A new family of maximum rank distance codes

or: Maximum rank distance codes and finite semifields

John Sheekey

Universiteit Gent, Belgium

Alcoma, March 2015

Rank metric codes

A rank metric code is a set $\mathcal{C} \subset M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ with the distance function

$$d(X, Y) := \mathrm{rank}(X - Y).$$

- Mostly we will be concerned with $\mathbb{F} = \mathbb{F}_q$.
- A code is $\mathbb{F}_{q_0}$-linear if it is a subspace over $\mathbb{F}_{q_0} \leq \mathbb{F}_q$.
- Goals:
  - Illustrate the link with semifields.
  - Construct a new family of linear MRD-codes for all parameters.

Rank metric codes

A rank metric code is a set $\mathcal{C} \subset M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ with the distance function

$$d(X, Y) := \mathrm{rank}(X - Y).$$

- Mostly we will be concerned with $\mathbb{F} = \mathbb{F}_q$.
- A code is $\mathbb{F}_{q_0}$-linear if it is a subspace over $\mathbb{F}_{q_0} \leq \mathbb{F}_q$.
- Goals:
  - Illustrate the link with semifields.
  - Construct a new family of linear MRD-codes for all parameters.

Rank metric codes

A rank metric code is a set $\mathcal{C} \subset M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ with the distance function

$$d(X, Y) := \mathrm{rank}(X - Y).$$

- Mostly we will be concerned with $\mathbb{F} = \mathbb{F}_q$.
- A code is $\mathbb{F}_{q_0}$-linear if it is a subspace over $\mathbb{F}_{q_0} \leq \mathbb{F}_q$.
- Goals:
  - Illustrate the link with semifields.
  - Construct a new family of linear MRD-codes for all parameters.

Rank metric codes

A rank metric code is a set $\mathcal{C} \subset M_n(\mathbb{F})$ of $n \times n$ matrices over a field $\mathbb{F}$ with the distance function

$$d(X, Y) := \mathrm{rank}(X - Y).$$

- Mostly we will be concerned with $\mathbb{F} = \mathbb{F}_q$.
- A code is $\mathbb{F}_{q_0}$-linear if it is a subspace over $\mathbb{F}_{q_0} \leq \mathbb{F}_q$.
- Goals:
  - Illustrate the link with semifields.
  - Construct a new family of linear MRD-codes for all parameters.

Rank metric codes

Introduced and constructed by Delsarte (1978), who studied them via association schemes.

Gabidulin (1985) provided more constructions and decoding algorithms.

Have seen renewed interest in recent years, in part due to their connections to subspace codes and q-designs.

Rank metric codes

Introduced and constructed by Delsarte (1978), who studied them via association schemes.

Gabidulin (1985) provided more constructions and decoding algorithms.

Have seen renewed interest in recent years, in part due to their connections to subspace codes and q-designs.

Rank metric codes

Introduced and constructed by Delsarte (1978), who studied them via association schemes.

Gabidulin (1985) provided more constructions and decoding algorithms.

Have seen renewed interest in recent years, in part due to their connections to subspace codes and q-designs.

Equivalence of rank metric codes

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be equivalent if there exist invertible matrices A, B, a matrix D, and an automorphism ρ of $\mathbb{F}$ such that

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

or

$$\mathcal{C}_2 = \{A(X^T)^\rho B + D : X \in \mathcal{C}_1\}$$

Clearly operations of this form preserve rank distance.

Can be viewed as codes in $(\mathbb{F}_{q^n})^n$.

Note: two notions of equivalence... one restricts A to a certain subgroup of $\mathrm{GL}(n, \mathbb{F})$.

Equivalence of rank metric codes

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be equivalent if there exist invertible matrices A, B, a matrix D, and an automorphism ρ of $\mathbb{F}$ such that

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

or

$$\mathcal{C}_2 = \{A(X^T)^\rho B + D : X \in \mathcal{C}_1\}$$

Clearly operations of this form preserve rank distance.

Can be viewed as codes in $(\mathbb{F}_{q^n})^n$.

Note: two notions of equivalence... one restricts A to a certain subgroup of $\mathrm{GL}(n, \mathbb{F})$.

Equivalence of rank metric codes

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be equivalent if there exist invertible matrices A, B, a matrix D, and an automorphism ρ of $\mathbb{F}$ such that

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

or

$$\mathcal{C}_2 = \{A(X^T)^\rho B + D : X \in \mathcal{C}_1\}$$

Clearly operations of this form preserve rank distance.

Can be viewed as codes in $(\mathbb{F}_{q^n})^n$.

Note: two notions of equivalence... one restricts A to a certain subgroup of $\mathrm{GL}(n, \mathbb{F})$.

Equivalence of rank metric codes

Two codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are said to be equivalent if there exist invertible matrices A, B, a matrix D, and an automorphism ρ of $\mathbb{F}$ such that

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

or

$$\mathcal{C}_2 = \{A(X^T)^\rho B + D : X \in \mathcal{C}_1\}$$

Clearly operations of this form preserve rank distance.

Can be viewed as codes in $(\mathbb{F}_{q^n})^n$.

Note: two notions of equivalence... one restricts A to a certain subgroup of $\mathrm{GL}(n, \mathbb{F})$.

Easy upper bound (Singleton-like)

Suppose $\mathcal{C} \subset M_n(\mathbb{F}_q)$ is a rank metric code with minimum distance d. Then $|\mathcal{C}| \leq q^{n(n-d+1)}$.

Over any field, a *linear* rank metric code with minimum distance d can have dimension at most $n(n-d+1)$.

Easy upper bound (Singleton-like)

Suppose $\mathcal{C} \subset M_n(\mathbb{F}_q)$ is a rank metric code with minimum distance d. Then $|\mathcal{C}| \leq q^{n(n-d+1)}$.

Over any field, a *linear* rank metric code with minimum distance d can have dimension at most $n(n-d+1)$.

MRD codes

A code meeting this bound is said to be a Maximum Rank Distance (MRD) code.

