A New Approach to Permutation Polynomials over Finite Fields

Neranga Fernando

Joint work with Dr. Xiang-dong Hou and Stephen Lappano

Department of Mathematics and Statistics
University of South Florida

Discrete Seminar

November 19, 2012

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 $\gcd(n, q-1) = 1$.

Dickson polynomial

Let $n \geq 0$ be an integer.

Elementary symmetric polynomials $x_1 + x_2$ and $x_1 x_2$ form a $\mathbb{Z}-$basis of the ring of symmetric polynomials in $\mathbb{Z}[x_1, x_2]$.

There exists $D_n(x, y) \in \mathbb{Z}[x, y]$ such that

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1 x_2)$$

$$D_n(x, y) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-y)^i x^{n-2i}$$

Dickson polynomial

$$D_0(x,y) = 2,$$
$$D_1(x,y) = x,$$
$$D_n(x,y) = xD_{n-1}(x,y) - yD_{n-2}(x,y), \qquad n \geq 2.$$

[Dickson 1897]

For fixed $a \in \mathbb{F}_q$, $D_n(x,a) \in \mathbb{F}_q[\mathrm{x}]$ is the Dickson polynomial of degree n and parameter a.

When $a = 0$, $D_n(x,a) = x^n$, PP if and only if $(n, q-1) = 1$.

When $0 \neq a \in \mathbb{F}_q$, PP if and only if $(n, q^2-1) = 1$.

Reversed Dickson polynomial

[Hou, Mullen, Sellers, Yucas 2009]

Fix $a \in \mathbb{F}_q$. Interchanged the roles of x and a.

$D_n(a, x) \in \mathbb{F}_q[\mathrm{x}]$ - reversed Dickson polynomial.

When $a = 0$, $D_n(0, x)$ is a PP if and only if $n = 2k$ with $(k, q-1) = 1$.

When $a \neq 0$,

$$D_n(a, x) = a^n D_n(1, \frac{x}{a^2})$$

$D_n(a, x)$ is a PP on $\mathbb{F}_q$ if and only if $D_n(1, x)$ is a PP on $\mathbb{F}_q$.

The nth Reversed Dickson Polynomial $D_n(1, x) \in \mathbb{Z}[x]$ is defined by

$$D_n(1, x(1-x)) = x^n + (1-x)^n$$

Polynomial $g_{n,q}$

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

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 $g_{n,q}$

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

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 $n \in \mathbb{Z}$.

The nth Reversed Dickson Polynomial $D_n(1,x) \in \mathbb{Z}[x]$ is defined by

$$D_n(1, x(1-x)) = x^n + (1-x)^n$$

When $q = 2$,

$$g_{n,2}(x(1-x)) = x^n + (1-x)^n \quad \in \quad \mathbb{F}_2[x]$$

$g_{n,2} = D_n(1,x) \quad \in \quad \mathbb{F}_2[x].$

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

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

[Hou 2011]

If $(n, e; 2)$ is desirable , $\gcd(n, 2^{2e} - 1) = 3$.

If $(n, e; q)$ is desirable , $\gcd(n, q - 1) = 1$.

Generating function

A Quick Reminder :

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

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

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

$$\sum_{n \geq 0} g_{n,q} \mathtt{t}^n = \frac{-\mathtt{t}^{q-1}}{1 - \mathtt{t}^{q-1} - \mathtt{x}\mathtt{t}^q}$$

Theorem

$$\sum_{n\geq 0} g_{n,q}\mathtt{t}^n \equiv \frac{-(\mathtt{xt})^{q-1}}{1-(\mathtt{xt})^{q-1}-(\mathtt{xt})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}^q-\mathtt{x}}.$$

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

Proof of the Theorem

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

$$\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^q} \equiv \frac{-(\mathtt{x}\mathtt{t})^{q-1}}{1-(\mathtt{x}\mathtt{t})^{q-1}-(\mathtt{x}\mathtt{t})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}^{q-1}-1}$$

and

$$\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^q} \equiv \frac{-(\mathtt{x}\mathtt{t})^{q-1}}{1-(\mathtt{x}\mathtt{t})^{q-1}-(\mathtt{x}\mathtt{t})^q} + (1-\mathtt{x}^{q-1})\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}} \pmod{\mathtt{x}}$$

The case e = 1

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

Proof.

