A New Approach to Permutation Polynomials over Finite Fields

Xiang-dong Hou

Department of Mathematics and Statistics
University of South Florida

Coding, Cryptology and Combinatorial Designs
Singapore, 2011-05-30

outline

1. Introduction
2. Reversed Dickson Polynomials in Characteristic 2
3. Desirable Triples
4. Families of Desirable Triples
5. Open Questions

1. Introduction

the polynomial $g_{q,n}$

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

There exists a polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ satisfying

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

We want to know when $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Call the triple $(n, e; q)$ desirable if $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$.

Waring's formula

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

Not useful for our purpose!

recurrence / negative n

$$\begin{cases} g_{0,q} = \cdots = g_{q-2,q} = 0, \\ g_{q-1,q} = -1, \\ g_{n,q} = \mathrm{x} g_{n-q,q} + g_{n-q+1,q}, \qquad n \geq q. \end{cases}$$

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

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

$g_{n,q}$ satisfies the above recurrence relation for all $n \in \mathbb{Z}$.

about $g_{n,q}$

- introduced recently (2009 - 2010)
- q-ary version of the reversed Dickson polynomial in characteristic 2
- $q = 2$: PPs $g_{2,n}$ are related to APN; all known desirable triples $(n, e; 2)$ are contained in 4 families.
- $q > 2$: several families of desirable triples are found; computer search ($q = 3, e \leq 6$ and $q = 5, e \leq 2$) produced many desirable triples that need explanation.

2. Reversed Dickson Polynomials in Characteristic 2

$p = 2$ / reversed Dickson polynomial

$p = 2$, $g_{2,n} \in \mathbb{F}_2[\mathrm{x}]$ defined by

$$g_{n,2}(x(1-x)) = x^n + (1-x)^n.$$

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

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

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

$g_{2,n}$ and APN

APN

A function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$ is called almost perfect nonlinear (APN) if for each $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation $f(x+a) - f(x) = b$ has at most two solutions in $\mathbb{F}_q$.

Power APN

A power function x^n is an APN function on $\mathbb{F}_q$ if and only if for each $b \in \mathbb{F}_q$, the equation $(x+1)^n - x^n = b$ has at most two solutions in $\mathbb{F}_q$.

$g_{2,n}$ and power APN

x^n is an APN on $\mathbb{F}_{2^{2e}} \Rightarrow g_{2,n}$ is a PP of $\mathbb{F}_{2^e} \Rightarrow x^n$ is an APN on $\mathbb{F}_{2^e}$.

desirable triples with $q = 2$

Known desirable triples $(n, e; 2)$

e	n	ref
	$2^k + 1, \quad (k, 2e) = 1$	Gold
	$2^{2k} - 2^k + 1, \quad (k, 2e) = 1$	Kasami
even	$2^e + 2^k + 1, \quad k > 0, (k-1, e) = 1$	HMSY
$5k$	$2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$	Dobbertin

Conjecture. The above table is complete for $q = 2$ (up to equivalence).

3. Desirable Triples

equivalence

Facts

- $g_{pn,q} = g_{n,q}^p$.
- If $n_1, n_2 > 0$ are integers such that $n_1 \equiv n_2 \pmod{q^{pe} - 1}$, then $g_{n_1,q} \equiv g_{n_2,q} \pmod{\mathrm{x}^{q^e} - \mathrm{x}}$.

Equivalence.

If $n_1, n_2 > 0$ are in the same p-cyclotomic coset modulo $q^{pe} - 1$, we say that the two triples $(n_1, e; q)$ and $(n_2, e; q)$ are equivalent and we denote this as $(n_1, e; q) \sim (n_2, e; q)$.
If $(n_1, e; q) \sim (n_2, e; q)$, then $(n_1, e; q)$ is desirable if and only if $(n_2, e; q)$ is.

necessary conditions

Assume that $(n, e; q)$ is desirable.

- $\gcd(n, q-1) = 1$.
- If $q = 2$, then $\gcd(n, 2^{2e} - 1) = 3$.
- If $q > 2$ or $e > 1$, then the p-cyclotomic coset of n modulo $q^{pe} - 1$ has cardinality $pe\kappa$ $(q = p^{\kappa})$.

power sum

Theorem. Let $\epsilon \in \mathbb{F}_{q^{pe}}$ such that $\epsilon^{q^e} - \epsilon = 1$. Then

$$\sum_{x \in \mathbb{F}_{q^e}} g_{n,q}(x)^k = \sum_{(a,b) \in \mathbb{F}_q \times \mathbb{F}_{q^e}} (a\epsilon + b)^n \left[\sum_{c \in \mathbb{F}_q} (a\epsilon + b + c)^n \right]^{k-1}.$$

Consequently, $(n, e; q)$ is desirable if and only if

$$\sum_{(a,b) \in \mathbb{F}_q \times \mathbb{F}_{q^e}} (a\epsilon + b)^n \left[\sum_{c \in \mathbb{F}_q} (a\epsilon + b + c)^n \right]^{k-1} \begin{cases} = 0 & \text{if } 1 \le k < q^e - 1, \\ \ne 0 & \text{if } k = q^e - 1. \end{cases}$$

4. Families of Desirable Triples

easy cases

The following triples are desirable. In all these cases $g_{n,q} \equiv -x^{q^e-2} \pmod{x^{q^e} - x}$.

