Cryptography and its applications in the Italian scenario

Giuseppe Marino

Department of Mathematics and Its Applications “Renato Caccioppoli”
University of Naples Federico II

De Componendis Cifris (vice president)

OpeRa 2024
16$^{\mathrm{th}}$ Febraury 2024

Cryptography is a subject which distinguishes itself in the context of investigations in Cybersecurity.

Cryptography is a subject which distinguishes itself in the context of investigations in Cybersecurity.
Research of secure cryptographic algorithms needs deep knowledge of specific mathematical topics. In fact, all modern cryptosystems rely on computational security, that is on the assumption that certain mathematical problems, acknowledged by the global scientific community, are not solvable.

Cryptography is a subject which distinguishes itself in the context of investigations in Cybersecurity.
Research of secure cryptographic algorithms needs deep knowledge of specific mathematical topics. In fact, all modern cryptosystems rely on computational security, that is on the assumption that certain mathematical problems, acknowledged by the global scientific community, are not solvable.
The time necessary to perform a research in cryptography and to make it applicable is usually very long, unlike cybersecurity which has to respond constantly and quickly to new threats.

Cryptography is a subject which distinguishes itself in the context of investigations in Cybersecurity.
Research of secure cryptographic algorithms needs deep knowledge of specific mathematical topics. In fact, all modern cryptosystems rely on computational security, that is on the assumption that certain mathematical problems, acknowledged by the global scientific community, are not solvable.
The time necessary to perform a research in cryptography and to make it applicable is usually very long, unlike cybersecurity which has to respond constantly and quickly to new threats.
Of course, purely mathematical investigation of algorithms has to go along with research in computers science and engineering, otherwise bad protocols and bad implementations would jeopardize theoretical security.

What are the main lines of research in cryptography in 2024?

What are the main lines of research in cryptography in 2024?

On the one hand, they comprises the investigation of topics that have been there for a few decades but are still of crucial importance, such as symmetric encryption (both block ciphers and stream ciphers), hash functions and public key cryptography.

What are the main lines of research in cryptography in 2024?

On the one hand, they comprises the investigation of topics that have been there for a few decades but are still of crucial importance, such as symmetric encryption (both block ciphers and stream ciphers), hash functions and public key cryptography.
On the other hand, recent technological innovations stimulated new lines of research and determined advances in Cryptography in the last ten/fifteen years.

Some breakthrough innovations in modern cryptography are

Some breakthrough innovations in modern cryptography are

- homomorphic encryption

Some breakthrough innovations in modern cryptography are

- homomorphic encryption
- blockchain technology

Some breakthrough innovations in modern cryptography are

- homomorphic encryption
- blockchain technology
- cryptography for IoT

Some breakthrough innovations in modern cryptography are

- homomorphic encryption
- blockchain technology
- cryptography for IoT
- post-quantum cryptography

Already in the " Piano nazionale per la protezione cibernetica e la sicurezza informatica " of 2017, the Presidency of the Council of Ministers, in outlining the measures needed for a significant improvement in cybersecurity, invoked the world of research.
The plan envisioned the establishment of a National Cryptography Center, explicitly as-signing it four specific tasks: designing ciphers, creating a national encryption algorithm, developing a national blockchain, and providing security assessments.
Unfortunately, the realization of the Center has remained on paper so far.

Already in the " Piano nazionale per la protezione cibernetica e la sicurezza informatica " of 2017, the Presidency of the Council of Ministers, in outlining the measures needed for a significant improvement in cybersecurity, invoked the world of research.
The plan envisioned the establishment of a National Cryptography Center, explicitly as-signing it four specific tasks: designing ciphers, creating a national encryption algorithm, developing a national blockchain, and providing security assessments.
Unfortunately, the realization of the Center has remained on paper so far.
If on the one hand it is true that the national centre is still on paper, it is also true that the Italian cryptographic community, composed of many disciplinary and/or territorial entities, managed to join together to form a single national entity, the association De Componendis Cifris, that made itself available to the country.

Last December De Cifris celebrated its first anniversary, having been founded on December 21, 2022.

Last December De Cifris celebrated its first anniversary, having been founded on December 21, 2022.
It has 55 founding/benefactor members and around 200 regular or young members.

Last December De Cifris celebrated its first anniversary, having been founded on December 21, 2022.
It has 55 founding/benefactor members and around 200 regular or young members.
Additionally, there are 4 major companies and 3 entities in the process of affiliation.

Last December De Cifris celebrated its first anniversary, having been founded on December 21, 2022.
It has 55 founding/benefactor members and around 200 regular or young members.
Additionally, there are 4 major companies and 3 entities in the process of affiliation.
However, De Cifris, as an informal initiative, was born in 2017 and boasts a much larger community.

Last December De Cifris celebrated its first anniversary, having been founded on December 21, 2022.
It has 55 founding/benefactor members and around 200 regular or young members.
Additionally, there are 4 major companies and 3 entities in the process of affiliation.
However, De Cifris, as an informal initiative, was born in 2017 and boasts a much larger community.
For instance, there are over 3000 members on their LinkedIn channel, including professors or researchers from 27 universities or research institutions such as CNR.
There are over 1000 members from the business world and almost as many students or recent graduates.

The main statutory objectives are the following:

The main statutory objectives are the following:

- to disseminate and promote cryptography

The main statutory objectives are the following:

- to disseminate and promote cryptography
- to encourage its study and research, including the development, evaluation, and ideation of algorithms and cryptographic suites

The main statutory objectives are the following:

- to disseminate and promote cryptography
- to encourage its study and research, including the development, evaluation, and ideation of algorithms and cryptographic suites
- to bring the community together, mainly to assist institutions.

De Cifris organized conferences, both territorial events across Italy and specific conferences on topics such as post-quantum cryptography, cryptography applied to blockchains and cryptocurrencies, and military cryptography.

De Cifris organized conferences, both territorial events across Italy and specific conferences on topics such as post-quantum cryptography, cryptography applied to blockchains and cryptocurrencies, and military cryptography.
In terms of outreach, apart from the aformentioned LinkedIn channel, there are a mailing list, a website, and a YouTube channel with recordings of over 150 seminars or conference presentations.

De Cifris organized conferences, both territorial events across Italy and specific conferences on topics such as post-quantum cryptography, cryptography applied to blockchains and cryptocurrencies, and military cryptography.
In terms of outreach, apart from the aformentioned LinkedIn channel, there are a mailing list, a website, and a YouTube channel with recordings of over 150 seminars or conference presentations.
They published a book containing summaries of 100 cryptography theses from various Italian universities and they also organized events for young people.

Looking from outside, what does De Cifris offer as an association?

Looking from outside, what does De Cifris offer as an association?

To a student, they provide information about where cryptography is taught, specific courses, thesis opportunities, and offer internship opportunities and connections with companies.
They also offer scholarships funded by companies.

Looking from outside, what does De Cifris offer as an association?

To a student, they provide information about where cryptography is taught, specific courses, thesis opportunities, and offer internship opportunities and connections with companies.
They also offer scholarships funded by companies.
The Virtual Meeting Centre, an online platform managed by De Cifris, facilitates interactions between job offers and requests, allowing members to upload their CVs and documents expressing their needs or preferences.

For researchers, De Cifris offer information on potential collaborators, support in project activities, and opportunities for publishing in our book series and the upcoming scientific journal.

For researchers, De Cifris offer information on potential collaborators, support in project activities, and opportunities for publishing in our book series and the upcoming scientific journal. For companies and public administrations, they offer qualified training, involvement in projects, and a national overview of cryptographic expertise.

To sum up the association aim to be a reliable point of reference for high-level national research and contribute concretely to the cryptographic community when called upon by the country's institutions.

Next conference is held on 25-26-27 September, 2024 at Bank of Italy's conference theater "Salone Margherita", Via Due Macelli 75 – 00187 Roma (Italy).
For more info, please check website https://www.decifris.it/eventi or contact cifris24@decifris.it.

Cutting blocking sets, saturating linear sets and rank-metric codes

Giuseppe Marino

University of Naples Federico II

OpeRa 2024
16$^{\text{th}}$ Febraury 2024

Definition of linear set

$$\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n) \qquad V = V(r, \mathbb{F}_{q^n})$$

$L \subseteq \Lambda$ is an $\mathbb{F}_q$-linear set if

$$L = L_U = \{P = \langle \mathbf{u} \rangle_{q^n} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

U subspace of V over $\mathbb{F}_q$

Definition of linear set

$$\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n) \qquad V = V(r, \mathbb{F}_{q^n})$$

$L \subseteq \Lambda$ is an $\mathbb{F}_q$-linear set if

$$L = L_U = \{P = \langle \mathbf{u} \rangle_{q^n} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

U subspace of V over $\mathbb{F}_q$

$\dim_{\mathbb{F}_q} U = k \quad \Rightarrow L_U$ is an $\mathbb{F}_q$–linear set of Λ of *rank* k

Definition of linear set

$$\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n) \qquad V = V(r, \mathbb{F}_{q^n})$$

$L \subseteq \Lambda$ is an $\mathbb{F}_q$-linear set if

$$L = L_U = \{P = \langle \mathbf{u} \rangle_{q^n} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

U subspace of V over $\mathbb{F}_q$

- Every projective subspace of Λ is an $\mathbb{F}_{q^n}$-linear set.

Definition of linear set

$$\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n) \qquad V = V(r, \mathbb{F}_{q^n})$$

$L \subseteq \Lambda$ is an $\mathbb{F}_q$-linear set if

$$L = L_U = \{P = \langle \mathbf{u} \rangle_{q^n} : \mathbf{u} \in U \setminus \{\mathbf{0}\}\}$$

U subspace of V over $\mathbb{F}_q$

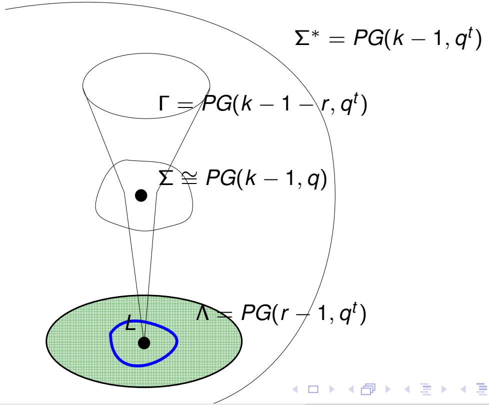
- Every projective subspace of Λ is an $\mathbb{F}_{q^n}$-linear set.
- Every subgeometry $\mathrm{PG}(s, q)$ of Λ $(s < r$ and $n > 1)$ is an $\mathbb{F}_q$-linear set.

Linear sets by projections

Theorem [Lunardon-Polverino 2004]

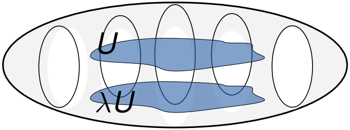
A linear set of a projective space Λ either is a subgeometry or is a projection of a subgeometry.

$rk_q\, L = k$



Definition of linear set

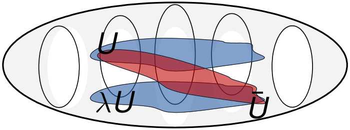
$$\forall \lambda \in \mathbb{F}_{q^n} \Rightarrow L_{\lambda U} = L_U$$



Definition of linear set

$\forall \lambda \in \mathbb{F}_{q^n} \Rightarrow L_{\lambda U} = L_U$

Different $\mathbb{F}_q$-subspaces can define the same linear set



Definition of linear set

$\forall \lambda \in \mathbb{F}_{q^n} \Rightarrow L_{\lambda U} = L_U$

Different $\mathbb{F}_q$-subspaces can define the same linear set

$$\downarrow$$

Definition of linear set

$\forall \lambda \in \mathbb{F}_{q^n} \Rightarrow L_{\lambda U} = L_U$

Different $\mathbb{F}_q$-subspaces can define the same linear set

$$\downarrow$$

An $\mathbb{F}_q$-linear set and the vector space defining it must be considered as coming in pair

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

$L_U \cap \mathrm{PG}(W) = L_{U \cap W}$ $\mathbb{F}_q$-linear set

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

$L_U \cap \mathrm{PG}(W) = L_{U \cap W}$ $\mathbb{F}_q$-linear set

$\dim_{\mathbb{F}_q}(W \cap U) = i$ $\quad$ Ω has *weight* i in L_U

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

$L_U \cap \mathrm{PG}(W) = L_{U\cap W}$ $\mathbb{F}_q$-linear set

$\dim_{\mathbb{F}_q}(W \cap U) = i$ $\quad$ Ω has *weight* i in L_U

Remark

A point of Λ belongs to L_U iff it has weight 1 in L_U

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

$L_U \cap \mathrm{PG}(W) = L_{U \cap W}$ $\mathbb{F}_q$-linear set

$\dim_{\mathbb{F}_q}(W \cap U) = i$ $\quad \Omega$ has *weight* i in L_U

Remark

A point of Λ belongs to L_U iff it has weight 1 in L_U

If L_U has rank k then $|L_U| \leq \frac{q^k - 1}{q-1}$

Weight of a subspace

L_U $\mathbb{F}_q$-linear set of $\Lambda = \mathrm{PG}(V) = \mathrm{PG}(r-1, q^n)$

$\Omega = \mathrm{PG}(W)$, $W \leq V$, projective subspace of $\mathrm{PG}(V)$

$L_U \cap \mathrm{PG}(W) = L_{U \cap W}$ $\mathbb{F}_q$-linear set

$\dim_{\mathbb{F}_q}(W \cap U) = i \quad \Omega$ has *weight* i in L_U

Remark

A point of Λ *belongs to* L_U *iff it has weight* 1 *in* L_U

If L_U has rank k then $|L_U| \leq \frac{q^k-1}{q-1}$

Definition

If $|L_U| = \frac{q^k-1}{q-1}$, then L_U is said to be *scattered* (and U is said to be *scattered subspace*)

Blokhuis-Lavrauw 2000

If L_U is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$ then $\mathrm{rk}\, L_U \leq \lfloor \frac{rn}{2} \rfloor$

.

