Fourteenth International Workshop on Algebraic and Combinatorial Coding Theory
September 7–13, 2014, Svetlogorsk (Kaliningrad region), Russia *pp. 46–50*

A projection construction for semifields and APN functions in characteristic 2

Daniele Bartoli, Massimo Giulietti, Stefano Marcugini, Fernanda Pambianco
{daniele.bartoli,gino,fernanda}@dmi.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, Italy
Jürgen Bierbrauer
Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA

Abstract. Semifields (or: non-associative division algebras) are the algebraic structures which coordinatize an important class of geometric objects, projective planes which are translation planes and also the duals of translation planes. We apply the projection construction (see [2]) in characteristic 2. Finally we give an application of the projection construction to APN functions. Those are a second analogue, besides semifields in characteristic 2, of the theory of planar functions. They have important applications in cryptography and coding theory (see [6]).

1 The background

A large family of (pre)semifields of odd order is constructed in [2] as follows. Let p be an odd prime, $q = p^m, L = \mathbb{F}_q \subset F = \mathbb{F}_{q^2}$. Let $\overline{x} = x^q$ and $T : F \longrightarrow L$ the trace. Let $0 < s < 2m, \sigma = p^s, l \in L^*$ such that $-l \notin (L^*)^{\sigma-1}$. Further let $C_1, C_2 \in F$ such that the polynomial

$$P_{C_1,C_2,s}(X) = C_2X^{\sigma+1} + \overline{C_1}X^{\sigma} + C_1X + \overline{C_2} \in F[X]$$

has no root z such that $z^{q+1} = 1$. Then presemifields $B(p, m, s, l, C_1, C_2)$ of order p^{2m} are defined such that the addition coincides with the addition in the field F and the multiplication is given by

$$x * y = (1/2)T((C_1y^{\sigma} + C_2\overline{y}^{\sigma})x) + (l/2)T((\overline{C_1}y + C_2\overline{y})x^{\sigma}) + (xy - \overline{xy})/2 \quad (1)$$

which clearly is identical to

$$x * y = c_0(y)x + c_m(y)\overline{x} + c_s(y)x^{\sigma} + c_{m+s}(y)\overline{x}^{\sigma} \quad (2)$$

where

$$c_0(y) = (1/2)(y + C_1y^\sigma + C_2\overline{y}^\sigma), c_m(y) = (1/2)(-\overline{y} + \overline{C_2}y^\sigma + \overline{C_1}\overline{y}^\sigma)$$

and

$$c_s(y) = (l/2)(\overline{C_1}y + C_2\overline{y}), c_{m+s}(y) = \overline{c_s(y)}.$$

It is important here to realize that F can be written as a direct sum

$$F = L \oplus L\omega \tag{3}$$

where ω has trace $T(\omega) = 0$ and $L\omega = \{x \mid x \in F, T(x) = 0\}$. Then $\mu = \omega^2$ is a non-square in L. This comes down to describe the quadratic extension F of L by the irreducible polynomial $X^2 - \mu$ where μ is a non-square in L. It is then natural to use the language of pairs: Let $x = a + b\omega$. We write

$$x = (\underbrace{a}_{Re}, \underbrace{b}_{Im})$$

and refer to $a = Re(x)$ and $b = Im(x)$ as the real and imaginary part of x, respectively. This terminology is natural as the first two terms of Equation (1) are in the subfield L and the last term is $(ad+bc)\omega \in L\omega$. It follows that $x*y = 0$ if and only if $ad+bc = 0$ and also $Re(x*y) = 0$. This greatly simplifies the proof that $B(p, m, s, l, C_1, C_2)$ is indeed a presemifield (equivalently: $x * y = 0$ only if $xy = 0$). For any presemifield $(F, +, *)$ where F is a field and the addition is as in the field F, we define the **associated semifield** $(F, +, \circ)$ by

$$x \circ y := \beta\big(\gamma(x) * y\big). \tag{4}$$

where $\beta, \gamma \colon F \to F$ are invertible linear mappings defined by

$$1 * \beta(x) = x \quad \text{and} \quad \gamma(x) * 1 = 1 * x \tag{5}$$

It is then easy to verify that $(F, +, \circ)$ is indeed a semifield with $1 \in F$ as neutral element of multiplication.