- $(q^{pe} - 2, e; q)$, $q > 2$.
- $(q^{2e} - q^e - 1,\ e;\ q)$, $q = 3^\kappa$.
- $(3^{2e+1} - 2 \cdot 3^e - 2,\ e;\ 3)$.

proposition

For $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \le \alpha_i \le q-1$, $w_q(n) = \alpha_0 + \cdots + \alpha_t$.

Proposition. Let $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \le \alpha_i \le q-1$. Then

$$g_{n,q} = \begin{cases} 0 & \text{if } w_q(n) < q-1, \\ -1 & \text{if } w_q(n) = q-1, \\ \alpha_0 x^{q^0} + (\alpha_0+\alpha_1)x^{q^1} + \cdots + (\alpha_0 + \cdots + \alpha_{t-1})x^{q^{t-1}} + \delta & \\ & \text{if } w_q(n) = q, \end{cases}$$

where

$$\delta = \begin{cases} 1 & \text{if } q = 2, \\ 0 & \text{if } q > 2. \end{cases}$$

the case $w_q(n) = q$

Theorem. Let $n = \alpha_0 q^0 + \cdots + \alpha_t q^t$, $0 \le \alpha_i \le q - 1$, with $w_q(n) = q$. Then $(n, e; q)$ is desirable if and only if

$$\gcd\big(\alpha_0 + (\alpha_0 + \alpha_1)\mathrm{x} + \cdots + (\alpha_0 + \cdots + \alpha_{t-1})\mathrm{x}^{t-1},\ \mathrm{x}^e - 1\big) = 1.$$

a useful lemma

Lemma. Let $n = \alpha(p^{0e} + p^{1e} + \cdots + p^{(p-1)e}) + \beta$, where $\alpha, \beta \geq 0$ are integers. Then for $x \in \mathbb{F}_{p^e}$,

$$g_{n,p}(x) = \begin{cases} g_{\alpha p+\beta,p}(x) & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0, \\ x^\alpha g_{\beta,p}(x) & \text{if } \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) \neq 0. \end{cases}$$

Note. The lemma does not hold if p is replaced with q. We do not know if there is a q-ary version of the lemma.

Theorem. Let $p > 2$, $n = \alpha(p^{0e} + p^{1e} + \cdots + p^{(p-1)e}) + \beta$, where $\alpha, \beta \geq 0$. Then $(n, e; p)$ is desirable if the following two conditions are satisfied.

(i) Both $g_{\alpha p+\beta,p}$ and $\mathrm{x}^{\alpha} g_{\beta,p}$ are $\mathbb{F}_p$-linear on $\mathbb{F}_{p^e}$ and are 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(0) = \{x \in \mathbb{F}_{p^e} : \mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0\}$.

(ii) $g_{\beta,p}(1) \neq 0$.

Note. There are many instances where (i) and (ii) are satisfied.

example

Example.
Let $p = 3$, $n = 8(1 + 3^e + 3^{2e}) + 7$. ($\alpha = 8$, $\beta = 7$.)

$$g_{n,3}(x) = \begin{cases} g_{8\cdot 3+7,3}(x) = g_{31,3}(x) = x^{3^0} - x^{3^1} - x^{3^2} \\ \qquad\qquad\qquad \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0, \\ x^8 g_{7,3} = \mathrm{x}^9 \qquad \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0. \end{cases}$$

We have $-g_{31,3}(x^3 - x) = x + x^3 + x^{3^3}$. So $g_{31,3}$ is 1-1 on $\mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$ if and only if $\gcd(1 + \mathrm{x} + \mathrm{x}^3, \mathrm{x}^e - 1) = \mathrm{x} - 1$.

Conclusion: $(n, e; 3)$ is desirable if and only if $\gcd(1 + \mathrm{x} + \mathrm{x}^3, \mathrm{x}^e - 1) = \mathrm{x} - 1$.

a more interesting family

Theorem. Let $n = 4(3^0 + 3^e + 3^{2e}) - 7$. Then $(n, e; 3)$ is desirable.

