Semifields, Planar Functions and MRD Codes

Yue Zhou

LOOPS 2019 Conference, Budapest, July 9, 2019

National University of Defense Technology

Outline

Semifields

Semifields

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

In other words,

- $(\mathbb{S}, +)$ is an abelian group;

Semifields

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

In other words,

- $(\mathbb{S}, +)$ is an abelian group;
- $*$ is both left- and right-distributive over $+$;

Semifields

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

In other words,

- $(\mathbb{S}, +)$ is an abelian group;
- $*$ is both left- and right-distributive over $+$;
- there is a multiplicative identity;

Semifields

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

In other words,

- $(\mathbb{S}, +)$ is an abelian group;
- $*$ is both left- and right-distributive over $+$;
- there is a multiplicative identity;
- for each a and each nonzero $b \in \mathbb{S}$, there exist unique x and y such that $b * x = a$ and $y * b = a$.

Semifields

Definition

A semifield $(\mathbb{S}, +, *)$ is a non-associative ring whose nonzero elements form a loop under multiplication.

In other words,

- $(\mathbb{S}, +)$ is an abelian group;
- $*$ is both left- and right-distributive over $+$;
- there is a multiplicative identity;
- for each a and each nonzero $b \in \mathbb{S}$, there exist unique x and y such that $b * x = a$ and $y * b = a$.

If $\mathbb{S}$ does not necessarily have a multiplicative identity, then it is a presemifield.

Semifields

- In this talk, we only concern finite semifields.

Semifields

- In this talk, we only concern finite semifields.
- $|\mathbb{S}|$ is a prime power, and its additive group is elementary abelian.

Semifields

- In this talk, we only concern finite semifields.
- $|\mathbb{S}|$ is a prime power, and its additive group is elementary abelian.
- $\mathbb{S}$ can be identified as $\mathbb{F}_q^m$.

Semifields

- In this talk, we only concern finite semifields.
- $|\mathbb{S}|$ is a prime power, and its additive group is elementary abelian.
- $\mathbb{S}$ can be identified as $\mathbb{F}_q^m$.
- When $*$ is commutative, $\mathbb{S}$ is called a commutative semifield.

Semifields

- In this talk, we only concern finite semifields.
- $|\mathbb{S}|$ is a prime power, and its additive group is elementary abelian.
- $\mathbb{S}$ can be identified as $\mathbb{F}_q^m$.
- When $*$ is commutative, $\mathbb{S}$ is called a commutative semifield.

Dickson's semifield $(\mathbb{F}_q^2, +, *)$ (1906)

Let q be a power of an odd prime p, α a non-square in $\mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$.

Semifields

- In this talk, we only concern finite semifields.
- $|\mathbb{S}|$ is a prime power, and its additive group is elementary abelian.
- $\mathbb{S}$ can be identified as $\mathbb{F}_q^m$.
- When $*$ is commutative, $\mathbb{S}$ is called a commutative semifield.

Dickson's semifield $(\mathbb{F}_q^2, +, *)$ **(1906)**

Let q be a power of an odd prime p, α a non-square in $\mathbb{F}_q$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$.

$$(a, b) + (c, d) := (a + c, b + d),$$
$$(a, b) * (c, d) := (ac + \alpha(bd)^\sigma, ad + bc).$$

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$,

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$,

Lines: $\ell_{a,b} = \{(x, a * x + b) : x \in \mathbb{S}\}$,

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$, (a),

Lines: $\ell_{a,b} = \{(x, a * x + b) : x \in \mathbb{S}\}$,

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$, (a),

Lines: $\ell_{a,b} = \{(x, a * x + b) : x \in \mathbb{S}\}$, $\ell_c = \{(c, y) : y \ \in \mathbb{S}\}$,

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$, (a), (∞).

Lines: $\ell_{a,b} = \{(x, a * x + b) : x \in \mathbb{S}\}$, $\ell_c = \{(c, y) : y \ \in \mathbb{S}\}$,

Projective planes

$\mathbf{P} := (\mathcal{P}, \mathcal{L} \subseteq 2^{\mathcal{P}})$ is a projective plane, if

- for $P \neq Q \in \mathcal{P}$, $\exists$ unique $\ell \in \mathcal{L}$ such that $P, Q \in \ell$;
- for $\ell \neq m \in \mathcal{L}$, $\exists$ unique $P \in \mathcal{P}$ such that $P \in \ell, m$;
- there exists quadrangle, i.e. four points no three of which belong to one line.

Given a semifield $(\mathbb{S}, +, *)$, it coordinatizes a projective plane.

Points: $(x, y) \in \mathbb{S} \times \mathbb{S}$, (a), (∞).

Lines: $\ell_{a,b} = \{(x, a * x + b) : x \in \mathbb{S}\}$, $\ell_c = \{(c, y) : y \ \in \mathbb{S}\}$,
$\ell_\infty = \{(a) : a \in \mathbb{S} \cup \{\infty\}\}$.

Isotopism

Definition

Given two (pre)semifields $(\mathbb{F}_q^m, +, *)$ and $(\mathbb{F}_q^m, +, \star)$.

Isotopism

Definition

Given two (pre)semifields $(\mathbb{F}_q^m, +, *)$ and $(\mathbb{F}_q^m, +, \star)$. If there exist three bijective additive mappings $L, M, N : \mathbb{F}_q^m \to \mathbb{F}_q^m$ such that

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_q^m$, then they are isotopic.

Isotopism

Definition

Given two (pre)semifields $(\mathbb{F}_q^m, +, *)$ and $(\mathbb{F}_q^m, +, \star)$. If there exist three bijective additive mappings $L, M, N : \mathbb{F}_q^m \to \mathbb{F}_q^m$ such that

$$M(x) \star N(y) = L(x * y)$$

for any $x, y \in \mathbb{F}_q^m$, then they are isotopic.

Theorem (Albert 1960)

Two (pre)semifields coordinatize isomorphic projective planes if and only if they are isotopic.

Isotopism

- Presemifields can be "normalized" to semifields via isotopism. Given $(\mathbb{S}, +, *)$ and $a \neq 0$, $a * a$ is the identity of $\circ$

$$(x * a) \circ (a * y) = x * y.$$

Isotopism

- Presemifields can be “normalized” to semifields via isotopism. Given $(\mathbb{S}, +, *)$ and $a \neq 0$, $a * a$ is the identity of $\circ$

$$(x * a) \circ (a * y) = x * y.$$

- Left nucleus:
$N_l(\mathbb{S}) = \{\, a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S} \,\}.$

Isotopism

- Presemifields can be "normalized" to semifields via isotopism. Given $(\mathbb{S}, +, *)$ and $a \neq 0$, $a * a$ is the identity of $\circ$
$$(x * a) \circ (a * y) = x * y.$$
- Left nucleus:
$N_l(\mathbb{S}) = \{ a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S} \}$.
- Middle nucleus:
$N_m(\mathbb{S}) = \{ a \in \mathbb{S} : (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathbb{S} \}$.

Isotopism

- Presemifields can be "normalized" to semifields via isotopism. Given $(\mathbb{S}, +, *)$ and $a \neq 0$, $a * a$ is the identity of $\circ$

$$(x * a) \circ (a * y) = x * y.$$

- Left nucleus:
$N_l(\mathbb{S}) = \{\, a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S} \,\}.$
- Middle nucleus:
$N_m(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathbb{S} \,\}.$
- Right nucleus:
$N_r(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * y) * a = x * (y * a) \text{ for all } x, y \in \mathbb{S} \,\}.$

Isotopism

- Presemifields can be "normalized" to semifields via isotopism. Given $(\mathbb{S}, +, *)$ and $a \neq 0$, $a * a$ is the identity of $\circ$
$$(x * a) \circ (a * y) = x * y.$$
- Left nucleus:
$N_l(\mathbb{S}) = \{\, a \in \mathbb{S} : (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathbb{S} \,\}$.
- Middle nucleus:
$N_m(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathbb{S} \,\}$.
- Right nucleus:
$N_r(\mathbb{S}) = \{\, a \in \mathbb{S} : (x * y) * a = x * (y * a) \text{ for all } x, y \in \mathbb{S} \,\}$.
- All these nuclei of semifields are invariant under isotopism and they are all finite fields.

