New Classes of Permutation Polynomials over Finite Fields defined by Functional Equations

Neranga Fernando

Joint work with Xiang-dong Hou and Stephen Lappano

Department of Mathematics and Statistics
University of South Florida

Joint Mathematics Meeting, San Diego 2013

January 09, 2013

Permutation polynomials

Let $\mathbb{F}_q$ be the finite field with q elements.

Definition

A polynomial $f(x) \in \mathbb{F}_q[\mathrm{x}]$ is called a permutation polynomial (PP) over finite field $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$.

Facts

- Every linear polynomial over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$.
- The monomial x^n is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

Polynomial $g_{n,q}$

[Hou 2011]

$q = p^k, n \geq 0.$

There exists a unique polynomial $g_{n,q} \in \mathbb{F}_p[x]$ such that

$$\sum_{a \in \mathbb{F}_q} (x+a)^n = g_{n,q}(x^q - x)$$

Question : When is $g_{n,q}$ a permutation polynomial(PP) of $\mathbb{F}_{q^e}$?

If $g_{n,q}$ is a PP, we call triple $(n, e; q)$ **desirable**.

Outline

- Basic properties of the polynomial $g_{n,q}$
- The Case $e = 1$
- The Case $n = q^a - q^b - 1$, $0 < b < a < pe$.
- Results with even q

Polynomial $g_{n,q}$

$$g_{n,q}(x) = \sum_{\frac{n}{q} \le l \le \frac{n}{q-1}} \frac{n}{l} \binom{l}{n - l(q-1)} x^{n-l(q-1)}$$

The Polynomial $g_{n,q}$

Recurrence

$$g_{0,q} = \ldots = g_{q-2,q} = 0,$$

$$g_{q-1,q} = -1,$$

$$g_{n,q} = xg_{n-q,q} + g_{n-q+1,q} \quad , \quad n \geq q$$

When $n < 0$

Recurrence relation for $n \geq 0$ can be used to define $g_{n,q}$ for $n < 0$:

$$g_{n,q} = \frac{1}{x}(g_{n+q,q} - g_{n+1,q}).$$

For $n < 0$, there exists a $g_{n,q} \in \mathbb{F}_p[x, x^{-1}]$ such that

$$\sum_{a \in \mathbb{F}_q} (x+a)^n = g_{n,q}(x^q - x)$$

Recurrence relation holds for all $n \in \mathbb{Z}$.

Desirable Triples

Equivalence

(1) $g_{pn,q} = g_{n,q}^p$.

(2) If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{q^{pe} - 1}$, then $g_{n_1,q} \equiv g_{n_2,q} \pmod{x^{q^e} - x}$.

(3) If $m, n > 0$ belong to the same p-cyclotomic coset modulo q^{pe} - 1, we say that two triples $(m, e; q)$ and $(n, e; q)$ are *equivalent* and write $(m, e; q) \sim (n, e; q)$.

If $(m, e; q) \sim (n, e; q)$,

$$g_{m,q} \text{ is a PP if and only if } g_{n,q} \text{ is a PP.}$$

The case $e = 1$

Namely, modulo $\mathtt{x}^q - \mathtt{x}$,

$$g_{n,q}(\mathtt{x}) \equiv a_n \mathtt{x}^n + \begin{cases} \mathtt{x}^{q-1} - 1 & \text{if } n > 0,\ n \equiv 0 \pmod{q-1}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\displaystyle\sum_{n \geq 0} a_n \mathtt{t}^n = \frac{-\mathtt{t}^{q-1}}{1 - \mathtt{t}^{q-1} - \mathtt{t}^q}$.

When $q > 2$,

$(n, 1; q)$ is desirable if and only if $\gcd(n, q-1) = 1$ and $a_n \neq 0$.

When $q = 2$,

$(n, 1; 2)$ is desirable if and only if $a_n = 0$ (in $\mathbb{F}_2$).

The case $n = q^a - q^b - 1$, $0 < b < a < pe$.

Define $S_a = x + x^q + \cdots + x^{q^{a-1}}$ for every integer $a \geq 0$.

For $0 < b < a < pe$, we have

$$g_{q^a-q^b-1,q} = -\frac{1}{\mathtt{x}} - \frac{(S_b^{q-1} - 1)S_{a-b}^{q^b}}{\mathtt{x}^{q^b+1}}.$$

Assume $e \geq 2$. Write

$$a - b = a_0 + a_1 e, \quad b = b_0 + b_1 e,$$

where $a_0, a_1, b_0, b_1 \in \mathbb{Z}$ and $0 \leq a_0, b_0 < e$. Then we have

Namely modulo $\mathtt{x}^{q^e} - \mathtt{x}$,

$$g_{q^a-q^b-1,q} \equiv -\mathtt{x}^{q^e-2} - \mathtt{x}^{q^e-q^{b_0}-2}(a_1 S_e + S_{a_0}^{q^{b_0}})\big((b_1 S_e + S_{b_0})^{q-1} - 1\big).$$

If $b=0$ and $a>0$, we have $n \equiv q^a-2 \pmod{q^{pe}-1}$.

$$g_{q^a-2,q} = \mathtt{x}^{q-2} + \mathtt{x}^{q^2-2} + \cdots + \mathtt{x}^{q^{a-1}-2}.$$

Conjecture 1

Let $e \geq 2$ and $2 \leq a < pe$. Then $(q^a-2, e; q)$ is desirable if and only if

(i) $a=3$ and $q=2$, or
(ii) $a=2$ and $\gcd(q-2, q^e-1)=1$.

