Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 2(4): 586-609
DOI:10.3934/Math.2017.4.586
Received: 6 June 2017
Accepted: 16 October 2017
Published: 6 November 2017

Research article

Permutational behavior of reversed Dickson polynomials over finite fields II

Kaimin Cheng

School of Mathematics and Information, China West Normal University, Nanchong 637009, P.R. China

* **Correspondence:** ckm20@126.com

Abstract: In this paper, we study the special reversed Dickson polynomial of the form $D_{p^{e_1}+...+p^{e_s}+\ell,k}(1,x)$, where $s, e_1, ..., e_s$ are positive integers, ℓ is an integer with $0 \le \ell < p$. In fact, by using Hermite criterion we first give an answer to the question that the reversed Dickson polynomials of the forms $D_{p^s+1,k}(1,x)$, $D_{p^s+2,k}(1,x)$, $D_{p^s+3,k}(1,x)$, $D_{p^s+4,k}(1,x)$, $D_{p^s+p^t,k}(1,x)$ and $D_{p^s+p^t+1,k}(1,x)$ are permutation polynomials of $\mathbb{F}_q$ or not. Finally, utilizing the recursive formula of the reversed Dickson polynomials, we represent $D_{p^{e_1}+...+p^{e_s}+\ell,k}(1,x)$ as the linear combination of the elementary symmetric polynomials with the power of $1-4x$ being the variables. From this, we present a necessary and sufficient condition for $D_{p^{e_1}+...+p^{e_s}+\ell,k}(1,x)$ to be a permutation polynomial of $\mathbb{F}_q$.

Keywords: Permutation polynomial; Reversed Dickson polynomial of $(k+1)$-th kind; Hermite's Criterion
Mathematics Subject Classification: Primary 11T06, 11T55, 11C08

1. Introduction

Permutation polynomials and Dickson polynomials are two of the most important topics in the area of finite fields. Let $\mathbb{F}_q$ be the finite field of characteristic p with q elements. Let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in the indeterminate x. If the polynomial $f(x) \in \mathbb{F}_q[x]$ induces a bijective map from $\mathbb{F}_q$ to itself, then $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (denoted as PP for convenience) of $\mathbb{F}_q$. Properties, constructions and applications of permutation polynomials may be found in [5], [6] and [7]. The *reversed Dickson polynomial of the first kind*, denoted by $D_n(a,x)$, was introduced in [4] and defined as follows

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

if $n \ge 1$ and $D_0(a,x) = 2$, where $[\frac{n}{2}]$ means the largest integer no more than $\frac{n}{2}$. Wang and Yucas [8] extended this concept to that of *the n-th reversed Dickson polynomial of $(k+1)$-th kind* $D_{n,k}(a,x) \in$

$\mathbb{F}_q[x]$, which is defined for $n \geq 1$ by

$$D_{n,k}(a,x) := \sum_{i=0}^{[\frac{n}{2}]} \frac{n-ki}{n-i}\binom{n-i}{i}(-x)^i a^{n-2i} \tag{1.1}$$

and $D_{0,k}(a,x) = 2-k$. Some families of permutation polynomials from the revered Dickson polynomials of the first kind were obtained in [4]. Hong, Qin and Zhao [3] studied the revered Dickson polynomial $E_n(a,x)$ of the second kind. Very recently, the author [1] investigated the reversed Dickson polynomial $D_{n,k}(a,x)$ of the $(k+1)$-th kind and obtained some properties and permutational behaviors of them.

In this paper, we study the special reversed Dickson polynomial of the form $D_{p^{e_1}+\ldots+p^{e_s}+\ell,k}(1,x)$, where $s, e_1, ..., e_s$ are positive integers, ℓ is an integer with $0 \leq \ell < p$. In fact, by using Hermite criterion we first give an answer to the question that the reversed Dickson polynomials of the forms $D_{p^s+1,k}(1,x)$, $D_{p^s+2,k}(1,x)$, $D_{p^s+3,k}(1,x)$, $D_{p^s+4,k}(1,x)$, $D_{p^s+p^t,k}(1,x)$ and $D_{p^s+p^t+1,k}(1,x)$ are permutation polynomials of $\mathbb{F}_q$ or not. Finally, utilizing the recursive formula of the reversed Dickson polynomials, we represent $D_{p^{e_1}+\ldots+p^{e_s}+\ell,k}(1,x)$ as the linear combination of the elementary symmetric polynomials with the power of $1-4x$ being the variables. From this, we present a necessary and sufficient condition for $D_{p^{e_1}+\ldots+p^{e_s}+\ell,k}(1,x)$ to be a permutation polynomial of $\mathbb{F}_q$.

Throughout this paper, as usual, for any given prime number p, we let $v_p(x)$ denote the p-adic valuation of any positive integer x, i.e., $v_p(x)$ is the largest nonnegative integer k such that p^k divides x. We also assume $p = \mathrm{char}(\mathbb{F}_q) \geq 3$ and restrict $0 \leq k < p$.

2. Preliminary lemmas

In this section, we list several properties of the reversed Dickson polynomials $D_{n,k}(a,x)$ of the $(k+1)$-th kind and some useful lemmas.

Lemma 2.1. *[5] Let $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $cf(dx)+b$ is a PP of $\mathbb{F}_q$ for any given $c, d \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$.*

Lemma 2.2. *Let $s \geq 0$ be an integer and a, b be in $\mathbb{F}_q{}^*$. Then the binomial $ax^{\frac{p^s-1}{2}} + bx^{\frac{p^s+1}{2}}$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$.*

Proof. First we assume that the binomial $ax^{\frac{p^s-1}{2}} + bx^{\frac{p^s+1}{2}}$ is a PP of $\mathbb{F}_q$. If $s > 0$, then the equation $ax^{\frac{p^s-1}{2}} + bx^{\frac{p^s+1}{2}} = x^{\frac{p^s-1}{2}}(a+bx) = 0$ has two distinct roots $0, -\frac{b}{a}$ which are in $\mathbb{F}_q$. This is a contradiction. So the integer s must be zero. Conversely, if $s = 0$, then it is easy to check that $ax^{\frac{p^s-1}{2}} + bx^{\frac{p^s+1}{2}}$ is a PP of $\mathbb{F}_q$. Therefore Lemma 2.2 is proved. □

Lemma 2.3. *[1] For any integer $n \geq 0$, we have*

$$D_{n,k}\Big(1, \frac{1}{4}\Big) = \frac{kn-k+2}{2^n}$$

and

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

if $x = y(1-y) \neq \frac{1}{4}$.

Lemma 2.4. *[1] Let $n \geq 2$ be an integer. Then the recursion*

$$D_{n,k}(1,x) = D_{n-1,k}(1,x) - xD_{n-2,k}(1,x)$$

holds for any $x \in \mathbb{F}_q$.

Lemma 2.5. *[1] Let $p = \mathrm{char}(\mathbb{F}_q) \geq 3$ and s be a positive integer. Then*

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

Lemma 2.6. *[2] Let α and e be positive integers. Let $d = \gcd(\alpha, e)$ and p be an odd prime. Then*

$$\gcd(p^\alpha + 1, p^e - 1) = \begin{cases} 2, & if\ \frac{e}{d}\ is\ odd, \\ p^d + 1, & if\ \frac{e}{d}\ is\ even. \end{cases}$$

Lemma 2.7. *[5] Let $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is permutation polynomial of $\mathbb{F}_q$ if and only if the following conditions hold:*

(i) $f(x)$ has exactly one root in $\mathbb{F}_q$;

(ii) For each integer t with $0 < t < q-1$ and $t \not\equiv 0 \pmod p$, the reduction of $f(x)^t \pmod{x^q - x}$ has degree less than $q-1$.

Lemma 2.8. *Let p be a prime with $p > 3$ and a be a nonzero element in $\mathbb{F}_p$. Then the binomial $x^{\frac{p^s-1}{2}} + ax$ is a PP of $\mathbb{F}_{p^e}$ if and only if $s = 0$.*

Proof. Let $p > 3, a \in \mathbb{F}_p^*$. Clearly, if $s = 0$, then $w(x) := x^{\frac{p^s-1}{2}} + ax = 1 + ax$ is a PP of $\mathbb{F}_{p^e}$. In what follows, we show that $w(x) = x^{\frac{p^s-1}{2}} + ax$ is not a PP of $\mathbb{F}_{p^e}$ when $s > 0$. Let $s > 0$ and $s \equiv s_0 \pmod{2e}$ with $0 \leq s_0 \leq 2e-1$. Then

$$w(x) \equiv x^{\frac{p^{s_0}-1}{2}} + ax \pmod{x^{p^e} - x}$$

for any $x \in \mathbb{F}_{p^e}^*$ since $\frac{p^s-1}{2} \equiv \frac{p^{s_0}-1}{2} \pmod{p^e - 1}$, i.e. ,

$$w(x) = x^{\frac{p^{s_0}-1}{2}} + ax \tag{2.1}$$

for any $x \in \mathbb{F}_{p^e}^*$. We consider the following three cases.

Case 1. $s > 0$ and $s_0 = 0$. Then by (2.1) one has $w(x) = 1 + ax$ for any $x \in \mathbb{F}_{p^e}^*$. So $f_2(\frac{1}{a}) = 0$. It then follows from $f_2(0) = 0$ that $w(x) = x^{\frac{p^s-1}{2}} + ax$ is not a PP of $\mathbb{F}_{p^e}$.

Case 2. $s > 0$ and s_0 is a positive even number. Then $x^{\frac{p^{s_0}-1}{2}} = 1$ for each $x \in \mathbb{F}_p^*$. By (2.1) one get $w(x) = 1 + ax$ for any $x \in \mathbb{F}_p^*$. Therefore $w(x) = 0$ has one nonzero root $-\frac{1}{a} \in \mathbb{F}_p^*$. Hence $w(x) = x^{\frac{p^s-1}{2}} + ax$ does not permute $\mathbb{F}_p$ since $f_2(0) = 0$. Note that $f_2(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So one has that $w(x) = x^{\frac{p^s-1}{2}} + ax$ does not permute $\mathbb{F}_{p^e}$.

Case 3. $s > 0$ and s_0 is an odd number. Then $x^{\frac{p^{s_0}-1}{2}} = x^{\frac{p-1}{2}}$ for each $x \in \mathbb{F}_p^*$. It follows from (2.1) that

$$w(x) = x^{\frac{p-1}{2}} + ax$$

for any $x \in \mathbb{F}_p^*$. Then we have

$$(w(x))^2 = x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $w(x)$ is not a PP of $\mathbb{F}_p$. Also note that $f_2(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $w(x)$ is not a PP of $\mathbb{F}_{p^e}$.

The above three cases tell us that $w(x) = x^{\frac{p^s-1}{2}} + ax$ is not a PP of $\mathbb{F}_{p^e}$ when $s > 0$. This finishes the proof of Lemma 2.8. □

3. Reversed Dickson polynomials $D_{p^s+\ell,k}(1, x)$

In this section, we present an explicit formula for $D_{n,k}(1, x)$ when $n = p^s + \ell$ with $s \geq 0$ and $0 \leq \ell < p$. Then we characterize $D_{n,k}(1, x)$ to be a PP of $\mathbb{F}_q$ in this case.

