Des. Codes Cryptogr. (2012) 63:413–423
DOI 10.1007/s10623-011-9564-3

Further results on planar DO functions and commutative semifields

Guobiao Weng · Xiangyong Zeng

Received: 6 June 2010 / Revised: 8 September 2011 / Accepted: 8 September 2011 /
Published online: 27 September 2011

Abstract It is proven that any Dembowski–Ostrom polynomial is planar if and only if its evaluation map is 2-to-1, which can be used to explain some known planar Dembowski–Ostrom polynomials. A direct connection between a planar Dembowski–Ostrom polynomial and a permutation polynomial is established if the corresponding semifield is of odd dimension over its nucleus. In addition, all commutative semifields of order 3^5 are classified.

Keywords Semifields · Planar functions · Difference sets

Mathematics Subject Classification (2000) 12K10 · 05B10

1 Introduction

Throughout this paper, let p be an odd prime and $q = p^n$ for a positive integer n. We denote the finite field of order q by $\mathbf{F}_q$, the set of its nonzero elements by $\mathbf{F}_q^*$ and the ring of polynomials in the indeterminate x over $\mathbf{F}_q$ by $\mathbf{F}_q[x]$. A finite *semifield* $\mathcal{S}$ is a ring with no zero-divisors, a multiplicative identity and left and right distributive laws. A *subsemifield* of $\mathcal{S}$ is any subset of $\mathcal{S}$ which is also a semifield under its addition and multiplication. If a multiplicative identity is not insisted upon, then we talk of *presemifields*. Let $\mathcal{S}$ be a finite

Communicated by D. Ghinelli.

G. Weng (✉)
School of Mathematical Sciences, Dalian University of Technology, Liaoning 116024,
People's Republic of China
e-mail: gbweng@dlut.edu.cn

X. Zeng
Faculty of Mathematics and Computer Science, Hubei University, Hubei 430062,
People's Republic of China
e-mail: xzeng@hubu.edu.cn

semifield. The three sets

$$\mathcal{N}_l = \{a \in \mathcal{S} | (a * x) * y = a * (x * y) \text{ for all } x, y \in \mathcal{S}\},$$
$$\mathcal{N}_m = \{a \in \mathcal{S} | (x * a) * y = x * (a * y) \text{ for all } x, y \in \mathcal{S}\},$$
$$\mathcal{N}_r = \{a \in \mathcal{S} | (x * y) * a = x * (y * a) \text{ for all } x, y \in \mathcal{S}\}$$

are called the *left, middle and right nucleus* of $\mathcal{S}$, respectively. The set $\mathcal{N} = \mathcal{N}_l \bigcap \mathcal{N}_m \bigcap \mathcal{N}_r$ is called the *nucleus* of $\mathcal{S}$. A semifield (or presemifield) $\mathcal{S}$ is *commutative* if $a * b = b * a$ holds for all $a, b \in \mathcal{S}$. For a commutative semifield $\mathcal{S}$, we have $\mathcal{N}_l = \mathcal{N}_r = \mathcal{N}$, and $\mathcal{N}$ is a finite field and $\mathcal{S}$ can be viewed as a vector space over $\mathcal{N}$. Therefore, the additive group of a semifield is an elementary abelian p-group where p is the characteristic of $\mathcal{N}$. We shall call this prime p as the *characteristic* of the semifield $\mathcal{S}$. Then we can denote a semifield (or presemifield) as $\mathcal{S} = (\mathbf{F}_{q^m}, +, *)$, where $\mathcal{N} = \mathbf{F}_q$ and m is the dimension of $\mathcal{S}$ over $\mathcal{N}$. For any $x, y \in \mathbf{F}_{q^m}$, $x * y$ can be viewed as a function valued in $\mathbf{F}_{q^m}$ and bilinear over $\mathbf{F}_q$ as

$$x * y = P(x, y) = \sum_{0 \le i, j \le m-1} a_{ij} x^{q^i} y^{q^j}, \quad a_{ij} \in \mathbf{F}_{q^m}.$$

Two presemifields $\mathcal{S} = (\mathbf{F}_{q^m}, +, *)$ and $\mathcal{T} = (\mathbf{F}_{q^m}, +, \circ)$ are *isotopic* if there exist three automorphisms σ_1, σ_2 and σ_3 of $(\mathbf{F}_{q^m}, +)$ such that

$$\sigma_3(x * y) = \sigma_1(x) \circ \sigma_2(y), \quad x, y \in \mathbf{F}_{q^m}.$$

In this paper, all semifields (or presemifields) will contain a finite number of elements unless it is specifically stated. Furthermore, we always assume that each semifield (or presemifield) is commutative and has an odd order.

