Reversed Dickson polynomials of the $(k+1)$-th kind over finite fields, II

Neranga Fernando

Department of Mathematics
Northeastern University
Boston

AMS Fall Central Sectional Meeting
University of North Texas, Denton, TX

September 9, 2017

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

Background

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 $0 \leq k \leq p-1$.

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

Results from Part I

1. The case $a = 0$

2. Some general properties of $D_{n,k}(a, x)$.

3. To discuss the permutaion behaviour of $D_{n,k}(a, x)$, one only has to consider $a = 1$.

4. The case $n = p^\ell$, where $\ell \geq 0$ is an integer.

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

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

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

8. The sum $\sum_{a \in \mathbb{F}_q} D_{n,k}(1, a)$.

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

Outline of the rest of the talk

1. The case $n = p^\ell + 3$.
2. The case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$.
3. The case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3} + p^{\ell_4}$.
4. A generalization to $n = p^{\ell_1} + p^{\ell_2} + \cdots + p^{\ell_i}$.
5. Permutation behaviour of $D_{p^{\ell_1}+p^{\ell_2},k}$.
6. More results on $D_{n,k}(1, x)$.
7. A Matrix Form of $D_{n,k}(1, x)$.

ℓ and ℓ_i are non-negative integers throughout the talk.

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 $\mathbb{F}_{p^e}$.

The Case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$

Proposition

$D_{p^{\ell_1}+p^{\ell_2}+p^{\ell_3},k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the seven-term polynomial

$$k\,x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}-1}{2}} + (2-k)\,[x^{\frac{p^{\ell_1}+p^{\ell_2}}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_3}}{2}} + x^{\frac{p^{\ell_2}+p^{\ell_3}}{2}}]$$
$$+ k[x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}} + x^{\frac{p^{\ell_3}-1}{2}}]$$

is a PP of $\mathbb{F}_q$.

The Case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$ with $p = 3$

Theorem

Let $k = 0$, $p = 3$, and $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$, where ℓ_1, ℓ_2, and ℓ_3 are non-negative integers. Then $D_{n,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

Theorem

Let $k = 1$, $p = 3$, and $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$. Assume that exactly one of ℓ_1, ℓ_2, ℓ_3 is zero. Then $D_{n,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

Theorem

Let $k = 1$, $p = 3$, and $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$. Assume that $\ell_1 \neq 0$, $\ell_2 \neq 0$ and $\ell_3 \neq 0$. Then $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if

$$x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}-1}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_2}}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_3}}{2}} + x^{\frac{p^{\ell_2}+p^{\ell_3}}{2}} + x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}} + x^{\frac{p^{\ell_3}-1}{2}}.$$

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

The Case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$ with $p = 3$ (contd.)

Theorem

Let $k = 2$, $p = 3$, and $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$. Assume that exactly one of ℓ_1, ℓ_2, ℓ_3 is zero. Then $D_{n,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

Theorem

Let $k = 2$, $p = 3$, and $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$. Assume that $\ell_1 \neq 0$, $\ell_2 \neq 0$ and $\ell_3 \neq 0$. Then $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if

$$x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}-1}{2}} + x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}} + x^{\frac{p^{\ell_3}-1}{2}}$$

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

The Case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3}$ with $p > 3$

Theorem

Let $p > 3$, $k \neq 3$, and $\frac{3k}{2(k-3)}$ be a quadratic residue of p. Then $D_{p^{\ell_1}+p^{\ell_2}+p^{\ell_3},k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $\ell_1 = \ell_2 = \ell_3 = 0$.

Theorem

Let $p > 3$, $k \neq 3$, and $\frac{3k}{2(k-3)}$ be a quadratic non-residue of p. Then $D_{p^{\ell_1}+p^{\ell_2}+p^{\ell_3},k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if

$$k\, x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}-1}{2}}$$

$$+ (2-k)\left[x^{\frac{p^{\ell_1}+p^{\ell_2}}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_3}}{2}} + x^{\frac{p^{\ell_2}+p^{\ell_3}}{2}}\right] + k\left[x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}} + x^{\frac{p^{\ell_3}-1}{2}}\right]$$

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

Remark

Let $p > 3$ and $k = 3$. Then $D_{p^{\ell_1}+p^{\ell_2}+p^{\ell_3},k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ for any ℓ_1, ℓ_2, and ℓ_3.

The Case $n = p^{\ell_1} + p^{\ell_2} + p^{\ell_3} + p^{\ell_4}$

Proposition

$D_{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}+p^{\ell_4},k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$
\begin{aligned}
&(2-k)\,x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}+p^{\ell_4}}{2}} \\
&+ k\,[x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_3}-1}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_2}+p^{\ell_4}-1}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_3}+p^{\ell_4}-1}{2}} + x^{\frac{p^{\ell_2}+p^{\ell_3}+p^{\ell_4}-1}{2}}] \\
&+ (2-k)\,[x^{\frac{p^{\ell_1}+p^{\ell_2}}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_3}}{2}} + x^{\frac{p^{\ell_2}+p^{l}3}{2}} + x^{\frac{p^{\ell_1}+p^{\ell_4}}{2}} + x^{\frac{p^{\ell_2}+p^{\ell_4}}{2}} + x^{\frac{p^{\ell_3}+p^{\ell_4}}{2}}] \\
&+ k\,[x^{\frac{p^{\ell_1}-1}{2}} + x^{\frac{p^{\ell_2}-1}{2}} + x^{\frac{p^{\ell_3}-1}{2}} + x^{\frac{p^{\ell_4}-1}{2}}]
\end{aligned}
$$

is a PP of $\mathbb{F}_q$.

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

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 (from Part I) 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*. arXiv:1706.01391

Acknowledgement

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

Thank you!