Blokhuis-Lavrauw 2000

If L_U is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$ then $\mathrm{rk}\, L_U \leq \lfloor \frac{rn}{2} \rfloor$ and if this bound is reached L_U is said to be *maximum scattered*.

Blokhuis-Lavrauw 2000

If L_U is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1, q^n)$ then rk $L_U \leq \lfloor \frac{rn}{2} \rfloor$ and if this bound is reached L_U is said to be *maximum scattered*.

After a series of paper [Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, G.M., Polverino, Zullo] it is know that when $2|rn$ there always exist scattered subspaces of maximum dimension.

Blokhuis-Lavrauw 2000

If L_U is a scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1,q^n)$ then $\operatorname{rk} L_U \leq \lfloor \frac{rn}{2} \rfloor$ and if this bound is reached L_U is said to be *maximum scattered*.

After a series of paper [Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, G.M., Polverino, Zullo] it is know that when $2|rn$ there always exist scattered subspaces of maximum dimension.

If L_U is a maximum scattered $\mathbb{F}_q$-linear set of $\mathrm{PG}(r-1,q^n)$, rn even, then L_U is a two-intersection set (wrt hyperplanes) with intersection numbers

$$\Theta_{\frac{rn}{2}-n-1}(q) = \frac{q^{\frac{rn}{2}-n}-1}{q-1} \qquad \Theta_{\frac{rn}{2}-n}(q) = \frac{q^{\frac{rn}{2}-n+1}-1}{q-1}$$

Linear sets and applications

- Blocking sets in finite projective spaces
- Two intersection sets in finite projective spaces
- Translation spreads of the Cayley Generalized Hexagon
- Translation ovoids of polar spaces
- Semifield flocks
- Finite semifields and finite semifield planes

Linear sets and applications

- Blocking sets in finite projective spaces
- Two intersection sets in finite projective spaces
- Translation spreads of the Cayley Generalized Hexagon
- Translation ovoids of polar spaces
- Semifield flocks
- Finite semifields and finite semifield planes
- Translation caps in affine and projective spaces

Linear sets and applications

- Blocking sets in finite projective spaces
- Two intersection sets in finite projective spaces
- Translation spreads of the Cayley Generalized Hexagon
- Translation ovoids of polar spaces
- Semifield flocks
- Finite semifields and finite semifield planes
- Translation caps in affine and projective spaces
- MRD-codes

Linear sets and applications

- Blocking sets in finite projective spaces
- Two intersection sets in finite projective spaces
- Translation spreads of the Cayley Generalized Hexagon
- Translation ovoids of polar spaces
- Semifield flocks
- Finite semifields and finite semifield planes
- Translation caps in affine and projective spaces
- MRD-codes

[O. Polverino: Linear sets in finite projective spaces, Discrete Math. **310** (2010), 3096–3107.]

Linear sets and applications

- Blocking sets in finite projective spaces
- Two intersection sets in finite projective spaces
- Translation spreads of the Cayley Generalized Hexagon
- Translation ovoids of polar spaces
- Semifield flocks
- Finite semifields and finite semifield planes
- Translation caps in affine and projective spaces
- MRD-codes

[O. Polverino: Linear sets in finite projective spaces, Discrete Math. **310** (2010), 3096–3107.]

[M. Lavrauw: Scattered spaces in Galois Geometry, *Contemporary Developments in Finite Fields and Applications*, 2016, 195–216.]

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$$

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q}$$ **rank weight** of v

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q} \qquad \textbf{rank weight of } v$$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q} \qquad \textbf{rank weight of } v$$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$
$\Gamma(v) \in \mathbb{F}_q^{m \times n}$ whose columns are the coordinates of v_i wrt Γ

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij} \gamma_j$$

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$, $u = (v_1, \ldots, u_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q} \qquad \textbf{rank weight of } v$$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$
$\Gamma(v) \in \mathbb{F}_q^{m \times n}$ whose columns are the coordinates of v_i wrt Γ

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij} \gamma_j$$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \mathrm{rk}(\Gamma(v))$$

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \dots, v_n) \in V$, $u = (v_1, \dots, u_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \dots, v_n \rangle_{\mathbb{F}_q}$$ **rank weight** of v

$$\mathrm{d}_{\mathrm{rk}}(u, v) = \mathrm{wt}_{\mathrm{rk}}(u - v)$$ **rank distance**

Rank-metric codes - Delsarte 1978 - Gabidulin 1985

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$, $u = (v_1, \ldots, u_n) \in V$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q} \qquad \textbf{rank weight of } v$$

$$\mathrm{d}_{\mathrm{rk}}(u, v) = \mathrm{wt}_{\mathrm{rk}}(u - v) \qquad \textbf{rank distance}$$

Definition

*An $[n, k]_{q^m/q}$ **(rank-metric) code** is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $V(n, q^m)$ endowed with the rank distance.*

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

$\Gamma(v) \in \mathbb{F}_q^{m\times n}$ defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij}\gamma_j$$

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \dots, v_n) \in V$

$\Gamma := \{\gamma_1, \dots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

$\Gamma(v) \in \mathbb{F}_q^{m \times n}$ defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij} \gamma_j$$

$\sigma_\Gamma(v) = \langle \text{rows of } \Gamma(v) \rangle_{\mathbb{F}_q}$ **Γ-support** of v

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

$\Gamma(v) \in \mathbb{F}_q^{m \times n}$ defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij} \gamma_j$$

$\sigma_\Gamma(v) = \langle \text{rows of } \Gamma(v) \rangle_{\mathbb{F}_q}$ **Γ-support** of v

The Γ-support does not depend on the choice of Γ

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

$\Gamma(v) \in \mathbb{F}_q^{m\times n}$ defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij}\gamma_j$$

$$\sigma_\Gamma(v) = \langle \text{rows of } \Gamma(v)\rangle_{\mathbb{F}_q} \quad \textbf{Γ-support} \text{ of } v$$

The Γ-support does not depend on the choice of Γ

Definition

$\sigma^{rk}(v) := \sigma_\Gamma(v)$ ***(rank) support*** *of* v

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

$V = V(n, q^m) = \mathbb{F}_{q^m}^n = \mathbb{F}_{q^m} \times \cdots \times \mathbb{F}_{q^m}$

$v = (v_1, \ldots, v_n) \in V$

$\Gamma := \{\gamma_1, \ldots, \gamma_m\}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^m}$

$\Gamma(v) \in \mathbb{F}_q^{m\times n}$ defined by

$$v_i = \sum_{j=1}^{m} \Gamma(v)_{ij}\gamma_j$$

$$\sigma_\Gamma(v) = \langle \text{rows of } \Gamma(v) \rangle_{\mathbb{F}_q} \quad \textbf{Γ-support} \text{ of } v$$

The Γ-support does not depend on the choice of Γ

Definition

$\sigma^{rk}(v) := \sigma_\Gamma(v)$ ***(rank) support*** *of v*

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \sigma^{rk}(v)$$

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

Generalized rank weights

Kurihara, Uyematsu, Matsumoto 2012, 2015

Oggier, Sboui 2012 - Jurrius, Pellikaan 2017

Definition

*Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. A codeword $v \in \mathcal{C}$ is a **minimal codeword** if, for every $v' \in \mathcal{C}$, $\sigma^{\mathrm{rk}}(v') \subseteq \sigma^{\mathrm{rk}}(v)$ implies $v' = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$. $\mathcal{C}$ is **minimal** if all its codewords are minimal.*

Definition

*Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. A codeword $v \in \mathcal{C}$ is a **minimal codeword** if, for every $v' \in \mathcal{C}$, $\sigma^{\mathrm{rk}}(v') \subseteq \sigma^{\mathrm{rk}}(v)$ implies $v' = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$. $\mathcal{C}$ is **minimal** if all its codewords are minimal.*

Definition

*Let $\mathcal{D}$ be an $\mathbb{F}_{q^m}$-subcode of an $[n,k]_{q^m/q}$ code $\mathcal{C}$. The **rank support** of $\mathcal{D}$, $\sigma^{\mathrm{rk}}(\mathcal{D})$, is the $\mathbb{F}_q$-subspace spanned by the rank support of all its codewords. The **rank weight** of $\mathcal{D}$, $\mathrm{wt}_{\mathrm{rk}}(D)$, is the dimension of $\sigma^{\mathrm{rk}}(\mathcal{D})$.*

Definition

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code. A codeword $v \in \mathcal{C}$ is a ***minimal codeword*** *if, for every $v' \in \mathcal{C}$, $\sigma^{\mathrm{rk}}(v') \subseteq \sigma^{\mathrm{rk}}(v)$ implies $v' = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$. $\mathcal{C}$ is* ***minimal*** *if all its codewords are minimal.*

Definition

Let $\mathcal{D}$ be an $\mathbb{F}_{q^m}$-subcode of an $[n,k]_{q^m/q}$ code $\mathcal{C}$. The ***rank support*** *of $\mathcal{D}$, $\sigma^{\mathrm{rk}}(\mathcal{D})$, is the $\mathbb{F}_q$-subspace spanned by the rank support of all its codewords. The* ***rank weight*** *of $\mathcal{D}$, $\mathrm{wt}_{\mathrm{rk}}(D)$, is the dimension of $\sigma^{\mathrm{rk}}(\mathcal{D})$.*

Definition

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code and let $1 \leq j \leq k$. Then the ***j-th generalized rank weight*** *of $\mathcal{C}$ is*

$$d_{\mathrm{rk},j} = \min\left\{\mathrm{wt}_{\mathrm{rk}}(D) :\ \mathcal{D} \subseteq \mathcal{C}, \dim \mathcal{D} = j\right\}$$

Rank-metric codes

Rank-metric codes

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

Rank-metric codes

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

$$d(\mathcal{C}) := d_1 = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \ v \in \mathcal{C}, v \neq 0\}$$

Rank-metric codes

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

$$d(\mathcal{C}) := d_1 = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ is an $[n, k, d]_{q^m/q}$ code

Let $\mathcal{C}$ be an $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

$$d(\mathcal{C}) := d_1 = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \ v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ is an $[n,k,d]_{q^m/q}$ code

Theorem (Singleton Bound - Delsarte 1978)

Let $\mathcal{C}$ be an $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code. Then

$$mk \leq \min\{m(n-d_1+1), n(m-d_1+1)\}. \tag{1}$$

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

$$d(\mathcal{C}) := d_1 = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \; v \in \mathcal{C}, v \neq 0\}$$

$$\mathcal{C} \text{ is an } [n, k, d]_{q^m/q} \text{ code}$$

Theorem (Singleton Bound - Delsarte 1978)

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code. Then

$$mk \leq \min\{m(n - d_1 + 1), n(m - d_1 + 1)\}. \tag{1}$$

A code $\mathcal{C}$ is said to be **maximum rank distance (MRD)** if Bound (1) is met with equality.

Rank-metric codes

Let $\mathcal{C}$ be an $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code, with $d_i := d_{\mathrm{rk},i}(\mathcal{C})$.

$$d(\mathcal{C}) := d_1 = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ is an $[n,k,d]_{q^m/q}$ code

Theorem (Singleton Bound - Delsarte 1978)

Let $\mathcal{C}$ be an $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code. Then

$$mk \leq \min\{m(n-d_1+1), n(m-d_1+1)\}. \tag{1}$$

A code $\mathcal{C}$ is said to be **maximum rank distance (MRD)** if Bound (1) is met with equality.

Proposition (U. Martínez-Peñas 2016)

Let $\mathcal{C}$ be an $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code. Then for each $s \in \{1,\ldots,k\}$ we have

$$d_s \leq \min\left\{n-k+s, sm, \frac{m}{n}(n-k)+m(s-1)+1\right\}. \tag{2}$$

Rank-metric codes

Proposition (Kurihara, Matsumoto, Uyematsu 2015 - Ducoat, Kyureghyan 2015)

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code and let $\mathcal{C}^\perp$ be its dual $[n, n-k, (d_1^\perp, \ldots, d_{n-k}^\perp)]_{q^m/q}$ code. Then

Proposition (Kurihara, Matsumoto, Uyematsu 2015 - Ducoat, Kyureghyan 2015)

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code and let $\mathcal{C}^\perp$ be its dual $[n, n-k, (d_1^\perp, \ldots, d_{n-k}^\perp)]_{q^m/q}$ code. Then

1. $1 \leq d_1 < d_2 < \ldots < d_k \leq n$. ***(Monotonicity)***

The **dual code** $\mathcal{C}^\perp$ of $\mathcal{C}$ is the $[n, n-k]_{q^m/q}$ code given by

$$\mathcal{C}^\perp = \{u \in V(n, q^m) \,:\, uv^\top = 0, \text{ for every } v \in \mathcal{C}\}.$$

Proposition (Kurihara, Matsumoto, Uyematsu 2015 - Ducoat, Kyureghyan 2015)

Let $\mathcal{C}$ be an $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code and let $\mathcal{C}^\perp$ be its dual $[n, n-k, (d_1^\perp, \ldots, d_{n-k}^\perp)]_{q^m/q}$ code. Then

1. $1 \leq d_1 < d_2 < \ldots < d_k \leq n$. ***(Monotonicity)***
2. $\{d_1, \ldots, d_k\} \cup \{n+1-d_1^\perp, \ldots, n+1-d_{n-k}^\perp\} = \{1, \ldots, n\}$. ***(Wei-type duality)***

Rank-metric codes

Definition

An $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ *code is* ***nondegenerate*** *if* $\sigma^{\mathrm{rk}}(\mathcal{C}) = \mathbb{F}_q^n$

