Rank Metric Codes and related Structures

Yue Zhou

July 5, 2017

The 2nd International Workshop on Boolean Functions and their Applications (BFA)

Outline

Introduction

Maximum rank distance codes

Quadratic bent-Negabent functions

Vectorial quadratic bent functions

Exceptional scattered polynomials

Introduction

Rank metric codes

Definition

The rank metric on $\mathbb{K}^{m \times n}$ is defined by

$$d(A, B) = \mathrm{rank}(A - B)$$

for $A, B \in \mathbb{K}^{m \times n}$.

Rank metric codes

Definition

The rank metric on $\mathbb{K}^{m \times n}$ is defined by

$$d(A, B) = \mathrm{rank}(A - B)$$

for $A, B \in \mathbb{K}^{m \times n}$.

- It is not difficult to show that

$$\mathrm{rank}(A) + \mathrm{rank}(B) \geqslant \mathrm{rank}(A + B).$$

Rank metric codes

Definition

The rank metric on $\mathbb{K}^{m\times n}$ is defined by

$$d(A,B) = \mathrm{rank}(A-B)$$

for $A, B \in \mathbb{K}^{m\times n}$.

- It is not difficult to show that

$$\mathrm{rank}(A) + \mathrm{rank}(B) \geqslant \mathrm{rank}(A+B).$$

- $\mathcal{C} \subseteq \mathbb{K}^{m\times n}$ is a rank metric code.

Rank metric codes

Definition

The rank metric on $\mathbb{K}^{m\times n}$ is defined by

$$d(A,B) = \mathrm{rank}(A-B)$$

for $A, B \in \mathbb{K}^{m\times n}$.

- It is not difficult to show that

$$\mathrm{rank}(A) + \mathrm{rank}(B) \geqslant \mathrm{rank}(A+B).$$

- $\mathcal{C} \subseteq \mathbb{K}^{m\times n}$ is a rank metric code.
- The minimum distance of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min_{A,B\in\mathcal{C},A\neq B}\{d(A,B)\}.$$

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
    - (Pre)quasifield, translation planes.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
    - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
    - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
    - Quadratic APN functions.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
  - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
  - Quadratic APN functions.
- Vectorial (quadratic) bent functions.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
    - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
    - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
  - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
  - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.
- $\cdots$.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
  - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
  - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.
- $\cdots$.

Applications:

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
  - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
  - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.
- $\cdots$.

Applications:

- Construction of subspace codes in network coding.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
    - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
    - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.
- $\cdots$.

Applications:

- Construction of subspace codes in network coding.
- McEliece cryptosystem.

Rank metric codes

We are interested in $\mathcal{C}$ with extreme properties ($\#\mathcal{C}$ and $d(\mathcal{C})$):

- Maximum rank distance (MRD) codes.
  - (Pre)quasifield, translation planes.
- Splitting dimensional dual hyperovals.
  - Quadratic APN functions.
- Vectorial (quadratic) bent functions.
- Scattered linear sets.
- $\cdots$.

Applications:

- Construction of subspace codes in network coding.
- McEliece cryptosystem.
- $\cdots$.

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m \times n}$ are equivalent

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$ are equivalent if there are $A \in \mathrm{GL}(m, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m \times n}$ are equivalent if there are $A \in \mathrm{GL}(m, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m \times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AX^\gamma B + C : X \in \mathcal{C}_1\},$$

where $X^\gamma := (x_{ij}^\gamma)$.

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$ are equivalent if there are $A \in \mathrm{GL}(m, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AX^\gamma B + C : X \in \mathcal{C}_1\},$$

where $X^\gamma := (x_{ij}^\gamma)$.

- (A, B, C, γ) is an isometry over $\mathbb{K}^{m\times n}$.

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$ are equivalent if there are $A \in \mathrm{GL}(m,\mathbb{K})$, $B \in \mathrm{GL}(n,\mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AX^{\gamma}B + C : X \in \mathcal{C}_1\},$$

where $X^{\gamma} := (x_{ij}^{\gamma})$.

- (A, B, C, γ) is an isometry over $\mathbb{K}^{m\times n}$.
- When $m = n$, another definition of equivalence:

$$AX^{\gamma}B + C \text{ or } A(X^{\gamma})^T B + C.$$

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$ are equivalent if there are $A \in \mathrm{GL}(m, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AX^\gamma B + C : X \in \mathcal{C}_1\},$$

where $X^\gamma := (x_{ij}^\gamma)$.

- (A, B, C, γ) is an isometry over $\mathbb{K}^{m\times n}$.
- When $m = n$, another definition of equivalence:

$$AX^\gamma B + C \text{ or } A(X^\gamma)^T B + C.$$

- If $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear over $\mathbb{K}$, then we can assume that $C = O$.

Definition

Two rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$ are equivalent if there are $A \in \mathrm{GL}(m, \mathbb{K})$, $B \in \mathrm{GL}(n, \mathbb{K})$, $C \in \mathbb{K}^{m\times n}$ and $\gamma \in \mathrm{Aut}(\mathbb{K})$ such that

$$\mathcal{C}_2 = \{AX^\gamma B + C : X \in \mathcal{C}_1\},$$

where $X^\gamma := (x_{ij}^\gamma)$.

- (A, B, C, γ) is an isometry over $\mathbb{K}^{m\times n}$.
- When $m = n$, another definition of equivalence:

$$AX^\gamma B + C \text{ or } A(X^\gamma)^T B + C.$$

- If $\mathcal{C}_1$ and $\mathcal{C}_2$ are linear over $\mathbb{K}$, then we can assume that $C = O$.
- When $\mathcal{C}_1 = \mathcal{C}_2$, all (A, B, C, γ) form the automorphism group.

Maximum rank distance codes

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$.

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$.
- We assume that $m \leqslant n$.

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$.
- We assume that $m \leqslant n$.
- When $d(\mathcal{C}) = d$, it is well-known that (Singleton bound)

$$\#\mathcal{C} \leqslant q^{n(m-d+1)}.$$

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$.
- We assume that $m \leqslant n$.
- When $d(\mathcal{C}) = d$, it is well-known that (Singleton bound)

$$\#\mathcal{C} \leqslant q^{n(m-d+1)}.$$

- Proof: $k := m - d + 1$, look at any k rows of

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & \cdots \end{pmatrix}.$$

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m \times n}$.
- We assume that $m \leqslant n$.
- When $d(\mathcal{C}) = d$, it is well-known that (Singleton bound)

$$\#\mathcal{C} \leqslant q^{n(m-d+1)}.$$

- Proof: $k := m - d + 1$, look at any k rows of

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & \cdots \end{pmatrix}.$$

- When the equality holds, we call $\mathcal{C}$ a maximum rank distance (MRD for short) code.

Maximum rank distance codes

- Let $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$.
- We assume that $m \leqslant n$.
- When $d(\mathcal{C}) = d$, it is well-known that (Singleton bound)

$$\#\mathcal{C} \leqslant q^{n(m-d+1)}.$$

- Proof: $k := m - d + 1$, look at any k rows of

$$\begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ c_{m1} & c_{m2} & \cdots & \cdots \end{pmatrix}.$$

- When the equality holds, we call $\mathcal{C}$ a maximum rank distance (MRD for short) code.
- How to construct MRD codes?

Gabidulin codes

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.

Gabidulin codes

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.
- Gabidulin codes ($k = n - d + 1$, $m = n$)

  $\mathcal{G} = \{a_0 X + a_1 X^q + \ldots a_{k-1} X^{q^{k-1}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$.

