Hokkaido Mathematical Journal Vol. 37 (2008) p. 531–544

On planar functions of elementary abelian *p*-group type

Kaori Minami and Nobuo Nakagawa

(Received May 9, 2007)

Abstract. We proved affine planes corresponding to quadratic planar functions over $\mathbb{F}_{p^n}$ are semifield planes, and we determined affine planes corresponding to planar functions $f(x) = x^{10} - \alpha x^6 - \alpha^2 x^2$ by Ding and Yuan. Moreover we calculated explicit shapes of planar functions from the square mappings of almost all known finite commutative semifields.

Key words: planar function, projective plane, finite field, finite semifield, relative difference set, collineation group.

1. Introduction

Planar functions have been researched for long years by many mathematicians as an interesting problem related to affine planes admitting regular collineation groups (cf. [1], [3], [5], [6], [7], [8], [9], [11], [12], [13], [14], [18], [19], [20], [21], [22], [24]). Let G and H be finite groups of the same order n and f be a function from G into H. Moreover let f_a be a function from G into H defined by $f_a(x) = f(ax)f(x)^{-1}$ for an element a of G. Then f is named a planar function from G into H of degree n if and only if f_a is bijective for every element a of G except $a = 1$. Suppose that f is a planar function from G into H, and put $D = \{(x, f(x)) \mid x \in G\}$. Then D is a relative difference set in $G \times H$ relative to H with parameters $(n, n, n, 1)$. Moreover if we take $\mathbf{P} := G \times H$ as the set of points and $\mathbf{L} := \{Hx \mid x \in G\} \cup \{Dv \mid v \in G \times H\}$ as the set of lines, then $I(G, H; f) := (\mathbf{P}, \mathbf{L}, \in)$ is an affine plane in which $G \times H$ acts regularly on $\mathbf{P}$. Then H is the elation subgroup with the center (∞) and the axis l_∞ of the projective plane extended from this affine plane, and G acts transitively on the points of l_∞ except (∞). Conversely we can construct a planar function from G to H if $G \times H$ acts on an affine plane as the above action. Thus the planar functions problem is a special case of the classification problem of affine planes admitting regular collineation groups.

2000 Mathematics Subject Classification : 51E20.

Example 1.1 $f\colon \mathbb{F}_q \longrightarrow \mathbb{F}_q\colon x \longmapsto x^2$
where $\mathbb{F}_q$ is the additive group of a finite field of cardinality q for an odd prime power q. An affine plane corresponding to this function is desarguesian.

Example 1.2 $f\colon \mathbb{F}_{p^{2n}} \longrightarrow \mathbb{F}_{p^{2n}}$
$$x \longmapsto x^2 + 4^{-1}j^{1-p^r}(x^{2p^r} + x^{2p^{(n+r)}} - 2x^{p^r+p^{(n+r)}}) - 4^{-1}(x^2 + x^{2p^n} - 2x^{p^n+1})$$
where p is an odd prime and $1 \leq r < n$ and let j be any element of $\mathbb{F}_{p^n}$ which is not square. An affine plane corresponding to this function is a semifield plane (not desarguesian). These examples are the square mappings on Dickson semifields in section 4.

The following example was given by R.S. Coulter and R.W. Matthews ([3]).

Example 1.3 $f\colon \mathbb{F}_{3^e} \longrightarrow \mathbb{F}_{3^e}\colon x \longmapsto x^{(3^\alpha+1)/2}$
where $\gcd(\alpha, 2e) = 1$. Affine planes corresponding to these functions are not translation planes if $1 < \alpha < 2e$.

Examples of such planar functions as G or H is not an elementary abelian p-group are not known.

After reviewing known main results concerning planar functions in Section 2 it is discussed that affine planes corresponding to quadratic planar functions over finite fields become semifield planes and we determined affine planes corresponding to planar functions $f(x) = x^{10} - \alpha x^6 - \alpha^2 x^2$ by Ding and Yuan in Section 3. In Section 4 it is proved that square mappings of finite commutative semifields are planar functions of elementary abelian p-group type in the background of relative difference sets with parameters $(q, q, q, 1)$. Moreover we will calculate explicit shapes of planar functions from the square mappings of almost all known finite commutative semifields.

2. Known results

The following theorems are known.

Theorem 2.1 (Dembowski and Ostrom [5]) *Suppose that there exists a planar function of degree n. Then n is odd.*

Theorem 2.2 (Gluck, Hiramine, Ronyai and Szonyi, [9] [11] [24]) *Suppose that there exists a planar function of degree p for an odd prime p. Then f is a quadratic polynomial on $\mathbb{F}_p$ and an affine plane corresponding to f is desarguesian.*

Theorem 2.3 (Nakagawa [19] [20]) *Suppose that G and H are finite abelian groups of order p^n for an odd prime p, and there exists a planar function from G into H. Then*

$$\exp(H) \leq \begin{cases} p^{(n+1)/2} & (n\colon \textit{odd}) \\ p^{n/2} & (n\colon \textit{even}). \end{cases}$$

Moreover G is not cyclic if $n \geq 2$.

