathbb{F}_q^{n\times m}$ whose column space is contained in U.
  Note: $\mathbb{F}_q^{n\times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathscr{U}$.

- We let $\mathscr{A} = \{\mathbb{F}_q^{n\times m}(U) \mid U \in \mathscr{U}\}$. Then the common complements of the spaces in $\mathscr{A}$ are exactly the MRD codes $\mathscr{C} \leq \mathbb{F}_q^{n\times m}$ with $d^{\mathrm{rk}}(\mathscr{C}) = d$.

A. Gruica, A. R., *Common Complements of Linear Subspaces and the Sparseness of MRD Codes.*

Refining the methods described so far seems unfeasible $\to$ look for a different viewpoint.

Recall: Let $\mathscr{X}$ be a linear space and let $\mathscr{C}, \mathscr{D} \leq \mathscr{X}$ be subspaces. Then $\mathscr{D}$ is a **complement** of $\mathscr{C}$ if $\mathscr{C} \cap \mathscr{D} = \{0\}$ and $\mathscr{C} + \mathscr{D} = \mathscr{X}$ (lattice theory).

Remark

- Let $\mathscr{U}$ be the set of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathscr{U}$, denote by $\mathbb{F}_q^{n \times m}(U)$ the set of matrices $X \in \mathbb{F}_q^{n \times m}$ whose column space is contained in U.
  Note: $\mathbb{F}_q^{n \times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathscr{U}$.

- We let $\mathscr{A} = \{\mathbb{F}_q^{n \times m}(U) \mid U \in \mathscr{U}\}$. Then the common complements of the spaces in $\mathscr{A}$ are exactly the MRD codes $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ with $d^{\mathrm{rk}}(\mathscr{C}) = d$.

- $|\mathscr{A}| = |\mathscr{U}| = \begin{bmatrix} n \\ d-1 \end{bmatrix}_q \sim q^{(d-1)(n-d+1)}$ as $q \to +\infty$.

We investigate the following general question:

Problem

- Let $\mathscr{X}$ be a linear space over $\mathbb{F}_q$ of dimension $N \geq 3$.
- Fix $1 \leq k \leq N-1$.
- Let $\mathscr{A}$ be a collection of $(n-k)$-subspaces of $\mathscr{X}$.

Estimate the number of common complements of the spaces in $\mathscr{A}$, in terms of some properties of $\mathscr{A}$.

In this talk: applications to MRD codes

In our paper: the problem in general (and MRD codes as a special example)

Approach 4: Extremal Combinatorics

We use some graph theory.

Definition

A **bipartite graph** is a 3-tuple $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$, where:

- $\mathscr{V}$, $\mathscr{W}$ are finite non-empty sets (vertices);
- $\mathscr{E} \subseteq \mathscr{V} \times \mathscr{W}$ (edges).

We say that:

- $W \in \mathscr{W}$ is **isolated** if there is no $V \in \mathscr{V}$ with $(V, W) \in \mathscr{E}$;
- $\mathscr{B}$ is **left-regular** of **degree** ∂ if, for all $V \in \mathscr{V}$, $\partial = |\{W \in \mathscr{W} \mid (V, W) \in \mathscr{E}\}|$.

<u>Task</u>: say something about the isolated and non-isolated vertices.

Approach 4: Extremal Combinatorics

We use some graph theory.

Definition

A **bipartite graph** is a 3-tuple $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$, where:

- $\mathscr{V}$, $\mathscr{W}$ are finite non-empty sets (vertices);
- $\mathscr{E} \subseteq \mathscr{V} \times \mathscr{W}$ (edges).

We say that:

- $W \in \mathscr{W}$ is **isolated** if there is no $V \in \mathscr{V}$ with $(V, W) \in \mathscr{E}$;
- $\mathscr{B}$ is **left-regular** of **degree** ∂ if, for all $V \in \mathscr{V}$, $\partial = |\{W \in \mathscr{W} \mid (V, W) \in \mathscr{E}\}|$.

Task: say something about the isolated and non-isolated vertices.