Rank-metric codes

Definition

An $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ *code is* ***nondegenerate*** *if* $\sigma^{\mathrm{rk}}(\mathcal{C}) = \mathbb{F}_q^n$

Definition

An $[n, k]_{q^m/q}$ *codes* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *are* ***(linearly) equivalent*** *if there exist* $A \in \mathrm{GL}(n, q)$ *and* $a \in \mathbb{F}_{q^m}^*$ *such that* $\mathcal{C}_2 = a\mathcal{C}_1 A := \{avA \,:\, v \in \mathcal{C}_1\}$

q-systems (Randrianarisoa 2020)

q-systems (Randrianarisoa 2020)

Definition

Let U an $\mathbb{F}_q$-subspace of $V(k,q^m)$. For an $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$, the ***weight*** *of H in U is*

$$\mathrm{wt}_U(H) := \dim_{\mathbb{F}_q}(H \cap U).$$

q-systems (Randrianarisoa 2020)

Definition

*Let U an $\mathbb{F}_q$-subspace of $V(k,q^m)$. For an $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$, the **weight** of H in U is*

$$\mathrm{wt}_U(H) := \dim_{\mathbb{F}_q}(H \cap U).$$

Definition

*An $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ **system** U is an $\mathbb{F}_q$-subspace of $V(k,q^m)$, with $\dim_{\mathbb{F}_q}(U)=n$ and such that $\langle U\rangle_{\mathbb{F}_{q^m}} = V(k,q^m)$. For each $i \in \{1,\ldots,k\}$, the parameter d_i is defined as*

$$d_i := n - \max\{\mathrm{wt}_U(H) \,:\, H \subseteq V(k,q^m) \text{ with } \dim_{\mathbb{F}_{q^m}}(H) = k-i\}.$$

Definition

*Let U an $\mathbb{F}_q$-subspace of $V(k,q^m)$. For an $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$, the **weight** of H in U is*

$$\mathrm{wt}_U(H) := \dim_{\mathbb{F}_q}(H \cap U).$$

Definition

*An $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ **system** U is an $\mathbb{F}_q$-subspace of $V(k,q^m)$, with $\dim_{\mathbb{F}_q}(U)=n$ and such that $\langle U\rangle_{\mathbb{F}_{q^m}} = V(k,q^m)$. For each $i \in \{1,\ldots,k\}$, the parameter d_i is defined as*

$$d_i := n - \max\{\mathrm{wt}_U(H) \,:\, H \subseteq V(k,q^m) \text{ with } \dim_{\mathbb{F}_{q^m}}(H) = k-i\}.$$

Definition

*Two $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ systems U_1, U_2 are **(linearly) equivalent** if there exists $A \in \mathrm{GL}(k,q^m)$ such that $U_2 = U_1 \cdot A := \{uA \,:\, u \in U_1\}$.*

Let $\mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q}$ denote the set of equivalence classes $[U]$ of $[n,k,d]_{q^m/q}$ systems, and let $\mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q}$ denote the set of equivalence classes $[\mathcal{C}]$ of nondegenerate $[n,k,d]_{q^m/q}$ codes. One can define the maps

$$\begin{array}{rccc} \Phi: & \mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q} & \longrightarrow & \mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q} \\ & [\mathrm{rowsp}(u_1^\top \mid \ldots \mid u_n^\top)] & \longmapsto & [\langle u_1,\ldots u_n\rangle_{\mathbb{F}_q}] \end{array},$$

$$\begin{array}{rccc} \Psi: & \mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q} & \longrightarrow & \mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q} \\ & [\langle u_1,\ldots u_n\rangle_{\mathbb{F}_q}] & \longmapsto & [\mathrm{rowsp}(u_1^\top \mid \ldots \mid u_n^\top)] \end{array}.$$

Theorem (Randrianarisoa 2020)

The maps Φ and Ψ are well-defined and they are one the inverse of each other. Hence, they define a one-to-one correspondence between equivalence classes of $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ codes and equivalence classes of $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ systems.

Let $\mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q}$ denote the set of equivalence classes $[U]$ of $[n,k,d]_{q^m/q}$ systems, and let $\mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q}$ denote the set of equivalence classes $[\mathcal{C}]$ of nondegenerate $[n,k,d]_{q^m/q}$ codes. One can define the maps

$$\begin{array}{rccc} \Phi: & \mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q} & \longrightarrow & \mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q} \\ & [\mathrm{rowsp}(u_1^\top \mid \ldots \mid u_n^\top)] & \longmapsto & [\langle u_1,\ldots u_n\rangle_{\mathbb{F}_q}] \end{array},$$

$$\begin{array}{rccc} \Psi: & \mathfrak{U}(n,k,(d_1,\ldots,d_k))_{q^m/q} & \longrightarrow & \mathfrak{C}(n,k,(d_1,\ldots,d_k))_{q^m/q} \\ & [\langle u_1,\ldots u_n\rangle_{\mathbb{F}_q}] & \longmapsto & [\mathrm{rowsp}(u_1^\top \mid \ldots \mid u_n^\top)] \end{array}.$$

Theorem (Randrianarisoa 2020)

The maps Φ and Ψ are well-defined and they are one the inverse of each other. Hence, they define a one-to-one correspondence between equivalence classes of $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ codes and equivalence classes of $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ systems. Moreover, codewords of $\mathcal{C}$ of rank weight w correspond to $\mathbb{F}_{q^m}$-hyperplanes of $V(k,q^m)$ with $\dim_{\mathbb{F}_q}(H\cap U)=n-w$.

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n, k]_{q^m/q}$ system U is said to be an $(h, r)_q$-**evasive subspace** (or simply $(h, r)_q$-**evasive**) if $\langle U\rangle_{\mathbb{F}_{q^m}} = V(k, q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k, q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n, k]_{q^m/q}$ system U is said to be an $(h, r)_q$-**evasive subspace** (or simply $(h, r)_q$-**evasive**) if $\langle U \rangle_{\mathbb{F}_{q^m}} = V(k, q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k, q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*
*When $r = h$, an $(h, h)_q$-evasive subspace is called h-**scattered**.*

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n,k]_{q^m/q}$ system U is said to be an $(h,r)_q$-**evasive subspace** (or simply $(h,r)_q$-**evasive**) if $\langle U\rangle_{\mathbb{F}_{q^m}} = V(k,q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*
*When $r = h$, an $(h,h)_q$-evasive subspace is called h-**scattered**. Furthermore, when $h = 1$, a 1-scattered subspace will be simply called **scattered**.*

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n,k]_{q^m/q}$ system U is said to be an $(h,r)_q$-**evasive subspace** (or simply $(h,r)_q$-**evasive**) if $\langle U \rangle_{\mathbb{F}_{q^m}} = V(k,q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*
*When $r = h$, an $(h,h)_q$-evasive subspace is called h-**scattered**. Furthermore, when $h = 1$, a 1-scattered subspace will be simply called **scattered**.*

Theorem (Blokhuis, Lavrauw 2000)

If U is a 1-scattered of $V(k,q^m)$, then $\dim_{\mathbb{F}_q} U \leq \left\lfloor \frac{km}{2} \right\rfloor$.

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n,k]_{q^m/q}$ system U is said to be an $(h,r)_q$-**evasive subspace** (or simply $(h,r)_q$-**evasive**) if $\langle U\rangle_{\mathbb{F}_{q^m}} = V(k,q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*
*When $r = h$, an $(h,h)_q$-evasive subspace is called h-**scattered**. Furthermore, when $h = 1$, a 1-scattered subspace will be simply called **scattered**.*

Theorem (Blokhuis, Lavrauw 2000)

If U is a 1-scattered of $V(k,q^m)$, then $\dim_{\mathbb{F}_q} U \leq \left\lfloor \frac{km}{2} \right\rfloor$.

Theorem (Csajbók, M., Polverino, Zullo 2021)

If U is an h-scattered of $V(k,q^m)$, then either $\dim_{\mathbb{F}_q} U = k$ and U defines a subgeometry of $\mathrm{PG}(k-1,q^m)$ (and it is $(k-1)$-scattered) or $\dim_{\mathbb{F}_q}(U) \leq \left\lfloor \frac{km}{h+1} \right\rfloor$.

Evasive subspace (Bartoli, Csajbók, M., Trombetti 2021)

Definition

*Let h, r be positive integers such that $h < k$. An $[n, k]_{q^m/q}$ system U is said to be an $(h, r)_q$-**evasive subspace** (or simply $(h, r)_q$-**evasive**) if $\langle U \rangle_{\mathbb{F}_{q^m}} = V(k, q^m)$ and $\dim_{\mathbb{F}_q}(U \cap H) \leq r$ for each $\mathbb{F}_{q^m}$-subspace H of $V(k, q^m)$ with $\dim_{\mathbb{F}_{q^m}}(H) = h$.*
*When $r = h$, an $(h, h)_q$-evasive subspace is called h-**scattered**. Furthermore, when $h = 1$, a 1-scattered subspace will be simply called **scattered**.*

Theorem (Blokhuis, Lavrauw 2000)

If U is a 1-scattered of $V(k, q^m)$, then $\dim_{\mathbb{F}_q} U \leq \left\lfloor \frac{km}{2} \right\rfloor$.

Theorem (Csajbók, M., Polverino, Zullo 2021)

If U is an h-scattered of $V(k, q^m)$, then either $\dim_{\mathbb{F}_q} U = k$ and U defines a subgeometry of $\mathrm{PG}(k-1, q^m)$ (and it is $(k-1)$-scattered) or $\dim_{\mathbb{F}_q}(U) \leq \left\lfloor \frac{km}{h+1} \right\rfloor$.

When the previous equality is reached, then U is said be **maximum**.

Existence results of h-scattered subspaces

Theorem

Let k, m be positive integers and let q be a prime power. The following hold.

Existence results of h-scattered subspaces

Theorem

Let k, m be positive integers and let q be a prime power. The following hold.

1. *There exist maximum $(k-1)$-scattered $[m, k, m-k+1]_{q^m/q}$ systems (Delsarte).*

Existence results of h-scattered subspaces

Theorem

Let k, m be positive integers and let q be a prime power. The following hold.

1. *There exist maximum $(k-1)$-scattered $[m, k, m-k+1]_{q^m/q}$ systems (Delsarte).*
2. *Assume that km is even. Then, there exist maximum scattered $[\frac{km}{2}, k, m-1]_{q^m/q}$ systems (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, G.M., Polverino, Zullo).*

Existence results of h-scattered subspaces

Theorem

Let k, m be positive integers and let q be a prime power. The following hold.

1. *There exist maximum $(k-1)$-scattered $[m, k, m-k+1]_{q^m/q}$ systems (Delsarte).*
2. *Assume that km is even. Then, there exist maximum scattered $[\frac{km}{2}, k, m-1]_{q^m/q}$ systems (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, G.M., Polverino, Zullo).*

Theorem (Zini, Zullo 2021)

Let $n := \frac{km}{h+1}$ and $m \geq h+3$. Let U be an $[n, k]_{q^m/q}$ system and let $\mathcal{C} \in \Psi([U])$ be any of its associated $[n, k]_{q^m/q}$ codes. Then, U is maximum h-scattered if and only if $\mathcal{C}$ is an MRD code.

Evasive subspace and rank-metric codes

Theorem (G.M., Neri, Trombetti 2023)

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$. Then, the following are equivalent.

1. *U is an $(h,r)_q$-evasive subspace.*
2. $\mathrm{d}_{\mathrm{rk},k-h}(\mathcal{C}) \geq n-r$.
3. $\mathrm{d}_{\mathrm{rk},r-h+1}(\mathcal{C}^{\perp}) \geq r+2$.

Evasive subspace and rank-metric codes

Theorem (G.M., Neri, Trombetti 2023)

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$. Then, the following are equivalent.

1. *U is an $(h,r)_q$-evasive subspace.*
2. $\mathrm{d}_{\mathrm{rk},k-h}(\mathcal{C}) \geq n-r$.
3. $\mathrm{d}_{\mathrm{rk},r-h+1}(\mathcal{C}^{\perp}) \geq r+2$.

In particular, $\mathrm{d}_{\mathrm{rk},k-h}(\mathcal{C}) = n-r$ if and only if U is $(h,r)_q$-evasive but not $(h,r-1)_q$-evasive.

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U \rangle_{\mathbb{F}_{q^m}} = H$. When $t = 1$, we simply say that U is **(linear) cutting**.*

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U \rangle_{\mathbb{F}_{q^m}} = H$. When $t=1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U \rangle_{\mathbb{F}_{q^m}} = H$. When $t = 1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Proposition

- *Let U be a cutting $[n,k]_{q^m/q}$ system, with $k \geq 2$. Then $n \geq m + k - 1$.*

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H\cap U\rangle_{\mathbb{F}_{q^m}} = H$. When $t=1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Proposition

- *Let U be a cutting $[n,k]_{q^m/q}$ system, with $k\geq 2$. Then $n \geq m+k-1$.*
- *If U is a scattered $[n,3]_{q^m/q}$ system with $n\geq m+2$, then U is cutting.*

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U \rangle_{\mathbb{F}_{q^m}} = H$. When $t=1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Proposition

- *Let U be a cutting $[n,k]_{q^m/q}$ system, with $k \geq 2$. Then $n \geq m+k-1$.*
- *If U is a scattered $[n,3]_{q^m/q}$ system with $n \geq m+2$, then U is cutting.*

Questions:

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U\rangle_{\mathbb{F}_{q^m}} = H$. When $t = 1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Proposition

- *Let U be a cutting $[n,k]_{q^m/q}$ system, with $k \geq 2$. Then $n \geq m+k-1$.*
- *If U is a scattered $[n,3]_{q^m/q}$ system with $n \geq m+2$, then U is cutting.*

Questions:

1. Can we generalize this result to larger value of $k > 3$?

Linear cutting q-systems (Alfarano, Borello, Neri, Ravagnani 2022)

Definition

*An $[n,k]_{q^m/q}$ system U is said to be t-**cutting** if for every $\mathbb{F}_{q^m}$-subspace H of $V(k,q^m)$ of codimension t we have $\langle H \cap U\rangle_{\mathbb{F}_{q^m}} = H$. When $t = 1$, we simply say that U is **(linear) cutting**.*

Theorem

Let $\mathcal{C}$ be an $[n,k]_{q^m/q}$ code, and let $U \in \Phi([\mathcal{C}])$ be any of the associated $[n,k]_{q^m/q}$ systems. Then, $\mathcal{C}$ is a minimal rank-metric code if and only if U is cutting.