Theorem 2.4 (Blokhuis, Jungnickel and Schmidt [1]) *If there exists a planar function of degree n between abelian groups G and H, then n is an odd prime power, say $n = p^m$ then the p-rank of $G \times H$ is at least $m + 1$.*

Given two primes p and q, $\mathrm{ord}_p(q)$ denotes the order of q in the multiplicative group of $\mathbb{F}_p$.

Theorem 2.5 (Hiramine [12]) *Let f be a planar function of degree n from a group G into an abelian group H. Let p and q be distinct prime factors of n. If $\mathrm{ord}_p(q)$ is even, then the square free part of n is not divisible by q.*

Suppose that φ is a function from $\mathbb{F}_{p^n}$ into $\mathbb{F}_p$ for a prime p and ω be a primitive p-th root of unity. We define a mapping $\hat{\varphi}$ from $\mathbb{F}_{p^n}$ into the complex number field $\mathbb{C}$ as

$$\hat{\varphi}(x) := \sum_{y \in \mathbb{F}_{p^n}} \omega^{(\mathrm{Tr}(xy)+\varphi(y))}.$$

Here Tr is the absolute trace mapping. Then φ is named bent functions if and only if $|\hat{\varphi}(u)| = p^{n/2}$ for any $u \in \mathbb{F}_{p^n}$. Bent functions are important ones in the cryptography theory and the coding theory.

Theorem 2.6 (Nakagawa [20]) *We assume $G \cong H \cong \mathbb{Z}_p^n$, and $f(\mathbb{X}) = (f_1(\mathbb{X}), \ldots, f_n(\mathbb{X}))$ is a function from G into H for $\mathbb{X} = (u_1, \ldots, u_n)$. Then f is planar if and only if*

$$s_1 f_1 + \cdots + s_n f_n$$

is a bent function for each $(s_1, \ldots, s_n) \in \mathbb{Z}_p^n$ *such that* $(s_1, \ldots, s_n) \neq (0, \ldots, 0)$.

In the following theorem, we consider that $\mathbb{F}_{p^n}$ is a n dimensional vector space over $\mathbb{F}_p$.

Theorem 2.7 (Nakagawa [22]) *Suppose that* f *is a planar function from* $\mathbb{F}_{p^n}$ *into* $\mathbb{F}_{p^n}$ *such that* $f(0) = 0$ *and* $\gcd(n, p) = 1$ *for an odd prime* p. *Then the following* (i) *and* (ii) *are equivalent.*

(i) *The affine plane corresponding to* f *is desarguesian.*

(ii) *There are bijective linear mappings* ℓ, α, *and* β *from* $\mathbb{F}_{p^n}$ *into* $\mathbb{F}_{p^n}$ *such that*

$$\ell(f(x+y)) = \ell(f(x) + f(y)) + \alpha(x)\beta(y), \quad \textit{and}$$
$$\alpha(x)\beta(y) = \alpha(y)\beta(x) \quad \textit{for any } x, y \in \mathbb{F}_{p^n}.$$

Example 2.8 Let θ be an element of $\mathbb{F}_9$ such that $\theta^2 = -1$ and $f(X)$ be a planar function on $\mathbb{F}_9$ such that $f(X) = \theta X^2 + X^4 + X^6$. Set $\ell(x + y\theta) = (x - y) + y\theta$, $\alpha(x + y\theta) = (x - y) - x\theta$ and $\beta(x + y\theta) = -y + (x + y)\theta$ where $x, y \in \mathbb{F}_3$. Then $\alpha(X)\beta(Y) = \beta(X)\alpha(Y)$ for $\forall X, Y \in \mathbb{F}_9$ and they satisfy $\ell(f(X + Y)) = \ell(f(X)) + \ell(f(Y)) - \alpha(Y)\beta(X)$. Therefore $I(\mathbb{F}_9, \mathbb{F}_9; f)$ is desarguesian from the Theorem 2.7.

3. Planar functions of quadratic polynomials

A finite algebraic structure $G(+, \circ)$ which is a group with respect to addition, and whose nonzero elements form a loop with respect to multiplication, such that the mappings

$$x \mapsto -xa + xb \quad \text{and} \quad x \mapsto ax - bx$$

are permutations of G whenever $a \neq b$ is called a cartesian group. A cartesian group $T(+, \circ)$ satisfying the left distribution law is called a finite left quasifield which correspond to a translation plane and a left quasifield $E(+, \circ)$ satisfying also the right distribution law is called a finite semifield which correspond to a semifield plane. We note a left quasifield is always commutative with addition (see, [2], [15], [16], [17]).