If $\mathcal{C}$ is an MRD-code which is linear over $\mathbb{F}_q$ with dimension nk and minimum distance $n-k+1$, we say it has parameters $[n^2, nk, n-k+1]_q$.

Duality: $\mathcal{C}^\perp$ the orthogonal space with respect to e.g. $b(X,Y) := \mathrm{tr}(\mathrm{Tr}(XY^T))$.

Delsarte: $\mathcal{C}$ MRD $\Leftrightarrow$ $\mathcal{C}^\perp$ MRD; parameters $[n^2, n(n-k), k+1]_q$.

Delsarte, and later Gabidulin, constructed examples for all parameters using linearized polynomials.

MRD codes

A code meeting this bound is said to be a Maximum Rank Distance (MRD) code.

If $\mathcal{C}$ is an MRD-code which is linear over $\mathbb{F}_q$ with dimension nk and minimum distance $n-k+1$, we say it has parameters $[n^2, nk, n-k+1]_q$.

Duality: $\mathcal{C}^\perp$ the orthogonal space with respect to e.g. $b(X,Y) := \mathrm{tr}(\mathrm{Tr}(XY^T))$.

Delsarte: $\mathcal{C}$ MRD $\Leftrightarrow$ $\mathcal{C}^\perp$ MRD; parameters $[n^2, n(n-k), k+1]_q$.

Delsarte, and later Gabidulin, constructed examples for all parameters using linearized polynomials.

MRD codes

A code meeting this bound is said to be a Maximum Rank Distance (MRD) code.

If $\mathcal{C}$ is an MRD-code which is linear over $\mathbb{F}_q$ with dimension nk and minimum distance $n-k+1$, we say it has parameters $[n^2, nk, n-k+1]_q$.

Duality: $\mathcal{C}^\perp$ the orthogonal space with respect to e.g. $b(X, Y) := \mathrm{tr}(\mathrm{Tr}(XY^T))$.

Delsarte: $\mathcal{C}$ MRD $\Leftrightarrow$ $\mathcal{C}^\perp$ MRD; parameters $[n^2, n(n-k), k+1]_q$.

Delsarte, and later Gabidulin, constructed examples for all parameters using linearized polynomials.

MRD codes

A code meeting this bound is said to be a Maximum Rank Distance (MRD) code.

If $\mathcal{C}$ is an MRD-code which is linear over $\mathbb{F}_q$ with dimension nk and minimum distance $n-k+1$, we say it has parameters $[n^2, nk, n-k+1]_q$.

Duality: $\mathcal{C}^\perp$ the orthogonal space with respect to e.g. $b(X, Y) := \mathrm{tr}(\mathrm{Tr}(XY^T))$.

Delsarte: $\mathcal{C}$ MRD $\Leftrightarrow$ $\mathcal{C}^\perp$ MRD; parameters $[n^2, n(n-k), k+1]_q$.

Delsarte, and later Gabidulin, constructed examples for all parameters using linearized polynomials.

MRD codes

A code meeting this bound is said to be a Maximum Rank Distance (MRD) code.

If $\mathcal{C}$ is an MRD-code which is linear over $\mathbb{F}_q$ with dimension nk and minimum distance $n-k+1$, we say it has parameters $[n^2, nk, n-k+1]_q$.

Duality: $\mathcal{C}^\perp$ the orthogonal space with respect to e.g. $b(X, Y) := \mathrm{tr}(\mathrm{Tr}(XY^T))$.

Delsarte: $\mathcal{C}$ MRD $\Leftrightarrow \mathcal{C}^\perp$ MRD; parameters $[n^2, n(n-k), k+1]_q$.

Delsarte, and later Gabidulin, constructed examples for all parameters using linearized polynomials.

Linearized polynomials

A linearized polynomial is a polynomial in $\mathbb{F}_{q^n}[x]$ of the form

$$f(x) = f_0 x + f_1 x^q + \cdots + f_{n-1} x^{q^{n-1}}.$$

Each such polynomial is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to itself.

In fact, every $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$ can be uniquely realised as a linearized polynomial of degree at most q^{n-1} (q-degree at most $n-1$).

Linearized polynomials	$\Leftrightarrow$	$M_n(\mathbb{F}_q)$
Composition mod $x^{q^n} - x$	$\Leftrightarrow$	Matrix multiplication

Linearized polynomials

A linearized polynomial is a polynomial in $\mathbb{F}_{q^n}[x]$ of the form

$$f(x) = f_0 x + f_1 x^q + \cdots + f_{n-1} x^{q^{n-1}}.$$

Each such polynomial is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to itself.

In fact, every $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$ can be uniquely realised as a linearized polynomial of degree at most q^{n-1} (q-degree at most $n-1$).

Linearized polynomials	$\Leftrightarrow$	$M_n(\mathbb{F}_q)$
Composition mod $x^{q^n} - x$	$\Leftrightarrow$	Matrix multiplication

Linearized polynomials

A linearized polynomial is a polynomial in $\mathbb{F}_{q^n}[x]$ of the form

$$f(x) = f_0 x + f_1 x^q + \cdots + f_{n-1} x^{q^{n-1}}.$$

Each such polynomial is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to itself.

In fact, every $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$ can be uniquely realised as a linearized polynomial of degree at most q^{n-1} (q-degree at most $n-1$).

Linearized polynomials	$\Leftrightarrow$	$M_n(\mathbb{F}_q)$
Composition mod $x^{q^n} - x$	$\Leftrightarrow$	Matrix multiplication

Linearized polynomials

A linearized polynomial is a polynomial in $\mathbb{F}_{q^n}[x]$ of the form

$$f(x) = f_0 x + f_1 x^q + \cdots + f_{n-1} x^{q^{n-1}}.$$

Each such polynomial is an $\mathbb{F}_q$-linear map from $\mathbb{F}_{q^n}$ to itself.

In fact, every $\mathbb{F}_q$-linear map on $\mathbb{F}_{q^n}$ can be uniquely realised as a linearized polynomial of degree at most q^{n-1} (q-degree at most $n-1$).