A long list of known semifields

- Albert's twisted fields, 1961

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields
- Ganley commutative semifields, 1981

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields
- Ganley commutative semifields, 1981
- Cohen-Ganley commutative semifields, 1982

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields
- Ganley commutative semifields, 1981
- Cohen-Ganley commutative semifields, 1982
- Cyclic semifields (Jha and Johnson 1989), generalizing Sandler(1962)'s semifields

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields
- Ganley commutative semifields, 1981
- Cohen-Ganley commutative semifields, 1982
- Cyclic semifields (Jha and Johnson 1989), generalizing Sandler(1962)'s semifields
- Kantor(2003) commutative semifields generalizing Knuth(1965)'s binary semifields.

A long list of known semifields

- Albert's twisted fields, 1961
- Knuth(1965)'s semifields, containing Dickson(1906)'s semifields and Hughes-Kleinfeld(1960) semifields
- Ganley commutative semifields, 1981
- Cohen-Ganley commutative semifields, 1982
- Cyclic semifields (Jha and Johnson 1989), generalizing Sandler(1962)'s semifields
- Kantor(2003) commutative semifields generalizing Knuth(1965)'s binary semifields.
- Bierbrauer, Budaghyan-Helleseth, Coulter-Matthews-Ding-Yuan, Lunardon-Marino-Polverino-Trombetti, Zha-Kyureghyan-Wang$\cdots$

Conjecture (Kantor,2003)

The number of pairwise non-isotopic semifields of order N is not bounded above by a polynomial in N.

Conjecture (Kantor,2003)

The number of pairwise non-isotopic semifields of order N is not bounded above by a polynomial in N.

- For N even, the conjecture is true (Kantor's commutative semifields).

Conjecture (Kantor,2003)

The number of pairwise non-isotopic semifields of order N is not bounded above by a polynomial in N.

- For N even, the conjecture is true (Kantor's commutative semifields).
- For N odd, the number of known semifields is less than $c\sqrt{N}\log_2(N)$.

Conjecture (Kantor,2003)

The number of pairwise non-isotopic semifields of order N is not bounded above by a polynomial in N.

- For N even, the conjecture is true (Kantor's commutative semifields).
- For N odd, the number of known semifields is less than $c\sqrt{N}\log_2(N)$.
- The number of known commutative semifields of order N is bounded above by $c(\log_p N)^2$.

Cyclic semifields

Let p be a prime.

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * y = \sum_{1 \le i,j < n} c_{ij} x^{p^i} y^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * a = \sum_{1 \leq i,j < n} c_{ij} x^{p^i} a^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * a = \sum_{1 \le i,j < n} c_{ij} x^{p^i} a^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

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 $\mathbb{F}_{q^n}[X]$.

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * a = \sum_{1 \le i,j < n} c_{ij} x^{p^i} a^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

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 $\mathbb{F}_{q^n}[X]$.

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

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * a = \sum_{1 \le i,j < n} c_{ij} x^{p^i} a^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

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 $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong \mathbb{F}_q^{n \times n}$.
- $ax^{q^i} \circ bx^{q^j} = a(bx^{q^j})^{q^i} = ab^{q^i} x^{q^{i+j}} = ab^{q^i} x^{q^i} \circ x^{q^j}$.

Cyclic semifields

Let p be a prime. For each semifield $(\mathbb{F}_{p^n}, +, *)$,

$$x * a = \sum_{1\le i,j<n} c_{ij} x^{p^i} a^{p^j},$$

for some $c_{ij} \in \mathbb{F}_{p^n}$.

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 $\mathbb{F}_{q^n}[X]$.

- $\mathscr{L}_{(n,q)}[X]/(X^{q^n} - X) \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong \mathbb{F}_q^{n\times n}$.
- $ax^{q^i} \circ bx^{q^j} = a(bx^{q^j})^{q^i} = ab^{q^i}x^{q^{i+j}} = ab^{q^i}x^{q^i} \circ x^{q^j}$.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g \in R : \deg(g) \leq s-1\}$. Define $g * h := gh$ mod $_r$ $f(X^n)$.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g \in R : \deg(g) \leq s-1\}$. Define $g * h := gh \mod_r f(X^n)$.
- $(\mathbb{S}, +, *)$ is a semifield.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g \in R : \deg(g) \leq s-1\}$. Define $g * h := gh \mod_r f(X^n)$.
- $(\mathbb{S}, +, *)$ is a semifield.
- $(\mathbb{F}_{q^n}[X;(\cdot)^q], +, \cdot) \cong (\mathscr{L}_{(n,q)}[X], +, \circ)$

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g \in R : \deg(g) \leq s-1\}$. Define $g * h := gh$ mod $_r$ $f(X^n)$.
- $(\mathbb{S}, +, *)$ is a semifield.
- $(\mathbb{F}_{q^n}[X;(\cdot)^q], +, \cdot) \cong (\mathscr{L}_{(n,q)}[X], +, \circ)$ and take $f(X) = X - 1$, $(\mathbb{F}_{q^n}[X;(\cdot)^q], +, \cdot)/(X^n - 1) \cong (\mathscr{L}_{(n,q)}[X], +, \circ)/(X^{q^n} - X)$.

Cyclic semifields

For $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$, i.e. $x^\sigma = x^{q^i}$, let $R = \mathbb{F}_{q^n}[X;\sigma]$ be a skew polynomial ring in which $Xa = a^\sigma X$.

- R is a non-commutative integral domain.
- R is both left- and right-Euclidean domain, with the usual degree function.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g \in R : \deg(g) \leq s-1\}$. Define $g * h := gh \mod_r f(X^n)$.
- $(\mathbb{S}, +, *)$ is a semifield.
- $(\mathbb{F}_{q^n}[X;(\cdot)^q], +, \cdot) \cong (\mathscr{L}_{(n,q)}[X], +, \circ)$ and take $f(X) = X - 1$, $(\mathbb{F}_{q^n}[X;(\cdot)^q], +, \cdot)/(X^n - 1) \cong (\mathscr{L}_{(n,q)}[X], +, \circ)/(X^{q^n} - X)$.
- For given $N = q^n$, there are at most $\sqrt{N}\log_2(N)$ cyclic semifields (Kantor,Liebler 2008).

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution.

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Then $(\mathbb{F}_q, +, *)$ is a presemifield, called Albert's twisted field.

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Then $(\mathbb{F}_q, +, *)$ is a presemifield, called Albert's twisted field.

By twisting some other known semifields, people have found more new semifields.

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Then $(\mathbb{F}_q, +, *)$ is a presemifield, called Albert's twisted field.

By twisting some other known semifields, people have found more new semifields.

- Pott-Z. commutative semifields, 2013.

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Then $(\mathbb{F}_q, +, *)$ is a presemifield, called Albert's twisted field.

By twisting some other known semifields, people have found more new semifields.

- Pott-Z. commutative semifields, 2013.
- Dempwolff semifields, 2013.

Twisting approach

Definition

Let $\sigma, \tau \in \mathrm{Aut}(\mathbb{F}_q)$ and $a \in \mathbb{F}_q$ such that $a = x^{\sigma-1}y^{\tau-1}$ has no solution. Define

$$x * y = xy - ax^{\sigma}y^{\tau}.$$

Then $(\mathbb{F}_q, +, *)$ is a presemifield, called Albert's twisted field.