Theorem 3.1. *Let $p = \mathrm{char}(\mathbb{F}_q) \geq 3$ and s be a positive integer. Then*

$$D_{p^s+1,k}(1, x) = \frac{2-k}{4}(1-4x)^{\frac{p^s+1}{2}} + \frac{k}{4}(1-4x)^{\frac{p^s-1}{2}} + \frac{1}{2}. \tag{3.1}$$

Furthermore, we have

$$D_{p^s+2\ell,k}(1, x) = \sum_{i=0}^{\ell} A_{2\ell,p^s+2i-1}(1-4x)^{\frac{p^s+2i-1}{2}} + \sum_{j=0}^{\ell} A_{2\ell,2j}(1-4x)^j, \ell \geq 0$$

and

$$D_{p^s+2\ell+1,k}(1, x) = \sum_{i=0}^{\ell+1} A_{2\ell+1,p^s+2i-1}(1-4x)^{\frac{p^s+2i-1}{2}} + \sum_{j=0}^{\ell} A_{2\ell+1,2j}(1-4x)^j, \ell \geq 0,$$

where all the coefficients $A_{i,j}$ are given as follows:

$$A_{0,p^s-1} = \frac{k}{2}, A_{0,0} = \frac{2-k}{2}, A_{1,p^s+1} = \frac{2-k}{4}, A_{1,p^s-1} = \frac{k}{4}, A_{1,0} = \frac{1}{2},$$

and

$$\begin{cases} A_{2m+2,p^s+2m+1} = A_{2m+1,p^s+2m+1} + \frac{1}{4}A_{2m,p^s+2m-1}, & \text{if } m \geq 0 \\ A_{2m+2,p^s+2i-1} = A_{2m+1,p^s+2i-1} - \frac{1}{4}A_{2m,p^s+2i-1} + \frac{1}{4}A_{2m,p^s+2i-3}, & \text{if } 1 \leq i \leq m \\ A_{2m+2,p^s-1} = A_{2m+1,p^s-1} - \frac{1}{4}A_{2m,p^s-1}, & \text{if } m \geq 0 \\ A_{2m+2,0} = A_{2m+1,0} - \frac{1}{4}A_{2m,0}, & \text{if } m \geq 0 \\ A_{2m+2,2j} = A_{2m+1,2j} - \frac{1}{4}A_{2m,2j} + \frac{1}{4}A_{2m,2j-2}, & \text{if } 1 \leq j \leq m \\ A_{2m+2,2m+2} = \frac{1}{4}A_{2m,2m}, & \text{if } m \geq 0 \end{cases} \tag{3.2}$$

as well as

$$\begin{cases} A_{2m+1,p^s+2m+1} = \frac{1}{4}A_{2m-1,p^s+2m-1}, & \text{if } m \geq 0 \\ A_{2m+1,p^s+2i-1} = A_{2m,p^s+2i-1} - \frac{1}{4}A_{2m-1,p^s+2i-1} + \frac{1}{4}A_{2m-1,p^s+2i-3}, & \text{if } 1 \leq i \leq m \\ A_{2m+1,p^s-1} = A_{2m,p^s-1} - \frac{1}{4}A_{2m-1,p^s-1}, & \text{if } m \geq 0 \\ A_{2m+1,0} = A_{2m,0} - \frac{1}{4}A_{2m-1,0}, & \text{if } m \geq 0 \\ A_{2m+1,2j} = A_{2m,2j} - \frac{1}{4}A_{2m-1,2j} + \frac{1}{4}A_{2m-1,2j-2}, & \text{if } 1 \leq j \leq m-1 \\ A_{2m+1,2m} = A_{2m,2m} + \frac{1}{4}A_{2m-1,2m-2}, & \text{if } m \geq 0. \end{cases} \tag{3.3}$$

Proof. First of all, we show (3.1) is true. We consider the following two cases.

CASE 1. $x \neq \frac{1}{4}$. For this case, putting $x = y(1-y)$ in second identity of Lemma 2.3 gives us that

$$\begin{aligned}
&D_{p^s+1,k}(1,x) = D_{p^s+1,k}(1, y(1-y))\\
=&\frac{\frac{k+(2-k)u}{2}(\frac{u+1}{2})^{p^s+1} - \frac{k+(k-2)u}{2}(\frac{1-u}{2})^{p^s+1}}{u}\\
=&\frac{2-k}{8}\Big((u+1)^{p^s}(u+1) + (1-u)^{p^s}(1-u)\Big) + \frac{k}{8u}\Big((u+1)^{p^s}(u+1) - (1-u)^{p^s}(1-u)\Big)\\
=&\frac{2-k}{4}(u^{p^s+1}+1) + \frac{k}{4}(u^{p^s-1}+1)\\
=&\frac{2-k}{4}((u^2)^{\frac{p^s+1}{2}}) + \frac{k}{4}((u^2)^{\frac{p^s-1}{2}}) + \frac{1}{2},
\end{aligned}$$

where $u = 2y-1$ and $u^2 = 1-4x$. So (3.1) follows if $x \neq \frac{1}{4}$.

CASE 2. $x = \frac{1}{4}$. By the first identity of Lemma 2.3, one has

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

as required. Thus (3.1) is true for any $x \in \mathbb{F}_q$.

Now we give the the remainder proof of Theorem 3.1. By Lemmas 2.4-2.5 and (3.1), we readily find that there exists coefficients $A_{i,j} \in \mathbb{F}_q$ such that

$$D_{p^s+2\ell,k}(1,x) = \sum_{i=0}^{\ell} A_{2\ell,p^s+2i-1}(1-4x)^{\frac{p^s+2i-1}{2}} + \sum_{j=0}^{\ell} A_{2\ell,2j}(1-4x)^j \tag{3.4}$$

with $0 \le \ell \le \frac{p-1}{2}$ and

$$D_{p^s+2\ell+1,k}(1,x) = \sum_{i=0}^{\ell+1} A_{2\ell+1,p^s+2i-1}(1-4x)^{\frac{p^s+2i-1}{2}} + \sum_{j=0}^{\ell} A_{2\ell+1,2j}(1-4x)^j \tag{3.5}$$

with $0 \le \ell < \frac{p-1}{2}$. Therefore we now only need to determine all the coefficients $A_{i,j}$. Let $u^2 = 1-4x$. On the one hand, by (3.4) and (3.5), one then has

$$\begin{aligned}
&D_{p^s+2\ell,k}(1,x) - xD_{p^s+2\ell-1,k}(1,x) = D_{p^s+2\ell,k}(1,x) - \frac{1-u^2}{4}D_{p^s+2\ell-1,k}(1,x)\\
&= \sum_{i=0}^{\ell+1} A_{2\ell,p^s+2i-1}u^{p^s+2i-1} + \sum_{j=0}^{\ell} A_{2\ell,2j}u^{2j} - \frac{1}{4}\sum_{i=0}^{\ell} A_{2\ell-1,p^s+2i-1}u^{p^s+2i-1}\\
&\quad - \frac{1}{4}\sum_{j=0}^{\ell-1} A_{2\ell-1,2j}u^{2j} + \frac{1}{4}\sum_{i=0}^{\ell} A_{2\ell-1,p^s+2i-1}u^{p^s+2i+1} + \frac{1}{4}\sum_{j=0}^{\ell-1} A_{2\ell-1,2j}u^{2j+2}\\
&= \frac{1}{4}A_{2\ell-1,p^s+2\ell-1}u^{p^s+2\ell+1} + \sum_{i=1}^{\ell}(A_{2\ell,p^s+2i-1} - \frac{1}{4}A_{2\ell-1,p^s+2i-1} + \frac{1}{4}A_{2\ell-1,p^s+2i-3})u^{p^s+2i-1}\\
&\quad + (A_{2\ell,p^s-1} - \frac{1}{4}A_{2\ell-1,p^s-1})u^{p^s-1} + (A_{2\ell,2\ell} + \frac{1}{4}A_{2\ell-1,2\ell-2})u^{2\ell}
\end{aligned}$$

$$+\sum_{j=1}^{\ell-1}(A_{2\ell,2j}-\frac{1}{4}A_{2\ell-1,2j}+\frac{1}{4}A_{2\ell-1,2j-2})u^{2j}+A_{2\ell,0}-\frac{1}{4}A_{2\ell-1,0}. \tag{3.6}$$

On the other hand, Lemma 2.4 tells us that

$$D_{p^s+2\ell+1,k}(1,x)=D_{p^s+2\ell,k}(1,x)-xD_{p^s+2\ell-1,k}(1,x).$$

So by comparing the coefficient of the term u^i in the right hand side of (3.6) and (3.5), one can get the desired results as (3.3). Following the similar way, one also obtain the recursions of $A_{i,j}$ as (3.2). So the proof Theorem 3.1 is complete. □

For any nonzero integer x, let $v_2(x)$ be the *2-adic valuation* of x. By Theorem 3.1, the following results are established.

Theorem 3.2. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s be a nonnegative integer. Then each of following is true.*

(i). *If $k = 0$, then $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if either $p \equiv 1 \pmod 4$ and $v_2(s) \geq v_2(e)$, or $p \equiv 3 \pmod 4$ and $v_2(s) \geq \max\{v_2(e), 1\}$.*

(ii). *If $k = 2$, then $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $p = 3$, $v_2(s) = 0$ and $\gcd(s, e) = 1$.*

(iii). *If $k \neq 2$ and $k \neq 0$, then $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$.*

Proof. By (3.1) of Theorem 3.1, we have that $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$(2-k)x^{\frac{p^s+1}{2}}+kx^{\frac{p^s-1}{2}}$$

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

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

$$\gcd\Big(\frac{p^s+1}{2},p^e-1\Big)=1.$$

So we consider the following two cases on the odd prime p.

Case 1. $p \equiv 1 \pmod 4$. Then $\frac{p^s+1}{2}$ must be odd. It then follows that

$$\gcd\Big(\frac{p^s+1}{2},p^e-1\Big)=\gcd\Big(\frac{p^s+1}{2},\frac{p^e-1}{2}\Big)=\frac{1}{2}\gcd(p^s+1,p^e-1).$$

So in this case, by Lemma 2.6 we get that $\gcd(\frac{p^s+1}{2}, p^e-1) = 1$ if and only if $\frac{e}{\gcd(s,e)}$ is odd which is equivalent to $v_2(e) \leq v_2(s)$.

Case 2. $p \equiv 3 \pmod 4$. Then $v_2(\frac{p^s+1}{2}) \geq 1$ when s is odd. In this case we have $2|\gcd(\frac{p^s+1}{2}, p^e-1)$ which is not allowed. So in the case of $p \equiv 3 \pmod 4$, s must be even. Then $\frac{p^s+1}{2}$ is an odd number. It follows from Lemma 2.6 that $\gcd(\frac{p^s+1}{2}, p^e-1) = 1$ if and only if $\frac{e}{\gcd(s,e)}$ is odd which is equivalent to $v_2(e) \leq v_2(s)$ and $v_2(s) \geq 1$, i.e., $v_2(s) \geq \max\{1, v_2(e)\}$ as desired. Part (i) is proved.

(ii). Let $k = 2$. Assume that $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$. Then $D_{p^s+1,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $x^{\frac{p^s-1}{2}}$ is a PP of $\mathbb{F}_{p^e}$. Clearly, $s > 0$ in this case. Suppose $p > 3$, then $x^{\frac{p^s-1}{2}}$ is a PP of $\mathbb{F}_{p^e}$ if and only if

$$\gcd\Big(\frac{p^s-1}{2},p^e-1\Big)=1.$$

This is impossible since $\frac{p-1}{2} | \gcd(\frac{p^s-1}{2}, q-1)$ implies that

$$\gcd\Big(\frac{p^s-1}{2}, q-1\Big) \geq \frac{p-1}{2} > 1.$$

So $p = 3$ and $s > 0$ in what follows. Now Suppose $s > 0$ is even, then it is easy to see that $2 | \gcd(\frac{3^s-1}{2}, 3^e-1)$ which is a contradiction. This means that s must be an odd number and then so is $\frac{3^s-1}{2}$. Thus we have that $x^{\frac{3^s-1}{2}}$ is a PP of $\mathbb{F}_{3^e}$ if and only if

$$\gcd\Big(\frac{3^s-1}{2}, 3^e-1\Big) = \frac{1}{2}\gcd(3^s-1, 3^e-1) = \frac{1}{2}(3^{\gcd(s,e)}-1) = 1,$$

which is equivalent to that s is odd and $\gcd(s, e) = 1$. So Part (ii) is proved.

(iii). $k \neq 0$ and $k \neq 2$. Then the desired result follows from Lemma 2.2 that $(2-k)x^{\frac{p^s+1}{2}} + kx^{\frac{p^s-1}{2}}$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$. Part (iii) is proved. □

Theorem 3.3. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s be a nonnegative integer and s_0 be the least nonnegative residue of s modulo $2e$. Then each of following is true.*

(i). *If $k = 0, p = 3$, then $D_{p^s+2,k}(1, x)$ is not a PP of $\mathbb{F}_{3^e}$.*

(ii). *If $k = 0, p > 3, s_0 = 0$, then $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$.*

(iii). *If $k = 0, p > 3, s = e$, then $D_{p^e+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $q = p^e \equiv 1 \pmod 3$.*

(iv). *If $k = 2$, then $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$.*

(v). *Let $k = 4, p = 3$. If $s = 0$ or $s_0 = 1$, then the binomial $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_{3^e}$. If $s > 0$ and s_0 is even, then $D_{p^s+2,k}(1, x)$ is not a PP of $\mathbb{F}_{3^e}$.*

(vi). *Let $k = 4, p > 3$. Then $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $s = 0$.*

(vii). *If $k \neq 0, 2, 4$ and $p \nmid (4-k)$, then $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$ and $k \neq 3$.*

Proof. By Theorem 3.1, we have that $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$(4-k)x^{\frac{p^s+1}{2}} + kx^{\frac{p^s-1}{2}} + (2-k)x$$

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

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

$$f_1(x) := x^{\frac{p^s+1}{2}} + \frac{1}{2}x.$$

It is easy to see that $f_1(x)$ is not a PP of $\mathbb{F}_{3^e}$ since $f_1(0) = f_1(1) = 0$. So in this case $D_{p^s+2,k}(1, x)$ is not a PP of $\mathbb{F}_{3^e}$.

