Reversed Dickson permutation polynomials

Neranga Fernando

Department of Mathematics
Northeastern University
Boston

Algebra, Number Theory, and Discrete Mathematics Seminar
Department of Mathematics
California State University
Northridge, CA

March 7, 2018

Introduction

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

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

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

Example 1. Every linear polynomial is a PP of $\mathbb{F}_q$.

Example 2. The monomial x^n is a PP of $\mathbb{F}_q$ if and only if $(n, q-1) = 1$.

Background

The n-th Dickson polynomial of the first kind $D_n(x, a)$ is defined by

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

where $a \in \mathbb{F}_q$ is a parameter.

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

Background (contd.)

The n-th reversed Dickson polynomial of the first kind $D_n(a, x)$ is defined by

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

where $a \in \mathbb{F}_q$ is a parameter.

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

Background (contd.)

The n-th Dickson polynomial of the second kind $E_n(x, a)$ can be defined by

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

where $a \in \mathbb{F}_q$ is a parameter.

- Stephen D. Cohen (University of Glasgow, UK)
- Mihai Cipu (The Institute of Mathematics of the Romanian Academy)
- Rex Matthews (University of Queensland, Australia)
- Robert Coulter (University of Delaware, USA)
- Marie Henderson (New Zealand)

Background (contd.)

The n-th reversed Dickson polynomial of the second kind $E_n(a, x)$ can be defined by

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

where $a \in \mathbb{F}_q$ is a parameter.

S. Hong, X. Qin, W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational*, Finite Fields Appl. **37** (2016), 54 – 71.

Background (contd.)

For $a \in \mathbb{F}_q$, the n-th Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(x,a)$ is defined by

$$D_{n,k}(x,a) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i},$$

and $D_{0,k}(x,a) = 2-k$.

Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl. **18** (2012), 814 – 831.

Background (contd.)

For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i},$$

and $D_{0,k}(a,x) = 2-k$.

Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl. **18** (2012), 814 – 831.

Reversed Dickson Polynomials of the $(k+1)$-th kind

For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i},$$

and $D_{0,k}(a,x) = 2-k$.

I am primarily interested in the question: When is $D_{n,k}(a,x)$ a PP of $\mathbb{F}_q$?

- $D_{n,0}(a,x) = D_n(a,x)$ and $D_{n,1}(a,x) = E_n(a,x)$.
- Only need to consider $0 \leq k \leq p-1$.

$$D_{n,k}(a,x) = kE_n(a,x) - (k-1)D_n(a,x).$$

$D_{n,k}(a,x)$ in characteristic 2

$$D_{n,k}(a,x) = kE_n(a,x) - (k-1)D_n(a,x).$$

$$D_{n,k}(a,x) = \begin{cases} E_n(a,x) & \text{if } k \text{ is odd,} \\ D_n(a,x) & \text{if } k \text{ is even.} \end{cases}$$

• Hereafter always assume, unless specified, in this talk that p is odd.

Outline of the rest of the talk

1. The case $a = 0$
2. Some general properties of $D_{n,k}(a, x)$.
3. The case $n = p^\ell$, where $\ell \geq 0$ is an integer.
4. The case $n = p^\ell + 1$, where $\ell \geq 0$ is an integer.
5. The case $n = p^\ell + 2$, where $\ell \geq 0$ is an integer.
6. An explicit expression for $D_{n,k}(1, x)$.
7. The sum $\sum_{a \in \mathbb{F}_q} D_{n,k}(1, a)$.
8. The case $n = p^\ell + 3$, where $\ell \geq 0$ is an integer.
9. A generalization to $n = p^{\ell_1} + p^{\ell_2} + \cdots + p^{\ell_i}$.
10. Permutation behaviour of $D_{p^{\ell_1}+p^{\ell_2},k}$.
11. More results on $D_{n,k}(1, x)$.
12. A Matrix Form of $D_{n,k}(1, x)$.

The case $a = 0$

$$D_{n,k}(0,x) = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ (2-k)(-x)^{\ell} & \text{if } n = 2\ell. \end{cases}$$

Theorem

When $a = 0$, $D_{n,k}(a,x)$ is a PP of $\mathbb{F}_q$ if and only if $k \neq 2$ and $n = 2\ell$ with $(\ell, q-1) = 1$.

- Hereafter, assume that $a \in \mathbb{F}_q^*$.

