Reversed Dickson Polynomials of the Third Kind

Neranga Fernando

Department of Mathematics
Northeastern University

47th Southeastern International Conference on
Combinatorics, Graph Theory & Computing

Florida Atlantic University
Boca Raton

March 7 - 11 ,2016

Motivation

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

(2) X. Hou, T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl. **16** (2010), 436 – 448.

(3) 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.

Outline

- Introduction
- Properties of the reversed Dickson polynomials of the third kind $F_n(a, x)$
- Necessary conditions for the reversed Dickson polynomials of the third kind to be a permutation of $\mathbb{F}_q$
- The sum $\sum_{a \in \mathbb{F}_q} F_n(1, a)$

Introduction

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

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. Selelrs, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009), 748 – 773.

Introduction

The n-th reversed Dickson polynomial of the second kind $E_n(a, x)$ is 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.

Introduction

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

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

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

Introduction

The n-th reversed Dickson polynomial of the third kind $D_{n,2}(a,x)$ is given by

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

We denote the n-th reversed Dickson polynomial of the third kind $D_{n,2}(a,x)$ by $F_n(a,x)$.

The Case $a = 0$

When $a = 0$, the reversed Dickson polynomials of the first kind satisfy

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

and the reversed Dickson polynomials of the second kind satisfy

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

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

$F_n(0, x) = 2E_n(0, x) - D_n(0, x) \Rightarrow F_n(0, x) = 0$ for all n.

Hence $F_n(a, x)$ is not a PP when $a = 0$.

Let $a \in \mathbb{F}_q^*$. Then

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

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

The functional equation

For $a \neq 0$, Let $x = y + ay^{-1}$ for some $y \in \mathbb{F}_{q^2}$ with $y \neq 0$ and $y^2 \neq a$. Then the functional equation of $F_n(a, x)$ is given by

$$F_n(a, x) = \frac{a}{2y - a}(y^n - (a - y)^n), \text{ where } y \neq \frac{a}{2}.$$

If $char(\mathbb{F}_q) = 2$, then $F_n(1, x)$ is the n-th reversed Dickson polynomial of the first kind $D_n(1, x)$.

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

Recurrence

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

$$F_0(1, x) = 0, \ F_1(1, x) = 1, \text{ and}$$

$$F_n(1, x) = F_{n-1}(1, x) - x\, F_{n-2}(1, x), \text{ for } n \geq 2.$$

Theorem

let p be an odd prime, n and k be positive integers. Then we have the following.

(1) If $y \neq \frac{1}{2}$, then $F_n(1, y(1-y)) = \dfrac{y^n - (1-y)^n}{2y-1}$.

Also, $F_n(1, \frac{1}{4}) = \frac{n}{2^{n-1}}$.

(2) If $\gcd(n, k) = 1$, then $F_{np^k}(1, x) = (F_n(1, x))^{p^k}(1-4x)^{\frac{p^k-1}{2}}$.

(3) If $n_1 \equiv n_2 \pmod{q^2-1}$, then $F_{n_1}(1, x_0) = F_{n_2}(1, x_0)$ for any $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.

Two Theorems

Theorem

Let p be an odd prime. $q = p^e$, $e, k \in \mathbb{Z}^+$, $1 \leq k \leq e$. Then $F_{p^k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $\left(\frac{p^k-1}{2}, q-1\right) = 1$.

Theorem

Let p be an odd prime. $q = p^e$, $e, k \in \mathbb{Z}^+$, $1 \leq k \leq e$. Then $F_{2 \cdot p^k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $\left(\frac{p^k-1}{2}, q-1\right) = 1$.

Theorem

Let p be an odd prime. Then

$F_n(1, x)$ is a PP of $\mathbb{F}_q$ if and only if the function $y \mapsto \dfrac{y^n - (1-y)^n}{2y-1}$ is a 2-to-1 mapping on $(\mathbb{F}_q \cup V) \setminus \frac{1}{2}$ and $\dfrac{y^n - (1-y)^n}{2y-1} \neq \dfrac{n}{2^{n-1}}$ for any $y \in (\mathbb{F}_q \cup V) \setminus \frac{1}{2}$.

Necessary Conditions

$$F_n(1,1) = \begin{cases} 0 & , \quad n \equiv 0,3 \pmod 6, \\ 1 & , \quad n \equiv 1,2 \pmod 6, \\ -1 & , \quad n \equiv 4,5 \pmod 6. \end{cases}$$

Note that $F_n(1,0) = 1$.

Theorem

Assume that $F_n(1,x)$ is a PP of $\mathbb{F}_q$. If $p = 2$, then $3|n$. If p is an odd prime, then $n \not\equiv 1,2 \pmod 6$.

An Explicit Expression of $F_n(a, x)$

Define

$$f_n(x) = \sum_{j \geq 0} \binom{n}{2j+1} x^j.$$

Proposition

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

$$F_n(1, x) = \left(\frac{1}{2}\right)^{n-1} f_n(1 - 4x).$$

In particular, $F_n(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $f_n(x)$ is a PP of $\mathbb{F}_q$.

