数理解析研究所講究録 1440 巻 2005 年 82-96

The behavior of the number of solutions of the difference equations coming from power functions over finite fields

中川 暢夫 (Nobuo Nakagawa)
近畿大学 (Kinki University)

[PARTI]
Finite projective planes and finite affine planes which admit transitive collineation groups on the set of points.

[PARTII]
Planar functions and bent functions.

[PARTIII]
The behavior of the number of solutions of the difference equations coming from power functions over finite fields

[PARTI]

What are finite projective planes and finite affine planes which admit transitive collineation groups on the set of points?

Theorem 1(Kantor)
Let $\mathcal{P}$ be a projective plane of order n. Suppose that a collineation group G acts tansitively on the set of flags of $\mathcal{P}$, and n^2+n+1 is not a prime. Then $\mathcal{P}$ is Desarguesian.
(When n^2+n+1 is a prime, it is solved except the case $n\equiv 0(mod\ \ 8)$ by Feit and others.)

Open problem 1
Suppose that a colliniation group G acts imprimitively on the set of points of a finite projective plane. Then detemine this plane.(Prove this plane is Desarguesian.)
Specially prove when G is a cyclic group and G acts regularly on the set of points.
(Ott and Ho solved partially when a cyclic group acts regularly, under additinal conditions.)

Theorem 2(Hiramine)
Let $\mathcal{P}$ be a finite affine plane. Suppose that a collineation group G acts primitively on the set of points of $\mathcal{P}$. Then $\mathcal{P}$ is a translation plane.

Open problem 2

Suppose that a colliniation group G acts imprimitively on the set of points of a finite affine plane $\mathcal{P}$ of order n. Then detemine $\mathcal{P}$ and G.

Specially prove when G acts regularly on the set of points.

Concerning this problem, when G acts regularly on the set of points and G is abelian, it is known that n is a prime power and $\mathcal{P}$ is a translation plane, a dual translation plane or a type (b) plane with special three orbits of points and lines under action of G.

(Dembowski,Piper,Andre,Blokhuis,Jungnickel and Schmidt.)

Moreover about type (b) plane, if n is even, then exponent(G)=4 (Ganley).

And if n is odd and $G = H \times K$ where H is a elation group of $\mathcal{P}$ of order n, then **a planar function** (from K into H) is constructed and the affine plane reconstructed by this planar function is isomorphic to $\mathcal{P}$.

PARTII

(Definition)

Let G and H be groups of order n. For a mapping

$$f : G \longrightarrow H, \quad x \longmapsto f(x)$$

and $u \in G$,the mapping f_u is defined as

$$f_u : G \longrightarrow H, \quad x \longmapsto f(ux)f(x)^{-1}$$

Then f is called a planar function if and only if f_u is bijective for each $u \in G$ except $u = 0$.

From **a planar function** (f:$G \longrightarrow H$), we can construct an affine plane $\mathcal{A}(f; G, H)$ as the followimg.

the set of points: $G \times H$

the set of lines: $(g, H) = \{(g, h) \mid h \in H\}$ wkere $g \in G$ and $\{ L(g, h) \mid g \in G,\ h \in H \}$ where $L = \{ (x, f(x)) \mid x \in G \}$. Obviously $G \times H$ acts on $\mathcal{A}(f, G, H)$ as a regular group on the set of points.

Remark that G and H are odd order groups if there is a planar function from G into H.(Ganley)

[Examples]

(1):

$$f : GF(q) \longrightarrow GF(q) \quad x \longmapsto x^2$$

where $GF(q)$ is the additive group for an odd prime power q. (An affine plane corresponding this function is Desarguesian.)

(2):

$$f : GF(3^4) \longrightarrow GF(3^4) \quad x \longmapsto a(x^6 + x^{30} + x^{54}) - x^{10} - x^{18}$$

where $a^2 = -1$.

(An affine plane corresponding this function is a semifield plane(not Desarguesian.))

(3):

$$f : GF(3^e) \longrightarrow GF(3^e) \quad x \longmapsto x^{\frac{3^a+1}{2}}$$

where $\gcd(a, 2e) = 1$ and $1 < a < 2e$.
(An affine plane corresponding this function is not a translation plane.)