Why only consider $a = 1$?

Let $a \in \mathbb{F}_q^*$. Then it follows from the definition that

$$D_{n,k}(a, x) = a^n \, D_{n,k}(1, \frac{x}{a^2}).$$

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

Functional expression

$$D_{n,k}(a,x) = k\left[\frac{y^{n+1} - (a-y)^{n+1}}{2y-a}\right] - (k-1)\{y^n + (a-y)^n\},$$

where $y \neq \frac{a}{2}$. This can be simplified to

$$D_{n,k}(a,x) = k\left[\frac{y^n(a-y) - y(a-y)^n}{2y-a}\right] + D_n(a,x).$$

Functional expression with $a = 1$

Let $x = y(1-y)$. The functional expression can be written as

$$D_{n,k}(1, y(1-y)) = k\left[\frac{y^n(1-y) - y(1-y)^n}{2y-1}\right] + D_n(1, y(1-y)),$$

where $y \neq \frac{1}{2}$.

When $y = \frac{1}{2}$, $\quad D_{n,k}\left(1, \frac{1}{4}\right) = \frac{k(n-1)+2}{2^n}$.

if $n_1 \equiv n_2 \pmod{q^2-1}$, then $D_{n_1,k}(1,x) = D_{n_2,k}(1,x)$ for any $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.

Recursion

Proposition

Let p be an odd prime and n be a non-negative integer. Then

$$D_{0,k}(1,x) = 2 - k, \;\; D_{1,k}(1,x) = 1, \;\; \text{and}$$

$$D_{n,k}(1,x) = D_{n-1,k}(1,x) - x\, D_{n-2,k}(1,x), \;\; \text{for } n \geq 2.$$

The Case $n = p^\ell$, $\ell \geq 0$ is an integer

Let $x = y(1-y)$. When $y \neq \frac{1}{2}$,

$$D_{p^\ell,k}(1, y(1-y)) = k\left[\frac{y^{p^\ell}(1-y) - y(1-y)^{p^\ell}}{2y-1}\right] + D_{p^\ell}(1, y(1-y))$$

$$= \frac{k}{2}\left((2y-1)^2\right)^{\frac{p^\ell-1}{2}} + 1 - \frac{k}{2}$$

Note that $(2y-1)^2 = 1 - 4x$. Hence,

$$D_{p^\ell,k}(1, x) = \frac{k}{2}(1-4x)^{\frac{p^\ell-1}{2}} + 1 - \frac{k}{2}$$

The case $n = p^\ell$, $\ell \geq 0$ is an integer (contd.)

When $y = \frac{1}{2}$,

$$D_{p^\ell,k}\left(1, \frac{1}{4}\right) = \frac{k(p^\ell - 1) + 2}{2^{p^\ell}} = \frac{2-k}{2} = 1 - \frac{k}{2} = \frac{k}{2}(1-4x)^{\frac{p^\ell - 1}{2}} + 1 - \frac{k}{2}.$$

Hence for all $x \in \mathbb{F}_q$, we have

$$D_{p^\ell,k}(1, x) = \frac{k}{2}(1 - 4x)^{\frac{p^\ell - 1}{2}} + 1 - \frac{k}{2}$$

Theorem

Consider

$$D_{p^\ell,k}(1,x) = \frac{k}{2}\left(1-4x\right)^{\frac{p^\ell-1}{2}} + 1 - \frac{k}{2}.$$

Theorem

Let $0 < \ell \leq e$. Then $D_{3^\ell,k}(1,x)$ is a PP of $\mathbb{F}_{3^e}$ if and only if $k \neq 0$ and $(\frac{3^\ell-1}{2}, 3^e-1) = 1$. Also, $D_{p^\ell,k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p > 3$.

The case $n = p^\ell + 1$, $\ell \geq 0$ is an integer

For all $x \in \mathbb{F}_q$, we have

$$D_{p^\ell+1,k}(1,x) = \left(\frac{1}{2} - \frac{k}{4}\right)(1-4x)^{\frac{p^\ell+1}{2}} + \frac{k}{4}(1-4x)^{\frac{p^\ell-1}{2}} + \frac{1}{2}.$$

Theorem

Let $k = 2$. Then $D_{p^\ell+1,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $\left(\frac{p^\ell-1}{2}, q-1\right) = 1$.

