Tatra Mt. Math. Publ. **45** (2010), 15–25
DOI: 10.2478/v10127-010-0002-0

TATRA MOUNTAINS
Mathematical Publications

PLANAR FUNCTIONS AND COMMUTATIVE SEMIFIELDS

Lilya Budaghyan — Tor Helleseth

ABSTRACT. This paper gives a short survey on planar functions and commutative semifields and considers a possible extension of CCZ-equivalence which is the most general known equivalence relation of functions preserving the planar property.

1. PN and APN functions

Let p be any prime number and n any positive integer. A function F from the field $\mathbf{F}_{p^n}$ to itself is called **planar** if all the equations

$$F(x+a)-F(x)=b, \qquad \forall\, a,b\in \mathbf{F}_{p^n}, a\neq 0 \tag{1}$$

have exactly one solution, that is, if for any non-zero element a of $\mathbf{F}_{p^n}$ the function

$$D_aF(x)=F(x+a)-F(x),$$

called the **derivative of F in the direction of** a, is a permutation. Planar functions were introduced in 1968 by Dembowski and Ostrom [18] in context of finite geometry to describe projective planes with specific properties. Since 1991 planar functions have attracted interest also from cryptography as functions with optimal resistance to differential cryptanalysis. In this context they were first considered in the work of Nyberg [32], where they were given a new name "**perfect nonlinear**" (PN) which described their important cryptographic property of being as far as possible from being linear (in certain sense). However, it is obvious that planar or PN functions exist only for p odd since if p is even and x_0 is a solution of (1) then x_0+a is a solution too, and the functions, whose derivatives D_aF, $a\in\mathbf{F}_{p^n}^*$, are 2-to-1 mappings, possess the best

2010 Mathematics Subject Classification: Primary: 94A60, 68P25; Secondary 14G50.
Keywords: commutative semifield, equivalence of functions, perfect nonlinear, planar function.
This work was supported by Norwegian Research Council and partially by the grant NIL-I-004 from Iceland, Liechtenstein and Norway through the EEA and Norwegian Financial Mechanisms.

possible resistance to differential cryptanalysis and are called **almost perfect nonlinear** (APN).

There are several equivalence relations of functions for which PN and APN properties are invariant. Due to these equivalence relations, having only one PN (or APN) function one can generate a huge class of PN (resp. APN) functions. The terminology for these equivalence relations was introduced in 2005 in [10] while the ideas behind this terminology go back to the works of Nyberg [33] and Carlet, Charpin and Zinoviev [13]. To continue we need first to recall the following definitions:

Definition 1. A function F from $\mathbf{F}_{p^n}$ to itself is called:

- **linear** if $F(x) = \sum_{0 \le i < n} a_i x^{p^i}$, $a_i \in \mathbf{F}_{p^n}$;
- **affine** if F is a sum of a linear function and a constant;
- **Dembowski-Ostrom polynomial** (DO polynomial) if $F(x) = \sum_{0 \le k,j < n} a_{kj} x^{p^k + p^j}$, $a_{ij} \in \mathbf{F}_{p^n}$;
- **quadratic** if it is a sum of a DO polynomial and an affine function.

Definitions for equivalences below are given for functions from $\mathbf{F}_{p^n}$ to itself. However, they can be naturally extended to functions from A to B, where A and B are arbitrary groups [10].

Definition 2. Two functions F and F' from $\mathbf{F}_{p^n}$ to itself are called:

- **affine equivalent** (or **linear equivalent**) if $F' = A_1 \circ F \circ A_2$, where the mappings A_1, A_2 are affine (resp. linear) permutations of $\mathbf{F}_{p^n}$;
- **extended affine equivalent** (EA-equivalent) if $F' = A_1 \circ F \circ A_2 + A$, where the mappings A, A_1, A_2 are affine, and where A_1, A_2 are permutations of $\mathbf{F}_{p^n}$;
- **Carlet-Charpin-Zinoviev equivalent** (CCZ-equivalent) if for some affine permutation $\mathcal{L}$ of $\mathbf{F}_{p^n}^2$ the image of the graph of F is the graph of F', that is, $\mathcal{L}(G_F) = G_{F'}$, where
$$G_F = \big\{(x, F(x)) | x \in \mathbf{F}_{p^n}\big\} \quad \text{and} \quad G_{F'} = \big\{(x, F'(x)) | x \in \mathbf{F}_{p^n}\big\}.$$

