Finite Fields and Their Applications 15 (2009) 748–773

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Reversed Dickson polynomials over finite fields

Xiang-dong Hou [a], Gary L. Mullen [b], James A. Sellers [b], Joseph L. Yucas [c,*]

[a] Department of Mathematics, University of South Florida, Tampa, FL 33620, United States
[b] Department of Mathematics, The Pennsylvania State University, University Park, PA 16802, United States
[c] Department of Mathematics, Southern Illinois University, Carbondale, IL 62901, United States

ARTICLE INFO

Article history:
Received 27 March 2009
Available online 29 August 2009
Communicated by Rudolf Lidl

Keywords:
Almost perfect nonlinear function
Dickson polynomial
Finite field
Reversed Dickson polynomial

ABSTRACT

Reversed Dickson polynomials over finite fields are obtained from Dickson polynomials $D_n(x,a)$ over finite fields by reversing the roles of the indeterminate x and the parameter a. We study reversed Dickson polynomials with emphasis on their permutational properties over finite fields. We show that reversed Dickson permutation polynomials (RDPPs) are closely related to almost perfect nonlinear (APN) functions. We find several families of nontrivial RDPPs over finite fields; some of them arise from known APN functions and others are new. Among RDPPs on $\mathbb{F}_q$ with $q < 200$, with only one exception, all belong to the RDPP families established in this paper.

1. Introduction

Let $n \geqslant 0$ be an integer and consider the symmetric polynomial $x_1^n + x_2^n \in \mathbb{Z}[x_1, x_2]$. Since the elementary symmetric polynomials $x_1 + x_2$ and x_1x_2 form a $\mathbb{Z}$-basis of the ring of symmetric polynomials in $\mathbb{Z}[x_1, x_2]$, there exists $D_n(x, y) \in \mathbb{Z}[x, y]$ such that

$$x_1^n + x_2^n = D_n(x_1 + x_2, x_1x_2); \tag{1}$$

* Corresponding author.
E-mail addresses: xhou@cas.usf.edu (X.-d. Hou), mullen@math.psu.edu (G.L. Mullen), sellersj@math.psu.edu (J.A. Sellers), jyucas@math.siu.edu (J.L. Yucas).

1071-5797/$ – see front matter
doi:10.1016/j.ffa.2009.06.004

see [14]. The polynomial $D_n(x, y)$ is given by Waring's formula [13, Theorem 1.76]

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

and is the solution of the recurrence relation [12, Lemma 2.3]

$$\begin{cases} D_0(x, y) = 2, \\ D_1(x, y) = x, \\ D_n(x, y) = xD_{n-1}(x, y) - yD_{n-2}(x, y), \quad n \geqslant 2. \end{cases}$$

For a prime power $q = p^e$ with p a prime and e a positive integer, let $\mathbb{F}_q$ denote the finite field of order q. For fixed $a \in \mathbb{F}_q$, $D_n(x, a) \in \mathbb{F}_q[x]$ is the *Dickson polynomial of degree n and parameter a*. These polynomials were studied by L.E. Dickson for their permutational properties over $\mathbb{F}_q$ [5]. In 1923 Schur [16] named these polynomials Dickson polynomials in Dickson's honor.

When $a = 0$, $D_n(x, 0) = x^n$, which induces a permutation of $\mathbb{F}_q$, i.e., is a *permutation polynomial* (PP) on $\mathbb{F}_q$, if and only if $(n, q-1) = 1$.

When $0 \neq a \in \mathbb{F}_q$, it is known that the Dickson polynomial $D_n(x, a)$ induces a permutation of $\mathbb{F}_q$ if and only if $(n, q^2-1) = 1$; see [13, Theorem 7.16] or [12, Theorem 3.2]. This simple condition provides a very effective test to determine which Dickson polynomials induce permutations of $\mathbb{F}_q$, and moreover once the condition is satisfied, we obtain $q-1$ different permutations, one for each of the elements $a \in \mathbb{F}_q^*$. The *value set* V_f of a polynomial $f \in \mathbb{F}_q[x]$ is defined to be $V_f = \{f(b)\colon\ b \in \mathbb{F}_q\}$. In [2] the authors determined the cardinality $|V_{D_n(x,a)}|$ of the value set $V_{D_n(x,a)}$ of the Dickson polynomial $D_n(x, a)$ over $\mathbb{F}_q$. For many additional algebraic and number theoretic properties of Dickson polynomials, we refer to [12].

