Gloria Scientiam Golden Jubilee Commemorative Volume, Faculty of Science, University of Kelaniya 2017. Chapter 50: 585 - 598

Reversed Dickson polynomials of the third kind

Neranga Fernando

Department of Mathematics, Northeastern University, Boston, MA 02115, USA

Email: w.fernando@northeastern.edu

Abstract

Let p be a prime and $q = p^e$. We discuss the properties of the reversed Dickson polynomial $D_{n,2}(1, x)$ of the third kind. We also give several necessary conditions for the reversed Dickson polynomial of the third kind $D_{n,2}(1, x)$ to be a permutation of $\mathbb{F}_q$. In particular, we give explicit evaluation of the sum $\sum_{a\in\mathbb{F}_q} D_{n,2}(1, a)$.

Keywords: Finite field, Permutation polynomial, Dickson polynomial, Chebyshev polynomial, Integer sequence.

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 $f \in \mathbb{F}_q[\mathbf{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. In the study of permutation polynomials over finite fields, Dickson polynomials have played a pivotal role.

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.

The permutation property of the Dickson polynomials of the first kind is completely known. When $a = 0$, $D_n(x, a) = x^n$, which is a PP over $\mathbb{F}_q$ if and only if $(n, q-1) = 1$. When $0 \neq a \in \mathbb{F}_q$, $D_n(x, a)$ is a PP over $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$; see Theorem 7.16 in Lidl *et al.* 1997 or Theorem 3.2 in Lidl *et al.* 1993.

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

The permutation behavior of the Dickson polynomials of the second kind has been extensively studied by many authors. We refer the reader to Cohen (1994) for more details about the Dickson polynomials of the second kind.

Dickson polynomials are closely related to the well-known Chebyshev polynomials over the complex numbers by

$$D_n(2x,1) = 2T_n(x) \qquad \text{and} \qquad E_n(2x,1) = U_n(x),$$

where $T_n(x)$ and $U_n(x)$ are Chebyshev polynonmials of degree n of the first kind and the second kind, respectively.

The n-th reversed Dickson polynomial of the first kind $D_n(a,x)$ was first introduced by Hou, Mullen, Sellers and Yucas in Hou *et al.* 2009 by reversing the roles of the variable and the parameter in the n-th Dickson polynomial of the first kind $D_n(x,a)$. It was shown that when $a=0$, $D_n(0,x)$ is a PP over $\mathbb{F}_q$ if and only if $n=2k$ with $(k,q-1)=1$. Also, when $a \neq 0$,

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

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

In Hou *et al.* 2010, Hou and Ly further studied the reversed Dickson polynomials of the first kind $D_n(1,x)$ and explained several necessary conditions for $D_n(1,x)$ to be a permutation of $\mathbb{F}_q$.

Recently, Hong, Qin, and Zhao studied reversed Dickson polynomials of the second kind in Hong *et al.* 2016. They presented several necessary conditions for the reversed Dickson polynomial of the second kind $E_n(1,x)$ to be a permutation of $\mathbb{F}_q$.

In Wang *et al.* 2012, Wang and Yucas introduced the n-th Dickson polynomial of the $(k+1)$-th kind and the n-th reversed Dickson polynomial of the $(k+1)$-th kind.

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

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

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

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}. \tag{1}$$

Then clearly $D_{n,0}(a,x) = D_n(a,x)$ and $D_{n,1}(a,x) = E_n(a,x)$. In Wang *et al.* 2012, they defined

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

They also showed that $D_{n,k}(x,a) = kE_n(x,a) - (k-1)D_n(x,a)$. A simple computation shows that the reversed Dickson polynomials agree with the above equation as well, i.e.

$$D_{n,k}(a,x) = kE_n(a,x) - (k-1)D_n(a,x). \tag{3}$$

In Wang *et al.* 2012, Wang and Yucas completely described the permutation behavior of the Dickson polynomials of the third kind $D_{n,2}(x,a)$ over any prime field, but the permutation property of $D_{n,2}(x,a)$ over an arbitrary finite field is still an open problem.