Linearized polynomials	$\Leftrightarrow$	$M_n(\mathbb{F}_q)$
Composition mod $x^{q^n} - x$	$\Leftrightarrow$	Matrix multiplication

Gabidulin codes (1985)

The Delsarte/Gabidulin code $\mathcal{G}_k$ is a the set of linearized polynomials of q-degree at most $k-1$, i.e.

$$\mathcal{G}_k := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}.$$

Clearly each element of $\mathcal{G}_k$ has at most q^{k-1} roots, and hence rank at least $n-k+1$.

$\mathcal{G}_k$ has dimension nk over $\mathbb{F}_q$. (In fact, it is linear over $\mathbb{F}_{q^n}$).

Hence $\mathcal{G}_k$ is a linear MRD-code with parameters $[n^2, nk, n-k+1]_q$.

Can replace q with q^m for any m with $(n,m)=1$, and define $\mathcal{G}_{k,m}$ (Gabidulin).

Gabidulin codes (1985)

The Delsarte/Gabidulin code $\mathcal{G}_k$ is a the set of linearized polynomials of q-degree at most $k-1$, i.e.

$$\mathcal{G}_k := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}.$$

Clearly each element of $\mathcal{G}_k$ has at most q^{k-1} roots, and hence rank at least $n-k+1$.

$\mathcal{G}_k$ has dimension nk over $\mathbb{F}_q$. (In fact, it is linear over $\mathbb{F}_{q^n}$).

Hence $\mathcal{G}_k$ is a linear MRD-code with parameters $[n^2, nk, n-k+1]_q$.

Can replace q with q^m for any m with $(n,m)=1$, and define $\mathcal{G}_{k,m}$ (Gabidulin).

Gabidulin codes (1985)

The Delsarte/Gabidulin code $\mathcal{G}_k$ is a the set of linearized polynomials of q-degree at most $k-1$, i.e.

$$\mathcal{G}_k := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}.$$

Clearly each element of $\mathcal{G}_k$ has at most q^{k-1} roots, and hence rank at least $n-k+1$.

$\mathcal{G}_k$ has dimension nk over $\mathbb{F}_q$. (In fact, it is linear over $\mathbb{F}_{q^n}$).

Hence $\mathcal{G}_k$ is a linear MRD-code with parameters $[n^2, nk, n-k+1]_q$.

Can replace q with q^m for any m with $(n, m) = 1$, and define $\mathcal{G}_{k,m}$ (Gabidulin).

Gabidulin codes (1985)

The Delsarte/Gabidulin code $\mathcal{G}_k$ is a the set of linearized polynomials of q-degree at most $k-1$, i.e.

$$\mathcal{G}_k := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}.$$

Clearly each element of $\mathcal{G}_k$ has at most q^{k-1} roots, and hence rank at least $n-k+1$.

$\mathcal{G}_k$ has dimension nk over $\mathbb{F}_q$. (In fact, it is linear over $\mathbb{F}_{q^n}$).

Hence $\mathcal{G}_k$ is a linear MRD-code with parameters $[n^2, nk, n-k+1]_q$.

Can replace q with q^m for any m with $(n,m) = 1$, and define $\mathcal{G}_{k,m}$ (Gabidulin).

Gabidulin codes (1985)

The Delsarte/Gabidulin code $\mathcal{G}_k$ is a the set of linearized polynomials of q-degree at most $k-1$, i.e.

$$\mathcal{G}_k := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} : f_i \in \mathbb{F}_{q^n}\}.$$

Clearly each element of $\mathcal{G}_k$ has at most q^{k-1} roots, and hence rank at least $n-k+1$.

$\mathcal{G}_k$ has dimension nk over $\mathbb{F}_q$. (In fact, it is linear over $\mathbb{F}_{q^n}$).

Hence $\mathcal{G}_k$ is a linear MRD-code with parameters $[n^2, nk, n-k+1]_q$.

Can replace q with q^m for any m with $(n,m)=1$, and define $\mathcal{G}_{k,m}$ (Gabidulin).

Other known examples

The first non-trivial example of a non-linear MRD-code was recently given by Cossidente, Marino and Pavese for the case $n = 3$, $d = 2$ (presented at Irsee 2014).

No others were known (up to equivalence)... except in the case $k \in \{1, n-1\}$ ($d \in \{n, 2\}$)... semifields.

Wassermann (also at Irsee 2014) asked for more examples for $1 < k < n - 1$.

Other known examples

The first non-trivial example of a non-linear MRD-code was recently given by Cossidente, Marino and Pavese for the case $n = 3$, $d = 2$ (presented at Irsee 2014).

No others were known (up to equivalence)... except in the case $k \in \{1, n-1\}$ ($d \in \{n, 2\}$)... semifields.

Wassermann (also at Irsee 2014) asked for more examples for $1 < k < n - 1$.

Other known examples

The first non-trivial example of a non-linear MRD-code was recently given by Cossidente, Marino and Pavese for the case $n = 3$, $d = 2$ (presented at Irsee 2014).

No others were known (up to equivalence)... except in the case $k \in \{1, n-1\}$ ($d \in \{n, 2\}$)... semifields.

Wassermann (also at Irsee 2014) asked for more examples for $1 < k < n-1$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

(Pre)semifields

A (pre)semifield is a division algebra in which multiplication is not necessarily associative (or commutative).

First non-trivial examples were constructed by Dickson (1906).

They correspond to a particular class of projective planes.

If $\mathbb{S}$ is n-dimensional over $\mathbb{F}_q$, we identify the elements of $\mathbb{S}$ with $\mathbb{F}_{q^n}$. We write the product of two elements x and y by $\mathbb{S}(x, y)$.

Every algebra multiplication can be written as

$$\mathbb{S}(x, y) = \sum_{i,j} c_{ij} x^{q^i} y^{q^j}.$$

for some $c_{i,j} \in \mathbb{F}_{q^n}$.