Although different these equivalence relations are connected to each other. It is obvious that linear equivalence is a particular case of affine equivalence, and that affine equivalence is a particular case of EA-equivalence. As it is shown in [13] EA-equivalence is a particular case of CCZ-equivalence and every permutation is CCZ-equivalent to its inverse. For quite a long time it was believed that CCZ-equivalence class of an arbitrary function F can be completely described by means of EA-equivalence and of the inverses of permutations EA-equivalent to F. In [6], [10], it is proven to be false: CCZ-equivalence is much more general. However, there are particular cases of functions for which CCZ-equivalence can be reduced to EA-equivalence. For instance, CCZ-equivalence coincides with:

- EA-equivalence for planar functions [11], [27];
- linear equivalence for DO planar functions [11];
- EA-equivalence for all functions whose derivatives are surjective [12];
- EA-equivalence for all Boolean functions [7];
- EA-equivalence for all vectorial bent functions with p even [8].

It is useful to know cases where CCZ- and EA-equivalences coincide because, in general, it is very difficult to determine whether two functions are CCZ--equivalent or not while EA-equivalence is much simpler and has a nice invariant, algebraic degree of a function.

Nowadays, CCZ-equivalence is the most general known equivalence relation of functions preserving PN and APN properties and it is appealing to find a more general equivalence for which PN and APN properties are invariants. The first attempts in this direction were made in [7], [22]. In [7] the first author and Carlet consider two functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ equivalent if the indicators of the graphs of F and F' are CCZ-equivalent. Recall that for a given function F from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ the indicator 1_{G_F} of its graph G_F is

$$1_{G_F}(x,y) = \begin{cases} 1 & \text{if } y = F(x), \\ 0, & \text{otherwise.} \end{cases}$$

However, as proven in [7], for p even that equivalence coincides with original CCZ-equivalence of functions, and we prove in Section 4 of this paper that it coincides with CCZ-equivalence for p odd as well. In [22] E d e l and P o t t present so-called "switching construction" which is proven to be an appropriate method for constructing APN functions. This approach can be used potentially for planar functions as well but it is not developed yet for this case. Basing on this construction they define an equivalence relation, called switching equivalence, over APN functions. But when considered over all functions switching equivalence does not preserve APN property, that is, if two functions are switching equivalent and one of them is APN the second is not necessarily APN.

2. Commutative presemifields and semifields

As it is shown in [18], [16] quadratic planar functions have important connection with commutative semifields. A ring with left and right distributivity and with no zero divisors is called a **presemifield**. A presemifield with a multiplicative identity is called a **semifield**. Any finite presemifield can be represented by

$$\mathbf{S} = (\mathbf{F}_{p^n}, +, \star),$$

where $(\mathbf{F}_{p^n}, +)$ is the additive group of $\mathbf{F}_{p^n}$ and $x \star y = \phi(x, y)$ with ϕ a function from $\mathbf{F}_{p^n}^2$ onto $\mathbf{F}_{p^n}$, see [16].

Let

$$\mathbf{S}_1 = (\mathbf{F}_{p^n}, +, \circ) \quad \text{and} \quad \mathbf{S}_2 = (\mathbf{F}_{p^n}, +, \star)$$

be two presemifields. They are called **isotopic** if there exist three linear permutations L, M, N over $\mathbf{F}_{p^n}$ such that

$$L(x \circ y) = M(x) \star N(y),$$

for any $x, y \in \mathbf{F}_{p^n}$. The triple (M, N, L) is called the **isotopism** between $\mathbf{S}_1$ and $\mathbf{S}_2$. If $M = N$ then $\mathbf{S}_1$ and $\mathbf{S}_2$ are called **strongly isotopic**.

