Planar functions over fields of characteristic two

Yue Zhou
joint work with Kai-Uwe Schmidt

Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, Germany

June 11, 2013

Planar functions

Definition

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is planar or perfect nonlinear if

$$x \mapsto f(x+a) - f(x)$$

is a permutation of $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$.

Planar functions

Definition

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is planar or perfect nonlinear if

$$x \mapsto f(x+a) - f(x)$$

is a permutation of $\mathbb{F}_q$ for each $a \in \mathbb{F}_q^*$.

Example

$f(x) = x^2$ is planar on $\mathbb{F}_q$, q odd, since

$$f(x+a) - f(x) = 2ax + a^2.$$

Planar functions and relative difference sets

- Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be planar.

Planar functions and relative difference sets

- Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be planar.
- $D := \{(x, f(x)) : x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$.

Planar functions and relative difference sets

- Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be planar.
- $D := \{(x, f(x)) : x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$.
- Nonzero differences of elements in D:

Planar functions and relative difference sets

- Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be planar.
- $D := \{(x, f(x)) : x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$.
- Nonzero differences of elements in D:

$$\{(a, f(x+a) - f(x)) : a \in \mathbb{F}_q^*,\ x \in \mathbb{F}_q\} = \mathbb{F}_q^* \times \mathbb{F}_q$$

Planar functions and relative difference sets

- Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be planar.
- $D := \{(x, f(x)) : x \in \mathbb{F}_q\} \subseteq \mathbb{F}_q \times \mathbb{F}_q$.
- Nonzero differences of elements in D:

$$\{(a, f(x+a) - f(x)) : a \in \mathbb{F}_q^*,\ x \in \mathbb{F}_q\} = \mathbb{F}_q^* \times \mathbb{F}_q$$

- $D \subseteq \mathbb{F}_q \times \mathbb{F}_q$ is a $(q, q, q, 1)$-relative difference set in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$.

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$
- $G = (\mathbb{F}_q \times \mathbb{F}_q, +)$,

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$
- $G = (\mathbb{F}_q \times \mathbb{F}_q, +)$, $N = (\{0\} \times \mathbb{F}_q, +)$.

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$
- $G = (\mathbb{F}_q \times \mathbb{F}_q, +)$, $N = (\{0\} \times \mathbb{F}_q, +)$.
- List of differences: $\mathbb{F}_q^* \times \mathbb{F}_q$.

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$
- $G = (\mathbb{F}_q \times \mathbb{F}_q, +)$, $N = (\{0\} \times \mathbb{F}_q, +)$.
- List of differences: $\mathbb{F}_q^* \times \mathbb{F}_q$.
- $(|G|/|N|, |N|, |D|, \lambda) =$

Relative difference sets

Definition

Let G be a group and N a subgroup. A subset D of G is called a relative difference set with parameters $(|G|/|N|, |N|, |D|, \lambda)$, if the list of differences of D covers every element in $G \setminus N$ exactly λ times, and no element in $N \setminus \{0\}$; N is the forbidden subgroup.

- $D := \{(x, f(x)) : x \in \mathbb{F}_q\}$
- $G = (\mathbb{F}_q \times \mathbb{F}_q, +)$, $N = (\{0\} \times \mathbb{F}_q, +)$.
- List of differences: $\mathbb{F}_q^* \times \mathbb{F}_q$.
- $(|G|/|N|, |N|, |D|, \lambda) = (q, q, q, 1)$.

Combinatorial objects from planar functions

- Planar functions over $\mathbb{F}_q$ and $(q, q, q, 1)$-relative difference sets in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$ are equivalent objects.

Combinatorial objects from planar functions

- Planar functions over $\mathbb{F}_q$ and $(q, q, q, 1)$-relative difference sets in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$ are equivalent objects.
- Every $(q, q, q, 1)$-relative difference set can be used to construct a projective plane by its development. (Ganley, Spence 1975, Dembowski 1968)

Combinatorial objects from planar functions

- Planar functions over $\mathbb{F}_q$ and $(q, q, q, 1)$-relative difference sets in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$ are equivalent objects.
- Every $(q, q, q, 1)$-relative difference set can be used to construct a projective plane by its development. (Ganley, Spence 1975, Dembowski 1968) That's why these functions are called planar.

