Rank-Metric Codes and Geometry: A Two-Way Street

John Sheekey

UCD

Opera, February 2026

Rank Metric Codes

Matrices

A (matrix) *rank-metric code* is a subset $\mathcal{U}$ of a matrix space equipped with the rank metric $d(X, Y) = \mathrm{rank}(X - Y)$.

We will assume throughout that U is additively closed, in which case it is a vector space over some field $\mathbb{F}_q$.

$$\mathcal{U} \leq_{\mathbb{F}_q} M_{s\times t}(\mathbb{F}_{q^m}) = \mathbb{F}_{q^m}^{s\times t} \simeq (\mathbb{F}_{q^m})^{st}.$$

Rank Metric Codes

Matrices

A (matrix) *rank-metric code* is a subset $\mathcal{U}$ of a matrix space equipped with the rank metric $d(X, Y) = \mathrm{rank}(X - Y)$.

We will assume throughout that U is additively closed, in which case it is a vector space over some field $\mathbb{F}_q$.

$$\mathcal{U} \leq_{\mathbb{F}_q} M_{s\times t}(\mathbb{F}_{q^m}) = \mathbb{F}_{q^m}^{s\times t} \simeq (\mathbb{F}_{q^m})^{st}.$$

$\mathcal{U}$ is MRD if $\dim_{\mathbb{F}_q}(\mathcal{U}) = ms(t - d(\mathcal{U}) + 1)$ when $s \geq t$. When $t = s = d(\mathcal{U})$ we have $\dim_{\mathbb{F}_q}(\mathcal{U}) = ms$, and $\mathcal{U}$ is a *semifield spread set*.

Rank Metric Codes

Matrices

Two $\mathbb{F}_q$-subspaces $\mathcal{U}_1, \mathcal{U}_2$ of $M_{s\times t}(\mathbb{F}_{q^m})$ are *equivalent* if there exist

$$A \in \mathrm{GL}(s, q^m)$$
$$B \in \mathrm{GL}(t, q^m)$$
$$\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$$

such that $\mathcal{U}_2 = A\mathcal{U}_1^{\rho}B$.

Rank Metric Codes

Matrices

Two $\mathbb{F}_q$-subspaces $\mathcal{U}_1, \mathcal{U}_2$ of $M_{s\times t}(\mathbb{F}_{q^m})$ are *equivalent* if there exist

$$A \in \mathrm{GL}(s, q^m)$$
$$B \in \mathrm{GL}(t, q^m)$$
$$\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$$

such that $\mathcal{U}_2 = A\mathcal{U}_1^{\rho} B$.

If we vectorise our matrices to elements of $(\mathbb{F}_{q^m})^{st}$ (written as columns) to obtain U_1 and U_2, then we have

$$U_2 = (A \otimes B^T)U_1^{\rho}.$$

Rank Metric Codes

Vectors

An ($\mathbb{F}_{q^m}$-linear) rank-metric code is an $\mathbb{F}_{q^m}$-subspace C of $(\mathbb{F}_{q^m})^n$.

Rank Metric Codes

Vectors

An ($\mathbb{F}_{q^m}$-linear) rank-metric code is an $\mathbb{F}_{q^m}$-subspace C of $(\mathbb{F}_{q^m})^n$.

We can choose a *generator matrix*, $G \in (\mathbb{F}_{q^m})^{k \times n}$.

$$C = \{xG : x \in (\mathbb{F}_{q^m})^k\}$$

So C is the $\mathbb{F}_{q^m}$-span of the row of G. Note that here we are (unusually) not assuming that C has dimension k.

An ($\mathbb{F}_{q^m}$-linear) rank-metric code is an $\mathbb{F}_{q^m}$-subspace C of $(\mathbb{F}_{q^m})^n$.

We can choose a *generator matrix*, $G \in (\mathbb{F}_{q^m})^{k \times n}$.

$$C = \{xG : x \in (\mathbb{F}_{q^m})^k\}$$

So C is the $\mathbb{F}_{q^m}$-span of the row of G. Note that here we are (unusually) not assuming that C has dimension k.

The *q-system* of G is the $\mathbb{F}_q$-span of the columns of G;

$$U_G := \{Gy^t : y \in \mathbb{F}_q^n\} \subset (\mathbb{F}_{q^m})^k$$

Two matrices G_1, G_2 define equivalent codes if and only if there exist invertible $Z \in \mathbb{F}_{q^m}^{k\times k}$, $Q \in \mathbb{F}_q^{n\times n}$, and $\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$ such that $G_2 = ZG_1^{\rho}Q$.