(ii). Let $k = 0, p > 3, s_0 = 0$. Then $\frac{p^s+1}{2} \equiv 1 \pmod{p^e-1}$ which implies that

$$f_1(x) \equiv \frac{3}{2}x \pmod{x^{p^e} - x}$$

for any $x \in \mathbb{F}_q^*$. Note that $f_1(0) = \frac{3}{2} \times 0 = 0$ and the monomial $\frac{3}{2}x$ is a PP of $\mathbb{F}_q$. So $f_1(x)$ is a PP of $\mathbb{F}_q$. That is to say $D_{p^s+2,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.

(iii). Let $k = 0, p > 3, s = e$. Then by Theorem 7.11 in [5] we have $f_1(x)$ is a PP of $\mathbb{F}_q$ if and only if $\eta((\frac{1}{2})^2 - 1) = 1$, i.e., $\eta(-3) = 1$, where $\eta(\cdot)$ denotes the quadratic character of $\mathbb{F}_q$. One can also find that $\eta(-3) = 1$ if and only if $q = p^e \equiv 1 \pmod 3$, as desired.

(iv). If $k = 2$, then the desired result follows from Lemma 2.2 that the binomial $2x^{\frac{p^s+1}{2}} + 2x^{\frac{p^s-1}{2}}$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$. So $D_{p^s+2,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ if and only if $s = 0$.

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

$$f_2(x) := x^{\frac{p^s-1}{2}} + \frac{1}{2}x.$$

Obviously $f_2(x) = x^{\frac{3^s-1}{2}} + x = 1 + x$ is a PP of $\mathbb{F}_{3^e}$ when $s = 0$. Now let $0 < s \equiv s_0 \pmod{2e}$ with $0 \le s_0 \le 2e - 1$. Then $\frac{p^s-1}{2} \equiv \frac{p^{s_0}-1}{2} \pmod{p^e - 1}$. Therefore

$$f_2(x) \equiv x^{\frac{3^{s_0}-1}{2}} + x \pmod{x^{3^e} - x}$$

for any $x \in \mathbb{F}_q^*$. If $s_0 = 1$, $f_2(x) \equiv 2x \pmod{x^{3^e} - x}$ and $f_2(0) = 2 \times 0 = 0$. This means that $f_2(x) = 2x$ for any $x \in \mathbb{F}_q$. So $f_2(x)$ is a PP of $\mathbb{F}_q$ when $s_0 = 1$. If $s > 0$ and s_0 is even, then $x^{\frac{3^{s_0}-1}{2}} + x = 1 + x$ for any $x \in \mathbb{F}_3^*$. Note that $f_2(\mathbb{F}_3) \subseteq \mathbb{F}_3$ and $f_2(0) = f_2(-1) = 0$, which tells us that $f_2(x)$ is not a PP of $\mathbb{F}_3$. Thus the desired results follows. Unfortunately, following the similar way, we cannot say anything for the case of $s > 0$ and s_0 being odd with $s_0 \ge 3$.

(vi). Let $k = 4, p > 3$. Then $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $2x^{\frac{p^s-1}{2}} - x$ is a PP of $\mathbb{F}_q$. It then follows from Lemma 2.8 that $D_{p^s+2,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $s = 0$, as required.

(vii). Let $p \ge 3$, $k \ne 0, 2, 4$ and $p \nmid (k - 4)$. Denote

$$f_3(x) := (4 - k)x^{\frac{p^s+1}{2}} + kx^{\frac{p^s-1}{2}} + (2 - k)x.$$

First, if $s = 0$, then $f_3(x) = (6 - 2k)x + k$ which is a PP of $\mathbb{F}_{p^e}$ if and only if $k \ne 3$. In what follows we will show that $f_3(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $s > 0$. Let $0 < s \equiv s_0 \pmod{2e}$ with $0 \le s_0 \le 2e - 1$. Then

$$f_3(x) \equiv (4 - k)x^{\frac{p^{s_0}+1}{2}} + kx^{\frac{p^{s_0}-1}{2}} + (2 - k)x \pmod{x^{p^e} - x}. \tag{3.7}$$

We consider the following cases.

Case 1. $s > 0, s_0 = 0$. By (3.7) we have $f_3(x) \equiv (6 - 2k)x + k \pmod{x^{p^e} - x}$, which means that $f_3(x) = (6 - 2k)x + k$ for any $x \in \mathbb{F}_{p^e}^*$. If $k = 3$, then $\forall x \in \mathbb{F}_{p^e}^*$ $f_3(x) = k$. Obviously, $f_3(x)$ is not a PP of $\mathbb{F}_{p^e}$. If $k \ne 3$, then $f_3(x) = 0$ has one nonzero root $\frac{k}{2k-6} \in \mathbb{F}_{p^e}^*$ since $k \ne 0$. But $f_3(0) = 0$. So $f_3(x)$ is not a PP of $\mathbb{F}_{p^e}$ in this case.

Case 2. $s > 0$ and s_0 is a positive even number. Then $x^{\frac{p^{s_0}+1}{2}} = x$ and $x^{\frac{p^{s_0}-1}{2}} = 1$ for each $x \in \mathbb{F}_p^*$, which together with (3.7) imply that $f_3(x) = (6 - 2k)x + k$ for any $x \in \mathbb{F}_p^*$. If $k = 3$, then $\forall x \in \mathbb{F}_p^*$, $f_3(x) = k$. Obviously, $f_3(x)$ is not a PP of $\mathbb{F}_p$. If $k \ne 3$, then $f_3(x) = 0$ has one nonzero root $\frac{k}{2k-6} \in \mathbb{F}_p^*$ since $k \ne 0$. But $f_3(0) = 0$. Therefore $f_3(x)$ is not a PP of $\mathbb{F}_p$ in this case. So is $f_3(x)$ of $\mathbb{F}_{p^e}$ since $f_3(\mathbb{F}_p) \subseteq \mathbb{F}_p$.

Case 3. $s > 0$ and s_0 is odd. Then $x^{\frac{p^{s_0}+1}{2}} = x^{\frac{p+1}{2}}$ and $x^{\frac{p^{s_0}-1}{2}} = x^{\frac{p-1}{2}}$ for each $x \in \mathbb{F}_p^*$, which together with (3.7) imply that $f_3(x) = (4 - k)x^{\frac{p+1}{2}} + kx^{\frac{p-1}{2}} + (2 - k)x$ for any $x \in \mathbb{F}_p^*$. If $p = 3$, then k must equal 1 since $0 \le k < p$ and $k \ne 0, 2, 4$, which contradicts to the condition $p \nmid (4 - k)$. So one has $p > 3$. Then

$$[f_3(x)]^2 \equiv k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p - 1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_3(x)$ is not a PP of $\mathbb{F}_p$. Also note that $f_3(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_3(x)$ is not a PP of $\mathbb{F}_{p^e}$.

Combining the above cases, we verify that $f_3(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $s > 0$. Thus Part (vii) is proved. So the proof of Theorem 3.3 is complete. □

Theorem 3.4. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s be a nonnegative integer and s_0 be the least nonnegative residue of s modulo $2e$. Then each of following is true.*

(i). *If $k = 0, p = 3$, then $D_{3^s+3,0}(1, x)$ is a PP of $\mathbb{F}_{3^e}$ if and only if $v_2(s-1) \geq \max\{1, v_2(e)\}$.*

(ii). *Let $k = 0, p > 3$. If s_0 is an even number, then $D_{p^s+3,0}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.*

(iii). *If $k = 2, s = 0$, then $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$*

(iv). *Let $k = 2, s > 0, p = 3$. If $s_0 = 1$, then $D_{3^s+3,2}(1, x)$ is a PP of $\mathbb{F}_{3^e}$. If s_0 is even, then $D_{3^s+3,2}(1, x)$ is not a PP of $\mathbb{F}_{3^e}$.*

(v). *Let $k = 2, p > 3$. Then $D_{p^s+3,2}(1, x)$ is a PP of $\mathbb{F}_{p^e}$ if and if $s = 0$.*

(vi). *If $k = 3$, then $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $p = 3$ and $v_2(s-1) \geq \max\{1, v_2(e)\}$.*

(vii). *If $k \neq 0, 2, 3$, then $D_{p^s+3,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$.*

Proof. By Theorem 3.1, we have that $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$(2-k)x^{\frac{p^s+3}{2}} + 6x^{\frac{p^s+1}{2}} + kx^{\frac{p^s-1}{2}} + (6-2k)x \tag{3.8}$$

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

(i). Letting $k = 0$, we have $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if (3.8) is a PP of $\mathbb{F}_q$, i.e., the trinomial $x^{\frac{p^s+3}{2}} + 3x^{\frac{p^s+1}{2}} + 3x$ is a PP of $\mathbb{F}_q$. Let

$$f_4(x) := x^{\frac{p^s+3}{2}} + 3x^{\frac{p^s+1}{2}} + 3x.$$

Now let $p = 3$. Then $f_4(x)$ is a PP of $\mathbb{F}_q$ if and only if $x^{\frac{3^s+3}{2}}$ is a PP of $\mathbb{F}_q$. The latter is equivalent to $\gcd(\frac{3^s+3}{2}, 3^e-1) = 1$. Now we let $\gcd(\frac{3^s+3}{2}, 3^e-1) = 1$. If s is even, then one has $v_2(\frac{3^s+3}{2}) \geq 1$. It follows that $2|\gcd(\frac{3^s+3}{2}, 3^e-1)$, which is a contradiction. So s must be odd. Then $\frac{3^s+3}{2}$ is an odd integer. It follows from Lemma 2.6 that $\gcd(\frac{3^s+3}{2}, 3^e-1) = \gcd(\frac{3^{s-1}+1}{2}, \frac{3^e-1}{2}) = \frac{1}{2}\gcd(3^{s-1}+1, 3^e-1) = 1$ if and only if $\frac{e}{\gcd(s-1,e)}$ is odd. This means that $\gcd(\frac{3^s+3}{2}, 3^e-1) = 1$ if and only if $v_2(e) \leq v_2(s-1)$ and $v_2(s-1) \geq 1$, namely, $v_2(s-1) \geq \max\{1, v_2(e)\}$, as desired.

(ii). Let $k = 0, p > 3$. Then $\frac{p^s+3}{2} \equiv \frac{p^{s_0}+3}{2} \pmod{p^e-1}$ and $\frac{p^s+1}{2} \equiv \frac{p^{s_0}+1}{2} \pmod{p^e-1}$. So

$$f_4(x) \equiv x^{\frac{p^{s_0}+3}{2}} + 3x^{\frac{p^{s_0}+1}{2}} + 3x \pmod{x^{p^e} - x}. \tag{3.9}$$

Clearly, if s_0 is even, then $x^{\frac{p^{s_0}+3}{2}} = x^2$ and $x^{\frac{p^{s_0}+1}{2}} = x$ for any $x \in \mathbb{F}_p^*$. Then by (3.9) we have $f_4(x) = x^2 + 6x = x(x+6)$ for any $x \in \mathbb{F}_p^*$. Hence $f_4(x) = 0$ has one nonzero root -6 in $\mathbb{F}_p^*$. But $f_4(0) = 0$. It then follows that $f_4(x)$ is not a PP of $\mathbb{F}_p$. One notes that $f_4(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_4(x)$ is not a PP of $\mathbb{F}_{p^e}$. It follows that $D_{p^s+3,k}(1, x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even.

(iii). Letting $k = 2$, we have $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if (3.8) is a PP of $\mathbb{F}_q$, i.e. , $3x^{\frac{p^s+1}{2}} + x^{\frac{p^s-1}{2}} + x$ is a PP of $\mathbb{F}_q$. Let

$$f_5(x) := 3x^{\frac{p^s+1}{2}} + x^{\frac{p^s-1}{2}} + x.$$

Let $s = 0$. Then $f_5 = 4x + 1$, which clearly is a PP of $\mathbb{F}_q$. So $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$.