Let g be a planar function over $\mathbb{F}_{p^n}$. If we put $f(x) := g(x - a) + b$ we see f is also planar and $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; f) = I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; g)$. We can choose elements a, b such that $f(0) = 0$ and $f(1) = 0$. Then we call f is the normed function

of g. We define $x^\mu := -f(x)+f(x+1)$ where $x \in \mathbb{F}_{p^n}$ and consider $\varphi = \mu^{-1}$. Now we introduce a new multiplication $(\circ)$ in the additive group $\mathbb{F}_{p^n}$ by P. Dembowski and T.G. Ostrom.

Theorem 3.1 (Dembowski and Ostrom, Th. 6 and Cor. 4 in [5]) *Let f be a normed planar function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$, and define a multiplication in $\mathbb{F}_{p^n}$ by the rule*

$$u \circ v = -f(u^\varphi) + f(u^\varphi + v^\varphi) - f(v^\varphi).$$

Then

(i) *$\mathbb{F}_{p^n}$ becomes, with the original addition and this multiplication, a cartesian group coordinatizing the affine plane $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; f)$.*

(ii) *The affine plane $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; f)$ is a translation plane if and only if*

$$\begin{aligned} &-f(x)+f(x+z)-f(z)-f(y)+f(y+z) \\ &\qquad = -f((x^\mu+y^\mu)^\varphi)+f((x^\mu+y^\mu)^\varphi+z) \end{aligned}$$

for all x, y, $z \in \mathbb{F}_{p^n}$.

We define a quadratic planar function over $\mathbb{F}_{p^n}$ as a planar function such that

$$g(x) = \sum_{0 \le i \le j \le n-1} \alpha_{i,j} x^{p^i} x^{p^j},$$

regarded a function between the additive group $\mathbb{F}_{p^n}$ for $\alpha_{i,j} \in \mathbb{F}_{p^n}$. We obtain the following theorem.

Theorem 3.2 *Suppose that g is a quadratic planar function over $\mathbb{F}_{p^n}$. Then $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; g)$ is a semifield plane.*

Proof. Suppose that g is a quadratic planar function over $\mathbb{F}_{p^n}$. We consider the normed planar function f of g and μ and φ as above. Then we have the following.

$$f(x) = \sum_{0 \le i \le j \le n-1} \alpha_{i,j} (x-a)^{p^i} (x-a)^{p^j} + b$$

where $\sum_{0 \le i \le j \le n-1} \alpha_{i,j} a^{p^i} a^{p^j} + b = 0$ and $\sum_{0 \le i \le j \le n-1} \alpha_{i,j} (1-a)^{p^i} (1-a)^{p^j} + b = 0$, and

$$x^\mu = \sum_{0 \le i \le j \le n-1} \alpha_{i,j} (x^{p^i} + x^{p^j}).$$

Therefore μ is additive. Hence we obtain the following equation from (ii) in Theorem 3.1.

$$\begin{aligned} -f(x)+f(x+z)-f(z)-f(y)+f(y+z)& \\ =-f(x+y)+f(x+y+z)& \end{aligned}$$

This equation is easily verified. Hence $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; f)$ is a translation plane by Theorem 3.1. Then since $(\mathbb{F}_{p^n}, +, \circ)$ is commutative with respect to addition, it is also commutative with respect to multiplication by the definition of multiplication. Thus left and right distribution laws are satisfied in it. Hence $(\mathbb{F}_{p^n}, +, \circ)$ is a commutative semifield and the affine plane $I(\mathbb{F}_{p^n}, \mathbb{F}_{p^n}; g)$ is a semifield plane. □

Theorem 3.3 *Suppose that n is odd with $n \geq 3$ and α is an element of $\mathbb{F}_{3^n}^*$. For the function $g(x) = x^{10} - \alpha x^6 - \alpha^2 x^2$ over $\mathbb{F}_{3^n}$, the following statements are equivalent.*

(i) *$I(\mathbb{F}_{3^n}, \mathbb{F}_{3^n}; g)$ is the desarguesian plane.*

(ii) *$n = 3$ and α is square of $\mathbb{F}_{3^3}$*

Proof. We argue in the general form of a quadratic planar function g over $\mathbb{F}_{p^n}$ and from a half of the proof we shall specify g to be one of Ding and Yuan. Let g be a quadratic planar function and f be the normed planar function of g for $\alpha_{i,j} \in \mathbb{F}_{p^n}$.