By the Theorem , we have
Namely, modulo $\mathrm{x}^q - \mathrm{x}$,

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

$g_{n,q}(\mathrm{x}) = a_n \mathrm{x}^n$ for all $\mathrm{x} \in \mathbb{F}_q^*$.
($\Rightarrow$)
Since $g_{n,q}$ is PP , by a previous fact, $\gcd(n, q-1) = 1$.
So $g_{n,q}(\mathrm{x}) \equiv a_n \mathrm{x}^n \pmod{\mathrm{x}^q - \mathrm{x}}$ which implies $a_n \neq 0$.
($\Leftarrow$)
$\gcd(n, q-1) = 1$ and $a_n \neq 0 \Rightarrow g_{n,q}(\mathrm{x}) \equiv a_n \mathrm{x}^n \pmod{\mathrm{x}^q - \mathrm{x}} \Rightarrow g_{n,q}$ is PP.

Open question : Determine n s.t. $a_n \neq 0$. □

The case e $= 1$ contd

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

Proof.

By the Theorem , we have

$$g_{n,2} \equiv a_n \mathrm{x} + \mathrm{x} - 1 (\bmod\ \mathrm{x}^2 - \mathrm{x}).$$ □

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

$g_{q^a - q^b - 1, q}$

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

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

The case $b = 0$

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

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

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 $\gcd(q - 2, q^e - 1) = 1$.

The case $e \geq 3$

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) $a \equiv b \equiv 0 \pmod{e}$.

The Case $b = p$

Theorem

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

(i) $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ consists of the roots of $(\mathtt{x} - \mathtt{x}^q)^{q-1} + 1$.

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

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

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

The Case $b = p$

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 $4i \not\equiv 3 \pmod{p}$.

Results

Result 1 $q = 5$ $2x^3 + 2x^{19}$ is a PP of $\mathbb{F}_{q^2}$.

Result 2 $q = 13$ $6x^{11} + 6x^{155}$ is a PP of $\mathbb{F}_{q^2}$.

Result 3 $q = 121$ $6x^{119} + 4x^{14519}$ is a PP of $\mathbb{F}_{q^2}$.

Result 4 $q = 11$ $8x^9 + 2x^{109}$ is a PP of $\mathbb{F}_{q^2}$.

Result 5 $q = 29$ $7x^{27} + 21x^{811}$ is a PP of $\mathbb{F}_{q^2}$.

Conjecture 3

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) $t = 3$, $q \equiv -1 \pmod 6$.

Results

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

Result 1 $q \equiv 1 \pmod 4$ $(q^{p+5} - q^9 - 1, 2; q)$ is desirable.

Result 2 $(q^{p+3} - q^5 - 1, 2; q)$ is desirable.

Result 3 $(q^{p+4} - q^7 - 1, 2; q)$ is desirable.

Result 4 $(q^{p+6} - q^{11} - 1, 2; q)$ is desirable.

A most recent result

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

Outline of the proof

$e = 2, a = p + i + 1, b = 2i + 1.$

Case 1 - i is odd.

$a_0 = 0, a_1 = \frac{p-i}{2}, b_0 = 1, b_1 = i$

$$g \equiv -x^{q^2-2} + \frac{i}{2}x^{q^2-q-2}(x + x^q)[((i+1)x + ix^q)^{q-1} - 1].$$

Clearly, $g(0) = 0$. When $x \in \mathbb{F}_{q^2}^*$,

$g(x) =$

$$\frac{i((i+1)w^q - iw)^2 + i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1}}{(4i+2)^2 w}.$$

Outline of the proof contd

$$\frac{i((i+1)w^q - iw)^2 + i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1}}{w} = c$$

Assume $c \neq 0$. Let $t = wc \quad \Rightarrow \quad t \in \mathbb{F}_q$.

$$t = \frac{1}{i(u)^{2q} + 2(i+1)(u)^{q+1} + i(u)^2},$$

where $u = (i+1)c^{-q} - ic^{-1}$.

t is unique $\Rightarrow$ w is unique.

