AKCE J. Graphs. Combin., 5, No. 1 (2008), pp. 21-28

A note on planar functions of degree p^2

Nobuo Nakagawa
Department of Mathematics
Faculty of Science and Technology
Kinki University, 3-4-1 Kowakae, Higashi Osaka
Osaka 577-8502, Japan
e-mail: *nakagawa@math.kindai.ac.jp*
and
Naomi Watanabe
Toobu junior highschool
20 Nishigouchi, Simo-nagarachiyo,Nishio-shi
Aichi 445-0016, Japan

Communicated by: Mariko Hagita
Received 6 February 2008; revised 28 April 2008; accepted 1 May 2008

Abstract

We determined planar functions which are power functions on the additive group $GF(p^2)$ where p is an odd prime. This result asserts that a planar power function on the additive group $GF(p^{2n})$ shoud be of the form $f(x) = x^{t(p^2-1)+2p^i}$ for a suitable non-negative integer t and $i \in \{0, 1\}$.

Keywords: finite fields, planar functions, permutation polynomials, differential equations.

2000 Mathematics Subject Classification: 51E20

1. Introduction

Planar functions were defined by T.G. Ostrom and P. Dembowski in a paper they researched finite affine planes admitting a regular collineation groups on the set of points [4]. Suppose that G and H are finite groups of order n. Then a mapping f from G into H is called a planar function of degree n if f satisfies the following condition.
($\bigstar$) A mapping f_a defined by $f_a(x) = f(ax)f(x)^{-1}$ is a bijection from G onto H for any nontrivial element $a \in G$.

If f is a planar function of degree n from G into H then we can construct the affine plane $\mathbf{A}(f; G, H)$ of order n by taking $G \times H$ as the set of points and $\{(g, 1)H \mid g \in G\} \cup \{(g, h)D \mid g \in G, h \in H\}$ where $D := \{(x, f(x)) \mid x \in G\}$ as the set of lines. Naturally the group $G \times H$ acts regularly on the set of points of $\mathbf{A}(f; G, H)$ and the set

D above is a $(n, n, n, 1)$ relative difference set in $G \times H$ with respect to H. Moreover an algebraic structure which is called a cartesian group is constructed from a planar function. A cartesian group corresponds to an affine plane $\mathbf{A}$ having the (P, ℓ)-transitive property for a flag (P, ℓ) of $\mathbf{A}$ (see [3], [4]). It was shown that the degree of a planar function is an odd positive integer in [4].

We give the main results concerning planar functions by a series of theorems.

Theorem 1.1. [5],[6] and [13] *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 the desarguesian.*

Theorem 1.2. [10] and [11] *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*

$$\exp(H) \leqq \begin{cases} p^{\frac{n+1}{2}} & (n : odd) \\ p^{\frac{n}{2}} & (n : even) \end{cases}$$

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

Theorem 1.3. [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 1.4. [7] *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 $ord_p(q)$ is even, then the square free part of n is not divisible by q.*

Example 1.5. *Suppose that G is the Frobenius group of order 21 and H is the cyclic group of order 21. Then there exists no planar functions from G into H because $ord_7(3) = 6$ and 21 is divisible by 3.*

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

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

Here Tr is the trace mapping of the extension $GF(p^n)/GF(p)$. Namely $\hat{\varphi}$ is the Fourier coefficient of φ. Then φ is named a bent function if and only if $|\hat{\varphi}(u)| = p^{\frac{n}{2}}$ for any $u \in GF(p^n)$. Bent functions are important ones in the field of the cryptography theory and the coding theory.

Theorem 1.6. [12] *We assume* $G \cong H \cong \mathbb{Z}_p^n$ *where* $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, *and* $f(\mathbb{X}) = (f_1(\mathbb{X}), \cdots, f_n(\mathbb{X}))$ *is a function from* G *into* H *for* $\mathbb{X} = (u_1, \cdots, u_n)$. *Then* f *is planar if and only if*

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

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

Many planar functions are known, however known examples are all functions between the additive group $GF(p^n)$ for an odd prime p (see [9]).