Any function from the finite field $\mathbf{F}_q$ to itself can be expressed as a polynomial of degree less than q. A polynomial $f \in \mathbf{F}_q[x]$ is called a *planar function* if for every nonzero $a \in \mathbf{F}_q$ the mapping $f_a(x) = f(a + x) - f(x)$ induces a permutation of $\mathbf{F}_q$, that is to say, $f_a(x)$ is a *permutation polynomial* (PP). A polynomial $L \in \mathbf{F}_q[x]$ is called a *linearized polynomial* (it is also called a p-polynomial) if it can be represented as

$$L(x) = \sum_{i=0}^{n-1} a_i x^{p^i},$$

where $a_i \in \mathbf{F}_q$. For any $c \in \mathbf{F}_q$, the polynomial $L(x) + c$ is called an *affine* p-polynomial if L is a p-polynomial. Two planar functions f and g over $\mathbf{F}_q$ are *equivalent* if there exist two linearized PPs $\sigma_1(x), \sigma_2(x) \in \mathbf{F}_q[x]$, an affine p-polynomial $A(x)$, and $c \in \mathbf{F}_q$ such that

$$f(x) = \sigma_1(g(\sigma_2(x) + c)) + A(x), \quad x \in \mathbf{F}_q. \tag{1}$$

A polynomial $f \in \mathbf{F}_q[x]$ is a *Dembowski–Ostrom (DO) polynomial* if f can be written as

$$f(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i + p^j}.$$

Each planar DO function f over $\mathbf{F}_q$ determines a commutative presemifield by $x * y = \frac{1}{2}(f(x + y) - f(x) - f(y))$ and vice versa. The following theorem is well known. For example, see [8] and [9].

Theorem 1.1 *Let $(\mathcal{S}, +, *)$ be a finite presemifield with commutative multiplication and odd order q. Define $f : \mathcal{S} \to \mathcal{S}$ by $f(x) = x * x$. Then f is a planar DO function from $(\mathcal{S}, +)$ to itself.*

Let f and g be two equivalent planar DO functions with $f(x) = \sigma_1(g(\sigma_2(x)+c))+A(x)$ for all $x \in \mathbf{F}_q$, where $\sigma_1(x)$ and $\sigma_2(x) \in \mathbf{F}_q[x]$ are two linearized PPs, $A(x)$ is an affine p-polynomial, and $c \in \mathbf{F}_q$. Since g is a DO polynomial, $g(\sigma_2(x)+c) - g(\sigma_2(x))$ is a affine p-polynomial. Thus, without loss of generality, we can take $c = 0$ here, i.e., $f(x) = \sigma_1(g(\sigma_2(x))) + A(x)$ for all $x \in \mathbf{F}_q$. Since $f(x) = f(-x)$ and $g(x) = g(-x)$ for all $x \in \mathbf{F}_q$, we have $\sigma_1(g(\sigma_2(x))) + A(x) = \sigma_1(g(\sigma_2(-x))) + A(-x)$. Then, $A(x) = A(-x)$ for all $x \in \mathbf{F}_q$. As $f(0) = g(0) = 0$, we have $A(x) = 0$, i.e.,

$$f(x) = \sigma_1(g(\sigma_2(x))) \text{ for all } x \in \mathbf{F}_q. \tag{2}$$

In this case, the equality (2) is more simple than (1), and $\sigma_1(x)$, $\sigma_2(x)$ induce two automorphisms of $(\mathbf{F}_q, +)$. Thus, the commutative presemifields $\mathcal{S} = (\mathbf{F}_q, +, *)$ and $\mathcal{T} = (\mathbf{F}_q, +, \circ)$ given by $x * y = \frac{1}{2}(f(x+y) - f(x) - f(y))$ and $x \circ y = \frac{1}{2}(g(x+y) - g(x) - g(y))$ are isotopic since $x * y = \sigma_1(\sigma_2(x) \circ \sigma_2(y))$.

On the other direction, for two isotopic commutative semifields $\mathcal{S} = (\mathbf{F}_q, +, *)$ and $\mathcal{T} = (\mathbf{F}_q, +, \circ)$, however, the planar DO polynomials $f(x) = x * x$ and $g(x) = x \circ x$ are not always equivalent, which is well discussed in [3].

Theorem 1.2 [3] *Let $\mathcal{S} = (\mathbf{F}_q, +, *)$ and $\mathcal{T} = (\mathbf{F}_q, +, \circ)$ be two isotopic commutative semifields of characteristic p, and $f(x) = x * x$, $g(x) = x \circ x$ be two planar DO functions derived from $\mathcal{S}$ and $\mathcal{T}$ respectively. Let $\mathcal{N}_m$ and $\mathcal{N}$ be the middle nucleus and nucleus of $\mathcal{S}$ with $|\mathcal{N}_m| = p^m$, $|\mathcal{N}| = p^t$. Then one of the following statements must hold.*

(1) *m/t is even, and f, g are two equivalent planar functions.*
(2) *m/t is even, q is odd, and $h(x) = (\alpha * x) * x$ is a planar DO function equivalent to g where α is a non-square element of the field $(\mathcal{N}_m, +, *)$.*

The equivalence, described by Coulter and Henderson [3], between commutative presemifields of odd order and planar DO polynomials provides an approach, by which we can study commutative presemifields of odd order from the perspective of planar DO polynomials over finite fields of odd characteristic. In this paper, we establish a necessary and sufficient condition for a DO function to be planar over a finite field of odd characteristic. With this, several constructions of known planar DO functions can be explained in a simple way. We also obtain a property of the images of planar DO functions, which closely connects a planar DO function to a permutation polynomial when the corresponding commutative semifield is of odd dimension over its nucleus. Finally, we discuss the subsemifields of a commutative semifield and the equivalence of planar DO functions. All commutative semifields of order 3^5 are classified.

2 A necessary and sufficient condition for planar DO polynomials

In this section, a necessary and sufficient condition for a DO polynomial to be planar is established.