By twisting some other known semifields, people have found more new semifields.

- Pott-Z. commutative semifields, 2013.
- Dempwolff semifields, 2013.
- Twisted cyclic semifields by Sheekey, arxiv.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^{\sigma} y^{\sigma^{-1}}$.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ $(y \mapsto y^\sigma)$.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^{\sigma} y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^{\sigma} y + x y^{\sigma}$ where $\sigma = p^k$ $(y \mapsto y^{\sigma})$.
- $(a, b) * (c, d) := (ac + \alpha (bd)^{\sigma}, ad + bc)$ (Dickson's semifields), where α a non-square.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ $(y \mapsto y^\sigma)$.
- $(a, b) * (c, d) := (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc)$, where α a non-square.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ ($y \mapsto y^\sigma$).
- $(a, b) * (c, d) := (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc)$, where α a non-square.
- $(\mathbb{F}_{q^2}, +, *)$ is a commutative presemifield (Pott, Z. 2013).

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ $(y \mapsto y^\sigma)$.
- $(a, b) * (c, d) := (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc)$, where α a non-square.
- $(\mathbb{F}_{q^2}, +, *)$ is a commutative presemifield (Pott, Z. 2013).
- This construction has two parameters k and σ.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ $(y \mapsto y^\sigma)$.
- $(a, b) * (c, d) := (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc)$, where α a non-square.
- $(\mathbb{F}_{q^2}, +, *)$ is a commutative presemifield (Pott, Z. 2013).
- This construction has two parameters k and σ.
- Let $q = p^m$ where p is a prime, $m = 2^e\mu$ with $\gcd(\mu, 2) = 1$. This construction gives exactly $\lfloor \frac{\mu}{2} \rfloor \lceil \frac{m}{2} \rceil$ non-isotopic presemifields.

Twisting approach

- By taking $\tau = \sigma^{-1}$ and $a = -1$, one has $x \circ y = xy + x^\sigma y^{\sigma^{-1}}$.
- It is isotopic to $x \circ_k y := x^\sigma y + xy^\sigma$ where $\sigma = p^k$ $(y \mapsto y^\sigma)$.
- $(a, b) * (c, d) := (a \circ_k c + \alpha(b \circ_k d)^\sigma, ad + bc)$, where α a non-square.
- $(\mathbb{F}_{q^2}, +, *)$ is a commutative presemifield (Pott, Z. 2013).
- This construction has two parameters k and σ.
- Let $q = p^m$ where p is a prime, $m = 2^e\mu$ with $\gcd(\mu, 2) = 1$. This construction gives exactly $\lfloor \frac{\mu}{2} \rfloor \lceil \frac{m}{2} \rceil$ non-isotopic presemifields.
- It gives us the bound $c(\log_p q)^2$ of known commutative semifields.

Twisting approach

$$x \circ y = xy - a x^{\sigma} y^{\tau}$$

Twisting approach

$$x \circ y = xy - ax^{\sigma} y^{\tau}$$

- Dempwolff's semifields

$$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

where $\circ$ defines a twisted field.

Twisting approach

$$x \circ y = xy - ax^{\sigma} y^{\tau}$$

- Dempwolff's semifields

$$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

  where $\circ$ defines a twisted field.

- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g = \sum g_i X^i \in \mathbb{F}_{q^n}[X; \sigma] : \deg(g) \leq s - 1\}$.
  Define $g * h := gh \mod {}_r f(X^n)$ for $g, h \in \mathbb{S}$. $(\mathbb{S}, +, *)$ is a cyclic semifield.

Twisting approach

$$x \circ c = cx - ac^{\tau} x^{\sigma}$$

- Dempwolff's semifields

  $$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

  where $\circ$ defines a twisted field.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g = \sum g_i X^i \in \mathbb{F}_{q^n}[X; \sigma] : \deg(g) \leq s - 1\}$.
  Define $g * h := gh \mod {}_r f(X^n)$ for $g, h \in \mathbb{S}$. $(\mathbb{S}, +, *)$ is a cyclic semifield.

Twisting approach

$$x \circ c = cx - ac^{\tau} x^{\sigma}$$

- Dempwolff's semifields

  $$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

  where $\circ$ defines a twisted field.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g = \sum g_i X^i \in \mathbb{F}_{q^n}[X; \sigma] : \deg(g) \leq s, g_s = \eta g_0^{\rho}\}$. Define $g * h := gh \mod {}_r f(X^n)$ for $g, h \in \mathbb{S}$. $(\mathbb{S}, +, *)$ is a twisted cyclic semifield (Sheekey arxiv).

Twisting approach

$$x \circ c = cx - ac^{\tau} x^{\sigma}$$

- Dempwolff's semifields

$$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

  where $\circ$ defines a twisted field.

- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g = \sum g_i X^i \in \mathbb{F}_{q^n}[X; \sigma] : \deg(g) \leq s, g_s = \eta g_0^{\rho}\}$.
  Define $g * h := gh \mod {}_r f(X^n)$ for $g, h \in \mathbb{S}$. $(\mathbb{S}, +, *)$ is a twisted cyclic semifield (Sheekey arxiv).
- Hughes-Kleinfeld (1960) semifields and generalized Dickson's (1965) semifields actually belong to this new construction.

Twisting approach

$$x \circ c = cx - ac^{\tau} x^{\sigma}$$

- Dempwolff's semifields

  $$(u, v) * (x, y) = (ux + v \circ y, uy + \zeta(v \circ x))$$

  where $\circ$ defines a twisted field.
- Let f be an irreducible polynomial in R, $\deg(f) = s$, $\mathbb{S} = \{g = \sum g_i X^i \in \mathbb{F}_{q^n}[X;\sigma] : \deg(g) \leq s, g_s = \eta g_0^{\rho}\}$. Define $g * h := gh \mod {}_r f(X^n)$ for $g, h \in \mathbb{S}$. $(\mathbb{S}, +, *)$ is a twisted cyclic semifield (Sheekey arxiv).
- Hughes-Kleinfeld (1960) semifields and generalized Dickson's (1965) semifields actually belong to this new construction.
- Question: how may non-isotopic twisted cyclic semifields are there?

Kantor's commutative semifields

Given a chain of fields $\mathbb{F} = \mathbb{F}_0 \supset \mathbb{F}_1 \supset \cdots \supset \mathbb{F}_m$ of characteristic 2 with $[\mathbb{F} : \mathbb{F}_m]$ odd and corresponding trace mappings $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$, $\zeta_i \in \mathbb{F}$.

Kantor's commutative semifields

Given a chain of fields $\mathbb{F} = \mathbb{F}_0 \supset \mathbb{F}_1 \supset \cdots \supset \mathbb{F}_m$ of characteristic 2 with $[\mathbb{F} : \mathbb{F}_m]$ odd and corresponding trace mappings $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$, $\zeta_i \in \mathbb{F}$.

$$x * y := xy + \left(x \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i y) + y \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i x) \right)^2 .$$

Then $(\mathbb{F}, +, *)$ is a presemifield.

Kantor's commutative semifields

Given a chain of fields $\mathbb{F} = \mathbb{F}_0 \supset \mathbb{F}_1 \supset \cdots \supset \mathbb{F}_m$ of characteristic 2 with $[\mathbb{F} : \mathbb{F}_m]$ odd and corresponding trace mappings $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$, $\zeta_i \in \mathbb{F}$.

$$x * y := xy + \left(x \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i y) + y \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i x) \right)^2 .$$

Then $(\mathbb{F}, +, *)$ is a presemifield.