Proof.

$$g_{n,3}(x) = \begin{cases} g_{4\cdot 3-7,3}(x) = g_{5,3}(x) & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0, \\ x^4 g_{-7,3}(x) & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0. \end{cases}$$

We have $g_{5,3} = -\mathrm{x}$, $g_{-7,3} = -\mathrm{x}^{-3} + \mathrm{x}^{-5} - \mathrm{x}^{-7}$. So

$$g_{n,3}(x) = \begin{cases} -x & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) = 0, \\ -x + x^{-1} - x^{-3} & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(x) \neq 0. \end{cases}$$

It is known that $-\mathrm{x} + \mathrm{x}^{-1} - \mathrm{x}^{-3}$ is 1-1 on $\mathbb{F}_{3^e} \setminus \mathrm{Tr}^{-1}_{\mathbb{F}_{3^e}/\mathbb{F}_3}(0)$. (Hollmann and Xiang 04; Yuan, Ding, Wang, Pieprzyk, 08)

theorem

For $m \in \mathbb{Z}$, let $m^\dagger$ be the integer such that $0 \le m^\dagger \le p^e - 2$ and $m^\dagger \equiv m \pmod{p^e - 1}$.

Theorem. Let p be a prime. Assume $e \equiv 0 \pmod 2$ if $p = 2$. Let $0 < \alpha, \beta < p^{pe} - 1$ such that

(i) $\alpha \equiv p^\ell \pmod{\frac{p^e-1}{p-1}}$ for some $0 \le \ell < e$;

(ii) $w_p(\beta) = p - 1$;

(iii) $w_p((\alpha p + \beta)^\dagger) = p$.

Let $n = \alpha(1 + p^e + \cdots + p^{(p-1)e}) + \beta$ and write

$$(\alpha p + \beta)^\dagger = a_0 p^0 + \cdots + a_t p^t, \quad 0 \le a_i \le p - 1.$$

Then $(n, e; p)$ is desirable if and only if

$$\gcd(a_0 + (a_0 + a_1)x + \cdots + (a_0 + \cdots + a_{t-1})x^{t-1}, x^e - 1) = 1.$$

proof of the theorem

Let $x \in \mathbb{F}_{p^e}$. If $\mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) = 0$,

$$g_{n,p}(x) = a_0 x^{p^0} + (a_0 + a_1) x^{p^1} + \cdots + (a_0 + \cdots + a_{t-1}) x^{p^{t-1}}.$$

If $\mathrm{Tr}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x) \neq 0$,

$$g_{n,p}(x) = -x^{p^\ell} \mathrm{N}_{\mathbb{F}_{p^e}/\mathbb{F}_p}(x)^s,$$

where s is defined by $\alpha = p^\ell + s\frac{p^e-1}{p-1}$.

The rest is easy.

5. Open Questions

a difficult one

Prove that for $p = 2$, all desirable triples are given in the table. (A similar conjecture for binary power APN has been standing for many years.)

Known desirable triples $(n, e; 2)$

e	n	ref
	$2^k + 1, \quad (k, 2e) = 1$	Gold
	$2^{2k} - 2^k + 1, \quad (k, 2e) = 1$	Kasami
even	$2^e + 2^k + 1, \quad k > 0, (k - 1, e) = 1$	HMSY
$5k$	$2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$	Dobbertin

another question

Recall:

Theorem. Let $\epsilon \in \mathbb{F}_{q^{pe}}$ such that $\epsilon^{q^e} - \epsilon = 1$. Then $(n, e; q)$ is desirable if and only if

$$\sum_{(a,b)\in\mathbb{F}_q\times\mathbb{F}_{q^e}} (a\epsilon+b)^n \Big[\sum_{c\in\mathbb{F}_q} (a\epsilon+b+c)^n\Big]^{k-1} \begin{cases} = 0 & \text{if } 1 \le k < q^e - 1, \\ \neq 0 & \text{if } k = q^e - 1. \end{cases}$$

Question: What can be said about the sum

$$\sum_{(a,b)\in\mathbb{F}_q\times\mathbb{F}_{q^e}} (a\epsilon + b)^n \Big[\sum_{c\in\mathbb{F}_q} (a\epsilon + b + c)^n\Big]^{k-1}?$$

a specific questions

$p = 3$, $e = 4$, $n = 20(1 + 3^e + 3^{2e}) + 219$. ($\alpha = 20$, $\beta = 219$.)

$$g_{n,3}(x) = \begin{cases} (x - x^3 - x^{3^2})^{3^2} & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^4}/\mathbb{F}_3}(x) = 0, \\ [x^{-20}(x + x^3) + x^{-1} + x]^3 & \text{if } \mathrm{Tr}_{\mathbb{F}_{3^4}/\mathbb{F}_3}(x) \neq 0. \end{cases}$$

$(n, e; 3)$ is desirable because of the following curious fact:

($*$) $\mathrm{x}^{-20}(\mathrm{x} + \mathrm{x}^3) + \mathrm{x}^{-1} + \mathrm{x}$ is a permutation of $\mathbb{F}_{3^4} \setminus \mathrm{Tr}_{\mathbb{F}_{3^4}/\mathbb{F}_3}(0)$.

Question: Can ($*$) be generalized to $\mathbb{F}_{3^e}$ for a general e?

Thank you!