Two matrices G_1, G_2 define equivalent codes if and only if there exist invertible $Z \in \mathbb{F}_{q^m}^{k\times k}$, $Q \in \mathbb{F}_q^{n\times n}$, and $\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$ such that $G_2 = ZG_1^\rho Q$.

Two q-systems U_{G_1}, U_{G_2} are equivalent if and only if there exist invertible $Z \in \mathbb{F}_{q^m}^{k\times k}$ and $\rho \in \mathrm{Aut}(\mathbb{F}_{q^m})$ such that $U_{G_2} = ZU_{G_1}^\rho$.

This is the action of $\Gamma L(k, q^m)$.

Rank Metric Codes

Matrices and Vectors

So we can consider $\mathbb{F}_q$-linear matrix rank-metric codes in $M_{s\times t}(\mathbb{F}_{q^m})$ of dimension n as defining $\mathbb{F}_{q^m}$-linear vector rank-metric codes in $(\mathbb{F}_{q^m})^n$ of dimension at most st.

Equivalence in $M_{s\times t}(\mathbb{F}_{q^m}) \Rightarrow$ Equivalence in $(\mathbb{F}_{q^m})^n$
Equivalence in $M_{s\times t}(\mathbb{F}_{q^m}) \not\Leftarrow$ Equivalence in $(\mathbb{F}_{q^m})^n$

Rank Metric Codes

Matrices and Vectors

So we can consider $\mathbb{F}_q$-linear matrix rank-metric codes in $M_{s\times t}(\mathbb{F}_{q^m})$ of dimension n as defining $\mathbb{F}_{q^m}$-linear vector rank-metric codes in $(\mathbb{F}_{q^m})^n$ of dimension at most st.

Equivalence in $M_{s\times t}(\mathbb{F}_{q^m}) \Rightarrow$ Equivalence in $(\mathbb{F}_{q^m})^n$
Equivalence in $M_{s\times t}(\mathbb{F}_{q^m}) \not\Leftarrow$ Equivalence in $(\mathbb{F}_{q^m})^n$

- Equivalence in $M_{s\times t}(\mathbb{F}_{q^m})$ is difficult to determine.
- Equivalence in $(\mathbb{F}_{q^m})^n$ is easy to determine (Couvreur et al).
- Ideas and results from both sides can inform the other.

Rank Metric Codes

Examples

The field $\mathbb{F}_{q^{2m}}$ gives rise to a MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

where η is a non-square in $\mathbb{F}_{q^m}$. Here we assume q odd for simplicity; a similar construction works for q even.

Rank Metric Codes

Examples

The field $\mathbb{F}_{q^{2m}}$ gives rise to a MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

where η is a non-square in $\mathbb{F}_{q^m}$. Here we assume q odd for simplicity; a similar construction works for q even.

From this we obtain

$$G = \begin{pmatrix} \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \eta\alpha_1 & \cdots & \eta\alpha_m \\ 0 & \cdots & 0 & \alpha_1 & \cdots & \alpha_m \\ \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \end{pmatrix}$$

This generates a code C of dimension 2, isomorphic to the direct sum of two 1-dimensional Gabidulin codes.

Note that it is clear that equivalence in $(\mathbb{F}_{q^m})^n$ does not imply equivalence in $M_{s\times t}(\mathbb{F}_{q^m})$.The following matrix defines the same code as G.

$$G' = \begin{pmatrix} \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \alpha_1 & \cdots & \alpha_m \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

However the corresponding space of matrices is

$$\mathcal{U}' = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

which is clearly not MRD and not equivalent to $\mathcal{U}$.

Rank Metric Codes

Examples

The *Dickson semifields* correspond to MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b^q \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

where η is a non-square in $\mathbb{F}_{q^m}$. Here we need q odd.

Rank Metric Codes

Examples

The *Dickson semifields* correspond to MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b^{q} \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

where η is a non-square in $\mathbb{F}_{q^m}$. Here we need q odd.

From this we obtain

$$G = \begin{pmatrix} \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \eta\alpha_1^q & \cdots & \eta\alpha_m^q \\ 0 & \cdots & 0 & \alpha_1 & \cdots & \alpha_m \\ \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \end{pmatrix}$$

This generates a code C of dimension 3, isomorphic to the direct sum of a 1-dimensional and a 2-dimensional Gabidulin code.