$$g(x) = \sum_{0 \leq i \leq j \leq n-1} \alpha_{i,j} x^{p^i} x^{p^j} \tag{1}$$

$$f(x) = \sum_{0 \leq i \leq j \leq n-1} \alpha_{i,j} (x^{p^i} x^{p^j} - a^{p^i} x^{p^j} - x^{p^i} a^{p^j}) \tag{2}$$

$$\begin{aligned} x^\mu &= \sum_{0 \leq i \leq j \leq n-1} \alpha_{i,j} (x^{p^i} + x^{p^j}) \\ &= \sum_{0 \leq k \leq n-1} \alpha_k x^{p^k} \end{aligned} \tag{3}$$

Since μ is bijective and linear over $\mathbb{F}_p$, $\varphi = \mu^{-1}$ is also written as

$$x^\varphi = \sum_{0 \leq k \leq n-1} \beta_k x^{p^k}$$

where $\beta_k \in \mathbb{F}_{p^n}$. We get the following equation because of $(x^\mu)^\varphi = x$.

$$\begin{pmatrix} \alpha_0 & {\alpha_{n-1}}^p & \cdots & \cdots & {\alpha_2}^{p^{n-2}} & {\alpha_1}^{p^{n-1}} \\ \alpha_1 & {\alpha_0}^p & \cdots & \cdots & {\alpha_3}^{p^{n-2}} & {\alpha_2}^{p^{n-1}} \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \alpha_{n-1} & \cdots & \cdots & \cdots & {\alpha_1}^{p^{n-2}} & {\alpha_0}^{p^{n-1}} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \vdots \\ \beta_{n-2} \\ \beta_{n-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad (4)$$

We denote the square matrix of (4) by M, and the matrix giving p-power to each component of M by M^p. We permute rows and columns of M respectively by the permutation $(n, n-1, \ldots, 2, 1)$. Then we obtain the matrix M^p. Therefore $|M| = |M^p|$. However $|M|^p = |M^p|$ by the definition of the determinant of the matrix. Therefore $|M| = |M|^p$. Hence we have $|M| \in \mathbb{F}_p$.

If it is satisfied the associative law of multiplication in the commutative semifield $(\mathbb{F}_{p^n}, +, \circ)$ with the multiplication in Theorem 3.1, the corresponding semifield plane become desarguesian. Suppose that the associative law holds in $(\mathbb{F}_{p^n}, +, \circ)$. Now $u \circ v = f(x+y) - f(x) - f(y)$ where $x = u^\varphi$ and $y = v^\varphi$. We put $u \circ v = \ell(x, y)$. Then $\ell(x, y) = \sum_{0 \le i \le j \le n-1} \alpha_{i,j}(x^{p^i} y^{p^j} + x^{p^j} y^{p^i})$. Then the following equivalence holds.

$$(u \circ v) \circ w = u \circ (v \circ w) \Longleftrightarrow \ell(\ell(x, y)^\varphi, z) = \ell(x, \ell(y, z)^\varphi)$$

where $w^\varphi = z$.

$$\begin{aligned} \ell(\ell(x, y)^\varphi, z) = \sum_{0 \le h \le k \le n-1} \sum_{t=0}^{n-1} \sum_{0 \le i \le j \le n-1} \big(& \alpha_{h,k} \beta_t^{p^h} \\ & \times \alpha_{i,j}^{p^{t+h}} (x^{p^{i+t+h}} y^{p^{j+t+h}} z^{p^k} + x^{p^{j+t+h}} y^{p^{i+t+h}} z^{p^k}) \\ & + \alpha_{h,k} \beta_t^{p^k} \alpha_{i,j}^{p^{t+k}} (x^{p^{i+t+k}} y^{p^{j+t+k}} z^{p^h} + x^{p^{j+t+k}} y^{p^{i+t+k}} z^{p^h}) \big) \end{aligned} \quad (5)$$

$$\begin{aligned} \ell(x, \ell(y, z)^\varphi) = \sum_{0 \le h \le k \le n-1} \sum_{t=0}^{n-1} \sum_{0 \le i \le j \le n-1} \big(& \alpha_{h,k} \beta_t^{p^k} \\ & \times \alpha_{i,j}^{p^{t+k}} (x^{p^h} y^{p^{i+t+k}} z^{p^{j+t+k}} + x^{p^h} y^{p^{j+t+k}} z^{p^{i+t+k}}) \\ & + \alpha_{h,k} \beta_t^{p^h} \alpha_{i,j}^{p^{t+h}} (x^{p^k} y^{p^{i+t+h}} z^{p^{j+t+h}} + x^{p^k} y^{p^{j+t+h}} z^{p^{i+t+h}}) \big) \end{aligned} \quad (6)$$