The purpose of the present paper is to explore the permutation behavior of the reversed Dickson polynomials of the third kind. By (1), the n-th reversed Dickson polynomial of the third kind $D_{n,2}(a,x)$ is given by

$$D_{n,2}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-2i}{n-i}\binom{n-i}{i}(-x)^i a^{n-2i}. \tag{4}$$

Throughout the paper, we denote the n-th reversed Dickson polynomial of the third kind $D_{n,2}(a,x)$ by $F_n(a,x)$. Here is an overview of the paper.

In the next section, we present several properties of the reversed Dickson polynomials of the third kind. After that, we survey some miscellaneous necessary conditions for $F_n(a,x)$ to be a permutation of $\mathbb{F}_q$. In the last section, we compute the sum $\sum_{a\in\mathbb{F}_q} F_n(1,a)$.

Reversed Dickson polynomials of the third kind

We study the properties of reversed Dickson polynomials of the third kind in this section.

Lemma 1. *$F_n(a,x)$ is not a PP when $a = 0$.*

Proof. When $a = 0$, the reversed Dickson polynomials of the first kind satisfy (See Hou *et al.* 2009)

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

and the reversed Dickson polynomials of the second kind satisfy (See Hong *et al.* 2016)

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

From (3), we have $F_n(0,x) = 2E_n(0,x) - D_n(0,x)$ which implies $F_n(0,x) = 0$ for all n. Hence $F_n(a,x)$ is not a PP when $a = 0$.

□

We thus hereafter assume that $a \in \mathbb{F}_q^*$.

Lemma 2. *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*

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

Proof. Note that

$$D_n(a,x) = y^n + (a-y)^n$$

and

$$E_n(a,x) = \frac{y^{n+1} - (a-y)^{n+1}}{2y-a}$$

are the functional expressions of the reversed Dickson polynomial of the first kind and second kind, respectively. Hence the rest of the proof immediately follows from (3). □

Let $a \in \mathbb{F}_q^*$. Then it follows from (4) that

$$F_n(a,x) = a^n F_n(1, \frac{x}{a^2}). \tag{5}$$

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

Theorem 3. *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 $F_n(1, y(1-y)) = \frac{y^n - (1-y)^n}{2y-1}$. 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 $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.*

Proof.

(1) Let $a = 1$ in Lemma 2, and write $x = y(1-y)$. Then for $y \neq \frac{1}{2}$, we have

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

When $a = 2$ and $x = 1$, from (5) we have

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

which implies

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

We have $D_n(2,1) = 2$ and $E_n(2,1) = n+1$ (See Lidl *et al.* 1993). Then it follows from (3) that

$$F_n(2,1) = 2E_n(2,1) - D_n(2,1) = 2(n+1) - 2 = 2n.$$

Hence

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

(2) Let $x = y(1-y)$ with $y \neq \frac{1}{2}$. Then we have

$$\begin{aligned}
F_{np^k}(1,x) = F_{np^k}(1, y(1-y)) &= \frac{y^{np^k} - (1-y)^{np^k}}{2y-1} \\
&= \frac{(y^n - (1-y)^n)^{p^k}}{2y-1} \\
&= \frac{(y^n - (1-y)^n)^{p^k}}{(2y-1)^{p^k}} \ (2y-1)^{p^k-1} \\
&= (\frac{y^n - (1-y)^n}{2y-1})^{p^k} \ (2y-1)^{p^k-1} \\
&= (F_n(1, y(1-y)))^{p^k} \ (2y-1)^{p^k-1} \\
&= F_n(1,x)^{p^k} \ (2y-1)^{p^k-1} \\
&= F_n(1,x)^{p^k} \ (1-4x)^{\frac{p^k-1}{2}}.
\end{aligned}$$

If $y = \frac{1}{2}$, then

$$F_{np^k}(1, \frac{1}{4}) = \frac{np^k}{2^{np^k} - 1} = 0 = F_n(1,x)^{p^k}(1-4x)^{\frac{p^k-1}{2}}.$$

(3) For $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$, there exists $y_0 \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$ such that $x_0 = y_0(1-y_0)$. Then we have

$$\begin{aligned}
F_{n_1}(1, x_0) &= \frac{y_0^{n_1} - (1-y_0)^{n_1}}{2y_0 - 1} \\
&= \frac{y_0^{n_2} - (1-y_0)^{n_2}}{2y_0 - 1} \\
&= F_{n_2}(1, x_0).
\end{aligned}$$

□

Remark 4. *If $char(\mathbb{F}_q) = 2$, then $F_n(1,x)$ is the n-th reversed Dickson polynomial of the first kind $D_n(1,x)$ since from (1) in Theorem 3 we have*

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

We thus hereafter always assume, unless specified, in this paper that p is odd.