2. Planar functions of degree p^2 which are power functions on $GF(p^2)$

We give the following two lemmas which are available to prove the main theorem.

Lemma 2.1. ([8], pp.349) *Let* $a_0, a_1, \cdots, a_{q-1}$ *be elements of the finite field* $GF(q)$. *Then the following two conditions are equivalent:*
(i) $a_0, a_1, \cdots, a_{q-1}$are distinct,
(ii) $\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for t} = 0, 1, \cdots, \text{q} - 2 \\ -1 & \text{for t} = \text{q} - 1. \end{cases}$
(Here it is defined as $0^0 = 1$.)

Lemma 2.2. *Let* p *be an odd prime and* m, n *be integers such that* $0 \leq m < p$ *and* $0 \leq n < p$. *Then the congruent equation*

$$(pm + n)!/n!(p!)^m \equiv m! \pmod{\text{p}}$$

holds.

The lemma is proved as the following. We have
$(pm + n)! = (pm + n)(pm + n - 1) \cdots (pm + 1)(pm)!$ and $n!(p!)^m = n!p^m((p-1)!)^m$
Therefore

$$(pm + n)!/(p^m) \equiv n!((p-1)!)^m m! \pmod{\text{p}}$$
$$\text{and } (n!(p!)^m)/(p^m) \equiv n!((p-1)!)^m \pmod{\text{p}}.$$

Thus our assertion is verified.

We prove the following theorem in this section.

Theorem 2.3. *Suppose that* $f(x) = x^d$ *is a power function on* $GF(p^2)$ *for an integer* d *with* $0 \leq d < p^2$. *If* f *is a planar function between the additive group* $GF(p^2)$, *then* $d = 2$ *or* $d = 2p$.

Proof. We may prove that $g(x) := (x+1)^d - x^d$ is a permutation polynomioal on $GF(p^2)$ if and only if $d = 2$ or $d = 2p$ from Proposition 2.4 in [2]. Moreover we also have $d = k(p-1)+2$ for an integer k such that $0 \leq k \leq p$ from Proposition 2.4 in [2]. It is clear that $f(x) = x^2$ and $f(x) = x^{2p}$ are planar functions on $GF(p^2)$. On the other hand $(x+1)^{p+1} - x^{p+1} = 1$ for any $x \in \mathrm{Ker(Tr)}$ where Tr is the trace mapping on $GF(p^2)$. Therefore $f(x) = x^{p+1}$ is not a planar function on $GF(p^2)$. Thus we may assume that $k > 2$.

If $p = 3$, then $k = 3$. Therefore $d = 8$. We can easily check that $f(x) = x^8$ is not a planar function on $GF(9)$. Thus we may assume that $p \geq 5$.

We prove that

$$\sum_{x \in GF(p^2)} ((x+1)^d - x^d)^{p+1} \neq 0.$$

Then it holds that $f(x) = x^d$ is not planar on $GF(p^2)$ by Lemma 2.2. We have the following.

$$\begin{aligned}((x+1)^d - x^d)^{p+1} &= ((x+1)^{pd} - x^{pd})((x+1)^d - x^d) \\ &= (x+1)^{(p+1)d} + x^{(p+1)d} - (x+1)^{pd}x^d - x^{pd}(x+1)^d.\end{aligned}$$

It is clear that d is not divisible by $p-1$. Hence $(p+1)d$ is not divisible by p^2-1. Therefore $\sum_{x \in GF(p^2)} (x+1)^{(p+1)d} = 0$ and $\sum_{x \in GF(p^2)} x^{(p+1)d} = 0$ at $GF(p^2)$ by Lemm2.1. Next we calculate

$$\sum_{x \in GF(p^2)} (x+1)^{pd}x^d \text{ and } \sum_{x \in GF(p^2)} (x+1)^d x^{pd}.$$

It holds that $(x+1)^{pd}x^d = (x^p+1)^d x^d = \sum_{i=0}^{d} \binom{d}{i} x^{pi+d}$ and $(x+1)^d x^{pd} = \sum_{i=0}^{d} \binom{d}{i} x^{i+pd}$. Hence $\sum_{x \in GF(p^2)} ((x+1)^d - x^d)^{p+1} = -\sum_{x \in GF(p^2)} (\sum_{i=0}^{d} \binom{d}{i} x^{pi+d} + \sum_{i=0}^{d} \binom{d}{i} x^{i+pd}) = -\sum_{i=0}^{d} \binom{d}{i} (\sum_{x \in GF(p^2)} x^{pi+d}) - \sum_{i=0}^{d} \binom{d}{i} (\sum_{x \in GF(p^2)} x^{i+pd})$.