The following lemmas will be used to prove results in this paper.

Lemma 2.1 [13] *Let $L \in \mathbf{F}_q[x]$ be a p-polynomial. Then the evaluation map of L is a $\mathbf{F}_p$-homomorphism from $(\mathbf{F}_q, +)$ to itself, and each element x in its image has p^r pre-images, where p^r is the number of roots (counted without multiplicities) of L in $\mathbf{F}_q$. In particular, L is a PP over $\mathbf{F}_q$ if and only if L has no roots in $\mathbf{F}_q$ other than 0.*

We say a function f over $\mathbf{F}_q$ is *even* if $f(x) = f(-x)$ for all $x \in \mathbf{F}_q$. The function f is called *2-to-1* if (1) $f(x) = 0$ if and only if $x = 0$; and (2) every image of f except 0 has exactly 2 pre-images.

We recall some preliminaries of difference sets here.

Let G be a finite multiplicative group of order v, and e be the identity of G. A k-element subset D of G is called a (v, k, λ) *difference set* if the list of "differences" $xy^{-1}, x, y \in D$, represents each non-identity element in G exactly λ times. A (v, k, λ, μ) *partial difference set* is a k-element subset D of G for which the list of "differences" xy^{-1}, $x, y \in D$, represents each non-identity element in D exactly λ times and each non-identity element in $G \backslash D$ exactly μ times, and a *skew Hadamard difference set* (SHDS) is a (v, k, λ) difference set D such that G is the disjoint union of D, $D^{(-1)}$, and $\{e\}$, where $D^{(-1)} = \{x^{-1} | x \in D\}$. A partial difference set D in G is of *Paley type* if its parameter is $(v, \frac{v-1}{2}, \frac{v-5}{4}, \frac{v-1}{4})$. We say two subsets D and E of G are *equivalent* if there exist an automorphism σ of G and an element $g \in G$ such that $D = g\sigma(E) := \{g\sigma(x) \mid x \in E\}$. We shall consider these objects in more detail in Sect. 3.

Lemma 2.2 *[17] Let f be an even planar function from $\mathbf{F}_q$ to itself with $f(0) = 0$. Then f is 2-to-1, furthermore, $Im(f) \setminus \{0\}$ is a skew Hadamard difference set if $q \equiv 3 \pmod 4$, or a Paley type partial difference set if $q \equiv 1 \pmod 4$.*

This lemma also appears in [12]. Note that for a DO polynomial $f(x) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i+p^j}$ from $\mathbf{F}_q$ to itself, one has $f(0) = 0$ and $f(x) = f(-x)$ for any $x \in \mathbf{F}_q$. It follows from Lemma 2.2 that if a DO function over $\mathbf{F}_q$ is planar, then it is 2-to-1. In fact, the converse is also true, which is shown in the following theorem.

Theorem 2.3 *Let f be a DO polynomial from $\mathbf{F}_q$ to itself. Then f is planar if and only if f is 2-to-1.*[1]

Proof By Lemma 2.2, it is sufficient to prove that a 2-to-1 DO polynomial is planar.

If the DO polynomial f is 2-to-1, then $f(x) = f(y)$ if and only if $x = \pm y$. Notice that $f_a(x) = f(x+a) - f(x)$ is an affine p-polynomial for each $a \in \mathbf{F}_q^*$. From Lemma 2.1, every image of f_y has the same number of pre-images. For any $a \in \mathbf{F}_q^*$, we have $f_a(-\frac{1}{2}a) = 0$. Further, if $f_a(x) = 0$, then $f(x + a) = f(x)$, which implies $x + a = \pm x$, i.e., $x = -\frac{1}{2}a$. Hence, 0 has exactly one pre-image, and so does every image of f_a. This shows that f_a is a PP and then f is planar. □

From the proof, Theorem 2.3 is also true for infinite commutative semifields of odd characteristic.

For an arbitrary polynomial over $\mathbf{F}_q$, it is difficult to check algebraically whether it is 2-to-1 (or a PP). But for some special polynomials, one can easily answer this question. For a monomial x^d, it is 2-to-1 if and only if $(q - 1, d) = 2$, and it is a PP if and only if $(q - 1, d) = 1$. Dickson polynomials of the first kind are another special case. The Dickson polynomial $D_d(x, a)$ of the first kind of degree d in the indeterminate x and with the parameter $a \in \mathbf{F}_q$ is given as

$$D_d(x, a) = \sum_{i=0}^{\lfloor d/2 \rfloor} \frac{d}{d-i} \binom{d-i}{i} (-a)^i x^{d-2i},$$

[1] We have been informed that R.S Coulter and R.W Matthews have a different proof of Theorem 2.3.

where $\lfloor d/2 \rfloor$ denotes the largest integer less than or equal to $d/2$. It is well known that for $a \neq 0$, $D_d(x, a)$ permutes the field $\mathbf{F}_q$ if and only if $(q^2-1, d) = 1$. We refer readers to [14] for more details on Dickson polynomials. Then a natural question arises as below. When is $D_d(x^s, a) - D_d(0, a)$ a DO polynomial? In [6], it is well discussed, and we list the result as the following.