Gabidulin codes

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.
- Gabidulin codes ($k = n - d + 1$, $m = n$)

  $\mathcal{G} = \{a_0 X + a_1 X^q + \ldots a_{k-1} X^{q^{k-1}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$.

  ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.

Gabidulin codes

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0 X + a_1 X^q + \cdots + a_i X^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.
- Gabidulin codes ($k = n - d + 1$, $m = n$)

  $\mathcal{G} = \{a_0 X + a_1 X^q + \ldots a_{k-1} X^{q^{k-1}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$.
  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(m-d+1)}$ with $d = m - k + 1$.

Gabidulin codes

Definition

A linearized polynomial (q-polynomial) is in $\mathbb{F}_{q^n}[X]$ of the form

$$a_0X + a_1X^q + \cdots + a_iX^{q^i} + \cdots .$$

Let $\mathscr{L}_{(n,q)}[X]$ denote all linearized polynomials in $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n})$.
- Gabidulin codes ($k = n - d + 1$, $m = n$)

  $$\mathcal{G} = \{a_0X + a_1X^q + \ldots a_{k-1}X^{q^{k-1}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}.$$

  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(m-d+1)}$ with $d = m - k + 1$.
  - ▷ Gabidulin codes are $\mathbb{F}_{q^n}$-linear MRD codes.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ ($k = 1$), $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ $(k = 1)$, $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ $(k = 1)$, $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

- (Pre)quasifield $\mathcal{Q}$;

Known families of MRD codes ($d = m = n$)

When $m = n = d$ $(k = 1)$, $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

- (Pre)quasifield $\mathcal{Q}$;
  - ▷ When $\mathcal{C}$ is $\mathbb{F}_q$-linear, $\mathcal{Q}$ is a (pre)semifield.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ ($k = 1$), $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

- (Pre)quasifield $\mathcal{Q}$;
  - ▷ When $\mathcal{C}$ is $\mathbb{F}_q$-linear, $\mathcal{Q}$ is a (pre)semifield.
- Spreads.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ $(k = 1)$, $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

- (Pre)quasifield $\mathcal{Q}$;
  - ▷ When $\mathcal{C}$ is $\mathbb{F}_q$-linear, $\mathcal{Q}$ is a (pre)semifield.
- Spreads.

There are a considerable amount of inequivalent quasifields and semifields.

Known families of MRD codes ($d = m = n$)

When $m = n = d$ $(k = 1)$, $\mathcal{G} = \{a_0 * X : a_0 \in \mathbb{F}_{q^n}\}$.

MRD codes $\mathcal{C}$ and the following algebraic/geometric objects are equivalent.

- (Pre)quasifield $\mathcal{Q}$;
  - ▷ When $\mathcal{C}$ is $\mathbb{F}_q$-linear, $\mathcal{Q}$ is a (pre)semifield.
- Spreads.

There are a considerable amount of inequivalent quasifields and semifields. In particular, for $q = 2^m$, there are exponentially many inequivalent ones (Kantor).

Known families of F_q-linear MRD codes ($d \leq m = n$)

Let $m, n, k, s \in \mathbb{Z}^+$, $\gcd(n, s) = 1$, $k < m$ and q a power of prime.

Known families of F_q-linear MRD codes ($d \leq m = n$)

Let $m, n, k, s \in \mathbb{Z}^+$, $\gcd(n, s) = 1$, $k < m$ and q a power of prime.
(generalized) twisted Gabidulin codes [Sheekey 2016]:

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 X + \cdots + a_{k-1} X^{q^{s(k-1)}} + \eta a_0^{q^h} X^{q^{sk}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

where $h \in \mathbb{Z}^+$ and $\eta \in \mathbb{F}_{q^n}$ is such that $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$.

Known families of F_q-linear MRD codes ($d \leq m = n$)

Let $m, n, k, s \in \mathbb{Z}^+$, $\gcd(n, s) = 1$, $k < m$ and q a power of prime.
(generalized) twisted Gabidulin codes [Sheekey 2016]:

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 X + \cdots + a_{k-1} X^{q^{s(k-1)}} + \eta a_0^{q^h} X^{q^{sk}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

where $h \in \mathbb{Z}^+$ and $\eta \in \mathbb{F}_{q^n}$ is such that $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$.

- $\mathcal{H}_{k,s}(0, /)$ is a Gabidulin code [Delsarte 1978], [Gabidulin 1985], [Kshevetskiy and Gabidulin 2005].

Known families of F_q-linear MRD codes ($d \leq m = n$)

Let $m, n, k, s \in \mathbb{Z}^+$, $\gcd(n, s) = 1$, $k < m$ and q a power of prime.
(generalized) twisted Gabidulin codes [Sheekey 2016]:

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 X + \cdots + a_{k-1} X^{q^{s(k-1)}} + \eta a_0^{q^h} X^{q^{sk}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

where $h \in \mathbb{Z}^+$ and $\eta \in \mathbb{F}_{q^n}$ is such that $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$.

- $\mathcal{H}_{k,s}(0, /)$ is a Gabidulin code [Delsarte 1978], [Gabidulin 1985], [Kshevetskiy and Gabidulin 2005].
- When $q = 2$, η must be 0.

Known families of F_q-linear MRD codes ($d \leq m = n$)

Let $m, n, k, s \in \mathbb{Z}^+$, $\gcd(n, s) = 1$, $k < m$ and q a power of prime. (generalized) twisted Gabidulin codes [Sheekey 2016]:

$$\mathcal{H}_{k,s}(\eta, h) = \{a_0 X + \cdots + a_{k-1} X^{q^{s(k-1)}} + \eta a_0^{q^h} X^{q^{sk}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

where $h \in \mathbb{Z}^+$ and $\eta \in \mathbb{F}_{q^n}$ is such that $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$.

- $\mathcal{H}_{k,s}(0, /)$ is a Gabidulin code [Delsarte 1978], [Gabidulin 1985], [Kshevetskiy and Gabidulin 2005].
- When $q = 2$, η must be 0.
- The equivalence between different members and the automorphism groups can be completely determined (Lunardon, Trombetti, Z)

Known families of MRD codes ($d \leq m = n$)

Nonlinear families:

Known families of MRD codes ($d \leq m = n$)

Nonlinear families:

1. Size q^{2n} [Cossidente, Marino, Pavese 2016] [Durante, Siciliano].

Known families of MRD codes ($d \leq m = n$)

Nonlinear families:

1. Size q^{2n} [Cossidente, Marino, Pavese 2016] [Durante, Siciliano].
2. Slight modifications of twisted Gabidulin codes [Otal and Özbudak 2016].

Known families of MRD codes ($d \leq m = n$)

Nonlinear families:

1. Size q^{2n} [Cossidente, Marino, Pavese 2016] [Durante, Siciliano].
2. Slight modifications of twisted Gabidulin codes [Otal and Özbudak 2016].

Question

Find more new MRD codes for $d \leq m = n$.

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$:

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$: Take $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Then

$$\mathcal{C} = \{(f(\alpha_1), \cdots, f(\alpha_m))^T : f \in \mathcal{F}\}$$

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$: Take $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Then

$$\mathcal{C} = \{(f(\alpha_1), \cdots, f(\alpha_m))^T : f \in \mathcal{F}\}$$

2. For $k = m - d + 1$, randomly generate MRD codes [Neri,Trautmann,Randrianarisoa,Rosenthal,2016].

$$\Pr > 1 - kq^{km-n}.$$

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$: Take $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Then
$$\mathcal{C} = \{(f(\alpha_1), \cdots, f(\alpha_m))^T : f \in \mathcal{F}\}$$
2. For $k = m - d + 1$, randomly generate MRD codes [Neri,Trautmann,Randrianarisoa,Rosenthal,2016].
$$\Pr > 1 - kq^{km-n}.$$
3. Twisting construction using chains of subfields [Puchinger, Nielsen, Sheekey].

