数理解析研究所講究録
第846巻 1993年 28-38

Planar functions of type (p,p,···,p) and the numbers of solutions of special polynomial equations over Z_p for an odd prime p

近畿大学理工学部　中 川 暢 夫
(Nobuo Nakagawa)

1. Introduction

Let G and H be two finite groups of order n, and f be a mapping from G into H. If f satisfies the following condition, f is named a planar function from G into H of degree n. For any element u(u≠1) of G and any element α of H, there exists unique element x of G such that $f(ux)f(x)^{-1}=\alpha$.

Let f be a planar function of degree n from G into H. Then we can naturally construct an affine plane A of order n such that G×H acts on the set of points of A regularly. Therefore if we can construct a planar function of no prime power degree, it means to construct a counter example for the following famous conjecture.

Conjecture A; "Orders of finite projective planes are prime power."

One of our purpose is to construct planar functions of no prime power degree. Sorry to say I guess from known results that there is little possibility of the existence of such planar functions(cf.[1],[4],[5]). By the way our another purpose is to solve the following problem.

Problem B; "Determine all planar functions of prime power degree and classify affine planes corresponding to them." Concerning this problem, the following result obtained by Y. Hiramine and D.Gluck shines out.(They showed this theorem independently by different ways.)

Theorem C; "Supppose f is a planar function of degree p for an odd prime p. Then f is a quadratic polynomial as a mapping from Z_p into Z_p, and an affine plane corresponding to f is Desarguesian(cf.[2],[3]).

The following result was shown by N.Nakagawa, C.I.Fung, M.K.Siu and S.L.Ma. Let f be a planar function of degree p^n from G into H for an odd prime p and $n \geq 2$. Then G is not cyclic and H contains no relatively large cyclic subgroups as direct sumonds, specially H is not cyclic(cf.[1],[7],[8]).

Now in the rest of this paper we study about planar functions of degree $p^n (n \geq 2)$ from G into H where G and H are elementary abelian p-groups. Such planar functions is called type $(p,p,\cdots,p)$.

2. The deviation of numbers of the solutions of special polynomial equations in n indeterminates over Z_p.

Let $f(x_1,x_2,\cdots,x_n)$ be a polynomial in n indeterminates over Z_p for an odd prime p. We use $N(f=k)$ to denote the number of solutions of the equation $f(x_1,x_2,\cdots,x_n)=k$ for $k \in Z_p$ and deg(f) to denote the degree of $f(x_1,x_2,\cdots,x_n)$.

Problem 2.1. Let $f(x_1,x_2,\cdots,x_n)=\sum a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ be a polynomial over Z_p with $2\leq\deg(f)$, and λ be the multiplicative character of Z_p of order 2, namely $\lambda(c)=1$ if c is the square of an element of Z_p^* and $\lambda(c)=-1$ otherwise. Moreover we set $\lambda(c)=0$. Then $f(x_1,x_2,\cdots,x_n)$ is a nondegenerate quadratic form if $f(x_1,x_2,\cdots,x_n)$ satisfies the folloeing equations for any fixed element $k\in Z_p$ and a element $k_0\in Z_p$ which depends to k.

(i) Let n be even. $N(i_1x_1+i_2X_2+\cdots+i_nx_n+f(x_1,x_2,\cdots,x_n)=k)$

$$=\begin{cases} p^{(n-1)}+\varepsilon_k p^{(n/2)}-\varepsilon_k p^{(n-2)/2} & (\text{ if } k=k_0 \text{ }) \\ p^{(n-1)}-\varepsilon_k p^{(n-2)/2} & (\text{ otherwise }) \end{cases} \quad (\varepsilon_k\in\{\pm1\}) \text{ for}$$

any elements $i_1,i_2,\cdots,i_n\in Z_p$.

(ii) Let n be odd. $N(i_1x_1+i_2X_2+\cdots+i_nx_n+f(x_1,x_2,\cdots,x_n)=k)$ $= p^{(n-1)}+\varepsilon_k\lambda(k+k_0)p^{(n-1)/2}$ $(\varepsilon_k\in\{\pm1\})$ for any elements $i_1,i_2,\cdots,i_n\in Z_p$.