Theorem 2.4 [6] *Let $D_d(x, a)$ be the Dickson polynomial of the first kind of degree d, where $(p, d) = 1$ and $d > 1$. Let the integer s satisfy $(p, s) = 1$ and $s > 1$. Then $D_d(x^s, a) - D_d(0, a)$ is a DO polynomial if and only if*

(1) $a = 0$, *and* $sd = 1 + p^j$ *for some integer* j;
(2) $a \neq 0, d = 2, s = \frac{1+p^j}{2}$;
(3) $a \neq 0, d = 3, s = 2$ *and* $p = 5$;
(4) $a \neq 0, d = 4, s = 1$ *and* $p = 3$;
(5) $a \neq 0, d = 5, s = 2$ *and* $p = 3$.

Thus, Theorem 2.3 gives an alternative explanation of the following planar DO polynomials.

(1) The polynomial $f(x) = x^2$ is a planar DO polynomial over any finite field, where the corresponding semifield is a field.
(2) Let $f(x) = x^{p^l+1}$ be defined over $\mathbf{F}_q$. Then f is a planar polynomial if and only if $n/(n, l)$ is odd, where (n, l) denotes the greatest common divisor of the integers n and l. In such cases, the resulting semifield is isotopic to the commutative twisted field generated by the field automorphism x^{p^l} defined by Albert [1].
(3) For $a \in \mathbf{F}_{3^l}^*$, $D_5(x^2, a)$ is planar over $\mathbf{F}_{3^l}$ if and only if l is odd or both $l = 2$ and $a = \pm 1$, see [5] and [7], and their corresponding semifields are not isotopic to the above ones [3].

3 Images of planar DO polynomials

In this section, we characterize a property of the images of planar DO polynomials, and derive a relation between a planar DO polynomial and a permutation polynomial.

For a commutative ring R with identity 1, the group ring $R[G] = \{\sum_{g\in G} a_g g \mid a_g \in R\}$ with the multiplication rule "$\cdot$" as

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h g\right) = \sum_{g\in G}\sum_{h\in G} (a_h b_{h^{-1}g})g$$

is a free R-module of rank v. Obviously, e is the identity of $R[G]$. We use the same symbol D to denote the element $\sum_{g\in D} g$ in $R[G]$ for a subset D of G.

Usually, R is taken as the ring $\mathbf{Z}$ of integers, the field $\mathbf{Q}$ of rational numbers, or the complex field $\mathbf{C}$. In particular, in $\mathbf{Z}[G]$, D is a (v, k, λ) difference set if and only if

$$DD^{(-1)} = (k-\lambda)e + \lambda G,$$

and D is a (v, k, λ, μ) partial difference set if and only if

$$DD^{(-1)} = se + \mu G + (\lambda - \mu)D,$$

where $s = k(k-\lambda) - \mu(v-k)$.

When G is abelian, we can also use the notion of a character. A character of G is a group homomorphism $\chi : G \to \mathbf{C}^*$, where $\mathbf{C}^*$ is the multiplicative group of $\mathbf{C}$. The set $\widehat{G}$ of all characters of G is a group and is isomorphic to G. For the sake of completeness, we list two well known fundamental results on characters as below.

Lemma 3.1 (Orthogonality relations) *Let G be a finite abelian group of order v and with identity e. Then*

$$\sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} 0, & \text{if } g \neq e, \\ v, & \text{if } g = e \end{cases} \quad \text{and} \quad \sum_{g\in G} \chi(g) = \begin{cases} 0, & \text{if } \chi \neq \chi_0, \\ v, & \text{if } \chi = \chi_0, \end{cases}$$

where χ_0 is the trivial character of G, that is, $\chi_0(g) = 1$ for all $g \in G$.

Lemma 3.2 (Inversion formula) *Let G be a finite abelian group of order v. Let $A = \sum_{g\in G} a_g g \in \mathbf{C}[G]$, and $\chi(A) := \sum_{g\in G} a_g \chi(g)$. Then the coefficients of A are determined as*

$$a_g = \frac{1}{v} \sum_{\chi\in\widehat{G}} \chi(A)\chi(g^{-1}).$$

Hence, if $A, B \in \mathbf{C}[G]$ satisfy $\chi(A) = \chi(B)$ for each character χ of G, then $A = B$.

In this section, we only focus on the case $G = (\mathbf{F}_{q^m}, +)$. The *trace function* $\mathrm{Tr}_n^{mn}(\cdot)$ from $\mathbf{F}_{q^m}$ to $\mathbf{F}_q$ is defined by

$$\mathrm{Tr}_n^{mn}(x) = \sum_{i=0}^{m-1} x^{q^i}, \ x \in \mathbf{F}_{q^m}.$$

The trace function obeys the transitivity law, i.e., $\mathrm{Tr}_1^{mn}(x) = \mathrm{Tr}_1^n(\mathrm{Tr}_n^{mn}(x))$ for all $x \in \mathbf{F}_{q^m}$. Moreover, each character χ_β for $\beta \in \mathbf{F}_{q^m}$ could be written as

$$\chi_\beta(\alpha) = \xi^{\mathrm{Tr}_1^{mn}(\alpha\beta)}, \quad \alpha \in \mathbf{F}_{q^m},$$

where ξ is a p-th primitive root of unity in $\mathbf{C}$.

