The Typical Code over a Large Alphabet

Alberto Ravagnani

Eindhoven University of Technology

UMI – MathCifris

joint work with Anina Gruica

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

We say that C is **MDS** if the bound is attained with equality.

Most Block Codes are MDS

Theorem (Folklore)

Fix $1 \leq k \leq n$ and let $C \leq \mathbb{F}_q^n$ be a uniformly random block code of dimension k. We have

$$\lim_{q \to +\infty} \mathbb{P}\left[C \text{ is MDS}\right] = 1.$$

Most Block Codes are MDS

Theorem (Folklore)

Fix $1 \leq k \leq n$ and let $C \leq \mathbb{F}_q^n$ be a uniformly random block code of dimension k. We have

$$\lim_{q \to +\infty} \mathbb{P}\left[C \text{ is MDS}\right] = 1.$$

One way to see this is to use the following observation:

Proposition

Let $G \in \mathbb{F}_q^{k \times n}$ be a matrix. The following are equivalent:

1. the rows of G generate a k-dimensional MDS code;
2. all the $k \times k$ minors of G are non-zero (in particular, $\text{pivots}(G) = \{1, \dots, k\}$).

Most Block Codes are MDS

Consider a matrix of the form $G = (I_k \mid Y)$, where Y is a $k \times (n-k)$ matrix of independent variables $(z_i \mid 1 \leq i \leq N)$ and $N = k(n-k)$.

$$\text{e.g.} \qquad \begin{pmatrix} 1 & 0 & z_1 & z_2 & z_3 & z_4 \\ 0 & 1 & z_5 & z_6 & z_7 & z_8 \end{pmatrix} \qquad N = 8$$

Most Block Codes are MDS

Consider a matrix of the form $G = (I_k \mid Y)$, where Y is a $k \times (n-k)$ matrix of independent variables $(z_i \mid 1 \leq i \leq N)$ and $N = k(n-k)$.

$$\text{e.g.} \qquad \begin{pmatrix} 1 & 0 & z_1 & z_2 & z_3 & z_4 \\ 0 & 1 & z_5 & z_6 & z_7 & z_8 \end{pmatrix} \qquad N = 8$$

Let $p_1, \dots, p_M \in \mathbb{F}_q[z_1, \dots, z_N]$ be the maximal minors of G, where $M = \binom{n}{k}$. The MDS codes correspond to the vectors $(\alpha_1, \dots, \alpha_N) \in \mathbb{F}_q^N$ with

$$(p_1 p_2 \cdots p_M)(\alpha_1, \dots, \alpha_N) \neq 0.$$

Most Block Codes are MDS

Consider a matrix of the form $G = (I_k \mid Y)$, where Y is a $k \times (n-k)$ matrix of independent variables $(z_i \mid 1 \leq i \leq N)$ and $N = k(n-k)$.

$$\text{e.g.} \qquad \begin{pmatrix} 1 & 0 & z_1 & z_2 & z_3 & z_4 \\ 0 & 1 & z_5 & z_6 & z_7 & z_8 \end{pmatrix} \qquad N = 8$$

Let $p_1, \ldots, p_M \in \mathbb{F}_q[z_1, \ldots, z_N]$ be the maximal minors of G, where $M = \binom{n}{k}$. The MDS codes correspond to the vectors $(\alpha_1, \ldots, \alpha_N) \in \mathbb{F}_q^N$ with

$$(p_1 p_2 \cdots p_M)(\alpha_1, \ldots, \alpha_N) \neq 0.$$

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1, \ldots, \alpha_N) \in \mathbb{F}_q^N$ of a nonzero polynomial $p := p_1 p_2 \cdots p_M \in \mathbb{F}_q[z_1, \ldots, z_N]$.

Most Block Codes are MDS

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1, \dots, \alpha_N) \in \mathbb{F}_q^N$ of a nonzero polynomial $p := p_1 p_2 \cdots p_M \in \mathbb{F}_q[z_1, \dots, z_N]$.

Note: $\deg(p) \leq kM = k\binom{n}{k}$

Most Block Codes are MDS

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1,\dots,\alpha_N)\in\mathbb{F}_q^N$ of a nonzero polynomial $p := p_1p_2\cdots p_M \in \mathbb{F}_q[z_1,\dots,z_N]$.