- When $m = 1$, they are Knuth's binary presemifields.

Kantor's commutative semifields

Given a chain of fields $\mathbb{F} = \mathbb{F}_0 \supset \mathbb{F}_1 \supset \cdots \supset \mathbb{F}_m$ of characteristic 2 with $[\mathbb{F} : \mathbb{F}_m]$ odd and corresponding trace mappings $\mathrm{Tr}_i : \mathbb{F} \to \mathbb{F}_i$, $\zeta_i \in \mathbb{F}$.

$$x * y := xy + \left(x \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i y) + y \sum_{i=1}^{m} \mathrm{Tr}_i(\zeta_i x) \right)^2 .$$

Then $(\mathbb{F}, +, *)$ is a presemifield.

- When $m = 1$, they are Knuth's binary presemifields.
- For almost each different choice of $(\zeta_1, \cdots, \zeta_m)$, the presemifields are non-isotopic.

Planar Functions

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.
- For every $a \neq 0$, $x \mapsto f(x+a) - f(x) = 2a * x + a * a$ is a permutation on $\mathbb{F}_q$.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.
- For every $a \neq 0$, $x \mapsto f(x+a) - f(x) = 2a * x + a * a$ is a permutation on $\mathbb{F}_q$.

Definition (Dembowski and Ostrom 1968)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$. If for every $a \neq 0$, $f(x+a) - f(x)$ defines a permutation on $\mathbb{F}_q$, then f is a planar function.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.
- For every $a \neq 0$, $x \mapsto f(x+a) - f(x) = 2a * x + a * a$ is a permutation on $\mathbb{F}_q$.

Definition (Dembowski and Ostrom 1968)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$. If for every $a \neq 0$, $f(x+a) - f(x)$ defines a permutation on $\mathbb{F}_q$, then f is a planar function.

- Commutative (pre)semifields (q odd) $\Rightarrow$ Planar functions.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.
- For every $a \neq 0$, $x \mapsto f(x+a) - f(x) = 2a * x + a * a$ is a permutation on $\mathbb{F}_q$.

Definition (Dembowski and Ostrom 1968)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$. If for every $a \neq 0$, $f(x+a) - f(x)$ defines a permutation on $\mathbb{F}_q$, then f is a planar function.

- Commutative (pre)semifields (q odd) $\Rightarrow$ Planar functions.
- Planar functions from commutative semifields can always be written as a Dembowski-Ostrom (DO) polynomial $\sum a_{ij} x^{p^i + p^j}$.

Planar functions (q odd)

- Take a commutative (pre)semifield $(\mathbb{F}_q, +, *)$, where q is odd.
- Define $f : \mathbb{F}_q \to \mathbb{F}_q$ by $f(x) := x * x$.
- For every $a \neq 0$, $x \mapsto f(x+a) - f(x) = 2a * x + a * a$ is a permutation on $\mathbb{F}_q$.

Definition (Dembowski and Ostrom 1968)

Let $f : \mathbb{F}_q \to \mathbb{F}_q$. If for every $a \neq 0$, $f(x+a) - f(x)$ defines a permutation on $\mathbb{F}_q$, then f is a planar function.

- Commutative (pre)semifields (q odd) $\Rightarrow$ Planar functions.
- Planar functions from commutative semifields can always be written as a Dembowski-Ostrom (DO) polynomial $\sum a_{ij} x^{p^i + p^j}$.
- $x \circ_k y := x^\sigma y + x y^\sigma$ with $\sigma = p^k$, $f(x) = 2x^{p^k+1}$.

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?
  (Conjectured by Dembowksi and Ostrom 1968)

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?
  (Conjectured by Dembowksi and Ostrom 1968)
- Counter-example: (1997) Coulter-Matthews monomials $x^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$.

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?
  (Conjectured by Dembowksi and Ostrom 1968)
- Counter-example: (1997) Coulter-Matthews monomials $x^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$.
- Other examples? $p > 3$?

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields? (Conjectured by Dembowksi and Ostrom 1968)
- Counter-example: (1997) Coulter-Matthews monomials $x^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$.
- Other examples? $p > 3$?
- By a planar function f over $\mathbb{F}_q$, one can always define an affine plane Π_f using $D = \{(x, f(x)) : x \in \mathbb{F}_q\}$.

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?
  (Conjectured by Dembowksi and Ostrom 1968)

- Counter-example: (1997) Coulter-Matthews monomials $x^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$.

- Other examples? $p > 3$?

- By a planar function f over $\mathbb{F}_q$, one can always define an affine plane Π_f using $D = \{(x, f(x)) : x \in \mathbb{F}_q\}$.

  Points: $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$

Planar functions (q odd)

- Planar functions $\Rightarrow$ commutative (pre)semifields?
  (Conjectured by Dembowksi and Ostrom 1968)
- Counter-example: (1997) Coulter-Matthews monomials $x^{\frac{3^k+1}{2}}$ over $\mathbb{F}_{3^n}$.
- Other examples? $p > 3$?
- By a planar function f over $\mathbb{F}_q$, one can always define an affine plane Π_f using $D = \{(x, f(x)) : x \in \mathbb{F}_q\}$.

  Points: $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$

  Lines: $\ell_{a,b} = D + (a, b) = \{(x + a, f(x) + b) : x \in \mathbb{F}_q\}$,
  $\ell_a = \{(a, y) : y \in \mathbb{F}_q\}$.

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij}x^{p^i+p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij} x^{p^i + p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij} x^{p^i+p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).
- In general, Π_f is a semifield plane $\Rightarrow$ f is DO+affine?

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij}x^{p^i+p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).
- In general, Π_f is a semifield plane $\Rightarrow$ f is DO+affine?
- Dembowski and Ostrom gave a criterion (1968).

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij} x^{p^i + p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).
- In general, Π_f is a semifield plane $\Rightarrow$ f is DO+affine?
- Dembowski and Ostrom gave a criterion (1968).
- Dempwolff and Röder investigated the case in which f is a monomial (2006).

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij} x^{p^i + p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).
- In general, Π_f is a semifield plane $\Rightarrow$ f is DO+affine?
- Dembowski and Ostrom gave a criterion (1968).
- Dempwolff and Röder investigated the case in which f is a monomial (2006).
- Partially answered by Coulter and Henderson (2008).

Planar functions (q odd)

- When f is a DO+affine polynomial, i.e. $f(x) = \sum a_{ij} x^{p^i+p^j} + \sum c_i x^{p^i}$, Π_f is a semifield plane.
- Coulter-Matthews planar functions define a very special plane (Lenz-Barlotti II.1).
- In general, Π_f is a semifield plane $\Rightarrow$ f is DO+affine?
- Dembowski and Ostrom gave a criterion (1968).
- Dempwolff and Röder investigated the case in which f is a monomial (2006).
- Partially answered by Coulter and Henderson (2008).

Theorem (Z., 2018)

The plane Π_f is a commutative semifield plane if and only if f is a DO+affine polynomial.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$,

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0+a)+f(x_0) = b$, then $f((x_0+a)+a)+f(x_0+a) = b$.
- x_0 and $x_0 + a$ are both mapped to b.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.
- x_0 and $x_0 + a$ are both mapped to b. Not a permutation.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.
- x_0 and $x_0 + a$ are both mapped to b. Not a permutation.
- Hence the previous definition of planar functions does not work for even q.