Isotopic if $\mathbb{S}'(x, y)^A = \mathbb{S}(x^B, y^C)$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Denote by R_y the endomorphism of right multiplication by y, i.e. $R_y(x) = \mathbb{S}(x, y)$.

Let $\mathcal{C}(\mathbb{S})$ be the set of all such endomorphisms: semifield spread set.

Then every nonzero element of $\mathcal{C}(\mathbb{S})$ is invertible, i.e. is an $\mathbb{F}_q$-linear $[n^2, n, n]_q$ MRD-code (k=1).

Conversely, every linear $[n^2, n, n]_q$ MRD-code defines a presemifield of order q^n.

This connection is *well-known, but often forgotten*. [Bruck-Bose, Dembowski]

The Gabidulin code $\mathcal{G}_1$ corresponds to the field $\mathbb{F}_{q^n}$.

Semifields and rank metric codes

Two semifields are isotopic if $\mathbb{S}'(x,y)^A = \mathbb{S}(x^B, y^C)$ for invertible A, B, C.

[Maduram]: $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist invertible A, B such that

$$\mathcal{C}(\mathbb{S}') = \{A^{-1}X^{\rho}B \mid X \in \mathcal{C}(\mathbb{S})\}.$$

The Knuth orbit of a semifield is the set of (up to) six semifields obtained via the two operations transpose and dual:

$$\mathcal{C}(\mathbb{S}^t) := \{X^T \mid X \in \mathcal{C}(\mathbb{S})\}.$$

$$\mathcal{C}(\mathbb{S}^d) := \{L_x : y \mapsto \mathbb{S}(x,y) \mid x \in \mathbb{S}\}.$$

Code equivalence $\leftrightarrow$ isotopy + transpose.

Semifields and rank metric codes

Two semifields are isotopic if $\mathbb{S}'(x,y)^A = \mathbb{S}(x^B, y^C)$ for invertible A, B, C.

[Maduram]: $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist invertible A, B such that

$$\mathcal{C}(\mathbb{S}') = \{A^{-1}X^{\rho}B \mid X \in \mathcal{C}(\mathbb{S})\}.$$

The Knuth orbit of a semifield is the set of (up to) six semifields obtained via the two operations transpose and dual:

$$\mathcal{C}(\mathbb{S}^t) := \{X^T \mid X \in \mathcal{C}(\mathbb{S})\}.$$

$$\mathcal{C}(\mathbb{S}^d) := \{L_x : y \mapsto \mathbb{S}(x,y) \mid x \in \mathbb{S}\}.$$

Code equivalence $\leftrightarrow$ isotopy + transpose.

Semifields and rank metric codes

Two semifields are isotopic if $\mathbb{S}'(x,y)^A = \mathbb{S}(x^B, y^C)$ for invertible A, B, C.

[Maduram]: $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist invertible A, B such that

$$\mathcal{C}(\mathbb{S}') = \{A^{-1}X^{\rho}B \mid X \in \mathcal{C}(\mathbb{S})\}.$$

The Knuth orbit of a semifield is the set of (up to) six semifields obtained via the two operations transpose and dual:

$$\mathcal{C}(\mathbb{S}^t) := \{X^T \mid X \in \mathcal{C}(\mathbb{S})\}.$$

$$\mathcal{C}(\mathbb{S}^d) := \{L_x : y \mapsto \mathbb{S}(x,y) \mid x \in \mathbb{S}\}.$$

Code equivalence $\leftrightarrow$ isotopy + transpose.

Semifields and rank metric codes

Two semifields are isotopic if $\mathbb{S}'(x,y)^A = \mathbb{S}(x^B, y^C)$ for invertible A, B, C.

[Maduram]: $\mathbb{S}$ and $\mathbb{S}'$ are isotopic if and only if there exist invertible A, B such that

$$\mathcal{C}(\mathbb{S}') = \{A^{-1}X^{\rho}B \mid X \in \mathcal{C}(\mathbb{S})\}.$$

The Knuth orbit of a semifield is the set of (up to) six semifields obtained via the two operations transpose and dual:

$$\mathcal{C}(\mathbb{S}^t) := \{X^T \mid X \in \mathcal{C}(\mathbb{S})\}.$$

$$\mathcal{C}(\mathbb{S}^d) := \{L_x : y \mapsto \mathbb{S}(x,y) \mid x \in \mathbb{S}\}.$$

Code equivalence $\leftrightarrow$ isotopy + transpose.

Semifields and rank metric codes

Nonlinear MRD-codes with minimum distance $n \leftrightarrow$ Quasifields

$\mathbb{F}_{q_0}$-linear MRD-code in $M_n(\mathbb{F}_q)$, $d = n \leftrightarrow$ semifields with a nucleus containing $\mathbb{F}_q$.

Subspace code from a quasifield/semifield $=$ Spread/semifield spread.

Equivalent* codes $\leftrightarrow$ Isotopic presemifields $\leftrightarrow$ isomorphic planes $\leftrightarrow$ equivalent spreads.

Commutative/symplectic semifields $\leftrightsquigarrow$ MRD-code consisting of symmetrics [Kantor].

Semifields and rank metric codes

Nonlinear MRD-codes with minimum distance $n \leftrightarrow$ Quasifields

$\mathbb{F}_{q_0}$-linear MRD-code in $M_n(\mathbb{F}_q)$, $d = n \leftrightarrow$ semifields with a nucleus containing $\mathbb{F}_q$.

Subspace code from a quasifield/semifield = Spread/semifield spread.

Equivalent* codes $\leftrightarrow$ Isotopic presemifields $\leftrightarrow$ isomorphic planes $\leftrightarrow$ equivalent spreads.

Commutative/symplectic semifields $\leftrightsquigarrow$ MRD-code consisting of symmetrics [Kantor].

Semifields and rank metric codes

Nonlinear MRD-codes with minimum distance $n \leftrightarrow$ Quasifields

$\mathbb{F}_{q_0}$-linear MRD-code in $M_n(\mathbb{F}_q)$, $d = n \leftrightarrow$ semifields with a nucleus containing $\mathbb{F}_q$.

