Codes with good distance properties from a density perspective

Algebraic Coding Theory e-Summer School - ACT21

Anina Gruica

June 9, 2021

Eindhoven University of Technology

joint work with Alberto Ravagnani

Codes with good distance properties from a density perspective

Throughout this talk q denotes a prime power and the alphabet we consider is the finite field $\mathbb{F}_q$ of q elements.

Codes with good distance properties from a density perspective

Throughout this talk q denotes a prime power and the alphabet we consider is the finite field $\mathbb{F}_q$ of q elements.

QUESTION: What is the density of codes with good distance properties within the set of all codes of the same cardinality?

Codes with good distance properties from a density perspective

Throughout this talk q denotes a prime power and the alphabet we consider is the finite field $\mathbb{F}_q$ of q elements.

QUESTION: What is the density of codes with good distance properties within the set of all codes of the same cardinality?

We will fill in the question mark for the following codes:

	Hamming metric	rank-metric	injection metric
linear	**MDS**	?	———————
non-linear	?	?	?

Linear codes in the rank-metric

Let $m \geq n \geq 2$ be integers.

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-linear subspace $\mathcal{C} \leq \mathbb{F}_q^{n \times m}$. The **minimum distance** of $\mathcal{C}$ is $d(\mathcal{C}) := \min\{\mathrm{rk}(X) \mid X \in \mathcal{C},\ X \neq 0\}$.

Linear codes in the rank-metric

Let $m \geq n \geq 2$ be integers.

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-linear subspace $\mathcal{C} \leq \mathbb{F}_q^{n \times m}$. The **minimum distance** of $\mathcal{C}$ is $d(\mathcal{C}) := \min\{\mathrm{rk}(X) \mid X \in \mathcal{C},\ X \neq 0\}$.

Singleton-like bound: $\dim(\mathcal{C}) \leq m(n - d(\mathcal{C}) + 1)$

We call a rank-metric code meeting the Singleton-like bound with equality a **Maximum Rank Distance** (**MRD**) code.

Linear codes in the rank-metric

Let $m \geq n \geq 2$ be integers.

Definition

A **rank-metric code** is a non-zero $\mathbb{F}_q$-linear subspace $\mathcal{C} \leq \mathbb{F}_q^{n \times m}$. The **minimum distance** of $\mathcal{C}$ is $d(\mathcal{C}) := \min\{\mathrm{rk}(X) \mid X \in \mathcal{C},\ X \neq 0\}$.

Singleton-like bound: $\dim(\mathcal{C}) \leq m(n - d(\mathcal{C}) + 1)$

We call a rank-metric code meeting the Singleton-like bound with equality a **Maximum Rank Distance** (**MRD**) code.

Definition

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

$$\delta_q(n \times m, d) := \frac{\#\ k\text{-dim MRD codes in } \mathbb{F}_q^{n \times m}}{\#\ k\text{-dim codes in } \mathbb{F}_q^{n \times m}}$$

denote the **density** (**function**) of MRD codes among all k-dimensional rank-metric codes.

Current Literature on the density of MRD Codes ($m \geq n \geq 2$)

Theorem [Byrne and Ravagnani, 2018]

If $d \geq 2$, then

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

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

Theorem [Antrobus and Gluesing-Luerssen, 2018]

For $d \geq 1$ we have

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

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

Current Literature on the density of MRD Codes

This gives an example of MRD codes that are neither sparse nor dense:

Theorem [Antrobus and Gluesing-Luerssen, 2018]

For $m \geq 2$ we have

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

In particular, $0 < \lim_{q \to +\infty} \delta_q(2 \times m, 2) < 1$.

Current Literature on the density of MRD Codes

This gives an example of MRD codes that are neither sparse nor dense:

Theorem [Antrobus and Gluesing-Luerssen, 2018]

For $m \geq 2$ we have

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

In particular, $0 < \lim_{q \to +\infty} \delta_q(2 \times m, 2) < 1$.

This gives an example of MRD codes that are sparse:

Theorem [Gluesing-Luerssen, 2019]

We have

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

In particular, $\lim_{q \to +\infty} \delta_q(3 \times 3, 3) = 0$.