Proposition

- *Let U be a cutting $[n,k]_{q^m/q}$ system, with $k \geq 2$. Then $n \geq m+k-1$.*
- *If U is a scattered $[n,3]_{q^m/q}$ system with $n \geq m+2$, then U is cutting.*

Questions:

1. Can we generalize this result to larger value of $k > 3$?
2. Does the converse of this result hold?

Theorem (Bartoli-G.M.-Neri 2023)

Let U be an $[n,k]_{q^m/q}$ system. Then, U is $(k-2, n-m-1)_q$-evasive if and only if it is cutting.

Theorem (Bartoli-G.M.-Neri 2023)

Let U be an $[n, k]_{q^m/q}$ system. Then, U is $(k-2, n-m-1)_q$-evasive if and only if it is cutting.

Corollary (Bartoli-G.M.-Neri 2023)

Let $\mathcal{C}$ be a nondegenerate $[n, k, (d_1, \ldots, d_k)]_{q^m/q}$ code. Then, $\mathcal{C}$ is minimal if and only if $d_2 \geq m+1$.

Evasive subspaces and cutting q-systems

Theorem (Bartoli-G.M.-Neri 2023)

Let U be an $[n,k]_{q^m/q}$ system. Then, U is $(k-2, n-m-1)_q$-evasive if and only if it is cutting.

Corollary (Bartoli-G.M.-Neri 2023)

Let $\mathcal{C}$ be a nondegenerate $[n,k,(d_1,\ldots,d_k)]_{q^m/q}$ code. Then, $\mathcal{C}$ is minimal if and only if $d_2 \geq m+1$.

Corollary (Bartoli-G.M.-Neri 2023)

If $m < (k-1)^2$ then there are no cutting $[m+k-1,k]_{q^m/q}$ systems.

Cutting q-systems and rank-metric codes

Problem

Construct minimal rank-metric codes reaching the lower bound on the dimension of the associated q-system and with the maximum value for the corresponding values of generalized rank weights.

Shortest minimal $[n,3]_{q^m/q}$ code

Shortest minimal $[n,3]_{q^m/q}$ code

Minimal $[m+2,3]_{q^m/q}$ code

Shortest minimal $[n, 3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3, q^m)$ of dimension $m + 2$

$$\Updownarrow$$

Minimal $[m + 2, 3]_{q^m/q}$ code

Shortest minimal $[n,3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3,q^m)$ of dimension $m+2$

$$\Updownarrow$$

Minimal $[m+2,3]_{q^m/q}$ code

Shortest minimal $[n, 3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3, q^m)$ of dimension $m + 2$

$$\Updownarrow$$

Minimal $[m + 2, 3]_{q^m/q}$ code

- (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, M., Polverino, Zullo)
  If $m \geq 4$ is even there always exists maximum scattered in $V(3, q^m)$ and hence scattered of dimension $m + 2$

Shortest minimal $[n,3]_{q^m/q}$ code

$$\mathbb{F}_q\text{-scattered subspace in } V(3,q^m) \text{ of dimension } m+2$$

$$\Updownarrow$$

$$\text{Minimal } [m+2,3]_{q^m/q} \text{ code}$$

- (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, M., Polverino, Zullo)
  If $m \geq 4$ is even there always exists maximum scattered in $V(3,q^m)$ and hence scattered of dimension $m+2$
- (Alfarano-Borello-Neri-Ravagnani 2022)
  If $m \not\equiv 3,5 \pmod 6$ and $m \geq 4$ there are scattered in $V(3,q^m)$ of dimension $m+2$

Shortest minimal $[n, 3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3, q^m)$ of dimension $m + 2$

$$\Updownarrow$$

Minimal $[m + 2, 3]_{q^m/q}$ code

- (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, M., Polverino, Zullo)
  If $m \geq 4$ is even there always exists maximum scattered in $V(3, q^m)$ and hence scattered of dimension $m + 2$
- (Alfarano-Borello-Neri-Ravagnani 2022)
  If $m \not\equiv 3, 5 \pmod 6$ and $m \geq 4$ there are scattered in $V(3, q^m)$ of dimension $m + 2$
- (Bartoli-Csajbók-G.M.-Trombetti 2021)
  There are examples of scattered in $V(3, q^5)$ of dimension 7, $q = p^{15s+1}$, $(15, s) = 1$ if $p = 2, 3$ and $s = 1$ if $p = 5$

Shortest minimal $[n,3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3,q^m)$ of dimension $m+2$

$$\Updownarrow$$

Minimal $[m+2,3]_{q^m/q}$ code

- (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, M., Polverino, Zullo)
  If $m \geq 4$ is even there always exists maximum scattered in $V(3,q^m)$ and hence scattered of dimension $m+2$
- (Alfarano-Borello-Neri-Ravagnani 2022)
  If $m \not\equiv 3,5 \pmod 6$ and $m \geq 4$ there are scattered in $V(3,q^m)$ of dimension $m+2$
- (Bartoli-Csajbók-G.M.-Trombetti 2021)
  There are examples of scattered in $V(3,q^5)$ of dimension 7, $q = p^{15s+1}$, $(15,s) = 1$ if $p = 2,3$ and $s = 1$ if $p = 5$
- (Gruica-Ravagnani-Sheekey-Zullo, arxiv)
  Examples of minimal $[m+3,3]_{q^m/q}$-codes for all $m \geq 4$ (they correspond to $(1,2)$-evasive subspaces)

Shortest minimal $[n,3]_{q^m/q}$ code

$\mathbb{F}_q$-scattered subspace in $V(3,q^m)$ of dimension $m+2$

$$\Updownarrow$$

Minimal $[m+2,3]_{q^m/q}$ code

- (Ball, Bartoli, Blokhuis, Csajbók, Giulietti, Lavrauw, M., Polverino, Zullo)
  If $m \geq 4$ is even there always exists maximum scattered in $V(3,q^m)$ and hence scattered of dimension $m+2$
- (Alfarano-Borello-Neri-Ravagnani 2022)
  If $m \not\equiv 3,5 \pmod 6$ and $m \geq 4$ there are scattered in $V(3,q^m)$ of dimension $m+2$
- (Bartoli-Csajbók-G.M.-Trombetti 2021)
  There are examples of scattered in $V(3,q^5)$ of dimension 7, $q=p^{15s+1}$, $(15,s)=1$ if $p=2,3$ and $s=1$ if $p=5$
- (Gruica-Ravagnani-Sheekey-Zullo, arxiv)
  Examples of minimal $[m+3,3]_{q^m/q}$-codes for all $m \geq 4$ (they correspond to $(1,2)$-evasive subspaces)

Question

Are there examples of minimal $[m+2,3]_{q^m/q}$-codes for infinitely values of q and m?

Minimal $[m+2,3]_{q^m/q}$-code

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $V = \mathbb{F}_{q^m}^3$, $q = p^e$ *and* $m \geq 5$ *odd. Consider the* $(m+2)$*-dimensional subspace*

$$\mathcal{U}_\sigma = \{(x, x^\sigma + a, x^{\sigma^2} + b) : x \in \mathbb{F}_{q^m}, a, b \in \mathbb{F}_q\}$$

of V, *where* $\sigma : x \in \mathbb{F}_{q^m} \longrightarrow x^{q^s} \in \mathbb{F}_{q^m}$, $1 \leq s \leq m-1$ *and* $(s, m) = 1$. *If*

- *i*) $(q-1, m) = 1$,
- *ii*) *p does not divide m,*
- *iii*) *the polynomial*

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^\sigma + X \in \mathbb{F}_q[X]$$

has not roots in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$,

then $\mathcal{U}_\sigma$ *is scattered.*

Minimal $[m+2,3]_{q^m/q}$-code

Minimal $[m+2,3]_{q^m/q}$-code

Trivial cases:

Minimal $[m+2,3]_{q^m/q}$-code

Trivial cases:

Trivial cases:

- $q = 2$, $s = 1$ and $(m, 3) = 1$
  iii) $\to X^5 + X^3 + X^2 + X = X(X+1)(X^3 + X^2 + 1)$ has no roots in $\mathbb{F}_{2^m} \setminus \mathbb{F}_2$. This is equivalent to say that the polynomial $X^3 + X^2 + 1$ has no roots in $\mathbb{F}_{2^m}$. Since the latter polynomial has degree 3, has no roots in $\mathbb{F}_2$ and $(m, 3) = 1$, it also has no roots in $\mathbb{F}_{2^m}$.

Minimal $[m+2,3]_{q^m/q}$-code

Trivial cases:

- $q=2$, $s=1$ and $(m,3)=1$
  iii) $\rightarrow X^5+X^3+X^2+X = X(X+1)(X^3+X^2+1)$ has no roots in $\mathbb{F}_{2^m}\setminus\mathbb{F}_2$. This is equivalent to say that the polynomial X^3+X^2+1 has no roots in $\mathbb{F}_{2^m}$. Since the latter polynomial has degree 3, has no roots in $\mathbb{F}_2$ and $(m,3)=1$, it also has no roots in $\mathbb{F}_{2^m}$.
- $q=3$, $s=1$ and $(m,12)=1$
  iii) $\rightarrow X^3+2X^2+2X+2$ and X^4+X^3+2X+1, have no roots in $\mathbb{F}_{3^m}$. Since the latter polynomials have degrees 3 and 4, they have no roots in $\mathbb{F}_3$ and $(m,12)=1$, they also have no roots in $\mathbb{F}_{3^m}$.

Minimal $[m+2,3]_{q^m/q}$-code

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $V = \mathbb{F}_{q^m}^3$, $q = p^e$ *and* $m \geq 5$ *odd. Consider the* $(m+2)$*-dimensional subspace*

$$\mathcal{U}_\sigma = \{(x, x^\sigma + a, x^{\sigma^2} + b) : x \in \mathbb{F}_{q^m}, a, b \in \mathbb{F}_q\}$$

of V*, where* $\sigma : x \in \mathbb{F}_{q^m} \longrightarrow x^{q^s} \in \mathbb{F}_{q^m}$, $1 \leq s \leq m-1$ *and* $(s, m) = 1$*. If*

i) $(q-1, m) = 1$,

ii) p *does not divide* m,

iii) *the polynomial*

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^\sigma + X \in \mathbb{F}_q[X]$$

has not roots in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$,

then $\mathcal{U}_\sigma$ *is scattered.*

Sketch of the proof

Sketch of the proof

Consider the 2-dimensional $\mathbb{F}_{q^m}$-vector subspaces of $\mathbb{F}_{q^m}^3$ containing the vector $(0,0,1)$, they have equation

$$\ell_\lambda : x_1 = \lambda x_0 \text{ or } \ell_\infty : x_0 = 0$$

Sketch of the proof

Consider the 2-dimensional $\mathbb{F}_{q^m}$-vector subspaces of $\mathbb{F}_{q^m}^3$ containing the vector $(0,0,1)$, they have equation

$$\ell_\lambda : x_1 = \lambda x_0 \text{ or } \ell_\infty : x_0 = 0$$

and define $\mathcal{Z}_{\lambda,\sigma} = \mathcal{U}_\sigma \cap \ell_\lambda$ with $\lambda \in \mathbb{F}_{q^m} \cup \{\infty\}$.

Sketch of the proof

Consider the 2-dimensional $\mathbb{F}_{q^m}$-vector subspaces of $\mathbb{F}^3_{q^m}$ containing the vector $(0,0,1)$, they have equation

$$\ell_\lambda : x_1 = \lambda x_0 \text{ or } \ell_\infty : x_0 = 0$$

and define $\mathcal{Z}_{\lambda,\sigma} = \mathcal{U}_\sigma \cap \ell_\lambda$ with $\lambda \in \mathbb{F}_{q^m} \cup \{\infty\}$. Since $\mathcal{U}_\sigma \cap \langle v \rangle_{\mathbb{F}_{q^m}} = \mathcal{Z}_{\lambda,\sigma} \cap \langle v \rangle_{\mathbb{F}_{q^m}}$ for some $\lambda \in \mathbb{F}_q \cup \{\infty\}$, then

$\mathcal{U}_\sigma$ is a scattered subspace if and only if $\mathcal{Z}_{\lambda,\sigma}$ is scattered as well for any $\lambda \in \mathbb{F}_{q^m} \cup \{\infty\}$.

Sketch of the proof

Sketch of the proof

Note that

$$\mathcal{U}_\sigma = \mathcal{W}_\sigma \oplus \mathcal{Z}_{\infty,\sigma},$$

where $\mathcal{W}_\sigma = \{(x, x^\sigma, x^{\sigma^2}) : x \in \mathbb{F}_{q^m}\}$ and $\mathcal{Z}_{\infty,\sigma} = \langle (0,0,1), (0,1,0) \rangle_{\mathbb{F}_q}$.

Sketch of the proof

Note that

$$\mathcal{U}_\sigma = \mathcal{W}_\sigma \oplus \mathcal{Z}_{\infty,\sigma},$$

where $\mathcal{W}_\sigma = \{(x, x^\sigma, x^{\sigma^2}) : x \in \mathbb{F}_{q^m}\}$ and $\mathcal{Z}_{\infty,\sigma} = \langle (0,0,1), (0,1,0) \rangle_{\mathbb{F}_q}$.