All known examples of planar functions untill now are elementary abelian groups type.

Open problem 3
(1):Prove that there are no planar functions of nonabelian groups type.
(2):Prove that there are no planar functions of abelian but nonelementary abelian groups type or construct a planar function of this type.

Theorem 3(Hiramine,Ronyai and Szonyi)
Suppose that there exists a planar function f from G into H where $|G| = |H| = p$ for an odd prime p, then f is a quadratic polynomial and an affine plane corresponding to f is Desargusian.

Theorem 4(Blokhuis, Jugnickel, Schmidt, Ma,Fung and Siu)
Suppose that there exsits a planar function from $\mathbf{Z}_n$ into $\mathbf{Z}_n$, then n is an odd prime.

Theorem 5(N.N.)
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

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

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

I would like to determine all monomial polynomials over the additive group $GF(p^n)$ which are planar functions.

For $f(x) = x^d$, $(x+u)^d - x^d$ is bijective if and only if $(x+1)^d - x^d$ is bijective if $u \neq 0$.
Therefore when we put

$$N(b) := \sharp\{ \ x \in GF(p^n) \mid (x+1)^d - x^d = b \ \}$$

, $f(x) = x^d$ is planar if and only if $N(b) = 1$ for each $b \in GF(p^n)$.

Theorem 6(N.N.)

Let $f(x) = x^d$ be a power function over $GF(p^n)$. Suppose that one of the following conditions is satisfied. (1): $\gcd(d, p^n - 1) \neq 2$ (2): $p^n - 1$ is divisible by $d - 1$, $d \neq 2$ and d is not divisible by p. (3): $5 \leq p$ and $d = \frac{p^a+1}{2}(a = 0, 1, 2, \cdots)$ Then $f(x)$ is not a planar function.

(Definition)

Let f be a function from $GF(p^n)$ into $GF(p)$ and ω be a primitive p-th root of 1. Fourier transform $\hat{f}$ is defined as

$$\hat{f}(a) = \sum_{x \in GF(p^n)} \omega^{f(x)+Tr(ax)}$$

where $a \in GF(p^n)$.

Then f is called a bent function if $|\hat{f}(a)| = p^{\frac{n}{2}}$ for all $a \in GF(p^n)$. (This definition is also available for $p = 2$)

For example, a nondegenerate quadratic form over $GF(p)$ is always a bent function.

Theorem 7(N.N.)

Let $f(X)$ be a function over $GF(p^n)$. We identify the additive group $GF(p^n)$ and n dimensional vecter space $(\mathbf{Z}_p)^n$ over $GF(p)$ for a fixed basis of $GF(p^n)$.
We put $X = (x_1, x_2, \cdots, x_n)$.
Then $f(X) = (f_1(X), f_2(X), \cdots, f_n(X))$ is a planar function if and only if

$$s_1 f_1 + s_2 f_2 + \cdots + s_n f_n$$

is a bent function for each $(s_1, s_2, \cdots, s_n) \in (\mathbf{Z}_p)^n$ such that $(s_1, s_2, \cdots, s_n) \neq (0, 0, \cdots, 0)$

PARTIII

The behavior of the number of solutions of the difference equations coming from power functions over finite fields

[Definition]

Suppose that a function $f(x) = x^d$ is a power function over the finite field $\mathbf{F}_q$.
We consider the difference equation
$f(x+1) - f(x) = (x+1)^d - x^d = b$ of $f(x)$.
Let

$$N(b) := \{\ x \in \mathbf{F}_q \mid (x+1)^d - x^d = b\ \}$$

,

$$N(q,d) := max_{b\in \mathbf{F}_q} N(b)$$

Note that $f(x)$ is a planar over $\mathbf{F}_q$ if $N(q,d)=1$

Problem 4
Detemine all q and d such that $N(q,d)\le 4$
(Significant from the view point of the cryptography(cipher))

The case q is odd.
We will examine the vehavior of the number of solutions of the eqations $(x+1)^d - x^d = b$ for a while regardless of the problem above where $d = \frac{q-1}{2}, \frac{q-1}{2}+1, \frac{q-1}{2}-1, \frac{q-1}{2}+2$.