If $f(x_1,x_2,\cdots,x_n)$ is a nondegenerate quadratic form, then $f(x_1,x_2,\cdots,x_n)$ satisfies the above equations in Problem 2.1(cf.[6], Theorem 6.26 and 6.27). We would like to show that if Problem 2.1 is solved affirmatively, then planar functions of type $(p,p,\cdots,p)$ are nearly decided in the following arguments. On the first time we show the key lemma.

Let G and H be finite groups of order m, and f be a mapping from G into H. We define the Gauss sum $z_{\chi,\rho}$ obtained from f with respect to $\chi\in\mathrm{Irr}(G)$ and $\rho\in\mathrm{Irr}(H)$ as follows.

$$z_{\chi,\rho}=\sum_{\alpha\in H}\Big(\sum_{x\in f^{-1}(\alpha)}\chi(x)\Big)\rho(\alpha).$$

(Here if $f^{-1}(\alpha)=\phi$, we define $\sum_{x\in f^{-1}(\alpha)}\chi(x)$ to be 0.)

Then $z_{\chi,\rho}=\sum_{x\in G}\chi(x)\rho(f(x))$ holds.

Lemma 2.2. Suppose that G and H are abelian groups. Then f is a planar function from G into H if and only if $z_{\chi,p}\overline{z_{\chi,\rho}}=m$ holds for any $\chi\in Irr(G)$ and any $\rho\in Irr(H)$ such that $\rho\neq 1_H$(cf.[5],Theorem 2.6 and [9],Lemma 2.4).

In the remainder of the paper we suppose p is an odd prime and G and H are the additive groups of a finite field $GF(p^n)$. A mapping f from G into H is described as $f(x)=\sum_{i=1}^{p^n-1} a_i x^i$ $(a_i\in GF(p^n))$. We fix an element $\theta\in GF(p^n)$ such that $GF(p^n)=\mathbb{Z}_p(\theta)$, and we set $a_i=a_1^{(i)}+a_2^{(i)}\theta+\cdots+a_n^{(i)}\theta^{(n-1)}$ $(a_j^{(i)}\in\mathbb{Z}_p, 0\leq i\leq p^n-1, 1\leq j\leq n$. Then the indeterminate X over $GF(p^n)$ may be described as $X=x_1+x_2\theta+\cdots+x_n\theta^{(n-1)}$ where $\{x_i \mid 1\leq i\leq n\}$ are indeterminates over $\mathbb{Z}_p$. Then we may set $f(X)=\alpha_1(x_1,\cdots,x_n)+\alpha_2(x_1,\cdots,x_n)\theta+\cdots+\alpha_n(x_1,\cdots,x_n)\theta^{(n-1)}$ for suitable polynomials $\alpha_i(x_1,\cdots,x_n)$ with respect to indeterminates $\{x_1,x_2,\cdots,x_n\}$ over $\mathbb{Z}_p$. Let ω be a primitive p-th root of unity. We put $\tau=\sum_{x\in\mathbb{Z}_p}\lambda(x)\omega^x$. Then it is well known that $\tau\bar{\tau}=p$ holds. For $i_1,i_2,\cdots,i_n\in\mathbb{Z}_p$, we define $\widehat{(i_1,i_2,\cdots,i_n)}\in Irr(G)$ as $\widehat{(i_1,i_2,\cdots,i_n)}(x_1+x_2\theta+\cdots+x_n\theta^{(n-1)})=\omega^{(i_1x_1+i_2x_2+\cdots+i_nx_n)}$. For $s_1, s_2,\cdots,s_n\in\mathbb{Z}_p$, we define $\widehat{(s_1,s_2,\cdots,s_n)}\in Irr(H)$ as well as $\widehat{(i_1,i_2,\cdots,i_n)}$. Moreover $s_1\alpha_1(x_1,x_2,\cdots,x_n)+\cdots+s_n\alpha_n(x_1,x_2,\cdots,x_n)$ will be denoted by $f_{s_1,\cdots,s_n}(x_1,x_2,\cdots,x_n)$.