Note: $\deg(p) \leq kM = k\binom{n}{k}$

Using the Schwartz-Zippel Lemma: the number of such non-zeros is at least

$$q^N\left(1-q^{-1}kM\right) \;=\; q^{k(n-k)}\left(1-\frac{k}{q}\binom{n}{k}\right)$$

Most Block Codes are MDS

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1, \dots, \alpha_N) \in \mathbb{F}_q^N$ of a nonzero polynomial $p := p_1 p_2 \cdots p_M \in \mathbb{F}_q[z_1, \dots, z_N]$.

Note: $\deg(p) \leq kM = k\binom{n}{k}$

Using the Schwartz-Zippel Lemma: the number of such non-zeros is at least

$$q^N \left(1 - q^{-1} kM\right) = q^{k(n-k)} \left(1 - \frac{k}{q}\binom{n}{k}\right)$$

and therefore

$$\frac{\#\text{ of } k\text{-dim MDS codes in } \mathbb{F}_q^n}{\#\text{ of } k\text{-dim codes in } \mathbb{F}_q^n} \geq \frac{q^{k(n-k)} \left(1 - \frac{k}{q}\binom{n}{k}\right)}{\begin{bmatrix} n \\ k \end{bmatrix}_q}$$

Most Block Codes are MDS

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1,\dots,\alpha_N) \in \mathbb{F}_q^N$ of a nonzero polynomial $p := p_1 p_2 \cdots p_M \in \mathbb{F}_q[z_1,\dots,z_N]$.

Note: $\deg(p) \le kM = k\binom{n}{k}$

Using the Schwartz-Zippel Lemma: the number of such non-zeros is at least

$$q^N\left(1 - q^{-1}kM\right) \;=\; q^{k(n-k)}\left(1 - \frac{k}{q}\binom{n}{k}\right)$$

and therefore

$$\lim_{q \to +\infty} \frac{\#\text{ of } k\text{-dim MDS codes in } \mathbb{F}_q^n}{\#\text{ of } k\text{-dim codes in } \mathbb{F}_q^n} \quad \ge \quad \lim_{q \to +\infty} \frac{q^{k(n-k)}\left(1 - \frac{k}{q}\binom{n}{k}\right)}{\begin{bmatrix} n \\ k \end{bmatrix}_q}$$

Most Block Codes are MDS

Claim

The k-dimensional MDS codes in $\mathbb{F}_q^n$ correspond to the non-zeros $(\alpha_1, \ldots, \alpha_N) \in \mathbb{F}_q^N$ of a nonzero polynomial $p := p_1 p_2 \cdots p_M \in \mathbb{F}_q[z_1, \ldots, z_N]$.

<u>Note</u>: $\deg(p) \leq kM = k\binom{n}{k}$

Using the Schwartz-Zippel Lemma: the number of such non-zeros is at least

$$q^N \left(1 - q^{-1} kM\right) \; = \; q^{k(n-k)} \left(1 - \frac{k}{q}\binom{n}{k}\right)$$

and therefore

$$\lim_{q \to +\infty} \frac{\#\text{ of } k\text{-dim MDS codes in } \mathbb{F}_q^n}{\#\text{ of } k\text{-dim codes in } \mathbb{F}_q^n} \quad \geq \quad \lim_{q \to +\infty} \frac{q^{k(n-k)} \left(1 - \frac{k}{q}\binom{n}{k}\right)}{\begin{bmatrix} n \\ k \end{bmatrix}_q} \; = \; 1$$

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

We say that $\mathscr{C}$ 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 would be natural to imitate what we did for MDS codes (with the Schwartz-Zippel lemma) and hopefully prove that

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

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 would be natural to imitate what we did for MDS codes (with the Schwartz-Zippel lemma) and hopefully prove 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 would be natural to imitate what we did for MDS codes (with the Schwartz-Zippel lemma) and hopefully prove 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*

What this talk is about

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.

What this talk is about

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

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

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 these matrices and studying their asymptotic properties:

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 neither sparse, nor dense, 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

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

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 $d \geq 2$.

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 $d \geq 2$.

Summary

- 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 builds a highly specialized weapon 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.

The argument is technical, but the final result is very clean:

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 <u>sparse</u> for q large.

Approach 3: Theory of Semifields

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

This paper builds a highly specialized weapon 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.

The argument is technical, but the final result is very clean:

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.

Summary

- 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.

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).

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 $d^{\mathrm{rk}}(\mathscr{C}) = d$.

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

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)

We use a bit of 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** (or **in quarantine**) 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.