Theorem

Let $n = p^\ell + 1$ and $k \neq 0, 2$. Then $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $\ell = 0$.

Remark

Let $k = 0$. Then, $D_{p^\ell+1,k}(1,x) = \frac{1}{2}(1-4x)^{\frac{p^\ell+1}{2}} + \frac{1}{2}$ which is a PP of $\mathbb{F}_q$ if and only if $\left(\frac{p^\ell+1}{2}, q-1\right) = 1$.

The case $n = p^\ell + 2$, $\ell \geq 0$ is an integer

For all $x \in \mathbb{F}_q$, we have

$$D_{p^\ell+2,k}(1,x) = \frac{1}{2}(1-4x)^{\frac{p^\ell+1}{2}} + \frac{k}{2}x(1-4x)^{\frac{p^\ell-1}{2}} - \left(1-\frac{k}{2}\right)x + \frac{1}{2}.$$

Remark

Let $k = 0$ and $\ell = e$. Then we have

$$D_{p^e+2,0}(1,x) = \frac{1}{2}(1-4x)^{\frac{p^e+1}{2}} - x + \frac{1}{2}$$

which is a PP of $\mathbb{F}_{p^e}$ if and only if $p^e \equiv 1 \pmod 3$.

Let $u = 1 - 4x$. Then we have

$$D_{p^\ell+2,k}(1,x) = \left(\frac{1}{2} - \frac{k}{8}\right)u^{\frac{p^\ell+1}{2}} + \frac{k}{8}u^{\frac{p^\ell-1}{2}} + \left(1-\frac{k}{2}\right)\frac{u}{4} + \frac{k}{8} + \frac{1}{4}$$

The case $n = p^\ell + 2$, $\ell \geq 0$ is an integer (contd.)

$$D_{p^\ell+2,k}(1,x) = \left(\frac{1}{2} - \frac{k}{8}\right) u^{\frac{p^\ell+1}{2}} + \frac{k}{8}\, u^{\frac{p^\ell-1}{2}} + \left(1 - \frac{k}{2}\right)\frac{u}{4} + \frac{k}{8} + \frac{1}{4}$$

Theorem

Let $k = 2$. Then $D_{p^\ell+2,k}(1,x) = x^{\frac{p^\ell+1}{2}} + x^{\frac{p^\ell-1}{2}}$ is a PP of $\mathbb{F}_q$ if and only if $\ell = 0$.

Theorem

Let $p > 3$ and $k = 4$. Then $D_{p^\ell+2,k}(1,x) = x^{\frac{p^\ell-1}{2}} - \frac{1}{2}x$ is a PP of $\mathbb{F}_q$ if and only if $\ell = 0$.

Theorem

Let $n = p^\ell + 2$ and $k \neq 0, 2, 4$. Then $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the trinomial $(4-k)\,x^{\frac{p^\ell+1}{2}} + k\,x^{\frac{p^\ell-1}{2}} + (2-k)x$ is a PP of $\mathbb{F}_q$.

Theorem

Theorem

Let p be an odd prime. Then $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the function

$$y \mapsto k\,\frac{y^n(1-y)-y(1-y)^n}{2y-1}+y^n+(1-y)^n$$

is a 2-to-1 mapping on $(\mathbb{F}_q \cup V)\setminus\{\frac{1}{2}\}$ and

$$k\,\frac{y^n(1-y)-y(1-y)^n}{2y-1}+y^n+(1-y)^n \neq \frac{k(n-1)+2}{2^n}$$

for any $y \in (\mathbb{F}_q \cup V)\setminus\{\frac{1}{2}\}$.

An explicit expression for $D_{n,k}(1,x)$

For $n \geq 1$, define

$$f_{n,k}(x) = k \sum_{j \geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j \geq 0} \binom{n}{2j} x^j \in \mathbb{Z}[x],$$

and

$$f_{0,k}(x) = 2 - k.$$

Then for $n \geq 0$

$$D_{n,k}(1,x) = \left(\frac{1}{2}\right)^n f_{n,k}(1-4x).$$

An explicit expression for $D_{n,k}(1, x)$ (contd.)

Let p be an odd prime and $n > 0$ be an integer. Then in $\mathbb{F}_q[x]$,

$$D_{n,k}(1, x) = \left(\frac{1}{2}\right)^n f_{n,k}(1 - 4x).$$

In particular, $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $f_{n,k}(x)$ is a PP of $\mathbb{F}_q$.