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$: Take $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Then
$$\mathcal{C} = \{(f(\alpha_1), \cdots, f(\alpha_m))^T : f \in \mathcal{F}\}$$
2. For $k = m - d + 1$, randomly generate MRD codes [Neri,Trautmann,Randrianarisoa,Rosenthal,2016].
$$\mathrm{Pr} > 1 - kq^{km-n}.$$
3. Twisting construction using chains of subfields [Puchinger, Nielsen, Sheekey].
4. Using maximum scattered linear sets [Csajbók, Marino, Polverino, Zullo].

Known families of MRD codes ($d \leq m < n$)

1. Puncturing $n \times n$ MRD codes $\mathcal{F}$: Take $\mathbb{F}_q$-linearly independent elements $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$. Then
$$\mathcal{C} = \{(f(\alpha_1), \cdots, f(\alpha_m))^T : f \in \mathcal{F}\}$$
2. For $k = m - d + 1$, randomly generate MRD codes [Neri,Trautmann,Randrianarisoa,Rosenthal,2016].
$$\Pr > 1 - kq^{km-n}.$$
3. Twisting construction using chains of subfields [Puchinger, Nielsen, Sheekey].
4. Using maximum scattered linear sets [Csajbók, Marino, Polverino, Zullo].
5. Other constructions [Trautmann, Marshall 2016].

Known families of MRD codes ($d \leq m < n$)

How many inequivalent MRD codes are there in $\mathbb{F}_q^{m\times n}$?

Known families of MRD codes ($d \leq m < n$)

How many inequivalent MRD codes are there in $\mathbb{F}_q^{m\times n}$?

- By looking at Gabidulin codes for different $U = \langle \alpha_1, \cdots, \alpha_m \rangle$, we [Schmidt, Z] can show that this number

$$\geq \frac{(q-1)\begin{bmatrix} n \\ m \end{bmatrix}_q}{n(q^n-1)}.$$

Known families of MRD codes ($d \leq m < n$)

How many inequivalent MRD codes are there in $\mathbb{F}_q^{m\times n}$?

- By looking at Gabidulin codes for different $U = \langle \alpha_1, \cdots, \alpha_m \rangle$, we [Schmidt, Z] can show that this number

$$\geq \frac{(q-1)\left[{n \atop m} \right]_q}{n(q^n-1)}.$$

- Proved by investigating their right nuclei and middle nuclei.

Nuclei of rank metric codes

Definition

For rank metric codes in $\mathbb{K}^{m \times n}$:

Right nucleus: $N_r(\mathcal{C}) = \{Y \in \mathbb{K}^{n \times n} \ : \ CY \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Nuclei of rank metric codes

Definition

For rank metric codes in $\mathbb{K}^{m\times n}$:

Right nucleus: $N_r(\mathcal{C}) = \{Y \in \mathbb{K}^{n\times n} \,:\, CY \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Middle nucleus: $N_m(\mathcal{C}) = \{Z \in \mathbb{K}^{m\times m} : ZC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Nuclei of rank metric codes

Definition

For rank metric codes in $\mathbb{K}^{m\times n}$:

Right nucleus: $N_r(\mathcal{C}) = \{Y \in \mathbb{K}^{n\times n} : CY \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Middle nucleus: $N_m(\mathcal{C}) = \{Z \in \mathbb{K}^{m\times m} : ZC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

- When $\mathcal{C}$ is a spreadset defining a semifield $\mathbb{S}$, then $N_m(\mathcal{C})$ and $N_r(\mathcal{C})$ correspond to the middle nucleus and the right nucleus of $\mathbb{S}$ respectively.

Nuclei of rank metric codes

Definition

For rank metric codes in $\mathbb{K}^{m\times n}$:

Right nucleus: $N_r(\mathcal{C}) = \{Y \in \mathbb{K}^{n\times n} \,:\, CY \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Middle nucleus: $N_m(\mathcal{C}) = \{Z \in \mathbb{K}^{m\times m} : ZC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

- When $\mathcal{C}$ is a spreadset defining a semifield $\mathbb{S}$, then $N_m(\mathcal{C})$ and $N_r(\mathcal{C})$ correspond to the middle nucleus and the right nucleus of $\mathbb{S}$ respectively.
- For MRD codes with $d < m$, we can also define the *left nucleus* which is always $\mathbb{K}$.

Nuclei of rank metric codes

Definition

For rank metric codes in $\mathbb{K}^{m\times n}$:

Right nucleus: $N_r(\mathcal{C}) = \{Y \in \mathbb{K}^{n\times n} : CY \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

Middle nucleus: $N_m(\mathcal{C}) = \{Z \in \mathbb{K}^{m\times m} : ZC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$.

- When $\mathcal{C}$ is a spreadset defining a semifield $\mathbb{S}$, then $N_m(\mathcal{C})$ and $N_r(\mathcal{C})$ correspond to the middle nucleus and the right nucleus of $\mathbb{S}$ respectively.
- For MRD codes with $d < m$, we can also define the *left nucleus* which is always $\mathbb{K}$.
- Not invariant for nonlinear rank metric codes.

Nuclei of rank metric codes

- For two equivalent linear rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{K}^{m\times n}$, their right (resp. middle) nuclei are also equivalent.

Nuclei of rank metric codes

- For two equivalent linear rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{K}^{m\times n}$, their right (resp. middle) nuclei are also equivalent.

  $\mathcal{C}_2 = \{AX^\gamma B : X \in \mathcal{C}_1\} \Rightarrow Z \in N_m(\mathcal{C}_1)$ iff $AZ^\gamma A^{-1} \in N_m(\mathcal{C}_2)$

Nuclei of rank metric codes

- For two equivalent linear rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{K}^{m\times n}$, their right (resp. middle) nuclei are also equivalent.

  $\mathcal{C}_2 = \{AX^\gamma B : X \in \mathcal{C}_1\} \Rightarrow Z \in N_m(\mathcal{C}_1)$ iff $AZ^\gamma A^{-1} \in N_m(\mathcal{C}_2)$

  If $\gamma = \mathrm{id}$ and $\mathcal{C}_1 = \mathcal{C}_2$, then $A \in N_{GL(m,q)}(N_m(\mathcal{C}))$.

Nuclei of rank metric codes

- For two equivalent linear rank metric codes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $\mathbb{K}^{m\times n}$, their right (resp. middle) nuclei are also equivalent.

  $\mathcal{C}_2 = \{AX^\gamma B : X \in \mathcal{C}_1\} \Rightarrow Z \in N_m(\mathcal{C}_1)$ iff $AZ^\gamma A^{-1} \in N_m(\mathcal{C}_2)$

  If $\gamma = \mathrm{id}$ and $\mathcal{C}_1 = \mathcal{C}_2$, then $A \in N_{GL(m,q)}(N_m(\mathcal{C}))$.

- For (generalized) Gabidulin codes $\mathcal{G}_s = \{a_0X + a_1X^{q^s} + \ldots a_{k-1}X^{q^{s(k-1)}} : a_0, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\}$,

$$N_r(\mathcal{G}_s) = \{g : g \circ f \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n},$$
$$N_m(\mathcal{G}_s) = \{g : f \circ g \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n}.$$

Quadratic bent-Negabent functions

Maximum rank metric codes with restrictions

- Restrictions: Symmetric, symplectic, hermitian...