Rank Metric Codes

Examples

The *Hughes-Kleinfeld semifields* correspond to MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = m = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b^{q} \\ b & a^{q} \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

The *Hughes-Kleinfeld semifields* correspond to MRD codes in $M_{2\times 2}(\mathbb{F}_{q^m})$ with $d = m = 2$, and hence $\mathbb{F}_q$-dimension $2m$.

$$\mathcal{U} = \left\{ \begin{pmatrix} a & \eta b^q \\ b & a^q \end{pmatrix} : a, b \in \mathbb{F}_{q^m} \right\},$$

From this we obtain

$$G = \begin{pmatrix} \alpha_1 & \cdots & \alpha_m & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \eta\alpha_1^q & \cdots & \eta\alpha_m^q \\ 0 & \cdots & 0 & \alpha_1 & \cdots & \alpha_m \\ \alpha_1^q & \cdots & \alpha_m^q & 0 & \cdots & 0 \end{pmatrix}$$

This generates a code C of dimension 4, isomorphic to the direct sum of two 2-dimensional Gabidulin codes.

Linear Sets

This approach was used to great effect in classifying semifields/MRD codes with certain small parameters.

Linear Sets

This approach was used to great effect in classifying semifields/MRD codes with certain small parameters.

- Cardinali-Polverino-Trombetti (2006): $s = t = m = d = 2$ classification; 4-dimensional $\mathbb{F}_q$-subspaces of $M_{2\times 2}(\mathbb{F}_{q^2})$ where all nonzero elements are invertible.

Linear Sets

This approach was used to great effect in classifying semifields/MRD codes with certain small parameters.

- Cardinali-Polverino-Trombetti (2006): $s = t = m = d = 2$ classification; 4-dimensional $\mathbb{F}_q$-subspaces of $M_{2\times 2}(\mathbb{F}_{q^2})$ where all nonzero elements are invertible.
- Marino-Polverino-Trombetti (2007), MPT+Ebert (2008), MPT+Lavrauw (2010): $t = s = d = 2$, $m = 3$ partial classification.

Linear Sets

This approach was used to great effect in classifying semifields/MRD codes with certain small parameters.

- Cardinali-Polverino-Trombetti (2006): $s = t = m = d = 2$ classification; 4-dimensional $\mathbb{F}_q$-subspaces of $M_{2\times 2}(\mathbb{F}_{q^2})$ where all nonzero elements are invertible.
- Marino-Polverino-Trombetti (2007), MPT+Ebert (2008), MPT+Lavrauw (2010): $t = s = d = 2$, $m = 3$ partial classification.
- Studied projectively using the related notion of *linear sets* in $\mathrm{PG}(st - 1, q^m)$. These had been studied for other reasons previously, e.g. small blocking sets.

Linear Sets

This approach was used to great effect in classifying semifields/MRD codes with certain small parameters.

- Cardinali-Polverino-Trombetti (2006): $s = t = m = d = 2$ classification; 4-dimensional $\mathbb{F}_q$-subspaces of $M_{2\times 2}(\mathbb{F}_{q^2})$ where all nonzero elements are invertible.
- Marino-Polverino-Trombetti (2007), MPT+Ebert (2008), MPT+Lavrauw (2010): $t = s = d = 2$, $m = 3$ partial classification.
- Studied projectively using the related notion of *linear sets* in $\mathrm{PG}(st-1, q^m)$. These had been studied for other reasons previously, e.g. small blocking sets.
- Exploited the fact that rank one matrices in $M_2(\mathbb{F}_{q^m})$ correspond projectively to a *hyperbolic quadric* $Q^+(3, q^m)$ in $\mathrm{PG}(3, q^m)$.

Basic Idea

We need to study $\mathbb{F}_q$-subspaces of $(\mathbb{F}_{q^m})^n$ up to the action of $\Gamma L(n, q^m)$.

Any property that is invariant under the action of $\Gamma L(n, q^m)$ can be used as an invariant of the corresponding code.

Basic Idea

We need to study $\mathbb{F}_q$-subspaces of $(\mathbb{F}_{q^m})^n$ up to the action of $\Gamma L(n, q^m)$.

Any property that is invariant under the action of $\Gamma L(n, q^m)$ can be used as an invariant of the corresponding code.

(See also: talk of Arani Paul on Thursday)

Dimension

The first obvious invariant of a q-system of fixed effective length is the dimension of the corresponding code C; in other words, the rank of the matrix G, or the dimension of the $\mathbb{F}_{q^m}$-span of U.