From now on we consider the planar functions $g(x) = x^{10} - \alpha x^6 - \alpha^2 x^2$ by Ding and Yuan for $p = 3$. Then we put $\alpha_{0,2} = 1$, $\alpha_{1,1} = -\alpha$, $\alpha_{0,0} =$

$-\alpha^2$, and the others $\alpha_{i,j} = 0$. Suppose that $n \geq 5$. We compare with the coefficient of $x^3y^{3^2}z$ in (5) and (6). Then we have the coefficient of $x^3y^{3^2}z$ in (5) is zero because of $n \geq 5$ and the coefficient of $x^3y^{3^2}z$ in (6) is $\alpha\beta_{n-1}^3$, thus $\beta_{n-1} = 0$. Next the coefficient of xyz^3 in (5) is $\alpha^3\beta_{n-1}^3 + \alpha^{3^{n-1}+1}\beta_{n-2}^3$ and the coefficient of xyz^3 in (6) is zero. Therefore $\beta_{n-2} = 0$. Now we write down simultaneous equations of (4) as the following.

$$\begin{cases} (1+\alpha^2)\beta_0 + \beta_{n-2} + \alpha^{3^{n-1}}\beta_{n-1} = 1 \\ \alpha\beta_0 + (1+\alpha^2)^3\beta_1 + \beta_{n-1} = 0 \\ \beta_0 + \alpha^3\beta_1 + (1+\alpha^2)^{3^2}\beta_2 = 0 \\ \beta_1 + \alpha^{3^2}\beta_2 + (1+\alpha^2)^{3^3}\beta_3 = 0 \\ \cdots \\ \beta_{n-3} + \alpha^{3^{n-2}}\beta_{n-2} + (1+\alpha^2)^{3^{n-1}}\beta_{n-1} = 0 \end{cases}$$

Therefore we have $\beta_{n-3} = 0$ from $\beta_{n-1} = \beta_{n-2} = 0$ and $\beta_{n-4} = 0$ from $\beta_{n-2} = \beta_{n-3} = 0$. Repeating these we obtain $\beta_i = 0$ for any $i = 0, 1, 2, \ldots, n-1$. However it contradicts to the first equation. Thus if $n \geq 5$ then $I(\mathbb{F}_{3^n}, \mathbb{F}_{3^n}; g)$ is not desarguesian. Suppose that $n = 3$ and $\ell(\ell(x, y)^\varphi, z) = \ell(x, \ell(y, z)^\varphi)$ for any elements x, y and z of $\mathbb{F}_{3^3}$. Then we have $\alpha^{13} = 1$ by comparing the corresponding coefficients of right sides of (5) and (6). For example coefficients of xyz^3 are the following

$$\begin{aligned} &\varepsilon(-\alpha^3 - \alpha^{21} + \alpha^{10} - \alpha^{13}) \quad \text{in } \ell(\ell(x, y)^\varphi, z) \\ &\varepsilon(-1 + \alpha^{10} - \alpha^3 - \alpha^{21}) \quad \text{in } \ell(x, \ell(y, z)^\varphi) \end{aligned}$$

where $\varepsilon = 1$ or $\varepsilon = -1$. Here we used the fact $|M| = \varepsilon \in \{\pm 1\}$ which is obtained by the previous comments. Conversely $\ell(\ell(x, y)^\varphi, z) = \ell(x, \ell(y, z)^\varphi)$ holds if $\alpha^{13} = 1$. We note $\alpha^{13} = 1$ iff α is square. Thus the theorem is proved. □

4. Planar functions and commutative semifields

The square mapping of a finite commutative semifield E of the characteristic p ($p \neq 2$) is a planar function on the additive group E (see pp. 245 in [4]). Now we state this fact against the background of a relative difference set in an automorphism group of E.

Theorem 4.1 (cf. [23]) *Let G and H be finite groups of same order n. Then the following* (i) *and* (ii) *are equivalent.*

(i) *f is a planar function from G into H.*
(ii) *$\{(x, f(x)) \mid x \in G\}$ is a relative difference set in $G \times H$ with respect to H with parameters $(n, n, n, 1)$.*

Let $E(+, \circ)$ be a commutative semifield of order $q = p^e$ where p is an odd prime. Naturally an affine plane $\boldsymbol{A}(E)$ is defined by taking $E \times E = \{(x, y) \mid x, y \in E\}$ as the set of points and a second copy $E \times E = \{[x, y] \mid x, y \in E\}$ as the set of lines. The point (x, y) lies on the line $[a, b]$ if and only if

$$y = a \circ x + b.$$

Moreover we adjoin to them lines with slope ∞, namely the line consisting of the points

$$(c, y) \quad (y \in E)$$

for each c in E. Then we consider following two groups of order q^2.