Here $k(p-1)+2 = d \leq pi+d \leq pd+d = k(p^2-1)+2(p+1)$ because $0 \leq i \leq d$. Suppose that $ip + d = n(p^2-1)$ for a positive integer n such that $n \leq k$. Then $i = np - k + (k-n-2)/p$. Since $-p < k-n-2 < p$ and $i \in \mathbf{Z}$ we have $n = k-2$ and $i = (k-2)p - k$.

Therefore $\binom{d}{i} = \binom{k(p-1)+2}{(k-2)p-k} = (k(p-1)+2)!/((k-2)p-k)!(2p+2)!$. However $(k(p-1)+2)!/((k-2)p-k)!(2p+2)! \equiv ((k-1)p+(p-k+2))!/((k-3)p+(p-k))!(2p+2)! \equiv ((k-1)!(p-k+2)!(p!)^{(k-1)})/((k-3)!(p-k)!(p!)^{(k-3)})((2!)(2!)(p!)^2)$ by Lemma 2.2.

Thus the right side of the equation above is congruent $(k-1)^2(k-2)^2/4$ modulo p. Therefore

$$\sum_{x \in GF(p^2)} (x+1)^{pd}x^d \equiv -((k-1)^2(k-2)^2)/4 \pmod{\mathrm{p}} \tag{1}$$

by Lemma 2.1. Now we calculate $\sum_{i=0}^{d} \binom{d}{i} (\sum_{x\in GF(p^2)} x^{i+pd})$. Since $pd = k(p^2-1) - (k-2)p + k$ and $d + pd = k(p^2-1) + 2(p+1)$, it holds that $k(p^2-1) - (k-2)p + k \leq i + pd \leq k(p^2-1) + 2(p+1)$. Therefore if p^2-1 divide $i+pd$ then $i + pd = k(p^2-1)$, namely $i = (k-2)p - k$. Thus we also obtain

$$\sum_{x\in GF(p^2)} (x+1)^d x^{pd} \equiv -((k-1)^2(k-2)^2)/4 \pmod{\text{p}} \tag{2}$$

by Lemma 2.1 and Lemma 2.2 again. Hence

$$\sum_{x\in GF(p^2)} ((x+1)^d - x^d)^{p+1} = ((k-2)^2(k-1)^2)/2 \text{ at } GF(p^2)$$

from (1) and (2). However the right hand value of the equation above is not zero because $2 < k \leq p$. That is $(x+1)^d - x^d$ is not a permutation polynomial where $d = k(p-1)+2$ and $2 < k \leq p$ by Lemma 2.1. It completes the proof of the theorem. □

We note that an affine plane corresponding to $f(x) = x^2$ or $f(x) = x^{2p}$ is desarguesian.

We have the following corollary.

Corollary 2.4. *Suppose that $f(x) = x^d$ is a planar function on $GF(p^{2e})$ for an odd prime p and $e \geq 2$. Then it holds that $d = k(p^2-1)+2$ or $d = k(p^2-1)+2p$ for an integer k such that $0 \leq k \leq (p^{2e}-1)/(p^2-1)$.*

Proof. Set $T := \sum_{i=0}^{e-1} p^{2i}$ and $\mathbf{F} := \{x^T \mid x \in GF(p^{2e})\}$. If $f(x) = x^d$ is planar on $GF(p^{2e})$, then $f(y) = y^2$ or $f(y) = y^{2p}$ for each $y \in \mathbf{F}$ from Theorem 2.3 because $\mathbf{F}$ is isomorphic to $GF(p^2)$ and $f|\mathbf{F}$ is a planar function on $\mathbf{F}$. Therefore $(d-2)T$ or $(d-2p)T$ is divisible by $p^{2e}-1 = (p^2-1)T$. Thus the corollary is verified. □

3. Discussions

It is an important problem to construct planar functions corresponding to non-desarguesian planes. Concerning this problem we proved the following theorem about power functions on $GF(p^4)$ by the similar arguments as in Section 2.