Current Literature on the density of MRD Codes

This gives an example of MRD codes that are neither sparse nor dense:

Theorem [Antrobus and Gluesing-Luerssen, 2018]

For $m \geq 2$ we have

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

In particular, $0 < \lim_{q \to +\infty} \delta_q(2 \times m, 2) < 1$.

This gives an example of MRD codes that are sparse:

Theorem [Gluesing-Luerssen, 2019]

We have

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

In particular, $\lim_{q \to +\infty} \delta_q(3 \times 3, 3) = 0$.

$\rightarrow$ **In general, MRD codes are neither sparse nor dense.**

Upper bound

Definition

A **bipartite graph** is a 3-tuple $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where $\mathcal{V}$, $\mathcal{W}$ are finite non-empty sets (vertices) and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{W}$ (edges).

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

Upper bound

Definition

A **bipartite graph** is a 3-tuple $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where $\mathcal{V}$, $\mathcal{W}$ are finite non-empty sets (vertices) and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{W}$ (edges).

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

GOAL: Give upper and lower bounds on the number of non-isolated vertices.

Upper bound

Definition

A **bipartite graph** is a 3-tuple $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$, where $\mathcal{V}$, $\mathcal{W}$ are finite non-empty sets (vertices) and $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{W}$ (edges).

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

GOAL: Give upper and lower bounds on the number of non-isolated vertices.

Lemma

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

$$|\mathcal{F}| \leq |\mathcal{V}|\,\partial.$$

Lower bound

Definition

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

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

Lower bound

Definition

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

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

If $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$ is a finite bipartite graph and α an association on $\mathcal{V}$, then $\mathcal{B}$ is called α-**regular** if for all $(V, V') \in \mathcal{V} \times \mathcal{V}$ the number

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

only depends on $\alpha(V, V')$. Then we call this number $\mathcal{W}_\ell(\alpha)$, where $\ell = \alpha(V, V')$.

Lower bound

Definition

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

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

If $\mathcal{B} = (\mathcal{V}, \mathcal{W}, \mathcal{E})$ is a finite bipartite graph and α an association on $\mathcal{V}$, then $\mathcal{B}$ is called α-**regular** if for all $(V, V') \in \mathcal{V} \times \mathcal{V}$ the number

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

only depends on $\alpha(V, V')$. Then we call this number $\mathcal{W}_\ell(\alpha)$, where $\ell = \alpha(V, V')$.

Lemma [G. - Ravagnani]

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

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

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes in $\mathbb{F}_q^{n \times m}$ are $\mathbb{F}_q$-subspaces of dimension $k = m(n - d + 1)$ and minimum distance d.

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes in $\mathbb{F}_q^{n \times m}$ are $\mathbb{F}_q$-subspaces of dimension $k = m(n - d + 1)$ and minimum distance d.

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

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes in $\mathbb{F}_q^{n \times m}$ are $\mathbb{F}_q$-subspaces of dimension $k = m(n-d+1)$ and minimum distance d.

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

MRD codes as common complements:

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

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes in $\mathbb{F}_q^{n\times m}$ are $\mathbb{F}_q$-subspaces of dimension $k = m(n-d+1)$ and minimum distance d.

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

MRD codes as common complements:

- Consider the collection $\mathcal{U}$ of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathcal{U}$, denote by $\mathbb{F}_q^{n\times m}(U)$ the set of all matrices whose column space is contained in U. $\Longrightarrow \mathbb{F}_q^{n\times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathcal{U}$.
- We let $\mathcal{A} = \{\mathbb{F}_q^{n\times m}(U) \mid U \in \mathcal{U}\}$. Then the common complements of the spaces in $\mathcal{A}$ are exactly the rank-metric codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ with $d(\mathcal{C}) = d$ and $\dim(\mathcal{C}) = mn - m(d-1) = m(n-d+1)$.

MRD codes as common complements

Let $m \geq n \geq 2$ and $n \geq d \geq 1$.

MRD codes in $\mathbb{F}_q^{n\times m}$ are $\mathbb{F}_q$-subspaces of dimension $k = m(n-d+1)$ and minimum distance d.