Theorem 8(N.N.)
Let d be $\frac{q-1}{2}$.
Then (1):the case of $q \equiv 1 (mod\ \ 4)$.

$$N(0) = \frac{q-3}{2},\ \ N(2) = N(-2) = \frac{q-1}{4},\ \ N(1) = n(-1) = 1$$

and $N(b) = 0$ for other $b \in \mathbf{F}_q$.

(2): the case of $q \equiv 3(mod\ 4)$.

$$N(0) = \frac{q-3}{2},\ \ N(-2) = \frac{q+1}{4},\ \ N(2) = \frac{q-3}{4},\ \ N(1) = 2$$

and $N(b) = 0$ for other $b \in \mathbf{F}_q$.

Theorem 9(N.N.)

Let d be $\frac{q-1}{2} + 1$ and χ be the quadratic character of $\mathbf{F}_q$. Then

(1):the case of $q \equiv 1(mod\ 4)$

$$N(1) = \frac{q+3}{4},\ \ N(-1) = \frac{q-1}{4},$$

$$N(b) = 2 \quad \text{for} \quad \chi(b+1) = \chi(2) \quad \text{and} \quad \chi(b-1) = -\chi(2)$$

(There are $\frac{q-1}{4}$ these b.)

and $N(b) = 0$ for other $b \in \mathbf{F}_q$.

(2):the case of $q \equiv 3(mod\ 4)$

$$N(1) = N(-1) = \frac{q+1}{4},\ \ N(0) = 1,\ \ N(b) = 1 \ \ \text{for} \ \ \chi(b^2-1) = -1$$

(There are $\frac{q-5}{2}$ these b.)

and $N(b) = 0$ for other $b \in \mathbf{F}_q$.

Theorem 10(Helleseth and Sandberg)

Let d be $\frac{q-1}{2} + 2$ and $q = p^e$ be an odd prime power. Then

$$N(q,d) = 1 \quad \text{for} \quad q = 3^n \ \ \text{where } n \ \text{ is even.}$$

$$N(q,d) = 3 \quad \text{for} \quad p \neq 3 \quad \text{and} \quad q \equiv 1 (mod \;\; 4)$$

$$N(q,d) = 4 \quad \text{otherwise.}$$

Theorem 11(Helleseth and Sandberg)
Let d be $\frac{q-1}{2} - 1, q \equiv 3(mod \;\; 4)$ and $q > 7$. Then

$$N(q,d) = 1 \quad \text{for} \quad q = 3^3.$$

$$N(q,d) = 2 \quad \text{if} \quad \chi(5) = -1.$$

$$N(q,d) = 3 \quad \text{if} \quad \chi(5) = 1.$$

Here χ be the quadratic character of $\mathbf{F}_q$.

Theorem 12(N.N.)
Let d be $\frac{q-1}{2} - 1, q \equiv 1(mod \;\; 4)$. Then

$$N(q,d) \leq 8.$$

Specially,

$$N(b) \leq 4 \quad \text{if} \quad \chi(b) = -1.$$

$$N(b) \leq 4 \quad \text{if} \quad \chi(b-4) = -1 \quad \text{and} \quad \chi(b+4) = -1.$$

Here χ be the quadratic character of $\mathbf{F}_q$.
This Theorem shoud be improved more sharply. My conjecture is that $N(q,d) = 4$ holds.

Problem 5

(1): Detemine $N(q,d)$ for $d = p^i + p^j$ such that all $0 \leq i, j \leq e$ where $q = p^e$.

(2): Suppose that $q-1$ is dividable by 3.Then
Detemine $N(q,d)$ for $d = \frac{q-1}{3}$, $\frac{q-1}{3}+1$ and $\frac{q-1}{3}-1$.

The case q is even.
We remark that $N(q,d) = 1$ does not occur if q is even.