- Self-reciprocal property of $f_{n,k}$ is completely explained in

N. F., *Self-reciprocal polynomials and coterm polynomials*, Designs, Codes and Cryptography (2018), Available Online.

The generating function

The generating function of $D_{n,k}(1,x)$ is given by

$$\sum_{n=0}^{\infty} D_{n,k}(1,x)\, z^n = \frac{2-k+(k-1)z}{1-z+xz^2}.$$

Computation of $\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)$

$$\sum_{n=0}^{\infty} D_{n,k}(1,x)\,z^n \equiv \frac{2-k+(k-1)z}{1-z}\left[1+\sum_{m=1}^{q-1}\frac{(z-1)^{q-1-m}\,z^{2m}}{(z-1)^{q-1}-z^{2(q-1)}}\,x^m\right] \pmod{x^q-x}$$

Since $D_{n_1,k}(1,x) = D_{n_2,k}(1,x)$ for any $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$ when $n_1, n_2 > 0$ and $n_1 \equiv n_2 \pmod{q^2-1}$, we have the following for all $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.

$$\sum_{n\geq 0} D_{n,k}(1,x)\,z^n = 2-k+\frac{1}{1-z^{q^2-1}}\sum_{n=1}^{q^2-1} D_{n,k}(1,x)\,z^n$$

Computation of $\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)$ (contd.)

$$\sum_{n=1}^{q^2-1} D_{n,k}(1,x)\,z^n = \frac{z\,(z^{q^2-1}-1)}{z-1} + \; h(z) \sum_{m=1}^{q-1}(z-1)^{q-1-m}\; z^{2m}\; x^m$$

$$\text{for all } x \in \mathbb{F}_q \setminus \{\tfrac{1}{4}\},$$

where

$$h(z) = \frac{[2-k+(k-1)z]\,(-1-(z-z^q)^{q-1})}{z^q - z^{q-1} - 1}.$$

Write

$$h(z) = \frac{1}{z^q - z^{q-1} - 1} \sum_{j=0}^{q^2-q+1} b_j z^j.$$

Computation of $\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)$ (contd.)

Write $j = \alpha + \beta q$ where $0 \leq \alpha, \beta \leq q-1$. Then we have the following.

$$b_j = \begin{cases} (-1)^{\beta+1}(2-k)\binom{q-1}{\beta} & \text{if } \alpha+\beta = q-1, \\ (-1)^{\beta+1}(k-1)\binom{q-1}{\beta} & \text{if } \alpha+\beta = q, \\ 1-k & \text{if } \alpha+\beta = 1, \\ k-2 & \text{if } \alpha+\beta = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Computation of $\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)$ (contd.)

$$\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)\Big)z^n = \sum_{n=1}^{q^2-1}\frac{k(n-1)+2}{2^n}z^n - \frac{z(1-z^{q^2-1})}{1-z} - h(z)\,z^{2(q-1)}$$
$$- h(z)\sum_{m=1}^{q-1}(z-1)^{q-1-m}\,z^{2m}\left(\frac{1}{4}\right)^m,$$

$$(z^q - z^{q-1} - 1)\sum_{n=1}^{q^2-1}\left[\Big(\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)\Big) - \left(\frac{k(n-1)+2}{2^n}\right)\right]z^n$$
$$= (1+z^{q-1}-z^q)\sum_{i=1}^{q^2-1} z^i - \left(z^{2(q-1)} + \sum_{m=1}^{q-1}(z-1)^{q-1-m}\,z^{2m}\left(\frac{1}{4}\right)^m\right)\left(\sum_{j=0}^{q^2-q+1} b_j z^j\right)$$

$$(z^q - z^{q-1} - 1)\sum_{n=1}^{q^2-1}\left[\Big(\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)\Big) - \left(\frac{k(n-1)+2}{2^n}\right)\right]z^n = \sum_{i=1}^{q^2+q-1} c_i z^i$$

Theorem

Let c_j be defined as on the previous slide for $1 \leq j \leq q^2+q-1$. Then we have the following.