2. Reversed Dickson polynomials: A different perspective

In this paper, we consider a different perspective; namely we fix $a \in \mathbb{F}_q$, and study the polynomial $D_n(a, x) \in \mathbb{F}_q[x]$ with emphasis on its permutational behavior over $\mathbb{F}_q$. We call $D_n(a, x) \in \mathbb{F}_q[x]$ a *reversed Dickson polynomial*. (One should refrain from calling $D_n(a, x)$ a Dickson polynomial of the second kind since the latter terminology already exists; see Definition 2.2 of [12].)

We emphasize that a reversed Dickson polynomial is in general, not a Dickson polynomial. We use the terminology "reversed" Dickson polynomial to indicate that we start with a Dickson polynomial $D_n(x, a)$ as defined above, and then we interchange the roles of x and a to obtain what we call a reversed Dickson polynomial.

In fact, reversed Dickson polynomials have been studied in [9–11] by Kang in the form of $D_n(a, -x)$. However, Kang did not consider the permutational properties of these polynomials. Also see Chapter 2 of [12] for some basic properties of Kang's polynomials. A reversed Dickson polynomial which induces a permutation of $\mathbb{F}_q$ is called a *reversed Dickson permutation polynomial* (reversed Dickson PP or RDPP) on $\mathbb{F}_q$.

When $a = 0$, we have

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

Hence $D_n(0, x)$ is a PP on $\mathbb{F}_q$ if and only if $n = 2k$ with $(k, q-1) = 1$. We thus hereafter assume that $a \in \mathbb{F}_q^*$.

It follows from (2) that

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

Hence $D_n(a,x)$ is a PP on $\mathbb{F}_q$ if and only if $D_n(1,x)$ is a PP on $\mathbb{F}_q$. Therefore it suffices to consider the reversed Dickson polynomial $D_n(1,x)$. The ultimate question is for which n the polynomial $D_n(1,x)$ is a PP on $\mathbb{F}_q$. This question, unlike the same question for Dickson polynomials $D_n(x,a)$, does not seem to have an easy answer.

We obtain numerous sufficient conditions for when the RDP $D_n(1,x)$ is a PP on $\mathbb{F}_q$; see for example Theorem 4.4, Corollary 5.2, and Theorems 5.3 and 5.7. Moreover, in Conjecture 7.1 we postulate the complete set of values of n for which $D_n(1,x)$ is a PP on $\mathbb{F}_p$, when $p>3$ is prime.

In the next proposition, we list some basic facts about the reversed Dickson polynomial $D_n(1,x)$.

Proposition 2.1. *Let $q=p^e$, where p is a prime and e is a positive integer, and let $n\geqslant 0$ be an integer.*

(i) *In $\mathbb{Z}[x]$, we have*

$$D_n\big(1,x(1-x)\big)=x^n+(1-x)^n. \tag{3}$$

(ii) *In $\mathbb{F}_q[x]$, we have*

$$D_{np}(1,x)=\big(D_n(1,x)\big)^p.$$

(iii) *If $n_1,n_2>0$ are integers such that $n_1\equiv n_2 \pmod{p^{2e}-1}$, then $D_{n_1}(1,x)=D_{n_2}(1,x)$ for all $x\in\mathbb{F}_q$.*

(iv) *If two positive integers n_1 and n_2 belong to the same p-cyclotomic coset modulo $p^{2e}-1$, then $D_{n_1}(1,x)$ is a PP on $\mathbb{F}_q$ if and only if $D_{n_2}(1,x)$ is a PP on $\mathbb{F}_q$.*

Proof. Parts (i) and (ii) follow immediately from (1).