(iv). Let $k = 2, p = 3, s > 0$. Then the desired result follows from the proof of Part (v) of Theorem 3.3.

(v). Let $k = 2, p > 3$. By Part (iii) we only need to show that $D_{p^s+3,k}(1, x)$ is not a PP of $\mathbb{F}_q$ when $s > 0$. Let $0 < s \equiv s_0 \pmod{2e}$ with $0 \le s_0 \le 2e - 1$. Then one has

$$f_5(x) \equiv 3x^{\frac{p^s+1}{2}} + x^{\frac{p^s-1}{2}} + x \pmod{x^{p^e} - x}.$$

If s_0 is even, then $f_5(x) = 4x + 1$ for any $x \in \mathbb{F}_p^*$. In this situation, $f_5(x) = 0$ has one nonzero root $-\frac{1}{4} \in \mathbb{F}_p^*$. So $f_5(x)$ is not a PP of $\mathbb{F}_p$ since $f_5(0) = 0$. Also note that $f_5(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Thus $f_5(x)$ is not a PP of $\mathbb{F}_{p^e}$ in this case. If s_0 is odd, then $f_5(x) = 3x^{\frac{p+1}{2}} + x^{\frac{p-1}{2}} + x$ for any $x \in \mathbb{F}_p^*$. So in $\mathbb{F}_p^*$, we have

$$(f_5(x))^2 \equiv x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_5(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_5(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_5(x)$ is not a PP of $\mathbb{F}_{p^e}$. It infers that $D_{p^s+3,k}(1, x)$ is not a PP of $\mathbb{F}_q$ when $s > 0$. Part (v) is proved.

(vi). Let $k = 3$. Then $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if (3.8) is a PP of $\mathbb{F}_q$, i.e., the trinomial

$$f_6(x) := -x^{\frac{p^s+3}{2}} + 6x^{\frac{p^s+1}{2}} + 3x^{\frac{p^s-1}{2}}$$

is a PP of $\mathbb{F}_q$. By the result of Part (i), we then have from the fact $D_{3^s+3,3}(1, x) = D_{3^s+3,0}(1, x)$ that $f_6(x)$ is a PP of of $\mathbb{F}_{3^e}$ if and only if $v_2(s - 1) \ge \max\{1, v_2(e)\}$. Then we only need to show that $f_6(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p > 3$. Let $s \equiv s_0 \pmod{2e}$ with $0 \le s_0 \le 2e - 1$. Then one has

$$f_6(x) \equiv -x^{\frac{p^{s_0}+3}{2}} + 6x^{\frac{p^{s_0}+1}{2}} + 3x^{\frac{p^{s_0}-1}{2}} \pmod{x^{p^e} - x}.$$

If s_0 is even, then $f_6(x) = -x^2 + 6x + 3$ for any $x \in \mathbb{F}_p^*$. Then $f_6(x)$ is not a PP of $\mathbb{F}_p$ since $f_6(2) = f_6(4) = 11$. Also note that $f_6(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Thus $f_6(x)$ is not a PP of $\mathbb{F}_{p^e}$ for $p > 3$ and s_0 being even. If s_0 is odd, then $f_6(x) = -x^{\frac{p+3}{2}} + 6x^{\frac{p+1}{2}} + 3x^{\frac{p-1}{2}}$ for any $x \in \mathbb{F}_p^*$. So in $\mathbb{F}_p^*$, we have

$$(f_6(x))^2 \equiv 9x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_6(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_6(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_6(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p > 3$ and s_0 is odd. So $f_6(x)$ is a PP of $\mathbb{F}_q$ if and only if $p = 3$ and $v_2(s - 1) \ge \max\{1, v_2(e)\}$, that is, $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $p = 3$ and $v_2(s - 1) \ge \max\{1, v_2(e)\}$. Part (vi) is proved.

(iv). Let $k \ne 0, 2, 3$ and $0 \le k < p$. Then $D_{p^s+3,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if (3.8) is a PP of $\mathbb{F}_q$, i.e., if and only if

$$f_7(x) := (2 - k)x^{\frac{p^s+3}{2}} + 6x^{\frac{p^s+1}{2}} + kx^{\frac{p^s-1}{2}} + (6 - 2k)x$$

is a PP of $\mathbb{F}_q$. Let $s \equiv s_0 \pmod{2e}$ with $0 \le s_0 \le 2e - 1$. Then one has

$$f_7(x) \equiv (2 - k)x^{\frac{p^{s_0}+3}{2}} + 6x^{\frac{p^{s_0}+1}{2}} + kx^{\frac{p^{s_0}-1}{2}} + (6 - 2k)x \pmod{x^{p^e} - x}.$$

If s_0 is even, then $f_7(x) = (2-k)x^2 + (12-2k)x + k$ for any $x \in \mathbb{F}_p^*$. One then finds that $f_7(\frac{4}{k-2}) = f_7(\frac{8-2k}{k-2})$ and $\frac{4}{k-2} \ne \frac{8-2k}{k-2}$ when $k \ne 4$. If $k = 4$, then $p \ge 5$. In this case, $f_7(x) = -2x^2 + 4x + 4$ for any $x \in \mathbb{F}_p^*$, which implies $f_7(-1) = f_7(3)$ when $k = 4$. Therefore $f_7(x)$ is not a PP of $\mathbb{F}_p$. Also note that $f_7(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Thus $f_7(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is even. If s_0 is odd, then

$$f_7(x) = (2-k)x^{\frac{p+3}{2}} + 6x^{\frac{p+1}{2}} + kx^{\frac{p-1}{2}} + (6-2k)x \tag{3.10}$$

for any $x \in \mathbb{F}_p^*$. We consider the following two cases.
Case 1. Let $p = 3$. Then $k = 1$ since $k < p$ and $k \neq 0, 2$. Hence $\forall x \in \mathbb{F}_3^*$, $f_7(x) = x^3 + 2x$. It then follows from $f_7(0) = f_7(1) = 0$ that $f_7(x)$ is not a PP of $\mathbb{F}_3$. We note that $f_7(\mathbb{F}_3) \subseteq \mathbb{F}_3$. Therefore $f_7(x)$ is not a PP of $\mathbb{F}_{3^e}$.
Case 2. Let $p > 3$. By (3.10), in $\mathbb{F}_p$ we have

$$(f_7(x))^2 \equiv k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_7(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_7(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_7(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p > 3$ and s_0 is odd.

Hence $f_7(x)$ is not a PP of $\mathbb{F}_{p^e}$ when $k \neq 0, 2, 3$, from which we deduce immediately that $D_{p^s+3,k}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ when $k \neq 0, 2, 3$. Part (vii) is proved. So we completes the proof of Theorem 3.4. □

Theorem 3.5. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s be a nonnegative integer and s_0 be the least nonnegative residue of s modulo $2e$. If $D_{p^s+4,k}(1, x)$ is a PP of $\mathbb{F}_q$, then either $k = 0$ and s_0 is odd, or $k > 0, k \neq 2$ and $s = 0$.*

Proof. It is sufficient to show that $D_{p^s+4,k}(1, x)$ is not a PP of $\mathbb{F}_q$ when $k = 0$, s_0 is even, or $k > 0, s > 0$. By Theorem 3.1, we get

$$\begin{aligned}32D_{p^s+4,k}(1, x) = {} & k(1-4x)^{\frac{p^s-1}{2}} + (8+2k)(1-4x)^{\frac{p^s+1}{2}} \\ & + (8-3k)(1-4x)^{\frac{p^s+3}{2}} + 2 + 3k + (12-2k)(1-4x) + (2-k)(1-4x)^2.\end{aligned}$$

Then $D_{p^s+4,k}(1, x)$ is a PP of $\mathbb{F}_q$ if and only if $kx^{\frac{p^s-1}{2}} + (8+2k)x^{\frac{p^s+1}{2}} + (8-3k)x^{\frac{p^s+3}{2}} + (12-2k)x + (2-k)x^2$ is a PP of $\mathbb{F}_q$. Let

$$f_8(x) := kx^{\frac{p^s-1}{2}} + (8+2k)x^{\frac{p^s+1}{2}} + (8-3k)x^{\frac{p^s+3}{2}} + (12-2k)x + (2-k)x^2.$$

Now we show that $f_8(x)$ is not a PP of $\mathbb{F}_q$ when $k = 0$, s_0 is even, or $k > 0, s > 0$. Then the following cases are considered.

Case 1. $k = 0$ and s_0 is an even. Then $f_8(x) = 4x^{\frac{p^{s_0}+1}{2}} + 4x^{\frac{p^{s_0}+3}{2}} + 6x + x^2$. It infers that

$$f_8(x) \equiv 4x^{\frac{p^{s_0}+1}{2}} + 4x^{\frac{p^{s_0}+3}{2}} + 6x + x^2 \pmod{x^q - x}.$$

Additionally, $\forall x \in \mathbb{F}_p^*$, $x^{\frac{p^{s_0}+1}{2}} = x$ and $x^{\frac{p^{s_0}+3}{2}} = x^2$ since s_0 is an even. Therefore

$$f_8(x) = 5x(x+2)$$

for any $x \in \mathbb{F}_p^*$. Then $f_8(0) = f_8(-2) = 0$. So $f_8(x)$ is not a PP of $\mathbb{F}_p$. Also $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ since $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$.

Case 2. $k = 2$. Then
$$f_8(x) = 2x^{\frac{p^s-1}{2}} + 12x^{\frac{p^s+1}{2}} + 2x^{\frac{p^s+3}{2}} + 8x.$$

subcase 2-1. $p = 3$. Then $f_8(x) = 2x^{\frac{p^s-1}{2}} + 2x^{\frac{p^s+3}{2}} + 2x$. So $f_8(x) = 2x^2 + 2x + 2$ when $s = 0$, which then follows that $f_8(0) = f_8(2) = 2$. If $s > 0$, we have easily that $f_8(0) = f_8(1) = 0$. Thus $f_8(x)$ is not a PP of $\mathbb{F}_{3^e}$ whenever.

subcase 2-2. $p > 3$. Then

$$f_8(x) \equiv 2x^{\frac{p^{s_0}-1}{2}} + 12x^{\frac{p^{s_0}+1}{2}} + 2x^{\frac{p^{s_0}+3}{2}} + 8x \pmod{x^{p^e} - x}.$$

If s_0 is even, then $f_8(x) = 2x^2 + 20x + 2$ for any $x \in \mathbb{F}_p^*$. This implies that $f_8(-4) = f_8(-6)$, which then follows that $f_8(x)$ is not a PP of $\mathbb{F}_p$. Note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_8(x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even. If s_0 is odd, then $f_8(x) = 2x^{\frac{p-1}{2}} + 12x^{\frac{p+1}{2}} + 2x^{\frac{p+3}{2}} + 8x$ for any $x \in \mathbb{F}_p^*$. We then deduces that

$$(f_8(x))^2 \equiv 4x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_8(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is odd.

Thus $D_{p^s+4,2}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ for any nonnegative integer s and odd prime p.

Case 3. $k = 6, s > 0$. Then $p \geq 7$ and

$$f_8(x) = 6x^{\frac{p^s-1}{2}} + 20x^{\frac{p^s+1}{2}} - 10x^{\frac{p^s+3}{2}} - 4x^2.$$

If $s > 0$ and s_0 is even, then $f_8(x) = -14x^2+20x+6$ for any $x \in \mathbb{F}_p^*$. This implies that $f_8(0) = f_8(-1) = 0$ if $p = 7$, or $f_8(\frac{4}{7}) = f_8(\frac{6}{7})$ if $p > 7$. This means that $f_8(x)$ is not a PP of $\mathbb{F}_p$. Note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_8(x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even. If $s > 0$ and s_0 is odd, then $f_8(x) = 6x^{\frac{p-1}{2}} + 20x^{\frac{p+1}{2}} - 10x^{\frac{p+3}{2}} - 4x^2$ for any $x \in \mathbb{F}_p^*$, which implies that

$$(f_8(x))^2 \equiv 36x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_8(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is odd.

Thus $D_{p^s+4,6}(1, x)$ is not a PP of $\mathbb{F}_{p^e}$ when $s > 0$.