Approach 4: Extremal Combinatorics

We use a bit of 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** (or **in quarantine**) 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 $\alpha : \mathscr{V} \times \mathscr{V} \to \{0, \ldots, r\}$ 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 $\alpha : \mathscr{V} \times \mathscr{V} \to \{0, \ldots, r\}$ 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 vertices. If $\mathscr{W}_r(\alpha) > 0$, then

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

We apply the machinery to our 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 $\mathscr{A}$.

Approach 4: Extremal Combinatorics

We apply the machinery to our 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 $\mathscr{A}$.

- $\mathscr{B} = (\mathscr{A}, \mathscr{W}, \mathscr{E})$ is a bipartite graph where $\mathscr{W}$ is the collection of k-subspaces of $\mathscr{X}$ and $(A, W) \in \mathscr{E}$ if W intersects A nontrivially
- $\alpha(A, A') := \dim(A \cap A')$ for all $A, A' \in \mathscr{A}$ (association on $\mathscr{A}$ of magnitude $N-k$)
- $\mathscr{B}$ is α-regular
- $|\alpha^{-1}(\ell)| = |\{(A, A') \in \mathscr{A}^2 \mid \dim(A \cap A') = \ell\}|$

Approach 4: Extremal Combinatorics

We apply the machinery to our 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 $\mathscr{A}$.

Theorem (Gruica, R.)

Let $\mathscr{F}$ be the family of k-spaces in $\mathscr{X}$ that are not common complements of the spaces in $\mathscr{A}$. Then

$$\frac{v_q(N,k,N-k)^2\,|\mathscr{A}|^2}{\sum_{\ell=0}^{N-k} v_q(N,k,\ell)\cdot|\{(A,A')\in\mathscr{A}^2 \mid \dim(A\cap A')=\ell\}|} \leq |\mathscr{F}| \leq |\mathscr{A}|\,v_q(N,k,N-k),$$

where

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

Other expressions for $v_q(N,k,\ell)$ can be found, but they are not friendly to estimate. We obtain this one passing through the theory of *critical problems* by Crapo and Rota.

Approach 4: Extremal Combinatorics

Asymptotic analysis for $q \to +\infty$:

- N and k are fixed,
- everything else is a sequence in q, i.e., $\mathscr{X}_q$, $\mathscr{A}_q$, $\mathscr{F}_q$.

Let

$$\delta_q := 1 - \frac{|\mathscr{F}_q|}{\begin{bmatrix} N \\ k \end{bmatrix}_q}$$

be the proportion of the common complements of the spaces in $\mathscr{A}_q$.

Approach 4: Extremal Combinatorics

Asymptotic analysis for $q \to +\infty$:

- N and k are fixed,
- everything else is a sequence in q, i.e., $\mathscr{X}_q$, $\mathscr{A}_q$, $\mathscr{F}_q$.

Let

$$\delta_q := 1 - \frac{|\mathscr{F}_q|}{\begin{bmatrix} N \\ k \end{bmatrix}_q}$$

be the proportion of the common complements of the spaces in $\mathscr{A}_q$.

Theorem (Gruica, R.)

1. If $|\mathscr{A}_q| \in o(q)$ as $q \to +\infty$, then $\lim_{q\to+\infty} \delta_q = 1$ and the common complements are dense.
2. If $q \in o(|\mathscr{A}_q|)$ as $q \to +\infty$, then (under certain assumptions) $\lim_{q\to+\infty} \delta_q = 0$ and the common complements are sparse.

When studying the asymptotics for $q \to +\infty$, in most cases the decisive property for density/sparseness is whether or not the size of $\mathscr{A}_q$ is negligible with respect to the field size q (there are few exceptions).

Approach 4: Extremal Combinatorics

Back to MRD codes: Let $1 \leq d \leq n$ and $k = m(n-d+1)$. Recall that we described the MRD codes in $\mathbb{F}_q^{n \times m}$ of dimension k as the common complements of

$$\begin{bmatrix} n \\ d-1 \end{bmatrix}_q$$

subspaces on $\mathbb{F}_q^{n \times m}$ of dimension $m(d-1)$.

<u>Back to MRD codes</u>: Let $1 \leq d \leq n$ and $k = m(n-d+1)$. Recall that we described the MRD codes in $\mathbb{F}_q^{n \times m}$ of dimension k as the common complements of

$$\begin{bmatrix} n \\ d-1 \end{bmatrix}_q$$

subspaces on $\mathbb{F}_q^{n \times m}$ of dimension $m(d-1)$. We also have

$$\begin{bmatrix} n \\ d-1 \end{bmatrix}_q \sim q^{(d-1)(n-d+1)} \quad \text{as } q \to +\infty$$

and $(d-1)(n-d+1) > 1$ unless $d = 1$ or $n = d = 2$.