Combinatorial objects from planar functions

- Planar functions over $\mathbb{F}_q$ and $(q, q, q, 1)$-relative difference sets in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$ are equivalent objects.
- Every $(q, q, q, 1)$-relative difference set can be used to construct a projective plane by its development. (Ganley, Spence 1975, Dembowski 1968) That's why these functions are called planar.
- "Good" code defined over $\mathbb{F}_q$ by parity check matrix (α is a primitive element of $\mathbb{F}_{q^n}$)

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^n-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^n-2}) \end{bmatrix}$$

Combinatorial objects from planar functions

- Planar functions over $\mathbb{F}_q$ and $(q, q, q, 1)$-relative difference sets in $\mathbb{F}_q \times \mathbb{F}_q$ relative to $\{0\} \times \mathbb{F}_q$ are equivalent objects.
- Every $(q, q, q, 1)$-relative difference set can be used to construct a projective plane by its development. (Ganley, Spence 1975, Dembowski 1968) That's why these functions are called planar.
- "Good" code defined over $\mathbb{F}_q$ by parity check matrix (α is a primitive element of $\mathbb{F}_{q^n}$)

$$\begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{q^n-2} \\ f(1) & f(\alpha) & f(\alpha^2) & \cdots & f(\alpha^{q^n-2}) \end{bmatrix}$$

- "Quadratic" planar functions (degree of every term: $q^i + q^j$) and commutative semifields are equivalent objects.

Examples: Planar monomials

Examples: Planar monomials

List of planar monomials and their semifields:

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2,

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.
- x^{p^k+1},

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.
- x^{p^k+1}, Albert's twisted fields.

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.
- x^{p^k+1}, Albert's twisted fields.
- $x^{\frac{3^k+1}{2}}$ on $\mathbb{F}_{3^n}$,

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.
- x^{p^k+1}, Albert's twisted fields.
- $x^{\frac{3^k+1}{2}}$ on $\mathbb{F}_{3^n}$, no semifields (nonquadratic).

Examples: Planar monomials

List of planar monomials and their semifields:

- x^2, finite fields.
- x^{p^k+1}, Albert's twisted fields.
- $x^{\frac{3^k+1}{2}}$ on $\mathbb{F}_{3^n}$, no semifields (nonquadratic).

Classification of exceptional planar monomials:
Leducq 2010, Hernando, McGuire and Monserrat 2013, Zieve 2013.

What happens for even characteristic?

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

What happens for even characteristic?

- 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

What happens for even characteristic?

- 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
- If x_0 is a solution to $f(x+a) - f(x) = b$,

What happens for even characteristic?

- 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
- If x_0 is a solution to $f(x+a) - f(x) = b$, so is $x_0 + a$.

What happens for even characteristic?

- 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
- If x_0 is a solution to $f(x+a) - f(x) = b$, so is $x_0 + a$.
- Not a permutation.

What happens for even characteristic?

- 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
- If x_0 is a solution to $f(x+a) - f(x) = b$, so is $x_0 + a$.
- Not a permutation.
- Hence planar functions do not exist for even q.

What happens for even characteristic?

- 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
- If x_0 is a solution to $f(x+a) - f(x) = b$, so is $x_0 + a$.
- Not a permutation.
- Hence planar functions do not exist for even q.
- Dead end?

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set?

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane?

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes?

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.
  - Commutative semifields?

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.
  - Commutative semifields? No.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.
  - Commutative semifields? No.
- But: $(2^n, 2^n, 2^n, 1)$-relative difference sets exist in $\mathbb{Z}_4^n$.

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.
  - Commutative semifields? No.
- But: $(2^n, 2^n, 2^n, 1)$-relative difference sets exist in $\mathbb{Z}_4^n$.
- $\mathbb{Z}_4^n \ncong \mathbb{Z}_2^n \times \mathbb{Z}_2^n$,

APN functions

- A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is almost perfect nonlinear (APN) if

$$f(x+a) - f(x) = b$$

has at most two solutions for all $a \in \mathbb{F}_{2^n}^*$ and $b \in \mathbb{F}_{2^n}$.

  - $(2^n, 2^n, 2^n, 1)$-relative difference set? No.
  - Plane? No.
  - "Good" codes? Yes, but not "good" enough.
  - Commutative semifields? No.
- But: $(2^n, 2^n, 2^n, 1)$-relative difference sets exist in $\mathbb{Z}_4^n$.
- $\mathbb{Z}_4^n \ncong \mathbb{Z}_2^n \times \mathbb{Z}_2^n$, no finite fields.