Case 4. $k = p - 4, s > 0$. Then $p \geq 5$ and

$$f_8(x) = (p-4)x^{\frac{p^s-1}{2}} + (20-3p)x^{\frac{p^s+3}{2}} + (20-2p)x + (6-p)x^2.$$

If $s > 0, s_0$ is even, then $f_8(x) = 26x^2 + 20x - 4$ for any $x \in \mathbb{F}_p^*$. This implies that $f_8(0) = f_8(\frac{1}{5}) = 0$ if $p = 13$, or $f_8(\frac{-4}{13}) = f_8(\frac{-6}{13})$ if $p \neq 13$. This means that $f_8(x)$ is not a PP of $\mathbb{F}_p$. Note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_8(x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even. If $s > 0, s_0$ is odd, then $f_8(x) = -4x^{\frac{p-1}{2}} + 20x^{\frac{p+3}{2}} + 20x + 6x^2$ for any $x \in \mathbb{F}_p^*$, which implies that

$$(f_8(x))^2 \equiv 16x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

Then by Lemma 2.7, we know that $f_8(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is odd.

Thus $D_{p^s+4,p-4}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$ when $s>0$.

Case 5. $p \mid (3k-8)$, $s>0$. Then $p \geq 5$, $p \nmid (2-k)$ and

$$f_8(x) = kx^{\frac{p^s-1}{2}} + (8+2k)x^{\frac{p^s+1}{2}} + (12-2k)x + (2-k)x^2.$$

If $s>0$, s_0 is even, then $f_8(x) = (2-k)x^2+20x+k$ for any $x \in \mathbb{F}_p^*$. This implies that $f_8(\frac{-11}{2-k}) = f_8(\frac{-9}{2-k}) = 0$. This means that $f_8(x)$ is not a PP of $\mathbb{F}_p$. Note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_8(x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even. If $s>0$, s_0 is odd, then $f_8(x) = kx^{\frac{p-1}{2}} + (8+2k)x^{\frac{p+1}{2}} + (12-2k)x + (2-k)x^2$ for any $x \in \mathbb{F}_p^*$, which implies that

$$(f_8(x))^2 \equiv k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p-x}.$$

Then by Lemma 2.7, we know that $f_8(x)$ is not a PP of $\mathbb{F}_p$. We note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is odd.

Thus $D_{p^s+4,k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$ when $p \mid (3k-8)$ and $s>0$.

Case 6. $k \neq 0,2,6,p-4$, $s>0$ and $p \nmid (3k-8)$. Then

$$f_8(x) = kx^{\frac{p^s-1}{2}} + (8+2k)x^{\frac{p^s+1}{2}} + (8-3k)x^{\frac{p^s+3}{2}} + (12-2k)x + (2-k)x^2.$$

If $s>0$, s_0 is even, then $f_8(x) = (10-4k)x^2+20x+k$ for any $x \in \mathbb{F}_p^*$. If $p \mid (2k-5)$, then $p \neq 5$ and $f_8(x) = 20x+k, \forall x \in \mathbb{F}_p^*$. It implies that $f_8(0) = f_8(\frac{-k}{20}) = 0$. So $f_8(x)$ is not a PP of $\mathbb{F}_p$ when $p \mid (2k-5)$. If $p \nmid (2k-5)$, then $f_8(\frac{4}{2k-5}) = f_8(\frac{6}{2k-5})$, which means that $f_8(x)$ is not a PP of $\mathbb{F}_p$ when $p \nmid (2k-5)$. Thus $f_8(x)$ is not a PP of $\mathbb{F}_p$ when $s>0$, s_0 is even. Note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $f_8(x)$ is not a PP of $\mathbb{F}_q$ when s_0 is even. If $s>0$, s_0 is odd, then $f_8(x) = kx^{\frac{p-1}{2}} + (8+2k)x^{\frac{p+1}{2}} + (8-3k)x^{\frac{p+3}{2}} + (12-2k)x + (2-k)x^2$ for any $x \in \mathbb{F}_p^*$. If $p=3$, then $k=1$. In this case $f_8(x) = 2x+2x^2+2x^3$, which implies that $f_8(0) = f_8(1) = 0$. It then follows that $f_8(x)$ is not a PP of $\mathbb{F}_3$. If $p>3$, then

$$(f_8(x))^2 \equiv k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p-x}.$$

Then by Lemma 2.7, we know that $f_8(x)$ is not a PP of $\mathbb{F}_p$. Thus $f_8(x)$ is not a PP of $\mathbb{F}_p$ when s_0 is odd. We note that $f_8(\mathbb{F}_p) \subseteq \mathbb{F}_p$. Therefore $f_8(x)$ is not a PP of $\mathbb{F}_{p^e}$ when s_0 is odd.

Thus $D_{p^s+4,k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$ when $k \neq 0,2,6,p-4$, $s>0$ and $p \nmid (3k-8)$. Combining all of the above cases, we have the desired result. Therefore Theorem 3.5 is proved. □

Corollary 3.6. *Let $q=p^e$ with p being an odd prime and e being a positive integer. Let s and k be nonnegative integers with $0<k<p$. Then $D_{p^s+4,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $s=0$ and $p \mid (2k-5)$.*

Proof. The desired result follows immediately from the proof of Theorem 3.5. □

4. Reversed Dickson polynomials $D_{p^s+p^t+\ell,k}(1,x)$

In this section, we present an explicit formula for $D_{n,k}(1,x)$ when $n = p^s+p^t+\ell$ with $\leq s<t$ and $0 \leq \ell < p$. Then we characterize $D_{n,k}(1,x)$ to be a PP of $\mathbb{F}_q$ in this case.

Theorem 4.1. *Let $p = \mathrm{char}(\mathbb{F}_q)$ be an odd prime. Let s and t be integers such that $0 \leq s < t$. Then*

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

Proof. We consider the following two cases.

Case 1. $x \neq \frac{1}{4}$. For this case, putting $x = y(1-y)$ in the second identity of Lemma 2.3 gives us that

$$\begin{aligned} D_{p^s+p^t,k}(1,x) =& D_{p^s+p^t,k}(1,y(1-y)) \\ =& \frac{(k-1-(k-2)y)y^{p^s+p^t} - (1+(k-2)y)(1-y)^{p^s+p^t}}{2y-1} \\ =& \frac{\frac{k+(2-k)u}{2}(\frac{u+1}{2})^{p^s+p^t} - \frac{k+(k-2)u}{2}(\frac{1-u}{2})^{p^s+p^t}}{u} \\ =& \frac{k}{4}(u^{p^s-1} + u^{p^t-1}) - \frac{k-2}{4}(1+u^{p^s+p^t}) \\ =& \frac{k}{4}((u^2)^{\frac{p^s-1}{2}} + (u^2)^{\frac{p^t-1}{2}}) - \frac{k-2}{4}(1+(u^2)^{\frac{p^s+p^t}{2}}), \end{aligned}$$

where $u = 2y-1$ and $u^2 = 1-4x$. So we obtain that

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

as desired.

Case 2. $x = \frac{1}{4}$. By the first identity of Lemma 2.3, one has

$$D_{p^s+p^t,k}(1,\frac{1}{4}) = \frac{k(p^s+p^t)-k+2}{2^{p^s+p^t}} = \frac{-k+2}{4}.$$

Besides,

$$\frac{k}{4}((1-4\times\frac{1}{4})^{\frac{p^s-1}{2}} + (1-4\times\frac{1}{4})^{\frac{p^t-1}{2}}) - \frac{k-2}{4}(1+(1-4\times\frac{1}{4})^{\frac{p^s+p^t}{2}}) = \frac{-k+2}{4}.$$

Thus the required result follows. So Theorem 4.1 is proved. □

Theorem 4.2. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s and t be positive integers with $s < t$. Then each of following is true.*

(i). *If $k = 0$, then $D_{p^s+p^t,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if either $p \equiv 1 \pmod 4$ and $v_2(t-s) \geq v_2(e)$, or $p \equiv 3 \pmod 4$ and $v_2(t-s) \geq \max\{v_2(e), 1\}$.*

(ii). *Let $k = 2$. If $p > 3$, then $D_{p^s+p^t,k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$. If $p = 3$ and st is even, then $D_{p^s+p^t,k}(1,x)$ is not a PP of $\mathbb{F}_{p^e}$.*

(iii). *If $k \neq 0, 2$, then $D_{p^s+p^t,k}(1,x)$ is not a PP of $\mathbb{F}_q$.*

Proof. By Theorem 4.1, we have that $D_{p^s+p^t,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if

$$k(x^{\frac{p^s-1}{2}} + x^{\frac{p^t-1}{2}}) - (k-2)x^{\frac{p^s+p^t}{2}}$$

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

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

$$\gcd\Big(\frac{p^s+p^t}{2}, p^e-1\Big) = 1.$$

Additionally, $\gcd\left(\frac{p^s+p^t}{2}, p^e-1\right) = \gcd\left(\frac{p^{t-s}+1}{2}, p^e-1\right)$. Then the desired result follows from the same way as proving Part (i) of Theorem 3.2.

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

$$g_1(x) := x^{\frac{p^s-1}{2}} + x^{\frac{p^t-1}{2}}.$$

So

$$g_1(x) \equiv x^{\frac{p^{s_0}-1}{2}} + x^{\frac{p^{t_0}-1}{2}} \pmod{x^{p^e}-x}.$$

Then the following cases are considered.

Case 1. $s>0$ and both s_0 and t_0 are even. Then $g_1(x)=2$ for any $x\in\mathbb{F}_p^*$. So $g_1(x)$ is not a PP of $\mathbb{F}_p$. One also notices that $g_1(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Thus $g_1(x)$ is not a PP of $\mathbb{F}_q$.

Case 2. $s>0$ and one of s_0 and t_0 is even, the other is odd. Then $g_1(x)=x^{\frac{p-1}{2}}+1$ for any $x\in\mathbb{F}_p^*$. If $p=3$, then $\forall x\in\mathbb{F}_p^*$, $g_1(x)=x+1$, which implies $g_1(0)=g_1(-1)=0$. So $g_1(x)$ is not a PP of $\mathbb{F}_3$. If $p>3$, then

$$(g_1(x))^2 \equiv x^{p-1} + 2x^{\frac{p-1}{2}} + 1 \pmod{x^p-x}.$$

It follows from Lemma 2.7 that $g_1(x)$ is not a PP of $\mathbb{F}_p$ when $p>3$. Therefore $g_1(x)$ is not a PP of $\mathbb{F}_p$. Obviously, $g_1(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Hence $g_1(x)$ is not a PP of $\mathbb{F}_q$ in this case.

Case 3. $s>0, p>3$ and both s_0 and t_0 are odd. Then $g_1(x)=2x^{\frac{p-1}{2}}$ for any $x\in\mathbb{F}_p$. But $\gcd(\frac{p-1}{2}, p-1)=\frac{p-1}{2}>1$. Therefore $g_1(x)$ is not a PP of $\mathbb{F}_p$. Note that $g_1(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Hence $g_1(x)$ is not a PP of $\mathbb{F}_q$ in this case.

Combining the above cases, we know that part (ii) is true.

(iii). Let $k\neq 0$ and $k\neq 2$. Let

$$g_2(x) := k(x^{\frac{p^s-1}{2}} + x^{\frac{p^t-1}{2}}) - (k-2)x^{\frac{p^s+p^t}{2}}.$$

Then

$$g_2(x) \equiv k(x^{\frac{p^{s_0}-1}{2}} + x^{\frac{p^{t_0}-1}{2}}) - (k-2)x^{\frac{p^{s_0}+p^{t_0}}{2}} \pmod{x^q-x}.$$

Then we divide the proof into the following three cases.

Case 1. Both s_0 and t_0 are even. Then $g_2(x)=2k-(k-2)x$ for any $x\in\mathbb{F}_p^*$. So $g_2(x)$ is not a PP of $\mathbb{F}_p$ since $g_2(0)=g_2(\frac{2k}{k-2})$. One also notices that $g_2(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Thus $g_2(x)$ is not a PP of $\mathbb{F}_q$.

Case 2. One of s_0 and t_0 is even, the other is odd. Then $g_2(x)=k+kx^{\frac{p-1}{2}}-(k-2)x^{\frac{p+1}{2}}$ for any $x\in\mathbb{F}_p^*$. If $p=3$, then $k=1$ and so $g_2(0)=g_2(1)=0$, which implies $g_2(x)$ is not a PP of $\mathbb{F}_3$. If $p>3$, then

$$(g_2(x))^2 \equiv k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p-x}.$$

It follows from Lemma 2.7 that $g_2(x)$ is not a PP of $\mathbb{F}_p$ when $p>3$. Therefore $g_2(x)$ is not a PP of $\mathbb{F}_p$. Obviously, $g_2(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Hence $g_2(x)$ is not a PP of $\mathbb{F}_q$ in this case.