Dimension

The first obvious invariant of a q-system of fixed effective length is the dimension of the corresponding code C; in other words, the rank of the matrix G, or the dimension of the $\mathbb{F}_{q^m}$-span of U.

If U arises from an MRD code of dimension $ms(t-d+1)$ in $M_{s\times t}(\mathbb{F}_{q^m})$, then we have

$$s(t-d+1) \leq \dim(C) \leq \min\{st, ms(t-d+1)\}.$$

For example with $t=d=m=2, s=3$, we have

$$3 \leq \dim(C) \leq 6.$$

Dimension

The first obvious invariant of a q-system of fixed effective length is the dimension of the corresponding code C; in other words, the rank of the matrix G, or the dimension of the $\mathbb{F}_{q^m}$-span of U.

If U arises from an MRD code of dimension $ms(t-d+1)$ in $M_{s\times t}(\mathbb{F}_{q^m})$, then we have

$$\boxed{s(t-d+1) \leq \dim(C) \leq \min\{st, ms(t-d+1)\}.}$$

For example with $t = d = m = 2, s = 3$, we have

$$3 \leq \dim(C) \leq 6.$$

The lower bound is reached if and only if $\mathcal{U}$ is in fact an $\mathbb{F}_{q^m}$-subspace.

Small dimension

For example with $t = s = d = m = 2$, we are considering 4-dimensional subspaces $\mathcal{U}$ of $M_2(\mathbb{F}_{q^2})$. The corresponding code C has

$$2 \leq \dim(C) \leq 4.$$

Small dimension

For example with $t = s = d = m = 2$, we are considering 4-dimensional subspaces $\mathcal{U}$ of $M_2(\mathbb{F}_{q^2})$. The corresponding code C has

$$2 \leq \dim(C) \leq 4.$$

In Cardinali-Polverino-Trombetti a classification was shown.

- If $\dim(C) = 2$ then $\mathcal{U}$ is the example arising from $\mathbb{F}_{q^4}$.
- If $\dim(C) = 3$ then $\mathcal{U}$ is the example arising from the Dickson semifields.
- If $\dim(C) = 4$, then C is the whole space and U is a *canonical subgeometry*. Further geometric subdivision of this case is possible.

Small dimension

For example with $t = d = m = 2, s = 3$, we have

$$3 \leq \dim(C) \leq 6.$$

Small dimension

For example with $t = d = m = 2, s = 3$, we have

$$3 \leq \dim(C) \leq 6.$$

All $\mathbb{F}_{q^m}$-subspaces of $M_{3\times 2}(\mathbb{F}_{q^m})$ have been classified (Lavrauw-Sheekey). These are the cases where $\dim(C) = 3$.

Small dimension

For example with $t = d = m = 2, s = 3$, we have

$$3 \leq \dim(C) \leq 6.$$

All $\mathbb{F}_{q^m}$-subspaces of $M_{3\times 2}(\mathbb{F}_{q^m})$ have been classified (Lavrauw-Sheekey). These are the cases where $\dim(C) = 3$.

Question

Can we characterise MRD codes in $M_{3\times 2}(\mathbb{F}_{q^2})$ of dimension 6 over $\mathbb{F}_q$? Perhaps where C has dimension 4?

Literature

A lot of research has gone into establishing correspondences between q-systems/linear sets and rank-metric codes. The following telling is drawn from various sources, using my own biased preferences for notation and exposition!

- Blokhuis-Lavrauw, Ball-Blokhuis-Lavrauw
- Randrianarisoa
- Lunardon
- Sheekey-Van de Voorde
- Alfarano-Borello-Neri-Ravagnani
- Marino-Neri-Trombetti
- Bartoli-Marino-Neri
- Bartoli-Csajbòk-Marino-Trombetti
- Csajbók-Marino-Polverino-Zullo

Rank Metric Codes

Weights and Supports

The *rank weight* of a vector $v = (v_1, v_2, \dots, v_n) \in (\mathbb{F}_{q^m})^n$ is defined as

$$\mathrm{wt}_R(v) := \dim_{\mathbb{F}_q} \langle v_1, v_2, \dots, v_n \rangle$$

Note that $\mathrm{wt}_R(v) = \dim_{\mathbb{F}_q}(\{vy^t : y \in \mathbb{F}_q^n\})$.

So $\mathrm{wt}_R(v) = \dim_{\mathbb{F}_q} U_v$.