Lemma 3.3 *Let $\mathcal{S} = (\mathbf{F}_{q^m}, +, *)$ be a commutative semifield with the nucleus $\mathbf{F}_q$, and*

$$f(x) = x * x = \sum_{i,j=0}^{m-1} a_{ij} x^{q^i+q^j}$$

be the corresponding planar DO polynomial. If we view $\mathbf{F}_{q^m}$ as a vector space over $\mathbf{F}_q$, then for all $\alpha \in \mathbf{F}_{q^m}^*$, $\mathrm{Tr}_n^{mn}(\alpha f(x))$ can be viewed as a nondegenerate quadratic form over $\mathbf{F}_q$.

Proof By the expression of $f(x)$, it is sufficient to prove that $\mathrm{Tr}_n^{mn}(\alpha f(x))$ is nondegenerate. Otherwise, there exists some $\alpha \in \mathbf{F}_{q^m}^*$ such that $\mathrm{Tr}_n^{mn}(\alpha f(x))$ is degenerate. As a consequence, there is an element $\beta \in \mathbf{F}_{q^m}^*$ such that $\mathrm{Tr}_n^{mn}(\alpha f(x)) = \mathrm{Tr}_n^{mn}(\alpha f(x+\beta))$ for all $x \in \mathbf{F}_{q^m}$. Then $\mathrm{Tr}_n^{mn}(\alpha f_\beta(x)) = 0$ for all $x \in \mathbf{F}_{q^m}$. This shows that $f_\beta(x)$ cannot be bijective, contradicting with the fact that $f(x)$ is planar and this finishes the proof. □

The following lemmas come from [13].

Lemma 3.4 [13] *Let f be a nondegenerate quadratic form over $\mathbf{F}_q$ in an odd number m of indeterminates. Then for $b \in \mathbf{F}_q$, the number of solutions of the equation $f(x_1, x_2, \ldots, x_m) = b$ in $\mathbf{F}_q^m$ is*

$$q^{m-1} + q^{\frac{m-1}{2}} \eta\left((-1)^{\frac{m-1}{2}} b\delta\right),$$

where $\delta = \det(f)$ and η is the quadratic character of $\mathbf{F}_q$ with

$$\eta(a) = \begin{cases} 0, & a = 0, \\ 1, & \text{if } a \text{ is a square in } \mathbf{F}_q^*, \\ -1, & \text{if } a \text{ is a non-square in } \mathbf{F}_q^*. \end{cases}$$

Lemma 3.5 [13] *Let f be a nondegenerate quadratic form over $\mathbf{F}_q$ in an even number m of indeterminates. Then for $b \in \mathbf{F}_q$, the number of solutions of the equation $f(x_1, x_2, \ldots, x_m) = b$ in $\mathbf{F}_q^m$ is*

$$q^{m-1} + v(b) q^{\frac{m-2}{2}} \eta\left((-1)^{\frac{m}{2}} \delta\right),$$

where $\delta = \det(f)$, η is the quadratic character of $\mathbf{F}_q$ and

$$v(b) = \begin{cases} q-1, & b = 0, \\ -1, & otherwise. \end{cases}$$

Given the above, we have the following result.

Proposition 3.6 *Let $\mathcal{S} = (\mathbf{F}_{q^m}, +, *)$ be a commutative semifield with the nucleus $\mathbf{F}_q$, and*

$$f(x) = x * x = \sum_{i,j=0}^{m-1} a_{ij} x^{q^i + q^j}$$

be the corresponding planar DO polynomial. Denote $D = Im(f) \setminus \{0\}$, $E = \mathbf{F}_{q^m} \setminus Im(f)$, and $aD = \{ad \mid d \in D\}$ for $a \in \mathbf{F}_q^*$. Then one of the following statements must hold.

(1) *when m is even, or m is odd and a is a square, $aD = D$;*
(2) *when m is odd and a is a non-square, $aD = E$.*

Proof For $\beta \in \mathbf{F}_{q^m}$, each character χ_β of $(\mathbf{F}_{q^m}, +)$ can be written as

$$\chi_\beta(\alpha) = \xi^{\mathrm{Tr}_1^{mn}(\alpha\beta)}, \quad \alpha \in \mathbf{F}_{q^m}.$$

By Theorem 2.3 together with f being a planar DO polynomial, we have

$$1 + 2\chi_\beta(D) = \sum_{x \in \mathbf{F}_{q^m}} \xi^{\mathrm{Tr}_1^{mn}(\beta f(x))},$$

by which $1 + 2\chi_\beta(aD) = \sum_{x \in \mathbf{F}_{q^m}} \xi^{\mathrm{Tr}_1^n(a\mathrm{Tr}_n^{mn}(\beta f(x)))}$.

When m is even, for any fixed $a \in \mathbf{F}_q^*$, by Lemmas 3.3 and 3.5 the numbers of the solutions of the two equations $\mathrm{Tr}_n^{mn}(\beta f(x)) = b$ and $\mathrm{Tr}_n^{mn}(\beta f(x)) = ab$ are equal for all $b \in \mathbf{F}_q$. Thus $\chi_\beta(aD) = \chi_\beta(D)$ for any $a \in \mathbf{F}_q^*$. By Lemma 3.2, we have $aD = D$.