Case 3. Both s_0 and t_0 are odd. Then $g_2(x)=2kx^{\frac{p-1}{2}}-(k-2)x$ for any $x\in\mathbb{F}_p^*$. If $p=3$, then $k=1$ and so $g_2(x)=0, \forall x\in\mathbb{F}_p$, which implies $g_2(x)$ is not a PP of $\mathbb{F}_3$. If $p>3$, then

$$(g_2(x))^2 \equiv 4k^2x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p-x}.$$

Since $4k^2\in\mathbb{F}_p^*$, it then follows from Lemma 2.7 that $g_2(x)$ is not a PP of $\mathbb{F}_p$ when $p>3$. Therefore $g_2(x)$ is not a PP of $\mathbb{F}_p$. Obviously, $g_2(\mathbb{F}_p)\subseteq\mathbb{F}_p$. Hence $g_2(x)$ is not a PP of $\mathbb{F}_q$ in this case.

Combining the above cases, we deduce that $g_2(x)$ is not a PP of $\mathbb{F}_q$ in the condition of $k\neq 0,2$. Thus $D_{p^s+p^t,k}(1,x)$ is not a PP of $\mathbb{F}_q$. The proof of Theorem 4.2 is completed. □

Theorem 4.3. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s and t be positive integers with $s < t$. Then*

$$\begin{aligned} D_{p^s+p^t+1,k}(1,x) = & \frac{1}{4}(1-4x)^{\frac{p^s+p^t}{2}} + \frac{1}{4} + \frac{1}{8}((1-4x)^{\frac{p^s-1}{2}} + (1-4x)^{\frac{p^t-1}{2}}) \\ & - \frac{k-2}{8}((1-4x)^{\frac{p^s+1}{2}} + (1-4x)^{\frac{p^t+1}{2}}). \end{aligned} \tag{4.1}$$

Furthermore, $D_{p^s+p^t+1,k}(1,x)$ is not a PP of $\mathbb{F}_q$.

Proof. We consider the following two cases.

CASE 1. $x \neq \frac{1}{4}$. For this case, putting $x = y(1-y)$ in the second identity of Lemma 2.3 gives us that

$$\begin{aligned} & D_{p^s+p^t+1,k}(1,x) = D_{p^s+p^t+1,k}(1,y(1-y)) \\ = & \frac{(k-1-(k-2)y)y^{p^s+p^t+1} - (1+(k-2)y)(1-y)^{p^s+p^t+1}}{2y-1} \\ = & \frac{\frac{k+(2-k)u}{2}(\frac{u+1}{2})^{p^s+p^t+1} - \frac{k+(k-2)u}{2}(\frac{1-u}{2})^{p^s+p^t+1}}{u} \\ = & \frac{k}{8}(1+u^{p^s-1}+u^{p^t-1}+u^{p^s+p^t}) - \frac{k-2}{8}(1+u^{p^s+1}+u^{p^t+1}+u^{p^s+p^t}) \\ = & \frac{1}{4}u^{p^s+p^t} + \frac{1}{4} + \frac{k}{8}(u^{p^s-1}+u^{p^t-1}) - \frac{k-2}{8}(u^{p^s+1}+u^{p^t+1}), \end{aligned}$$

where $u = 2y-1$ and $u^2 = 1-4x$. Then we have that

$$\begin{aligned} D_{p^s+p^t+1,k}(1,x) = & \frac{1}{4}(1-4x)^{\frac{p^s+p^t}{2}} + \frac{1}{4} \\ & + \frac{1}{8}((1-4x)^{\frac{p^s-1}{2}} + (1-4x)^{\frac{p^t-1}{2}}) - \frac{k-2}{8}((1-4x)^{\frac{p^s+1}{2}} + (1-4x)^{\frac{p^t+1}{2}}) \end{aligned}$$

as desired.

CASE 2. $x = \frac{1}{4}$. On the one hand, by the first identity of Lemma 2.3, one has

$$D_{p^s+p^t+1,k}(1,\frac{1}{4}) = \frac{k(p^s+p^t+1)-k+2}{2^{p^s+p^t}} = \frac{1}{4}.$$

On the other hand,

$$\frac{1}{4}(1-4\times\frac{1}{4})^{\frac{p^s+p^t}{2}} + \frac{1}{4} + \frac{1}{8}((1-4\times\frac{1}{4})^{\frac{p^s-1}{2}} + (1-4\times\frac{1}{4})^{\frac{p^t-1}{2}}) - \frac{k-2}{8}((1-4\times\frac{1}{4})^{\frac{p^s+1}{2}} + (1-4\times\frac{1}{4})^{\frac{p^t+1}{2}}) = \frac{1}{4}.$$

Combing Case 1 and Case 2, we know that (4.1) always holds. So $D_{p^s+p^t+1,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$g_3(x) := 2x^{\frac{p^s+p^t}{2}} + 2(x^{\frac{p^s-1}{2}} + x^{\frac{p^t-1}{2}}) - (k-2)(x^{\frac{p^s+1}{2}} + x^{\frac{p^t+1}{2}})$$

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

In what follows, we show that $g_3(x)$ is not a PP of $\mathbb{F}_q$. Now let $s \equiv s_0 \pmod{2e}$ and $t \equiv t_0 \pmod{2e}$ with $0 \le s_0 \le 2e-1, 0 \le t_0 \le 2e-1$. Then

$$g_3(x) \equiv 2x^{\frac{p^{s_0}+p^{t_0}}{2}} + 2(x^{\frac{p^{s_0}-1}{2}} + x^{\frac{p^{t_0}-1}{2}}) - (k-2)(x^{\frac{p^{s_0}+1}{2}} + x^{\frac{p^{t_0}+1}{2}}) \pmod{x^q - x}.$$

First we let $k = 2$. In this case we have

$$g_3(x) \equiv 2x^{\frac{p^{s_0}+p^{t_0}}{2}} + 2x^{\frac{p^{s_0}-1}{2}} + 2x^{\frac{p^{t_0}-1}{2}} \pmod{x^q - x}.$$

If both s_0 and t_0 are even, then $\forall x \in \mathbb{F}_p^*$, $g_3(x) = 2x + 4$. It follows that $g_3(x)$ is not a PP of $\mathbb{F}_p$ since $g_3(0) = g_3(-2) = 0$.

If exactly one of s_0 and t_0 is even, then $g_3(x) = 2x^{\frac{p-1}{2}} + 2x^{\frac{p+1}{2}} + 2$ for any $x \in \mathbb{F}_p^*$. In this case if $p = 3$, then $g_3(0) = g_3(1) = 0$, which implies $g_3(x)$ is not a PP of $\mathbb{F}_3$. If $p > 3$, then

$$(g_3(x))^2 \equiv 4x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

It follows from Lemma 2.7 that $g_3(x)$ is not a PP of $\mathbb{F}_p$ when $p > 3$. Therefore $g_3(x)$ is not a PP of $\mathbb{F}_p$.

If both s_0 and t_0 are odd, then $g_3(x) = 2x + 4x^{\frac{p-1}{2}}$ for any $x \in \mathbb{F}_p^*$. If $p = 3$, then $g_3(x) = 0, \forall x \in \mathbb{F}_p^*$, which implies $g_3(x)$ is not a PP of $\mathbb{F}_3$. If $p > 3$, then

$$(g_3(x))^2 \equiv 4x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

It follows from Lemma 2.7 that $g_3(x)$ is not a PP of $\mathbb{F}_p$ when $p > 3$. Therefore $g_3(x)$ is not a PP of $\mathbb{F}_p$.

Combining the above discussions, we derive that $g_3(x)$ is not a PP of $\mathbb{F}_p$. Note that $g_3(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $g_3(x)$ is not a PP of $\mathbb{F}_q$ when $k = 2$.

Now let $k \neq 2$. The following cases are considered.

If both s_0 and t_0 are even, then $\forall x \in \mathbb{F}_p^*$, $g_3(x) = (6-2k)x + 4$. Clearly, if $k = 3$, then $g_3(x)$ is not a PP of $\mathbb{F}_p$. If $k \neq 3$, then $g_3(0) = g_3(\frac{2}{k-3}) = 0$. This implies that $g_3(x)$ is not a PP of $\mathbb{F}_p$.

If exactly one of s_0 and t_0 is even then $g_3(x) = (4-k)x^{\frac{p+1}{2}} + 2x^{\frac{p-1}{2}} - (k-2)x + 2$ for any $x \in \mathbb{F}_p^*$. If $p = 3$, then $k = 0$ or $k = 1$. And $g_3(0) = 0, g_3(1) = k+2, g_3(-1) = 2$. So in this case, either $g_3(1) = g_3(-1) = 2$ if $k = 0$, or $g_3(1) = g_3(0) = 0$ if $k = 1$, which implies $g_3(x)$ is not a PP of $\mathbb{F}_3$. If $p > 3$, then

$$(g_3(x))^2 \equiv 4x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

It follows from Lemma 2.7 that $g_3(x)$ is not a PP of $\mathbb{F}_p$ when $p > 3$. Therefore $g_3(x)$ is not a PP of $\mathbb{F}_p$.

If both s_0 and t_0 are odd then $g_3(x) = 2x^p + 4x^{\frac{p-1}{2}} - 2(k-2)x^{\frac{p+1}{2}}$ for any $x \in \mathbb{F}_p^*$. If $p = 3$, then $g_3(1) = g_3(-1) = k-2$, which implies $g_3(x)$ is not a PP of $\mathbb{F}_3$. If $p > 3$, then

$$(g_3(x))^2 \equiv 16x^{p-1} + \text{the terms of } x \text{ with the degree less than } p-1 \pmod{x^p - x}.$$

It follows from Lemma 2.7 that $g_3(x)$ is not a PP of $\mathbb{F}_p$ when $p > 3$. Therefore $g_3(x)$ is not a PP of $\mathbb{F}_p$.

From them, we derive that $g_3(x)$ is not a PP of $\mathbb{F}_p$ when $k \neq 2$. Note that $g_3(\mathbb{F}_p) \subseteq \mathbb{F}_p$. So $g_3(x)$ is not a PP of $\mathbb{F}_q$ when $k \neq 2$. Hence $g_3(x)$ is not a PP of $\mathbb{F}_q$. Thus $D_{p^s+p^t+1,k}(1, x)$ is not a PP of $\mathbb{F}_q$. $\square$

By Lemma 2.4 , Theorem 4.1 and Theorem 4.3, we have the following general result.