Generator Matrix

Consider the map

$$\begin{aligned}\phi_G &: \mathbb{F}_q^n \to (\mathbb{F}_{q^m})^k \\ &: y \mapsto Gy^t\end{aligned}$$

Generator Matrix

Consider the map

$$\begin{aligned}\phi_G : \mathbb{F}_q^n &\to (\mathbb{F}_{q^m})^k \\ : y &\mapsto Gy^t\end{aligned}$$

$$U_G = \{Gy^t : y \in \mathbb{F}_q^n\} = \mathrm{Im}(\phi_G).$$

Generator Matrix

Consider the map

$$\begin{aligned}\phi_G &: \mathbb{F}_q^n \to (\mathbb{F}_{q^m})^k \\ &: y \mapsto Gy^t\end{aligned}$$

$$U_G = \{Gy^t : y \in \mathbb{F}_q^n\} = \mathrm{Im}(\phi_G).$$

By the rank-nullity theorem, we have

$$\begin{aligned}\dim_{\mathbb{F}_q} U_G &= \dim_{\mathbb{F}_q} \mathrm{Im}(\phi_G) \\ &= n - \dim_{\mathbb{F}_q} \ker(\phi_G)\end{aligned}$$

Note that

$$\ker(\phi_G) = \{y \in \mathbb{F}_q^n | Gy^t = 0\}$$

Subcodes

Let D be a n i-dimensional subcode of C, and G a generator matrix for C. Then there exists $X \in \mathbb{F}_{q^m}^{i \times k}$ of rank i such that XG is a generator matrix for D.

Subcodes

Let D be a n i-dimensional subcode of C, and G a generator matrix for C. Then there exists $X \in \mathbb{F}_{q^m}^{i \times k}$ of rank i such that XG is a generator matrix for D.

For example, if $D = \langle x_1 G, \cdots, x_i G \rangle$, then let the x_j be the rows of X.

Subcodes

Let D be a n i-dimensional subcode of C, and G a generator matrix for C. Then there exists $X \in \mathbb{F}_{q^m}^{i \times k}$ of rank i such that XG is a generator matrix for D.

For example, if $D = \langle x_1 G, \cdots, x_i G \rangle$, then let the x_j be the rows of X.

In fact, we can identify subcodes of C with subspaces of $\mathbb{F}_{q^m}^{k}$ via G.

Subcodes

Let D be a n i-dimensional subcode of C, and G a generator matrix for C. Then there exists $X \in \mathbb{F}_{q^m}^{i \times k}$ of rank i such that XG is a generator matrix for D.

For example, if $D = \langle x_1 G, \cdots, x_i G \rangle$, then let the x_j be the rows of X.

In fact, we can identify subcodes of C with subspaces of $\mathbb{F}_{q^m}^k$ via G.

Subcodes of C of dimension i

$\leftrightarrow$

Rowspaces of XG for $X \in M_{i \times k}(\mathbb{F}_{q^m})$

Subcodes

Let us consider the q-system of a subcode. To calculate its dimension, it suffices to calculate

$$\begin{aligned}\ker(\phi_{XG}) &= \{y \in \mathbb{F}_q^n | (XG)y^t = 0\} \\ &= \{y \in \mathbb{F}_q^n | (X(Gy^t) = 0\},\end{aligned}$$

Subcodes

Let us consider the q-system of a subcode. To calculate its dimension, it suffices to calculate

$$\begin{aligned}\ker(\phi_{XG}) &= \{y \in \mathbb{F}_q^n | (XG)y^t = 0\} \\ &= \{y \in \mathbb{F}_q^n | (X(Gy^t) = 0\},\end{aligned}$$

and so we have

$$\dim_{\mathbb{F}_q} U_{XG} = n - \dim_{\mathbb{F}_q} \ker(\phi_{XG}) = n - \dim_{\mathbb{F}_q}(R(X)^\perp \cap U_G)$$

Subcodes

Let us consider the q-system of a subcode. To calculate its dimension, it suffices to calculate

$$\begin{aligned}\ker(\phi_{XG}) &= \{y \in \mathbb{F}_q^n | (XG)y^t = 0\} \\ &= \{y \in \mathbb{F}_q^n | (X(Gy^t) = 0\},\end{aligned}$$

and so we have

$$\dim_{\mathbb{F}_q} U_{XG} = n - \dim_{\mathbb{F}_q} \ker(\phi_{XG}) = n - \dim_{\mathbb{F}_q}(R(X)^{\perp} \cap U_G)$$