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

MRD codes as common complements:

- Consider the collection $\mathcal{U}$ of subspaces $U \leq \mathbb{F}_q^n$ with $\dim(U) = d-1$. For $U \in \mathcal{U}$, denote by $\mathbb{F}_q^{n\times m}(U)$ the set of all matrices whose column space is contained in U. $\Longrightarrow \mathbb{F}_q^{n\times m}(U)$ is a linear space of dimension $m(d-1)$ for all $U \in \mathcal{U}$.
- We let $\mathcal{A} = \{\mathbb{F}_q^{n\times m}(U) \mid U \in \mathcal{U}\}$. Then the common complements of the spaces in $\mathcal{A}$ are exactly the rank-metric codes $\mathcal{C} \leq \mathbb{F}_q^{n\times m}$ with $d(\mathcal{C}) = d$ and $\dim(\mathcal{C}) = mn - m(d-1) = m(n-d+1)$.
- $|\mathcal{A}| = |\mathcal{U}| = \begin{bmatrix} n \\ d-1 \end{bmatrix}_q \sim q^{(d-1)(n-d+1)}$ as $q \to +\infty$.

Density of linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ and set $k = m(n - d + 1)$.

- $\mathcal{B} = (\mathcal{A}, \mathcal{W}, \mathcal{E})$ is a bipartite graph where $\mathcal{W}$ is the collection of k-subspaces of $\mathbb{F}_q^{n \times m}$ and $(A, \mathcal{C}) \in \mathcal{E}$ if $\mathcal{C}$ intersects A nontrivially
- $\alpha(A, A') := \dim(A \cap A')$ for all A, $A' \in \mathcal{A}$ (association on $\mathcal{A}$ of magnitude $m(d-1)$)
- $\mathcal{B}$ is α-regular
- $|\alpha^{-1}(\ell)| = |\{(A, A') \in \mathcal{A}^2 \mid \dim(A \cap A') = \ell\}|$

The following result computes the asymptotic density of MRD codes for all parameter sets, showing that they are (very) sparse whenever $n \geq 3$ and $d \geq 2$:

Density of linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ and set $k = m(n-d+1)$.

- $\mathcal{B} = (\mathcal{A}, \mathcal{W}, \mathcal{E})$ is a bipartite graph where $\mathcal{W}$ is the collection of k-subspaces of $\mathbb{F}_q^{n\times m}$ and $(A, \mathcal{C}) \in \mathcal{E}$ if $\mathcal{C}$ intersects A nontrivially
- $\alpha(A, A') := \dim(A \cap A')$ for all A, $A' \in \mathcal{A}$ (association on $\mathcal{A}$ of magnitude $m(d-1)$)
- $\mathcal{B}$ is α-regular
- $|\alpha^{-1}(\ell)| = |\{(A, A') \in \mathcal{A}^2 \mid \dim(A \cap A') = \ell\}|$

The following result computes the asymptotic density of MRD codes for all parameter sets, showing that they are (very) sparse whenever $n \geq 3$ and $d \geq 2$:

Theorem [Antrobus and Gluesing-Luerssen, G. and Ravagnani]

We have

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

In particular,

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

Non-linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ be integers.

Definition

A **rank-metric code** is a subset $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| \geq 2$. Its minimum distance is

$$d(\mathcal{C}) = \min\{\mathrm{rk}(X - Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}.$$

Recall: MRD codes are codes of minimum distance d and cardinality $|\mathcal{C}| = q^{m(n-d+1)}$.

Non-linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ be integers.

Definition

A **rank-metric code** is a subset $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| \geq 2$. Its minimum distance is

$$d(\mathcal{C}) = \min\{\mathrm{rk}(X - Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}.$$

Recall: MRD codes are codes of minimum distance d and cardinality $|\mathcal{C}| = q^{m(n-d+1)}$.

We use the bounds on the number of non-isolated vertices on the following bipartite graph:

- $\mathcal{B} = (\mathcal{A}, \mathcal{W}, \mathcal{E})$ is a bipartite graph where

  $$\mathcal{A} = \{\{X, Y\} \subseteq \mathbb{F}_q^{n \times m} \mid X \neq Y,\ \mathrm{rk}(X - Y) \leq d - 1\},$$

  $\mathcal{W}$ is the collection of subsets $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| = q^{m(n-d+1)}$ and $(\{X, Y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{X, Y\} \subseteq \mathcal{C}$

Non-linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ be integers.