Theorem 4.4. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s and t be positive integers with $s < t$. Then*

$$D_{p^s+p^t+2,k}(1,x) = \frac{2-k}{16}(1-4x)^{\frac{p^s+p^t+2}{2}} + \frac{2+k}{16}(1-4x)^{\frac{p^s+p^t}{2}} + \frac{4-k}{16}\Big((1-4x)^{\frac{p^s+1}{2}} + (1-4x)^{\frac{p^t+1}{2}}\Big)$$
$$+ \frac{2-k}{16}\Big((1-4x)^{\frac{p^s-1}{2}} + (1-4x)^{\frac{p^t11}{2}}\Big) + \frac{2-k}{16}(1-4x) + \frac{2-k}{16}. \tag{4.2}$$

Consequently, $D_{p^s+p^t+2,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$(2-k)(x^{\frac{p^s+p^t+2}{2}} + x^{\frac{p^s-1}{2}} + x^{\frac{p^t-1}{2}}) + (2+k)x^{\frac{p^s+p^t}{2}} + (4-k)(x^{\frac{p^s+1}{2}} + x^{\frac{p^t+1}{2}})$$

is a PP of $\mathbb{F}_q$. Furthermore, let $\ell \geq 0$ be an integer. Then

$$D_{p^s+p^t+2\ell,k}(1,x) = \sum_{i=0}^{\ell} B_{2\ell,p^s+p^t+2i}(1-4x)^{\frac{p^s+p^t+2i}{2}} + \sum_{j=0}^{\ell} B_{2\ell,2j}(1-4x)^j$$
$$+ \sum_{i=0}^{\ell} B_{2\ell,p^s+2i-1}((1-4x)^{\frac{p^s+2i-1}{2}} + (1-4x)^{\frac{p^t+2i-1}{2}}), \quad 0 \leq \ell \leq \frac{p-1}{2},$$

and

$$D_{p^s+p^t+2\ell+1,k}(1,x) = \sum_{i=0}^{\ell} B_{2\ell+1,p^s+p^t+2i}(1-4x)^{\frac{p^s+p^t+2i}{2}} + \sum_{j=0}^{\ell} B_{2\ell+1,2j}(1-4x)^j$$
$$+ \sum_{i=0}^{\ell+1} B_{2\ell+1,p^s+2i-1}((1-4x)^{\frac{p^s+2i-1}{2}} + (1-4x)^{\frac{p^t+2i-1}{2}}), \quad 0 \leq \ell < \frac{p-1}{2},$$

where all the coefficients $B_{i,j}$ are given as follows:

$$B_{0,p^s+p^t} = \frac{2-k}{4}, B_{0,p^s-1} = \frac{k}{4}, B_{0,0} = \frac{2-k}{4},$$

$$B_{1,p^s+p^t} = \frac{1}{4}, B_{1,p^s+1} = \frac{2-k}{8}, B_{1,p^s-1} = \frac{1}{8}, B_{1,0} = \frac{1}{4},$$

and

$$\begin{cases} B_{2m+2,p^s+p^t+2m+2} = \frac{1}{4}B_{2m,p^s+p^t+2m}, & \text{if } m \geq 0 \\ B_{2m+2,p^s+p^t+2i} = B_{2m+1,p^s+2i} - \frac{1}{4}B_{2m,p^s+p^t+2i} + \frac{1}{4}B_{2m,p^s+2i-2}, & \text{if } 1 \leq i \leq m \\ B_{2m+2,p^s+p^t} = B_{2m+1,p^s+p^t} - \frac{1}{4}B_{2m,p^s+p^t}, & \text{if } m \geq 0 \\ B_{2m+2,p^s+2m+1} = B_{2m+1,p^s+2m+1} + \frac{1}{4}B_{2m,p^s+2m-1}, & \text{if } m \geq 0 \\ B_{2m+2,p^s+2i-1} = B_{2m+1,p^s+2i-1} - \frac{1}{4}B_{2m,p^s+2i-1} + \frac{1}{4}B_{2m,p^s+2i-3}, & \text{if } 1 \leq i \leq m \\ B_{2m+2,p^s-1} = B_{2m+1,p^s-1} - \frac{1}{4}B_{2m,p^s-1}, & \text{if } m \geq 0 \\ B_{2m+2,0} = B_{2m+1,0} - \frac{1}{4}B_{2m,0}, & \text{if } m \geq 0 \\ B_{2m+2,2j} = B_{2m+1,2j} - \frac{1}{4}B_{2m,2j} + \frac{1}{4}B_{2m,2j-2}, & \text{if } 1 \leq j \leq m \\ B_{2m+2,2m+2} = \frac{1}{4}B_{2m,2m}, & \text{if } m \geq 0 \end{cases} \tag{4.3}$$

as well as

$$\begin{cases} B_{2m+1,p^s+p^t+2m} = B_{2m,p^s+p^t+2m} + \frac{1}{4}B_{2m-1,p^s+p^t+2m-2}, & \text{if } m \geq 0 \\ B_{2m+1,p^s+p^t+2i} = B_{2m,p^s+2i} - \frac{1}{4}B_{2m-1,p^s+p^t+2i} + \frac{1}{4}B_{2m-1,p^s+2i-2}, & \text{if } 1 \leq i \leq m-1 \\ B_{2m+1,p^s+p^t} = B_{2m,p^s+p^t} - \frac{1}{4}B_{2m-1,p^s+p^t}, & \text{if } m \geq 0 \\ B_{2m+1,p^s+2m+1} = \frac{1}{4}B_{2m-1,p^s+2m-1}, & \text{if } m \geq 0 \\ B_{2m+1,p^s+2i-1} = B_{2m,p^s+2i-1} - \frac{1}{4}B_{2m-1,p^s+2i-1} + \frac{1}{4}B_{2m-1,p^s+2i-3}, & \text{if } 1 \leq i \leq m \\ B_{2m+1,p^s-1} = B_{2m,p^s-1} - \frac{1}{4}B_{2m-1,p^s-1}, & \text{if } m \geq 0 \\ B_{2m+1,0} = B_{2m,0} - \frac{1}{4}B_{2m-1,0}, & \text{if } m \geq 0 \\ B_{2m+1,2j} = B_{2m,2j} - \frac{1}{4}B_{2m-1,2j} + \frac{1}{4}B_{2m-1,2j-2}, & \text{if } 1 \leq j \leq m-1 \\ B_{2m+1,2m} = B_{2m,2m} + \frac{1}{4}B_{2m-1,2m-2}, & \text{if } m \geq 0 \end{cases} \tag{4.4}$$

Proof. The identity immediately follows from Lemma 2.4 , Theorem 4.1 and Theorem 4.3. Moreover we readily find that there exists coefficients $B_{i,j} \in \mathbb{F}_q$ such that

$$\begin{aligned} D_{p^s+p^t+2\ell,k}(1,x) &= \sum_{i=0}^{\ell} B_{2\ell,p^s+p^t+2i}u^{p^s+p^t+2i} + \sum_{j=0}^{\ell} B_{2\ell,2j}u^{2j} \\ &+ \sum_{i=0}^{\ell+1} B_{2\ell,p^s+2i-1}(u^{p^s+2i-1} + u^{p^t+2i-1}), \quad 0 \leq \ell < \frac{p-1}{2}, \end{aligned} \tag{4.5}$$

and

$$\begin{aligned} D_{p^s+p^t+2\ell-1,k}(1,x) &= \sum_{i=0}^{\ell} B_{2\ell-1,p^s+p^t+2i}u^{p^s+p^t+2i} + \sum_{j=0}^{\ell} B_{2\ell-1,2j}u^{2j} \\ &+ \sum_{i=0}^{\ell+1} B_{2\ell-1,p^s+2i-1}(u^{p^s+2i-1} + u^{p^t+2i-1}), \quad 0 \leq \ell < \frac{p-1}{2}, \end{aligned} \tag{4.6}$$

where $u^2 = 1 - 4x$. Now let's determine all the coefficients $B_{i,j}$. On the one hand, by (4.5) and (4.6), one then has

$$\begin{aligned} &D_{p^s+p^t+2\ell,k}(1,x) - xD_{p^s+p^t+2\ell-1,k}(1,x) = D_{p^s+p^t+2\ell,k}(1,x) - \frac{1-u^2}{4}D_{p^s+p^t+2\ell-1,k}(1,x) \\ &= \sum_{i=0}^{\ell} B_{2\ell,p^s+p^t+2i}u^{p^s+p^t+2i} + \sum_{i=0}^{\ell} B_{2\ell,p^s+2i-1}(u^{p^s+2i-1} + u^{p^t+2i-1}) + \sum_{j=0}^{\ell} B_{2\ell,2j}u^{2j} \\ &\quad - \frac{1}{4}\sum_{i=0}^{\ell-1} B_{2\ell-1,p^s+p^t+2i}u^{p^s+p^t+2i} - \frac{1}{4}\sum_{j=0}^{\ell} B_{2\ell-1,p^s+2i-1}(u^{p^s+2i-1} + u^{p^t+2i-1}) \\ &\quad - \frac{1}{4}\sum_{j=0}^{\ell-1} B_{2\ell-1,2j}u^{2j} + \frac{1}{4}\sum_{j=0}^{\ell-1} B_{2\ell-1,p^s+p^t+2i}u^{p^s+p^t+2i+2} \\ &\quad + \frac{1}{4}\sum_{j=0}^{\ell} B_{2\ell-1,p^s+2i-1}(u^{p^s+2i+1} + u^{p^t+2i+1}) + \frac{1}{4}\sum_{j=0}^{\ell-1} B_{2\ell-1,2j}u^{2j+2} \end{aligned}$$

$$
\begin{aligned}
&= (B_{2\ell,p^s+p^t+2l} + \frac{1}{4})u^{p^s+p^t+2\ell} + \sum_{i=1}^{\ell-1}(B_{2\ell,p^s+p^t+2i} - \frac{1}{4}B_{2\ell-1,p^s+p^t+2i} + \frac{1}{4}B_{2\ell-1,p^s+p^t+2i-2})u^{p^s+p^t+2i} \\
&\quad + (B_{2\ell,p^s+p^t} - \frac{1}{4}B_{2\ell-1,p^s+p^t})u^{p^s+p^t} + \frac{1}{4}B_{2\ell-1,p^s+2\ell-1}(u^{p^s+2\ell+1} + u^{p^t+2\ell+1}) \\
&+ \sum_{i=1}^{\ell}(B_{2\ell,p^s+2i-1} - \frac{1}{4}B_{2\ell-1,p^s+2i-1} + \frac{1}{4}B_{2\ell-1,p^s+2i-3})(u^{p^s+2i-1} + u^{p^t+2i-1}) \\
&+ (B_{2\ell,p^s-1} - \frac{1}{4}B_{2\ell-1,p^s-1})(u^{p^s-1} + u^{p^t-1}) + (B_{2\ell,2\ell} + \frac{1}{4}B_{2\ell-1,2\ell-2})u^{2\ell} \\
&+ \sum_{j=1}^{\ell-1}(B_{2\ell 2j} - \frac{1}{4}B_{2\ell-1,2j} + \frac{1}{4}B_{2\ell-1,2j-2})u^{2j} + B_{2\ell,0} - \frac{1}{4}B_{2\ell-1,0}. \qquad (4.7)
\end{aligned}
$$

On the other hand, Lemma 2.4 tells us that

$$D_{p^s+p^t+2\ell+1,k}(1,x) = D_{p^s+p^t+2\ell,k}(1,x) - xD_{p^s+p^t+2\ell-1,k}(1,x).$$

So by comparing the coefficient of the term u^i in the right hand side of (4.6) and (4.7), one can get the desired results as (4.4). Following the similar way, one also obtain the recursions of $B_{i,j}$ as (4.3). So the proof Theorem 4.4 is complete. □

5. Reversed Dickson polynomials $D_{p^{e_1}+p^{e_2}+\cdots+p^{e_s}+\ell,k}(1,x)$

Let $s \geq 1$ be an integer. Let $e_1, e_2, \cdots, e_s, \ell$ be integers with $0 \leq e_1 < e_2 < \cdots < e_s$ and $0 \leq \ell < p$. In this section, we present an explicit formula for $D_{n,k}(1,x)$ presented by elementary symmetric polynomials in terms of the power of $(1-4x)$ when $n = p^{e_1} + p^{e_2} + \cdots + p^{e_s} + \ell$. Then we characterize $D_{n,k}(1,x)$ to be a PP of $\mathbb{F}_q$ in this case.

Let $\sigma_i(x_1, x_2, \cdots, x_s)$ be the elementary polynomials in s variables $x_1, x_2, \cdots, x_s$ which are defined by

$$
\begin{aligned}
\sigma_0(x_1, x_2, \cdots, x_s) &= 1, \\
\sigma_1(x_1, x_2, \cdots, x_s) &= \sum_{1\leq j\leq n} x_j, \\
\sigma_2(x_1, x_2, \cdots, x_s) &= \sum_{1\leq j<k\leq n} x_j x_k, \\
\sigma_3(x_1, x_2, \cdots, x_s) &= \sum_{1\leq j<k<\ell\leq n} x_j x_k x_\ell,
\end{aligned}
$$

and so forth, ending with

$$\sigma_s(x_1, x_2, \cdots, x_s) = x_1 x_2 \cdots x_s.$$

Now we give the first result of this section.

Theorem 5.1. *Let $q = p^e$ with p being an odd prime and e being a positive integer. Let s be a positive integer. Let $e_1, \cdots, e_s$ be nonnegative integers with $e_1 < \cdots < e_s$. Then*

$$D_{p^{e_1}+\ldots+p^{e_s},k}(1,x) = \frac{1}{2^s}\Big((2-k)\sum_{\substack{1\le i\le s\\ i \text{ even}}} \sigma_i((1-4x)^{\frac{p^{e_1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}}) + k\sum_{\substack{1\le i\le s\\ i \text{ odd}}} \sigma_i((1-4x)^{\frac{p^{e_1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}})\Big).$$

Consequently, $D_{p^{e_1}+\ldots+p^{e_s},k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$(2-k)\sum_{\substack{0\le i\le s\\ i \text{ even}}} \sigma_i(x^{\frac{p^{e_1}}{2}},\cdots,x^{\frac{p^{e_s}}{2}}) + k\sum_{\substack{1\le i\le s\\ i \text{ odd}}} \sigma_i(x^{\frac{p^{e_1}-1/i}{2}},\cdots,x^{\frac{p^{e_s}-1/i}{2}})$$

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

Proof. We divide the proof into the following two cases.