Let $\mathbf{S}$ be a finite semifield. The subsets

$$\begin{aligned} N_l(\mathbf{S}) &= \big\{\alpha \in \mathbf{S} : (\alpha \star x) \star y = \alpha \star (x \star y) \text{ for all } x, y \in \mathbf{S}\big\}, \\ N_m(\mathbf{S}) &= \big\{\alpha \in \mathbf{S} : (x \star \alpha) \star y = x \star (\alpha \star y) \text{ for all } x, y \in \mathbf{S}\big\}, \\ N_r(\mathbf{S}) &= \big\{\alpha \in \mathbf{S} : (x \star y) \star \alpha = x \star (y \star \alpha) \text{ for all } x, y \in \mathbf{S}\big\}, \end{aligned}$$

are called the **left, middle** and **right nucleus** of $\mathbf{S}$, respectively, and the set $N(\mathbf{S}) = N_l(\mathbf{S}) \cap N_m(\mathbf{S}) \cap N_r(\mathbf{S})$ is called the **nucleus**. These sets are finite fields and, if $\mathbf{S}$ is commutative then $N_l(\mathbf{S}) = N_r(\mathbf{S})$. The nuclei measure how far $\mathbf{S}$ is from being associative. *The orders of the respective nuclei are invariant under isotopism* [16].

Every commutative presemifield can be transformed into a commutative semifield. Indeed, let $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$ be a commutative presemifield which does not contain an identity. To create a semifield from $\mathbf{S}$ choose any $a \in \mathbf{F}_{p^n}^*$ and define a new multiplication $\circ$ by

$$(x \star a) \circ (a \star y) = x \star y$$

for all $x, y \in \mathbf{F}_{p^n}$. Then $\mathbf{S}' = (\mathbf{F}_{p^n}, +, \circ)$ is a commutative semifield isotopic to $\mathbf{S}$ with identity $a \star a$. We say $\mathbf{S}'$ is a commutative semifield **corresponding** to the commutative presemifield $\mathbf{S}$. An isotopism between $\mathbf{S}$ and $\mathbf{S}'$ is a strong isotopism $\big(L_a(x), L_a(x), x\big)$ with a linear permutation $L_a(x) = a \star x$, see [16].

Every commutative presemifield defines a planar DO polynomial and vice versa [16]. Let F be a quadratic PN function over $\mathbf{F}_{p^n}$. Then $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$, with

$$x \star y = F(x + y) - F(x) - F(y)$$

for any $x, y \in \mathbf{F}_{p^n}$, is a commutative presemifield. We denote by

$$\mathbf{S}_F = (\mathbf{F}_{p^n}, +, \circ)$$

the commutative semifield corresponding to the commutative presemifield $\mathbf{S}$ with isotopism $\big(L_1(x), L_1(x), x\big)$ and we call $\mathbf{S}_F = (\mathbf{F}_{p^n}, +, \circ)$ the **commutative semifield defined by the quadratic PN function** F. Conversely, given a commutative presemifield $\mathbf{S} = (\mathbf{F}_{p^n}, +, \star)$ of odd order, the function given by

$$F(x) = \frac{1}{2}(x \star x)$$

is a planar DO polynomial [16].

We have the following facts on connection between CCZ-equivalence, isotopisms and strong isotopisms:

- two planar DO polynomials F and F' are CCZ-equivalent if and only if the corresponding commutative semifields $\mathbf{S}_F$ and $\mathbf{S}_{F'}$ are strongly isotopic [11];
- two commutative presemifields of order p^n with n odd are isotopic if and only if they are strongly isotopic [16];
- any commutative presemifield can generate at most two equivalence classes of planar DO polynomials [16];
- if S_1 and S_2 are isotopic commutative semifields of characteristic p with the order of the middle nuclei and nuclei p^m and p^k, respectively, then one of the following statements must hold
  (a) m/k is odd and S_1 and S_2 are strongly isotopic,
  (b) m/k is even and either S_1 and S_2 are strongly isotopic or the only isotopisms between S_1 and S_2 are of the form $(\alpha \star N, N, L)$, where α is a non-square element of $N_m(S_1)$.

Thus, in the case n even it is potentially possible that isotopic commutative presemifields define CCZ-inequivalent quadratic PN functions. However, in practice, no such cases are known.