Maximum rank metric codes with restrictions

- Restrictions: Symmetric, symplectic, hermitian...
- Given minimum distance d, the upper bound of $\mathcal{C}$ is not completely clear.

Maximum rank metric codes with restrictions

- Restrictions: Symmetric, symplectic, hermitian...
- Given minimum distance d, the upper bound of $\mathcal{C}$ is not completely clear.

For instance:

Maximum rank metric codes with restrictions

- Restrictions: Symmetric, symplectic, hermitian...
- Given minimum distance d, the upper bound of $\mathcal{C}$ is not completely clear.

For instance:

- Let $\mathcal{C}$ be an additive d-code consisting of $m \times m$ symmetric matrix over $\mathbb{F}_q$. If $2 \nmid q$ ($2|q$ and $2 \nmid d$ or $d = m$), then

$$\#\mathcal{C} \leq \begin{cases} q^{m(m-d+2)/2}, & \text{if } m-d \text{ is even;} \\ q^{(m+1)(m-d+1)/2}, & \text{if } m-d \text{ is odd.} \end{cases}$$

Maximum rank metric codes with restrictions

- Restrictions: Symmetric, symplectic, hermitian...
- Given minimum distance d, the upper bound of $\mathcal{C}$ is not completely clear.

For instance:

- Let $\mathcal{C}$ be an additive d-code consisting of $m \times m$ symmetric matrix over $\mathbb{F}_q$. If $2 \nmid q$ ($2|q$ and $2 \nmid d$ or $d = m$), then

$$\#\mathcal{C} \leq \begin{cases} q^{m(m-d+2)/2}, & \text{if } m-d \text{ is even;} \\ q^{(m+1)(m-d+1)/2}, & \text{if } m-d \text{ is odd.} \end{cases}$$

- Proved by using association schemes. The upper bound is tight. (Schmidt 2010, 2015)

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is quadratic if $\delta_{f,a} : x \mapsto f(x+a) - f(x) - f(a)$ is $\mathbb{F}_p$-linear for all a.

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is quadratic if $\delta_{f,a} : x \mapsto f(x+a) - f(x) - f(a)$ is $\mathbb{F}_p$-linear for all a.
- Quadratic APN: kernel of $\delta_{f,a}$ is of dimension 1 for $a \in \mathbb{F}_{2^n}^*$.

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is quadratic if $\delta_{f,a} : x \mapsto f(x+a) - f(x) - f(a)$ is $\mathbb{F}_p$-linear for all a.
- Quadratic APN: kernel of $\delta_{f,a}$ is of dimension 1 for $a \in \mathbb{F}_{2^n}^*$.
- $\{\delta_{f,a} : a \in \mathbb{F}_{2^n}\}$ is a subspace of binary $n \times n$ matrices of rank $n-1$.

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is quadratic if $\delta_{f,a} : x \mapsto f(x+a) - f(x) - f(a)$ is $\mathbb{F}_p$-linear for all a.
- Quadratic APN: kernel of $\delta_{f,a}$ is of dimension 1 for $a \in \mathbb{F}_{2^n}^*$.
- $\{\delta_{f,a} : a \in \mathbb{F}_{2^n}\}$ is a subspace of binary $n \times n$ matrices of rank $n-1$.
- Quadratic AB: the set of alternating bilinear forms $\{\mathrm{Tr}(c(f(x+y) - f(x) - f(y))) : c \in \mathbb{F}_{2^n}^*\}$ defines a subspace of alternating binary $n \times n$ matrices of rank $n-1$.

- Quadratic APN functions, AB functions, (vectorial) bent functions... can be considered as rank metric codes with special properties.
- $f : \mathbb{F}_p^n \to \mathbb{F}_p^m$ is quadratic if $\delta_{f,a} : x \mapsto f(x+a) - f(x) - f(a)$ is $\mathbb{F}_p$-linear for all a.
- Quadratic APN: kernel of $\delta_{f,a}$ is of dimension 1 for $a \in \mathbb{F}_{2^n}^*$.
- $\{\delta_{f,a} : a \in \mathbb{F}_{2^n}\}$ is a subspace of binary $n \times n$ matrices of rank $n-1$.
- Quadratic AB: the set of alternating bilinear forms $\{\mathrm{Tr}(c(f(x+y) - f(x) - f(y))) : c \in \mathbb{F}_{2^n}^*\}$ defines a subspace of alternating binary $n \times n$ matrices of rank $n-1$.
- See Edel and Dempwolff's work: Nuclei, dimensional dual hyperovals ...

Quadratic bent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

Quadratic bent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is bent if $x \mapsto f(x+a) - f(x)$ is balanced for all nonzero a (n has to be even).

Quadratic bent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is bent if $x \mapsto f(x+a) - f(x)$ is balanced for all nonzero a (n has to be even).
- it is quadratic bent if the alternating matrix associated with $f(x+y) - f(x) - f(y)$ is nonsingular.

Quadratic bent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is bent if $x \mapsto f(x+a) - f(x)$ is balanced for all nonzero a (n has to be even).
- it is quadratic bent if the alternating matrix associated with $f(x+y) - f(x) - f(y)$ is nonsingular.
- all quadratic bent functions are (extended affine) equivalent to $f(x_1, \cdots, x_{2m}) = x_1x_2 + x_3x_4 + \cdots + x_{2m-1}x_{2m}$.

$$\begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

Quadratic bent-Negabent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is quadratic negabent if the associated alternating matrix M is such that $M + I$ is nonsingular.

Quadratic bent-Negabent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is quadratic negabent if the associated alternating matrix M is such that $M + I$ is nonsingular.
- How many quadratic bent-negabent functions? (Pott, Parker 2008)

Quadratic bent-Negabent functions

For $f : \mathbb{F}_2^n \to \mathbb{F}_2$,

- it is quadratic negabent if the associated alternating matrix M is such that $M + I$ is nonsingular.
- How many quadratic bent-negabent functions? (Pott, Parker 2008)
- The number of bent-negabent quadratic forms on $\mathbb{F}_2^{2m}$ is

$$\frac{1}{2^m}\sum_{i=0}^{m}(-1)^i\, 2^{i(i-1)} \begin{bmatrix} m \\ i \end{bmatrix}_4 \prod_{k=1}^{m-i}(2^{2k-1}-1)^2.$$

(Pott, Schmidt, Z 2016)

Quadratic bent-Negabent functions

Let X_j stand for the $n \times n$ alternating matrices of rank j over $\mathbb{F}_q$ and $X = \bigcup X_j = \mathbb{F}_q^{n \times n}$.

Quadratic bent-Negabent functions

Let X_j stand for the $n \times n$ alternating matrices of rank j over $\mathbb{F}_q$ and $X = \bigcup X_j = \mathbb{F}_q^{n\times n}$.

- f is bent-negabent if and only if M and $M + I + J$ are both nonsingular (Pott, Parker 2008).

Quadratic bent-Negabent functions

Let X_j stand for the $n \times n$ alternating matrices of rank j over $\mathbb{F}_q$ and $X = \bigcup X_j = \mathbb{F}_q^{n \times n}$.

- f is bent-negabent if and only if M and $M + I + J$ are both nonsingular (Pott, Parker 2008).
- M and $M + I + J$ are both alternating.

Quadratic bent-Negabent functions

Let X_j stand for the $n \times n$ alternating matrices of rank j over $\mathbb{F}_q$ and $X = \bigcup X_j = \mathbb{F}_q^{n\times n}$.

- f is bent-negabent if and only if M and $M + I + J$ are both nonsingular (Pott, Parker 2008).
- M and $M + I + J$ are both alternating.
- We count $N_X(r, s, k) = \left|\{(A, B) \in X_r \times X_s : A + B \in X_k\}\right|$.

