A projection construction for semifields and APN functions in characteristic 2

Stefano Marcugini

joint work with
J. Bierbrauer, D. Bartoli, M. Giulietti, F. Pambianco

ACCT 2014

Outline

- A family of semifields in even characteristic
- A link to APN functions

p=2, the case $B(2, m, s, l, C_1, C_2)$

The definition of the fields

Let $q = 2^m$
$L = GF(q) \subset F = GF(q^2)$
$T, N : F \longrightarrow L$ the trace and norm.

Let $\mu \in L$ be of absolute trace $= 1$ and $z \in F$ s. t. $z^2 + z = \mu$.

Then $z \notin L$ and we use $1, z$ as a basis of $F|L$:

$$x = a + bz = (a, b) \text{ where } a, b \in L$$

$Re(x) := a \;\; Im(x) := b.$

p=2, the case $B(2, m, s, l, C_1, C_2)$

Definition 1

Let $s < 2m, \sigma = 2^s, \qquad 0 \neq l \in L$ such that $l \notin L^{\sigma-1}$.

$C_1, C_2 \in F$ such that the following equivalent conditions are satisfied:

- $T(C_1 x\overline{x}^\sigma + C_2 x^{\sigma+1}) \neq 0$ for all $0 \neq x \in F$.
- $P_{C_1,C_2,s}(X) = C_2 X^{\sigma+1} + \overline{C_1} X^\sigma + C_1 X + \overline{C_2} \in F[X]$ has no root of norm 1.

Define a product on F by

$$x * y = T((C_1 y^\sigma + C_2 \overline{y}^\sigma)x) + lT((\overline{C_1} y + C_2 \overline{y})x^\sigma) + T(xy)z$$

p=2, the case $B(2, m, s, l, C_1, C_2)$

Theorem

Under the conditions of Definition 1 $(F, +, *)$ *is a presemifield* $B(2, m, s, l, C_1, C_2)$ *on* F.

Proof.

Assume $x * y = 0, xy \neq 0$.
The imaginary part shows $y = e\overline{x}$ for $e \in L$.
The real part factorizes:

$$(e^\sigma + le)T(C_1 x\overline{x}^\sigma + C_2 x^{\sigma+1}) = 0.$$

The first factor is nonzero by the condition on l,
the non-vanishing of the trace term is the first condition of Definition 1. □

p=2, the case $B(2, m, s, l, C_1, C_2)$

Special cases

Let $C_i = (v_i, h_i)$.

$X = 1 \Rightarrow T(C_1) = h_1 \neq h_2 = T(C_2)$.

$x, y \in L \Rightarrow x * y = (h_1 + h_2)(xy^\sigma + lx^\sigma y)$, a generalized Albert twisted field.

$Im(x * y)$ is isotopic to the imaginary part of field multiplication
$Re(x * y)$ is isotopic to the real part of generalized twisted field.

$B(2, m, s, l, C_1, C_2)$ is not isotopic to the field.

p=2, the case $B(2, m, s, l, C_1, C_2)$

The question of commutativity

Theorem

$B(2, m, s, l, C_1, C_2)$ for $s < m$ is isotopic to commutative if and only if $C_1 C_2 \neq 0$ and there is $0 \neq x \in F$ such that

$$(C_1/\overline{C_2})x + l(\overline{C_1}/\overline{C_2})x^{\sigma} = (C_2/\overline{C_1})x + l(\overline{C_2}/\overline{C_1})\overline{x}^{\sigma} \in L$$

A computer search showed that there is no solution in case $m \leq 6$.

Conjecture

$B(2, m, s, l, C_1, C_2)$ is never isotopic to commutative.

p=2, the case $B(2, m, s, l, C_1, C_2)$

The question of commutativity

Theorem

$B(2, m, s, l, C_1, C_2)$ for $s < m$ is isotopic to commutative if and only if $C_1 C_2 \neq 0$ and there is $0 \neq x \in F$ such that

$$(C_1/\overline{C_2})x + l(\overline{C_1}/\overline{C_2})x^{\sigma} = (C_2/\overline{C_1})x + l(\overline{C_2}/\overline{C_1})\overline{x}^{\sigma} \in L$$

A computer search showed that there is no solution in case $m \leq 6$.

Conjecture

$B(2, m, s, l, C_1, C_2)$ is never isotopic to commutative.

Planar functions and a basic equivalence (p odd)

Quadratic polynomial (p odd)

$f = f(X)$ is quadratic if its monomial have exponents $p^i + p^j$

Quadratic form $f \longrightarrow$ bilinear form $*$

$x * y = (1/2)(f(x+y) - f(x) - f(y))$

Bilinear form $* \longrightarrow$ quadratic form f

$f(x) = x * x.$

Definition

f is planar if $x * y \neq 0$ for $xy \neq 0$.

The following are equivalent (p odd)

- Quadratic planar (PN) functions $f : F \longrightarrow F$
- Commutative presemifields $(F, *)$

Planar functions and a basic equivalence (p odd)

Quadratic polynomial (p odd)

$f = f(X)$ is quadratic if its monomial have exponents $p^i + p^j$

Quadratic form $f \longrightarrow$ bilinear form $*$

$x * y = (1/2)(f(x+y) - f(x) - f(y))$

Bilinear form $* \longrightarrow$ quadratic form f

$f(x) = x * x.$

Definition

f is planar if $x * y \neq 0$ for $xy \neq 0$.