Conjecture 2

Let $e \geq 3$ and $n = q^a - q^b - 1$, $0 < b < a < pe$. Then $(n, e; q)$ is desirable if and only if

(i) $a = 2,\ b = 1$, and $\gcd(q-2, q^e - 1) = 1$, or
(ii) $a \equiv b \equiv 0 \pmod{e}$.

Theorem

Let p be an odd prime and q a power of p.

(i) Let $0 < i \leq \frac{1}{2}(p-1)$ and $n = q^{p+2i} - q^p - 1$. Then

$$g_{n,q}(x) = \begin{cases} (2i-1)x^{q-2} & \text{if } x \in \mathbb{F}_q, \\ \dfrac{2i-1}{x} + \dfrac{2i}{x^q} & \text{if } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q. \end{cases}$$

(ii) For the n in (ii), $(n, 2; q)$ is desirable if and only if $4i \not\equiv 1 \pmod{p}$.

Theorem

Let p be an odd prime and q a power of p.

(i) Let $0 < i \le \frac{1}{2}(p-1)$ and $n = q^{p+2i-1} - q^p - 1$. Then

$$g_{n,q}(x) = \begin{cases} 2(i-1)x^{q-2} & \text{if } x \in \mathbb{F}_q, \\ \dfrac{2i-1}{x} + \dfrac{2i-2}{x^q} & \text{if } x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q. \end{cases}$$

(ii) For the n in (i), $(n, 2; q)$ is desirable if and only if $i > 1$ and $4i \not\equiv 3 \pmod{p}$.

Conjecture 3

1. Let $\mathtt{f} = \mathtt{x}^{q-2} + t\mathtt{x}^{q^2-q-1}$, $t \in \mathbb{F}_q^*$. Then $\mathtt{f}$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:
   (i) $t = 1$, $q \equiv 1 \pmod 4$;
   (ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$;
   (iii) $t = 3$, $q \equiv -1 \pmod 6$.

Conjecture 3

1. Let $\mathtt{f} = \mathtt{x}^{q-2} + t\mathtt{x}^{q^2-q-1}$, $t \in \mathbb{F}_q^*$. Then $\mathtt{f}$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:
   (i) $t = 1$, $q \equiv 1 \pmod 4$;
   (ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$;
   (iii) $t = 3$, $q \equiv -1 \pmod 6$.

2. Recently proved in the paper "A class of permutation binomials over finite fields" by X. Hou.

Theorem

Let p be an odd prime, $q = p^k$, $n = q^{p+i+1} - q^{2i+1} - 1$. If

$$\left(\frac{2i+1}{q}\right) = \begin{cases} 1 & : \text{if } \ i \ \text{ is odd,} \\ (-1)^{\frac{q-1}{2}} & : \text{if } \ i \ \text{ is even.} \end{cases}$$

where $\left(\dfrac{a}{b}\right)$ is the Jacobian symbol, then $(q^{p+i+1} - q^{2i+1} - 1, 2; q)$ is desirable.

Results with even q.

Theorem

Let $e = 3k$, $k \geq 1$, $q = 2^s$, $s \geq 2$, and $n = (q-3)q^0 + 2q^1 + q^{2k} + q^{4k}$. Then

$$g_{n,q} \equiv \mathtt{x}^2 + S_{2k}S_{4k} \pmod{\mathtt{x}^{q^e} - \mathtt{x}},$$

and $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Conjecture 3

Let $q = 4$, $e = 3k$, $k \geq 1$, and $n = 3q^0 + 3q^{2k} + q^{4k}$. Then

$$g_{n,q} \equiv \mathtt{x} + S_{2k} + S_{4k} + S_{4k}S_{2k}^3 \equiv \mathtt{x} + S_{2k}^{q^{2k}} + S_{2k}^{q^k+3} \pmod{\mathtt{x}^{q^e} - \mathtt{x}}.$$

$g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Theorem

Let $q = p^2$, $e > 0$, and $n = (p^2 - p - 1)q^0 + (p-1)q^e + pq^a + q^b$, $a, b \geq 0$. Then

$$g_{n,q} = -S_a^p - S_b S_e^{p-1}.$$

Assume that $a + b \not\equiv 0 \pmod{p}$ and

$$\gcd\left(\mathrm{x}^{2a+1} + 2\mathrm{x}^{a+1} + \mathrm{x} - \epsilon(\mathrm{x}^b + 1)^2,\ (\mathrm{x}+1)(\mathrm{x}^e + 1)\right) = (\mathrm{x}+1)^2,$$

for $\epsilon = 0, 1$. Then $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

References

- X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory A, **118** (2011), 448 – 454.
- X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012) 492 – 521.
- N. Fernando, X. Hou, S. D. Lappano, *A new approach to permutation polynomials over finite fields,* II, submitted (2012), Preprint available at http://arxiv.org/abs/1208.2942.
- R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge (1997).

Thank You!