Quadratic bent-Negabent functions

Let X_j stand for the $n \times n$ alternating matrices of rank j over $\mathbb{F}_q$ and $X = \bigcup X_j = \mathbb{F}_q^{n\times n}$.

- f is bent-negabent if and only if M and $M + I + J$ are both nonsingular (Pott, Parker 2008).
- M and $M + I + J$ are both alternating.
- We count $N_X(r, s, k) = \left|\{(A, B) \in X_r \times X_s : A + B \in X_k\}\right|$.
- # quadratic bent-negabent functions $= \frac{N_X(n,n,n)}{|X_n|}$.

Quadratic bent-Negabent functions

- $$\begin{aligned} N_X(r,s,k) &= \left|\{(A,B) \in X_r \times X_s :\ A+B \in X_k\}\right| \\ &= \frac{1}{|X|} \sum_{\phi \in \widehat{X}} \sum_{A \in X_r} \phi(A) \sum_{B \in X_s} \phi(B) \sum_{C \in X_k} \phi(C). \end{aligned}$$

Quadratic bent-Negabent functions

- $$\begin{aligned} N_X(r,s,k) &= \left|\{(A,B)\in X_r\times X_s :\ A+B\in X_k\}\right| \\ &= \frac{1}{|X|}\sum_{\phi\in\widehat{X}}\sum_{A\in X_r}\phi(A)\sum_{B\in X_s}\phi(B)\sum_{C\in X_k}\phi(C). \end{aligned}$$

- All X_0, $X_1, \cdots, X_n$ form a partition of $\mathbb{F}_q^{n\times n}$ and it is a translation scheme.

Quadratic bent-Negabent functions

- $$\begin{aligned} N_X(r,s,k) &= \left|\{(A,B)\in X_r\times X_s:\ A+B\in X_k\}\right| \\ &= \frac{1}{|X|}\sum_{\phi\in\widehat{X}}\sum_{A\in X_r}\phi(A)\sum_{B\in X_s}\phi(B)\sum_{C\in X_k}\phi(C). \end{aligned}$$

- All X_0, $X_1, \cdots, X_n$ form a partition of $\mathbb{F}_q^{n\times n}$ and it is a translation scheme.

- $$N_X(r,s,k) = \frac{1}{|X|}\sum_{i=0}^{m}|\widehat{X}_i|\ P_r(i)P_s(i)P_k(i).$$

Quadratic bent-Negabent functions

- $$\begin{aligned} N_X(r,s,k) &= \left|\{(A,B)\in X_r\times X_s:\ A+B\in X_k\}\right| \\ &= \frac{1}{|X|}\sum_{\phi\in\widehat{X}}\sum_{A\in X_r}\phi(A)\sum_{B\in X_s}\phi(B)\sum_{C\in X_k}\phi(C). \end{aligned}$$
- All X_0, $X_1,\cdots,X_n$ form a partition of $\mathbb{F}_q^{n\times n}$ and it is a translation scheme.
- $$N_X(r,s,k)=\frac{1}{|X|}\sum_{i=0}^{m}|\widehat{X}_i|\ P_r(i)P_s(i)P_k(i).$$
- The multiplicities $\widehat{X}_i$ and the eigenvalues $P_r(i)$ are known.

Vectorial quadratic bent functions

Vectorial quadratic bent functions

- bent-negabent: M, $I + J$, $M + I + J$ are nonsingular.

Vectorial quadratic bent functions

- bent-negabent: M, $I+J$, $M+I+J$ are nonsingular.
- $\{0, M, I+J, M+I+J\}$ is an $\mathbb{F}_2$-subspace of dimension 2 in $\mathbb{F}_2^{n\times n}$.

Vectorial quadratic bent functions

- bent-negabent: M, $I+J$, $M+I+J$ are nonsingular.
- $\{0, M, I+J, M+I+J\}$ is an $\mathbb{F}_2$-subspace of dimension 2 in $\mathbb{F}_2^{n\times n}$.
- Can we have larger subspaces $U \subseteq X$ such that each $A \in U \setminus \{0\}$ is nonsingular?

Vectorial quadratic bent functions

- bent-negabent: M, $I + J$, $M + I + J$ are nonsingular.
- $\{0, M, I + J, M + I + J\}$ is an $\mathbb{F}_2$-subspace of dimension 2 in $\mathbb{F}_2^{n \times n}$.
- Can we have larger subspaces $U \subseteq X$ such that each $A \in U \setminus \{0\}$ is nonsingular?
- Yes, we can get it from vectorial quadratic bent functions.

Vectorial quadratic bent functions

- bent-negabent: M, $I + J$, $M + I + J$ are nonsingular.
- $\{0, M, I + J, M + I + J\}$ is an $\mathbb{F}_2$-subspace of dimension 2 in $\mathbb{F}_2^{n \times n}$.
- Can we have larger subspaces $U \subseteq X$ such that each $A \in U \setminus \{0\}$ is nonsingular?
- Yes, we can get it from vectorial quadratic bent functions.
- A $(2m, k)$-vectorial bent function is a function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k$ such that

$$\#\{(x, y) : F(x + a, y + b) - F(x, y) = c\} = 2^{2m-k}$$

for all c and $(a, b) \neq (0, 0)$.

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.
- $k = 2$: total number is known. Inequivalent ones?

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.
- $k = 2$: total number is known. Inequivalent ones?
- It is well known $k \leq m$.

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.
- $k = 2$: total number is known. Inequivalent ones?
- It is well known $k \leq m$.
- $k = m$: rank metric codes with extreme property ($d = 2m$ and $\#\mathcal{C}$ is maximum).

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.
- $k = 2$: total number is known. Inequivalent ones?
- It is well known $k \leq m$.
- $k = m$: rank metric codes with extreme property ($d = 2m$ and $\#\mathcal{C}$ is maximum). How many inequivalent ones?

Vectorial quadratic bent functions

- Vectorial quadratic bent function $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^k \Leftrightarrow$ k-subspaces $U \subseteq X$ satisfying that each $A \in U \setminus \{0\}$ is nonsingular.
- $k = 1$ only one quadratic bent function up to equivalence.
- $k = 2$: total number is known. Inequivalent ones?
- It is well known $k \leq m$.
- $k = m$: rank metric codes with extreme property ($d = 2m$ and $\#\mathcal{C}$ is maximum). How many inequivalent ones?
- EA-Equivalence: $G = L \circ F \circ L' + \tilde{L}$, where L and L' are affine permutations and $\tilde{L}$ is affine.

Vectorial quadratic bent functions for $k = m$

We can show that there are many inequivalent k-vectorial quadratic bent functions by using semifields.

Vectorial quadratic bent functions for $k = m$

We can show that there are many inequivalent k-vectorial quadratic bent functions by using semifields.

- Take $F(x, y) = x * y$ where $*$ stands for the multiplication of a semifield of order 2^m.

Vectorial quadratic bent functions for $k = m$

We can show that there are many inequivalent k-vectorial quadratic bent functions by using semifields.

- Take $F(x, y) = x * y$ where $*$ stands for the multiplication of a semifield of order 2^m.
- Hence $x * y = \sum_{0 \le i \le j < n} c_{ij} x^{2^i} y^{2^j}$ for some $c_{ij} \in \mathbb{F}_{2^m}$.

Vectorial quadratic bent functions for $k = m$

We can show that there are many inequivalent k-vectorial quadratic bent functions by using semifields.