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.
- x_0 and $x_0 + a$ are both mapped to b. Not a permutation.
- Hence the previous definition of planar functions does not work for even q.
- However, for every semifield $\mathbb{S}$ of order q, there exits a group $(G, \cdot)$ of order q^2 and $D \subseteq G$ of size q defining a plane Π_D:

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.
- x_0 and $x_0 + a$ are both mapped to b. Not a permutation.
- Hence the previous definition of planar functions does not work for even q.
- However, for every semifield $\mathbb{S}$ of order q, there exits a group $(G, \cdot)$ of order q^2 and $D \subseteq G$ of size q defining a plane Π_D:

  Points: $g \in G$

Planar functions (q even)

- Recall that f is planar on $\mathbb{F}_q$ if $x \mapsto f(x+a) - f(x)$ is a permutation for every $a \neq 0$.
- q even, $a - b = a + b$
- If $f(x_0 + a) + f(x_0) = b$, then $f((x_0 + a) + a) + f(x_0 + a) = b$.
- x_0 and $x_0 + a$ are both mapped to b. Not a permutation.
- Hence the previous definition of planar functions does not work for even q.
- However, for every semifield $\mathbb{S}$ of order q, there exits a group $(G, \cdot)$ of order q^2 and $D \subseteq G$ of size q defining a plane Π_D:

  Points: $g \in G$

  Lines: $\ell_a = aD$ for $a \in G$ and the cosets of $H \trianglelefteq G$ which is of size q.

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd,

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$,

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$,

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$,

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$, $H = 2C_4^m \cong \mathbb{F}_2^m$

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$, $H = 2C_4^m \cong \mathbb{F}_2^m$ and $D = ?$

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$, $H = 2C_4^m \cong \mathbb{F}_2^m$ and $D = ?$

Definition

A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is (modified) planar if $x \mapsto f(x+a) + f(x) + xa$ is a permutation of $\mathbb{F}_{2^m}$ for each $a \in \mathbb{F}_{2^m}^*$.

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$, $H = 2C_4^m \cong \mathbb{F}_2^m$ and $D = ?$

Definition

A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is (modified) planar if $x \mapsto f(x+a) + f(x) + xa$ is a permutation of $\mathbb{F}_{2^m}$ for each $a \in \mathbb{F}_{2^m}^*$.

- Represent C_4^m as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with the group operation

$$(x, y) \star (x', y') = (x + x', y + y' + x \cdot x').$$

Planar functions (q even)

For instance,

- when $\mathbb{S}$ is commutative and q is odd, $G = (\mathbb{F}_q^2, +)$, $D = \{(x, x * x) : x \in \mathbb{F}_q\}$ and $H = \{(0, y) : y \in \mathbb{F}_q\}$;
- when $\mathbb{S}$ is commutative and $q = 2^m$, $G = C_4^m$, $H = 2C_4^m \cong \mathbb{F}_2^m$ and $D = \{(x, f(x)) : x \in \mathbb{F}_{2^n}\}$

Definition

A function $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is (modified) planar if $x \mapsto f(x+a) + f(x) + xa$ is a permutation of $\mathbb{F}_{2^m}$ for each $a \in \mathbb{F}_{2^m}^*$.

- Represent C_4^m as $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ with the group operation

$$(x, y) \star (x', y') = (x + x', y + y' + x \cdot x').$$

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003),

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}.

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}. For instance $q = 2^8$.

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}. For instance $q = 2^8$.
- Question: Are there any non-DO planar polynomials, like the Coulter-Matthews planar functions for q odd?

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}. For instance $q = 2^8$.
- Question: Are there any non-DO planar polynomials, like the Coulter-Matthews planar functions for q odd?
- Related to a long standing open problem in coding theory.

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}. For instance $q = 2^8$.
- Question: Are there any non-DO planar polynomials, like the Coulter-Matthews planar functions for q odd?
- Related to a long standing open problem in coding theory.
- The plane Π_f is a commutative semifield plane if and only if f is a DO+affine polynomial (Z., 2013).

Planar functions (q even)

- As there are exponentially many commutative semifields of even order q (Kantor 2003), there are many planar functions over $\mathbb{F}_q$.
- Only one family is known.
- No example of order 2^{2^k}. For instance $q = 2^8$.
- Question: Are there any non-DO planar polynomials, like the Coulter-Matthews planar functions for q odd?
- Related to a long standing open problem in coding theory.
- The plane Π_f is a commutative semifield plane if and only if f is a DO+affine polynomial (Z., 2013).
- Using algebraic geometry, one can get classification results of them (Schmidt, Z. 2013, Müller, Zieve 2015, Bartoli, Schmidt 2019).

Maximum Rank-Distance Codes

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n \times n}$

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n \times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n \times n}$, if

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,
- for each distinct $M, N \in \mathcal{C}$, $\mathrm{rank}(M - N) \geq n - k + 1$,

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,
- for each distinct $M, N \in \mathcal{C}$, $\mathrm{rank}(M - N) \geq n - k + 1$,

then $\mathcal{C}$ is a maximum rank-distance (MRD, for short) codes in $\mathbb{F}_q^{n\times n}$.

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,
- for each distinct $M, N \in \mathcal{C}$, $\mathrm{rank}(M - N) \geq n - k + 1$,

then $\mathcal{C}$ is a maximum rank-distance (MRD, for short) codes in $\mathbb{F}_q^{n\times n}$. Its minimum distance $d = n - k + 1$.

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements. $\mathcal{C}$ is an MRD code of minimum distance n in $\mathbb{F}_p^{n\times n}$,

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,
- for each distinct $M, N \in \mathcal{C}$, $\mathrm{rank}(M - N) \geq n - k + 1$,

then $\mathcal{C}$ is a maximum rank-distance (MRD, for short) codes in $\mathbb{F}_q^{n\times n}$. Its minimum distance $d = n - k + 1$.

MRD Codes

Let $(\mathbb{F}_{p^n}, +, *)$ be a semifield. Define $L_a : x \mapsto x * a$.

- L_a is $\mathbb{F}_p$-linear, can be viewed as a matrix in $\mathbb{F}_p^{n\times n}$
- $L_a - L_b$ is invertible for $a \neq b$;
- $\mathcal{C} = \{L_a : a \in \mathbb{F}_{p^n}\}$ has p^n elements. $\mathcal{C}$ is an MRD code of minimum distance n in $\mathbb{F}_p^{n\times n}$, and $L_a + L_b = L_{a+b}$.

Definition

Given $\mathcal{C} \subseteq \mathbb{F}_q^{n\times n}$, if

- $\#\mathcal{C} = q^{nk}$,
- for each distinct $M, N \in \mathcal{C}$, $\mathrm{rank}(M - N) \geq n - k + 1$,

then $\mathcal{C}$ is a maximum rank-distance (MRD, for short) codes in $\mathbb{F}_q^{n\times n}$. Its minimum distance $d = n - k + 1$.

Equivalence

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m \times n}$, they are equivalent

Equivalence

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$, they 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

Equivalence

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$, they 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 $X^\gamma := (x_{ij}^\gamma)$.

Equivalence

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$, they 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 $\mathbb{K}^{m\times n}$.

Equivalence

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m\times n}$, they 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 $m = n$, every isometry is

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

Definition

Given $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{K}^{m \times n}$, they 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 $m = n$, every isometry is

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

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

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

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

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

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

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

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

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

  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(n-d+1)}$ with $d = n - k + 1$.

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

  $\mathcal{G}_k = \{a_0X + a_1X^q + \dots a_{k-1}X^{q^{k-1}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$.
  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(n-d+1)}$ with $d = n - k + 1$.
- $\mathcal{G}_k$ is MRD.

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

  $\mathcal{G}_k = \{a_0 X + a_1 X^q + \dots a_{k-1} X^{q^{k-1}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$.
  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(n-d+1)}$ with $d = n - k + 1$.
- $\mathcal{G}_k$ is MRD.
- One may take $\sigma = q^t$ with $\gcd(t, n) = 1$ and replace q by σ.