Approach 4: Extremal Combinatorics

Back to MRD codes: Let $1 \le d \le n$ and $k = m(n-d+1)$. Recall that we described the MRD codes in $\mathbb{F}_q^{n \times m}$ of dimension k as the common complements of

$$\begin{bmatrix} n \\ d-1 \end{bmatrix}_q$$

subspaces on $\mathbb{F}_q^{n \times m}$ of dimension $m(d-1)$. We also have

$$\begin{bmatrix} n \\ d-1 \end{bmatrix}_q \sim q^{(d-1)(n-d+1)} \quad \text{as } q \to +\infty$$

and $(d-1)(n-d+1) > 1$ unless $d=1$ or $n=d=2$. Therefore:

Theorem (Gruica, R.)

MRD codes are sparse as $q \to +\infty$, unless $d=1$ or $n=d=2$.

For $d=1$ MRD codes are dense. For $n=d=2$ we know from Antrobus and Gluesing-Luerssen that MRD codes are neither sparse, nor dense. These are the only exceptions to the sparseness result, for $q \to +\infty$.

Approach 4: Extremal Combinatorics

One can explain the divergence between MDS and MRD codes with:

Theorem (Gruica, R.)

1. If $|\mathscr{A}_q| \in o(q)$ as $q \to +\infty$, then $\lim_{q\to+\infty} \delta_q = 1$ and the common complements are dense.
2. If $q \in o(|\mathscr{A}_q|)$ as $q \to +\infty$, then (under certain assumptions) $\lim_{q\to+\infty} \delta_q = 0$ and the common complements are sparse.

For $S \subseteq \{1,\dots,n\}$, let $\mathbb{F}_q^n(S) \leq \mathbb{F}_q^n$ be the space of vectors $x \in \mathbb{F}_q^n$ with $x_i = 0$ for all $i \notin S$.

Approach 4: Extremal Combinatorics

One can explain the divergence between MDS and MRD codes with:

Theorem (Gruica, R.)

1. If $|\mathscr{A}_q| \in o(q)$ as $q \to +\infty$, then $\lim_{q\to+\infty} \delta_q = 1$ and the common complements are dense.
2. If $q \in o(|\mathscr{A}_q|)$ as $q \to +\infty$, then (under certain assumptions) $\lim_{q\to+\infty} \delta_q = 0$ and the common complements are sparse.

For $S \subseteq \{1,\dots,n\}$, let $\mathbb{F}_q^n(S) \leq \mathbb{F}_q^n$ be the space of vectors $x \in \mathbb{F}_q^n$ with $x_i = 0$ for all $i \notin S$.

MDS codes of dimension k are the common complements of the spaces of the form $\mathbb{F}_q^n(S)$, where $S \subseteq \{1,\dots,n\}$ has size $n-k$. The number of such spaces is $\binom{n}{k}$, and we have $\binom{n}{k} \in o(q)$ as $q \to +\infty$.

Approach 4: Extremal Combinatorics

One can explain the divergence between MDS and MRD codes with:

Theorem (Gruica, R.)

1. If $|\mathscr{A}_q| \in o(q)$ as $q \to +\infty$, then $\lim_{q\to+\infty} \delta_q = 1$ and the common complements are dense.
2. If $q \in o(|\mathscr{A}_q|)$ as $q \to +\infty$, then (under certain assumptions) $\lim_{q\to+\infty} \delta_q = 0$ and the common complements are sparse.

For $S \subseteq \{1,\dots,n\}$, let $\mathbb{F}_q^n(S) \leq \mathbb{F}_q^n$ be the space of vectors $x \in \mathbb{F}_q^n$ with $x_i = 0$ for all $i \notin S$.

MDS codes of dimension k are the common complements of the spaces of the form $\mathbb{F}_q^n(S)$, where $S \subseteq \{1,\dots,n\}$ has size $n-k$. The number of such spaces is $\binom{n}{k}$, and we have $\binom{n}{k} \in o(q)$ as $q \to +\infty$.

MDS vs MRD codes

MDS/MRD codes are the common complements of families of spaces whose cardinalities are negligible/preponderant with respect to the field size q. This is the decisive property for density/sparseness.

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 <u>very</u> 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.