(iii) For each $x\in\mathbb{F}_q$, there exists $y\in\mathbb{F}_{q^2}$ such that $x=y(1-y)$. Then

$$\begin{aligned} D_{n_1}(1,x)&=D_{n_1}\big(1,y(1-y)\big)=y^{n_1}+(1-y)^{n_1}=y^{n_2}+(1-y)^{n_2}\\ &=D_{n_2}\big(1,y(1-y)\big)=D_{n_2}(1,x).\end{aligned}$$

Part (iv) follows from (ii) and (iii). □

This paper is organized as follows. In Section 3, we take on a very natural question: Given integers $n_1,n_2\geqslant 0$, when are $D_{n_1}(1,x)$ and $D_{n_2}(1,x)$ equal as functions on $\mathbb{F}_q$? We are able to answer this question in Theorems 3.1 and 3.2. The proofs of these two theorems are rather involved and technical; so they are given in Appendix A. In Section 4, we discuss some connections between reversed Dickson permutation polynomials on $\mathbb{F}_q$ and almost perfect nonlinear (APN) functions on $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. APN functions (defined in Section 4) have been attracting much attention because of their important applications in cryptography. We obtain several families of reversed Dickson PPs from some known families of APN functions. However, not all reversed Dickson PPs are obtained from APN functions. In Section 5, we present three families of reversed Dickson PPs which are not obtainable from APN functions, two of which seem to be new families of permutation polynomials over finite fields. In Section 6, we explore some necessary conditions on n and q for $D_n(1,x)$ to be a PP on $\mathbb{F}_q$. Section 7 contains a table which gives all values of p^e and n with $p^e<200$ such that $D_n(1,x)$ is a PP on $\mathbb{F}_{p^e}$. With only one exception, all RDPPs in this parameter range are covered by the families discussed in Sections 4 and 5.

3. When are $D_{n_1}(1,x)$ and $D_{n_2}(1,x)$ equal as functions on $\mathbb{F}_{p^e}$?

For $n_1,n_2\in\{0,1,\ldots,p^{2e}-1\}$, we say that $n_1\sim n_2$ if $D_{n_1}(1,x)\equiv D_{n_2}(1,x) \pmod{x^{p^e}-x}$. The relation $\sim$ is an equivalence relation whose equivalence classes can be described as follows.

Theorem 3.1. *Let $p = 2$. Then the $\sim$-equivalence classes of $\{0, 1, \ldots, 2^{2e} - 1\}$ are*

$$\begin{aligned}
&\{0\},\\
&\{2^k\colon 0 \leqslant k \leqslant 2e-1\},\\
&\{(2^e+1)2^k\colon 0 \leqslant k \leqslant e-1\},\\
&\{\alpha+\beta 2^e, \beta+\alpha 2^e\}, \quad 0 \leqslant \alpha, \beta \leqslant 2^e-1,\\
&\qquad\qquad \alpha+\beta 2^e \neq 0,\ 2^k\ (0 \leqslant k \leqslant 2e-1),\ (2^e+1)2^k\ (0 \leqslant k \leqslant e-1).
\end{aligned}$$

Theorem 3.2. *Let p be an odd prime. Then the $\sim$-equivalence classes of $\{0, 1, \ldots, p^{2e} - 1\}$ are*

$$\begin{aligned}
&\{0\},\\
&\{p^k\colon 0 \leqslant k \leqslant 2e-1\},\\
&\left\{\frac{p^{2e}-1}{2} + p^k\colon 0 \leqslant k \leqslant 2e-1\right\},\\
&\{\alpha+\beta p^e, \beta+\alpha p^e\}, \quad 0 \leqslant \alpha, \beta \leqslant p^e-1,\ \alpha+\beta p^e \neq 0, p^k, \frac{p^{2e}-1}{2}+p^k,\ 0 \leqslant k \leqslant 2e-1.
\end{aligned}$$

Remark. In Theorem 3.2, note that $\frac{p^{2e}-1}{2} + p^k \equiv \frac{p^{2e}+1}{2} \cdot p^k \pmod{p^{2e}-1}$.

The proofs of Theorems 3.1 and 3.2 are given in Appendix A.

