Two results on planar functions

Alexander Pott
(Gohar Kyureghyan, Yue Zhou, Ferruh Özbudak)

Otto-von-Guericke-University Magdeburg

Basic definitions (part 1)

$F : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is quadratic if

$$F(x+a) - F(x) - F(a) + F(0)$$

is linear for all a.

Example. $F(x) = x^2$ for any p, $F(x) = x^4$ for $p = 3$:

$$(x+a)^4 - x^4 - a^4 = x^3 a - a^3 x.$$

Basic definitions (part 1)

$F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is quadratic if

$$F(x+a) - F(x) - F(a) + F(0)$$

is linear for all a.

Example. $F(x) = x^2$ for any p, $F(x) = x^4$ for $p = 3$:

$$(x+a)^4 - x^4 - a^4 = x^3 a - a^3 x.$$

$F : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is planar or perfect nonlinear (PN) if

$$F(x+a) - F(x)$$

is a permutation for all $a \neq 0$.

Example. $F(x) = x^2$, p odd:

$$(x+a)^2 - x^2 = 2xa + a^2$$

Basic definitions (part 2)

Remark. No planar functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$:

$$F(x+a) + F(x) = F((x+a)+a) + F(x+a)$$

$F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is almost perfect nonlinear (*APN*) if

$$F(x+a) - F(x)$$

is $2 - -1$ for all $a \neq 0$.

Important remark. Quadratic is not invariant under equivalence.

Examples on $\mathbb{F}_p^n$

APN: many power mappings, for instance x^{2^k+1} (quadratic, GOLD) and $x^{2^{2k}-2^k+1}$ (non quadratic, KASAMI): $\gcd(n,k)=1$.

PN: many power mappings, for instance x^2 or x^{p^k+1}: $n/\gcd(n,k)$ odd (quadratic).

Examples on $\mathbb{F}_p^n$

APN: many power mappings, for instance x^{2^k+1} (quadratic, GOLD) and $x^{2^{2k}-2^k+1}$ (non quadratic, KASAMI): $\gcd(n,k)=1$.

PN: many power mappings, for instance x^2 or x^{p^k+1}: $n/\gcd(n,k)$ odd (quadratic).

Proof method. (quadratic) Check kernel of $F(x+a)-F(x)-F(a)+F(0)$, for instance for x^{p^k+1}:

$$(x+a)^{p^k+1}-x^{p^k+1}-a^{p^k+1}=x^{p^k}a+a^{p^k}x=a^{p^k}\cdot(y^{p^k}+y)$$

Condition: $y^{p^k-1}=-1$.

What is known and what we want to know

	quadratic	not quadratic
APN		
PN		

What is known and what we want to know

	quadratic	not quadratic
APN	very many	
PN		

- EDEL, KYUREGHYAN, P. (2006), then many authors, for instance BUDAGHYAN, CARLET, LEANDER, BRACKEN, MARKIN, MCGUIRE

What is known and what we want to know

	quadratic	not quadratic
APN	very many	
PN	many	

- EDEL, KYUREGHYAN, P. (2006), then many authors, for instance BUDAGHYAN, CARLET, LEANDER, BRACKEN, MARKIN, MCGUIRE
- ALBERT, DIXON(classical), BIERBRAUER, ZHA, KYUREGHYAN, WANG, G. WENG (more recent)

What is known and what we want to know

	quadratic	not quadratic
APN	very many	
PN	many	only 1

- EDEL, KYUREGHYAN, P. (2006), then many authors, for instance BUDAGHYAN, CARLET, LEANDER, BRACKEN, MARKIN, MCGUIRE
- ALBERT, DIXON(classical), BIERBRAUER, ZHA, KYUREGHYAN, WANG, G. WENG (more recent)
- COULTER, MATTHEWS (1998)

What is known and what we want to know

	quadratic	not quadratic
APN	very many	only a few, one sporadic
PN	many	only 1

- EDEL, KYUREGHYAN, P. (2006), then many authors, for instance BUDAGHYAN, CARLET, LEANDER, BRACKEN, MARKIN, MCGUIRE
- ALBERT, DIXON(classical), BIERBRAUER, ZHA, KYUREGHYAN, WANG, G. WENG (more recent)
- COULTER, MATTHEWS (1998)
- WELCH, KASAMI (classical), EDEL, P. (2009)

What is known and what we want to know

	quadratic	not quadratic
APN	very many	only a few, one sporadic
PN	many	only 1

- EDEL, KYUREGHYAN, P. (2006), then many authors, for instance BUDAGHYAN, CARLET, LEANDER, BRACKEN, MARKIN, MCGUIRE
- ALBERT, DIXON(classical), BIERBRAUER, ZHA, KYUREGHYAN, WANG, G. WENG (more recent)
- COULTER, MATTHEWS (1998)
- WELCH, KASAMI (classical), EDEL, P. (2009)

	quadratic	not quadratic
APN	exponentially many	many
PN	very many	more than 1?