Subspace code from a quasifield/semifield $=$ Spread/semifield spread.

Equivalent* codes $\leftrightarrow$ Isotopic presemifields $\leftrightarrow$ isomorphic planes $\leftrightarrow$ equivalent spreads.

Commutative/symplectic semifields $\leftrightsquigarrow$ MRD-code consisting of symmetrics [Kantor].

Semifields and rank metric codes

Nonlinear MRD-codes with minimum distance $n \leftrightarrow$ Quasifields

$\mathbb{F}_{q_0}$-linear MRD-code in $M_n(\mathbb{F}_q)$, $d = n \leftrightarrow$ semifields with a nucleus containing $\mathbb{F}_q$.

Subspace code from a quasifield/semifield $=$ Spread/semifield spread.

Equivalent* codes $\leftrightarrow$ Isotopic presemifields $\leftrightarrow$ isomorphic planes $\leftrightarrow$ equivalent spreads.

Commutative/symplectic semifields $\leftrightsquigarrow$ MRD-code consisting of symmetrics [Kantor].

Semifields and rank metric codes

Nonlinear MRD-codes with minimum distance $n \leftrightarrow$ Quasifields

$\mathbb{F}_{q_0}$-linear MRD-code in $M_n(\mathbb{F}_q)$, $d = n \leftrightarrow$ semifields with a nucleus containing $\mathbb{F}_q$.

Subspace code from a quasifield/semifield $=$ Spread/semifield spread.

Equivalent* codes $\leftrightarrow$ Isotopic presemifields $\leftrightarrow$ isomorphic planes $\leftrightarrow$ equivalent spreads.

Commutative/symplectic semifields $\leftrightsquigarrow$ MRD-code consisting of symmetrics [Kantor].

Examples

Albert (1965) defined a multiplication on $\mathbb{F}_{q^n}$ by

$$\mathbb{S}(x, y) = xy - cx^{q^i} y^{q^j},$$

$N(c) \neq 1$, named Generalized twisted fields.

MRD code of linearized polynomials: $\{xy - cx^{q^i} y^{q^j} : y \in \mathbb{F}_{q^n}\}$

A lot of other constructions.

Even more examples found by computer (e.g. 332 isotopy classes of order 2^6 [Rua-Combarro-Ranilla]; only 35 were from known constructions).

So, plenty of non-Gabidulin MRD-codes for $k = 1$ (and $k = n - 1$ by duality).

Examples

Albert (1965) defined a multiplication on $\mathbb{F}_{q^n}$ by

$$\mathbb{S}(x, y) = xy - cx^{q^i} y^{q^j},$$

$N(c) \neq 1$, named Generalized twisted fields.

MRD code of linearized polynomials: $\{xy - cx^{q^i} y^{q^j} : y \in \mathbb{F}_{q^n}\}$

A lot of other constructions.

Even more examples found by computer (e.g. 332 isotopy classes of order 2^6 [Rua-Combarro-Ranilla]; only 35 were from known constructions).

So, plenty of non-Gabidulin MRD-codes for $k = 1$ (and $k = n - 1$ by duality).

Examples

Albert (1965) defined a multiplication on $\mathbb{F}_{q^n}$ by

$$\mathbb{S}(x, y) = xy - cx^{q^i} y^{q^j},$$

$N(c) \neq 1$, named Generalized twisted fields.

MRD code of linearized polynomials: $\{xy - cx^{q^i} y^{q^j} : y \in \mathbb{F}_{q^n}\}$

A lot of other constructions.

Even more examples found by computer (e.g. 332 isotopy classes of order 2^6 [Rua-Combarro-Ranilla]; only 35 were from known constructions).

So, plenty of non-Gabidulin MRD-codes for $k = 1$ (and $k = n - 1$ by duality).

Examples

Albert (1965) defined a multiplication on $\mathbb{F}_{q^n}$ by

$$\mathbb{S}(x, y) = xy - cx^{q^i} y^{q^j},$$

$N(c) \neq 1$, named Generalized twisted fields.

MRD code of linearized polynomials: $\{xy - cx^{q^i} y^{q^j} : y \in \mathbb{F}_{q^n}\}$

A lot of other constructions.

Even more examples found by computer (e.g. 332 isotopy classes of order 2^6 [Rua-Combarro-Ranilla]; only 35 were from known constructions).

So, plenty of non-Gabidulin MRD-codes for $k = 1$ (and $k = n - 1$ by duality).

Examples

Albert (1965) defined a multiplication on $\mathbb{F}_{q^n}$ by

$$\mathbb{S}(x, y) = xy - cx^{q^i} y^{q^j},$$

$N(c) \neq 1$, named Generalized twisted fields.

MRD code of linearized polynomials: $\{xy - cx^{q^i} y^{q^j} : y \in \mathbb{F}_{q^n}\}$

A lot of other constructions.

Even more examples found by computer (e.g. 332 isotopy classes of order 2^6 [Rua-Combarro-Ranilla]; only 35 were from known constructions).

So, plenty of non-Gabidulin MRD-codes for $k = 1$ (and $k = n - 1$ by duality).

Semifields: classification results

Dickson: *Every semifield two-dimensional over its centre is isotopic to either a field*. Hence there is a unique $\mathbb{F}_q$-linear $[2^2, 2, 2]_q$ MRD code.

Menichetti (1977): *Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field*.

Hence $\mathbb{F}_q$-linear $[3^2, 3, 3]_q$ MRD codes are completely classified.

By duality, $\mathbb{F}_q$-linear $[3^2, 6, 2]_q$ MRD codes are also completely classified, and so all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$.

Menichetti also classified $\mathbb{F}_q$-linear $[n^2, n, n]_q$ codes over $\mathbb{F}_q$ for n prime and q large enough.