Effective lengths of subcodes of C of dimension i

$\leftrightarrow$

Intersections of U_G with $(k-i)$-dimensional subspaces

Generalised Weights and Evasiveness

Let C be a code with generator matrix G, and U_G the corresponding q-system. The *generalised weights* of C can be defined or characterised as follows.

$$d_i(C) = n - \max\{\dim_{\mathbb{F}_q}(U_G \cap W) : W \leq \mathbb{F}_{q^m}^k, \dim(W) = k-i\}$$

Generalised Weights and Evasiveness

Let C be a code with generator matrix G, and U_G the corresponding q-system. The *generalised weights* of C can be defined or characterised as follows.

$$d_i(C) = n - \max\{\dim_{\mathbb{F}_q}(U_G \cap W) : W \leq \mathbb{F}_{q^m}^k, \dim(W) = k - i\}$$

A q-system U is (h, r)-evasive if for every h-dimensional $\mathbb{F}_{q^m}$-subspace W of $(\mathbb{F}_{q^m})^k$ we have $\dim_{\mathbb{F}_q}(U \cap W) \leq r$.

Generalised Weights and Evasiveness

Let C be a code with generator matrix G, and U_G the corresponding q-system. The *generalised weights* of C can be defined or characterised as follows.

$$d_i(C) = n - \max\{\dim_{\mathbb{F}_q}(U_G \cap W) : W \leq \mathbb{F}_{q^m}^k, \dim(W) = k - i\}$$

A q-system U is (h, r)-evasive if for every h-dimensional $\mathbb{F}_{q^m}$-subspace W of $(\mathbb{F}_{q^m})^k$ we have $\dim_{\mathbb{F}_q}(U \cap W) \leq r$.

The case $h = r$ is also referred as *scattered*.

Generalised Weights and Evasiveness

Let C be a code with generator matrix G, and U_G the corresponding q-system. The *generalised weights* of C can be defined or characterised as follows.

$$d_i(C) = n - \max\{\dim_{\mathbb{F}_q}(U_G \cap W) : W \leq \mathbb{F}_{q^m}^k, \dim(W) = k-i\}$$

A q-system U is (h,r)-evasive if for every h-dimensional $\mathbb{F}_{q^m}$-subspace W of $(\mathbb{F}_{q^m})^k$ we have $\dim_{\mathbb{F}_q}(U \cap W) \leq r$.

The case $h = r$ is also referred as *scattered*.

Knowing all pairs $(\dim_{\mathbb{F}_{q^m}}(W), \dim_{\mathbb{F}_q}(U_G \cap W))$ determines both of the above.

Rank distribution

Effective lengths of subcodes of C of dimension 1

$\leftrightarrow$

Rank-weights of codewords of C

$\leftrightarrow$

Intersections of U_G with $(k-1)$-dimensional subspaces

So a code can be MRD in two different ways! As $\mathcal{U} \leq M_{s\times t}(\mathbb{F}_{q^m})$, and as $C \leq (\mathbb{F}_{q^m})^{st}$!

My favourite code

The following q-system was introduced by Bartoli-Neri-Marino.

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

The q-system is $(2, 3)$-evasive, and the corresponding code is MRD with generalised weights $(3, 5, 7, 8)$.

My favourite code

The following q-system was introduced by Bartoli-Neri-Marino.

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

The q-system is $(2,3)$-evasive, and the corresponding code is MRD with generalised weights $(3,5,7,8)$.

This lead to the first example of two MRD codes with the same parameters, but different generalised weights; for example, the direct sum of two 2-dimensional Gabidulin codes has generalised weights $(3,4,7,8)$.

My favourite code

The following q-system was introduced by Bartoli-Neri-Marino.

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

The q-system is $(2,3)$-evasive, and the corresponding code is MRD with generalised weights $(3,5,7,8)$.

This lead to the first example of two MRD codes with the same parameters, but different generalised weights; for example, the direct sum of two 2-dimensional Gabidulin codes has generalised weights $(3,4,7,8)$.

Further interesting examples, e.g. Bartoli-Giannoni-Marino, Longobardi-Marino-Trombetti-Zho.

Small parameters

Consider the case $t = s = d = 2, m = 3$. Then Mario-Polverino-Trombetti showed that one of the following possibilities must occur.