We want to extend the definition of $B(p, m, s, l, C_1, C_2)$ to the case $p = 2$ and to study some of the basic properties of the family $B(2, m, s, l, C_1, C_2)$. Among those properties are the dimensions of the nuclei and the question when our presemifields are isotopic to commutative semifields. In odd characteristic the commutative semifields from Budaghyan-Helleseth [4] are contained in our family (cases $C_1C_2 = 0$ and $\{C_1, C_2\} \subset L$). It is therefore an interesting question to decide if any of the $B(2, m, s, l, C_1, C_2)$ are isotopic to commutative. The most important among the facts that do not carry over from the odd characteristic case is the direct sum decomposition Equation (3). This needs to be modified.

2 A standard situation in characteristic 2

Let $Q = 2^m, F = GF(Q^2) \supset L = GF(Q)$ and $T, N : F \longrightarrow L$ the norm and trace. Let $\mu \in L$ be of absolute trace $= 1$ and $z \in F$ such that $z^2 + z = \mu$. Then $z \notin L$ and we use $1, z$ as a basis of $F|L$. In particular we write $x = a + bz = (a, b)$ where $a, b \in L$ and refer to a, b as the real and imaginary part of x, respectively.

Let $s < 2m, \sigma = 2^s$ and $K_1 = \mathbb{F}_{2^{\gcd(s,m)}}$ the fixed field of σ in L. Then $z^4 = z^2 + \mu^2 = z + \mu^2 + \mu$. Continuing like that we obtain the following:

Lemma 6. *Let $\mu_s = \sum_{i=0}^{s-1} \mu^{2^i}$. Then $z^\sigma = z + \mu_s$ and $x^\sigma = (a^\sigma + \mu_s b^\sigma, b^\sigma)$.*

In particular $\mu_1 = \mu, \mu_2 = \mu + \mu^2$ and $\mu_m = tr_{L|\mathbb{F}_2}(\mu) = 1$ (because of the transitivity of the trace) and $\overline{z} = z^{2^m} = z + 1$. Further $\mu_{s+m} = \mu_s + 1$. We have $\overline{x} = (a + b, b), T(x) = b$ and

$$(a, b)(c, d) = (ac + bd\mu, ad + bc + bd)$$

In particular

$$1/z = (1/\mu, 1/\mu) \text{ and } 1/(a, b) = (1/D)(a + b, b),$$

where $D = a^2 + ab + \mu b^2$. The conjugates of x are

$$x^2 = (a^2+\mu b^2, b^2), x^4 = (a^4+(\mu^2+\mu)b^4, b^4), \dots x^\sigma = (a^\sigma+(\mu^{2^{s-1}}+\dots+\mu)b^\sigma, b^\sigma).$$

Let $\mu' = \mu^{2^{s-1}} + \dots + \mu$. In the special case when m is odd we choose $\mu = 1$ and obtain $z = \omega \in \mathbb{F}_4$.

3 The definition

Definition 7. *Let the following equivalent conditions be 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.

Choose $0 \neq l \in L$ such that $l \notin L^{\sigma-1}$. Define a product on F by

$$x * y = T((C_1 y^\sigma + C_2 \overline{y}^\sigma)x) + lT((\overline{C_1} y + C_2 \overline{y})x^\sigma) + T(xy)z \tag{8}$$

Theorem 9. *Under the conditions of Definition 7 $(F, +, *)$ 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 second condition above. □