Proposition 5. *Let p be an odd prime and n be a non-negative integer. Then*

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

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

Proof. It follows from Theorem 3 (1) that $F_0(1,x) = 0,\ F_1(1,x) = 1$.

Let $n \geq 2$. When $x \neq \frac{1}{4}$, we write $x = y(1-y)$ with $y \neq \frac{1}{2}$. By Theorem 3 (1), we have

$$\begin{aligned} F_{n-1}(1,x) - x\,F_{n-2}(1,x) &= F_{n-1}(1, y(1-y)) \;-\; y(1-y)\,F_{n-2}(1, y(1-y)) \\ &= \frac{y^{n-1} - (1-y)^{n-1}}{2y-1} \;-\; y(1-y)\,\frac{y^{n-2} - (1-y)^{n-2}}{2y-1} \\ &= \frac{y^n - (1-y)^n}{2y-1} = F_n(1, y(1-y)) = F_n(1,x). \end{aligned}$$

When $x = \frac{1}{4}$,

$$F_{n-1}(1, \frac{1}{4}) - \frac{1}{4}\,F_{n-2}(1, \frac{1}{4}) = \frac{n-1}{2^{n-2}} - \frac{1}{4}\frac{n-2}{2^{n-3}} = \frac{n}{2^{n-1}} = F_n(1, \frac{1}{4}).$$

□

Theorem 6. *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 $\left(\frac{p^k-1}{2}, q-1\right) = 1$.*

Proof. Let $n = 1$ in Theorem 3 (2). Since $F_1(1,x) = 1$, we have $F_{p^k}(1,x) = (F_1(1,x))^{p^k}(1-4x)^{\frac{p^k-1}{2}} = (1-4x)^{\frac{p^k-1}{2}}$. Hence the proof. □

Theorem 7. *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 $\left(\frac{p^k-1}{2}, q-1\right) = 1$.*

Proof. Let $n = 2$ in Theorem 3 (2). Since $F_2(1,x) = 1$, we have $F_{2\cdot p^k}(1,x) = (F_2(1,x))^{p^k}(1-4x)^{\frac{p^k-1}{2}} = (1-4x)^{\frac{p^k-1}{2}}$. Hence the proof. □

Theorem 8. *The generating function of $F_n(1,x)$ is given by*

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

Proof.

$$\begin{aligned} (1 - z + xz^2)\sum_{n=0}^{\infty} F_n(1,x)\,z^n &= \sum_{n=0}^{\infty} F_n(1,x)\,z^n - \sum_{n=0}^{\infty} F_n(1,x)\,z^{n+1} + x\sum_{n=0}^{\infty} F_n(1,x)\,z^{n+2} \\ &= F_0(1,x) + F_1(1,x)z - F_0(1,x)z \\ &\quad + \sum_{n=0}^{\infty} \left(F_{n+2}(1,x) - F_{n+1}(1,x) + xF_n(1,x)\right) z^{n+2} \end{aligned}$$

Since $F_0(1,x) = 0$, $F_1(1,x) = 1$, and $F_{n+2}(1,x) = F_{n+1}(1,x) - xF_n(1,x)$ for $n \geq 0$, we have the desired result. □

Lemma 9. *(See Hou et al. 2009) Let $q = p^e$ and Let $x \in \mathbb{F}_{q^2}$. Then*

$$x(1-x) \in \mathbb{F}_q \text{ if and only if } x^q = x \text{ or } x^q = 1 - x.$$

Also, if we define

$$V = \{x \in \mathbb{F}_{q^2} \, ; \, x^q = 1 - x\},$$

then $\mathbb{F}_q \cap V = \{\frac{1}{2}\}$.