Theorem 3.1. *Let $f(x) = x^d$ be a function on $GF(p^4)$ for an odd prime p and put $A := \{\, ip + j \mid 1 \leq i \leq p-1,\ 3 \leq j \leq p-1 \,\} \cup \{p, 2p, \cdots, (p-1)p\,\}$. If an integer $k \in A$, then $f(x)$ is not a planar function for $d = (k(p^2-1)+2)p^t$ where $0 \leq t \leq 3$.*

Proof. We may assume that $t = 0$ and so $d = k(p^2-1)+2$, $k = ip+j$ and $j \notin \{1, 2\}$. By definition of A, $k \geq p \geq 3$. We may prove that

$$\sum_{x\in GF(p^4)} ((x+1)^d - x^d)^{p^2+1} \neq 0 \text{ at } GF(p^4).$$

Then $(x+1)^d - x^d$ is not a permutation polynomial on $GF(p^4)$ by Lemma 2.1. We note that

$$((x+1)^d - x^d)^{p^2+1} = (x+1)^{(p^2+1)d} + x^{(p^2+1)d} - (x^{p^2}+1)^d x^d - (x+1)^d x^{p^2 d}.$$

We have $\sum_{x\in GF(p^4)}(x+1)^{(p^2+1)d} = 0$ and $\sum_{x\in GF(p^4)} x^{(p^2+1)d} = 0$ because $(p^2-1)d$ is not divisible by p^4-1. Now we calculate

$$\sum_{x\in GF(p^4)} (x^{p^2}+1)^d x^d \text{ and } \sum_{x\in GF(p^4)} (x+1)^d x^{p^2 d}.$$

The former sum is $\sum_{t=0}^{d} \binom{d}{t} (\sum_{x\in GF(p^4)} x^{p^2 t+d})$. It holds that

$$k(p^2-1)+2 = d \le p^2 t + d \le p^2 d + d = (p^4-1)k + 2(p^2+1).$$

Suppose that $p^2 t + d = n(p^4-1)$ for a positive integer n such that $n \le k$. Then $t = (np^2 - k) + (k-n-2)/p^2$. Since $-p^2 < (k-n-2) < p^2$ and t is an integer, we have $n = k-2$, namely $t = (k-2)p^2 - k$. We calculate $\binom{d}{t} = \binom{k(p^2-1)+2}{(k-2)p^2-k} = \binom{k(p^2-1)+2}{2p^2+2.}$ Here we denote by $N_{(p)}([a,b])$ the non-negative integer c satisfying that $b!/a!$ is divisible by p^c but not divisible by p^{c+1} for two positive integers a, b such $a < b$. We obtain easily

$$N_{(p)}([1, 2p^2+2]) = 2p+2 \text{ and } N_{(p)}([(k-2)p^2 - k + 1, k(p^2-1)+2]) = 2p+2$$

because $j = 0$ or $j \ge 3$. Therefore $\binom{k(p^2-1)+2}{2p^2+2} \not\equiv 0 \pmod{p}$. We set $\binom{k(p^2-1)+2}{2p^2+2} = \alpha$. Then $\sum_{t=0}^{d} \binom{d}{t} (\sum_{x\in GF(p^4)} x^{p^2 t+d}) = -\alpha$ by Lemma 2.1. We note that $\alpha \neq 0$.