The following are equivalent (p odd)

- Quadratic planar (PN) functions $f : F \longrightarrow F$
- Commutative presemifields $(F, *)$

Planar functions and a basic equivalence (p odd)

Quadratic polynomial (p odd)

$f = f(X)$ is quadratic if its monomial have exponents $p^i + p^j$

Quadratic form $f \longrightarrow$ bilinear form $*$

$x * y = (1/2)(f(x + y) - f(x) - f(y))$

Bilinear form $* \longrightarrow$ quadratic form f

$f(x) = x * x.$

Definition

f is planar if $x * y \neq 0$ for $xy \neq 0$.

The following are equivalent (p odd)

- Quadratic planar (PN) functions $f : F \longrightarrow F$
- Commutative presemifields $(F, *)$

PN and APN functions

Equivalent expressions, different paradigms

$f : F \longrightarrow F$

$\delta_{f,a}(x) = x * a = f(x + a) - f(x) - f(a).$

- Additive directional derivative at $a \in F$
- Product
- Polarization

Definition: f is

- PN (or planar) if $x * a$ is one-to-one ($a \neq 0, p$ odd)
- APN if $x * a$ is two-to-one ($a \neq 0, p = 2$)

PN and APN functions

Equivalent expressions, different paradigms

$f : F \longrightarrow F$

$\delta_{f,a}(x) = x * a = f(x+a) - f(x) - f(a).$

- Additive directional derivative at $a \in F$
- Product
- Polarization

Definition: f is

- PN (or planar) if $x * a$ is one-to-one ($a \neq 0, p$ odd)
- APN if $x * a$ is two-to-one ($a \neq 0, p = 2$)

Motivations

From cryptography, when $p = 2$

Destroying linearity: protection against differential attacks (S-boxes)
Extremal correlation properties
Crooked functions, bent functions, ...

From coding theory

Cyclic codes, codes of Preparata type

Geometric representations, $p = 2$

Dual hyperovals, semi-biplanes

Motivations

From cryptography, when $p = 2$

Destroying linearity: protection against differential attacks (S-boxes)
Extremal correlation properties
Crooked functions, bent functions, ...

From coding theory

Cyclic codes, codes of Preparata type

Geometric representations, $p = 2$

Dual hyperovals, semi-biplanes

Motivations

From cryptography, when $p = 2$

Destroying linearity: protection against differential attacks (S-boxes)
Extremal correlation properties
Crooked functions, bent functions, ...

From coding theory

Cyclic codes, codes of Preparata type

Geometric representations, $p = 2$

Dual hyperovals, semi-biplanes

APN functions

Definition

$F = \mathbb{F}_{2^r}$

$f(x) = \sum_{i<j} a_{ij} X^{2^i+2^j} \in F[X]$ (Dembowski-Ostrom polynomial)

let $x * y = f(x+y) + f(x) + f(y)$ (polarization) of $f(x)$

$f(x)$ is called a quadratic APN function if

$$x * y = 0 \text{ is equivalent to } xy = 0 \text{ or } x = y.$$

APN functions

Theorem

Let

$$f(x) = T(x^{\sigma+1} + C_1 x\overline{x}^{\sigma} + N(x)) + N(x)^{\sigma} z.$$

Then the following are equivalent:

- $f(x) : F \longrightarrow F$ *is a (quadratic) APN function,*
- $\gcd(s, m) = 1$ *and*
  $P_{C_1,1,s}(X) = X^{\sigma+1} + \overline{C_1} X^{\sigma} + C_1 X + 1 \in F[X]$
  has no roots $z \in F = \mathbb{F}_{2^{2m}}$ *such that* $N(z) = 1$.

APN functions

Proof.

Let $x * y$ be the polarization of $f(x)$.
Applying the invertible linear mapping $(a, b) \mapsto (a + b^{1/\sigma}, b)$ we may cancel $N(x)$ in the real part of $f(x)$ obtaining:

$$x * y = T(xy^\sigma + x^\sigma y + C_1 x\overline{y}^\sigma + C_1 \overline{x}^\sigma y) + T((x\overline{y})^\sigma)z.$$

Assume $x * y = 0$ where $xy \neq 0$.
The imaginary part shows $y = ex$ for $e \in L$.
The real part shows $(e^\sigma + e)(x^{\sigma+1} + C_1 x\overline{x}^\sigma) \in L$.
Assume $e \neq 1$. The condition $\gcd(s, m) = 1$ shows $e^\sigma + e \neq 0$.
It follows that the second factor has to be in L.
As before write out the trace, divide by $\overline{x}^{\sigma+1}$.
This yields the familiar condition on $P_{C_1,1,s}(X)$.

APN functions

The theorem describes the APN hexanomials as constructed by [Budaghyan, Carlet 2008] which were further studied among others in [Bluher 2013].

THANKS FOR THE ATTENTION!