$$\sum_{a\in\mathbb{F}_q} D_{j,k}(1,a) = -c_j + \frac{k(j-1)+2}{2^j} \text{ if } 1 \leq j \leq q-1;$$

$$\sum_{a\in\mathbb{F}_q} D_{q,k}(1,a) = c_1 - c_q + \frac{2-k}{2^q};$$

$$\sum_{a\in\mathbb{F}_q} D_{\ell q+j,k} = \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+j,k} - \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+j+1,k} - c_{\ell q+j} + \frac{(kj+2)(1-2^q+2^{q-1})+k(2^q-1)}{2^{\ell q+j}} \text{ if } 1 \leq \ell \leq q-2 \text{ and } 1 \leq j \leq q-1;$$

$$\sum_{a\in\mathbb{F}_q} D_{\ell q,k} = \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q,k} - \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+1,k} - c_{\ell q} + \frac{(k-2)(2^q-1)+2^q}{2^{\ell q}} \text{ if } 2 \leq \ell \leq q-2;$$

$$\sum_{a\in\mathbb{F}_q} D_{q^2-q+j,k} = \sum_{i=j}^{q-1} c_{q^2+i} + \frac{k(j-1)+2}{2^{q^2-q+j}} \text{ if } 0 \leq j \leq q-1.$$

For further details

N. F., *Reversed Dickson polynomials of the* $(k+1)$*-th kind over finite fields*, J. Number Theory **172** (2017), 234 – 255.

Remember this Theorem?

Theorem

Let $n = p^\ell + 2$ and $k \neq 0, 2, 4$. Then $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if the trinomial $(4-k)\,x^{\frac{p^\ell+1}{2}} + k\,x^{\frac{p^\ell-1}{2}} + (2-k)x$ is a PP of $\mathbb{F}_q$.

Xiang-dong Hou asked me "when is the trinomial above a PP of $\mathbb{F}_q$?"

My answer

Theorem

Let $p > 3$ be an odd prime and $q = p^e$, where e is a positive integer. Let k be an integer such that $k \neq 0, 2, 4$ and $0 \leq k \leq p-1$. Let

$$f(x) = (4-k)x^{\frac{p^\ell+1}{2}} + kx^{\frac{p^\ell-1}{2}} + (2-k)x.$$

Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $\ell = 0$ and $k \neq 3$.

My answer (contd.)

Let $p = 3$. Since $k \neq 0, 2$, we have $k = 1$. Then

$$f(x) = (4-k)x^{\frac{p^\ell+1}{2}} + kx^{\frac{p^\ell-1}{2}} + (2-k)x = x^{\frac{p^\ell-1}{2}} + x.$$

Theorem

Let $p = 3$ and $q = 3^e$, where e is a positive integer. Let

$$f(x) = x^{\frac{p^\ell-1}{2}} + x.$$

Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if

(i) $\ell = 0$, *or*

(ii) $\ell = me + 1$, *where m is a non-negative even integer.*

For further details

N. F., *A note on permutation binomials and trinomials over finite fields*, to appear in New Zealand Journal of Mathemaics.

The Case $n = p^\ell + 3$

$D_{p^\ell+3,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $f(x)$ is a PP of $\mathbb{F}_{p^e}$, where

$$f(x) = (2-k)\,x^{\frac{p^\ell+3}{2}} + 6\,x^{\frac{p^\ell+1}{2}} + k\,x^{\frac{p^\ell-1}{2}} + 2(3-k)\,x.$$

The Case $n = p^\ell + 3$ with $p = 3$

In this case, $k = 0, 1,$ or 2.

Theorem

$D_{3^\ell+3,0}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $\gcd(\frac{3^\ell+3}{2}, 3^e - 1) = 1$.

Theorem

$D_{3^\ell+3,1}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

Theorem

$D_{3^\ell+3,2}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if

(i) $\ell = 0$, *or*

(ii) $\ell = me + 1$, *where m is a non-negative even integer.*

The Case $n = p^\ell + 3$ with $p > 3$

Theorem

Let $p > 5$ and $k = 2$. Assume that $(-\frac{1}{4})$ is a quadratic residue of p. Then $D_{p^\ell+3,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $\ell = 0$.

Remark

$D_{p^\ell+3,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p = 5$ and $k = 2$.

Theorem

Let $p > 5$, $k = 2$, and $\ell > 0$. Assume that $(-\frac{1}{4})$ is a quadratic non-residue of p. Then $D_{p^\ell+3,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $3x^{\frac{p^\ell+1}{2}} + x^{\frac{p^\ell-1}{2}} + x$ is a PP of $\mathbb{F}_{p^e}$.