Theorem 10. *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 $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$.*

Proof. For necessity, assume that $F_n(1, x)$ is a PP of $\mathbb{F}_q$ and $y_1, y_2 \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ such that $\dfrac{y_1^n - (1-y_1)^n}{2y_1 - 1} = \dfrac{y_2^n - (1-y_2)^n}{2y_2 - 1}$. Then $y_1(1-y_1), y_2(1-y_2) \in \mathbb{F}_q$ and $F_n(1, y_1(1-y_1)) = F_n(1, y_2(1-y_2))$. Since $F_n(1, x)$ is a PP of $\mathbb{F}_q$, we have $y_1(1-y_1) = y_2(1-y_2)$ which implies that $y_1 = y_2$ or $1 - y_2$. So $y \mapsto \dfrac{y^n - (1-y)^n}{2y-1}$ is a 2-to-1 mapping on $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$. If $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$, then $y(1-y) \in \mathbb{F}_q$ and $y(1-y) \neq \frac{1}{2}(1-\frac{1}{2})$. Thus $\dfrac{y^n - (1-y)^n}{2y-1} = F_n(1, y(1-y)) \neq F_n(1, \dfrac{1}{2}(1 - \dfrac{1}{2})) = \dfrac{n}{2^{n-1}}$.

For sufficiency, assume $x_1, x_2 \in \mathbb{F}_q$ such that $F_n(1, x_1) = F_n(1, x_2)$. Write $x_1 = y_1(1-y_1)$ and $x_2 = y_2(1-y_2)$, where $y_1, y_2 \in (\mathbb{F}_q \cup V)$. Then

$$\frac{y_1^n - (1-y_1)^n}{2y_1 - 1} = F_n(1, x_1) = F_n(1, x_2) = \frac{y_2^n - (1-y_2)^n}{2y_2 - 1}.$$

If $y_1 = \frac{1}{2}$, then

$$F_n(1, x_2) = F_n(1, x_1) = F_n(1, \frac{1}{4}) = \frac{n}{2^{n-1}},$$

which implies that $y_2 = \frac{1}{2}$. Hence $x_1 = x_2$.

If $y_1, y_2 \neq \frac{1}{2}$, since $y \mapsto \dfrac{y^n - (1-y)^n}{2y-1}$ is a 2-to-1 mapping on $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$, we have $y_1 = y_2$ or $y_1 = 1 - y_2$. Hence $x_1 = x_2$.

□

Miscellaneous Results

Note that $F_n(1, 0) = 1$ for $n \geq 1$. Also, we have the following recursion relation for $F_n(1, 1)$.

$$F_0(1,1) = 0, \; F_1(1,1) = 1,$$

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

It follows that

$$F_2(1,1) = 1, F_3(1,1) = 0, F_4(1,1) = -1, F_5(1,1) = -1, F_6(1,1) = 0.$$

Then we have

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

Theorem 11. *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 $n \not\equiv 1,2 \pmod 6$.*

Proof. If $p = 2$, since $F_n(1,x)$ is a PP of $\mathbb{F}_q$ and $F_n(1,0) = 1$, clearly $3|n$. If p is an odd prime, then a similar argument shows that $n \not\equiv 1,2 \pmod 6$. □

Let p be odd. We show that the n-th reversed Dickson polynomial of the third kind $F_n(1,x)$ can be written explicitly. For $n \geq 0$, define

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

Proposition 12. *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 $\mathbb{F}_q$.

Proof. Let $x \in \mathbb{F}_q$. There exists $y \in \mathbb{F}_{q^2}$ such that $x = y(1-y)$. If $x \neq \frac{1}{4}$, we have

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

Let $u = 2y - 1$. Then we have

$$\begin{aligned} F_n(1,x) &= \frac{1}{u}\left\{\left(\frac{1+u}{2}\right)^n - \left(\frac{1-u}{2}\right)^n\right\} \\ &= \left(\frac{1}{2}\right)^n \frac{1}{u}\left\{(1+u)^n - (1-u)^n\right\} \\ &= \left(\frac{1}{2}\right)^{n-1} \sum_{j \geq 0} \binom{n}{2j+1} u^{2j}. \end{aligned}$$

Then we have

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

Since $u = 2y - 1$, $u^2 = 1 - 4y(y-1)$.