Semifields: classification results

Dickson: *Every semifield two-dimensional over its centre is isotopic to either a field*. Hence there is a unique $\mathbb{F}_q$-linear $[2^2, 2, 2]_q$ MRD code.

Menichetti (1977): *Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field*.

Hence $\mathbb{F}_q$-linear $[3^2, 3, 3]_q$ MRD codes are completely classified.

By duality, $\mathbb{F}_q$-linear $[3^2, 6, 2]_q$ MRD codes are also completely classified, and so all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$.

Menichetti also classified $\mathbb{F}_q$-linear $[n^2, n, n]_q$ codes over $\mathbb{F}_q$ for n prime and q large enough.

Semifields: classification results

Dickson: *Every semifield two-dimensional over its centre is isotopic to either a field*. Hence there is a unique $\mathbb{F}_q$-linear $[2^2, 2, 2]_q$ MRD code.

Menichetti (1977): *Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field*.

Hence $\mathbb{F}_q$-linear $[3^2, 3, 3]_q$ MRD codes are completely classified.

By duality, $\mathbb{F}_q$-linear $[3^2, 6, 2]_q$ MRD codes are also completely classified, and so all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$.

Menichetti also classified $\mathbb{F}_q$-linear $[n^2, n, n]_q$ codes over $\mathbb{F}_q$ for n prime and q large enough.

Semifields: classification results

Dickson: *Every semifield two-dimensional over its centre is isotopic to either a field*. Hence there is a unique $\mathbb{F}_q$-linear $[2^2, 2, 2]_q$ MRD code.

Menichetti (1977): *Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field*.

Hence $\mathbb{F}_q$-linear $[3^2, 3, 3]_q$ MRD codes are completely classified.

By duality, $\mathbb{F}_q$-linear $[3^2, 6, 2]_q$ MRD codes are also completely classified, and so all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$.

Menichetti also classified $\mathbb{F}_q$-linear $[n^2, n, n]_q$ codes over $\mathbb{F}_q$ for n prime and q large enough.

Semifields: classification results

Dickson: *Every semifield two-dimensional over its centre is isotopic to either a field*. Hence there is a unique $\mathbb{F}_q$-linear $[2^2, 2, 2]_q$ MRD code.

Menichetti (1977): *Every semifield three-dimensional over its centre is isotopic to either a field or generalised twisted field*.

Hence $\mathbb{F}_q$-linear $[3^2, 3, 3]_q$ MRD codes are completely classified.

By duality, $\mathbb{F}_q$-linear $[3^2, 6, 2]_q$ MRD codes are also completely classified, and so all $\mathbb{F}_q$-linear MRD codes in $M_3(\mathbb{F}_q)$.

Menichetti also classified $\mathbb{F}_q$-linear $[n^2, n, n]_q$ codes over $\mathbb{F}_q$ for n prime and q large enough.

Semifields: classification results

A lot of recent work in semifields has been focussed on *rank two semifields*, which correspond to $\mathbb{F}_{q_0}$-linear MRD codes in $M_2(\mathbb{F}_q)$.

Full classification for $q = q_0^2$ (Cardinali-Polverino-Trombetti), partial classification for $q = q_0^3$ (Johnson-Lavrauw-Marino-Polverino-Trombetti...).

Full classification for $\mathbb{F}_{q_0}$-linear symmetric MRD-codes in $M_2(\mathbb{F}_q)$, $q = q_0^m$, q_0 large enough w.r.t m. [Ball-Blokhuis-Lavrauw].

Useful references: Kantor(2006); Lavrauw-Polverino (2011).

Semifields: classification results

A lot of recent work in semifields has been focussed on *rank two semifields*, which correspond to $\mathbb{F}_{q_0}$-linear MRD codes in $M_2(\mathbb{F}_q)$.

Full classification for $q = q_0^2$ (Cardinali-Polverino-Trombetti), partial classification for $q = q_0^3$ (Johnson-Lavrauw-Marino-Polverino-Trombetti...).

Full classification for $\mathbb{F}_{q_0}$-linear symmetric MRD-codes in $M_2(\mathbb{F}_q)$, $q = q_0^m$, q_0 large enough w.r.t m. [Ball-Blokhuis-Lavrauw].

Useful references: Kantor(2006); Lavrauw-Polverino (2011).

Semifields: classification results

A lot of recent work in semifields has been focussed on *rank two semifields*, which correspond to $\mathbb{F}_{q_0}$-linear MRD codes in $M_2(\mathbb{F}_q)$.

Full classification for $q = q_0^2$ (Cardinali-Polverino-Trombetti), partial classification for $q = q_0^3$ (Johnson-Lavrauw-Marino-Polverino-Trombetti...).

Full classification for $\mathbb{F}_{q_0}$-linear symmetric MRD-codes in $M_2(\mathbb{F}_q)$, $q = q_0^m$, q_0 large enough w.r.t m. [Ball-Blokhuis-Lavrauw].

Useful references: Kantor(2006); Lavrauw-Polverino (2011).

Semifields: classification results

A lot of recent work in semifields has been focussed on *rank two semifields*, which correspond to $\mathbb{F}_{q_0}$-linear MRD codes in $M_2(\mathbb{F}_q)$.

Full classification for $q = q_0^2$ (Cardinali-Polverino-Trombetti), partial classification for $q = q_0^3$ (Johnson-Lavrauw-Marino-Polverino-Trombetti...).

Full classification for $\mathbb{F}_{q_0}$-linear symmetric MRD-codes in $M_2(\mathbb{F}_q)$, $q = q_0^m$, q_0 large enough w.r.t m. [Ball-Blokhuis-Lavrauw].

Useful references: Kantor(2006); Lavrauw-Polverino (2011).

Enough about semifields already... what about $1 < k < n - 1$?

Minimum polynomial of a subspace

Suppose U is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension k. Then there exists a unique monic linearized polynomial of degree q^k annihilating U.

Hence a linearized polynomial of degree q^k has rank $n-k$ if and only if it is an $\mathbb{F}_{q^n}$-multiple of the minimum polynomial of some subspace of dimension k.