3. Known cases of planar functions and commutative semifields

Almost all known planar functions are DO polynomials. The only known non-quadratic PN functions are the power functions

$$x^{\frac{3^t+1}{2}}$$

over $\mathbf{F}_{3^n}$, where t is odd and $\gcd(t, n) = 1$ ([15], [25]). Although commutative semifields have been intensively studied for more than a hundred years, there are only a few cases of commutative semifields of odd order known (see [11], [16]):

(i) $$x^2$$
over $\mathbf{F}_{p^n}$ which corresponds to the finite field $\mathbf{F}_{p^n}$;

(ii) $$x^{p^t+1}$$
over $\mathbf{F}_{p^n}$, with $n/\gcd(t, n)$ odd, which correspond to Albert's commutative twisted fields [1], [18], [24];

(iii) the functions over $\mathbf{F}_{p^{2k}}$, which correspond to the Dickson semifields [19];

(iv) the functions over $\mathbf{F}_{p^{2k}}$

$$(ax)^{p^s+1} - (ax)^{p^k(p^s+1)} + \sum_{i=0}^{k-1} c_i x^{p^i(p^k+1)}, \tag{2}$$

$$bx^{p^s+1} + (bx^{p^s+1})^{p^k} + cx^{p^k+1} + \sum_{i=1}^{k-1} r_i x^{p^{k+i}+p^i}, \tag{3}$$

where $a, b \in \mathbf{F}_{p^{2k}}^*$, b is not a square, $c \in \mathbf{F}_{p^{2k}} \setminus \mathbf{F}_{p^k}$, $r_i \in \mathbf{F}_{p^k}$, $0 \le i < k$, $\sum_{i=0}^{k-1} c_i x^{p^i}$ is a permutation of $\mathbf{F}_{p^k}$ with coefficients in $\mathbf{F}_{p^k}$, $\gcd(k+s, 2k) = \gcd(k+s, k)$, and for (3) also $\gcd(p^s+1, p^k+1) \neq \gcd\left(p^s+1, (p^k+1)/2\right)$ (see [11], [12]);

(v) $$x^{p^s+1} - a^{p^t-1} x^{p^t+p^{2t+s}}$$

over $\mathbf{F}_{p^{3t}}$, where a is primitive in $\mathbf{F}_{p^{3t}}$, $\gcd(3,t) = 1$, $t - s = 0 \bmod 3$, $3t/\gcd(s, 3t)$ is odd (see [36]);

(vi) $$x^{p^s+1} - a^{p^t-1} x^{p^{3t}+p^{t+s}}$$

over $\mathbf{F}_{p^{4t}}$, where a is primitive in $\mathbf{F}_{p^{4t}}$, $p^s \equiv p^t \equiv 1 \bmod 4$, $2t/\gcd(s, 2t)$ is odd (see [3]);

(vii) $$x^{10} \pm x^6 - x^2$$

over $\mathbf{F}_{3^n}$, with n odd, corresponding to the Coulter-Matthews and Ding-Yuan semifields [15], [21];

(viii) the function over $\mathbf{F}_{3^{2k}}$, with k odd, corresponding to the Ganley semifield [23];

(ix) the function over $\mathbf{F}_{3^{2k}}$ corresponding to the Cohen-Ganley semifield [14];

(x) the function over $\mathbf{F}_{3^{10}}$ corresponding to the Penttila-Williams semifield [34];

(xi) the function over $\mathbf{F}_{3^8}$ corresponding to the Coulter-Henderson-Kosick semifield [17];

(xii) $$x^2 + x^{90}$$

over $\mathbf{F}_{3^5}$ (see [35]).

The first six cases above are defined for any odd prime p while the last six are defined only for $p = 3$. The polynomial representations of functions (iii), (viii)-(x) can be found in [29]. Note that PN functions (3) of family (iv) and families (v) and (vi) were constructed by following patterns of some known families of APN functions over fields of even characteristic, see [5], [9]. Further we have the following important results of classification of commutative presemifields:

- any semifield of order p^2 is a finite field [26];
- any semifield of order p^3 is either a finite field or Albert's commutative twisted field [28];
- if a commutative presemifield is isotopic to a finite field then it is strongly isotopic to it [16];
- if a commutative presemifield is isotopic to Albert's commutative twisted field then it is strongly isotopic to it [16];
- a commutative presemifield which is three dimensional over its middle nucleus is necessarily isotopic to Albert' commutative twisted field [28].

4. On possible extension of CCZ-equivalence

The following natural generalization of CCZ-equivalence of functions was considered in [7]. Let n and m be any positive integers, p any prime. Two functions F and F' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$ are considered equivalent if their graphs 1_{G_F} and $1_{G'_F}$ are CCZ-equivalent. However, as proven in [7], for p even this equivalence coincides with original CCZ-equivalence of functions. Below we prove that it coincides with CCZ-equivalence for p odd as well. First we need some auxiliary results.