Lemma 2.3. Let f be a mapping from G into H which is described as $f(x_1+x_2\theta+\cdots+x_n\theta^{(n-1)})=\alpha_1(x_1,\cdots,x_n)+\alpha_2(x_1,\cdots,x_n)\theta+\cdots+\alpha_n(x_{1,}x_2,\cdots,x_n)\theta^{(n-1)}$. Fix an arbitrary element k of Z_p. Then f is a planar function if and only if f satisfies the following equations. $N(i_1x_1+i_2x_2+\cdots+i_nx_n+f_{s_1,s_2,\cdots,s_n}(x_1,x_2,\cdots,x_n)=k)$

$$=\begin{cases} p^{(n-1)}+\varepsilon p^{(n/2)}-\varepsilon p^{(n-2)/2} & (\text{if } k=t) \\ p^{(n-1)}-\varepsilon p^{(n-2)/2} & (\text{otherwise}) \end{cases} \quad \text{in the case n is even,}$$

and $p^{(n-1)}+\varepsilon\lambda(k+t)p^{(n-1)/2}$ in the case n is odd for any $i_1,i_2,\cdots,i_n\in Z_p$ and any $s_1,s_2,\cdots,s_n\in Z_p$ such that $(s_1,s_2,\cdots,s_n)\neq(0,0,\cdots,0)$. Here $\varepsilon\in\{\pm1\}$ and t is a suitable element of Z_p,and ε, t depend on k.

Proof. From Lemma 2.2 f is a planar function if and only if $|Z_{\chi,\rho}|=\pm p^{(n/2)}\omega^t$ if n is even and $|z_{\chi,\rho}|=\pm p^{(n-1)/2}\tau\omega^t$ if n is odd for any $\chi\in Irr(G)$ and any $\rho\in Irr(H)$ such $\rho\neq 1_H$ and a suitable $t\in Z_p$. From the definition of $z_{\chi,\rho}$ above equations implies

$$\sum_{(x_1,x_2,\cdots,x_n)\in Z_p^n} \omega^{(i_1x_1+i_2x_2+\cdots+i_nx_n+f_{s_1,s_2,\cdots,s_n}(x_1,x_2,\cdots,x_n)-t)}$$

$$=\begin{cases} \pm p^{(n/2)} & (\text{if n is even}) \\ \pm p^{(n-1)/2}\tau & (\text{if n is odd}) \end{cases} \quad \text{for any } i_1,i_2,\cdots,i_n,s_1,s_2,\cdots,s_n$$

$\in Z_p$ such that $(s_1,s_2,\cdots,s_n)\neq(0,0,\cdots,0)$. We put

$$\sum_{(x_1,x_2,\cdots,x_n)\in Z_p^n} \omega^{(i_1x_1+i_2x_2+\cdots+i_nx_n+f_{s_1,s_2,\cdots,s_n}(x_1,x_2,\cdots,x_n)-t)}$$

$=\sum_{i=0}^{p-1} c_i\omega^i$. Then we have the following equation.

$c_k= N(i_1x_1+i_2x_2+\cdots+i_nx_n+f_{s_1,s_2,\cdots,s_n}(x_1,x_2,\cdots,x_n)-t=k)$ for any $k\in \mathbb{Z}_p$. Moreover from the equalities $\sum_{i=0}^{p-1} c_i=p^n$ and $\sum_{i=0}^{p-1} c_i\omega^i$

$$=\begin{cases} \pm p^{(n/2)} & \text{(if n is even)} \\ \pm p^{(n-1)/2}\tau & \text{(if n is odd)} \end{cases}$$, it can be shown that

$$\begin{cases} c_0=p^{(n-1)}+\varepsilon p^{(n/2)}-\varepsilon p^{(n-2)/2} & \\ c_i=p^{(n-1)}-\varepsilon p^{(n-2)/2} & (1\le i\le p-1) \end{cases} \text{ if n is even, and}$$

$c_i=p^{(n-1)}+\varepsilon\lambda(i)p^{(n-1)/2}$ $(0\le i\le p-1)$ if n is odd. (Here $\varepsilon\in\{\pm 1\}$.)