Galois rings

- Want: relative difference sets in $\mathbb{Z}_4^n$ relative to $2\mathbb{Z}_4^n$.

Galois rings

- Want: relative difference sets in $\mathbb{Z}_4^n$ relative to $2\mathbb{Z}_4^n$.
- $(R_n, +, \cdot)$: Galois ring of characteristic 4 and cardinality 4^n.

Galois rings

- Want: relative difference sets in $\mathbb{Z}_4^n$ relative to $2\mathbb{Z}_4^n$.
- $(R_n, +, \cdot)$: Galois ring of characteristic 4 and cardinality 4^n.
- $R_n \cong \mathbb{Z}_4^n$ and $2R_n \cong 2\mathbb{Z}_4^n$.

Galois rings

- Want: relative difference sets in $\mathbb{Z}_4^n$ relative to $2\mathbb{Z}_4^n$.
- $(R_n, +, \cdot)$: Galois ring of characteristic 4 and cardinality 4^n.
- $R_n \cong \mathbb{Z}_4^n$ and $2R_n \cong 2\mathbb{Z}_4^n$.
- $\Gamma(R_n)$: Teichmuller set of R_n.

Galois rings

- Want: relative difference sets in $\mathbb{Z}_4^n$ relative to $2\mathbb{Z}_4^n$.
- $(R_n, +, \cdot)$: Galois ring of characteristic 4 and cardinality 4^n.
- $R_n \cong \mathbb{Z}_4^n$ and $2R_n \cong 2\mathbb{Z}_4^n$.
- $\Gamma(R_n)$: Teichmuller set of R_n.
- $(\Gamma(R_n), \oplus, \cdot)$ is a finite field with 2^n elements, where

$$x \oplus y := x + y + 2\sqrt{xy}.$$

Relative difference sets in $\mathbb{Z}_4^n$

- $f : \Gamma(R_n) \to \Gamma(R_n)$ can be identified as $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.

Relative difference sets in $\mathbb{Z}_4^n$

- $f : \Gamma(R_n) \to \Gamma(R_n)$ can be identified as $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
- $D := \{x + 2\sqrt{f(x)} : x \in \Gamma(R_n)\}$.

Relative difference sets in $\mathbb{Z}_4^n$

- $f : \Gamma(R_n) \to \Gamma(R_n)$ can be identified as $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
- $D := \{x + 2\sqrt{f(x)} : x \in \Gamma(R_n)\}$.
- Nonzero differences of elements in D:

Relative difference sets in $\mathbb{Z}_4^n$

- $f : \Gamma(R_n) \to \Gamma(R_n)$ can be identified as $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
- $D := \{x + 2\sqrt{f(x)} : x \in \Gamma(R_n)\}$.
- Nonzero differences of elements in D:

$$\{a + 2\sqrt{f(x \oplus a) \oplus f(x) \oplus ax} : a \in \Gamma(R_n)^*, x \in \Gamma(R_n)\}$$

Relative difference sets in $\mathbb{Z}_4^n$

- $f : \Gamma(R_n) \to \Gamma(R_n)$ can be identified as $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$.
- $D := \{x + 2\sqrt{f(x)} : x \in \Gamma(R_n)\}$.
- Nonzero differences of elements in D:

$$\{a + 2\sqrt{f(x \oplus a) \oplus f(x) \oplus ax} : a \in \Gamma(R_n)^*, x \in \Gamma(R_n)\}$$

equals $R_n \setminus 2R_n$ if and only if

$$f(x \oplus a) \oplus f(x) \oplus ax$$

is a permutation of $\Gamma(R_n)$, for each $a \in \Gamma(R_n)^*$.

Planar functions over $\mathbb{F}_{2^n}$

Definition

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is planar if

$$x \mapsto f(x+a) + f(x) + xa$$

is a permutation of $\mathbb{F}_{2^n}$ for each $a \in \mathbb{F}_{2^n}^*$.

Planar functions over $\mathbb{F}_{2^n}$

Definition

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is planar if

$$x \mapsto f(x+a) + f(x) + xa$$

is a permutation of $\mathbb{F}_{2^n}$ for each $a \in \mathbb{F}_{2^n}^*$.