Lemma 1. *Let p be an odd prime, n a positive integer, $a \in \mathbf{F}_{p^n}$ and f any function from $\mathbf{F}_{p^n}$ to itself with the image set $\{0, a\}$. If the function $F(x) = x + f(x)$ is a permutation of $\mathbf{F}_{p^n}$, then $x - f(x)$ is its inverse.*

Proof. Denoting $F'(x) = x - f(x)$ we get

$$F' \circ F(x) = x + f\big(x) - f(x + f(x)\big).$$

If $f(x) = 0$, then obviously $F' \circ F(x) = x$. If $f(x) = a$, then $F' \circ F(x) = x+a-f(x+a)$. Moreover, we have $f(x+a) = a$, since otherwise, $F(x+a) = F(x)$ which contradicts F being a permutation. Hence, when $f(x) = a$, we have also $F' \circ F(x) = x$. Therefore, $F^{-1} = F'$. □

As mentioned in [10], CCZ-equivalence can be considered not only for functions from $\mathbf{F}_{p^n}$ to itself but also for functions between arbitrary groups H_1 and H_2. In the following proposition we consider CCZ-equivalence of functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_2$.

Proposition 1. *Let p be an odd prime and n a positive integer. Two functions f and f' from $\mathbf{F}_{p^n}$ to $\mathbf{F}_2$ are CCZ-equivalent if and only if $f' = f \circ A$ for some affine permutation A of $\mathbf{F}_{p^n}$.*

P r o o f. Let the functions f and f' be CCZ-equivalent. Then there exists an affine permutation $\mathcal{L}$ of $\mathbf{F}_{p^n} \times \mathbf{F}_2$ such that $\mathcal{L}(G_f) = G_{f'}$. Without loss of generality we can assume that $\mathcal{L}$ is linear. Then there exist linear functions $L : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}$, $\phi : \mathbf{F}_2 \to \mathbf{F}_{p^n}$, $l : \mathbf{F}_{p^n} \to \mathbf{F}_2$ and an element $a \in \mathbf{F}_2$ such that

$$\mathcal{L}(x, y) = \big(L(x) + \phi(y), l(x) + ay\big),$$

and for

$$F_{1(x)} = L(x) + \phi \circ f(x),$$
$$F_{2(x)} = l(x) + af(x),$$

F_1 is a permutation of $\mathbf{F}_{p^n}$ and

$$f'(x) = F_2 \circ F_1^{-1}(x).$$

Note that any linear function l from $\mathbf{F}_p^n \to \mathbf{F}_2$ must be 0 since, otherwise, it is balanced which is impossible since p^n is an odd number. Hence, we have $l(x) = 0$ and, since $\mathcal{L}$ is a permutation, $a = 1$, that is, $F_2(x) = f(x)$. Besides, if $\phi \circ f = 0$ then obviously L is a permutation and $f' = f \circ L^{-1}$ and we can take $A = L^{-1}$. Hence we assume that ϕ has the image set $\{0, b\}$, where $b \neq 0$ and $\phi \circ f$ is not a zero function.

Since F_1 is a permutation and the image of $\phi \circ f$ consists of 2 elements then the function L must have at most 2 zeros, and, since $p \geq 3$ and L is a linear function from $\mathbf{F}_{p^n}$ to itself then it has exactly one zero, that is, L is a permutation. Hence, and therefore, by Lemma 1 its inverse is

$$F_1(x) = L\big(x + L^{-1} \circ \phi \circ f(x)\big),$$

where the function

$$F_1^*(x) = x + L^{-1} \circ \phi \circ f(x)$$

is a permutation too, and therefore, by Lemma 1 its inverse is

$$F_1^{*-1}(x) = x - L^{-1} \circ \phi \circ f(x).$$

We get

$$F_1^{-1}(x) = F_1^{*-1} \circ L^{-1}(x)$$

and then

$$f' \circ L(x) = F_2 \circ F_1^{*-1}(x) = f\big(x - L^{-1} \circ \phi \circ f(x)\big).$$