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

  $\mathcal{G}_k = \{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$.
  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(n-d+1)}$ with $d = n - k + 1$.
- $\mathcal{G}_k$ is MRD.
- One may take $\sigma = q^t$ with $\gcd(t, n) = 1$ and replace q by σ.

MRD Codes

A semifield is just a linear MRD code of minimum distance n in $\mathbb{F}_q^{n\times n}$, where $\mathbb{F}_q$ is one of its nucleus.

How to construct MRD codes of minimum distance $d < n$?

- Gabidulin codes ($k = n - d + 1$) (Delsarte 1978), (Gabidulin 1985)

  $\mathcal{G}_k = \{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$.
  - ▷ For each $f \in \mathcal{G}$, f has at most q^{k-1} roots.
  - ▷ $\#\mathcal{G} = q^{nk} = q^{n(n-d+1)}$ with $d = n - k + 1$.
- $\mathcal{G}_k$ is MRD.
- One may take $\sigma = q^t$ with $\gcd(t, n) = 1$ and replace q by σ.
- More constructions?

More MRD Codes

There are mainly three approaches:

- Twisting

More MRD Codes

There are mainly three approaches:

- Twisting
- Scattered linear sets on a line ($k = 2$)

More MRD Codes

There are mainly three approaches:

- Twisting
- Scattered linear sets on a line ($k = 2$)
- Moore matrices

More MRD Codes

There are mainly three approaches:

- Twisting
- Scattered linear sets on a line ($k = 2$)
- Moore matrices

Besides, there are also two special nonlinear constructions of MRD codes.

More MRD Codes

There are mainly three approaches:

- Twisting
- Scattered linear sets on a line ($k = 2$)
- Moore matrices

Besides, there are also two special nonlinear constructions of MRD codes.

- Durante and Siciliano 2017 generalizing Cossidente, Marino and Pavese 2016.

More MRD Codes

There are mainly three approaches:

- Twisting
- Scattered linear sets on a line ($k = 2$)
- Moore matrices

Besides, there are also two special nonlinear constructions of MRD codes.

- Durante and Siciliano 2017 generalizing Cossidente, Marino and Pavese 2016.
- Otal and Özbudak 2018 (analogue of nearfields).

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Note that if $\eta = 0$, it is a Delsarte-Gabidulin code.

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Note that if $\eta = 0$, it is a Delsarte-Gabidulin code.

For even n (Trombetti and Z., 2019)

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Note that if $\eta = 0$, it is a Delsarte-Gabidulin code.

For even n (Trombetti and Z., 2019)

$$\{aX + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta b X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}, a, b \in \mathbb{F}^*_{q^{n/2}}\} \pmod{X^{q^n} - X}.$$

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Note that if $\eta = 0$, it is a Delsarte-Gabidulin code.

For even n (Trombetti and Z., 2019)

$$\{aX + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta b X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}, a, b \in \mathbb{F}^*_{q^{n/2}}\} \pmod{X^{q^n} - X}.$$

(Twisted) cyclic construction (Sheekey, arixv)

Twisting

Let $\sigma = q^t$ where $\gcd(t, n) = 1$.

Twisted Delsarte-Gabidulin codes (Sheekey, 2016)

$$\{a_0 X + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta a_0^{q^h} X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}\} \pmod{X^{q^n} - X}.$$

Note that if $\eta = 0$, it is a Delsarte-Gabidulin code.

For even n (Trombetti and Z., 2019)

$$\{aX + a_1 X^{\sigma} + \dots a_{k-1} X^{\sigma^{k-1}} + \eta b X^{\sigma^k} : a_i \in \mathbb{F}_{q^n}, a, b \in \mathbb{F}^*_{q^{n/2}}\} \pmod{X^{q^n} - X}.$$

(Twisted) cyclic construction (Sheekey, arixv)

$$\{\cdots\} \quad \bmod_r f(X^n) \quad (\text{in } \mathbb{F}_{q^n}[X;\sigma]),$$

where f is irreducible in $\mathbb{F}_{q^n}[X;\sigma]$.

Scattered linear sets

$\mathbb{F}_q$-linear MRD codes of $d = n - 1$ (i.e. $k = 2$) in $\mathbb{F}_q^{n\times n}$ has to be in the form

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

Scattered linear sets

$\mathbb{F}_q$-linear MRD codes of $d = n-1$ (i.e. $k = 2$) in $\mathbb{F}_q^{n\times n}$ has to be in the form

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

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

(apply $(\cdot)^{q^{(n-1)s}}$ and $\mod X^{q^n} - X$)

Scattered linear sets

$\mathbb{F}_q$-linear MRD codes of $d = n-1$ (i.e. $k = 2$) in $\mathbb{F}_q^{n\times n}$ has to be in the form

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

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

(apply $(\cdot)^{q^{(n-1)s}}$ and mod $X^{q^n} - X$)

- $\mathcal{F}$ is MRD if and only if

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

Scattered linear sets

$\mathbb{F}_q$-linear MRD codes of $d = n-1$ (i.e. $k=2$) in $\mathbb{F}_q^{n\times n}$ has to be in the form

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

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

(apply $(\cdot)^{q^{(n-1)s}}$ and mod $X^{q^n} - X$)

- $\mathcal{F}$ is MRD if and only if

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

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

Scattered polynomials

- In finite geometries, a maximum scattered linear set over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}^2,$$

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

$$\#L(U) = \frac{q^n - 1}{q - 1}.$$

Scattered polynomials

- In finite geometries, a maximum scattered linear set over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}^2,$$

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

$$\#L(U) = \frac{q^n - 1}{q - 1}.$$

- Hence it is equivalent to

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

Scattered polynomials

- In finite geometries, a maximum scattered linear set over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}^2,$$

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

$$\# L(U) = \frac{q^n - 1}{q - 1}.$$

- Hence it is equivalent to

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

- Constructions for $n = 6, 8$ (Csajbók, Marino, Polverino, Zanella, Zullo).

Scattered polynomials

- In finite geometries, a maximum scattered linear set over $\mathrm{PG}(1, q^n)$:

$$U = \{(x, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}^2,$$
$$L(U) = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\}\} = \left\{ \left(1, \frac{f(x)}{x}\right) : x \in \mathbb{F}_{q^n}^* \right\},$$
$$\#L(U) = \frac{q^n - 1}{q - 1}.$$

- Hence it is equivalent to

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

- Constructions for $n = 6, 8$ (Csajbók, Marino, Polverino, Zanella, Zullo).
- Classification results (Bartoli, Z. 2018) (Bartoli, Montanucci arxiv).

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent.

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

$$\mathcal{C}_\Lambda := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X],$$

where $\Lambda = \{t_0, \cdots, t_{k-1}\}$.

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

$$\mathcal{C}_\Lambda := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X],$$

where $\Lambda = \{t_0, \cdots, t_{k-1}\}$.

Theorem (Csajbók, Marino, Polverino, Z, submitted)

Let Λ_1 and Λ_2 be two k-subsets of $\{0, \ldots, n-1\}$.

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

$$\mathcal{C}_\Lambda := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X],$$

where $\Lambda = \{t_0, \cdots, t_{k-1}\}$.

Theorem (Csajbók, Marino, Polverino, Z, submitted)

Let Λ_1 and Λ_2 be two k-subsets of $\{0, \ldots, n-1\}$. Define $\mathcal{C}_j = \left\{\sum_{i \in \Lambda_j} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n}\right\}$ for $j = 1, 2$.

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

$$\mathcal{C}_\Lambda := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X],$$

where $\Lambda = \{t_0, \cdots, t_{k-1}\}$.