The latter sum is $\sum_{t=0}^{d} \binom{d}{t} (\sum_{x\in GF(p^4)} x^{t+p^2 d})$. It holds that

$$(p^4-p^2)k + 2p^2 \le t + p^2 d \le d + p^2 d = (p^4-1)k + 2(p^2+1).$$

Hence if $t + p^2 d$ is divisible by $p^4 - 1$, then $t + p^2 d = (p^4-1)k$, namely $t = (k-2)p^2 - k$. Thus we also have $\sum_{t=0}^{d} \binom{d}{t} (\sum_{x\in GF(p^4)} x^{t+p^2 d}) = -\alpha$ by Lemma 2.1. Therefore

$$\sum_{x\in GF(p^4)} ((x+1)^d - x^d)^{p^2+1} = 2\alpha \neq 0.$$

It completes the proof of the theorem. □

For example if we take $p = 5$, there is the possibility that $f(x) = x^d$ is a planar function on $GF(5^4)$ for $d = 146, 170, 266, 290$ or d is one of 5^t times of these numbers for $1 \le t \le 3$. Here the values of d is taken by modulo $5^4 - 1$.

Define as

$$\Delta_d(b) := \sharp\{x \in GF(p^n) \mid (x+1)^d - x^d = b\} \text{ and } \Delta_d := \max_{b\in GF(p^n)} \Delta_d(b).$$

Here we pose the following problem.

Problem 3.2. *Let p be an odd prime and d be an integer $(ip+j)(p^2-1)+2$ for $1 \leq i \leq p-1, j \in \{1,2\}$. Then determine the number Δ_d for $n=4$. Especially is there one pair (i,j) such that $\Delta_d = 1$?*

For a finite affine plane $\mathbf{A}$, if the automorphism group $\mathrm{Aut}(\mathbf{A})$ is (P,ℓ_∞)-transitive and (Q,ℓ_∞)-transitive for distinct points P and Q through the infinity line ℓ_∞ $\mathbf{A}$ is called a translation plane. Of course the desarguesian plane is a translation plane.

For $p=3$, there is an excellent result by S.R. Coulter and W.R. Mattews as the following.

Theorem 3.3. [2] *Let e be a positive integer which is greater than 3 and α be an integer such that* g.c.d.$(\alpha, 2e) = 1$ *and $1 < \alpha < 2e$. Then $f(x) = x^{\frac{3^\alpha+1}{2}}$ is a planar function on $GF(3^e)$. Moreover the affine plane coresponding to the function above is not a translation plane.*

Acknowledgement.

The author wishes to thank the referee for appropriate suggestions concerning many parts of this article.

References

[1] A. Blokhuis, D. Jungnickel and B. Schmidt, 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] S.R. Coulter and W.R.Mattews, Planar Functions and Planes of Lenz-Barlotti Class II, *Codes and Cryptography*, **10**(1997), 167-184.

[3] P. Dembowski, *Finite Geometries*, Springer-Verlag, (1968).

[4] P. Dembowski and T.G. Ostrom, Planes of order n with collineation groups of order n^2, *Math. Z.*, **103** (1968), 239-258.

[5] D. Glück, A note permutation polynomials and finite geometries, *Discrete Math.*, **80**(1990), 97-100.

[6] Y.Hiramine, A conjecture on affine planes of prime order, *J.Combin. Theory, Ser.A*, **52**(1987), 44-50.

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

[8] R. Lidle and H. Niederreiter, Finite Fields, in: *Encyclopedia of Mathematics and its Applications*, **20**, Addison-Wesley, Reading, Massachusetts, 1983.

[9] K. Minami and N. Nakagawa, On planar functions of elementary abelian p-group type, *Hokkaido Mathematical Journal*, (To appear).

[10] N. Nakagawa, The non-existence of right cyclic planar functions of degree p^n for $n \geqq 2$, *J. Combin. Theory, Ser. A*, **63**(1993), 55-64.

[11] N. Nakagawa, Left Cyclic Planar Functions Of Degree p^n, *Utilitas Math.,* **51**(1997), 89-96.

[12] N. Nakagawa, On Polynomial Families in n Indeterminates over Finite Prime Fields Coming Planar Functions, *Proceeding of the Sixth Internationa Conference on Finite Fields and Applications*, Edited by G.Mullen, H Stichtenoth and H.Tapia-Recillas, Springer(2001),251-262.

[13] L. Ronayi and T. Szonyi, Planar functions over finite fields, *Combinatorica*, **9**(1989), 315-320.