Definition

A **rank-metric code** is a subset $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| \geq 2$. Its minimum distance is

$$d(\mathcal{C}) = \min\{\mathrm{rk}(X - Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}.$$

Recall: MRD codes are codes of minimum distance d and cardinality $|\mathcal{C}| = q^{m(n-d+1)}$.

We use the bounds on the number of non-isolated vertices on the following bipartite graph:

- $\mathcal{B} = (\mathcal{A}, \mathcal{W}, \mathcal{E})$ is a bipartite graph where

  $$\mathcal{A} = \{\{X, Y\} \subseteq \mathbb{F}_q^{n \times m} \mid X \neq Y,\ \mathrm{rk}(X - Y) \leq d - 1\},$$

  $\mathcal{W}$ is the collection of subsets $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| = q^{m(n-d+1)}$ and $(\{X, Y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{X, Y\} \subseteq \mathcal{C}$
- $\alpha(\{X, Y\}, \{T, Z\}) := 4 - |\{X, Y, T, Z\}|$ for all $\{X, Y\}, \{T, Z\} \in \mathcal{A}$ (association on $\mathcal{A}$ of magnitude 4)

Non-linear MRD codes

Let $m \geq n \geq 2$ and $n \geq d \geq 1$ be integers.

Definition

A **rank-metric code** is a subset $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| \geq 2$. Its minimum distance is

$$d(\mathcal{C}) = \min\{\mathrm{rk}(X - Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}.$$

Recall: MRD codes are codes of minimum distance d and cardinality $|\mathcal{C}| = q^{m(n-d+1)}$.

We use the bounds on the number of non-isolated vertices on the following bipartite graph:

- $\mathcal{B} = (\mathcal{A}, \mathcal{W}, \mathcal{E})$ is a bipartite graph where

  $$\mathcal{A} = \{\{X, Y\} \subseteq \mathbb{F}_q^{n \times m} \mid X \neq Y,\ \mathrm{rk}(X - Y) \leq d - 1\},$$

  $\mathcal{W}$ is the collection of subsets $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ with $|\mathcal{C}| = q^{m(n-d+1)}$ and $(\{X, Y\}, \mathcal{C}) \in \mathcal{E}$ if and only if $\{X, Y\} \subseteq \mathcal{C}$
- $\alpha(\{X, Y\}, \{T, Z\}) := 4 - |\{X, Y, T, Z\}|$ for all $\{X, Y\}, \{T, Z\} \in \mathcal{A}$ (association on $\mathcal{A}$ of magnitude 4)
- $\mathcal{B}$ is α-regular

Density of non-linear MRD codes

Using the bound on the number of isolated vertices, we obtain:

Density of non-linear MRD codes

Using the bound on the number of isolated vertices, we obtain:

Theorem [G. and Ravagnani]

Let $m \geq n \geq 2$ and $n \geq d \geq 2$ be integers. Then

$$\lim_{q \to +\infty} \frac{\#\text{ MRD codes of cardinality } q^{m(n-d+1)} \text{ in } \mathbb{F}_q^{n \times m}}{\#\text{ codes of cardinality } q^{m(n-d+1)} \text{ in } \mathbb{F}_q^{n \times m}} = 0.$$

Therefore, the typical code in the rank-metric (both linear and non-linear) is not MRD for large q.

Density of non-linear MRD codes

Using the bound on the number of isolated vertices, we obtain:

Theorem [G. and Ravagnani]

Let $m \geq n \geq 2$ and $n \geq d \geq 2$ be integers. Then

$$\lim_{q \to +\infty} \frac{\#\text{ MRD codes of cardinality } q^{m(n-d+1)} \text{ in } \mathbb{F}_q^{n \times m}}{\#\text{ codes of cardinality } q^{m(n-d+1)} \text{ in } \mathbb{F}_q^{n \times m}} = 0.$$

Therefore, the typical code in the rank-metric (both linear and non-linear) is not MRD for large q.