Permutation APN if n even

- F quadratic: no permutation.
- There is only one permutation APN known! It has $n = 6$ and is equivalent to a quadratic function. **Remember:** Quadratic is not invariant under equivalence.
- BROWNING, DILLON, MCQUISTAN, WOLFE 2010
- Are there more?
- Related to rowspace (code) of

$$\begin{pmatrix} 1 & \cdots & 1 \\ \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{pmatrix}_{x \in \mathbb{F}_2^n}.$$

The graph of a planar function $F : \mathbb{F}_q \to \mathbb{F}_q$

The graph

$$G_F := \{(x, F(x)) \ : \ x \in \mathbb{F}_q\}$$

and its shifts (translates)

$$G_F + (a, b) := \{(x + a, F(x) + b) \ : \ x \in \mathbb{F}_q\}.$$

The graph of a planar function $F : \mathbb{F}_q \to \mathbb{F}_q$

The graph

$$G_F := \{(x, F(x)) \ : \ x \in \mathbb{F}_q\}$$

and its shifts (translates)

$$G_F + (a, b) := \{(x + a, F(x) + b) \ : \ x \in \mathbb{F}_q\}.$$

F planar, then

$$\sharp\ G_F \cap [G_F + (a, b)] = 1,$$

F APN, then

$$\sharp\ G_F \cap [G_F + (a, b)] = 0/2$$

for all $a, b \in \mathbb{F}_p^n$, $a \neq 0$.

All the information is in the graph.

Projective plane

Let G, H be groups. $F : G \to H$ is planar if $F(x + a) - F(x)$ is bijective G to H.

- points: elements in $G \times H$
- lines: $G_F + (a, b)$

This is a projective plane (minus one parallel class and line at infinity) if and only if F is planar.

$F(x) = x^2$: Desarguesian plane.

Replace G_F by any subset of any group?

Semifields

- F quadratic planar function on $\mathbb{F}_q$ with $F(0) = 0$, then

$$x * y := \frac{F(x+y) - F(x) - F(y)}{2}$$

  defines a pre-semifield (field without associativity of multiplication and without identity).
- Additive structure of a semifield: elementary-abelian.
- New multiplication (with identity): $x \cdot y := x' * y'$ with $a * x' = x, \;\; a * y' = y$, then $(a * a) \cdot y = y$ (semifield: field without associativity).
- Any commutative pre-semifield $*$ defines planar function

$$F(x) := x * x.$$

Isomorphism

- Semifield planes: Translation planes plus.

Question. Isomorphism of the plane on the level of semifields/planar functions?

Hope. Planes are isomorphic if and only if the planar functions are equivalent or isomorphic.

Equivalence for planar functions/semifields

- Functions F and F' are equivalent if a linear mapping $\mathcal{L}$ maps G_F to $G_{F'} + (a, b)$ (equivalence concept for difference sets!)
- Semifields with multiplication $*$ and $\odot$ are isotopic if

$$\mathcal{L}(x) * \mathcal{M}(y) = \mathcal{N}(x \odot y)$$

for linear bijective mappings $\mathcal{L}, \mathcal{M}, \mathcal{N}$ on $\mathbb{F}_p^n$.

Equivalence for planar functions/semifields

- Functions F and F' are equivalent if a linear mapping $\mathcal{L}$ maps G_F to $G_{F'} + (a, b)$ (equivalence concept for difference sets!)
- Semifields with multiplication $*$ and $\odot$ are isotopic if

$$\mathcal{L}(x) * \mathcal{M}(y) = \mathcal{N}(x \odot y)$$

  for linear bijective mappings $\mathcal{L}, \mathcal{M}, \mathcal{N}$ on $\mathbb{F}_p^n$.

Theorem. Semifield planes are isotopic if and only if the planes are isomorphic (ALBERT).

Theorem. For n odd, planar functions on $\mathbb{F}_p^n$ are isomorphic if and only if the functions are equivalent COULTER, HENDERSON. If n is even, there are counterexamples ZHOU, P., POLVERINO, MARINO.

Relative difference sets

Isotopism does not preserve commutativity! But planar functions only exist for commutative semifields!

Alternative. Γ group of order $m \cdot n$, N normal subgroup of order m, $R \subset \Gamma$, $|R| = n$ is a

$$(n, m, n, \frac{n}{m}) \text{ -relative difference set } (RDS) \text{ if}$$

$$r - r' = g, \quad r, r' \in R$$

has $\frac{n}{m}$ solutions for $g \in G \setminus N$, and no solution if $g \in N \setminus \{0\}$.

Example. F planar, then G_F is an RDS in $\mathbb{F}_p^n \times \mathbb{F}_p^n$ relative to $\{0\} \times \mathbb{F}_p^n$.

Some notes

- Non-commutative semifields give non-abelian RDS's.
- Planar functions (abelian relative difference sets) may be a good way to construct semifields, but perhaps not the best.
- But planar functions or their non-Abelian analogue may be used to construct planes which are not semifield planes COULTER, MATTHEWS 1998:

$$x^{\frac{3^k+1}{2}} \quad \text{on} \quad \mathbb{F}_{3^n}$$

- Interesting: Image sets of planar functions! (see Qiang's talk)

Characteristic 2: Planarity generalization

... almost perfect nonlinear ... NO plane, but semibiplane

Semifields and relative difference sets can be generalized!

