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

(Algebraic Combinatorics)

Author(s)
Nakagawa, Nobuo

Citation
数理解析研究所講究録 (2005), 1440: 82-96

Issue Date
2005-07

URL
http://hdl.handle.net/2433/47532

Type
Departmental Bulletin Paper

Textversion
publisher

Kyoto University
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

Theorem 1 (Kantor)
Let $\mathcal{P}$ be a projective plane of order $n$. Suppose that a collineation group $G$ acts transitively 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 determine 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 additional conditions.)

Theorem 2 (Hiramne)
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 determine $\mathcal{P}$ 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 $G$. 
Moreover about type (b) plane, if $n$ is even, then $\text{exponent}(G)=4$ (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

$$f : G \rightarrow H, \ x \mapsto f(x)$$

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

$$f_u : G \rightarrow H, \ x \mapsto f(ux)f(x)^{-1}$$

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 $(f:G \rightarrow H)$, we can construct an affine plane $A(f; G, H)$ as the following.
the set of points: $G \times H$

the set of lines: $(g, H) = \{(g, h) \mid h \in H\}$ where $g \in G$ 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 $A(f, G, H)$ 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): $f : GF(q) \rightarrow GF(q) \ x \mapsto x^2$

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

(2): $f : GF(3^4) \rightarrow GF(3^4) \ x \mapsto a(x^6 + x^{30} + x^{54}) - x^{10} - x^{18}$

where $a^2 = -1$.

(An affine plane corresponding this function is a semifield plane (not Desarguesian.))
(3): \[ f : GF(3^e) \rightarrow GF(3^e) \quad x \mapsto x^{3^a+1} \]

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 exists a planar function from $\mathbb{Z}_n$ into $\mathbb{Z}_n$, 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

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

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

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

, $f(x) = x^d$ 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 $\omega$ 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 vector space $(\mathbb{Z}_p)^n$ 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

$$s_1f_1 + s_2f_2 + \cdots + s_nf_n$$

is a bent function for each $(s_1, s_2, \cdots, s_n) \in (\mathbb{Z}_p)^n$ 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 $\mathbb{F}_q$.

We consider the difference equation

$$f(x + 1) - f(x) = (x + 1)^d - x^d = b \quad \text{of } f(x).$$

Let

$$N(b) := \{ x \in \mathbb{F}_q \mid (x + 1)^d - x^d = b \}$$
\[ N(q, d) := \max_{b \in \mathbb{F}_q} N(b) \]

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

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

The case \( q \) is odd.
We will examine the behavior of the number of solutions of the equations \((x + 1)^d - x^d = b\) 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 \( q \equiv 1(\text{mod } 4) \).

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

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

Theorem 9 (N.N.)

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

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

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

$N(b) = 2$ for $\chi(b + 1) = \chi(2)$ and $\chi(b - 1) = -\chi(2)$

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

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

(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 $b \in \mathbb{F}_q$.

Theorem 10 (Helleseth and Sandberg)

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

$$N(q, d) = 1 \text{ for } q = 3^n \text{ where } n \text{ is even.}$$
$N(q, d) = 3$ for $p \neq 3$ and $q \equiv 1 (mod\ 4)$

$N(q, d) = 4$ otherwise.

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

$N(q, d) = 1$ for $q = 3^3$.

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

$N(q, d) = 3$ if $\chi(5) = 1$.

Here $\chi$ be the quadratic character of $\mathbb{F}_q$.

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

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

Specially,

$N(b) \leq 4$ if $\chi(b) = -1$.

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

Here $\chi$ be the quadratic character of $\mathbb{F}_q$.

This Theorem should be improved more sharply. My conjecture is that $N(q, d) = 4$ holds.
Problem 5
(1): Determine $N(q, d)$ 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 divisible by 3. Then
Determine $N(q, d)$ 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): $d = 2^m + 2^m - 1$ if $m$ is even, $d = 2^m + 2^{3m+1} - 1$ 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 $gcd(k, n) = 1 (1 \leq k \leq m)$ (prove by Nyberg)
(2): $d = 2^{2k} - 2^k + 1$, where $gcd(k, n) = 1 (2 \leq k \leq m)$ (prove by
Dobbertin)

References