$$T := \{T_{a,b} \mid a, b \in E\} \quad \text{where } T_{a,b}(x, y) = (x + a, y + b)$$
$$S := \{S_{u,v} \mid u, v \in E\} \quad \text{where } S_{u.v}(x, y) = (x, y + u \circ x + v)$$

We note the group T acts regularly on points, and the group S acts regularly on the lines except lines with slope ∞. Set $H_{u,b} := T_{u,b}S_{u,0}$. Then $G := \{H_{u,b} \mid u, b \in E\}$ is an abelian group. Moreover set

$$D := \{H_{u,0} \mid u \in E\},\ H := \{H_{0,b} \mid b \in E\},\ K := \{H_{u,g(u)} \mid u \in E\}$$

where g satisfies $g(u + v) = g(u) + g(v) + u \circ v$. Then H, K are subgroups of G and D is a subset of G, and the following theorem is known.

Theorem 4.2 (C. Godsil and A. Roy [10]) *Let E be a commutative semifield of order q, where q is a prime power. Then the group G is abelian with order q^2, and the subset D is a relative difference set in G with parameters $(q, q, q, 1)$.*

We note $G = K \times H$. Hence this theorem and Theorem 4.1 implies that there is a planar function f from K into H. The semifield E and the group K are isomorphic as additive groups by a corresponding from u to $H_{u,g(u)}$, E and the group H are isomorphic as additive groups by a corresponding from b to $H_{0,b}$. The map f can be regarded as a function on E such that $f(u) = b = -(1/2)u \circ u$. Then $f(u) = -(1/2)u \circ u$ is planar. Therefore

if E is a commutative semifield of order q, then the function f defined by $f(x) = x \circ x$ $(x \in E)$ is a planar function on the additive group E.

We note that $I(\mathbb{F}_q, \mathbb{F}_q; f)$ is isomorphic to the plane coming from the original semifield E. We calculated explicit forms of the square mappings of known finite commutative semifields as polynomials on finite fields in the following.

Dickson semifields Assume that $q = p^n$ where p is an odd prime and $n > 1$ and let α be any element of $\mathbb{F}_q$ which is not square. The semifield E can be identified with the additive group $\mathbb{F}_{q^2}$ and be constituted as two dimensional vector space over $\mathbb{F}_q$ with basis 1 and λ where $\lambda^2 = \alpha$. Let σ be an automorphism of $\mathbb{F}_q$ given by $x^\sigma = x^{p^r}$, $1 \leq r < n$, we define a multiplication in E by

$$(a + \lambda b) \circ (c + \lambda d) := ac + \alpha(bd)^\sigma + \lambda(ad + bc).$$

We consider planar functions of quadratic polynomials and express them in the finite field, and put $X = x + \lambda y \in \mathbb{F}_{q^2}$.

$$\begin{aligned}
\mathbb{F}_{q^2} &\longrightarrow \mathbb{F}_{q^2} \\
f\colon X &\longmapsto X \circ X &&= x^2 + \alpha y^{2p^r} + 2\lambda xy \\
g_1\colon X &\longmapsto X^2 &&= x^2 + \alpha y^2 + 2\lambda xy \\
g_2\colon X &\longmapsto X^{1+p^n} &&= x^2 - \alpha y^2 \\
g_3\colon X &\longmapsto X^{2p^n} &&= x^2 + \alpha y^2 - 2\lambda xy
\end{aligned}$$

Consequently,

$$(g_1 + g_3 - 2g_2)(X) = X^2 + X^{2p^n} - 2X^{1+p^n} = 4\alpha y^2.$$

Therefore

$$\begin{aligned}
y^2 &= 4^{-1}\alpha^{-1}(X^2 + X^{2p^n} - 2X^{1+p^n}), \\
(y^2)^{p^r} &= 4^{-1}\alpha^{-p^r}(X^2 + X^{2p^n} - 2X^{1+p^n})^{p^r}, \\
&= 4^{-1}\alpha^{-p^r}(X^{2p^r} + X^{2p^{(n+r)}} - 2X^{p^r+p^{(n+r)}}).
\end{aligned}$$

On the other hand

$$(f - g_1)(X) = X \circ X - X^2 = \alpha(y^{2p^r} - y^2).$$

Hence

$$f(X) - g_1(X) = 4^{-1}\alpha^{1-p^r}(X^{2p^r} + X^{2p^{(n+r)}} - 2X^{p^r+p^{(n+r)}})$$

$$- 4^{-1}(X^2 + X^{2p^n} - 2X^{1+p^n}).$$

Therefore

$$f(X) = X^2 + 4^{-1}\alpha^{1-p^r}(X^{2p^r} + X^{2p^{(n+r)}} - 2X^{p^r+p^{(n+r)}}) \\ - 4^{-1}(X^2 + X^{2p^n} - 2X^{1+p^n}).$$

We calculate the square mappings of other known several semifields as functions over finite fields in the similar way.