The Case $n = p^\ell + 3$ with $p > 3$ (contd.)

Theorem

Let $p > 5$, $k = 0$, and -6 be a quadratic non-residue of p. Then $D_{p^\ell+3,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $x^{\frac{p^\ell+3}{2}} + 3x^{\frac{p^\ell+1}{2}} + 3x$ is a PP of $\mathbb{F}_{p^e}$.

Remark

Let $p > 7$, $k = 7$. Then $D_{p^\ell+3,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

Remark

Let $p > 5$, $k = 0$, and -6 be a quadratic residue of p. Then $D_{p^\ell+3,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

The Case $n = p^\ell + 3$ with $p > 3$ (contd.)

Theorem

Assume that

1. $p = 5$ *and* $k \neq 2$,
2. $p > 5$ *and* $k \neq 0, 2$, *or*
3. $p > 7$ *and* $k \neq 7$.

Then $D_{p^\ell+3,k}(1, x)$ *is a PP of* $\mathbb{F}_{p^e}$ *if and only if*

$$(2-k)\,x^{\frac{p^\ell+3}{2}} + 6\,x^{\frac{p^\ell+1}{2}} + k\,x^{\frac{p^\ell-1}{2}} + 2(3-k)\,x$$

is a PP of $\mathbb{F}_{p^e}$.

More Cases

1. $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$
2. $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3} + p^{\ell_4}$

How about a generalization to $n = p^{\ell_1} + p^{\ell_2} + \cdots + p^{\ell_i}$?

A Generalization

Case 1. Let i be odd and $n = p^{\ell_1} + p^{\ell_2} + \cdots + p^{\ell_i}$. For all $x \in \mathbb{F}_q$, we have

$$
\begin{aligned}
&D_{n,k}(1,x) \\
&= \frac{k}{2^i}(1-4x)^{\frac{p^{\ell_1}+p^{\ell_2}+\cdots+p^{\ell_i}-1}{2}} + \frac{(2-k)}{2^i} \sum_{j_1,j_2,\ldots,j_{i-1} \in \{\ell_1,\ell_2,\ldots,\ell_i\}} (1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_i}-1}{2}} \\
&+ \frac{k}{2^i} \sum_{j_1,j_2,\ldots,j_{i-2} \in \{\ell_1,\ell_2,\ldots,\ell_i\}} (1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_i-2}-1}{2}} \\
&+ \frac{(2-k)}{2^i} \sum_{j_1,j_2,\ldots,j_{i-3} \in \{\ell_1,\ell_2,\ldots,\ell_i\}} (1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_i-3}}{2}} + \cdots\cdots \\
&+ \frac{(2-k)}{2^i} \sum_{j_1,j_2 \in \{\ell_1,\ell_2,\ldots,\ell_i\}} (1-4x)^{\frac{p^{j_1}+p^{j_2}}{2}} + \frac{k}{2^i} \sum_{j_1 \in \{\ell_1,\ell_2,\ldots,\ell_i\}} (1-4x)^{\frac{p^{j_1}-1}{2}} + \frac{(2-k)}{2^i}.
\end{aligned}
$$

A Generalization (contd.)

Case 2. Let i be even and $n = p^{\ell_1} + p^{\ell_2} + \cdots + p^{\ell_i}$. For all $x \in \mathbb{F}_q$, we have

$$
\begin{aligned}
&D_{n,k}(1,x) \\
&= \frac{(2-k)}{2^i}(1-4x)^{\frac{p^{\ell_1}+p^{\ell_2}+\cdots+p^{\ell_i}}{2}} + \frac{k}{2^i}\sum_{j_1,j_2,\ldots,j_{i-1}\in\{\ell_1,\ell_2,\ldots,\ell_i\}}(1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_{i-1}}-1}{2}} \\
&+ \frac{(2-k)}{2^i}\sum_{j_1,j_2,\ldots,j_{i-2}\in\{\ell_1,\ell_2,\ldots,\ell_i\}}(1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_{i-2}}}{2}} \\
&+ \frac{k}{2^i}\sum_{j_1,j_2,\ldots,j_{i-3}\in\{\ell_1,\ell_2,\ldots,\ell_i\}}(1-4x)^{\frac{p^{j_1}+p^{j_2}+\cdots+p^{j_{i-3}}-1}{2}} + \cdots\cdots \\
&+ \frac{(2-k)}{2^i}\sum_{j_1,j_2\in\{\ell_1,\ell_2,\ldots,\ell_i\}}(1-4x)^{\frac{p^{j_1}+p^{j_2}}{2}} + \frac{k}{2^i}\sum_{j_1\in\{\ell_1,\ell_2,\ldots,\ell_i\}}(1-4x)^{\frac{p^{j_1}-1}{2}} + \frac{(2-k)}{2^i}.
\end{aligned}
$$