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

If $x = \frac{1}{4}$, since $f_n(0) = n$, we have

$$F_n(1,x) = \frac{n}{2^{n-1}} = \left(\frac{1}{2}\right)^{n-1} f_n(0) = \left(\frac{1}{2}\right)^{n-1} f_n(1-4x).$$

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

Theorem 13. *Let p be an odd prime, q a power of p, and n be a nonnegative even integer with $p \nmid n$. If $F_n(1,x)$ is a PP of $\mathbb{F}_q$, then $n \equiv 0 \pmod 4$ and $(\lfloor \frac{n-1}{2} \rfloor, q-1) = 1$.*

Proof. Assume that $F_n(1,x)$ is a PP of $\mathbb{F}_q$. Then by Proposition 12, $f_n(x)$ is PP of $\mathbb{F}_q$.

Let $x_0 \in \mathbb{F}_q$ such that $f_n(x_0) = 0$. $f_n(0) = n \neq 0$. Since f_n is a PP of $\mathbb{F}_q$, $x_0 \neq 0$.

$$f_n(x_0) = \sum_{j \geq 0} \binom{n}{2j+1} x_0^j$$

$$f_n(x_0^{-1}) = \sum_{j \geq 0} \binom{n}{2j+1} x_0^{-j}$$

It is easy to see that

$$f_n(x_0) = x_0^{\lfloor \frac{n-1}{2} \rfloor} f_n(x_0^{-1}).$$

So f_n is a self-reciprocal. Since $f_n(x_0) = 0$ and $x_0^{\lfloor \frac{n-1}{2} \rfloor} \neq 0$, $f_n(x_0^{-1}) = 0$. Since f_n is a PP of $\mathbb{F}_q$, $x_0 = x_0^{-1}$, i.e. $x_0 = \pm 1$.

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

Therefore, $x_0 = -1$.

$$\begin{aligned}
0 &= f_n(-1) \\
&= \sum_{j\geq 0} \binom{n}{2j+1} (-1)^j \\
&= \sum_{j\equiv 1 \pmod 4} \binom{n}{j} - \sum_{j\equiv 3 \pmod 4} \binom{n}{j} \\
&= \frac{1}{4}\Big[2^{n+1} + i^{-1}(1+i)^n - i^{-1}(1-i)^n\Big] \\
&- \frac{1}{4}\Big[2^{n+1} - i^{-1}(1+i)^n + i^{-1}(1-i)^n\Big] \text{(by Eq. 5.5 in Hou 2007)} \\
&= \frac{1}{2i}\Big[(1+i)^n - (1-i)^n\Big] \\
&= \frac{i}{2}\Big[(1-i)^n - (1+i)^n\Big] \\
&= \frac{i}{2}\Big[(\sqrt{2}\, e^{-\frac{\pi}{4}i})^n - (\sqrt{2}\, e^{\frac{\pi}{4}i})^n\Big] \\
&= 2^{\frac{n}{2}-1}\ i\ \Big[e^{-\frac{n\pi}{4}i} - e^{\frac{n\pi}{4}i}\Big].
\end{aligned}$$

We have $\Big[e^{-\frac{n\pi}{4}i} - e^{\frac{n\pi}{4}i}\Big] = 0$. It follows that $n \equiv 0 \pmod 4$.