Cohen-Ganley semifields A multiplication in $(\mathbb{F}_{q^2}, +)$ is defined as

$$(a + \lambda b) \circ (c + \lambda d) := (ac + \alpha bd + \alpha^3(bd)^9) + \lambda(ad + bc + \alpha(bd)^3)$$

with $q = 3^n$ $(n \geq 2)$ and α is nonsquare in $\mathbb{F}_q$ and $\{1, \lambda\}$ is a basis over $\mathbb{F}_q$ where $\lambda^2 = \alpha$.
Then $f(X) = X \circ X$ is expressed as the following.

$$f(X) = X^2 + \alpha^{-2}\lambda(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}}) \\ + \alpha^{-6}(X^{18} + X^{2\cdot 3^{n+2}} + X^{9+3^{n+2}})$$

Ganley semifields Consider $(\mathbb{F}_{q^2}, +)$ where $q = 3^n$, $n \geq 3$ where n is odd and α is nonsquare in $\mathbb{F}_q$ and $\{1, \lambda\}$ is a basis over $\mathbb{F}_q$ where $\lambda^2 = \alpha$. A multiplication is defined as

$$(a + \lambda b) \circ (c + \lambda d) := (ac - b^9 d - bd^9) + \lambda(ad + bc + b^3 d^3).$$

Then we have

$$f(X) = X^2 + \lambda^{-10}(X^{10} + X^{3^n+3^{n+2}} - X^{9+3^n} - X^{1+3^{n+2}}) \\ + \alpha^{-3}\lambda(X^6 + X^{2\cdot 3^{n+1}} + X^{3+3^{n+1}}) \\ - (X^2 + X^{2\cdot 3^n} + X^{1+3^n}).$$

Penttila-Williams semifields Consider $(\mathbb{F}_{q^2}, +)$ where $q = 3^5$ and α is nonsquare in $\mathbb{F}_q$ and $\{1, \lambda\}$ is a basis over $\mathbb{F}_q$ where $\lambda^2 = \alpha$. A multiplication is defined as

$$(a + \lambda b) \circ (c + \lambda d) := (ac + (bd)^9) + \lambda(ad + bc + (bd)^{27}).$$

Then we have

$$f(X) = X^2 + \alpha^{-9}(X^{18} + X^{2\cdot 3^7} + X^{9(1+3^5)}) \\ + \alpha^{-27}\lambda(X^{54} + X^{2\cdot 3^8} + X^{27(1+3^5)})$$

$$-(X^2 + X^{2\cdot 3^5} + X^{1+3^5}).$$

Coulter-Matthews semifields Consider $(\mathbb{F}_q, +)$ where $q = 3^n$, and n is odd with $n \geq 3$. A multiplication is defined as $x \circ y := x^9y + xy^9 + x^3y^3 - xy$. Then we have

$$f(x) = -x^{10} + x^6 - x^2.$$

Ding-Yuan semifields Consider $(\mathbb{F}_q, +)$ where $q = 3^n$ and n is odd with $n \geq 3$. A multiplication is defined as $x \circ y := x^9y + xy^9 - x^3y^3 - xy$. We have

$$f(x) = -x^{10} - x^6 - x^2.$$

5. Discussion

It is a difficult problem to determine whether planar functions coming from commutative semifields as square mappings are quadratic planar functions or not. This problem is related to the classification problem of finite commutative semifields. Let V be a n dimensional vector space over the prime field $\mathbb{F}_p$ for an odd prime p, and $\{v_1, \ldots, v_n\}$ be a basis of V. Now we give a set Ω of n symmetric square matrices of degree n where every entry is an element of $\mathbb{F}_p$, say $\Omega = \{A_1, \ldots, A_n\}$. Moreover we define a multiplication of V as the following

$$u \circ v := \sum_{i=1}^{n} (\alpha_1, \ldots, \alpha_n) A_i \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} v_i$$

for $u = \sum_{i=1}^n \alpha_i v_i$ and $v = \sum_{i=1}^n \beta_i v_i$.
If V has no zero factors with respect to this multiplication, then $(V, +, \circ)$ is a commutative semifield.
Here the addition is that of the vector space V. We consider the following condition (♣)

(♣): $$\det\left(A_1 \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \cdots, A_n \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \right) \neq 0$$

for any $(x_1, \ldots, x_n) \in (\mathbb{F}_p)^n$ except $(x_1, \ldots, x_n) = 0$.
Obviously V has no zero factors iff the condition (♣) holds. We can write

down the determinant above as

$$F(x_1, \ldots, x_n) = \sum_{i_1+\cdots+i_n=n} a_{i_1\cdots i_n} {x_1}^{i_1} \cdots {x_n}^{i_n}.$$