Theorem 13

The power function $f(x) = x^d$ on $GF(2^n)$ are almost perfect nonlinear(APN) for the following n and d. Namely the mapping $(x+1)^d - x^d$ is **two-to one** mapping from $GF(2^n)$ into $GF(2^n)$. Especially $N(q,d) = 2$.
In the case of n is odd $(n = 2m+1)$,
(1): $d = 2^k + 1$, where $gcd(k,n) = 1\,(1 \leq k \leq m)$(prove by Gold)
(2): $d = 2^{2k} - 2^k + 1$, where $gcd(k,n) = 1\,(2 \leq k \leq m)$(prove by Kasami)
(3): $d = 2^m + 3$, (conjectured by Welch, prove by Gold)
(4): $d = 2^m + 2^{\frac{m}{2}} - 1$ if m is even, $d = 2^m + 2^{\frac{3m+1}{2}} - 1$ if m is odd. (conjectured by Niho, prove by Dobbertin)
(5): $d = 2^{m+1} - 1$, (prove by Helleseth and Sandberg)
(6): $d = -1$, (prove by Beth, Ding and Nyberg).
In the case of n is even $(n = 2m)$,
(1): $d = 2^k + 1$, where $gcd(k,n) = 1\,(1 \leq k < m)$(prove by Nyberg)
(2): $d = 2^{2k} - 2^k + 1$, where $gcd(k,n) = 1\,(2 \leq k < m)$(prove by

Dobbertin)

References

[1] A.Blokhus,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(2001), 1473-1476.

[2] R.S.Coulter and R.W.Mattews, Planar Functions and Planes of Lenz-Barlotti Class II, Designs, Codes and Cryptography 10(1997),167-184.

[3] P.Dembowski and T.G.Ostrom, Planes of order n with collineation groups of order n^2 , Math. Zeitschrift 99(1967),53-75.

[4] H. Dobbertin, One to One Highly Nonlinear Power Functions on $GF(2^n)$, Applicable Algebra in Engineering, Communication and Computing, 9(1998), 139-152.

[5] H. Dobbertin, Almost Perfect Nonlinear Functions. The Niho Case, Inform. and Comput. 151(1999), 57-72.

[6] H. Dobbertin, Almost Perfect Nonlinear Functions. The Welch Case, IEEE Trans. Inform. Theory 45(1999), 1272-1275.

[7] H. Dobbertin, Kasami Power Functions, Permutation Polynomials and Cyclic Defference Sets, Nato Adv. Sci. Inst. Ser. C. Math. Phys. Sci.,542(1999),133-158.

[8] W. Feit, Finite projective planes and a question about primes, Proc. Amer. Math. Soc. 108(1990), 561-564.

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

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

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

[12] T. Helleseth and D. Sandberg, Some Power Mappings Low Differential Uniformity, Applicable Algebra in Engineering, Communication and Computing, 8(1997), 363-370.

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

[14] Y.Hiramine, Afinne Planes with Peimitive Collineation Groups, J. Algebra 128(1990), 366-383.

[15] Y.Hiramine, Factor sets assciated with regular collineation groups, J. Algebra 152(1992), 135-145.

[16] Y.Hiramine, Flanar functions and related group algebras, J. Algebra 142(1991), 414-423.

[17] P.V.K.Kumar, A. Scholt and R. Welch, Generalized bent functions and their properties, J.Combin. Theory Ser.A 40(1985), 90-107.

[18] K.H. Leung, S.L. Ma and A.V. Tan, Planar functions from Z_n to Z_n, Preprint.

[19] R.Lidl and H.Niederreiter, Finite Fields, Cambridge Univ. Press, Cambridge/London/New York, (1984).

[20] S.L. Ma, Planar functions, difference sets and character theorey, J. Algebra 185(1996), 342-356.

[21] S.L. Ma and A. Pott, Relative difference sets, planar functions and generalized Hadamard matrices, J. Algebra 175(1995), 505-525.

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

[23] N. Nakagawa, Left Planar Functions Of Degree p^n, Utilitas Mathematica 51(1997), 89-96.

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

[25] J.Wolfmann, Bent Functions and Coding Theory, NATO Adv. Sci. Inst. Ser. C. Math. Phys. Sci.,542(1999),393-418.

[26] U.Ott, Endliche zyklische Ebenen, Math. Zeitschrift 144(1975), 195-215.

[27] D.H.Xiang, Bent Functions, Pacial Difference Sets, and Quasi-Frobeniou Local Rings, Design, Codes and Cryptography 20(2000),251-268.

[28] X. Xiang, Maximall Nonlinea Functions and Bent Functions, Designs, Codes and Cryptography 17(1999),211-218.