Thus the lemma proved.

Now suppose that Problem 2.1 is true. Let $f(X)=\sum_{i=1}^{p^n-1} a_i X^i$ be a mapping from $GF(p^n)$ into $GF(p^n)$. We remark that we may assume $a_{(p^j)}=0$ for all j $(0\le j\le p^{(n-1)}-1)$ without loss of generality if f is a planar function. Then f is described as $f(x_1+x_2\theta+\cdots+x_n\theta^{(n-1)})=\alpha_1(x_1,\cdots,x_n)+\alpha_2(x_1,\cdots,x_n)\theta+\cdots+$ $\alpha_n(x_1,x_2,\cdots,x_n)\theta^{(n-1)}$ with $\deg(\alpha_i(x_1,x_2,\cdots,x_n))\ge 2$ $(1\le i\le n)$. If f is planar, from our assumption and Lemma 2.3 $f_{s_1,s_2,\cdots,s_n}(x_1,x_2,\cdots,x_n)$ is a non-degenerate quadatic form over $\mathbb{Z}_p$ for any $s_1,s_2,\cdots,s_n\in\mathbb{Z}_p$ such that $(s_1,s_2,\cdots,s_n)\ne(0,0,\cdots,0)$. Therefore $\alpha_i(x_1,x_2,\cdots,x_n)$ is a quadratic form for all i $(1\le i\le n)$, which implies $a_i=0$ for many elements i, namely the following equation holds. $f(X)=\sum_{i,j=0}^{n-1} a_{(p^i+p^j)}X^{(p^i+p^j)}$.

Problem 2.4. Let $f(X)=\sum_{i,j=0}^{n-1} a_{(p^i+p^j)}X^{(p^i+p^j)}$ be a mapping from $GF(p^n)$ into $GF(P^n)$. Then find out equivalent conditions for f to be a planar function and describe the equivalent conditions as equations to be satisfied between coefficients of $f(X)$.

3. A partial solutions for Problem 2.1 and Problem 2.4 for n=2

The following theorem is a solution for Problem 2.4 in the case $n=2$. For elements $a,b\in GF(p^2)$, we write $b=\sqrt{a}$ if $a=b^2$ holds.

Theorem 3.1. Let $f(X)=aX^2+bX^{(p+1)}+cX^{2p}$ be a mapping from $GF(p^2)$ into $GF(p^2)$ for an odd prime p. Then f is a planar function on the additive group $GF(p^2)$ if and only if

$$(\sqrt{(ba^p-cb^p)^{(p+1)}-(a^{(p+1)}-c^{(p+1)})^2}\pm(a^{(p+1)}-c^{(p+1)}))^{(p+1)}$$

$\neq(ba^p-cb^p)^{(p+1)}$ holds, and if $b\neq0$, then the following (i) and (ii) hold.

(i) $ba^p\neq cb^p$. (ii) $b^2-4ac\neq0$ if $b^{(p+1)}=4a^{(p+1)}$ or $b^{(p+1)}=4c^{(p+1)}$.

Proof. For $u\in GF(p^2)$ we define a mapping on $GF(p^2)$ f_u as $f_u(x)=f(u+x)-f(x)$. Then f is a planar function if and only if f_u is bijective for any $u\in GF(p^2)\setminus\{0\}$. That is $f_u(x)\neq f_u(y)$ if $x\neq y$. Therefore by direct calculation we get