4. Reversed Dickson PPs and APN functions

Lemma 4.1. *Let $x \in \mathbb{F}_{p^{2e}}$. Then $x(1-x) \in \mathbb{F}_{p^e}$ if and only if $x^{p^e} = x$ or $x^{p^e} = 1 - x$.*

Proof. We have

$$\left[x(1-x)\right]^{p^e} - x(1-x) = x^{p^e} - x^{2p^e} - x + x^2 = -\left(x^{p^e} - x\right)\left(x^{p^e} + x - 1\right).$$

The conclusion follows immediately. □

We define

$$V = \left\{x \in \mathbb{F}_{p^{2e}}\colon x^{p^e} = 1 - x\right\} \tag{4}$$

and note that

$$\mathbb{F}_{p^e} \cap V = \begin{cases} \emptyset & \text{if } p = 2,\\ \{\frac{1}{2}\} & \text{if } p > 2. \end{cases}$$

Proposition 4.2.

(i) *Let $p = 2$. Then $D_n(1, x)$ is PP on $\mathbb{F}_{2^e}$ if and only if the function $y \mapsto y^n + (1-y)^n$ is a 2-to-1 mapping on $\mathbb{F}_{2^e} \cup V$.*

(ii) *Let $p > 2$. Then $D_n(1, x)$ is a PP on $\mathbb{F}_{p^e}$ if and only if the function $y \mapsto y^n + (1-y)^n$ is a 2-to-1 mapping on $(\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$ and $y^n + (1-y)^n \neq (\frac{1}{2})^{n-1}$ for any $y \in (\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$.*

Proof. We only prove (ii) since the proof of (i) is similar.

For necessity, assume $y_1, y_2 \in (\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$ such that $y_1^n + (1-y_1)^n = y_2^n + (1-y_2)^n$. Then $y_1(1-y_1), y_2(1-y_2) \in \mathbb{F}_{p^e}$ and $D_n(1, y_1(1-y_1)) = D_n(1, y_2(1-y_2))$. Thus $y_1(1-y_1) = y_2(1-y_2)$ which implies that $y_1 = y_2$ or $1-y_2$. So $y \mapsto y^n + (1-y)^n$ is a 2-to-1 mapping on $(\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$. If $y \in (\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$, then $y(1-y) \in \mathbb{F}_{p^e}$ and $y(1-y) \neq \frac{1}{2}(1-\frac{1}{2})$. Thus $y^n + (1-y)^n = D_n(1, y(1-y)) \neq D_n(1, \frac{1}{2}(1-\frac{1}{2})) = (\frac{1}{2})^{n-1}$.

For sufficiency, assume $x_1, x_2 \in \mathbb{F}_{p^e}$ such that $D_n(1, x_1) = D_n(1, x_2)$. Write $x_i = y_i(1-y_i)$, where $y_i \in \mathbb{F}_{p^e} \cup V$, $i = 1, 2$. Then $y_1^n + (1-y_1)^n = D_n(1, x_1) = D_n(1, x_2) = y_2^n + (1-y_2)^n$. If $y_1 = \frac{1}{2}$, then $y_2^n + (1-y_2)^n = (\frac{1}{2})^{n-1}$ which forces $y_2 = \frac{1}{2}$, hence $x_1 = x_2$. If $y_1, y_2 \neq \frac{1}{2}$, since $y \mapsto y^n + (1-y)^n$ is a 2-to-1 mapping on $(\mathbb{F}_{p^e} \cup V) \setminus \{\frac{1}{2}\}$, we have $y_1 = y_2$ or $y_1 = 1 - y_2$, which also implies that $x_1 = x_2$. □

A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called *almost perfect nonlinear* (APN) if for each $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$, the equation $f(x+a) - f(x) = b$ has at most two solutions in $\mathbb{F}_q$. APN functions were introduced by Nyberg [15] for applications in cryptography. The differential uniformality of APN functions makes them highly immune to differential and linear cryptanalysis. Much work has been done on APN functions; we refer the reader to [1,6–8] and the references therein. It is clear that a power function x^n is an APN function on $\mathbb{F}_q$ if and only if for each $b \in \mathbb{F}_q$, the equation $(x+1)^n - x^n = b$ has at most two solutions in $\mathbb{F}_q$. The following proposition relates reversed Dickson PPs and power APN functions.

Proposition 4.3.