Thus $F(x_1, \ldots, x_n) = 0$ is a hyper surface in the $n-1$ dimensional projective space over $\mathbb{F}_{p^n}$. Suppose that the hyper surface has no zero points over $\mathbb{F}_p$. Then the condition (♣) holds, and the converse is also true. Hence a construction problem of commutative semifields results in the problem whether a suitable hyper surface of the projective space over a finite field has rational points or not over the prime field. For example

$$x^3 + y^3 + z^3 + x^2y + x^2z - 2xz^2 + y^2z - 3xyz = 0$$

is a hyper surface in $PG(2, 5^3)$ and it has no rational points over $\mathbb{F}_5$, though this example is one which comes from the $\mathbb{F}_{5^3}$, not a proper commutative semifield.

References

[1] Blokhuis A., Jungnickel D. and Schmidt B., *Proof of the prime power conjecture for projective planes of order n with abelian collineation groups*. Proc. Amer. Math. Soc. **130** (2002), 1473–1476.

[2] Cordero M. and Wene P.G., *A survey of finite semifields*. Disc. Math. **208/209** (1999), 125–137.

[3] Coulter S.R. and Matthews W.R., *Planar Functions and Planes of Lenz-Barlotti Class* II. Codes and Cryptography **10** (1997), 167–184.

[4] Dembowski P., *Finite Geometries*. Springer-Verlag New York Inc., 1968.

[5] Dembowski P. and Ostrom G.T., *Planes of Order n with Collineation Groups of Order n^2*. Math. Z. **103** (1968), 239–258.

[6] Ding C. and Yuan J., *A new family of skew Hadamard difference sets*. to appear in J. Combin. Theory Ser. A.

[7] Fung I.C., Siu K.M. and Ma L.S., *On arrays with small off-phase binary autocorrelation*. Ars Comb. **29A** (1990), 189–192.

[8] Ganley J.M., *On a paper of Dembowski and Ostrom*. Arch. Math. **27** (1976), 93–98.

[9] Gluck D., *A note on permutation polynomials and finite geometries*. Disc. Math. **80** (1990), 97–100.

[10] Godsil C. and Roy A., *Equiangular lines, mutually unbiased bases, and spin models*. preprint.

[11] Hiramine Y., *A conjecture on affine planes of prime order*. J. Combin. Theory Ser. A **52** (1989), 44–50.

[12] Hiramine Y., *On planar functions*. J. Algebra **133** (1990), 103–110.

[13] Hiramine Y., *Factor sets associated with regular collineation groups.* J. Algebra **142** (1991), 414–423.
[14] Hiramine Y., *Planar functions and related group algebras.* J. Algebra **152** (1992), 135–145.
[15] Kantor M.W., *Commutative semifields and symplectic spreads.* J. Algebra **270** (2003), 96–114.
[16] Kantor M.W., *Finite semifields.* Finite geometries, Groups and Computation, A. Hulpke, B. Liebler, T. Penttila and A. Seress, eds., Walder de Gruyter, Berlin-New York, 2006.
[17] Knuth E.D., *Finite Semifields and Projective Planes.* J. Algebra **2** (1965), 182–217.
[18] Ma L.S. and Pott A., *Relative difference sets, planar functions and generalized Hadamard matrices.* J. Algebra **175** (1995), 505–525.
[19] Nakagawa N., *The non-existence of right cyclic planar functions of degree p^n for $n \geq 2$.* J. Combin. Theory Ser. A **63** (1993), 55–64.
[20] Nakagawa N., *Left Cyclic Planar Functions Of Degree p^n.* Utilitas mathematica **51** (1997), 89–96.
[21] Nakagawa N., *On Polynomial Families in n Indeterminates over Finite Prime Fields Coming from Planar Functions, Proceedings of the sixth Conference of Finite Fields with Applications to Coding Theory, Cryptography and related Areas.* Springer-Verlag, Berlin, 2002.
[22] Nakagawa N., *Planar Functions between Elementary Abelian Groups.* preprint.
[23] Pott A., *Finite geometry and character theory.* Lecture Note, vol. 1601, Springer-Verlag, Berlin, 1995.
[24] Ronyai L. and Szonyi T., *Planar functions over finite fields.* Combinatorica, **9** (1989), 315–320.

K. Minami
Department of Mathematics
Faculty of Science and Technology
Kinki University
3-4-1 Kowakae, Higashi Osaka
Osaka 577-8502 Japan
minami@math.kindai.ac.jp

N. Nakagawa
Department of Mathematics
Faculty of Science and Technology
Kinki University
3-4-1 Kowakae, Higashi Osaka
Osaka 577-8502 Japan
nakagawa@math.kindai.ac.jp