When m is odd, for a given $a \in \mathbf{F}_q^*$, by Lemmas 3.3 and 3.4 the numbers of the solutions of the two equations $\mathrm{Tr}_n^{mn}(\beta f(x)) = b$ and $\mathrm{Tr}_n^{mn}(\beta f(x)) = ab$ are equal for all $b \in \mathbf{F}_q$ if

and only if a is a square. Notice that $\sum_{x\in\mathbf{F}_q}\xi^{\mathrm{Tr}_1^n(cx)}=\chi_c(\mathbf{F}_q)=0$ for $c\in\mathbf{F}_q^*$ by Lemma 3.1. Consequently, we have

$$1+2\chi_\beta(D)=\sum_{x\in\mathbf{F}_{q^m}}\xi^{\mathrm{Tr}_1^{mn}(\beta f(x))}=\sum_{b\in\mathbf{F}_q}q^{\frac{m-1}{2}}\eta\left((-1)^{\frac{m-1}{2}}b\delta_\beta\right)\xi^{\mathrm{Tr}_1^n(b)},$$

where $\delta_\beta=\det\left(\mathrm{Tr}_n^{mn}(\beta f(x))\right)$. Similarly, we have

$$1+2\chi_\beta(aD)=\sum_{b\in\mathbf{F}_q}q^{\frac{m-1}{2}}\eta\left((-1)^{\frac{m-1}{2}}ab\delta_\beta\right)\xi^{\mathrm{Tr}_1^n(b)}.$$

This implies

$$\chi_\beta(aD)=\begin{cases}\chi_\beta(D), & \text{if } a \text{ is a square},\\ \chi_\beta(E), & \text{otherwise}.\end{cases}$$

The proof follows from Lemma 3.2. □

For the case $n=1$, i.e., $q=p$ is a prime, Proposition 3.6 has already been proven by discussing the number of multipliers of difference sets. Readers may refer to [2,10,11,15], and [16] for more details on skew Hadamard difference sets or partial difference sets.

When m is odd in Proposition 3.6, the planar function f is closely related to a permutation polynomial.

Theorem 3.7 *Let $\mathcal{S}=(\mathbf{F}_{q^m},+,*)$ be a commutative semifield of the nucleus $\mathbf{F}_q$, and*

$$f(x)=x*x=\sum_{i,j=0}^{m-1}a_{ij}x^{q^i+q^j}$$

be the corresponding planar DO polynomial of $\mathcal{S}$. If m is odd, then the polynomial

$$g(x)=\sum_{i,j=0}^{m-1}a_{ij}d_{ij}(x)x^{\frac{q^i+q^j}{2}} \tag{3}$$

where

$$d_{ij}(x)=\begin{cases}1 & \text{if } i \text{ and } j \text{ have the same parity},\\ x^{\frac{q^m-1}{2}}, & \text{otherwise},\end{cases}$$

is a permutation polynomial over $\mathbf{F}_{q^m}$.

Proof It can be verified that $f(x)=g(x^2)$. By Theorem 2.3, $f(x)$ is a 2-to-1 planar DO function. Notice that x^2 is also a 2-to-1 planar function. Consequently, g must be bijective from $\mathrm{Im}(x^2)$ to $\mathrm{Im}(f)$. For a non-square element a of $\mathbf{F}_q$, by Proposition 3.6, we have

$$a\left(\mathrm{Im}(f)\setminus\{0\}\right)=\mathbf{F}_{q^m}\setminus\mathrm{Im}(f),\ \text{and}\ a(\mathrm{Im}(x^2)\setminus\{0\})=\mathbf{F}_{q^m}\setminus\mathrm{Im}(x^2). \tag{4}$$

By (3), it can be verified that $g(ax)=ag(x)$ for all $a\in\mathbf{F}_q$ and $x\in\mathbf{F}_{q^m}$. This together with (4) shows that g is a PP over $\mathbf{F}_{q^m}$.

The proof is finished. □

4 Commutative semifields of order 3^5

Recall that subsemifields of a semifield $\mathcal{S}$ are those subsets of $\mathcal{S}$ which are also semifields under its addition and multiplication. First, we give a result on the subsemifields of a commutative semifield of order p^5.

Lemma 4.1 *Let $(\mathcal{S}, +, *)$ be a commutative semifield with $|\mathcal{S}| = q = p^n$, where p is a prime and n is odd. If $\mathcal{T}$ is a subset of $\mathcal{S}$, and $(\mathcal{T}, +, *)$ is also a presemifield with $|\mathcal{T}| = p^k$, then k is odd.*

Proof From Proposition 3.6, the "square set" $\{x * x \mid x \in \mathcal{S}\}$ does not contain any nontrivial subgroup of $(\mathcal{S}, +)$, neither does $\{x * x \mid x \in \mathcal{T}\}$. This shows that k is odd. □

Lemma 4.2 *Let $(\mathcal{S}, +, *)$ be a presemifield with $|\mathcal{S}| = q = p^n$, where p is a prime and n is odd. If $\mathcal{T}$ is a proper subset of $\mathcal{S}$, and $(\mathcal{T}, +, *)$ is also a presemifield with $|\mathcal{T}| = p^k$, then $2k \leq n$.*

Proof We view $\mathcal{S}$ as a linear space over $\mathbf{F}_p$, and $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_n$ is a basis of $\mathcal{S}$. Without loss of generality, we assume that $\mathcal{T}$ is the linear span of $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k$.

As $\mathcal{T}$ is also a presemifield, $a * b$ is not in $\mathcal{T}$ for any $a \neq 0 \in \mathcal{T}$ and $b \notin \mathcal{T}$.