Case 1. $x \neq \frac{1}{4}$. For this case, putting $x = y(1-y)$ in the second identity of Lemma 2.3 gives us that

$$\begin{aligned}
&D_{p^{e_1}+\ldots+p^{e_s},k}(1,x) = D_{p^{e_1}+\ldots+p^{e_s},k}(1,y(1-y))\\
=&\frac{(k-1-(k-2)y)y^{p^{e_1}+\ldots+p^{e_s}} - (1+(k-2)y)(1-y)^{p^{e_1}+\ldots+p^{e_s}}}{2y-1}\\
=&\frac{\frac{k+(2-k)u}{2}(\frac{u+1}{2})^{p^{e_1}+\cdots+p^{e_s}} - \frac{k+(k-2)u}{2}(\frac{1-u}{2})^{p^{e_1}+\cdots+p^{e_s}}}{u}\\
=&\frac{k+(2-k)u}{2^{p^{e_1}+\cdots+p^{e_s}+1}u}\prod_{i=1}^{s}(u^{p^{e_i}}+1) - \frac{k+(k-2)u}{2^{p^{e_1}+\cdots+p^{e_s}+1}u}\prod_{i=1}^{s}(1-u^{p^{e_i}})\\
=&\frac{1}{2^{s+1}u}\Big((k+(2-k)u)\sum_{0\le i\le s}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}}) - (k+(k-2)u)\sum_{0\le i\le s}(-1)^i\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})\Big)\\
=&\frac{1}{2^s}\Big((2-k)\sum_{\substack{0\le i\le s\\ i \text{ even}}}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}}) + k\sum_{\substack{1\le i\le s\\ i \text{ odd}}}\sigma_i(u^{p^{e_1}-1/i},\cdots,u^{p^{e_s}-1/i})\Big),
\end{aligned}$$

where $u = 2y-1$ and $u^2 = 1-4x$. Then we have that

$$D_{p^{e_1}+\ldots+p^{e_s},k}(1,x) = \frac{1}{2^s}\Big((2-k)\sum_{\substack{0\le i\le s\\ i \text{ even}}} \sigma_i((1-4x)^{\frac{p^{e_1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}}) + k\sum_{\substack{1\le i\le s\\ i \text{ odd}}} \sigma_i((1-4x)^{\frac{p^{e_1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}})\Big).$$

as desired.

Case 2. $x = \frac{1}{4}$. On the one hand, by the first identity of Lemma 2.3, one has

$$D_{p^{e_1}+\ldots+p^{e_s},k}(1,\frac{1}{4}) = \frac{k(p^{e_1}+\cdots+p^{e_s})-k+2}{2^{p^{e_1}+\cdots+p^{e_s}}} = \frac{2-k}{2^s}.$$

On the other hand,

$$\frac{1}{2^s}\Big((2-k)\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i((1-4x)^{\frac{p^{e1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}})$$

$$+k\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i((1-4x)^{\frac{p^{e1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}})\Big)\Big|_{x=1/4}=\frac{2-k}{2^s}.$$

Thus the required result follows. So Theorem 5.1 is proved. □

Theorem 5.2. *Let $q=p^e$ with p being an odd prime and e being a positive integer. Let s be a positive integer. Let $e_1,\cdots,e_s$ be nonnegative integers with $e_1<\cdots<e_s$. Then*

$$D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,x)=\frac{1}{2^{s+1}}\Big(2\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i((1-4x)^{\frac{p^{e_1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}})$$

$$+((2-k)(1-4x)+k)\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i((1-4x)^{\frac{p^{e1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}})\Big).$$

Consequently, $D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if the polynomial

$$2\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i(x^{\frac{p^{e1}}{2}},\cdots,x^{\frac{p^{e_s}}{2}})+((2-k)x+k)\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i(x^{\frac{p^{e1}-1/i}{2}},\cdots,x^{\frac{p^{e_s}-1/i}{2}})$$

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

Proof. We consider the following two cases.

Case 1. $x\neq\frac{1}{4}$. For this case, putting $x=y(1-y)$ in the second identity of Lemma 2.3 gives us that

$$\begin{aligned}
&D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,x)=D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,y(1-y))\\
=&\frac{(k-1-(k-2)y)y^{p^{e_1}+\ldots+p^{e_s}+1}-(1+(k-2)y)(1-y)^{p^{e_1}+\ldots+p^{e_s}+1}}{2y-1}\\
=&\frac{\frac{k+(2-k)u}{2}(\frac{u+1}{2})^{p^{e_1}+\cdots+p^{e_s}+1}-\frac{k+(k-2)u}{2}(\frac{1-u}{2})^{p^{e_1}+\cdots+p^{e_s}+1}}{u}\\
=&\frac{k+(2-k)u}{2^{p^{e_1}+\cdots+p^{e_s}+2}u}\prod_{i=1}^{s}(u^{p^{e_i}}+1)(u+1)-\frac{k+(k-2)u}{2^{p^{e_1}+\cdots+p^{e_s}+2}u}\prod_{i=1}^{s}(1-u^{p^{e_i}})(1-u)\\
=&\frac{1}{2^{s+2}u}\Big((k+2+(2-k)u^2)\sum_{0\le i\le s}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})-(2k+(4-2k)u^2)\sum_{0\le i\le s}(-1)^i\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})\Big)\\
=&\frac{1}{2^{s+1}}\Big(2\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})+((2-k)u^2+k)\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i(u^{p^{e_1}-1/i},\cdots,u^{p^{e_s}-1/i})\Big),
\end{aligned}$$

where $u=2y-1$ and $u^2=1-4x$. Then we have

$$D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,x)=\frac{1}{2^{s+1}}\Big(2\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i((1-4x)^{\frac{p^{e1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}})$$

$$+\left((2-k)(1-4x)+k\right)\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i\big((1-4x)^{\frac{p^{e_1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}}\big)\Big).$$

as desired.

Case 2. $x=\frac{1}{4}$. On the one hand, by the first identity of Lemma 2.3, one has

$$D_{p^{e_1}+\ldots+p^{e_s}+1,k}(1,\frac{1}{4})=\frac{k(p^{e_1}+\cdots+p^{e_s}+1)-k+2}{2^{p^{e_1}+\cdots+p^{e_s}+1}}=\frac{2}{2^{s+1}}.$$

On the other hand,

$$\frac{1}{2^{s+1}}\Big(2\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i\big((1-4x)^{\frac{p^{e_1}}{2}},\cdots,(1-4x)^{\frac{p^{e_s}}{2}}\big)$$
$$+\left((2-k)(1-4x)+k\right)\sum_{\substack{1\le i\le s\\ i\text{ odd}}}\sigma_i\big((1-4x)^{\frac{p^{e_1}-1/i}{2}},\cdots,(1-4x)^{\frac{p^{e_s}-1/i}{2}}\big)\Big)\Big|_{x=1/4}=\frac{2}{2^{s+1}}.$$

Thus the required result follows. So Theorem 5.3 is proved. ◻

Then Theorems 5.1-5.2 together with Lemma 2.4 show that the general result is true.

Theorem 5.3. *Let $q=p^e$ with p being an odd prime and e being a positive integer. Let s be a positive integer. Let $e_1,\cdots,e_s$ be nonnegative integers with $e_1<\cdots<e_s$. Then for any $\ell\ge 0$ each of the identities is true.*

$$D_{p^{e_1}+\ldots+p^{e_s}+2\ell,k}(1,x)=\frac{1}{2^{s+2\ell}}\Big(\sum_{j=0}^{\ell}C_{2\ell,2j}u^{2j}\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})+\sum_{j=0}^{\ell}Q_{2\ell,2j}u^{2j}\sum_{\substack{0\le i\le s\\ i\text{ odd}}}\sigma_i(u^{p^{e_1}-\frac{1}{i}},\cdots,u^{p^{e_s}-\frac{1}{i}})\Big),$$

$$D_{p^{e_1}+\ldots+p^{e_s}+2\ell+1,k}(1,x)=\frac{1}{2^{s+2\ell+1}}\Big(\sum_{j=0}^{\ell}C_{2\ell+1,2j}u^{2j}\sum_{\substack{0\le i\le s\\ i\text{ even}}}\sigma_i(u^{p^{e_1}},\cdots,u^{p^{e_s}})+\sum_{j=0}^{\ell+1}Q_{2\ell+1,2j}u^{2j}\sum_{\substack{0\le i\le s\\ i\text{ odd}}}\sigma_i(u^{p^{e_1}-\frac{1}{i}},\cdots,u^{p^{e_s}-\frac{1}{i}})\Big),$$

where $u^2=1-4x$, and the coefficients $C_{a,2b}$ and $Q_{a,2b}$ can be determined as follows:

$$C_{0,0}=2-k,Q_{0,0}=k,C_{1,0}=k,Q_{1,2}=2-k,$$

$$\begin{cases}C_{2m+2,0}=2C_{2m+1,0}-C_{2m,0}, & \text{if } m\ge 0\\ C_{2m+2,2j}=2C_{2m+1,2j}+C_{2m,2j-2}-C_{2m,2j}, & \text{if } 1\le j\le m\\ C_{2m+2,2m+2}=C_{2m,2m}, & \text{if } m\ge 0\\ Q_{2m+2,0}=2Q_{2m+1,0}-Q_{2m,0}, & \text{if } m\ge 0\\ Q_{2m+2,2j}=2Q_{2m+1,2j}+Q_{2m,2j-2}-Q_{2m,2j}, & \text{if } 1\le j\le m\\ Q_{2m+2,2m+2}=2Q_{2m+1,2m+2}+Q_{2m,2m}, & \text{if } m\ge 0\end{cases}\tag{5.1}$$

as well as

$$\begin{cases}C_{2m+1,0}=2C_{2m,0}-C_{2m-1,0}, & \text{if } m\ge 1\\ C_{2m+1,2j}=2C_{2m,2j}+C_{2m-1,2j-2}-C_{2m-1,2j}, & \text{if } 1\le j\le m-1\\ C_{2m+1,2m}=2C_{2m,2m}+C_{2m-1,2m-2}, & \text{if } m\ge 1\\ Q_{2m+1,0}=2Q_{2m,2j}-Q_{2m-1,0}, & \text{if } m\ge 0\\ Q_{2m+1,2j}=2Q_{2m,2j}+Q_{2m-1,2j-2}-Q_{2m-1,2j}, & \text{if } 1\le j\le m\\ Q_{2m+1,2m+2}=2Q_{2m-1,2m}, & \text{if } m\ge 1\end{cases}\tag{5.2}$$

Acknowledgement

Cheng was supported partially by the General Project of Department of Education of Sichuan Province 15ZB0434. [2000]Primary 11T06, 11T55, 11C08.

Conflict of Interest

The author declares no conflicts of interest in this paper.

References

1. K. Cheng, *Permutational Behavior of Reversed Dickson Polynomials over Finite Fields*, AIMS Math., **2** (2017), 244-259.
2. R. Coulter, *Explicit evaluation of some Weil sums*, Acta Arith., **83** (1998), 241-251.
3. S. Hong, X. Qin and W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational,* Finite Fields Appl., **37** (2016), 54-71.
4. X. Hou, G. L. Mullen, J.A. Sellers and J.L. Yucas, *Reversed Dickson polynomials over finite fields,* Finite Fields Appl., **15** (2009), 748-773.
5. R. Lidl and H. Niederreiter, *Finite Fields, second ed., Encyclopedia of Mathematics and its Applications,* Cambridge University Press, Cambridge, **20**, 1997.
6. X. Qin and S. Hong, *Constructing permutation polynomials over finite fields,* Bull. Aust. Math. Soc., **89** (2014), 420-430.
7. X. Qin, G. Qian and S. Hong, *New results on permutation polynomials over finite fields,* Int. J. Number Theory, **11** (2015), 437-449.
8. Q. Wang and J. Yucas, *Dickson polynomials over finite fields,* Finite Fields Appl., **18** (2012), 814-831.