Lemma

Let $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ be a bipartite and left-regular graph of degree $\partial > 0$. Let $\mathscr{F} \subseteq \mathscr{W}$ be the collection of non-isolated vertices of $\mathscr{W}$. We have

$$|\mathscr{F}| \leq |\mathscr{V}|\partial.$$

This gives us an upper bound for the non-isolated vertices.

Definition

Let $\mathscr{V}$ be a finite non-empty set and let $r \geq 0$ be an integer. An **association** on $\mathscr{V}$ of **magnitude** r is a function $\alpha : \mathscr{V} \times \mathscr{V} \to \{0, \dots, r\}$ such that:

1. $\alpha(V, V) = r$ for all $V \in \mathscr{V}$;
2. $\alpha(V, V') = \alpha(V', V)$ for all $V, V' \in \mathscr{V}$.

Definition

Let $\mathscr{V}$ be a finite non-empty set and let $r \geq 0$ be an integer. An **association** on $\mathscr{V}$ of **magnitude** r is a function $\alpha : \mathscr{V} \times \mathscr{V} \to \{0, \dots, r\}$ such that:

1. $\alpha(V, V) = r$ for all $V \in \mathscr{V}$;
2. $\alpha(V, V') = \alpha(V', V)$ for all $V, V' \in \mathscr{V}$.

Let $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ be a finite bipartite graph and let α an association on $\mathscr{V}$. We say that $\mathscr{B}$ is α-**regular** if for all $(V, V') \in \mathscr{V} \times \mathscr{V}$ the number

$$|\{W \in \mathscr{W} \mid (V, W), (V', W) \in \mathscr{E}\}|$$

only depends on $\alpha(V, V')$. We denote this number by $\mathscr{W}_\ell(\alpha)$, where $\ell = \alpha(V, V')$.

Approach 4: Extremal Combinatorics

Definition

Let $\mathscr{V}$ be a finite non-empty set and let $r \geq 0$ be an integer. An **association** on $\mathscr{V}$ of **magnitude** r is a function $\alpha : \mathscr{V} \times \mathscr{V} \to \{0, ..., r\}$ such that:

1. $\alpha(V, V) = r$ for all $V \in \mathscr{V}$;
2. $\alpha(V, V') = \alpha(V', V)$ for all $V, V' \in \mathscr{V}$.

Let $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ be a finite bipartite graph and let α an association on $\mathscr{V}$. We say that $\mathscr{B}$ is α-**regular** if for all $(V, V') \in \mathscr{V} \times \mathscr{V}$ the number

$$|\{W \in \mathscr{W} \mid (V, W), (V', W) \in \mathscr{E}\}|$$

only depends on $\alpha(V, V')$. We denote this number by $\mathscr{W}_\ell(\alpha)$, where $\ell = \alpha(V, V')$.

Lemma (Gruica, R.)

Let $\mathscr{B} = (\mathscr{V}, \mathscr{W}, \mathscr{E})$ be a finite bipartite α-regular graph, where α is an association on $\mathscr{V}$ of magnitude r. Let $\mathscr{F} \subseteq \mathscr{W}$ be the collection of non-isolated right-vertices.
If $\mathscr{W}_r(\alpha) > 0$, then

$$|\mathscr{F}| \geq \frac{\mathscr{W}_r(\alpha)^2 \, |\mathscr{V}|^2}{\sum_{\ell=0}^{r} \mathscr{W}_\ell(\alpha) \, |\alpha^{-1}(\ell)|}.$$

Recall:

Remark

- Let $\mathscr{U}$ be the set of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathscr{U}$, denote by $\mathbb{F}_q^{n \times m}(U)$ the set of matrices $X \in \mathbb{F}_q^{n \times m}$ whose column space is contained in U.
  Note: $\mathbb{F}_q^{n \times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathscr{U}$.
- We let $\mathscr{A} = \{\mathbb{F}_q^{n \times m}(U) \mid U \in \mathscr{U}\}$. Then the common complements of the spaces in $\mathscr{A}$ are exactly the MRD codes $\mathscr{C} \leq \mathbb{F}_q^{n \times m}$ with $d^{\mathrm{rk}}(\mathscr{C}) = d$.
- $|\mathscr{A}| = |\mathscr{U}| = \begin{bmatrix} n \\ d-1 \end{bmatrix}_q \sim q^{(d-1)(n-d+1)}$ as $q \to +\infty$.