Outline of the proof contd

$$\frac{i((i+1)w^q - iw)^2 + i((i+1)w^q - iw)^{2q} + 2(i+1)((i+1)w^q - iw)^{q+1}}{w} = c$$

Now assume $c = 0$.

$$i((i+1)w^q - iw)^{2q-2} + 2(i+1)((i+1)w^q - iw)^{q-1} + i \ = 0.$$

Let $z = ((i+1)w^q - iw)^{q-1} \in \mathbb{F}_{q^2}^*$. Then

$$iz^2 + 2(i+1)z + i = 0. \tag{1}$$

Since i is odd $2i+1$ is a square in $\mathbb{F}_q$. So (1) implies that $z \in \mathbb{F}_q$. Then we have $z^2 = z^{q+1} = ((i+1)w^q - iw)^{q^2-1} = 1$. So $z = \pm 1$ and it contradicts (1).

Outline of the proof contd

Case 2 - i is even

$a_0 = 1, a_1 = \frac{p-i-1}{2}, b_0 = 1, b_1 = i$

Results with even q.

A Desirable Family

Theorem

Let $q = 2^s$, $s > 1$, $e > 0$, and let $n = (q-1)q^0 + \frac{q}{2}q^{e-1} + \frac{q}{2}q^e$. We have

$$g_{n,q} = \mathrm{x} + \mathrm{Tr}_{q^e/q}(\mathrm{x}) + \mathrm{x}^{\frac{1}{2}q^e}\mathrm{Tr}_{q^e/q}(\mathrm{x})^{\frac{1}{2}q}.$$

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

Example

Let $q = 4$, $e > 1$ and Let $n = 3q^0 + 2q^{e-1} + 2q^e$. Then

$$g_{3q^0+2q^{e-1}+2q^e} = x + \mathrm{Tr}_{q^e/q}(x) + x^{2q^{e-1}}\mathrm{Tr}^2_{q^e/q}(x)$$

We claim that when e is odd, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$. Assume that there exist $x, a \in \mathbb{F}_{q^e}$ such that $g(x) = g(x+a)$. Then we have

$$a + \mathrm{Tr}_{q^e/q}(a) + \mathrm{Tr}^2_{q^e/q}(x)a^{2q^{e-1}} + \mathrm{Tr}^2_{q^e/q}(a)x^{2q^{e-1}} + \mathrm{Tr}^2_{q^e/q}(a)a^{2q^{e-1}} = 0$$

$\Rightarrow \mathrm{Tr}_{q^e/q}(a) = 0.$

$$a + \mathrm{Tr}^2_{q^e/q}(x)a^{2q^{e-1}} = 0$$

$a = 0$ in all three following cases

- $\mathrm{Tr}_{q^e/q}(x) = 0$
- $\mathrm{Tr}_{q^e/q}(x) = 1$
- $\mathrm{Tr}_{q^e/q}(x) \neq 0, 1$

Conjecture 4

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

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

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

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

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

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

A most recent result

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

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

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

Example

Let $q = 4$, $e > 3$, $n = q^0 + 2q^1 + q^2 + q^e$. Then,

$$g_{n,q} \equiv x^2 + x\mathrm{Tr}_{q^e/q}(x) + x^q\mathrm{Tr}_{q^e/q}(x) \pmod{\mathrm{x}^{q^e} - \mathrm{x}}.$$

We claim that when $\gcd(1 + \mathrm{x} + \mathrm{x}^2, \mathrm{x}^e + 1) = 1$, $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Assume that $g_{n,q}(x) = g_{n,q}(y)$, $x, y \in \mathbb{F}_{q^e}$.

$\mathrm{Tr}_{q^e/q}(g_{n,q}(x)) = \mathrm{Tr}_{q^e/q}(g_{n,q}(y)) \Rightarrow \mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y)$.

Let $\mathrm{Tr}_{q^e/q}(x) = \mathrm{Tr}_{q^e/q}(y) = a \in \mathbb{F}_q$.

If $a = 0$, then $x = y$.
If $a \neq 0$, then $g_{n,q}(x) = g_{n,q}(y)$ becomes

$$z^2 = a(z + z^q)$$

where $z = x + y$. Substituting the above equation to itself we get $(z^2)^q = (z^2) + (z^2)^{q^2}$.

Since $\gcd(1 + \mathrm{x} + \mathrm{x}^2, \mathrm{x}^e + 1) = 1$, we have $z = 0$.

References

- X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009), 748 – 773.
- 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!