Theorem (Csajbók, Marino, Polverino, Z, submitted)

Let Λ_1 and Λ_2 be two k-subsets of $\{0, \ldots, n-1\}$. Define $\mathcal{C}_j = \left\{\sum_{i\in\Lambda_j} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n}\right\}$ for $j = 1, 2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent

Moore matrices

In general, it is quite difficult to tell whether $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent. However, for a very special type, this work is quite easy.

$$\mathcal{C}_\Lambda := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X],$$

where $\Lambda = \{t_0, \cdots, t_{k-1}\}$.

Theorem (Csajbók, Marino, Polverino, Z, submitted)

Let Λ_1 and Λ_2 be two k-subsets of $\{0, \ldots, n-1\}$. Define $\mathcal{C}_j = \left\{\sum_{i\in\Lambda_j} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n}\right\}$ for $j = 1, 2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent if and only if

$$\Lambda_2 = \Lambda_1 + s := \{i + s \pmod n : i \in \Lambda_1\}$$

for some $s \in \{0, \cdots, n-1\}$.

Moore matrices

For $A := (\alpha_0, \ldots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$ and $k \leq n$, a square Moore matrix is defined as

$$M_A := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{k-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{k-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \cdots & \alpha_{k-1}^{q^{k-1}} \end{pmatrix}.$$

Moore matrices

For $A := (\alpha_0, \ldots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$ and $k \leq n$, a square Moore matrix is defined as

$$M_A := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{k-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{k-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \cdots & \alpha_{k-1}^{q^{k-1}} \end{pmatrix}.$$

It is a q-analogue of Vandermonde matrices.

Moore matrices

For $A := (\alpha_0, \dots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$ and $k \le n$, a square Moore matrix is defined as

$$M_A := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{k-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{k-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \cdots & \alpha_{k-1}^{q^{k-1}} \end{pmatrix}.$$

It is a q-analogue of Vandermonde matrices.

$$\det(M_A) = \prod_{\mathbf{c}} (c_0\alpha_0 + c_1\alpha_1 + \cdots c_{k-1}\alpha_{k-1}),$$

where $\mathbf{c} = (c_0, c_1, \cdots, c_{k-1})$ runs over $\mathrm{PG}(k-1, q)$.

Moore matrices

For $A := (\alpha_0, \ldots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$ and $k \leq n$, a square Moore matrix is defined as

$$M_A := \begin{pmatrix} \alpha_0 & \alpha_1 & \cdots & \alpha_{k-1} \\ \alpha_0^q & \alpha_1^q & \cdots & \alpha_{k-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{k-1}} & \alpha_1^{q^{k-1}} & \cdots & \alpha_{k-1}^{q^{k-1}} \end{pmatrix}.$$

It is a q-analogue of Vandermonde matrices.

$$\det(M_A) = \prod_{\mathbf{c}} (c_0\alpha_0 + c_1\alpha_1 + \cdots c_{k-1}\alpha_{k-1}),$$

where $\mathbf{c} = (c_0, c_1, \cdots, c_{k-1})$ runs over $\mathrm{PG}(k-1, q)$. Therefore,

elements in A are $\mathbb{F}_q$-linearly independent iff $\det(M_A) \neq 0$.

Moore exponent sets

For any set of distinct nonnegative integers $I = \{t_0, t_1, \ldots, t_{k-1}\}$ and $A = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$, $k \leq n$ and let

$$M_{A,I} := \begin{pmatrix} \alpha_0^{q^{t_0}} & \alpha_1^{q^{t_0}} & \cdots & \alpha_{k-1}^{q^{t_0}} \\ \alpha_0^{q^{t_1}} & \alpha_1^{q^{t_1}} & \cdots & \alpha_{k-1}^{q^{t_1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{t_{k-1}}} & \alpha_1^{q^{t_{k-1}}} & \cdots & \alpha_{k-1}^{q^{t_{k-1}}} \end{pmatrix}.$$

Moore exponent sets

For any set of distinct nonnegative integers $I = \{t_0, t_1, \dots, t_{k-1}\}$ and $A = (\alpha_0, \alpha_1, \dots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$, $k \le n$ and let

$$M_{A,I} := \begin{pmatrix} \alpha_0^{q^{t_0}} & \alpha_1^{q^{t_0}} & \cdots & \alpha_{k-1}^{q^{t_0}} \\ \alpha_0^{q^{t_1}} & \alpha_1^{q^{t_1}} & \cdots & \alpha_{k-1}^{q^{t_1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{t_{k-1}}} & \alpha_1^{q^{t_{k-1}}} & \cdots & \alpha_{k-1}^{q^{t_{k-1}}} \end{pmatrix}.$$

Besides $I = \{0, 1, \cdots, k-1\}$, it is interesting to ask whether there exist other I sharing the same property.

Moore exponent sets

For any set of distinct nonnegative integers $I = \{t_0, t_1, \ldots, t_{k-1}\}$ and $A = (\alpha_0, \alpha_1, \ldots, \alpha_{k-1}) \subseteq \mathbb{F}_{q^n}^k$, $k \leq n$ and let

$$M_{A,I} := \begin{pmatrix} \alpha_0^{q^{t_0}} & \alpha_1^{q^{t_0}} & \cdots & \alpha_{k-1}^{q^{t_0}} \\ \alpha_0^{q^{t_1}} & \alpha_1^{q^{t_1}} & \cdots & \alpha_{k-1}^{q^{t_1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{q^{t_{k-1}}} & \alpha_1^{q^{t_{k-1}}} & \cdots & \alpha_{k-1}^{q^{t_{k-1}}} \end{pmatrix}.$$

Besides $I = \{0, 1, \cdots, k-1\}$, it is interesting to ask whether there exist other I sharing the same property.

Elements in A are $\mathbb{F}_q$-linearly independent iff $\det(M_{A,I}) \neq 0$.

We call such I a Moore exponent set for q and n.

A connection with MRD codes

Theorem

For q and n, $I = \{t_0, \cdots, t_{k-1}\}$ is a Moore exponent set if and only if

$$\mathcal{C}_I := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X]$$

is an MRD code.

A connection with MRD codes

Theorem

For q and n, $I = \{t_0, \cdots, t_{k-1}\}$ is a Moore exponent set if and only if

$$\mathcal{C}_I := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X]$$

is an MRD code.

Besides $I = \{0, 1, \cdots, k-1\}$, there are other known examples of Moore exponent sets.

A connection with MRD codes

Theorem

For q and n, $I = \{t_0, \cdots, t_{k-1}\}$ is a Moore exponent set if and only if

$$\mathcal{C}_I := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X]$$

is an MRD code.

Besides $I = \{0, 1, \cdots, k-1\}$, there are other known examples of Moore exponent sets.

- $I = \{0, s, \cdots, (k-1)s\}$ for any n satisfying $\gcd(s, n) = 1$ (Generalized Gabidulin codes);

A connection with MRD codes

Theorem

For q and n, $I = \{t_0, \cdots, t_{k-1}\}$ is a Moore exponent set if and only if

$$\mathcal{C}_I := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X]$$

is an MRD code.

Besides $I = \{0, 1, \cdots, k-1\}$, there are other known examples of Moore exponent sets.

- $I = \{0, s, \cdots, (k-1)s\}$ for any n satisfying $\gcd(s, n) = 1$ (Generalized Gabidulin codes);
- $I = \{0, 1, 3\}$ for $n = 7$ with odd q (Csajbók, Marino, Polverino, Z.);

A connection with MRD codes

Theorem

For q and n, $I = \{t_0, \cdots, t_{k-1}\}$ is a Moore exponent set if and only if

$$\mathcal{C}_I := \{a_0 X^{q^{t_0}} + a_1 X^{q^{t_1}} + \ldots + a_{k-1} X^{q^{t_{k-1}}} : a_i \in \mathbb{F}_{q^n}\} \subseteq \mathbb{F}_{q^n}[X]$$

is an MRD code.