Fix q, n, m, d. As left-vertices take the spaces of the form $\mathbb{F}_q^{n \times m}(U)$, where $\dim(U) = d-1$.

As right-vertices take the subspaces $\mathscr{C}$ of $\mathbb{F}_q^{n \times m}$ of dimension $m(n-d+1)$.

Connect $\mathbb{F}_q^{n \times m}(U)$ to $\mathscr{C}$ if they intersect nontrivially. Then the right-isolated vertices are the MRD codes of distance d.

We apply the machinery to MRD codes:

Theorem (Gruica, R.)

Suppose $d \geq 2$ and let $k = m(n-d+1)$. We have

$$\delta_q(n \times m, d) \leq 1 - \frac{\begin{bmatrix} n \\ d-1 \end{bmatrix}_q^2 v_q(mn, k, m(d-1))^2}{\begin{bmatrix} mn \\ k \end{bmatrix}_q \sum_{i=0}^{d-1} v_q(mn, k, mi) \sum_{j=i}^{d-1} (-1)^{j-i} q^{\binom{j-i}{2}} \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{bmatrix} n-i \\ j-i \end{bmatrix}_q \begin{bmatrix} n-j \\ d-1-j \end{bmatrix}_q^2},$$

where

$$v_q(N, k, \ell) = \begin{bmatrix} N \\ k \end{bmatrix}_q - 2q^{k(N-k)} + q^{(2k-N+\ell)(N-k)} \prod_{i=\ell}^{N-k-1} (q^{N-k} - q^i).$$

Approach 4: Extremal Combinatorics

Theorem (Gruica, R.)

We have

$$\delta_q(n \times m, d) \in O\left(q^{-(d-1)(n-d+1)+1}\right) \quad \text{as } q \to +\infty.$$

Therefore, MRD codes are almost always very sparse.

Corollary (Antrobus, Gluesing-Luerssen, Gruica, R.)

$$\lim_{q \to +\infty} \delta_q(n \times m, d) = \begin{cases} 1 & \text{if } d = 1, \\ \sum_{i=0}^{m} \frac{(-1)^i}{i!} & \text{if } n = d = 2, \\ 0 & \text{otherwise.} \end{cases}$$

This computes the asymptotic density of MRD codes as $q \to +\infty$ for all parameters.

The number of $n \times n$ full-rank MRD codes

Using the theory of semifields:

Theorem (Gruica, R., Sheekey, Zullo)

The number of full-rank MRD codes $\mathscr{C} \leq \mathbb{F}_q^{n \times n}$ is at least

$$\frac{|\mathrm{GL}_n(q)|^2}{n(q^n-1)^2}\left(1+\binom{n-1}{2}\frac{(q^n-1)(q-2)}{q-1}\right).$$

Moreover, the bound is sharp for n prime and q sufficiently large (and for any q if $n=3$).

This recovers the sparseness result for 3×3 full-rank MRD codes by Gluesing-Luerssen.

Exact Counts

Counting is harder than estimating.

Natural structures to consider to this end are posets.

The Critical Problem (Crapo&Rota, 1970)

Let $\mathscr{A} \subseteq \mathscr{G}_q(X,1)$, where X is an $\mathbb{F}_q$-space.

Let $\mathscr{L}$ be the lattice of subspaces of X that are spanned by some elements of $\mathscr{A}$, ordered by inclusion $\leq$.

Proposition (Folklore)

$\mathscr{L}$ is a geometric lattice and its rank function is the $\mathbb{F}_q$-dimension of spaces.