Example

$f(x) = 0$, or linearized polynomials.

Planar functions over $\mathbb{F}_{2^n}$

Definition

A function $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is planar if

$$x \mapsto f(x+a) + f(x) + xa$$

is a permutation of $\mathbb{F}_{2^n}$ for each $a \in \mathbb{F}_{2^n}^*$.

Example

$f(x) = 0$, or linearized polynomials.

- Zhou: $(2^n, 2^n, 2^n, 1)$-*relative difference sets and their representations*, to appear in JCD.
- Schmidt, Zhou: *Planar functions over fields of characteristic two*, arXiv.

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets?

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes?

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes? Yes, of course. (Ganley, Spence 1975)

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes? Yes, of course. (Ganley, Spence 1975)
- "Quadratic" planar functions on $\mathbb{F}_{2^n}$ and commutative semifields of characteristic 2 are equivalent objects.

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes? Yes, of course. (Ganley, Spence 1975)
- "Quadratic" planar functions on $\mathbb{F}_{2^n}$ and commutative semifields of characteristic 2 are equivalent objects.
- "Good" codes?

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes? Yes, of course. (Ganley, Spence 1975)
- "Quadratic" planar functions on $\mathbb{F}_{2^n}$ and commutative semifields of characteristic 2 are equivalent objects.
- "Good" codes?

  Code $\mathcal{C}_f$ over $\mathbb{Z}_4$ with parity check matrix (β: generator of Γ^*)

Properties

- $(2^n, 2^n, 2^n, 1)$-relative difference sets? Yes.
- Planes? Yes, of course. (Ganley, Spence 1975)
- "Quadratic" planar functions on $\mathbb{F}_{2^n}$ and commutative semifields of characteristic 2 are equivalent objects.
- "Good" codes?

  Code $\mathcal{C}_f$ over $\mathbb{Z}_4$ with parity check matrix (β: generator of Γ^*)

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 2\sqrt{f(0)} & 1+2\sqrt{f(1)} & \beta+2\sqrt{f(\beta)} & \cdots & \beta^{2^n-2}+2\sqrt{f(\beta^{2^n-2})} \end{bmatrix}$$

Codes over $\mathbb{Z}_4$

- $\mathcal{C}$: the code $\mathcal{C}_f$ when f is identically zero.

Codes over $\mathbb{Z}_4$

- $\mathcal{C}$: the code $\mathcal{C}_f$ when f is identically zero.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \cdots & \beta^{2^n-2} \end{bmatrix}.$$

Codes over $\mathbb{Z}_4$

- $\mathcal{C}$: the code $\mathcal{C}_f$ when f is identically zero.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \cdots & \beta^{2^n-2} \end{bmatrix}.$$

- $\mathcal{C}^{\perp}$ is the $\mathbb{Z}_4$-representation of the Kerdock code (Hammons, Kumar, Calderbank, Sloane and Solé, 1994).

Codes over $\mathbb{Z}_4$

- $\mathcal{C}$: the code $\mathcal{C}_f$ when f is identically zero.

$$\begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \beta & \cdots & \beta^{2^n-2} \end{bmatrix}.$$

- $\mathcal{C}^{\perp}$ is the $\mathbb{Z}_4$-representation of the Kerdock code (Hammons, Kumar, Calderbank, Sloane and Solé, 1994).

Theorem

The code $\mathcal{C}_f$ has the same Lee weight distribution as $\mathcal{C}$ if and only if f is planar.

Planar functions from semifields

- Kantor (2003) gives exponentially many commutative semifields.

Planar functions from semifields

- Kantor (2003) gives exponentially many commutative semifields.
- This gives many planar functions.

Planar functions from semifields

- Kantor (2003) gives exponentially many commutative semifields.
- This gives many planar functions.
- Only one family.

Planar functions from semifields

- Kantor (2003) gives exponentially many commutative semifields.
- This gives many planar functions.
- Only one family.
- All known planar functions on $\mathbb{F}_{2^n}$ are quadratic.

Planar functions from semifields

- Kantor (2003) gives exponentially many commutative semifields.
- This gives many planar functions.
- Only one family.
- All known planar functions on $\mathbb{F}_{2^n}$ are quadratic.
- Non-quadratic?

Planar monomials

Planar monomials

If $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$, then t is a planar exponent of $\mathbb{F}_{2^n}$.