- $\dim(C) = 3$;
  - unique 1-dimensional subspace W with $\dim(W \cap U) = 3$
  - no 1-dimensional subspace W with $\dim(W \cap U) = 3$ (U is $(1, 2)$-evasive)
- $\dim(C) = 4$:
  - unique 2-dimensional subspace W with $\dim(W \cap U) = 4$
  - no 2-dimensional subspace W with $\dim(W \cap U) \geq 4$ exists (U is $(2, 3)$-evasive)
  - no 1-dimensional subspace W with $\dim(W \cap U) \geq 2$ exists (U is $(1, 1)$-evasive, scattered)

Next smallest example

Question

Can we find a similar subdivision of q-systems by their evasiveness properties? For example

$$M_{2\times 2}(\mathbb{F}_{q^4}), d = 2$$
$$M_{3\times 3}(\mathbb{F}_{q^2}), d = 3$$
$$M_{4\times 4}(\mathbb{F}_{q^2}), d = 3$$

The last of these is the smallest case were we can consider square MRD codes which do not arise from semifields, or their rank-metric duals.

From vector codes to matrix codes

Suppose we have an “interesting” construction of a vector rank metric code. Can it arise from an MRD matrix rank-metric code?

From vector codes to matrix codes

Suppose we have an “interesting” construction of a vector rank metric code. Can it arise from an MRD matrix rank-metric code?

For example, consider the case $n = 8, k = m = 4$.

From vector codes to matrix codes

Suppose we have an “interesting” construction of a vector rank metric code. Can it arise from an MRD matrix rank-metric code?

For example, consider the case $n = 8, k = m = 4$.

Which codes can arise from an MRD code in $M_{2\times 2}(\mathbb{F}_{q^4})$ with $d = 2$?

From vector codes to matrix codes

Suppose we have an "interesting" construction of a vector rank metric code. Can it arise from an MRD matrix rank-metric code?

For example, consider the case $n = 8, k = m = 4$.

Which codes can arise from an MRD code in $M_{2\times 2}(\mathbb{F}_{q^4})$ with $d = 2$?

If U is the q-system of the given code, we need to find an invertible Z such that ZU does not contain any matrices of rank 1.

From vector codes to matrix codes

Suppose we have an "interesting" construction of a vector rank metric code. Can it arise from an MRD matrix rank-metric code?

For example, consider the case $n = 8, k = m = 4$.

Which codes can arise from an MRD code in $M_{2\times 2}(\mathbb{F}_{q^4})$ with $d = 2$?

If U is the q-system of the given code, we need to find an invertible Z such that ZU does not contain any matrices of rank 1.

Geometrically, we need to find a hyperbolic quadric meeting U trivially. Since any two such quadrics are equivalent, if we find one then we can find the matrix Z.

From vector codes to matrix codes

Given a q-system U in $(\mathbb{F}_{q^m})^4$, find a quadratic form Q such that

$$Q(u) \neq 0 \; \forall u \in U^{\times}.$$

From vector codes to matrix codes

Given a q-system U in $(\mathbb{F}_{q^m})^4$, find a quadratic form Q such that

$$Q(u) \neq 0 \; \forall u \in U^{\times}.$$

We can think of the coefficients of Q as indeterminates. Then we get a set of linear conditions from the image of the elements of u under the *veronese map*.

$$\sum_{i \leq j} Q_{ij} u_i u_j \neq 0$$

From vector codes to matrix codes

Given a q-system U in $(\mathbb{F}_{q^m})^4$, find a quadratic form Q such that

$$Q(u) \neq 0 \ \forall u \in U^{\times}.$$

We can think of the coefficients of Q as indeterminates. Then we get a set of linear conditions from the image of the elements of u under the *veronese map*.

$$\sum_{i \leq j} Q_{ij} u_i u_j \neq 0$$

This can actually be rephrased as a question about the existence of a codeword of maximum weight in a Hamming metric code (with an extra property).

From vector codes to matrix codes

Question

Can my favourite code of Bartoli-Marino-Neri arise from a matrix MRD code? I.e. a semifield?

From vector codes to matrix codes

Question

Can my favourite code of Bartoli-Marino-Neri arise from a matrix MRD code? I.e. a semifield?

Generalised weights correspond to how q-systems intersect linear subspaces.

From vector codes to matrix codes

Question

Can my favourite code of Bartoli-Marino-Neri arise from a matrix MRD code? I.e. a semifield?

Generalised weights correspond to how q-systems intersect linear subspaces.

Question

Does it make sense to define *quadratic* generalised weights? Using how U intersects with quadrics?