QUESTION: Do linear and non-linear codes over large alphabets behave similarly in other metrics as well?

Density of non-linear MDS codes

Definition

A **block code** of minimum distance d is a subset $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| \geq 2$ and $d = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}$. MDS codes correspond to $|\mathcal{C}| = q^{n-d+1}$.

Density of non-linear MDS codes

Definition

A **block code** of minimum distance d is a subset $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| \geq 2$ and $d = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}$. MDS codes correspond to $|\mathcal{C}| = q^{n-d+1}$.

Let $2 \leq S_q \leq q^{n-d+1}$ be a sequence in q and $2 \leq d \leq n$.

Theorem [G. and Ravagnani]

$$\lim_{q \to +\infty} \frac{\#\text{ codes of card. } S_q \text{ and min. dist. } \geq d \text{ in } \mathbb{F}_q^n}{\#\text{ codes of card. } S_q \text{ in } \mathbb{F}_q^n} = \begin{cases} 1 & \text{if } S_q \ll \sqrt{q^{n-d+1}}, \\ 0 & \text{if } S_q \gg \sqrt{q^{n-d+1}}. \end{cases}$$

Density of non-linear MDS codes

Definition

A **block code** of minimum distance d is a subset $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| \geq 2$ and $d = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}$. MDS codes correspond to $|\mathcal{C}| = q^{n-d+1}$.

Let $2 \leq S_q \leq q^{n-d+1}$ be a sequence in q and $2 \leq d \leq n$.

Theorem [G. and Ravagnani]

$$\lim_{q \to +\infty} \frac{\#\text{ codes of card. } S_q \text{ and min. dist. } \geq d \text{ in } \mathbb{F}_q^n}{\#\text{ codes of card. } S_q \text{ in } \mathbb{F}_q^n} = \begin{cases} 1 & \text{if } S_q \ll \sqrt{q^{n-d+1}}, \\ 0 & \text{if } S_q \gg \sqrt{q^{n-d+1}}. \end{cases}$$

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

Density of non-linear MDS codes

Definition

A **block code** of minimum distance d is a subset $\mathcal{C} \subseteq \mathbb{F}_q^n$ with $|\mathcal{C}| \geq 2$ and $d = \min\{\mathrm{d_H}(x, y) \mid x, y \in \mathcal{C},\ x \neq y\}$. MDS codes correspond to $|\mathcal{C}| = q^{n-d+1}$.

Let $2 \leq S_q \leq q^{n-d+1}$ be a sequence in q and $2 \leq d \leq n$.

Theorem [G. and Ravagnani]

$$\lim_{q \to +\infty} \frac{\#\text{ codes of card. } S_q \text{ and min. dist. } \geq d \text{ in } \mathbb{F}_q^n}{\#\text{ codes of card. } S_q \text{ in } \mathbb{F}_q^n} = \begin{cases} 1 & \text{if } S_q \ll \sqrt{q^{n-d+1}}, \\ 0 & \text{if } S_q \gg \sqrt{q^{n-d+1}}. \end{cases}$$

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

Corollary [G. and Ravagnani]

$$\lim_{q \to +\infty} \frac{\#\text{ MDS codes of card. } q^{n-d+1} \text{ in } \mathbb{F}_q^n}{\#\text{ codes of card. } q^{n-d+1} \text{ in } \mathbb{F}_q^n} = 0.$$

Subspace codes with the injection metric

Let $1 \leq k \leq n$ be integers. We denote by $\mathcal{G}_q(k, n)$ the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, also known as the **Grassmannian**.

Subspace codes with the injection metric

Let $1 \leq k \leq n$ be integers. We denote by $\mathcal{G}_q(k, n)$ the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, also known as the **Grassmannian**.

Definition

A subset $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ is called a **constant-dimension subspace code**. The **minimum (injection) distance** of a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ is

$$d(\mathcal{C}) = \min\{d(X, Y) \mid X, Y \in \mathcal{C},\, X \neq Y\}$$

where for $X, Y \in \mathcal{G}_q(k, n)$ is $d(X, Y) = k - \dim(X \cap Y)$.