(i) *The polynomial x^n is an APN function on $\mathbb{F}_{2^{2e}} \Rightarrow D_n(1, x)$ is a PP on $\mathbb{F}_{2^e} \Rightarrow x^n$ is an APN function on $\mathbb{F}_{2^e}$.*
(ii) *Let p be an odd prime and n an odd positive integer. Then the polynomial*

$$x^n \text{ is an APN function on } \mathbb{F}_{p^{2e}} \quad \Rightarrow \quad D_n(1, x) \text{ is a PP on } \mathbb{F}_{p^e} \quad \Rightarrow \quad x^n \text{ is an APN function on } \mathbb{F}_{p^e}.$$

Proof. Part (i) immediately follows from Proposition 4.2(i).

Part (ii) follows from Proposition 4.2(ii), where one only has to notice that since n is odd, $y^n + (1-y)^n = y^n - (y-1)^n$. □

For a survey of known power APN functions, we refer the reader to [7] (for $p = 2$) and [8] (for $p > 2$). The following theorem lists all reversed Dickson PPs obtained from known power APN functions using Proposition 4.3.

Theorem 4.4. *The reversed Dickson polynomial $D_n(1, x)$ is a PP on $\mathbb{F}_{p^e}$ in each of the following cases*:

I. $p = 2$. (*See* [7, Table 1].)
   (i) $n = 2^k + 1$, $(k, 2e) = 1$ (*Gold*).
   (ii) $n = 2^{2k} - 2^k + 1$, $(k, 2e) = 1$ (*Kasami*).
   (iii) $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$, $e = 5k$ (*Dobbertin*).

II. $p > 2$. (*See* [8].)
   (i) $n = 3$, $p > 3$ ($D_3(1, x) = -3x + 1$, *trivial*).
   (ii) $n = p^e + 2$, $p^e \equiv 1 \pmod 3$ [8, Theorem 8].
   (iii) $n = \frac{5^k+1}{2}$, $p = 5$, $(k, 2e) = 1$ [8, Corollary 1].

Remark. When $p=2$ and $n=2^{2k}-2^k+1$, in $\mathbb{F}_2[x]$, we have

$$\begin{aligned}
D_n\big(1,x(1+x)\big) &= x^n+(1+x)^n\\
&= \frac{x^{2^{2k}+1}}{x^{2^k}}+\frac{(1+x)^{2^{2k}+1}}{(1+x)^{2^k}}\\
&= \frac{x^{2^{2k}+1}+x^{2^{2k}+2^k}+x^{2^k+1}+x^{2^k}}{x^{2^k}(1+x)^{2^k}}\\
&= \frac{x^{2^{2k}+1}+x^{2^{2k}+2^k}+x^{2^k+1}+x^{2^k+2^k}}{x^{2^k}(1+x)^{2^k}}+1\\
&= \frac{(x^{2^k}+x)^{2^k+1}}{x^{2^k}(1+x)^{2^k}}+1\\
&= \frac{[(x(x+1))^{2^{k-1}}+(x(x+1))^{2^{k-2}}+\cdots+x(x+1)]^{2^k+1}}{[x(1+x)]^{2^k}}+1.
\end{aligned}$$

So

$$D_n(1,x)=\frac{(x^{2^{k-1}}+x^{2^{k-2}}+\cdots+x)^{2^k+1}}{x^{2^k}}+1=x\big(x^{2^{k-1}-1}+x^{2^{k-2}-1}+\cdots+1\big)^{2^k+1}+1.$$

We observe that $D_n(1,x)-1$ is the polynomial f_k in Theorem 1.1 of [3] and that Theorem 4.4.I(ii) of the present paper is a (partial) restatement of Theorem 1.1 of [3].

It is natural to ask if the converses of the statements in Proposition 4.3 are true. Some of the converses are known to be false while the statuses of others are not known. Here are some counterexamples.

Example 4.5. Let $p=2$, $e=2$, $n=2^4+2^2+1=21$. Then $D_{21}(1,x)$ is a PP on $\mathbb{F}_{2^4}$ (Theorem 5.3) but x^{21} is not an APN function on $\mathbb{F}_{2^8}$ (Proposition 5.4).

Example 4.6. Let $p=2$, $e=3$, $n=2^2+1=5$. Then x^5 is an APN function on $\mathbb{F}_{2^3}$ (the Gold case) but $D_5(1,x)=x^2+x+1$ is not a PP on $\mathbb{F}_{2^3}$.