Non-Linear Codes

It is natural to ask if non-linear codes behave like their linear brothers.

Definition

A **non-linear block code** is a subset $C \subseteq \mathbb{F}_q^n$ with $|C| \geq 2$. Its **minimum (Hamming) distance** is

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

Note: "non-linear" means "not necessarily linear" here.

Non-Linear Codes

It is natural to ask if non-linear codes behave like their linear brothers.

Definition

A **non-linear block code** is a subset $C \subseteq \mathbb{F}_q^n$ with $|C| \geq 2$. Its **minimum (Hamming) distance** is

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

Note: "non-linear" means "not necessarily linear" here.

Theorem (Singleton Bound)

Let $C \subseteq \mathbb{F}_q^n$ be a non-linear code. Then $|C| \leq q^{n-d+1}$, where $d = d^{\mathrm{H}}(C)$.

Definition

We say that C is **MDS** if the bound is attained with equality.

Question

Is the typical non-linear code of size q^{n-d+1} MDS?

Non-Linear Codes

Let

$$\delta_q(n, q^s, \geq d) = \frac{\#\{C \subseteq \mathbb{F}_q^n \,:\, |C| = q^s,\ d^{\mathrm{H}}(C) \geq d\}}{\binom{q^n}{q^s}}.$$

Then:

Theorem (Gruica, R.)

$$\lim_{q \to +\infty} \delta_q(n, q^s, \geq d) = \begin{cases} 1 & \text{if } s < (n-d+1)/2, \\ 0 & \text{if } s > (n-d+1)/2. \end{cases}$$

In particular, non-linear MDS codes are sparse.

Non-Linear Codes

Let

$$\delta_q(n, q^s, \geq d) = \frac{\#\{C \subseteq \mathbb{F}_q^n \,:\, |C| = q^s,\; d^{\mathrm{H}}(C) \geq d\}}{\binom{q^n}{q^s}}.$$

Then:

Theorem (Gruica, R.)

$$\lim_{q \to +\infty} \delta_q(n, q^s, \geq d) = \begin{cases} 1 & \text{if } s < (n-d+1)/2, \\ 0 & \text{if } s > (n-d+1)/2. \end{cases}$$

In particular, non-linear MDS codes are sparse.

Remark

Note that the "boundary cardinality" separating density/sparseness is the square root of the maximal cardinality that a code can attain for q large, i.e.,

$$\sqrt{q^{n-d+1}}.$$

Partial Spreads

Definition

A collection $\mathscr{S}$ of k-dimensional subspaces of $\mathbb{F}_q^n$ is called a **partial spread** if $U \cap V = \{0\}$ for all $U, V \in \mathscr{S}$ with $U \neq V$.

If $n \geq 2k$, there is always a partial spread of size $\sim q^{n-k}$.

Question

Are large partial spreads rare objects?

Partial Spreads

Definition

A collection $\mathscr{S}$ of k-dimensional subspaces of $\mathbb{F}_q^n$ is called a **partial spread** if $U \cap V = \{0\}$ for all $U, V \in \mathscr{S}$ with $U \neq V$.

If $n \geq 2k$, there is always a partial spread of size $\sim q^{n-k}$.

Question

Are large partial spreads rare objects?

Denote by $\mathscr{G}_q(k,n)$ the collection of k-spaces in $\mathbb{F}_q^n$.

Theorem (Gruica, R.)

Let n and k be integers with $n \geq 2k \geq 2$. We have

$$\lim_{q \to +\infty} \frac{\#\text{ partial spreads of card. } S_q \text{ in } \mathscr{G}_q(k,n)}{\#\text{ sets of card. } S_q \text{ in } \mathscr{G}_q(k,n)} = \begin{cases} 1 & \text{if } S_q \ll \sqrt{q^{n-2k+1}}, \\ 0 & \text{if } S_q \gg \sqrt{q^{n-2k+1}}. \end{cases}$$

Typical Objects

We answered the following

Question

Is the largest object with good distance properties "typical"?

- Hamming metric, linear: YES (folklore)
- Rank metric, linear: NO
- Hamming metric, non-linear: NO
- Rank-metric, non-linear: NO
- Subspace metric (partial spreads): NO

Typical Objects

We answered the following

Question

Is the largest object with good distance properties "typical"?

- Hamming metric, linear: YES (folklore)
- Rank metric, linear: NO
- Hamming metric, non-linear: NO
- Rank-metric, non-linear: NO
- Subspace metric (partial spreads): NO

Thank you very much!