Subspace codes with the injection metric

Let $1 \leq k \leq n$ be integers. We denote by $\mathcal{G}_q(k,n)$ the set of all k-dimensional subspaces of $\mathbb{F}_q^n$, also known as the **Grassmannian**.

Definition

A subset $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is called a **constant-dimension subspace code**. The **minimum (injection) distance** of a subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ is

$$d(\mathcal{C}) = \min\{d(X,Y) \mid X, Y \in \mathcal{C},\, X \neq Y\}$$

where for $X, Y \in \mathcal{G}_q(k,n)$ is $d(X,Y) = k - \dim(X \cap Y)$.

The following is the Singleton-like bound for subspace codes:

Theorem [Kötter and Kschischang, 2008]

Suppose $k \leq n-k$. For any subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with minimum distance $d(\mathcal{C}) \geq d$ we have

$$|\mathcal{C}| \leq \begin{bmatrix} n-d+1 \\ n-k \end{bmatrix}_q .$$

We call a code attaining this bound an **optimal** subspace code.

Density of optimal subspace codes with the injection metric

Let $k \leq n-k$ and $2 \leq d \leq k$ be integers and $2 \leq S_q \leq \begin{bmatrix} n-d+1 \\ n-k \end{bmatrix}_q$ a sequence in q.

As a consequence of the bounds we get from the graph theory lemmas:

Theorem [G. and Ravagnani]

Let $\gamma_q = \sqrt{q^{k(n-k)-(d-1)(n-d+1)}}$. We have

$$\lim_{q \to +\infty} \frac{\#\text{ codes of card. } S_q \text{ and min. dist. } \geq d \text{ in } \mathcal{G}_q(k,n)}{\#\text{ codes of card. } S_q \text{ in } \mathcal{G}_q(k,n)} = \begin{cases} 1 & \text{if } S_q \ll \gamma_q, \\ 0 & \text{if } S_q \gg \gamma_q. \end{cases}$$

In particular, the typical subspace code is not optimal.

Application to partial spreads

Definition

A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ with injection distance k (i.e. where all spaces in $\mathcal{C}$ intersect trivially) is called a **partial spread**.

Application to partial spreads

Definition

A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k, n)$ with injection distance k (i.e. where all spaces in $\mathcal{C}$ intersect trivially) is called a **partial spread**.

The previous results tell us for which cardinalities S_q a uniformly random collection of S_q subspaces in $\mathcal{G}_q(k, n)$ form a partial spread with high probability (for q large).

Application to partial spreads

Definition

A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with injection distance k (i.e. where all spaces in $\mathcal{C}$ intersect trivially) is called a **partial spread**.

The previous results tell us for which cardinalities S_q a uniformly random collection of S_q subspaces in $\mathcal{G}_q(k,n)$ form a partial spread with high probability (for q large).

Corollary [G. and Ravagnani]

Let $n \geq k \geq 1$ be integers. We have

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

Application to partial spreads

Definition

A subspace code $\mathcal{C} \subseteq \mathcal{G}_q(k,n)$ with injection distance k (i.e. where all spaces in $\mathcal{C}$ intersect trivially) is called a **partial spread**.

The previous results tell us for which cardinalities S_q a uniformly random collection of S_q subspaces in $\mathcal{G}_q(k,n)$ form a partial spread with high probability (for q large).

Corollary [G. and Ravagnani]

Let $n \geq k \geq 1$ be integers. We have

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

In particular, assume that $k \mid n$ and let $\mathcal{C}$ be a uniformly random collection of $(q^n-1)/(q^k-1)$ k-subspaces of $\mathbb{F}_q^n$. The probability that $\mathcal{C}$ is a spread goes to 0 as $q \to +\infty$.

Summary

What does the typical code over a large alphabet look like?

	Hamming metric	rank-metric	injection metric
linear	**MDS**	**not MRD***	————————
non-linear	**not MDS**	**not MRD**	**not optimal**

(* unless $n = d = 2$)

Summary

What does the typical code over a large alphabet look like?

	Hamming metric	rank-metric	injection metric
linear	**MDS**	**not MRD***	————————
non-linear	**not MDS**	**not MRD**	**not optimal**

(* unless $n = d = 2$)

THANK YOU FOR YOUR ATTENTION!!