More Necessary Conditions

Theorem

Let p be an odd prime, q a power of p, and n be a nonnegative integer with $p \nmid n$. If $F_n(1,x)$ is a PP of $\mathbb{F}_q$, then $n \equiv 0 \pmod 4$ and $(\lfloor \frac{n-1}{2} \rfloor, q-1) = 1$.

Theorem

Let $p > 3$ be an odd prime and $n \geq 0$ be an integer with $3|n$. If $F_n(1,x)$ is a PP of $\mathbb{F}_q$, then $(n, q^2-1) = 3$.

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

Generating Function of $F_n(1, x)$

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

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

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

Also, since $F_{n_1}(1,x) = F_{n_2}(1,x)$ 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

$$\sum_{n\geq 0} F_n\,z^n \equiv \frac{1}{1-z^{q^2-1}}\sum_{n=1}^{q^2-1} F_n\,z^n \pmod{x^q-x} \quad (2)$$

Combining (1) and (2) gives

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

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

$$\sum_{n=1}^{q^2-1} F_n z^n \equiv \frac{z\left(z^{q^2-1}-1\right)}{z-1} + h(z)\sum_{k=1}^{q-1}(z-1)^{q-1-k}\, z^{2k}\, x^k \pmod{x^q-x},$$

where

$$h(z) = \frac{z\left(-1-(z-z^q)^{q-1}\right)}{z^q-z^{q-1}-1}.$$

Let $\sum_{k=1}^{q^2-q+1} b_k z^k = z\left(-1-(z-z^q)^{q-1}\right)$. Write $k=\alpha+\beta q$ where $0\le\alpha,\beta\le q-1$. Then we have

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

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

$$\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q} F_n(1,a)\Big)z^n$$

$$= \sum_{n=1}^{q^2-1} \frac{n}{2^{n-1}}\, z^n - \frac{z(1-z^{q^2-1})}{1-z} - h(z)\, z^{2(q-1)} - h(z)\sum_{j=1}^{q-1}(z-1)^{q-1-j}\, z^{2j}\left(\frac{1}{4}\right)^j, \tag{3}$$

From (3), we have

$$(z^q - z^{q-1} - 1)\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q} F_n(1,a) - \frac{n}{2^{n-1}}\Big)z^n$$

$$= (1 + z^{q-1} - z^q)\sum_{k=1}^{q^2-1} z^k - \Big(z^{2(q-1)} + \sum_{j=1}^{q-1}(z-1)^{q-1-j}\, z^{2j}\left(\frac{1}{4}\right)^j\Big)\Big(\sum_{k=1}^{q^2-q+1} b_k z^k\Big). \tag{4}$$

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

Let $d_n = \sum_{a\in\mathbb{F}_q} F_n(1,a) - \frac{n}{2^{n-1}}$ and the right hand side of (4) be $\sum_{k=1}^{q^2+q-1} c_k z^k$.

Then we have

$$(z^q - z^{q-1} - 1) \sum_{n=1}^{q^2-1} d_n z^n = \sum_{k=1}^{q^2+q-1} c_k z^k. \qquad (5)$$

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

Theorem

Let c_k be defined as in (5) for $1 \le k \le q^2+q-1$. Then we have the following.

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

$$\sum_{a\in\mathbb{F}_q} F_q(1,a) = c_1 - c_q;$$

$$\sum_{a\in\mathbb{F}_q} F_{lq+j} = \sum_{a\in\mathbb{F}_q} F_{(l-1)q+j} - \sum_{a\in\mathbb{F}_q} F_{(l-1)q+j+1} - c_{lq+j} + \frac{2^q(1-j)+2j}{2^{lq+j}} \text{ if } 1 \le l \le q-2 \text{ and } 1 \le j \le q-1;$$

$$\sum_{a\in\mathbb{F}_q} F_{lq} = \sum_{a\in\mathbb{F}_q} F_{(l-1)q} - \sum_{a\in\mathbb{F}_q} F_{(l-1)q+1} - c_{lq} + \frac{1}{2^{(l-1)q}} \text{ if } 2 \le l \le q-2;$$

$$\sum_{a\in\mathbb{F}_q} F_{q^2-q+j} = \sum_{i=j}^{q-1} c_{q^2+i} + \frac{j}{2^{q^2-q+j-1}} \text{ if } 0 \le j \le q-1.$$

For more details

N. Fernando, *Reversed Dickson polynomials of the third kind*, arXiv:1602.04545.

References

(1) S. D. Cohen, *Dickson polynomials of the second kind that are permutations*, Can. J. Math. **16** (1994), 225 – 238.

(2) X. Hou, *On the asymptotic number of inequivalent binary self-dual codes*, J. Combin. Theory Ser. A **114** (2007), 522 – 544.

(3) R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

(4) R. Lidl, G. L. Mullen, G. Turnwald, *Dickson polynomials*, Longman Scientific and Technical, Essex, United Kingdom, 1993.

Thank You!