The ith **Whitney number** of $\mathscr{L}$ is

$$w_i(\mathscr{L}) = \sum_{\substack{V \in \mathscr{L} \\ \dim(V)=i}} \mu_{\mathscr{L}}(V).$$

The **characteristic polynomial** of $\mathscr{L}$ is

$$\chi(\mathscr{L},\lambda) = \sum_i w_i(\mathscr{L}) \lambda^{\mathrm{rk}(\mathscr{L})-i} \in \mathbb{Z}[\lambda].$$

Theorem (Crapo&Rota, 1970)

The largest k for which there exists a k-subspace of X *avoiding* all the elements of $\mathscr{A}$ is

$$\mathrm{rk}(\mathscr{L}) - \min\{r \mid \chi(\mathscr{L},q^r) \neq 0\}.$$

The value of the minimum is called **critical exponent**.

The Critical Problem (Crapo&Rota, 1970)

Refining the result of Crapo&Rota:

Theorem (R.)

The following are *equivalent*:

- (partial) knowledge of the number of "avoiders"
- (partial) knowledge of the Whitney numbers

More precisely, let $\alpha_k(\mathscr{A}) = \#\{\mathscr{C} \le X \mid \dim(\mathscr{C}) = k,\, \mathscr{C} \cap L = \{0\} \text{ for all } L \in \mathscr{A}\}$. Then

$$\alpha_k(\mathscr{A}) = \sum_{i=0}^{k} w_i(\mathscr{L}) \begin{bmatrix} N-i \\ k-i \end{bmatrix}_q \quad \text{for } 0 \le k \le N,$$

$$w_i(\mathscr{L}) = \sum_{k=0}^{i} \alpha_k(\mathscr{A}) \begin{bmatrix} N-k \\ i-k \end{bmatrix}_q (-1)^{i-k} q^{\binom{i-k}{2}} \quad \text{for } 0 \le i \le N.$$

The Critical Problem and Coding Theory

Having large minimum distance is an "avoiding-type" property:

Remark

Let $X = \mathbb{F}_q^n$ and let $2 \leq d \leq n$.

Let $\mathscr{A}$ be the collection of 1-dimensional subspaces of $\mathbb{F}_q^n$ generated by a vector of Hamming weight $< d$.

Then the avoiders of $\mathscr{A}$ are the codes $\mathscr{C} \leq \mathbb{F}_q^n$ of minimum Hamming distance $\geq d$.

The lattices that correspond to Hamming-metric codes are called **higher-weight Dowling lattices** ($\sim$ 1970).

Notation

$\mathscr{H}(q,n,r)$ is the lattice of subspaces of $\mathbb{F}_q^n$ that are generated by some vectors of Hamming weight $\leq r$. The ith Whitney number is $w_i(q,n,j)$.

The techniques for computing the Whitney numbers of these lattices have not been discovered yet $\rightarrow$ open problem, equivalent to counting codes.

Formulas can be nasty...

Theorem (R.)

For all $n \geq 9$ we have

$$-w_3(2,n,3) = \sum_{1 \leq \ell_1 < \ell_2 < \ell_3 \leq n-2} \left(\prod_{j=1}^{3} \binom{n-\ell_j-9+3j}{2} \right) + 8\binom{n}{3} \sum_{s=3}^{8} \binom{n-3}{n-s} (-1)^{s-3}$$
$$+ 106\binom{n}{4} \sum_{s=4}^{8} \binom{n-4}{n-s} (-1)^{s-4} + 820\binom{n}{5} \sum_{s=5}^{8} \binom{n-5}{n-s} (-1)^{s-5}$$
$$+ 4565\binom{n}{6} \sum_{s=6}^{8} \binom{n-6}{n-s} (-1)^{s-6}$$
$$+ 19810\binom{n}{8} \sum_{s=7}^{8} \binom{n-7}{n-s} (-1)^{s-7} + 70728\binom{n}{8}.$$

Higher-Weight Dowling Lattices

For some parameters, Bernoulli numbers show up:

Theorem (R.)