$U = \langle \alpha \rangle_{\mathbb{F}_q}$:

$$\alpha x^q - \alpha^q x$$

So a degree 1 linearized polynomial has rank $n-1$ if and only if $N(f_1) = N(-f_0)$.

Minimum polynomial of a subspace

Suppose U is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension k. Then there exists a unique monic linearized polynomial of degree q^k annihilating U.

Hence a linearized polynomial of degree q^k has rank $n-k$ if and only if it is an $\mathbb{F}_{q^n}$-multiple of the minimum polynomial of some subspace of dimension k.

$U = \langle \alpha \rangle_{\mathbb{F}_q}$:

$$\alpha x^q - \alpha^q x$$

So a degree 1 linearized polynomial has rank $n-1$ if and only if $N(f_1) = N(-f_0)$.

Minimum polynomial of a subspace

Suppose U is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension k. Then there exists a unique monic linearized polynomial of degree q^k annihilating U.

Hence a linearized polynomial of degree q^k has rank $n-k$ if and only if it is an $\mathbb{F}_{q^n}$-multiple of the minimum polynomial of some subspace of dimension k.

$U = \langle \alpha \rangle_{\mathbb{F}_q}$:

$$\alpha x^q - \alpha^q x$$

So a degree 1 linearized polynomial has rank $n-1$ if and only if $N(f_1) = N(-f_0)$.

Minimum polynomial of a subspace

Suppose U is an $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^n}$ of dimension k. Then there exists a unique monic linearized polynomial of degree q^k annihilating U.

Hence a linearized polynomial of degree q^k has rank $n-k$ if and only if it is an $\mathbb{F}_{q^n}$-multiple of the minimum polynomial of some subspace of dimension k.

$U = \langle\alpha\rangle_{\mathbb{F}_q}$:

$$\alpha x^q - \alpha^q x$$

So a degree 1 linearized polynomial has rank $n-1$ if and only if $N(f_1) = N(-f_0)$.

Minimum polynomial of a subspace

$U = \langle \alpha, \beta \rangle_{\mathbb{F}_q}$:

$$(\alpha\beta^q - \alpha^q\beta)x^{q^2} + (\alpha^{q^2}\beta - \alpha\beta^{q^2})x^q + (\alpha^q\beta^{q^2} - \alpha^{q^2}\beta^q)x$$

So a degree 2 linearized polynomial has rank $n-2$ only if $N(f_2) = N(f_0)$.

Key Lemma

Lemma

Suppose f is a linearized polynomial of degree q^k. If f has rank $n-k$, then $N(f_k) = (-1)^{nk} N(f_0)$.

(Proof is a simple induction argument, using the minimum polynomial of a subspace).

Hence if we can choose a subspace of linearized polynomials of degree at most q^k, avoiding $N(f_k) = (-1)^{nk} N(f_0)$, then each element would have rank at least $n-k+1$.

Key Lemma

Lemma

Suppose f is a linearized polynomial of degree q^k. If f has rank $n-k$, then $N(f_k) = (-1)^{nk} N(f_0)$.

(Proof is a simple induction argument, using the minimum polynomial of a subspace).

Hence if we can choose a subspace of linearized polynomials of degree at most q^k, avoiding $N(f_k) = (-1)^{nk} N(f_0)$, then each element would have rank at least $n-k+1$.

Key Lemma

Lemma

Suppose f is a linearized polynomial of degree q^k. If f has rank $n-k$, then $N(f_k) = (-1)^{nk}N(f_0)$.

(Proof is a simple induction argument, using the minimum polynomial of a subspace).

Hence if we can choose a subspace of linearized polynomials of degree at most q^k, avoiding $N(f_k) = (-1)^{nk}N(f_0)$, then each element would have rank at least $n-k+1$.

New construction

Define $\mathcal{H}_k(a,h)$ to be the set of linearized polynomials of degree at most k satisfying $f_k = af_0^{q^h}$, with $N(a) \neq (-1)^{nk}$.

$$\mathcal{H}_k(a,h) := \{f_0x + f_1x^q + \cdots + f_{k-1}x^{q^{k-1}} + af_0^{q^h}x^{q^k} : f_i \in \mathbb{F}_{q^n}\}.$$

Theorem (S.)

$\mathcal{H}_k(a,h)$ is an MRD-code with parameters $[n, nk, n-k+1]_q$. Furthermore, $\mathcal{H}_k(a,h)$ is not equivalent to $\mathcal{G}_k$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Choosing $a = 0$ returns the Gabidulin codes.

New construction

Define $\mathcal{H}_k(a,h)$ to be the set of linearized polynomials of degree at most k satisfying $f_k = af_0^{q^h}$, with $N(a) \neq (-1)^{nk}$.

$$\mathcal{H}_k(a,h) := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} + af_0^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n}\}.$$

Theorem (S.)

$\mathcal{H}_k(a,h)$ is an MRD-code with parameters $[n, nk, n-k+1]_q$. Furthermore, $\mathcal{H}_k(a,h)$ is not equivalent to $\mathcal{G}_k$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Choosing $a = 0$ returns the Gabidulin codes.

New construction

Define $\mathcal{H}_k(a, h)$ to be the set of linearized polynomials of degree at most k satisfying $f_k = af_0^{q^h}$, with $N(a) \neq (-1)^{nk}$.

$$\mathcal{H}_k(a, h) := \{f_0 x + f_1 x^q + \cdots + f_{k-1} x^{q^{k-1}} + af_0^{q^h} x^{q^k} : f_i \in \mathbb{F}_{q^n}\}.$$

Theorem (S.)

$\mathcal{H}_k(a, h)$ is an MRD-code with parameters $[n, nk, n-k+1]_q$. Furthermore, $\mathcal{H}_k(a, h)$ is not equivalent to $\mathcal{G}_k$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Choosing $a = 0$ returns the Gabidulin codes.