If $n - k < k$, then the k vectors $\varepsilon_1 * \varepsilon_{k+1} + \mathcal{T}, \varepsilon_2 * \varepsilon_{k+1} + \mathcal{T}, \cdots, \varepsilon_k * \varepsilon_{k+1} + \mathcal{T}$ are linearly dependent in the linear space $\mathcal{S} \setminus \mathcal{T}$ of dimension $n - k$ over $\mathbf{F}_p$. That implies that there exists a nonzero k-tuple $(c_1, c_2, \cdots, c_k) \in \mathbf{F}_p^k$ such that $\sum_{i=1}^{k}(c_i \varepsilon_i * \varepsilon_{k+1}) = (\sum_{i=1}^{k} c_i \varepsilon_i) * \varepsilon_{k+1} \in \mathcal{T}$.

It is a contradiction. □

By Lemmas 4.1 and 4.2, we immediately have

Theorem 4.3 *Let $\mathcal{S} = (\mathbf{F}_q, +, *)$ be a commutative semifield with order $q = p^5$. Then any subsemifield $(\mathcal{T}, +, *)$ of $\mathcal{S}$ has order either p or p^5.*

Secondly, we list all commutative semifields of order 3^5 by computer. As the semifield is a linear space over its nucleus, we always assume that the semifield $\mathcal{S}$ of order p^5 is viewed as a vector space over $\mathbf{F}_p$, and each element is written as a tuple $(x_1, x_2, \ldots, x_5) \in \mathbf{F}_p^5$. For $i \in \{1, 2, 3, 4, 5\}$, let ε_i denote the vector with 1 in the i-th component and 0 in other components.

By Theorem 2.3, in order to obtain all commutative semifields $\mathcal{S}$ of order p^5, we only need to determine all those symmetric matrices $A = (a_{ij})_{5\times 5}$ with $a_{ij} = \varepsilon_i * \varepsilon_j \in \mathcal{S}$, for which the associated quadratic function $f(X) = XAX^T$ is 2-to-1 over $\mathcal{S}$, where $X = (x_1, x_2, \ldots, x_5) \in \mathcal{S}$. Without loss of generality, we assume that ε_1 is the identity of semifield, i.e., $a_{1j} = a_{j1} = \varepsilon_j$.

As $\mathcal{S}$ has only subsemifields of order p and p^5, for each $x \in \mathcal{S}, x \neq k\varepsilon_1, k \in \mathbf{F}_p$, we have that ε_1, x and $x * x$ are linearly independent over $\mathbf{F}_p$. Furthermore, there exists $x \in \mathcal{S}$, such that $\varepsilon_1, x, x * x$ and $(x * x) * (x * x)$ are linearly independent over $\mathbf{F}_p$. If $(x * x) * (x * x)$ is a linear combination of ε_1, x and $x * x$, then $x * (x * x)$ cannot be a linear combination of ε_1, x and $x * x$, or there exists a subsemifield of order p^3 in $\mathcal{S}$, which is generated by ε_1, x and $x * x$. Then $y = \varepsilon_1 + x \in \mathcal{S}$ has the property that $\varepsilon_1, y, y * y$ and $(y * y) * (y * y)$ are linearly independent.

Thus, without loss of generality, we can assume $a_{22} = \varepsilon_2 * \varepsilon_2 = \varepsilon_3$, and $a_{33} = \varepsilon_3 * \varepsilon_3 = \varepsilon_4$. As $\varepsilon_1, \varepsilon_2, \varepsilon_3$ and ε_4 could not generate a subsemifield of order p^4, we also assume one of a_{23}, a_{24}, a_{34} and a_{44} to be ε_5. Therefore, there are less than $4p^{35}$ possibilities of the matrix A.

Table 1 Planar DO functions over $\mathbf{F}_{3^5}$

Polynomial	Commutative semifield type	Skew Hadamard difference set
x^2	Field	Paley difference set
x^4	Albert's twisted field	Paley difference set
x^{10}	Albert's twisted field	Paley difference set
$x^{90}+x^2$	See [4]	Paley difference set
$x^{10}+x^6-x^2$	Coulter–Matthews field	$DY(1)$
$x^{10}-x^6-x^2$	Ding-Yuan variation	$DY(-1)$
$x^{162}+x^{108}-x^{84}+x^2$	See [4]	Inequivalent to the above ones

For each matrix, we only need to calculate XAX^T for $\frac{p^5-1}{2}$ of X's in $\mathcal{S}$. We can check them one by one by computer when $p=3$. On a personal computer (CPU: Intel Core Duo T7300, 2.0 GHz), it takes about ten hours to perform an exhaustive search in the case of order 3^5. We found 18,096 examples in total.