Planar monomials

If $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$, then t is a planar exponent of $\mathbb{F}_{2^n}$.

Exponent t	Which field	Reference
2^k	every	trivial
2^k+1	$\mathbb{F}_{2^{2k}}$	Schmidt and Zhou
$4^k(4^k+1)$	$\mathbb{F}_{2^{6k}}$	Scherr and Zieve

Planar monomials

If $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$, then t is a planar exponent of $\mathbb{F}_{2^n}$.

Exponent t	Which field	Reference
2^k	every	trivial
2^k+1	$\mathbb{F}_{2^{2k}}$	Schmidt and Zhou
$4^k(4^k+1)$	$\mathbb{F}_{2^{6k}}$	Scherr and Zieve

Conjecture

This list is complete.

Planar monomials

If $x \mapsto cx^t$ is planar on $\mathbb{F}_{2^n}$ for some $c \in \mathbb{F}_{2^n}^*$, then t is a planar exponent of $\mathbb{F}_{2^n}$.

Exponent t	Which field	Reference
2^k	every	trivial
2^k+1	$\mathbb{F}_{2^{2k}}$	Schmidt and Zhou
$4^k(4^k+1)$	$\mathbb{F}_{2^{6k}}$	Scherr and Zieve

Conjecture

This list is complete.

Theorem (Schmidt, Zhou)

Let t be an integer satisfying $\gcd(t-2, 2^n-2) = 1$. Then t is a planar exponent of $\mathbb{F}_{2^n}$ if and only if t is a power of 2.

Exceptional planar exponents

An integer t is an exceptional planar exponent if t is a planar exponent of $\mathbb{F}_{2^n}$ for infinitely many n.

Exceptional planar exponents

An integer t is an exceptional planar exponent if t is a planar exponent of $\mathbb{F}_{2^n}$ for infinitely many n.

Exponent t	Which field	Reference
2^k	every	trivial
2^k+1	$\mathbb{F}_{2^{2k}}$	Schmidt and Zhou
$4^k(4^k+1)$	$\mathbb{F}_{2^{6k}}$	Scherr and Zieve

Exceptional planar exponents

An integer t is an exceptional planar exponent if t is a planar exponent of $\mathbb{F}_{2^n}$ for infinitely many n.

Exponent t	Which field	Reference
2^k	every	trivial
2^k+1	$\mathbb{F}_{2^{2k}}$	Schmidt and Zhou
$4^k(4^k+1)$	$\mathbb{F}_{2^{6k}}$	Scherr and Zieve

Conjecture

If t is an exceptional planar exponent then $t = 2^k$ for some k.

Exceptional planar exponents

Theorem (Schmidt, Zhou)

If t is an odd exceptional planar exponent, then $t = 1$.

Exceptional planar exponents

Theorem (Schmidt, Zhou)

If t is an odd exceptional planar exponent, then $t = 1$.

- define a curve;

Exceptional planar exponents

Theorem (Schmidt, Zhou)

If t is an odd exceptional planar exponent, then $t = 1$.

- define a curve;
- show the existence of an absolute irreducible component;

Exceptional planar exponents

Theorem (Schmidt, Zhou)

If t is an odd exceptional planar exponent, then $t = 1$.

- define a curve;
- show the existence of an absolute irreducible component;
- use Weil bound.

Exceptional planar exponents

Theorem (Schmidt, Zhou)

If t is an odd exceptional planar exponent, then $t = 1$.

- define a curve;
- show the existence of an absolute irreducible component;
- use Weil bound.

Theorem (Müller, Zieve)

If t is an exceptional planar exponent then t is a power of 2.

Planar Boolean functions

Theorem (Zhou)

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a mapping satisfying* $f(0) = 0$ *and* $\mathrm{Im}(f) = \{0, \xi\}$ *with* $\xi \neq 0$.

Planar Boolean functions

Theorem (Zhou)

Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *be a mapping satisfying* $f(0) = 0$ *and* $\mathrm{Im}(f) = \{0, \xi\}$ *with* $\xi \neq 0$. *Then* f *is a planar mapping if and only if* f *is a linearized polynomial.*

Many open questions...

Planar functions over fields of characteristic two

Yue Zhou
joint work with Kai-Uwe Schmidt

Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, Germany

June 11, 2013