Idea of (a) proof of inequivalence

- $\mathcal{H}_k$ contains a space equivalent to $\mathcal{G}_{k-1}$, and is contained in $\mathcal{G}_{k+1}$.
- Lemma: Every subspace of $\mathcal{G}_s$ equivalent to $\mathcal{G}_r$ is of the form
$$g\mathcal{G}_r h,$$
where g, h are invertible and $\deg_q(g) + \deg_q(h) \leq s - r$.
- Result follows quickly from this.

Idea of (a) proof of inequivalence

- $\mathcal{H}_k$ contains a space equivalent to $\mathcal{G}_{k-1}$, and is contained in $\mathcal{G}_{k+1}$.
- Lemma: Every subspace of $\mathcal{G}_s$ equivalent to $\mathcal{G}_r$ is of the form
$$g\mathcal{G}_r h,$$
where g, h are invertible and $\deg_q(g) + \deg_q(h) \leq s - r$.
- Result follows quickly from this.

Idea of (a) proof of inequivalence

- $\mathcal{H}_k$ contains a space equivalent to $\mathcal{G}_{k-1}$, and is contained in $\mathcal{G}_{k+1}$.
- Lemma: Every subspace of $\mathcal{G}_s$ equivalent to $\mathcal{G}_r$ is of the form
$$g\mathcal{G}_r h,$$
where g, h are invertible and $\deg_q(g) + \deg_q(h) \leq s - r$.
- Result follows quickly from this.

Twisted Gabidulin codes

When $k = 1$, $\mathcal{H}_1(a, h)$ corresponds to the spread set of a generalized twisted field.

$$f_0 x + a f_0^{q^h} x^q = \mathbb{S}(x, f_0).$$

Hence we propose to call these twisted Gabidulin codes.

Note that these codes are $\mathbb{F}_{q^n}$-linear if and only if $h = 0$,.

Twisted Gabidulin codes

When $k = 1$, $\mathcal{H}_1(a, h)$ corresponds to the spread set of a generalized twisted field.

$$f_0 x + a f_0^{q^h} x^q = \mathbb{S}(x, f_0).$$

Hence we propose to call these twisted Gabidulin codes.

Note that these codes are $\mathbb{F}_{q^n}$-linear if and only if $h = 0$,.

Twisted Gabidulin codes

When $k = 1$, $\mathcal{H}_1(a, h)$ corresponds to the spread set of a generalized twisted field.

$$f_0 x + a f_0^{q^h} x^q = \mathbb{S}(x, f_0).$$

Hence we propose to call these twisted Gabidulin codes.

Note that these codes are $\mathbb{F}_{q^n}$-linear if and only if $h = 0$,.

More examples?

These codes can be seen as part of a family of codes in one-to-one correspondence with maximum subspaces disjoint from a hyperregulus in $V(2n, q)$.

These were considered in Lavrauw-S.-Zanella (2014). Known examples give the $\mathcal{H}$'s.

New examples would not only give new codes, but also new semifields. Hence classifying such subspaces is an intriguing open problem.

More examples?

These codes can be seen as part of a family of codes in one-to-one correspondence with maximum subspaces disjoint from a hyperregulus in $V(2n, q)$.

These were considered in Lavrauw-S.-Zanella (2014). Known examples give the $\mathcal{H}$'s.

New examples would not only give new codes, but also new semifields. Hence classifying such subspaces is an intriguing open problem.

More examples?

These codes can be seen as part of a family of codes in one-to-one correspondence with maximum subspaces disjoint from a hyperregulus in $V(2n, q)$.

These were considered in Lavrauw-S.-Zanella (2014). Known examples give the $\mathcal{H}$'s.

New examples would not only give new codes, but also new semifields. Hence classifying such subspaces is an intriguing open problem.

Infinite fields

MRD codes over infinite fields have applications in space-time coding.

Let F be any field, and K a cyclic Galois extension of degree n. Let σ be a generator for $\mathrm{Gal}(K : F)$.

Then we can replace linearized polynomials with maps of the form

$$f : x \mapsto \sum_{i=0}^{n-1} f_i x^{\sigma^i}$$

Then the analogues of $\mathcal{G}_k$ and $\mathcal{H}_k$ are also MRD-codes.

$\mathcal{G}_k$: Gow-Quinlan (2009), Augot-Loidreau-Robert (201?).

Infinite fields

MRD codes over infinite fields have applications in space-time coding.

Let F be any field, and K a cyclic Galois extension of degree n. Let σ be a generator for $\mathrm{Gal}(K : F)$.

Then we can replace linearized polynomials with maps of the form

$$f : x \mapsto \sum_{i=0}^{n-1} f_i x^{\sigma^i}$$

Then the analogues of $\mathcal{G}_k$ and $\mathcal{H}_k$ are also MRD-codes.

$\mathcal{G}_k$: Gow-Quinlan (2009), Augot-Loidreau-Robert (201?).

Infinite fields

MRD codes over infinite fields have applications in space-time coding.

Let F be any field, and K a cyclic Galois extension of degree n. Let σ be a generator for $\mathrm{Gal}(K : F)$.

Then we can replace linearized polynomials with maps of the form

$$f : x \mapsto \sum_{i=0}^{n-1} f_i x^{\sigma^i}$$

Then the analogues of $\mathcal{G}_k$ and $\mathcal{H}_k$ are also MRD-codes.

$\mathcal{G}_k$: Gow-Quinlan (2009), Augot-Loidreau-Robert (201?).

Infinite fields

MRD codes over infinite fields have applications in space-time coding.

Let F be any field, and K a cyclic Galois extension of degree n. Let σ be a generator for $\mathrm{Gal}(K : F)$.

Then we can replace linearized polynomials with maps of the form

$$f : x \mapsto \sum_{i=0}^{n-1} f_i x^{\sigma^i}$$

Then the analogues of $\mathcal{G}_k$ and $\mathcal{H}_k$ are also MRD-codes.

$\mathcal{G}_k$: Gow-Quinlan (2009), Augot-Loidreau-Robert (201?).

Thank you for your attention!