Let $\lambda \in \mathbb{F}_{q^m}$ and $\bar{v} = (\bar{x}, \bar{x}^\sigma + \bar{a}, x^{\sigma^2} + \bar{b}) \in \mathcal{Z}_{\lambda,\sigma}$ with $\bar{x} \in \mathbb{F}^*_{q^m}$, $\bar{a}, \bar{b} \in \mathbb{F}_q$ and, hence, $\bar{x}^\sigma + \bar{a} = \lambda \bar{x}$.

Sketch of the proof

Note that

$$\mathcal{U}_\sigma = \mathcal{W}_\sigma \oplus \mathcal{Z}_{\infty,\sigma},$$

where $\mathcal{W}_\sigma = \{(x, x^\sigma, x^{\sigma^2}) : x \in \mathbb{F}_{q^m}\}$ and $\mathcal{Z}_{\infty,\sigma} = \langle (0,0,1),(0,1,0)\rangle_{\mathbb{F}_q}$.

Let $\lambda \in \mathbb{F}_{q^m}$ and $\bar{v} = (\bar{x}, \bar{x}^\sigma + \bar{a}, x^{\sigma^2} + \bar{b}) \in \mathcal{Z}_{\lambda,\sigma}$ with $\bar{x} \in \mathbb{F}^*_{q^m}$, $\bar{a}, \bar{b} \in \mathbb{F}_q$ and, hence, $\bar{x}^\sigma + \bar{a} = \lambda \bar{x}$.
The property of being scattered for $\mathcal{Z}_{\lambda,\sigma}$ is equivalent to require that the number of triples $(y, y^\sigma + a, y^{\sigma^2} + b)$ with $y \in \mathbb{F}_{q^m}$, $a, b \in \mathbb{F}_q$ such that

$$\begin{cases} \lambda y = y^\sigma + a \\ \frac{y}{\bar{x}}(\bar{x}^\sigma s + \bar{a}) = y^\sigma + a \\ \frac{y}{\bar{x}}(\bar{x}^{\sigma^2} + \bar{b}) = y^{\sigma^2} + b \end{cases}$$

is at most q.

Sketch of the proof

Note that

$$\mathcal{U}_\sigma = \mathcal{W}_\sigma \oplus \mathcal{Z}_{\infty,\sigma},$$

where $\mathcal{W}_\sigma = \{(x, x^\sigma, x^{\sigma^2}) : x \in \mathbb{F}_{q^m}\}$ and $\mathcal{Z}_{\infty,\sigma} = \langle (0,0,1), (0,1,0) \rangle_{\mathbb{F}_q}$.

Let $\lambda \in \mathbb{F}_{q^m}$ and $\bar{v} = (\bar{x}, \bar{x}^\sigma + \bar{a}, x^{\sigma^2} + \bar{b}) \in \mathcal{Z}_{\lambda,\sigma}$ with $\bar{x} \in \mathbb{F}^*_{q^m}$, $\bar{a}, \bar{b} \in \mathbb{F}_q$ and, hence, $\bar{x}^\sigma + \bar{a} = \lambda \bar{x}$.
The property of being scattered for $\mathcal{Z}_{\lambda,\sigma}$ is equivalent to require that the number of triples $(y, y^\sigma + a, y^{\sigma^2} + b)$ with $y \in \mathbb{F}_{q^m}$, $a, b \in \mathbb{F}_q$ such that

$$\begin{cases} \lambda y = y^\sigma + a \\ \frac{y}{\bar{x}}(\bar{x}^\sigma s + \bar{a}) = y^\sigma + a \\ \frac{y}{\bar{x}}(\bar{x}^{\sigma^2} + \bar{b}) = y^{\sigma^2} + b \end{cases}$$

is at most q. By using the second and third equation, then $\mathcal{Z}_{\lambda,\sigma}$ is scattered if and only if for any $\bar{v} \in \mathcal{Z}_{\lambda,\sigma}$, the previous System is satisfied by at most q values $y \in \mathbb{F}_{q^m}$.

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_q}$

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_q}$

From the previous system we get that if the equation

$$y^{\sigma^2} - (1+\lambda)y^{\sigma} + \lambda y = 0$$

has at most q solutions then the subspace $\mathcal{Z}_{\lambda,\sigma}$ of V is scattered.

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_q}$

From the previous system we get that if the equation

$$y^{\sigma^2} - (1+\lambda)y^{\sigma} + \lambda y = 0$$

has at most q solutions then the subspace $\mathcal{Z}_{\lambda,\sigma}$ of V is scattered.

By [McGuire-Sheekey, Csajbók-G.M.-Polverino-Zullo 2019], this polynomial has exactly q^2 solutions in $\mathbb{F}_{q^m}$ if and only if the m-th power of the matrix

$$A_\lambda = \begin{pmatrix} 0 & -\lambda \\ 1 & 1+\lambda \end{pmatrix}, \tag{3}$$

is equal to the identity matrix I_2.

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_q}$

From the previous system we get that if the equation

$$y^{\sigma^2} - (1+\lambda)y^{\sigma} + \lambda y = 0$$

has at most q solutions then the subspace $\mathcal{Z}_{\lambda,\sigma}$ of V is scattered.

By [McGuire-Sheekey, Csajbók-G.M.-Polverino-Zullo 2019], this polynomial has exactly q^2 solutions in $\mathbb{F}_{q^m}$ if and only if the m-th power of the matrix

$$A_\lambda = \begin{pmatrix} 0 & -\lambda \\ 1 & 1+\lambda \end{pmatrix}, \tag{3}$$

is equal to the identity matrix I_2.
This implies $\lambda = 1$ and the matrix

$$A_1^m = \begin{pmatrix} -(m-1) & -m \\ m & m+1 \end{pmatrix}$$

equals the identity matrix

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_q}$

From the previous system we get that if the equation

$$y^{\sigma^2} - (1+\lambda)y^{\sigma} + \lambda y = 0$$

has at most q solutions then the subspace $\mathcal{Z}_{\lambda,\sigma}$ of V is scattered.

By [McGuire-Sheekey, Csajbók-G.M.-Polverino-Zullo 2019], this polynomial has exactly q^2 solutions in $\mathbb{F}_{q^m}$ if and only if the m-th power of the matrix

$$A_\lambda = \begin{pmatrix} 0 & -\lambda \\ 1 & 1+\lambda \end{pmatrix}, \tag{3}$$

is equal to the identity matrix I_2.
This implies $\lambda = 1$ and the matrix

$$A_1^m = \begin{pmatrix} -(m-1) & -m \\ m & m+1 \end{pmatrix}$$

equals the identity matrix if and only if $p|m$.

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q}$

Sketch of the proof

$\boxed{\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q}$

If λ is not a root of the polynomial

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X \in \mathbb{F}_q[X],$$

then the subspace $\mathcal{Z}_{\lambda,\sigma}$ of V is scattered.

Minimal $[m+2,3]_{q^m/q}$-code

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $V=\mathbb{F}_{q^m}^3$, $q=p^e$ and $m\geq 5$ odd. Consider the $(m+2)$-dimensional subspace

$$\mathcal{U}_\sigma=\{(x,x^\sigma+a,x^{\sigma^2}+b) : x\in\mathbb{F}_{q^m}, a,b\in\mathbb{F}_q\}$$

of V, where $\sigma : x\in\mathbb{F}_{q^m}\longrightarrow x^{q^s}\in\mathbb{F}_{q^m}$, $1\leq s\leq m-1$ and $(s,m)=1$. If

i) $(q-1,m)=1$,

ii) *p does not divide m,*

iii) *the polynomial*

$$Q(X)=X^{\sigma^2+1}-X^{\sigma+1}-X^\sigma+X\in\mathbb{F}_q[X]$$

has not roots in $\mathbb{F}_{q^m}\setminus\mathbb{F}_q$,

then $\mathcal{U}_\sigma$ is scattered.

Minimal $[m+2,3]_{q^m/q}$-code

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $V=\mathbb{F}_{q^m}^3$, $q=p^e$ *and* $m\geq 5$ *odd. Consider the* $(m+2)$*-dimensional subspace*

$$\mathcal{U}_\sigma=\{(x,x^\sigma+a,x^{\sigma^2}+b): x\in\mathbb{F}_{q^m}, a,b\in\mathbb{F}_q\}$$

of V, *where* $\sigma: x\in\mathbb{F}_{q^m}\longrightarrow x^{q^s}\in\mathbb{F}_{q^m}$, $1\leq s\leq m-1$ *and* $(s,m)=1$. *If*

i) $(q-1,m)=1$,

ii) p *does not divide* m,

iii) *the polynomial*

$$Q(X)=X^{\sigma^2+1}-X^{\sigma+1}-X^\sigma+X\in\mathbb{F}_q[X]$$

has not roots in $\mathbb{F}_{q^m}\setminus\mathbb{F}_q$,

then $\mathcal{U}_\sigma$ *is scattered.*

Question

When $Q(X)$ *has no roots in* $\mathbb{F}_{q^m}\setminus\mathbb{F}_q$*?*

Minimal $[m+2,3]_{q^m/q}$-code

Minimal $[m+2,3]_{q^m/q}$-code

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X = Q_1(X)Q_2(X),$$

where $Q_1(X) = X^{\sigma} - X$ and $Q_2(X) = X(X^{\sigma} - X)^{\sigma-1} - 1$. The polynomial $Q_2(X)$ has degree $\sigma^2 - \sigma + 1$.

Minimal $[m+2,3]_{q^m/q}$-code

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X = Q_1(X)Q_2(X),$$

where $Q_1(X) = X^{\sigma} - X$ and $Q_2(X) = X(X^{\sigma} - X)^{\sigma-1} - 1$. The polynomial $Q_2(X)$ has degree $\sigma^2 - \sigma + 1$.

If $(r, m) = 1$ (where r is the degree of the splitting field over $\mathbb{F}_q$ of the polynomial

$$X(X^{\sigma} - X)^{\sigma-1} - 1 \in \mathbb{F}_q[X])$$

then $Q(X)$ has no roots in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$.

Minimal $[m+2,3]_{q^m/q}$-code

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X = Q_1(X)Q_2(X),$$

where $Q_1(X) = X^{\sigma} - X$ and $Q_2(X) = X(X^{\sigma} - X)^{\sigma-1} - 1$. The polynomial $Q_2(X)$ has degree $\sigma^2 - \sigma + 1$.

If $(r, m) = 1$ (where r is the degree of the splitting field over $\mathbb{F}_q$ of the polynomial

$$X(X^{\sigma} - X)^{\sigma-1} - 1 \in \mathbb{F}_q[X])$$

then $Q(X)$ has no roots in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$.

Recall that a polynomial $f(X)$ of degree n with coefficients over a field $\mathbb{F}$ has splitting field $\mathbb{K}$ of degree at most $n!$ over $\mathbb{F}$.

Minimal $[m+2,3]_{q^m/q}$-code

Corollary (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $V = \mathbb{F}_{q^m}^3$, $q = p^e$ *and* $m \geq 5$ *odd. Consider the* $(m+2)$*-dimensional subspace*

$$\mathcal{U}_\sigma = \{(x, x^\sigma + a, x^{\sigma^2} + b) : x \in \mathbb{F}_{q^m}, a, b \in \mathbb{F}_q\}$$

of V, *where* $\sigma : x \in \mathbb{F}_{q^m} \longrightarrow x^{q^s} \in \mathbb{F}_{q^m}$, $1 \leq s \leq m-1$ *and* $(s, m) = 1$. *If*

- *i)* $(q-1, m) = 1$,
- *ii)* *p does not divide m,*
- *iii)* $(m, (q^{2s} - q^s + 1)!) = 1$

then $\mathcal{U}_\sigma$ *is scattered.*

Question

When the polynomial

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X = Q_1(X)Q_2(X),$$

has no roots in $\mathbb{F}_{q^m} \setminus \mathbb{F}_q$*?*

Linearized & projective polynomials

Linearized & projective polynomials

$$L(X) = \sum_{i=0}^{d} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^m}[x]$$

σ-linearized polynomial

Linearized & projective polynomials

$$L(X) = \sum_{i=0}^{d} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^m}[x]$$

σ-linearized polynomial

$$P(X) = \sum_{i=0}^{d} \alpha_i X^{\frac{\sigma^i - 1}{\sigma - 1}} \in \mathbb{F}_{q^m}[X]$$

σ-projective polynomial

Linearized & projective polynomials

$$L(X) = \sum_{i=0}^{d} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^m}[x]$$

σ-linearized polynomial

$$P(X) = \sum_{i=0}^{d} \alpha_i X^{\frac{\sigma^i - 1}{\sigma - 1}} \in \mathbb{F}_{q^m}[X]$$

σ-projective polynomial

$$L(X) = XP_L(X^{\sigma - 1})$$

Linearized & projective polynomials

$$L(X) = \sum_{i=0}^{d} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^m}[x]$$

σ-linearized polynomial

$$P(X) = \sum_{i=0}^{d} \alpha_i X^{\frac{\sigma^i - 1}{\sigma - 1}} \in \mathbb{F}_{q^m}[X]$$

σ-projective polynomial

$$L(X) = X P_L(X^{\sigma - 1})$$

$$C_L = \begin{pmatrix} 0 & 0 & \dots & 0 & -\frac{\alpha_0}{\alpha_d} \\ 1 & 0 & \dots & 0 & -\frac{\alpha_1}{\alpha_d} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -\frac{\alpha_{d-1}}{\alpha_d} \end{pmatrix}.$$

Linearized & projective polynomials

$$L(X) = \sum_{i=0}^{d} \alpha_i X^{\sigma^i} \in \mathbb{F}_{q^m}[x]$$

σ-linearized polynomial

$$P(X) = \sum_{i=0}^{d} \alpha_i X^{\frac{\sigma^i - 1}{\sigma - 1}} \in \mathbb{F}_{q^m}[X]$$

σ-projective polynomial

$$L(X) = XP_L(X^{\sigma - 1})$$

$$C_L = \begin{pmatrix} 0 & 0 & \dots & 0 & -\frac{\alpha_0}{\alpha_d} \\ 1 & 0 & \dots & 0 & -\frac{\alpha_1}{\alpha_d} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -\frac{\alpha_{d-1}}{\alpha_d} \end{pmatrix}.$$

Consider the matrix

$$A_L = C_L C_L^{\sigma} \dots C_L^{\sigma^{m-1}}.$$

Linearized & projective polynomials

Linearized & projective polynomials

THEOREM. [McGuire-Sheekey 2019]

The number of roots of P_L in $\mathbb{F}_{q^m}$ equals

$$\sum_{\lambda\in\mathbb{F}_q} \frac{q^{n_\lambda}-1}{q-1},$$

where n_λ is the dimension of the eigenspace of A_L corresponding to the eigenvalue λ. The number of roots of $L(X)$ in $\mathbb{F}_{q^m}$ is equal to q^{n_1}, i.e., to the size of the eigenspace of A_L corresponding to the eigenvalue 1.