$(2a+bu^{(p-1)})+(b+2cu^{(p-1)})(x-y)^{(p-1)}\neq0$ for any $u\neq0$ if $x\neq y$ holds. Hence if $b=0$, then $a^{(p+1)}\neq c^{(p+1)}$ holds. Suppose that $b\neq0$. If $2a+bu^{(p-1)}=0$ holds for some $u\in GF(p^2)^*$, then $b+2cu^{(p-1)}\neq0$, and if $b+2cu^{(p-1)}=0$ holds for some $u\in GF(p^2)$, then $2a+bu^{(p-1)}\neq0$. Thus if $b^{(p+1)}=4a^{(p+1)}$ or $b^{(p+1)}=4c^{(p+1)}$ holds, then it follows that $b^2-4ac\neq0$. In other case we have

$((2a+bu^{(p-1)})/(b+2cu^{(p-1)}))^{(p+1)}\neq0$ for any $u\neq0$, which implies that $(ba^p-cb^p)s^2+2(a^{(p+1)}-c^{(p+1)})s+(ab^p-bc^p)\neq0$ for any

$s\in(GF(p^2)^*)^{(p-1)}$. Thus we have $ba^p\neq cb^p$ and $(A/B)^{(p+1)}\neq 1$ where $A=(\pm\sqrt{(ba^p-cb^p)^{(p+1)}-(a^{(p+1)}-c^{(p+1)})^2}-(a^{p+1)}-c^{(p+1)}))$ and $B=(ba^p-cb^p)$. (Here $(ba^p-cb^p)^{(p+1)}-(a^{(p+1)}-c^{(p+1)})^2$ is squre since it belongs to Z_p). Hence the theorem follows.

The following theorem is a partial solution at the case of $n=2$ and f is a cubic form in Problem 2.1.

Theorem 3.2. Let p be an odd prime. Suppose that $f(x,y)$ be a nontrivial cubic form over Z_p. Then there exists elements i,j and k of Z_p such that $N(ix+jy+f(x,y)=k)\notin\{1,p-1,p+1,2p-1\}$, that is a cubic form $f(x,y)$ does not satisfy the equations in Problem 2.1.

Proof. We have proved for the case $p\equiv 1 \pmod 3$ in [10]. Therefore we may assume that $p\not\equiv 1 \pmod 3$. Put $f(x,y)=ax^3+bx^2y+cxy^2+dy^3$. If $f(x,y)$ is transformed into a cubic form $g(X,Y)$ by means of a nonsingular linear substitution of indeterminates, it is named that $f(x,y)$ is equivalent to $g(X,Y)$. Then the deviation of the numbers of solutions of equations $\{ix+jy+f(x,y)=k|k\in Z_p\}$ coincides those of $\{iX+jY+g(X,Y)=k|k\in Z_p\}$. It is shown that the coefficient of X^3 of Y^3 of a suitable cubic form $g(X,Y)$ equivalent to $f(x,y)$ is nonzero. Therefore we may assume $a\neq 0$. Moreover if $b\neq 0$, then $f(x,y)$ is transformed into $AX^3+CXY^2+DY^3$ for some elements A,B and $C\in Z_p$ such that $A\neq 0$ by a linear substitution $x=X+Y, y=((-3a)/b)Y$. Hence we may assume $b=0$ and $a=1$, namely $f(x,y)=x^3+cxy^2+dy^3$. We set the following assumption.

Assumption (#); $N(ix+jy+f(x,y)=k)\in\{1,p-1,p+1,2p-1\}$ for any elements i,j and k of Z_p.

We lead a contradiction from Assumption (#). If $x=0$, then $f=dy^3$. We call dy^3 is the $(x=0)$-part of $f(x,y)$. If $x\neq 0$, we put $ix=y$ for any fixed $i\in Z_p$. Then $f(x,y)=A_ix^3$ where $A_i=1+ci^2+di^3$. We call A_ix^3 is the i-part of $f(x,y)$. (The 0-part of f corresponds to $(y=0)$ and $A_0=1$ holds.)

(1) $d\neq 0$ holds. Suppose that $d=0$. Then $N(f(x,y)=0)\geq p$, therefore by Assumption (#) $N(f=0)=p+1$ or $2p-1$, which implies $A_i=0$ for some $i\in Z_p$. Giving a linear substitution of indeterminates to f as $X=ix$ and $Y=y$, we may assume $A_1=0$. Then $c=-1$ holds and hence $A_{(-1)}=0$, which means that $N(f=0)=3p-2$. This contradicts to Assumption (#).