Permutation behaviour of $D_{p^{\ell_1}+p^{\ell_2},k}$

$$D_{p^{l_1}+p^{l_2},k}(1,x) = \frac{(2-k)}{4}(1-4x)^{\frac{p^{l_1}+p^{l_2}}{2}} + \frac{k}{4}(1-4x)^{\frac{p^{l_1}-1}{2}} + \frac{k}{4}(1-4x)^{\frac{p^{l_2}-1}{2}}.$$

Corollary

Let $k = 0$. Then $D_{p^{\ell_1}+p^{\ell_2},k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $\gcd(\frac{p^{\ell_1}+p^{\ell_2}}{2}, p^e - 1) = 1$.

Corollary

Let $p = 3$ and $k = 2$. Assume that both ℓ_1 and ℓ_2 are odd. Then $D_{p^{\ell_1}+p^{\ell_2},k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if the binomial $x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}}$ is a PP of $\mathbb{F}_q$.

Theorem

Let $p > 3$ and $k = 2$. Then $D_{p^{\ell_1}+p^{\ell_2},k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$.

Permutation behaviour of $D_{p^{\ell_1}+p^{\ell_2},k}$ (contd.)

Corollary

Let $k \neq 0, 2$ and $p > 3$. Assume that $\frac{2k}{(k-2)}$ is a quadratic residue of p. Then $D_{p^{\ell_1}+p^{\ell_2},k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $\ell_1 = \ell_2 = 0$.

Corollary

Let $k \neq 0, 2$ and $p > 3$. Assume that $\frac{2k}{(k-2)}$ is a quadratic non-residue of p. Then $D_{p^{\ell_1}+p^{\ell_2},k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if the trinomial $(2-k)\,x^{\frac{p^{\ell_1}+p^{\ell_2}}{2}} + k\,x^{\frac{p^{\ell_1}-1}{2}} + k\,x^{\frac{p^{\ell_2}-1}{2}}$ is a PP of $\mathbb{F}_{p^e}$.

More results on $D_{n,k}(1, x)$

Lemma

Let ℓ be a positive odd integer and let $n = \frac{3^\ell+1}{2}$. Then in $\mathbb{F}_3[x]$,

$$D_{n,k}(1, 1 - x^2) = \left(\frac{k}{2} - 1\right) D_n(x, 1) + \frac{k}{2} \frac{D_{n-1}(x, 1)}{x}.$$

Remark

This result generalizes Lemma 5.5 in X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, Reversed Dickson polynomials over finite fields, Finite Fields Appl. **15** *(2009), 748 – 773..*

More results on $D_{n,k}(1,x)$ (contd.)

For all $x \in \mathbb{F}_q$ we have

$$D_{n,k}(1,x) = k\,x\,D_{n-2,1}(1,x) + D_n(1,x), \quad n \geq 2,$$

and

$$D_{n,k}(1,x) = k\,x\,D_{n-1,2}(1,x) + D_n(1,x), \quad n \geq 1.$$

Recursion

Proposition

Let p be an odd prime and n be a non-negative integer. Then

$$D_{0,k}(1,x) = 2 - k, \;\; D_{1,k}(1,x) = 1, \;\; \text{and}$$

$$D_{n,k}(1,x) = D_{n-1,k}(1,x) - x\, D_{n-2,k}(1,x), \;\; \text{for } n \geq 2.$$

A Matrix Form of $D_{n,k}(1, x)$

$$D_{n,k}(1, x) = \begin{pmatrix} 2-k, & 1 \end{pmatrix} \begin{pmatrix} 0 & -x \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

For further details

N. F., *Reversed Dickson polynomials of the* $(k+1)$*-th kind over finite fields, II*, submitted for publication. arXiv:1706.01391

Acknowledgement

1. Ariane Masuda at CUNY.
2. Anthony Iarrobino at Northeastern University.

Thank you!