Linearized & projective polynomials

Theorem. [McGuire-Sheekey 2019]

The number of roots of P_L in $\mathbb{F}_{q^m}$ equals

$$\sum_{\lambda \in \mathbb{F}_q} \frac{q^{n_\lambda} - 1}{q - 1},$$

where n_λ is the dimension of the eigenspace of A_L corresponding to the eigenvalue λ. The number of roots of $L(X)$ in $\mathbb{F}_{q^m}$ is equal to q^{n_1}, i.e., to the size of the eigenspace of A_L corresponding to the eigenvalue 1.

Let $L(X) = \alpha_0 x + \alpha_1 x^\sigma + \alpha_2 x^{\sigma^2}$ with $\alpha_i \in \mathbb{F}^*_{q^m}$. Then putting $u = \frac{\alpha_0^\sigma \alpha_2}{\alpha_1^{\sigma+1}}$, one has

$$A_L = \begin{pmatrix} 0 & -\alpha_0/\alpha_2 \\ 1 & -\alpha_1/\alpha_2 \end{pmatrix}^{1+\sigma+\ldots+\sigma^{m-1}} = \mathrm{N}_{q^m/q}(\alpha_1/\alpha_2) \begin{pmatrix} -u^{\sigma^{-1}} G^\sigma_{m-2} & -(\alpha_0/\alpha_1) G^\sigma_{m-1} \\ (\alpha_2/\alpha_1)^{\sigma^{-1}} G_{m-1} & G_m \end{pmatrix},$$

$$G_0 = 1, \quad G_1 = -1, \quad G_k + G^\sigma_{k-1} + u G^{\sigma^2}_{k-2} = 0.$$

The polynomial $X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $m \geq 5$ *be an odd integer,* $\sigma : x \in \mathbb{F}_{q^m} \longmapsto x^{q^s} \in \mathbb{F}_{q^m}$ *with* $(m, s) = 1$ *and consider the projective polynomials*

$$P_\gamma(X) = X^{\sigma+1} - \gamma X + \gamma \in \mathbb{F}_q[X]$$

with $\gamma \in \mathbb{F}_q$*. The polynomial*

$$Q(X) = X^{\sigma^2+1} - X^{\sigma+1} - X^{\sigma} + X \in \mathbb{F}_q[X]$$

has exactly the elements of $\mathbb{F}_q$ *as roots in* $\mathbb{F}_{q^m}$ *if and only if the set*

$$\{x \in \mathbb{F}_{q^m} \mid P_\gamma(x) = 0 \text{ for some } \gamma \in \mathbb{F}_q\}$$

of zeros of the polynomials P_γ *has size at most* q*, namely if and only if* $G_{m-1}(\gamma) \neq 0$ *for any* $\gamma \in \mathbb{F}_q^*$*.*

The case $m = 7$

The case $m = 7$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $q = p^e$ *and*

$$\mathcal{U}_\sigma = \{(x, x^\sigma + a, x^{\sigma^2} + b) : x \in \mathbb{F}_{q^7}, a, b \in \mathbb{F}_q\} \subset \mathbb{F}_{q^7}^3,$$

where $\sigma : x \in \mathbb{F}_{q^7} \longrightarrow x^{q^s} \in \mathbb{F}_{q^7}$, $s \in \{1, \dots, 6\}$. *Then,*

- *for* $p = 2, 3, 5$, $\mathcal{U}_\sigma$ *is scattered if* $3 \nmid e$.
- *for* $p > 7$, $\mathcal{U}_\sigma$ *is scattered if* $7/18(1/3 + \sqrt{-3})$ *is not a cube in* $\mathbb{F}_q(\sqrt{-3})$.

The cases $m = 5$

The cases $m = 5$

If U is an $\mathbb{F}_q$-scattered subspace of $V(3, q^5)$ of dimension 7, then U is maximum

The cases $m = 5$

If U is an $\mathbb{F}_q$-scattered subspace of $V(3, q^5)$ of dimension 7, then U is maximum

$$G_L(\gamma) = \frac{\gamma^2 - 3\gamma + 1}{\gamma^2}$$

The cases $m = 5$

If U is an $\mathbb{F}_q$-scattered subspace of $V(3, q^5)$ of dimension 7, then U is maximum

$$G_L(\gamma) = \frac{\gamma^2 - 3\gamma + 1}{\gamma^2}$$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $q = p^e$ and

$$\mathcal{U}_\sigma = \{(x, x^\sigma + a, x^{\sigma^2} + b) : x \in \mathbb{F}_{q^5}, a, b \in \mathbb{F}_q\} \subset \mathbb{F}_{q^5}^3,$$

where $\sigma : x \in \mathbb{F}_{q^5} \longrightarrow x^{q^s} \in \mathbb{F}_{q^5}$, $s \in \{1, 2, 3, 4\}$. Then,

- *for $p = 2$ even, $\mathcal{U}_\sigma$ is maximum scattered if e is an odd positive integer.*
- *for p odd, $\mathcal{U}_\sigma$ is maximum scattered if $q \equiv 2, 3 \pmod 5$.*

Intersection characters of $\mathcal{L}_{\mathcal{U}}$

Intersection characters of $\mathcal{L}_{\mathcal{U}}$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $L_U \subseteq \mathrm{PG}(2, q^m)$ be a linear set of rank $m + 2$, $m \geq 5$. If U contains an m-dimensional 2-scattered subspace W, then the linear set $L_{\mathcal{U}}$ has exactly three characters $\{q + 1, q^2 + q + 1, q^3 + q^2 + q + 1\}$ with respect to the lines.

Intersection characters of $\mathcal{L}_{\mathcal{U}}$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $L_U \subseteq \mathrm{PG}(2, q^m)$ *be a linear set of rank* $m+2$*,* $m \geq 5$*. If* U *contains an* m*-dimensional* 2*-scattered subspace* W*, then the linear set* $L_{\mathcal{U}}$ *has exactly three characters* $\{q+1, q^2+q+1, q^3+q^2+q+1\}$ *with respect to the lines. The corresponding* $[m+2, 3]_{q^m/q}$ *code has minimum distance* $d = m-2$ *and has codewords with rank weights belonging to* $\{m-2, m-1, m\}$*.*

Intersection characters of $\mathcal{L}_{\mathcal{U}}$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $L_U \subseteq \mathrm{PG}(2, q^m)$ be a linear set of rank $m+2$, $m \geq 5$. If U contains an m-dimensional 2-scattered subspace W, then the linear set $L_{\mathcal{U}}$ has exactly three characters $\{q+1, q^2+q+1, q^3+q^2+q+1\}$ with respect to the lines. The corresponding $[m+2, 3]_{q^m/q}$ code has minimum distance $d = m-2$ and has codewords with rank weights belonging to $\{m-2, m-1, m\}$.

Remark

Intersection characters of $\mathcal{L}_{\mathcal{U}}$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $L_U \subseteq \mathrm{PG}(2, q^m)$ be a linear set of rank $m+2$, $m \geq 5$. If U contains an m-dimensional 2-scattered subspace W, then the linear set $L_{\mathcal{U}}$ has exactly three characters $\{q+1, q^2+q+1, q^3+q^2+q+1\}$ with respect to the lines. The corresponding $[m+2, 3]_{q^m/q}$ code has minimum distance $d = m-2$ and has codewords with rank weights belonging to $\{m-2, m-1, m\}$.

Remark

- *$d = m-2$ is the maximum possible value for the minimum distance of an $[m+2, 3]_{q^m/q}$ rank metric code for every $m \geq 3$.*

Intersection characters of $\mathcal{L}_\mathcal{U}$

Theorem (Lia-Longobardi-G.M.-Trombetti, submitted)

Let $L_U \subseteq \mathrm{PG}(2, q^m)$ be a linear set of rank $m + 2$, $m \geq 5$. If U contains an m-dimensional 2-scattered subspace W, then the linear set $L_\mathcal{U}$ has exactly three characters $\{q + 1, q^2 + q + 1, q^3 + q^2 + q + 1\}$ with respect to the lines. The corresponding $[m + 2, 3]_{q^m/q}$ code has minimum distance $d = m - 2$ and has codewords with rank weights belonging to $\{m - 2, m - 1, m\}$.

Remark

- *$d = m - 2$ is the maximum possible value for the minimum distance of an $[m + 2, 3]_{q^m/q}$ rank metric code for every $m \geq 3$.*
- *$d_2 = m + 1$ and this is the largest possible value of an $[m + 2, 3]_{q^m/q}$ rank metric code*

Open problems

Open problems

Open Problem 1. Construct minimal $[m+2,3]_{q^m/q}$ codes also for other values of m and q.

Open problems

Open Problem 1. Construct minimal $[m+2,3]_{q^m/q}$ codes also for other values of m and q.

Open Problem 2. Construct other examples of maximum scattered $\mathbb{F}_q$-subspaces in $V(r,q^m)$ when rm is odd and $(r,m) \notin \{(3,3),(3,5)\}$.

Open problems

Open Problem 1. Construct minimal $[m+2,3]_{q^m/q}$ codes also for other values of m and q.

Open Problem 2. Construct other examples of maximum scattered $\mathbb{F}_q$-subspaces in $V(r,q^m)$ when rm is odd and $(r,m) \notin \{(3,3),(3,5)\}$.

Open Problem 3. Compare examples of maximum scattered linear sets in $\mathrm{PG}(2,q^5)$ found by Bartoli, Csajbók, G.M., Trombetti with those belonging to our infinite family.

Cutting q-systems and rank-metric codes

Problem

Construct minimal rank-metric codes reaching the lower bound on the dimension of the associated q-system and with the maximum value for the corresponding values of generalized rank weights.

$(k, m) \in \{(4, 3), (4, 4)\}$

$(k, m) \in \{(4,3),(4,4)\}$

$c_q(k, m)$:= smallest dimension of a linear cutting $[n, k]_{q^m/q}$ system

$(k, m) \in \{(4,3),(4,4)\}$

$c_q(k, m)$:= smallest dimension of a linear cutting $[n, k]_{q^m/q}$ system

$$c_q(k, m) \geq k + m - 1$$

$(k, m) \in \{(4,3),(4,4)\}$

$c_q(k, m)$:= smallest dimension of a linear cutting $[n, k]_{q^m/q}$ system

$$c_q(k, m) \geq k + m - 1$$

If $m < (k-1)^2$ then there are no cutting $[m+k-1, k]_{q^m/q}$ systems

$(k, m) \in \{(4,3),(4,4)\}$

$c_q(k, m)$:= smallest dimension of a linear cutting $[n, k]_{q^m/q}$ system

$$c_q(k, m) \geq k + m - 1$$

If $m < (k-1)^2$ then there are no cutting $[m + k - 1, k]_{q^m/q}$ systems

$$(k, m) = (4,3) \implies c_q(4,3) \geq 7$$

$(k,m) \in \{(4,3),(4,4)\}$

$c_q(k,m)$:= smallest dimension of a linear cutting $[n,k]_{q^m/q}$ system

$$c_q(k,m) \geq k+m-1$$

If $m < (k-1)^2$ then there are no cutting $[m+k-1,k]_{q^m/q}$ systems

$$(k,m)=(4,3) \Longrightarrow c_q(4,3) \geq 7$$

There are no cutting $[7,4]_{q^3/q}$ systems

$(k, m) \in \{(4,3),(4,4)\}$

$c_q(k,m)$:= smallest dimension of a linear cutting $[n,k]_{q^m/q}$ system

$$c_q(k,m) \geq k+m-1$$

If $m < (k-1)^2$ then there are no cutting $[m+k-1,k]_{q^m/q}$ systems

$$(k,m) = (4,3) \Longrightarrow c_q(4,3) \geq 7$$

There are no cutting $[7,4]_{q^3/q}$ systems and

$(k,m) \in \{(4,3),(4,4)\}$

$c_q(k,m)$:= smallest dimension of a linear cutting $[n,k]_{q^m/q}$ system

$$c_q(k,m) \geq k+m-1$$

If $m < (k-1)^2$ then there are no cutting $[m+k-1,k]_{q^m/q}$ systems

$$(k,m) = (4,3) \implies c_q(4,3) \geq 7$$

There are no cutting $[7,4]_{q^3/q}$ systems and

Proposition (Bartoli-G.M.-Neri 2023)

Let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, the $\mathbb{F}_q$-subspace

$$U = \{(\alpha_0 + \alpha_1 u, \alpha_2 + \alpha_3 u, \alpha_4 + \alpha_5 u, \alpha_6 + \alpha_7 u) \;:\; \alpha_i \in \mathbb{F}_q\}$$

is a cutting $[8,4]_{q^3/q}$ system.