Let $(\lfloor \frac{n-1}{2} \rfloor, q-1) = d > 1$. Let $\epsilon \in \mathbb{F}_q^*$ such that $o(\epsilon) = d$. Then

$$f_n(\epsilon) = \epsilon^{\lfloor \frac{n-1}{2} \rfloor} f_n(\epsilon^{-1}).$$

$$f_n(\epsilon) = f_n(\epsilon^{-1}).$$

But $\epsilon \neq \epsilon^{-1}$. This contradicts the fact that f_n is a PP of $\mathbb{F}_q$. Hence $(\lfloor \frac{n-1}{2} \rfloor, q-1) = 1$. □

Lemma 14. *(See Hou et al. 2010) Let $\epsilon \neq 0, 1$ in some extension of $\mathbb{F}_q$ (q odd) and let $y = \dfrac{\epsilon+1}{\epsilon-1}$. Then $y^2 \in \mathbb{F}_q$ if and only if $\epsilon^{q+1} = 1$ or $\epsilon^{q-1} = 1$.*

Theorem 15. *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 $(n, q^2-1) = 3$.*

Proof. Since $p > 3$, we have $q \equiv 1$ or $-1 \pmod 3$. Since $3|n$, we have $3|(n, q^2-1)$. We show that $(n, q^2-1) \leq 3$. Assume to the contrary that $(n, q^2-1) > 3$. Let

$$E = \{\epsilon \in \mathbb{F}_{q^2}^* : \epsilon \neq 1,\ \epsilon^{(n,q+1)} = 1 \text{ or } \epsilon^{(n,q-1)} = 1\}.$$

$$\begin{aligned}
|E| &= |\{\epsilon \in \mathbb{F}_{q^2}^* : \epsilon \neq 1,\ \epsilon^{(n,q+1)} = 1\}| + |\{\epsilon \in \mathbb{F}_{q^2}^* : \epsilon \neq 1,\ \epsilon^{(n,q-1)} = 1\}| \\
&- |\{\epsilon \in \mathbb{F}_{q^2}^* : \epsilon \neq 1,\ \epsilon^{(n,q-1,q+1)} = 1\}| \\
&= ((n, q+1) - 1) + ((n, q-1) - 1) - 0 \\
&= (n, q+1) + (n, q-1) - 2.
\end{aligned}$$

Since $(n, q+1)(n, q-1) = (n, q^2-1) \geq 6$, we have $|E| \geq 4$. Let $\epsilon_1, \epsilon_2, \epsilon_3 \in E$ be distinct and let $y_i = \frac{\epsilon_i - 1}{\epsilon_i + 1}$, $i = 1, 2, 3$. By Lemma 14, $y_i \in \mathbb{F}_q$. Since $\epsilon_i = \frac{1+y_i}{1-y_i}$, we have $\left(\frac{1+y_i}{1-y_i}\right)^n = 1$, i.e. $(1+y_i)^n = (1-y_i)^n$, i.e.

$$f_n(y_i^2) = \frac{1}{2y_i}\ \{(1+y_i)^n - (1-y_i)^n\} = 0.$$

Since ϵ_1, ϵ_2, and ϵ_3 are distinct, y_1, y_2, and y_3 are distinct. This contradicts the fact that f_n is a PP of $\mathbb{F}_q$. □

COMPUTATION OF $\sum_{a \in \mathbb{F}_q} F_n(1, a)$

We compute the sum $\sum_{a \in \mathbb{F}_q} F_n(1, a)$ in this section. The result provides a necessary condition for $F_n(1, x)$ to be a PP of $\mathbb{F}_q$. By Theorem 8, we have

$$\begin{aligned}
\sum_{n=0}^{\infty} F_n(1,x)\, z^n &= \frac{z}{1 - z + xz^2} \\
&= \frac{z}{1-z}\ \frac{1}{1 - (\frac{z^2}{z-1})\, x} \\
&= \frac{z}{1-z}\ \sum_{k \geq 0} \Big(\frac{z^2}{z-1}\Big)^k\, x^k \\
&= \frac{z}{1-z}\ \Big[1 + \sum_{k=1}^{q-1} \sum_{l \geq 0} \Big(\frac{z^2}{z-1}\Big)^{k+l(q-1)}\ x^{k+l(q-1)}\Big] \qquad (6) \\
&\equiv \frac{z}{1-z}\ \Big[1 + \sum_{k=1}^{q-1} \sum_{l \geq 0} \Big(\frac{z^2}{z-1}\Big)^{k+l(q-1)}\ x^{k}\Big] \pmod{x^q - x} \\
&= \frac{z}{1-z}\ \Big[1 + \sum_{k=1}^{q-1} \frac{(\frac{z^2}{z-1})^k}{1 - (\frac{z^2}{z-1})^{q-1}}\ x^k\Big] \\
&= \frac{z}{1-z}\ \Big[1 + \sum_{k=1}^{q-1} \frac{(z-1)^{q-1-k}\ z^{2k}}{(z-1)^{q-1} - z^{2(q-1)}}\ x^k\Big]
\end{aligned}$$