If $f(x) = 0$, then $f' \circ L(x) = 0 = f(x)$. If $f(x) = 1$, then $f\big(x - L^{-1}(b)\big) = 1$. Indeed, if

$$f(x) = 1 \quad \text{and} \quad f\big(x - L^{-1}(b)\big) = 0,$$

then

$$\begin{aligned} F^{*-1}\big(x - L^{-1}(b)\big) &= x - L^{-1}(b) - L^{-1} \circ \phi \circ f\big(x - L^{-1}(b)\big) = x - L^{-1}(b), \\ F^{*-1}(x) &= x - L^{-1} \circ \phi \circ f(x) = x - L^{-1}(b), \end{aligned}$$

which contradict F^{*-1} being a permutation. Hence, $f' \circ L(x) = f(x)$ and we can take $A = L^{-1}$. □

Now we can proof the main result of this section:

Theorem 2. *Let n and m be any positive integers, p any prime, and F and F' any functions from $\mathbf{F}_{p^n}$ to $\mathbf{F}_{p^m}$. Then F and F' are CCZ-equivalent if and only if the indicators of their graphs 1_{G_F} and $1_{G_{F'}}$ are CCZ-equivalent.*

Proof. For the case p even this theorem states Corollary 1 of [7]. Let p be odd. Since 1_{G_F} and $1_{G_{F'}}$ are functions from $\mathbf{F}_{p^n} \times \mathbf{F}_{p^m}$ to $\mathbf{F}_2$, then according to Proposition 1 they are CCZ-equivalent if and only if there exists an affine permutation A of $\mathbf{F}_{p^n} \times \mathbf{F}_{p^m}$ that $1_{G_{F'}} = 1_{G_F} \circ A$, that is, if and only if F and F' are CCZ-equivalent. □

REFERENCES

[1] ALBERT, A. A.: *On nonassociative division algebras,* Trans. Amer. Math. Soc. **72** (1952), 296–309.

[2] ALBERT, A. A.: *Generalized twisted fields,* Pacific J. Math. **11** (1961), 1–8.

[3] BIERBRAUER, J.: *New semifields, PN and APN functions,* Des. Codes Cryptogr. **54** (2010), 189–200.

[4] BIHAM, E.—SHAMIR, A.: *Differential cryptanalysis of DES-like cryptosystems,* J. Cryptology **4** (1991), 3–72.

[5] BRACKEN, C.—BYRNE, E.—MARKIN, N.—MCGUIRE, G.: *New families of quadratic almost perfect nonlinear trinomials and multinomials,* Finite Fields Appl. **14** (2008), 703–714.

[6] BUDAGHYAN, L.: *The simplest method for constructing APN polynomials EA-inequivalent to power functions,* in: Proc. of 1st Internat. Workshop on Arithmetic of Finite Fields—WAIFI '07 (C. Carlet et al., eds.), Lecture Notes in Comput. Sci., Vol. 4547, Springer-Verlag, Berlin, 2007, pp. 177–188.

[7] BUDAGHYAN, L.—CARLET, C.: *CCZ-equivalence of single and multi output Boolean functions,* "Contemporary Mathematics" of Amer. Math. Soc., 2010 (to appear).

[8] BUDAGHYAN, L.—CARLET, C.: *On CCZ-equivalence and its use in secondary constructions of bent functions,* in: Preproc. of Internat. Workshop on Coding and Cryptography—WCC '09, pp. 19–36, 2009.

[9] BUDAGHYAN, L.—CARLET, C.—LEANDER, G.: *Two classes of quadratic APN binomials inequivalent to power functions,* IEEE Trans. Inform. Theory **54**, (2008), 4218–4229.

[10] BUDAGHYAN, L.—CARLET, C.—POTT, A.: *New classes of almost bent and almost perfect nonlinear functions,* IEEE Trans. Inform. Theory **52** (2006), 1141–1152.

[11] BUDAGHYAN, L.—HELLESETH, T.: *New perfect nonlinear multinomials over $\boldsymbol{F}_{p^{2k}}$ for any odd prime p,* in: Proc. of Internat. Conference on Sequences and Their Applications––SETA '08, Lecture Notes in Comput. Sci., Vol. 5203, Springer-Verlag, Berlin, 2008, pp. 401–414.

[12] BUDAGHYAN, L.—HELLESETH, T.: *New commutative semifields defined by new PN multinomials,* Cryptography and Communications: Discrete Structures, Boolean Functions and Sequences, 2010 (to appear).