Example 4.7. Let $p>3$ be a prime such that $p\equiv -1 \pmod 3$ and let $e=1$, $n=p+2$. Then x^{p+2} $(=x^3)$ is an APN function on $\mathbb{F}_p$ but $D_{p+2}(1,x)$ is not a PP on $\mathbb{F}_p$ (Corollary 5.2(ii)).

Example 4.8. Let $p>3$ be a prime such that $p\equiv 1 \pmod 3$ and let $e=2$, $n=p+2$. Then x^{p+2} is an APN function on $\mathbb{F}_{p^2}$ [8, Theorem 8]. However, we have $D_{p+2}(1,x)=2(-x+\frac{1}{4})^{\frac{p+1}{2}}+\frac{1}{2}-x$ (Proposition 5.1), which is not a PP on $\mathbb{F}_{p^2}$ since the degree of $D_{p+2}(1,x)=\frac{p+1}{2}$ is a divisor of p^2-1 [13, Corollary 7.5].

The case $p=3$ is special in Proposition 4.3(ii). In fact, if n is odd, x^n is not an APN function on $\mathbb{F}_{3^e}$ for any $e>0$. The function $(x+1)^n-x^n$ takes the value 1 at $x=0,\pm 1$. Therefore Proposition 4.3(ii) implies that if n is odd, $D_n(1,x)$ is never a PP on $\mathbb{F}_{3^e}$. (This fact also follows from Proposition 6.1.)

However, we do not know the answers to the following questions.

Open questions.

1. If $D_n(1,x)$ is a PP on $\mathbb{F}_{2^e}$, where e is odd, is x^n an APN function on $\mathbb{F}_{2^{2e}}$?
2. If $D_n(1,x)$ is a PP on $\mathbb{F}_{p^e}$, where $p>3$ and n is odd, is x^n an APN function on $\mathbb{F}_{p^{2e}}$?

5. Reversed Dickson PPs which do not arise from APN functions

Proposition 5.1. *Let p be an odd prime and $k \geqslant 0$. Then in $\mathbb{F}_p[x]$,*

$$D_{p^k+1}(1,x) = 2\left(-x+\frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2}, \tag{5}$$

$$D_{p^k+2}(1,x) = 2\left(-x+\frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2} - x. \tag{6}$$

Proof. We only prove (5) since $D_{p^k+2}(1,x) = D_{p^k+1}(1,x) - xD_{p^k}(1,x)$ and $D_{p^k}(1,x) = 1$. We have

$$\begin{aligned}
D_{p^k+1}\big(1, x(1-x)\big) &= x^{p^k+1} + (1-x)^{p^k+1} \\
&= \left[\frac{1}{2} + \left(x-\frac{1}{2}\right)\right]^{p^k+1} + \left[\frac{1}{2} - \left(x-\frac{1}{2}\right)\right]^{p^k+1} \\
&= 2\cdot\left(\frac{1}{2}\right)^{p^k+1} + 2\cdot\left(x-\frac{1}{2}\right)^{p^k+1} \\
&= 2\left(x^2-x+\frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2} \\
&= 2\left(-x(1-x)+\frac{1}{4}\right)^{\frac{p^k+1}{2}} + \frac{1}{2}.
\end{aligned}$$

Therefore (5) follows. □

Corollary 5.2. *Let p be an odd prime and let $e > 0$, $k \geqslant 0$ be integers.*

(i) *$D_{p^k+1}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $p^k \equiv 1 \pmod 4$ and $\nu_2(e) \leqslant \nu_2(k)$, where ν_2 is the 2-adic order.*
(ii) *$D_{p^e+2}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $p^e \equiv 1 \pmod 3$.*

Proof. (i) By (5), $D_{p^k+1}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if $(\frac{p^k+1}{2}, p^e-1) = 1$. By [4, Lemma 2.6], $(\frac{p^k+1}{2}, p^e-1) = 1$ if and only if $p^k \equiv 1 \pmod 4$ and $\nu_2(e) \leqslant \nu_2(k)$.