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 the following for all $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.

$$\begin{aligned}
\sum_{n \geq 0} F_n\, z^n &= \sum_{n \geq 1} F_n\, z^n \\
&= \sum_{n=1}^{q^2-1} \sum_{l \geq 0} F_{n+l(q^2-1)}\, z^{n+l(q^2-1)} \\
&= \sum_{n=1}^{q^2-1} F_n \sum_{l \geq 0} z^{n+l(q^2-1)} \qquad (7) \\
&= \frac{1}{1 - z^{q^2-1}} \sum_{n=1}^{q^2-1} F_n\, z^n
\end{aligned}$$

Combining (6) and (7) gives

$$\frac{1}{1-z^{q^2-1}}\sum_{n=1}^{q^2-1} F_n\, z^n = \frac{z}{1-z}\,\Big[1+\sum_{k=1}^{q-1}\frac{(z-1)^{q-1-k}\;z^{2k}}{(z-1)^{q-1}-z^{2(q-1)}}\;x^k\Big],\ \text{for all } x\in\mathbb{F}_q\setminus\{\tfrac{1}{4}\},$$

i.e.

$$\sum_{n=1}^{q^2-1} F_n\, z^n = \frac{z\,(z^{q^2-1}-1)}{z-1} + \;h(z)\;\sum_{k=1}^{q-1}(z-1)^{q-1-k}\;z^{2k}\;x^k,\ \text{for all } x\in\mathbb{F}_q\setminus\{\tfrac{1}{4}\},$$

where

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

Note that

$$\begin{aligned} h(z) &= \frac{z\,(z^{q^2-1}-1)}{(z-1)^q - z^{2(q-1)}(z-1)} \\ &= \frac{z\,(z^{q^2-1}-1)}{(1-z^{q-1})\,(z^q - z^{q-1}-1)} \\ &= \frac{z\,(z^{q^2}-z)}{(z-z^q)\,(z^q-z^{q-1}-1)} \\ &= \frac{z\,(-1-(z-z^q)^{q-1})}{z^q-z^{q-1}-1} \end{aligned}$$

Let $\displaystyle\sum_{k=1}^{q^2-q+1} b_k z^k = z\;(-1-(z-z^q)^{q-1})$.

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

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

A computation similar to (4.4) in Hong *et al.* 2016 yields

$$\begin{aligned} &\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q}F_n(1,a)\Big)z^n \\ &= \sum_{n=1}^{q^2-1} F_n(1,\frac{1}{4})\,z^n - \frac{z(1-z^{q^2-1})}{1-z} - h(z)\,z^{2(q-1)} - h(z)\sum_{j=1}^{q-1}(z-1)^{q-1-j}\,z^{2j}\left(\frac{1}{4}\right)^j, \end{aligned}$$

which implies

$$\begin{aligned} &\sum_{n=1}^{q^2-1}\Big(\sum_{a\in\mathbb{F}_q}F_n(1,a)\Big)z^n \\ &= \sum_{n=1}^{q^2-1}\frac{n}{2^{n-1}}\,z^n - \frac{z(1-z^{q^2-1})}{1-z} - h(z)\,z^{2(q-1)} - h(z)\sum_{j=1}^{q-1}(z-1)^{q-1-j}\,z^{2j}\left(\frac{1}{4}\right)^j, \end{aligned} \tag{8}$$

where

$$h(z) = \frac{1}{z^q - z^{q-1} - 1} \sum_{k=1}^{q^2-q+1} b_k z^k.$$

For all integers $1 \le n \le q^2 - 1$, define

$$f_n := \sum_{a \in \mathbb{F}_q} F_n(1, a).$$

Then from (8), we have

$$\begin{aligned} &(z^q - z^{q-1} - 1) \sum_{n=1}^{q^2-1} \Big(f_n - \frac{n}{2^{n-1}} \Big) z^n \\ &= (1 + z^{q-1} - z^q) \sum_{k=1}^{q^2-1} z^k - \Big(z^{2(q-1)} + \sum_{j=1}^{q-1} (z-1)^{q-1-j} z^{2j} \Big(\frac{1}{4}\Big)^j \Big) \Big(\sum_{k=1}^{q^2-q+1} b_k z^k \Big). \end{aligned} \tag{9}$$