$(k,m) \in \{(4,3),(4,4)\}$

$c_q(k,m)$:= smallest dimension of a linear cutting $[n,k]_{q^m/q}$ system

$$c_q(k,m) \geq k+m-1$$

If $m < (k-1)^2$ then there are no cutting $[m+k-1,k]_{q^m/q}$ systems

$$(k,m) = (4,3) \Longrightarrow c_q(4,3) \geq 7$$

There are no cutting $[7,4]_{q^3/q}$ systems and

Proposition (Bartoli-G.M.-Neri 2023)

Let $u \in \mathbb{F}_{q^3} \setminus \mathbb{F}_q$, the $\mathbb{F}_q$-subspace

$$U = \{(\alpha_0 + \alpha_1 u, \alpha_2 + \alpha_3 u, \alpha_4 + \alpha_5 u, \alpha_6 + \alpha_7 u) \ : \ \alpha_i \in \mathbb{F}_q\}$$

is a cutting $[8,4]_{q^3/q}$ system. Hence $c_q(4,3) = 8$.

$k = m = 4$

$k = m = 4$

$$c_q(4,4) \geq 8$$

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \, : \, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \,:\, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

Theorem (Bartoli-G.M.-Neri 2023)

U is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^4}^4$ if and only if $q = 2^h$ and $h \not\equiv 2 \pmod 4$

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \,:\, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

Theorem (Bartoli-G.M.-Neri 2023)

U is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^4}^4$ if and only if $q = 2^h$ and $h \not\equiv 2 \pmod 4$

Then U produces an $[8,4,3]_{q^4/q}$ MRD code

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \,:\, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

Theorem (Bartoli-G.M.-Neri 2023)

U is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^4}^4$ if and only if $q = 2^h$ and $h \not\equiv 2 \pmod 4$

Then U produces an $[8,4,3]_{q^4/q}$ MRD code

The know MRD codes with this parameters are direct sum of two $[4,2,3]_{q^4/q}$ MRD codes

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \,:\, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

Theorem (Bartoli-G.M.-Neri 2023)

U is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^4}^4$ if and only if $q = 2^h$ and $h \not\equiv 2 \pmod 4$

Then U produces an $[8,4,3]_{q^4/q}$ MRD code

The know MRD codes with this parameters are direct sum of two $[4,2,3]_{q^4/q}$ MRD codes not minimal since they are $(2,4)_q$-evasive

$k = m = 4$

$$c_q(4,4) \geq 8$$

$$U := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \,:\, x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

Theorem (Bartoli-G.M.-Neri 2023)

U is a maximum scattered $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^4}^4$ if and only if $q = 2^h$ and $h \not\equiv 2 \pmod 4$

Then U produces an $[8,4,3]_{q^4/q}$ MRD code

The know MRD codes with this parameters are direct sum of two $[4,2,3]_{q^4/q}$ MRD codes not minimal since they are $(2,4)_q$-evasive

Theorem (Bartoli-G.M.-Neri 2023)

If $q = 2^h$ and $h \equiv 1 \pmod 2$, then U is $(2,3)$-evasive, hence U is cutting and it produces a <u>minimal</u> $[8,4,3]_{q^4/q}$ MRD code.

$k = m = 4$

Code	is MRD?	$d_{rk,1}$	$d_{rk,2}$	$d_{rk,3}$	$d_{rk,4}$	is minimal?
$\mathcal{C}$	yes	3	5	7	8	yes
$\mathcal{D}_1 \oplus \mathcal{D}_2$	yes	3	4	7	8	no

Table: The table recaps the properties and the generalized rank weights of the code $\mathcal{C}$ compared to those of $[8,4]_{q^4/q}$ MRD codes obtained as direct sum of two $[4,2]_{q^4/q}$ MRD codes.

$k = m = 4$

Code	is MRD?	$d_{rk,1}$	$d_{rk,2}$	$d_{rk,3}$	$d_{rk,4}$	is minimal?
$\mathcal{C}$	yes	3	5	7	8	yes
$\mathcal{D}_1 \oplus \mathcal{D}_2$	yes	3	4	7	8	no

Table: The table recaps the properties and the generalized rank weights of the code $\mathcal{C}$ compared to those of $[8,4]_{q^4/q}$ MRD codes obtained as direct sum of two $[4,2]_{q^4/q}$ MRD codes.

Proposition

The dual code $\mathcal{C}^\perp$ is also an $[8,4,(3,5,7,8)]_{q^4/q}$ code. Also, $\mathcal{C}^\perp$ is equivalent to $\mathcal{C}$.

Open problems

Open problems

Open Problem 1. Find new bounds for the generalized rank weights of an $[n, k]_{q^m/q}$ code, improving on the known bounds.

Open problems

Open Problem 1. Find new bounds for the generalized rank weights of an $[n, k]_{q^m/q}$ code, improving on the known bounds.

Open Problem 2. Generalize the construction of the $[8, 4]_{q^m/q}$ q-system U in order to obtain more general MRD codes with higher generalized weights.

Open problems

Open Problem 1. Find new bounds for the generalized rank weights of an $[n, k]_{q^m/q}$ code, improving on the known bounds.

Open Problem 2. Generalize the construction of the $[8, 4]_{q^m/q}$ q-system U in order to obtain more general MRD codes with higher generalized weights.

Open Problem 3. Generalize the construction of the $[8, 4]_{q^m/q}$ q-system U in order to obtain more general short minimal rank-metric codes.

Covering problem [Cohen, Honkala, Litsyn, Lobstein 1997]

Given a vector space over a finite fied, a metric, and a positive integer ρ, what is the smallest number of sheres of radius ρ that can be placed in such a way that every vector in the space is contained in at least of them?

Covering radius

Covering radius

$\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ a linear code, $d_* : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{R}_{\geq 0}$ a distance

Covering radius

$\mathcal{C} \subseteq \mathbb{F}_{q^m}^n$ a linear code, $d_*: \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n \to \mathbb{R}_{\geq 0}$ a distance

Definition

The covering radius of $\mathcal{C}$ w.r.t. d_* is the integer

$$\rho_*(\mathcal{C}) := \max_{v \in \mathbb{F}_{q^m}^n} \min_{c \in \mathcal{C}} d_*(v, c) = \min \left\{ \rho : \bigcup_{c \in \mathcal{C}} B_*(c, \rho) = \mathbb{F}_{q^n} \right\}.$$

The metrics considered are

- the Hamming metric: $d_H(v, w) := |\{i : v_i \neq w_i\}|$
  [Brualdi-Pless-Wilson 1989, Cohen-Honkala-Litsyn-Lobstein 1997, Davydov-Östergard 2000, Davydov-Giulietti-Marcugini-Pambianco 2011, etc.]
- the rank metric $d_{\mathrm{rk}}(v, w) := \dim_{\mathbb{F}_q} \langle v_1 - w_1, \ldots, v_n - w_n \rangle_{\mathbb{F}_q}$
  [Byrne-Ravagnani 2020, Gadouleau 2009]

Covering radius

Covering radius

Definition

$\mathcal{S} \subseteq \mathrm{PG}(k-1, q^m)$ is $(\rho - 1)$-saturating if

- *for each point Q of $\mathrm{PG}(k-1, q^m)$ there exist ρ points $P_1, P_2, \ldots, P_\rho \in \mathcal{S}$ s.t.*

$$Q \in \langle P_1, \ldots, P_\rho \rangle_{\mathbb{F}_{q^m}};$$

- *ρ is the smallest value with this property.*

Covering radius

Definition

$\mathcal{S} \subseteq \mathrm{PG}(k-1, q^m)$ is $(\rho-1)$-saturating if

- *for each point Q of $\mathrm{PG}(k-1, q^m)$ there exist ρ points $P_1, P_2, \ldots, P_\rho \in \mathcal{S}$ s.t.*

$$Q \in \langle P_1, \ldots, P_\rho \rangle_{\mathbb{F}_{q^m}};$$

- *ρ is the smallest value with this property.*

Definition

An $[n,k]_{q^m/q}$ system $\mathcal{U}$ of $V(k, q^m)$ is a rank ρ-saturating system if $L_{\mathcal{U}}$ is a $(\rho-1)$-saturating set in $\mathrm{PG}(k-1, q^m)$

Covering radius

Covering radius

Theorem (Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system associated with a code $\mathcal{C}$. Then $\mathcal{U}$ is rank-ρ-saturating if and only if $\rho_{rk}(\mathcal{C}^{\perp}) = \rho$

Covering radius

Theorem (Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be an $[n, k]_{q^m/q}$ system associated with a code $\mathcal{C}$. Then $\mathcal{U}$ is rank-ρ-saturating if and only if $\rho_{rk}(\mathcal{C}^{\perp}) = \rho$

Corollary (Bonini-Borello-Byrne 2023)

Let $\mathcal{C}$ be an $[n, k]_{q^m/q}$ generalized Gabidulin code and let $\mathcal{U}$ be an $[n, k]_{q^m/q}$ system associated with $\mathcal{C}$. Then $\mathcal{U}$ is a rank-k-saturating system.

Covering problem

Classical covering problem: given n and ρ estimate the least number of spheres of radius ρ such that the union of the balls of radius ρ covers the ambient vector space of dimension n.

Covering problem

Classical covering problem: given n and ρ estimate the least number of spheres of radius ρ such that the union of the balls of radius ρ covers the ambient vector space of dimension n.
In terms of rank ρ-saturating system one may ask to find the least value of n such that an $[n, k]_{q^m/q}$ rank ρ-saturating system exists, for fixed k and ρ.

How small?

How small?

$$s_{q^m/q}(k,\rho) := \min\left\{\dim_{\mathbb{F}_q}\mathcal{U} \colon \mathcal{U} \text{ is a rank } \rho\text{-saturating system in } V(k,q^m)\right\}$$

How small?

$$s_{q^m/q}(k,\rho) := \min\left\{\dim_{\mathbb{F}_q}\mathcal{U} \colon \mathcal{U} \text{ is a rank } \rho\text{-saturating system in } V(k,q^m)\right\}$$

Theorem (Gadouleau-Yan 2008, Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be a rank ρ-saturating system in $V(k,q^m)$. Then

$$\begin{bmatrix} \dim_{\mathbb{F}_q}\mathcal{U} \\ \rho \end{bmatrix}_q \geq q^{m(k-\rho)}$$

In particular,

$$s_{q^m/q}(k,\rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1)+1 & \text{if } q = 2, \rho = 1. \end{cases}$$

How small?

How small?

Some upper bounds [Bonini-Borello-Byrne 2023]

$$\begin{aligned} s_{q^m/q}(k,\rho) &\leq m(k-\rho)+\rho \\ s_{q^m/q}(k,(s-1)t+1) &\leq tk-(t-1)((s-1)t+1) \end{aligned}$$

How small?

Some upper bounds [Bonini-Borello-Byrne 2023]

$$\begin{aligned} s_{q^m/q}(k,\rho) &\leq m(k-\rho)+\rho \\ s_{q^m/q}(k,(s-1)t+1) &\leq tk-(t-1)((s-1)t+1) \end{aligned}$$

and the equality holds:

$$\begin{aligned} s_{q^m/q}(k,1) &= m(k-1)+1 \\ s_{q^m/q}(k,k) &= k \\ s_{q^{2r}/q}(2r,2r-1) &= 2r+1 \end{aligned}$$

How small?

How small?

Theorem (Bartoli-Borello-G.M., 202?)

If $k = \rho t$ *for some integer* $t \geq 1$

$$s_{q^m/q}(\rho t, \rho) = m(t-1) + \rho.$$

How small?

Theorem (Bartoli-Borello-G.M., 202?)

If $k = \rho t$ for some integer $t \geq 1$

$$s_{q^m/q}(\rho t, \rho) = m(t-1) + \rho.$$

Proof.

$$\mathcal{U} := \{(x_1, x_1^q, \ldots, x_1^{q^{\rho-1}}, \ldots, x_{t-1}, x_{t-1}^q, \ldots, x_{t-1}^{q^{\rho-1}}, a_1, \ldots, a_\rho) : x_i \in \mathbb{F}_{q^m}, a_j \in \mathbb{F}_q\}$$

is rank ρ-saturating. □

How small?

How small?

Theorem (Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. If $\mathcal{U}$ is cutting, then it is a rank-$(k-1)$-saturating $[n,k]_{q^{m(k-1)}/q}$ system.

How small?

Theorem (Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. If $\mathcal{U}$ is cutting, then it is a rank-$(k-1)$-saturating $[n,k]_{q^{m(k-1)}/q}$ system.

Since, from [Alfarano-Borello-Neri-Ravagnani 2022],

- If $\mathcal{U}$ is a linear cutting $[n,k]_{q^m/q}$ system then $\dim_{\mathbb{F}_q}\mathcal{U} \geq m+k-1$
- for $m,k \geq 2$ there always exists a cutting subspace of dimension $m+2k-2$

How small?

Theorem (Bonini-Borello-Byrne 2023)

Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. If $\mathcal{U}$ is cutting, then it is a rank-$(k-1)$-saturating $[n,k]_{q^{m(k-1)}/q}$ system.

Since, from [Alfarano-Borello-Neri-Ravagnani 2022],

- If $\mathcal{U}$ is a linear cutting $[n,k]_{q^m/q}$ system then $\dim_{\mathbb{F}_q}\mathcal{U} \geq m+k-1$
- for $m,k \geq 2$ there always exists a cutting subspace of dimension $m+2k-2$

Corollary

For every $m,k \geq 2$,

$$k+m-1 \leq s_{q^{m(k-1)}/q}(k,k-1) \leq l_{q^m/q}(k) \leq 2k+m-2,$$

where $l_{q^m/q}(k)$ is the minimum $\mathbb{F}_q$-dimension of a linear cutting blocking set in $\mathbb{F}_{q^m}^k$.

How small?

How small?