Besides $I = \{0, 1, \cdots, k-1\}$, there are other known examples of Moore exponent sets.

- $I = \{0, s, \cdots, (k-1)s\}$ for any n satisfying $\gcd(s, n) = 1$ (Generalized Gabidulin codes);
- $I = \{0, 1, 3\}$ for $n = 7$ with odd q (Csajbók, Marino, Polverino, Z.);
- $I = \{0, 1, 3\}$ for $n = 8$ with $q \equiv 1 \pmod 3$ (Csajbók, Marino, Polverino, Z.).

$n = 7$

Theorem

The set $I = \{0, 1, 3\}$ is a Moore exponent set if and only if q is odd.

$n = 7$

Theorem

The set $I = \{0, 1, 3\}$ is a Moore exponent set if and only if q is odd.

Proof: q even

Theorem

The set $I = \{0, 1, 3\}$ is a Moore exponent set if and only if q is odd.

Proof: q even

The Dickson matrix associated with $X + X^q + X^{q^3} \in \mathbb{F}_{q^7}[X]$ is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1^q & 1^q & 0 & 1^q & 0 & 0 \\ 0 & 0 & 1^{q^2} & 1^{q^2} & 0 & 1^{q^2} & 0 \\ 0 & 0 & 0 & 1^{q^3} & 1^{q^3} & 0 & 1^{q^3} \\ 1^{q^4} & 0 & 0 & 0 & 1^{q^4} & 1^{q^4} & 0 \\ 0 & 1^{q^5} & 0 & 0 & 0 & 1^{q^5} & 1^{q^5} \\ 1^{q^6} & 0 & 1^{q^6} & 0 & 0 & 0 & 1^{q^6} \end{pmatrix}$$

$n = 7$

Theorem

The set $I = \{0, 1, 3\}$ is a Moore exponent set if and only if q is odd.

Proof: q even

The Dickson matrix associated with $X + X^q + X^{q^3} \in \mathbb{F}_{q^7}[X]$ is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$n = 7$

Theorem

The set $I = \{0, 1, 3\}$ is a Moore exponent set if and only if q is odd.

Proof: q even

The Dickson matrix associated with $X + X^q + X^{q^3} \in \mathbb{F}_{q^7}[X]$ is

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Rank $= 4$ for q even $\Rightarrow$ q^3 roots $\Rightarrow$ I is not an Moore exponent set.

Proof: q odd

Suppose to the contrary that $\{0, 1, 3\}$ is not a Moore exponent set.

Proof: q odd

Suppose to the contrary that $\{0, 1, 3\}$ is not a Moore exponent set.

- There exists u_1, u_2, u_3 which are $\mathbb{F}_q$-linearly independent.

Proof: q odd

Suppose to the contrary that $\{0,1,3\}$ is not a Moore exponent set.

- There exists u_1, u_2, u_3 which are $\mathbb{F}_q$-linearly independent.
- The rows/columns of $M := \begin{pmatrix} u_1 & u_2 & u_3 \\ u_1^q & u_2^q & u_3^q \\ u_1^{q^3} & u_2^{q^3} & u_3^{q^3} \end{pmatrix}$ are $\mathbb{F}_{q^7}$-linearly dependent.

Proof: q odd

Suppose to the contrary that $\{0,1,3\}$ is not a Moore exponent set.

- There exists u_1, u_2, u_3 which are $\mathbb{F}_q$-linearly independent.
- The rows/columns of $M := \begin{pmatrix} u_1 & u_2 & u_3 \\ u_1^q & u_2^q & u_3^q \\ u_1^{q^3} & u_2^{q^3} & u_3^{q^3} \end{pmatrix}$ are $\mathbb{F}_{q^7}$-linearly dependent.
- $P := \langle (u_1, u_2, u_3) \rangle_{\mathbb{F}_{q^7}}$, $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$.

Proof: q odd

Suppose to the contrary that $\{0, 1, 3\}$ is not a Moore exponent set.

- There exists u_1, u_2, u_3 which are $\mathbb{F}_q$-linearly independent.
- The rows/columns of $M := \begin{pmatrix} u_1 & u_2 & u_3 \\ u_1^q & u_2^q & u_3^q \\ u_1^{q^3} & u_2^{q^3} & u_3^{q^3} \end{pmatrix}$ are $\mathbb{F}_{q^7}$-linearly dependent.
- $P := \langle (u_1, u_2, u_3) \rangle_{\mathbb{F}_{q^7}}$, $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$.
- P, P^σ, P^{σ^3} are on a line ℓ.

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.
- $\ell \neq \ell^\sigma$, the length of the orbit of ℓ under σ is 7.

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.
- $\ell \neq \ell^\sigma$, the length of the orbit of ℓ under σ is 7.
- P^{σ^i}, ℓ^{σ^i} for $i = 0, \ldots, 6$ form a Fano plane.

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.
- $\ell \neq \ell^\sigma$, the length of the orbit of ℓ under σ is 7.
- P^{σ^i}, ℓ^{σ^i} for $i = 0, \ldots, 6$ form a Fano plane.
- A Fano plane cannot be embedded in $\mathrm{PG}(2, q^7)$ with q odd.

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.
- $\ell \neq \ell^\sigma$, the length of the orbit of ℓ under σ is 7.
- P^{σ^i}, ℓ^{σ^i} for $i = 0, \ldots, 6$ form a Fano plane.
- A Fano plane cannot be embedded in $\mathrm{PG}(2, q^7)$ with q odd.
- A contradiction!

Proof: q odd

- $\sigma(x_1, x_2, x_3) = (x_1^q, x_2^q, x_3^q)$, $\ell = \langle P, P^\sigma, P^{\sigma^3} \rangle_{\mathbb{F}_{q^7}}$.
- $\ell \neq \ell^\sigma$, the length of the orbit of ℓ under σ is 7.
- P^{σ^i}, ℓ^{σ^i} for $i = 0, \ldots, 6$ form a Fano plane.
- A Fano plane cannot be embedded in $\mathrm{PG}(2, q^7)$ with q odd.
- A contradiction!
- Therefore, $\alpha_1 X + \alpha_2 X^q + \alpha_3 X^{q^3}$ cannot have q^3 roots.

An asymptotic classification result

In general it seems illusive to give a complete list of Moore exponent set, because the associated Dickson matrices are getting larger.

An asymptotic classification result

In general it seems illusive to give a complete list of Moore exponent set, because the associated Dickson matrices are getting larger.

Theorem (Bartoli, Z. Submitted)

Assume that I is not an arithmetic progression. Then there exist integers N and $Q \leq 5$ depending on I such that I is not a Moore exponent set over $\mathbb{F}_{q^n}$ provided that $q > Q$ and $n > N$.

An asymptotic classification result

In general it seems illusive to give a complete list of Moore exponent set, because the associated Dickson matrices are getting larger.

Theorem (Bartoli, Z. Submitted)

Assume that I is not an arithmetic progression. Then there exist integers N and $Q \leq 5$ depending on I such that I is not a Moore exponent set over $\mathbb{F}_{q^n}$ provided that $q > Q$ and $n > N$.

We believe that the restriction on $q > Q$ can be removed.

An asymptotic classification result

In general it seems illusive to give a complete list of Moore exponent set, because the associated Dickson matrices are getting larger.

Conjecture

Assume that I is not an arithmetic progression. Then there exist integers N ~~and $Q \leq 5$~~ depending on I such that I is not a Moore exponent set over $\mathbb{F}_{q^n}$ provided that ~~$q > Q$ and~~ $n > N$.

We believe that the restriction on $q > Q$ can be removed.

Thanks for your attention!