[13] CARLET, C.—CHARPIN, P.—ZINOVIEV, V.: *Codes, bent functions and permutations suitable for DES-like cryptosystems,* Des. Codes Cryptogr. **15** (1998), 125–156.

[14] COHEN, S. D.—GANLEY, M. J.: *Commutative semifields, two-dimensional over there middle nuclei,* J. Algebra **75** (1982), 373–385.

[15] COULTER, R. S.—MATTHEWS, R. W.: *Planar functions and planes of Lenz-Barlotti class II,* Des. Codes Cryptogr. **10** (1997), 167–184.

[16] COULTER, R. S.—HENDERSON, M.: *Commutative presemifields and semifields,* Adv. Math. **217** (2008), 282–304.

[17] COULTER, R. S.—HENDERSON, M.—KOSICK, P.: *Planar polynomials for commutative semifields with specified nuclei,* Des. Codes Cryptogr. **44** (2007), 275–286.

[18] DEMBOWSKI, P.—OSTROM, T.: *Planes of order n with collineation groups of order n^2,* Math. Z. **103** (1968), 239–258.

[19] DICKSON, L. E.: *On commutative linear algebras in which division is always uniquely possible,* Trans. Amer. Math. Soc. **7** (1906), 514–522.

[20] DICKSON, L. E.: *Linear algebras with associativity not assumed,* Duke Math. J. **1** (1935), 113–125.

[21] DING, C.—YUAN, J.: *A new family of skew Paley-Hadamard difference sets,* J. Comb. Theory Ser. A **133** (2006), 1526–1535.

[22] EDEL, Y.—POTT, A.: *A new almost perfect nonlinear function which is not quadratic,* Adv. Math. Commun. **3** (2009), 59–81.

[23] GANLEY, M. J.: *Central weak nucleus semifields,* European J. Combin. **2** (1981), 339–347.

[24] HELLESETH, T.—RONG, C.—SANDBERG, D.: *New families of almost perfect nonlinear power mappings,* IEEE Trans. Inf. Theory **45** (1999), 475–485.

[25] HELLESETH, T.—SANDBERG, D.: *Some power mappings with low differential uniformity,* Appl. Algebra Engrg. Comm. Comput. **8** (1997), 363–370.

[26] KNUTH, D. E.: *Finite semifields and projective planes,* J. Algebra **2** (1965), 182–217.

[27] KYUREGHYAN, G.—POTT, A.: *Some theorems on planar mappings,* in: Proc. of Internat. Workshop on Arithmetic of Finite Fields—WAIFI '08 (J. von Gathen et al., eds.), Lecture Notes in Comput. Sci., Vol. 5130, Springer-Verlag, Berlin, 2008, pp. 117–122.

[28] MENICHETTI, G.: *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field,* J. Algebra **47** (1977), 400–410.

[29] MINAMI, K.—NAKAGAWA, N.: *On planar functions of elementary abelian p-group type* (submitted).

[30] NAKAGAWA, N.: *On functions of finite fields,* `http://www.math.is.tohoku.ac.jp/ taya/sendaiNC/2006/report/nakagawa.pdf`.

[31] NESS, G. J.: *Correlation of sequences of different lengths and related topics.* PhD Dissertation, University of Bergen, Norway, 2007.

[32] NYBERG, K.: *Perfect nonlinear S-boxes,* in: Advances in Cryptography—EUROCRYPT '91, Lecture Notes in Comput. Sci. **547** (1992), pp. 378–386.

[33] NYBERG, K.: *Differentially uniform mappings for cryptography.* in: Advances in Cryptography—EUROCRYPT '93, Lecture Notes in Comput. Sci., Vol. 765, Springer-Verlag, Berlin, 1994, pp. 55–64.

[34] PENTTILA, T.—WILLIAMS, B.: *Ovoids of parabolic spaces,* Geom. Dedicata **82** (2000), 1–19.

[35] WENG, G.: Private communications, 2007.

[36] ZHA, Z.—KYUREGHYAN, G.—WANG, X.: *Perfect nonlinear binomials and their semifields,* Finite Fields Appl. **15**(2009), 125–133.

Received April 30, 2010

Department of Informatics
University of Bergen
PB 7803
5020 Bergen
NORWAY

E-mail: lilya.budaghyan@ii.uib.no
tor.helleseth@ii.uib.no