For all integers $n \geq d \geq 2$ and any prime power q,

$$w_2(q,n,d) = (q^{n-1}-1)\sum_{j=1}^{d}\binom{n}{j}(q-1)^{j-2} - \sum_{1\leq \ell_1<\ell_2\leq n}\Bigg[q^{n-\ell_1-1}\left(\sum_{j=0}^{d-1}\binom{n-\ell_2}{j}(q-1)^j\right)$$
$$+\sum_{j=d}^{n-\ell_2}\sum_{h=0}^{d-1}\binom{n-\ell_2}{j}\binom{n-\ell_1-1}{h}(q-1)^{j+h}$$
$$+\sum_{s=d}^{n-\ell_2}\sum_{t=0}^{d-2}\binom{n-\ell_2}{s}\binom{n-\ell_1-1-s}{t}(q-1)^{s+t}\sum_{\nu=d-t}^{s}\gamma_q(s,s-d+t+2,\nu)\Bigg],$$

where the $\gamma_a(b,c,\nu)$'s are the *agreement numbers*.

$\gamma_a(b,c,\nu)$ is a polynomial in a (for any b, c and ν) whose coefficients are expressions involving the Bernoulli numbers:

$$\frac{x}{e^x-1} = \sum_{n=0}^{+\infty} B_n \frac{x^n}{n!}.$$

$\rightarrow$ polynomiality in q.

A Long-Term Effort

Dowling, *Codes, Packing and the Critical Problem*, 1973.

Dowling, *A q-analogue of the partition lattice*, 1973.

Zaslawsky, *The Mœbius function and the characteristic polynomial*, 1987.

Bonin, *Automorphism Groups of Higher-weight Dowling Geometries*, 1993.

Bonin, *Modular Elements of Higher-Weight Dowling Lattices*, 1993.

R., *Whitney Numbers of Combin. Geometries and Higher-Weight Dowling Lattices*, 2022.

Zaslavsky, *Whitney Numbers of Partial Dowling Lattices*, 2024.

Rank-Metric Lattices

Take the lattice $\mathscr{L}$ generated by vectors in $\mathbb{F}_{q^m}^n$ of rank weight $\leq d-1$.

Cotardo, R., *Rank-Metric Lattices*.

Counting codes of minimum rank-metric distance $\geq d$ is the same as computing the Whitney numbers of $\mathscr{L}$.

Cotardo, R., Zullo, *Whitney Numbers of Rank-Metric Lattices and Code Enumeration*.

Theorem (Cotardo, R., Zullo)

The density of MRD codes in $\mathbb{F}_{2^m}^m$ of dimension 2 is

$$\frac{2^{m^2}\varphi(m)\prod_{j=1}^m\left(1-\frac{1}{2^j}\right)(2^{2m}-1)}{(2^{m^2}-1)(2^{m^2-m}-1)} \in \mathscr{O}\left(m2^{-m^2+3m}\right) \text{ as } m \to +\infty,$$

where φ is Euler's totient function.

This Week (tentatively)

Dimension-Invariants of (Sum-)Rank-Metric Codes and Applications.

Some quantities are the same for all (nondegenerate) codes with a given dimension. E.g., the *total weight* of a Hamming-metric code $\rightarrow$ Plotkin Bound, minimal codes, ...

Alfarano, Borello, Neri, R., *Three Combinatorial Perspectives on Minimal Codes*

Some quantities aren't. For instance, the weight distribution.

A systematic study of these invariant quantities was never done for (sum-)rank-metric codes. Potential applications: bounds, distinguishers.

Dimension-Invariants of (Sum-)Rank-Metric Codes and Applications.

Some quantities are the same for all (nondegenerate) codes with a given dimension. E.g., the *total weight* of a Hamming-metric code $\rightarrow$ Plotkin Bound, minimal codes, ...

Alfarano, Borello, Neri, R., *Three Combinatorial Perspectives on Minimal Codes*

Some quantities aren't. For instance, the weight distribution.

A systematic study of these invariant quantities was never done for (sum-)rank-metric codes. Potential applications: bounds, distinguishers.

Thanks!