(2) $A_i=0$ for some $i\in Z_p$. Suppose that $A_i\neq 0$ for all $i\in Z_p$. The i-part of $sx+f(x,y)$ is $sx+A_ix^3$ for a fixed element $s\in Z_p$. It follows that $sx+A_ix^3=0$ has exactly two solutions except $x=0$ if and only if $\lambda(A_i)=\lambda(-s)$ holds. Set $|\{i\in Z_p|\lambda(A_i)=\lambda(-1)\}|=t$. Then we have $N(x+f(x,y)=0)=1+2t$. Hence by Assumption (#), $t=0$ or $t=p-1$ holds. We pick up a element $s\in Z_p$ such that $\lambda(s)=-1$. Then we get $|\{i\in Z_p|\lambda(A_i)=\lambda(-s)\}|=p-t$. Therefore $N(sx+f(x,y)=0)=1+2p$ if $t=0$, and $N(sx+f(x,y)=0)=3$ if $t=p-1$. Whichever we have a contradiction to Assumption (#). Thus we may assume $A_1=0$ as we did in previous arguments. Then $N(f=0)\geq p$ holds. If $A_i\neq 0$ for any element $i\in Z_p$ except $i=1$, it follows that $N(f=0)=p$, which is a contradiction. Therefore $A_j=0$ for some $j\in Z_p$ such that $j\neq 1$ and $j\neq 0$. Thus we get $1+c+d=0$ and $1+cj^2+dj^3=0$, which implies

$d=(j+1)/(j^2)$ and $c=-(j^2+j+1)/(j^2)$. Then since $A_i=((j+1)/(j^2))(i-1)(i-j)(i+(j/(j+1)))$ holds, we get $A_{(-j/(j+1))}=0$. If $-j/(j+1)\notin\{1,j\}$, it follows that $N(f=0)=3p-2$, which is a contradiction. Hence $(-j/(j+1))=1$ of $(-j/(j+1))=j$, that is $j=-2^{-1}$ or $j=-2$ holds. Suppose that $j=-2$. Then we have $A_i=4^{-1}(i+2)^2(1-i)$. Therefore it is shown that $x+A_ix^3=0$ has exactly two nonzero solutions if and only if $\lambda(i-1)=1$. On the other hand $|\{i\in Z_p|\lambda(i-1)=1,i\neq 1,i\neq -2\}|=(p-1)/2$ or $(p-3)/2$ holds. Therefore $N(x+f(x,y)=0)=p$ or $p-2$. This contradicts to Assumption (#). Next suppose that $j=-2^{-1}$. In this case we also have a contradiction as well as the case $j=-2$. Thus Theorem 3.2 proved.

References

[1]. C.I.Fung, M.K.Siu and S.L.Ma: On arrays with small off-phase binary auto correlation, to appear.

[2]. D.Gluck: A note on permutation polynomials and finite geometries, to appear in Discrete Math.

[3]. Y.Hiramine: A conjecture on affine planes of prime order, J. Comb.Theory(A) 52(1989),44-50.

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

[5]. Y.Hiramine: Planar functions and related group algebras, J.Algebra 152(1992),135-145.

[6]. R.Lidl and H.Niederreiter: Finite Fields, Cambridge Univ. Press, Cambridge/London/New York, 1984.

[7]. N.Nakagawa: The non-existence of right cyclic planar

functions of degree p^n for $n \geq 2$, to appear in J.Comb. Theory(A).

[8]. N.Nakagawa: Left cyclic planar functions of degree p^n for $n \geq 2$, submitted in J.Geometry.

[9]. N.Nakagawa: On the planar functions of degree p^n, thesis, 1992.

[10]. N.Nakagawa: (p,p,···,p)型の平面関数について，都筑先生退官記念シンポジウム報告，1993.