Let $C_i = (v_i, h_i)$. Case $X = 1$ shows that $T(C_1) = h_1 \neq h_2$. The restriction to $x, y \in L$ is $x * y = (h_1 + h_2)(xy^\sigma + lx^\sigma y)$, a generalized Albert twisted field. In particular $B(2, m, s, l, C_1, C_2)$ is not isotopic to the field. This restriction also explains the projection construction in this case. The imaginary part of $x * y$ is isotopic to the imaginary part of field multiplication, the real part of $x * y$ is isotopic to the real part of generalized twisted field. More precisely, with $x = (a, b), y = (c, d)$ and $c' = c + d$ the presemifield multiplication in the language of pairs is

$$x*y = (p_1 ac'^\sigma + lp_1 a^\sigma c' + p_2 bc'^\sigma + lp_2 a^\sigma d + p_3 ad^\sigma + lp_3 b^\sigma c' + p_4 bd^\sigma + lp_4 b^\sigma d, ad + bc').$$

Here $p_1 = h_1 + h_2, p_2 = v_1 + v_2 + h_1 + h_2, p_3 = v_1 + v_2 + \mu_s h_1 + (\mu_s + 1)h_2, p_4 = \mu_s v_1 + (\mu_s + 1)v_2 + (\mu_s + \mu)h_1 + (\mu_s + \mu + 1)h_2$.

4 The question of commutativity

Theorem 10. *$B(2, m, s, l, C_1, C_2)$ for $s < m$ is isotopic to commutative if and only if $C_1C_2 \neq 0$ 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 $m = 4, s = 2$. We conjecture that $B(2, m, s, l, C_1, C_2)$ is never isotopic to commutative.

5 A link to APN functions

Commutative semifields in odd characteristic $(F, +, *)$ can be described equivalently by the corresponding quadratic planar function $f(x) = x*x$. The reason is that $x*x$ is recovered from $f(x)$ by the polarization formula. This is not true for non-commutative semifields and it is not true in characteristic 2. Quadratic planar functions possess at least two different analogues in characteristic 2: commutative semifields and APN (almost perfectly nonlinear) functions. The latter form a core part of the theory of cryptographic S-boxes. They also describe the binary cyclic codes of minimum distance 5 (see [6] and [1], p. 210). More precisely, let $F = \mathbb{F}_{2^r}$ and $f(x) = \sum_{i<j} a_{ij} X^{2^i + 2^j} \in F[X]$ (such polynomials are known as **Dembowski-Ostrom polynomials**). Define the **polarization** of $f(x)$ by $x * y = f(x + y) + f(x) + f(y)$. Then $f(x)$ is called a **quadratic APN function** if $x*y$ is equivalent to $xy = 0$ or $x = y$. The projection method works also in this context, and the APN hexanomials of Budaghyan-Carlet [5] are characteristic 2 analogues of a special case of the family $B(p, m, s, l, 0, C_2)$ in odd characteristic. Here is an example of this type of construction in the situation of Section 2.

Theorem 11. *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* $N(z) = 1$.

Proof. Let $x * y$ be the polarization of $f(x)$. The invertible linear mapping $(a, b) \mapsto (a + b^{1/\sigma}, b)$ shows that we may cancel the term $N(x)$ in the real part of $f(x)$ and obtain the polarization

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

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 $P_{C_1,1,s}(X)$. □

Observe that the polynomial $P_{C_1,1,s}(X)$ and the condition it needs to satisfy are the same as we encountered in odd characteristic in Section 1. Theorem 11 describes the APN hexanomials as constructed by Budaghyan-Carlet, [5] which were further studied among others in [3].

References

[1] J. Bierbrauer: *Introduction to Coding Theory,* Chapman and Hall, CRC Press 2004.

[2] J. Bierbrauer: *Projective polynomials, a projection construction and a family of semifields,* manuscript.

[3] Antonia W. Bluher: *On existence of Budaghyan-Carlet APN hexanomials, Finite fields and their Applications* **24** (2013), 118-123.

[4] L. Budaghyan and T. Helleseth: *New commutative semifields defined by new PN multinomials, Cryptogr. Commun.* **3** (2011), 1-16.

[5] L. Budaghyan and C. Carlet: *Classes of quadratic APN trinomials and hexanomials and related structures, IEEE IT Transactions* **54** (2008), 2354–2357.

[6] C. Carlet, P. Charpin, V. Zinoviev: *Codes, bent functions and permutations suitable for DES-like cryptosystems, Designs, Codes and Cryptography* **15** (1998), 125–156.