Let $d_n = f_n - \frac{n}{2^{n-1}}$ and the right hand side of (9) be $\sum_{k=1}^{q^2+q-1} c_k z^k$.

Then we have

$$(z^q - z^{q-1} - 1) \sum_{n=1}^{q^2-1} d_n z^n = \sum_{k=1}^{q^2+q-1} c_k z^k. \tag{10}$$

Proposition 16. *(See Hong et al. 2016) By comparing the coefficient of z^i on both sides of* (10)*, we have the following.*

$d_j = -c_j$ *if* $1 \le j \le q-1$;

$d_q = c_1 - c_q$;

$d_{lq+j} = d_{(l-1)q+j} - d_{(l-1)q+j+1} - c_{lq+j}$ *if* $1 \le l \le q-2$ *and* $1 \le j \le q-1$;

$d_{lq} = d_{(l-1)q} - d_{(l-1)q+1} - c_{lq}$ *if* $2 \le l \le q-2$;

$d_{q^2-q+j} = \sum_{i=j}^{q-1} c_{q^2+i}$ *if* $0 \le j \le q-1$.

The following theorem is an immediate consequence of Proposition 16 and the fact that $d_n := \sum_{a \in \mathbb{F}_q} F_n(1, a) - \frac{n}{2^{n-1}}$.

Theorem 17. *Let c_k be defined as in* (10) *for $1 \le k \le q^2 + q - 1$. Then we have the following.*

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

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

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

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

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

Acknowledgements

The author would like to thank G. C. Greubel for pointing out an important connection of the reversed Dickson polynomials of the third kind to Jacobsthal polynomials and integer sequences. He pointed out the following.

(1) Proposition 5 is related to the Jacobsthal polynomials by $F_n(1,x) = J_n(-x/2)$.

(2) The generating function presented in Theorem 8 is another indicator to the connection to Jacobsthal polynomials.

(3) The third indicator is the reduction presented near the end of Theorem 10, namely, $F_n(1,\frac{1}{4}) = \frac{n}{2^{n-1}}$.

(4) The number set $\{0,1,1,0,-1,-1,0,1,1,..\}$ presented in miscellaneous results, directly before Theorem 11, is given as sequence $A010892$ in the On-line Encyclopedia of Integer Sequences. The starting point of this sequence mentioned is offset by one index. An alternate sequence is $A128834$.

References

Cohen, S. D. 1994.
Dickson polynomials of the second kind that are permutations. *Canadian Journal of Mathematics* 16: 225-238.

Hong, S., Qin, X., Zhao, W. 2016.
Necessary conditions for reversed Dickson polynomials of the second kind to be permutational. *Finite Fields and Their Applications* 37: 54-71.

Hou, X. and Ly, T. 2010.
Necessary conditions for reversed Dickson polynomials to be permutational. *Finite Fields and Their Applications* 16: 436-448.

Hou, X. 2007.
On the asymptotic number of inequivalent binary self-dual codes. *Journal of Combinatorial Theory Series A* 114: 522-544.

Hou, X., Mullen, G. L., Sellers, J. A., Yucas, J. L. 2009.
Reversed Dickson polynomials over finite fields. *Finite Fields and Their Applications* 15: 748-773.

Lidl, R. and Niederreiter, H. 1997.
Finite Fields, 2nd Edition, Cambridge University Press, Cambridge, Lidl, R., Mullen, G. L., Turnwald, G. 1993.
Dickson polynomials, Longman Scientific and Technical, Essex, United Kingdom,

Wang, Q. and Yucas, J. L. 2012.
Dickson polynomials over finite fields. Finite *Fields and Their Applications* 18: 814-831.