- Take $F(x, y) = x * y$ where $*$ stands for the multiplication of a semifield of order 2^m.
- Hence $x * y = \sum_{0 \le i \le j < n} c_{ij} x^{2^i} y^{2^j}$ for some $c_{ij} \in \mathbb{F}_{2^m}$.
- It is bent:

$$F(x + a, b + y) - F(x, y) - F(a, b) = x * b + a * y.$$

Vectorial quadratic bent functions for $k = m$

We can show that there are many inequivalent k-vectorial quadratic bent functions by using semifields.

- Take $F(x, y) = x * y$ where $*$ stands for the multiplication of a semifield of order 2^m.
- Hence $x * y = \sum_{0 \le i \le j < n} c_{ij} x^{2^i} y^{2^j}$ for some $c_{ij} \in \mathbb{F}_{2^m}$.
- It is bent:

$$F(x + a, b + y) - F(x, y) - F(a, b) = x * b + a * y.$$

- There are exponentially many inequivalent (isotopic) semifields, and we want to use them to derive inequivalent (EA) vectorial bent functions.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$. Then

$$G : (x, y) \mapsto M \circ F(L_0(x) + L_1(y), L_2(x) + L_3(y))$$

is again $(2m, m)$-vectorial bent and F and G are equivalent.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$. Then

$$G : (x, y) \mapsto M \circ F(L_0(x) + L_1(y), L_2(x) + L_3(y))$$

  is again $(2m, m)$-vectorial bent and F and G are equivalent.

- Assume that $F(x, y) = x * y$ and $G(x, y) = x \star y$ are equivalent.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$. Then

$$G : (x, y) \mapsto M \circ F(L_0(x) + L_1(y), L_2(x) + L_3(y))$$

is again $(2m, m)$-vectorial bent and F and G are equivalent.

- Assume that $F(x, y) = x * y$ and $G(x, y) = x \star y$ are equivalent.

- $F(L_0(x) + L_1(y), L_2(x) + L_3(y)) =$ $L_0(x) * L_2(x) + L_1(y) * L_3(y) + L_0(x) * L_3(y) + L_1(y) * L_2(x)$.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$. Then

$$G : (x, y) \mapsto M \circ F(L_0(x) + L_1(y), L_2(x) + L_3(y))$$

  is again $(2m, m)$-vectorial bent and F and G are equivalent.

- Assume that $F(x, y) = x * y$ and $G(x, y) = x \star y$ are equivalent.

- $F(L_0(x) + L_1(y), L_2(x) + L_3(y)) = L_0(x) * L_2(x) + L_1(y) * L_3(y) + L_0(x) * L_3(y) + L_1(y) * L_2(x)$.

- $M(L_0(x) * L_2(x))$ and $M(L_1(y) * L_3(y))$ must be zero.

- Let L_i be additive map over $\mathbb{F}_2^m$ for $i = 0, 1, 2, 3$. The map $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation on $\mathbb{F}_2^{2m}$, M is an additive permutation on $\mathbb{F}_2^m$. Then

$$G : (x, y) \mapsto M \circ F(L_0(x) + L_1(y), L_2(x) + L_3(y))$$

  is again $(2m, m)$-vectorial bent and F and G are equivalent.

- Assume that $F(x, y) = x * y$ and $G(x, y) = x \star y$ are equivalent.

- $F(L_0(x) + L_1(y), L_2(x) + L_3(y)) =$
  $L_0(x) * L_2(x) + L_1(y) * L_3(y) + L_0(x) * L_3(y) + L_1(y) * L_2(x)$.

- $M(L_0(x) * L_2(x))$ and $M(L_1(y) * L_3(y))$ must be zero.

- One of L_0 and L_2 (resp. L_1 and L_3) must be the zero map.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.
- $x \star y = M(L_0(x) * L_3(y))$ or $M(L_1(y) * L_2(x))$.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.
- $x \star y = M(L_0(x) * L_3(y))$ or $M(L_1(y) * L_2(x))$.
- $(\mathbb{F}_2^m, +, \star)$ is isotopic to $(\mathbb{F}_2^m, +, *)$ or $(\mathbb{F}_2^m, +, \hat{*})$, where $x \hat{*} y = y * x$.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.
- $x \star y = M(L_0(x) * L_3(y))$ or $M(L_1(y) * L_2(x))$.
- $(\mathbb{F}_2^m, +, \star)$ is isotopic to $(\mathbb{F}_2^m, +, *)$ or $(\mathbb{F}_2^m, +, \hat{*})$, where $x \hat{*} y = y * x$.
- Exactly the same as the isometry defined on $\mathbb{F}_2^{m\times m}$.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.
- $x \star y = M(L_0(x) * L_3(y))$ or $M(L_1(y) * L_2(x))$.
- $(\mathbb{F}_2^m, +, \star)$ is isotopic to $(\mathbb{F}_2^m, +, *)$ or $(\mathbb{F}_2^m, +, \hat{*})$, where $x \hat{*} y = y * x$.
- Exactly the same as the isometry defined on $\mathbb{F}_2^{m \times m}$.
- Using Kantor's commutative semifields, we get the same number of inequivalent $(2m, m)$-vectorial bent functions.

- $(x, y) \mapsto (L_0(x) + L_1(y), L_2(x) + L_3(y))$ is a permutation.
- $G(x, y) = M \circ F(L_0(x), L_3(y))$ or $M \circ F(L_1(y), L_2(x))$.
- $x \star y = M(L_0(x) * L_3(y))$ or $M(L_1(y) * L_2(x))$.
- $(\mathbb{F}_2^m, +, \star)$ is isotopic to $(\mathbb{F}_2^m, +, *)$ or $(\mathbb{F}_2^m, +, \hat{*})$, where $x \hat{*} y = y * x$.
- Exactly the same as the isometry defined on $\mathbb{F}_2^{m \times m}$.
- Using Kantor's commutative semifields, we get the same number of inequivalent $(2m, m)$-vectorial bent functions.
- Kantor's construction does not work for $m = 2^\ell$.

Exceptional scattered polynomials

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l.

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

We restrict ourselves to MRD codes in $\mathbb{F}_q^{n\times n}$:

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

We restrict ourselves to MRD codes in $\mathbb{F}_q^{n\times n}$:

- For (generalized) Gabidulin codes
  $\mathcal{G}_s = \{a_0X + a_1X^{q^s} + \dots a_{k-1}X^{q^{s(k-1)}} : a_0, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$,
  $$N_r(\mathcal{G}_s) = \{g : g \circ f \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n},$$
  $$N_m(\mathcal{G}_s) = \{g : f \circ g \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n}.$$

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

We restrict ourselves to MRD codes in $\mathbb{F}_q^{n\times n}$:

- For (generalized) Gabidulin codes
  $\mathcal{G}_s = \{a_0 X + a_1 X^{q^s} + \dots a_{k-1} X^{q^{s(k-1)}} : a_0, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$,
  $$N_r(\mathcal{G}_s) = \{g : g \circ f \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n},$$
  $$N_m(\mathcal{G}_s) = \{g : f \circ g \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n}.$$
- MRD codes with $N_r = N_m = \mathbb{F}_{q^n}$ are $\mathcal{G}_s$.

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

We restrict ourselves to MRD codes in $\mathbb{F}_q^{n\times n}$:

- For (generalized) Gabidulin codes $\mathcal{G}_s = \{a_0 X + a_1 X^{q^s} + \dots a_{k-1} X^{q^{s(k-1)}} : a_0, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$,
$$N_r(\mathcal{G}_s) = \{g : g \circ f \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n},$$
$$N_m(\mathcal{G}_s) = \{g : f \circ g \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n}.$$
- MRD codes with $N_r = N_m = \mathbb{F}_{q^n}$ are $\mathcal{G}_s$.
- For $N_r = \mathbb{F}_{q^n}$, there are at least:

Classify MRD codes

For semifields, we have classification results with certain assumptions on N_m, N_r and N_l. Can we classify MRD codes?