All these semifields can be classified from the view of planar DO functions. Let f and g be two equivalent planar DO functions, with $f(x)=\sigma_1(g(\sigma_2(x)))$ for all $x\in\mathbf{F}_q$, where σ_1,σ_2 are two automorphisms of $(\mathbf{F}_q,+)$. Then σ_1 is an automorphism of the difference sets $\mathrm{Im}(f)\setminus\{0\}$ and $\mathrm{Im}(g)\setminus\{0\}$, since $\mathrm{Im}(f)=\sigma_1(\mathrm{Im}(g))$. Thus

Proposition 4.4 *Let f and g be two planar DO functions over $\mathbf{F}_q$. If difference sets $Im(f)\setminus\{0\}$ and $Im(g)\setminus\{0\}$ are not equivalent, then f and g are two inequivalent planar DO functions.*

By Theorem 2.3, planar DO functions are 2-to-1. For two given planar DO functions f and g over $\mathbf{F}_q$, we can easily judge whether there exists an automorphism σ of $(\mathbf{F}_q,+)$ such that $f(x)=g(\sigma(x))$ for all $x\in\mathbf{F}_q$. Therefore, listing all automorphisms of two equivalent SHDS (or Paley type partial difference sets, abbreviated as PPDS) is an efficient way to determine whether two planar DO functions are equivalent or not. There are few results on equivalent SHDS or PPDS. Before 2005, there was a conjecture that all SHDS are equivalent to Paley difference sets, which are the SHDS derived from the planar DO function $f(x)=x^2$. In [7], Ding and Yuan gave a SHDS inequivalent to a Paley difference set, which is the SHDS derived from planar DO functions $f(x)=D_5(x^2,\pm1)$, and some other inequivalent SHDS are given in [17,18]. At present, there is no known proof that these SHDS are inequivalent in the general case. When q is small, we can perform an exhaustive search of all automorphisms of $(\mathbf{F}_q,+)$ by computer. For two equivalent SHDS D, E in $(\mathbf{F}_q,+)$, we can list all automorphisms σ such that $D=\sigma(E)$ by computer. When $q=p^5$, there are less than p^{25} automorphisms σ of $(\mathbf{F}_q,+)$. It takes several seconds for $q=3^5$ on a personal computer (CPU: Intel Core Duo T7300, 2.0GHz).

In Table 1, we list all planar DO functions over $\mathbf{F}_{3^5}$, which are also given in [4].

Acknowledgments This work was supported by the National Natural Science Foundation of China under grants (No. 10826072 and No. 60973130). The work of G. Weng was also partially supported by the Fundamental Research Funds for the Central Universities (FRSCU) 20091118. The authors would like to thank the editor and two anonymous reviewers for their constructive comments, and they are indebted to professor Matthew Geoffrey Parker for his help in revising this paper.

References

1. Albert A.A.: On nonassociative algebras. Trans. Am. Math. Soc. **72**, 296–309 (1952).
2. Camion P., Mann H.B.: Antisymmetric difference sets. J. Number Theory **4**, 266–268 (1972).
3. Coulter R.S., Henderson M.: Commutative presemifields and semifields. Adv. Math. **217**, 282–304 (2008).
4. Coulter R.S., Kosick P.: Commutative semifields of order 243 and 3125. In: McGuire G., Mullen G.L., Panario D., Shparlinski I.E. (eds.) Proceedings of the 9th International Conference on Finite Fields and Applications. Contemporary Mathematics, vol. 518, pp. 129–136. American Mathematical Society, Providence (2010).
5. Coulter R.S., Matthews R.W.: Planar functions and planes of Lenz–Barlotti class II. Des. Codes Cryptogr. **10**, 167–184 (1997)
6. Coulter R.S., Matthews R.W.: Dembowski–Ostrom polynomials from Dickson polynomials. Finite Fields Appl. **16**, 369–379 (2010).
7. Ding C., Yuan J.: A family of skew Hadamard difference sets. J. Combin. Theory Ser. A **113**, 1526–1535 (2006).
8. Ghinelli D., Jungnickel D.: Some geometric aspects of finite abelian groups. Rend. Mat. Appl. (7) **26**, 29–68 (2006).
9. Hughes D.R.: Partial difference sets. Am. J. Math. **78**, 650–674 (1956).
10. Johnsen E.C.: Skew–Hadamard abelian group difference sets. J. Algebra **4**, 388–402 (1966).
11. Jungnickel D.: On λ-ovals and difference sets. In: Bodendieck R. (ed.) Contemporary Methods in Graph Theory, pp. 429–448. Bibliographisches Institut, Mannheim (1990).
12. Kyureghyan G.M., Pott A.: Some theorems on planar mappings. In: Arithmetic of Finite Fields. Lecture Notes in Computer Science, vol. 5130, pp. 117–122. Springer, Berlin (2008).
13. Lidl R., Niederreiter H.: Finite Fields. Encyclopedia of Mathematics and Its Applications, vol. 20. Addison-Wesley Publishing Company, Reading (1983).
14. Lidl R., Mullen G.L., Turnwald G.: Dickson Polynomials. Pitman Monographs and Surveys in Pure and Applied Mathematics, vol. 65. Wiley, Inc., New York (1993).
15. Ma S.L.: A survey on partial difference sets. Des. Codes Cryptogr. **4**, 221–261 (1994).
16. Ma S.L.: Polynomial addition sets and symmetric difference sets. In: Ray-Chaudhuri D. (ed.) Coding Theory and Design Theory, Part 2, pp. 273–279. Springer, New York (1990).
17. Weng G., Qiu W., Wang Z., Xiang Q.: Pseudo-Paley graphs and skew Hadamard difference sets from presemifields. Des. Codes Cryptogr. **44**, 49–62 (2007).
18. Weng G., Hu L.: Some results on skew Hadamard difference sets. Des. Codes Cryptogr. **50**, 93–105 (2009).