From matrix codes to vector codes

Using *skew-polynomial rings*, we can construct $\mathbb{F}_q$-linear MRD codes in $M_{s\times s}(\mathbb{F}_{q^m})$ for all parameters.

The base case $t = s = d$ of this coincides with *cyclic semifields*, which were geometrically characterised.

Question

Can we geometrically characterise these constructions?

Cyclic semifieds have been generalised to other examples with $t = s = d$ (Johnson-Marino-Polverino-Trombetti)

Question

Can the generalisations for $t = s = d$ be generalised to $s = t > d$?

Further Geometry

For $M_2(\mathbb{F}_{q^3})$, further subdivision of the cases can be achieved.

(0) L is a union of either q^2+q+1 or q^2+1 lines of a pencil in Σ.
(1) L is a union of q^2+q+1 lines in a plane not belonging to a pencil.
(2) L is a union of q^2+q+1 lines through a point, not all lines in the same plane.
(3) L contains a unique point of weight 2, does not contain any line and is not contained in a plane.
(4) L contains exactly one line and such a line contains $q+1$ points of weight 2.
(5) Any point of L has weight 1 (that is, L is a scattered $\mathbb{F}_q$-linear set).

The corresponding classes of semifields are labeled $\mathcal{F}_i$, for $i=0,1,\ldots,5$. Moreover, in [10] the class $\mathcal{F}_4$ is further partitioned into three subclasses. Namely, if r is the unique line contained in the linear set $L=L(S)$ of type (4), then one of the following situations must occur:

(a) $r^\perp \cap L = \emptyset$,
(b) $|r^\perp \cap L| = 1$,
(c) $|r^\perp \cap L| = q+1$,

where $\perp$ is the polarity of Σ induced by the hyperbolic quadric $\mathcal{Q} \cong Q^+(3,q^3)$. The corresponding subclasses of semifields are denoted $\mathcal{F}_4^{(a)}$, $\mathcal{F}_4^{(b)}$, and $\mathcal{F}_4^{(c)}$, respectively. We now determine the general form for multiplication in each of these subclasses.

Question

Do any of these generalise to other parameters?

Further Geometry

Semifields of order q^6 with $|\mathbb{N}_l| = q^3$ and $|\mathbb{K}| = q$

Family	$\lvert\mathbb{N}_m\rvert$	$\lvert\mathbb{N}_r\rvert$	Existence results
$\mathcal{F}_0$	q	q	**Generalized Dickson semifields, q odd**
$\mathcal{F}_1$	q	q	**Semifields from Payne–Thas ovoid of $Q(4, 3^3)$**
$\mathcal{F}_2$	q	q	**Semifields from Ganley flock of $PG(3, 3^3)$**
$\mathcal{F}_3$	q	q	HJ semifields [9] of type II, III, IV, V for $q = 2$ Dempwolff
$\mathcal{F}_4^{(a)}$	q^2	q	**$\exists$! semifield for q odd, $\nexists$ semifields for q even**
	q	q^2	**$\exists$! semifield for q odd, $\nexists$ semifields for q even**
	q	q	?
$\mathcal{F}_4^{(b)}$	q	q	There exist semifields for $q = 3$ [7]
$\mathcal{F}_4^{(c)}$	q	q	There exist semifields for any q [6]
	q^2	q^2	**Cyclic semifields for any q**
$\mathcal{F}_5$	q^3	q^3	**Hughes Kleinfeld semifields**
	q^3	q	**Knuth semifields of type (17) for any q**
	q	q^3	**Knuth semifields of type (19) for any q**
	q^2	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q^2	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)
	q	q	$\exists$ for any $q \neq 2$ (e.g. Generalized Twisted Fields)

Further Results

The following cases have been classified by exhaustive computation.

- $M_2(\mathbb{F}_{2^3})$ and $M_3(\mathbb{F}_{2^2})$ follow from the full classification of semifields of order 2^6 (Rua-Combarro-Ranilla)
- $M_2(\mathbb{F}_{2^4})$ has been classified and will appear soon!

Further Directions

We could reduce the space of interest by considering only *symmetric matrices*; in the case $t = s = d$, this corresponds to *commutative semifields*.

The case $t = s = d = 2$ is fully classified for arbitrary m with q *large enough* (Blokhuis-Lavrauw-Ball, Lavrauw).

The case $t = s = d = 3$, $m = 2$ is fully classified (Marino-Pepe, Pepe).

Question

Can we address the smallest open cases?

Merci beaucoup!