We restrict ourselves to MRD codes in $\mathbb{F}_q^{n\times n}$:

- For (generalized) Gabidulin codes $\mathcal{G}_s = \{a_0 X + a_1 X^{q^s} + \dots a_{k-1} X^{q^{s(k-1)}} : a_0, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$,
$$N_r(\mathcal{G}_s) = \{g : g \circ f \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n},$$
$$N_m(\mathcal{G}_s) = \{g : f \circ g \in \mathcal{G}_s \text{ for all } f \in \mathcal{G}_s\} \cong \mathbb{F}_{q^n}.$$
- MRD codes with $N_r = N_m = \mathbb{F}_{q^n}$ are $\mathcal{G}_s$.
- For $N_r = \mathbb{F}_{q^n}$, there are at least:
$\mathcal{H}_{k,s}(\eta, h) = \{a_0 X + \dots + a_{k-1} X^{q^{s(k-1)}} + \eta a_0 X^{q^{sk}} : a_0, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$
where $\eta \in \mathbb{F}_{q^n}$ is such that $N_{q^{sn}/q^s}(\eta) \neq (-1)^{nk}$.

Classify MRD codes

We restrict ourselves to MRD codes of minimum distance $n-1$ in $\mathbb{F}_q^{n\times n}$ with $N_r = \mathbb{F}_{q^n}$.

$$\mathcal{F} = \{aX + bf(X) : a, b \in \mathbb{F}_{q^n}\}.$$

Classify MRD codes

We restrict ourselves to MRD codes of minimum distance $n-1$ in $\mathbb{F}_q^{n\times n}$ with $N_r = \mathbb{F}_{q^n}$.

$$\mathcal{F} = \{aX + bf(X) : a, b \in \mathbb{F}_{q^n}\}.$$

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0X + a_1X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' bX^{q^s} + bX^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

Classify MRD codes

We restrict ourselves to MRD codes of minimum distance $n-1$ in $\mathbb{F}_q^{n\times n}$ with $N_r = \mathbb{F}_{q^n}$.

$$\mathcal{F} = \{aX + bf(X) : a, b \in \mathbb{F}_{q^n}\}.$$

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0 X + a_1 X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' b X^{q^s} + b X^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

- $\mathcal{F}$ is MRD if and only if $\ker(f) \leq q$ and

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

Classify MRD codes

We restrict ourselves to MRD codes of minimum distance $n-1$ in $\mathbb{F}_q^{n\times n}$ with $N_r = \mathbb{F}_{q^n}$.

$$\mathcal{F} = \{aX + bf(X) : a, b \in \mathbb{F}_{q^n}\}.$$

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0X + a_1X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' bX^{q^s} + bX^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

- $\mathcal{F}$ is MRD if and only if $\ker(f) \leq q$ and

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

- A polynomial f satisfying the second condition is called scattered polynomial.

Classify scattered polynomials

- Maximum scattered linear set (MSLS) over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\},$$

$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\}.$$

Classify scattered polynomials

- Maximum scattered linear set (MSLS) over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\},$$
$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\}.$$

- Hence it is equivalent to

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

Classify scattered polynomials

- Maximum scattered linear set (MSLS) over $\mathrm{PG}(1,q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\},$$
$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\}.$$

- Hence it is equivalent to

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

- The equivalence of MSLS is more complicated.

Classify scattered polynomials

- Maximum scattered linear set (MSLS) over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\},$$

$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\}.$$

- Hence it is equivalent to

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

- The equivalence of MSLS is more complicated.
- By using finite geometry argument, $n = 4$ is completely classified [Csajbók, Zanella]

Classify scattered polynomials

- Maximum scattered linear set (MSLS) over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\},$$

$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\}.$$

- Hence it is equivalent to

$$\frac{f(x)}{x} = \frac{f(y)}{y} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

- The equivalence of MSLS is more complicated.
- By using finite geometry argument, $n = 4$ is completely classified [Csajbók, Zanella]
- $n = 5$ is almost done [Csajbók, Marino, Polverino].

Classify scattered polynomials

- A typical problem for APN functions and planar functions is to classify the “exceptional” ones.

Classify scattered polynomials

- A typical problem for APN functions and planar functions is to classify the "exceptional" ones.
- A polynomial $f \in \mathbb{F}_{2^n}[X]$ is APN (planar etc.) over $\mathbb{F}_{2^{mn}}$ for infinitely many m.

Classify scattered polynomials

- A typical problem for APN functions and planar functions is to classify the "exceptional" ones.
- A polynomial $f \in \mathbb{F}_{2^n}[X]$ is APN (planar etc.) over $\mathbb{F}_{2^{mn}}$ for infinitely many m.
- Exceptional APN power maps are X^{2^i+1} and $X^{4^i-2^i+1}$ (McGuire, Hernando 2011).

Classify scattered polynomials

- A typical problem for APN functions and planar functions is to classify the "exceptional" ones.
- A polynomial $f \in \mathbb{F}_{2^n}[X]$ is APN (planar etc.) over $\mathbb{F}_{2^{mn}}$ for infinitely many m.
- Exceptional APN power maps are X^{2^i+1} and $X^{4^i-2^i+1}$ (McGuire, Hernando 2011).
- Exceptional planar monomial, planar polynomials, APN polynomials, monomial hyperovals (Aubry, Caullery, Janwa, Jedlicka, Hernando, McGuire, Leducq, Rodier, Schmidt, Wilson, Z, Zieve)

Classify scattered polynomials

- We can also classify scattered polynomials.

Classify scattered polynomials

- We can also classify scattered polynomials.
- The unique known family:

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0 X + a_1 X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' b X^{q^s} + b X^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

Classify scattered polynomials

- We can also classify scattered polynomials.
- The unique known family:

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0 X + a_1 X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' b X^{q^s} + b X^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

- A slight modification:

$$\frac{f(x)}{x^{q^s}} = \frac{f(y)}{y^{q^s}} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

Classify scattered polynomials

- We can also classify scattered polynomials.
- The unique known family:

$$\begin{aligned}\mathcal{H}_{2,s}(\eta, h) &= \{a_0X + a_1X^{q^s} + \eta a_0 X^{q^{2s}} : a_0, a_1 \in \mathbb{F}_{q^n}\} \\ &= \{aX + \eta' bX^{q^s} + bX^{q^{(n-1)s}} : a, b \in \mathbb{F}_{q^n}\}\end{aligned}$$

- A slight modification:

$$\frac{f(x)}{x^{q^s}} = \frac{f(y)}{y^{q^s}} \Leftrightarrow \frac{y}{x} \in \mathbb{F}_q.$$

- We call a polynomial satisfying the above condition a scattered polynomial of index s.

Classify scattered polynomials

We (Bartoli, Z) can prove

Classify scattered polynomials

We (Bartoli, Z) can prove

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.

Classify scattered polynomials

We (Bartoli, Z) can prove

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.
- The only exceptional scattered monic polynomials f of index 1 over $\mathbb{F}_{q^n}$ are X and $bX + X^{q^2}$ where $b \in \mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(b) \neq 1$. When $q = 2$, $f(X)$ must be X.