Analogue of planar function is RDS in

$$\mathbb{Z}_4 \times \ldots, \times \mathbb{Z}_4$$

relative to

$$\mathbb{Z}_2 \times \ldots, \times \mathbb{Z}_2.$$

Example. $\{(0,0),(0,1),(1,0),(3,3)\} \subset \mathbb{Z}_4 \times \mathbb{Z}_4$.

- Semifields give RDS's.
- There are many commutative ones: KANTOR.

Connections

Planar functions are related to

- almost perfect nonlinear functions
- relative difference sets in $\mathbb{Z}_4^n$ (semifields)

Connections between these items:

- PN vs. APN: KYUREGHYAN, BIERBRAUER.
- APN vs. semifields: duality (KNUTH cube), non-Abelian difference set analogue (P.), KANTOR for APN?

New functions: Local change

$$F : \mathbb{F}_p^n \to \mathbb{F}_p^n, \quad F = \begin{pmatrix} F_1 \\ \vdots \\ F_n \end{pmatrix}$$

- change one (or more) coordinate functions F_i.
  Budaghyan, Carlet, P., Edel, Dillon if $p = 2$.
- Similarly: Permutation polynomials.
- Planar: Zhou, P.

Get away from finite fields

- PN (or planar) and APN are properties just of the additive group of a vector space.
- p odd, then F_i are bent: $F_i(x+a) - F_i(x) = b$ has p^{n-1} solutions.
- Millions of bent functions, try to combine?
- All F_i bent does not imply planarity: Also linear combinations must be bent!

A compromise

Decomposition

$$\mathbb{F}_{p^{2m}} = \mathbb{F}_{p^m} \times \mathbb{F}_{p^m}$$

used in bent functions, APN (Carlet), PN (Bierbrauer):

$$F(x) = \begin{pmatrix} F_1(x) \\ F_2(x) \end{pmatrix},$$

where $F_1, F_2 : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$.

Choices for F_1, F_2:

- F_1, F_2: Projections from planar functions
- $(x, F_1(x))$ is a $(p^{2m}, p^m, p^{2m}, p^m)$-relative difference set.

Our (P., ZHOU) contribution

Theorem. Let m, k be positive integers, such that $\frac{m}{\gcd(m,k)}$ is odd. Define $x \circ_k y = x^{p^k} y + y^{p^k} x$. For elements $a, b \in \mathbb{F}_{p^{2m}}$, define

$$F(a, b) := (a \circ_k a + u(b \circ_k b)^\sigma, 2ab),$$

where u is a non-square element in $\mathbb{F}_{p^m}$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{p^m})$. Then F is planar.

An interesting note

Theorem. Let $\psi : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be any permutation, and let $\varphi_1, \varphi_2 : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ be arbitrary functions. Then the mapping

$$f : \mathbb{F}_{p^m}^2 \to \mathbb{F}_{p^m}^2, \quad \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x^2 + \varphi_1(y) \\ 2x \cdot \psi(y) + \varphi_2(y) \end{pmatrix}$$

is planar if and only if

$$g : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}, \quad y \mapsto -u^2 \cdot \psi^2(y) + u \cdot w \cdot \psi(y) + \varphi_1(y) + u \cdot \varphi_2(y)$$

is planar for all $u, w \in \mathbb{F}_{p^m}$.

Proof uses character theory (Gaussian sums).

$x^{q^2+q} + ux^2$ on $\mathbb{F}_{q^3}$, $q \equiv 1 \bmod 3$

- Planar monomials: Do not expect more examples.
- Binomials: May be useful in the "subfield" construction.
- Related to the existence of nontrivial solution of

$$x^{q^2-1} + x^{q-1} + 2uy^{3(q-1)}$$

- No planar function if $q \not\equiv 1 \bmod 3$

Theorem and Conjecture (P., KYUREGHYAN, ÖZBUDAK

G subgroup of $\mathbb{F}_q^3$ of order q^2+q+1, $H < G$, $|H| = \frac{1}{3}|G|$.

Theorem. $F_u = x^{q^2-1} + x^{q-1} + 2uy^{3(q-1)}$ is planar if $\alpha \in -(G \setminus H)$ or $u \in \frac{1}{2}(G \setminus H)$.

Conjecture. That's all.

We also determined for many u the number of solutions of $x^{q^2-1} + x^{q-1} + 2uy^{3(q-1)}$

Conclusions

- Planar functions are related to APN functions and to semifields of even characteristic. Is there a nice connection between semifields and APN functions?
- Find families of planar/APN functions using
  - KANTOR for semifields of even characteristic.
  - subfields
  - coordinate functions
  - ???
- Characterize monomials/binomials which are planar/APN.
- Find more nonquadratic examples.