Alfarano-Borello-Neri-Ravagnani 2022

Bartoli-Csajbók-M.-Trombetti 2021

Lia-Longobardi-M.-Trombetti 202?

$\Downarrow$

$s_{q^{2r}/q}(3,2) = r+2,$ for $r \neq 3,5 \mod 6$ and $r \geq 4$,

$s_{q^{2r}/q}(3,2) = r+2,$ for $\gcd(r,(q^{2s}-q^s+1)!) = 1$, r odd, $1 \leq s \leq r$, $\gcd(r,s) = 1$,

$s_{q^{10}/q}(3,2) = 7,$ for $q = p^{15h+s}$, $p \in \{2,3\}$, $\gcd(s,15) = 1$ and for $q = 5^{15h+1}$,

$s_{q^{10}/q}(3,2) = 7,$ for q odd, $q = 2,3 \mod 5$ and for $q = 2^{2h+1}$, $h \geq 1$,

How small?

Theorem (Bonini-Borello-Byrne 2023)

For all positive integers m, k, k', $\rho \in [\min\{k, m\}]$, $\rho' \in [\min\{k', m\}]$.

(a) *If* $\rho < \min\{k, m\}$, *then* $s_{q^m/q}(k, \rho + 1) \leq s_{q^m/q}(k, \rho)$.

(b) $s_{q^m/q}(k, \rho) < s_{q^m/q}(k + 1, \rho)$.

(c) *If* $\rho < m$, *then* $s_{q^m/q}(k + 1, \rho + 1) \leq s_{q^m/q}(k, \rho) + 1$.

(d) *If* $\rho + \rho' \leq \min\{k + k', m\}$, $s_{q^m/q}(k + k', \rho + \rho') \leq s_{q^m/q}(k, \rho) + s_{q^m/q}(k', \rho')$.

How small?

How small?

Theorem (Bartoli-Borello-G.M., 202?)

Let $m \geq h+1$. If $\mathcal{U}$ is an h-scattered $\mathbb{F}_q$-subspace of $V(k, q^m)$ of $\mathbb{F}_q$-dimension (at least) $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$, then $\mathcal{U}$ is rank ρ-saturating, with $\rho \leq h+1$.

How small?

Theorem (Bartoli-Borello-G.M., 202?)

Let $m \geq h+1$. If $\mathcal{U}$ is an h-scattered $\mathbb{F}_q$-subspace of $V(k, q^m)$ of $\mathbb{F}_q$-dimension (at least) $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$, then $\mathcal{U}$ is rank ρ-saturating, with $\rho \leq h+1$.

Proof.

Let $v \notin \mathcal{U}$ and project $\mathcal{U}$ from v to a hyperplane Γ of $V(k, q^m)$ not containing v. The projection $\overline{\mathcal{U}}$ is a subspace of Γ of $\mathbb{F}_q$-dimension $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$ which is not h-scattered. Then there exists an $\mathbb{F}_{q^m}$-subspace M of Γ of $\mathbb{F}_{q^m}$-dimension h such that $\dim_{\mathbb{F}_q}(M \cap \overline{\mathcal{U}}) \geq h+1$. Let $N = \langle v, M \rangle_{\mathbb{F}_{q^m}}$ and $u_1, \ldots, u_{h+1} \in N \cap \mathcal{U}$ be $h+1$ linearly independent vectors over $\mathbb{F}_q$.
$N = \langle u_1, \ldots, u_{h+1} \rangle_{\mathbb{F}_{q^m}} \Rightarrow v \in N$ is $(h+1)$-saturated by $\mathcal{U}$. □

How small?

Theorem (Bartoli-Borello-G.M., 202?)

Let $m \geq h+1$. If $\mathcal{U}$ is an h-scattered $\mathbb{F}_q$-subspace of $V(k,q^m)$ of $\mathbb{F}_q$-dimension (at least) $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$, then $\mathcal{U}$ is rank ρ-saturating, with $\rho \leq h+1$.

Proof.

Let $v \notin \mathcal{U}$ and project $\mathcal{U}$ from v to a hyperplane Γ of $V(k,q^m)$ not containing v. The projection $\overline{\mathcal{U}}$ is a subspace of Γ of $\mathbb{F}_q$-dimension $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$ which is not h-scattered. Then there exists an $\mathbb{F}_{q^m}$-subspace M of Γ of $\mathbb{F}_{q^m}$-dimension h such that $\dim_{\mathbb{F}_q}(M \cap \overline{\mathcal{U}}) \geq h+1$. Let $N = \langle v, M \rangle_{\mathbb{F}_{q^m}}$ and $u_1, \ldots, u_{h+1} \in N \cap \mathcal{U}$ be $h+1$ linearly independent vectors over $\mathbb{F}_q$.
$N = \langle u_1, \ldots, u_{h+1} \rangle_{\mathbb{F}_{q^m}} \Rightarrow v \in N$ is $(h+1)$-saturated by $\mathcal{U}$. □

Corollary

The 2-maximum $\mathbb{F}_q$-scattered subspace of $V(4,q^6)$, $q = 2^{2h+1}$, $h \geq 1$ found by Bartoli-Giannoni-Ghiandoni-G.M. is rank ρ-saturating, with $\rho \leq 3$. MAGMA computations show that it is rank 2-saturating at least when $q = 2$.

How small?

Theorem (Bartoli-Borello-G.M., 202?)

Let $m \geq h+1$. If $\mathcal{U}$ is an h-scattered $\mathbb{F}_q$-subspace of $V(k, q^m)$ of $\mathbb{F}_q$-dimension (at least) $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$, then $\mathcal{U}$ is rank ρ-saturating, with $\rho \leq h+1$.

Proof.

Let $v \notin \mathcal{U}$ and project $\mathcal{U}$ from v to a hyperplane Γ of $V(k, q^m)$ not containing v. The projection $\overline{\mathcal{U}}$ is a subspace of Γ of $\mathbb{F}_q$-dimension $\left\lfloor \frac{m(k-1)}{h+1} \right\rfloor + 1$ which is not h-scattered. Then there exists an $\mathbb{F}_{q^m}$-subspace M of Γ of $\mathbb{F}_{q^m}$-dimension h such that $\dim_{\mathbb{F}_q}(M \cap \overline{\mathcal{U}}) \geq h+1$. Let $N = \langle v, M \rangle_{\mathbb{F}_{q^m}}$ and $u_1, \ldots, u_{h+1} \in N \cap \mathcal{U}$ be $h+1$ linearly independent vectors over $\mathbb{F}_q$.
$N = \langle u_1, \ldots, u_{h+1} \rangle_{\mathbb{F}_{q^m}} \Rightarrow v \in N$ is $(h+1)$-saturated by $\mathcal{U}$. $\square$

Corollary

The 2-maximum $\mathbb{F}_q$-scattered subspace of $V(4, q^6)$, $q = 2^{2h+1}$, $h \geq 1$ found by Bartoli-Giannoni-Ghiandoni-G.M. is rank ρ-saturating, with $\rho \leq 3$. MAGMA computations show that it is rank 2-saturating at least when $q = 2$.

Open Problem Show that the Bartoli-Giannoni-Ghiandoni-G.M. example is rank 2-saturating for each $q = 2^{2h+1}$, with $h > 1$

How small?

Corollary (Bartoli-Borello-G.M., 202?)

Let $m \geq 4$ be an even integer. For $q > 2$, if $r = 3$ and $m < 12$ or $r > 3$ odd, then

$$\frac{mr}{2} - 2 \leq s_{q^m/q}\left(\frac{r(m-2)}{2}, m-2\right) \leq \frac{mr}{2} - 1.$$

For $q = 2$, the same holds if $r = 3$ and $m < 10$ or $r > 3$ odd.

Corollary (Bartoli-Borello-G.M., 202?)

If mk is even, then

$$\left\lceil \frac{m(k-2)}{2} \right\rceil + 2 \leq s_{q^m/q}(k,2) \leq \left\lfloor \frac{m(k-1)}{2} \right\rfloor + 1 = \left\lceil \frac{m(k-2)}{2} \right\rceil + 2 + \left\lfloor \frac{m}{2} \right\rfloor - 1.$$

In particular $s_{q^2/q}(k,2) = k$. Moreover,

$$s_{q^5/q}(3,2) \in \{5,6\}$$

for $q = p^t$ with $p \in \{2,3,5\}$ and

$$s_{q^3/q}(3,2) = 4.$$

The bound is not tight!

The bound is not tight!

The bound

$$s_{q^m/q}(k,\rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1)+1 & \text{if } q = 2, \rho = 1. \end{cases}$$

is not tight in general.

The bound is not tight!

The bound

$$s_{q^m/q}(k,\rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1)+1 & \text{if } q = 2, \rho = 1. \end{cases}$$

is not tight in general.

We know

$$s_{q^4/q}(3,2) \geq 4.$$

MAGMA computations show that $s_{16/2}(3,2) = s_{81/3}(3,2) = 5$, so that the lower bound is not tight in the binary and ternary case.

The bound is not tight!

The bound

$$s_{q^m/q}(k,\rho) \geq \begin{cases} \left\lceil \frac{mk}{\rho} \right\rceil - m + \rho & \text{if } q > 2, \\ \left\lceil \frac{mk-1}{\rho} \right\rceil - m + \rho & \text{if } q = 2, \rho > 1, \\ m(k-1)+1 & \text{if } q = 2, \rho = 1. \end{cases}$$

is not tight in general.

We know

$$s_{q^4/q}(3,2) \geq 4.$$

MAGMA computations show that $s_{16/2}(3,2) = s_{81/3}(3,2) = 5$, so that the lower bound is not tight in the binary and ternary case.

Theorem (Bartoli-Borello-G.M., 202?)

If q is even and large enough, then

$$s_{q^4/q}(3,2) = 5 > 4.$$

The bound is not tight!

Sketch of the proof.

The bound is not tight!

Sketch of the proof.

Remark

Let L_U be a linear set in $\mathrm{PG}(k-1, q^m)$, H a hyperplane and P a point not belonging to L_U nor to H. If the projection of L_U from P to H is scattered, then the point is not 1-saturated, because otherwise in the projection we would find a point of weight at least 2.

The bound is not tight!

Sketch of the proof.

Remark

Let L_U be a linear set in $\mathrm{PG}(k-1,q^m)$, H a hyperplane and P a point not belonging to L_U nor to H. If the projection of L_U from P to H is scattered, then the point is not 1-saturated, because otherwise in the projection we would find a point of weight at least 2.

A rank 2-saturating U of rank 4 in $V(3,q^4)$, up to $\mathrm{GL}(3,q^4)$-equivalence, has one of these forms:

1) $U = \left\{(x, x^q, x^{q^2}) : x \in \mathbb{F}_{q^4}\right\}$;

2) $U_\alpha = \left\{(x, x^q + \alpha x^{q^2}, x^{q^3}) : x \in \mathbb{F}_{q^4}\right\}$, with $\alpha \in \mathbb{F}^*_{q^4}$;

3) $U_\alpha = \left\{(x, x^q + \alpha x^{q^3}, x^{q^2}) : x \in \mathbb{F}_{q^4}\right\}$ with $\alpha \in \mathbb{F}^*_{q^4}$;

4) $U_{\alpha,\beta} = \left\{(x, x^q + \alpha x^{q^3}, x^{q^2} + \beta x^{q^3}) : x \in \mathbb{F}_{q^4}\right\}$ with $\alpha, \beta \in \mathbb{F}^*_{q^4}$;

The bound is not tight!

Sketch of the proof.

Remark

Let L_U be a linear set in $\mathrm{PG}(k-1, q^m)$, H a hyperplane and P a point not belonging to L_U nor to H. If the projection of L_U from P to H is scattered, then the point is not 1-saturated, because otherwise in the projection we would find a point of weight at least 2.

A rank 2-saturating U of rank 4 in $V(3, q^4)$, up to $\mathrm{GL}(3, q^4)$-equivalence, has one of these forms:

1) $U = \left\{(x, x^q, x^{q^2}) : x \in \mathbb{F}_{q^4}\right\}$;
2) $U_\alpha = \left\{(x, x^q + \alpha x^{q^2}, x^{q^3}) : x \in \mathbb{F}_{q^4}\right\}$, with $\alpha \in \mathbb{F}^*_{q^4}$;
3) $U_\alpha = \left\{(x, x^q + \alpha x^{q^3}, x^{q^2}) : x \in \mathbb{F}_{q^4}\right\}$ with $\alpha \in \mathbb{F}^*_{q^4}$;
4) $U_{\alpha,\beta} = \left\{(x, x^q + \alpha x^{q^3}, x^{q^2} + \beta x^{q^3}) : x \in \mathbb{F}_{q^4}\right\}$ with $\alpha, \beta \in \mathbb{F}^*_{q^4}$;

In each case, we get a point of the plane not contained in L_U through which does not pass any secant line to L_U.

Open problems

Open problems

- $s_{q^4/q}(3,2) = 5$ also for q odd?

Open problems

- $s_{q^4/q}(3,2) = 5$ also for q odd? (but Ferdinando solved it!)

Open problems

- $s_{q^4/q}(3,2) = 5$ also for q odd? (but Ferdinando solved it!)
- For which parameters is the bound $s_{q^m/q}(k,\rho)$ tight?

Open problems

- $s_{q^4/q}(3,2) = 5$ also for q odd? (but Ferdinando solved it!)
- For which parameters is the bound $s_{q^m/q}(k,\rho)$ tight?
- Can we find additional examples of small rank saturating systems?

Open problems

- $s_{q^4/q}(3,2) = 5$ also for q odd? (but Ferdinando solved it!)
- For which parameters is the bound $s_{q^m/q}(k,\rho)$ tight?
- Can we find additional examples of small rank saturating systems?
- Can we generalize this framework to other metrics (e.g. the sum-rank metric)?

Thank you for your attention!