Sketch of the proof

- The curve $\mathcal{F}$:

$$F(X,Y) = \frac{f(X)Y^{q^s} - f(Y)X^{q^s}}{X^qY - XY^q} = 0$$

in $\mathrm{PG}(2,q^n)$ contains no affine point (x,y) such that $\frac{y}{x} \notin \mathbb{F}_q$.

Sketch of the proof

- The curve $\mathcal{F}$:

$$F(X,Y) = \frac{f(X)Y^{q^s} - f(Y)X^{q^s}}{X^qY - XY^q} = 0$$

in $\mathrm{PG}(2, q^n)$ contains no affine point (x, y) such that $\frac{y}{x} \notin \mathbb{F}_q$.

- Use Hasse-Weil theorem to show there exist other points.

Sketch of the proof

- The curve $\mathcal{F}$:

$$F(X,Y) = \frac{f(X)Y^{q^s} - f(Y)X^{q^s}}{X^qY - XY^q} = 0$$

in $\mathrm{PG}(2, q^n)$ contains no affine point (x, y) such that $\frac{y}{x} \notin \mathbb{F}_q$.

- Use Hasse-Weil theorem to show there exist other points.

- We have to show that $\mathcal{F}$ contains absolutely irreducible component over $\mathbb{F}_{q^n}$.

Sketch of the proof

- Assume that $F = AB$. If $\mathcal{F}$ has no absolutely irreducible component, we have a lower bound on $(\deg A)(\deg B)$.

Sketch of the proof

- Assume that $F = AB$. If $\mathcal{F}$ has no absolutely irreducible component, we have a lower bound on $(\deg A)(\deg B)$.
- By analyzing $I(P, \mathcal{A} \cap \mathcal{B})$, we have an upper bound on $\sum_P I(P, \mathcal{A} \cap \mathcal{B})$.

Sketch of the proof

- Assume that $F = AB$. If $\mathcal{F}$ has no absolutely irreducible component, we have a lower bound on $(\deg A)(\deg B)$.
- By analyzing $I(P, \mathcal{A} \cap \mathcal{B})$, we have an upper bound on $\sum_P I(P, \mathcal{A} \cap \mathcal{B})$.
- Use Bézout's Theorem $\sum_P I(P, \mathcal{A} \cap \mathcal{B}) = (\deg A)(\deg B)$ to get contradiction.

Sketch of the proof

- Assume that $F = AB$. If $\mathcal{F}$ has no absolutely irreducible component, we have a lower bound on $(\deg A)(\deg B)$.
- By analyzing $I(P, \mathcal{A} \cap \mathcal{B})$, we have an upper bound on $\sum_P I(P, \mathcal{A} \cap \mathcal{B})$.
- Use Bézout's Theorem $\sum_P I(P, \mathcal{A} \cap \mathcal{B}) = (\deg A)(\deg B)$ to get contradiction.
- The most involved part is to estimate $I(P, A \cap B)$ where P is a singular point.

Sketch of the proof

- Assume that $F = AB$. If $\mathcal{F}$ has no absolutely irreducible component, we have a lower bound on $(\deg A)(\deg B)$.
- By analyzing $I(P, \mathcal{A} \cap \mathcal{B})$, we have an upper bound on $\sum_P I(P, \mathcal{A} \cap \mathcal{B})$.
- Use Bézout's Theorem $\sum_P I(P, \mathcal{A} \cap \mathcal{B}) = (\deg A)(\deg B)$ to get contradiction.
- The most involved part is to estimate $I(P, A \cap B)$ where P is a singular point.
- When $s = 1$, the old approach does not work. We have to investigate the "branches" of $\mathcal{F}$ centered at P.

Sketch of the proof

- A branch representation is $(x(t), y(t), z(t)) \in \mathrm{PG}(2, \mathbb{K}((t)))$, where $\mathbb{K}((t))$ stands for the field of rational functions of the formal power series. $(x(0), y(0), z(0))$ is its center.

Sketch of the proof

- A branch representation is $(x(t), y(t), z(t)) \in \mathrm{PG}(2, \mathbb{K}((t)))$, where $\mathbb{K}((t))$ stands for the field of rational functions of the formal power series. $(x(0), y(0), z(0))$ is its center.
- A branch is an equivalence class of different representations.

Sketch of the proof

- A branch representation is $(x(t), y(t), z(t)) \in \mathrm{PG}(2, \mathbb{K}((t)))$, where $\mathbb{K}((t))$ stands for the field of rational functions of the formal power series. $(x(0), y(0), z(0))$ is its center.
- A branch is an equivalence class of different representations.
- A branch of a plane curve is a branch whose representation are zero of this curve.

Sketch of the proof

- A branch representation is $(x(t), y(t), z(t)) \in \mathrm{PG}(2, \mathbb{K}((t)))$, where $\mathbb{K}((t))$ stands for the field of rational functions of the formal power series. $(x(0), y(0), z(0))$ is its center.
- A branch is an equivalence class of different representations.
- A branch of a plane curve is a branch whose representation are zero of this curve.
- $I(P, \mathcal{G} \cap \mathcal{F}) = \sum_{\gamma} I(P, \mathcal{G} \cap \gamma)$ where γ runs over all branches of $\mathcal{F}$ centered at P.

Sketch of the proof

- A branch representation is $(x(t), y(t), z(t)) \in \mathrm{PG}(2, \mathbb{K}((t)))$, where $\mathbb{K}((t))$ stands for the field of rational functions of the formal power series. $(x(0), y(0), z(0))$ is its center.
- A branch is an equivalence class of different representations.
- A branch of a plane curve is a branch whose representation are zero of this curve.
- $I(P, \mathcal{G} \cap \mathcal{F}) = \sum_{\gamma} I(P, \mathcal{G} \cap \gamma)$ where γ runs over all branches of $\mathcal{F}$ centered at P.
- Use local quadratic transform $\mathcal{F} \mapsto \mathcal{F}'$, there exists a bijection between the branches of $\mathcal{F}$ centered at the origin and the branches of $\mathcal{F}'$ centered at an affine point on $X = 0$.

Classify scattered polynomials

For index $s = 0$:

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.

Classify scattered polynomials

For index $s = 0$:

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.
- For $q = 2, 3$, we can prove the exceptional scattered monic polynomial of index 0 have at most 2 or 3 consecutive terms. But we cannot give a complete classification.

Classify scattered polynomials

For index $s = 0$:

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.
- For $q = 2, 3$, we can prove the exceptional scattered monic polynomial of index 0 have at most 2 or 3 consecutive terms. But we cannot give a complete classification.

For index $s \geq 1$:

- The only exceptional scattered monic polynomials f of index 1 over $\mathbb{F}_{q^n}$ are X and $bX + X^{q^2}$ where $b \in \mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(b) \neq 1$. When $q = 2$, $f(X)$ must be X.

Classify scattered polynomials

For index $s = 0$:

- For $q \geq 4$, X^{q^k} is the unique exceptional scattered monic polynomial of index 0.
- For $q = 2, 3$, we can prove the exceptional scattered monic polynomial of index 0 have at most 2 or 3 consecutive terms. But we cannot give a complete classification.

For index $s \geq 1$:

- The only exceptional scattered monic polynomials f of index 1 over $\mathbb{F}_{q^n}$ are X and $bX + X^{q^2}$ where $b \in \mathbb{F}_{q^n}$ satisfying $\mathrm{Norm}_{q^n/q}(b) \neq 1$. When $q = 2$, $f(X)$ must be X.
- For index $s > 1$, our approach cannot offer a complete classification.

Thanks for your attention!

Rank Metric Codes and related Structures

Yue Zhou

July 5, 2017

The 2nd International Workshop on Boolean Functions and their Applications (BFA)