(ii) By (6), $D_{p^e+2}(1,x) = 2(y^{\frac{p^e+1}{2}} + \frac{1}{2}y) + \frac{1}{4}$, where $y = -x + \frac{1}{4}$. By [13, Theorem 7.11], $y^{\frac{p^e+1}{2}} + \frac{1}{2}y$ is a PP on $\mathbb{F}_{p^e}$ if and only if $\chi((\frac{1}{2})^2 - 1) = 1$, i.e., $\chi(-3) = 1$, where χ is the quadratic character of $\mathbb{F}_{p^e}$. When e is even, $\chi(-3) = 1$ if and only if $p \neq 3$ if and only if $p^e \equiv 1 \pmod 3$. When e is odd, $\chi(-3) = (\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}(\frac{p}{3}) = (\frac{p}{3})$. In this case $\chi(-3) = 1$ if and only if $(\frac{p}{3}) = 1$ if and only if $p \equiv 1 \pmod 3$ if and only if $p^e \equiv 1 \pmod 3$. □

The reversed Dickson PPs in Corollary 5.2(ii) arise from APN functions (Theorem 4.4.II(ii)). However, the reversed Dickson PPs in Corollary 5.2(i), which include the trivial case $D_2(1,x) = -2x+1$, are not obtainable from APN functions through Proposition 4.3 since p^k+1 is even.

Theorem 5.3. *Let e be a positive even integer and let $n = 2^e + 2^k + 1$, where k is a positive integer such that $(k-1, e) = 1$. Then $D_n(1,x)$ is a PP on $\mathbb{F}_{2^e}$.*

Proof. By Proposition 4.2(i), it suffices to show that the mapping $x \mapsto (x+1)^n + x^n$ is 2-to-1 on $\mathbb{F}_{2^e} \cup V$ where $V = \{x \in \mathbb{F}_{2^{2e}} : x^{2^e} = x+1\}$ (see (4)).

Choose $\epsilon \in \mathbb{F}_{2^e}$ such that $\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\epsilon) = 1$ and choose $a \in \mathbb{F}_{2^{2e}}$ such that $a^2 + a = \epsilon$. Then $V = a + \mathbb{F}_{2^e}$.

For $x \in \mathbb{F}_{2^e}$, we have

$$(x+1)^n + x^n = (x+1)^{2^k+2} + x^{2^k+2} = \left[(x+1)^{2^{k-1}+1} + x^{2^{k-1}+1}\right]^2.$$

Since $(k-1, e) = 1$, $x^{2^{k-1}+1}$ is an APN function on $\mathbb{F}_{2^e}$ (the Gold case), so $(x+1)^n + x^n$ is 2-to-1 on $\mathbb{F}_{2^e}$.

Again for $x \in \mathbb{F}_{2^e}$, we have

$$(x+a)^n = \left(x^{2^k} + a^{2^k}\right)(x+a)\left(x+a^{2^e}\right) = \left(x^{2^k} + a^{2^k}\right)(x+a)(x+a+1).$$

(Note that $a^{2^e} = a+1$ since $a \in V$.) Also,

$$(x+1+a)^n = \left((x+1)^{2^k} + a^{2^k}\right)(x+1+a)(x+a).$$

So we have

$$(x+a+1)^n + (x+a)^n = (x+a)(x+a+1) = x^2 + x + \epsilon.$$

Therefore, $(x+1)^n + x^n$ is 2-to-1 on $V = a + \mathbb{F}_{2^e}$.

Note that for $x \in \mathbb{F}_{2^e}$,

$$\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left((x+1)^n + x^n\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left(x^{2^k} + x^2 + 1\right) = 0 \quad (\text{since } e \text{ is even})$$

and

$$\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left((x+a+1)^n + (x+a)^n\right) = \mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}\left(x^2 + x + \epsilon\right) = 1.$$

So, the value sets of $(x+1)^n + x^n$ on $\mathbb{F}_{2^e}$ and on $a + \mathbb{F}_{2^e}$ are disjoint. Therefore, $(x+1)^n + x^n$ is a 2-to-1 mapping on $\mathbb{F}_{2^e} \cup (a + \mathbb{F}_{2^e})$. □

In Theorem 5.3, note that if $l > 0$ is such that $l \equiv k \pmod e$, then $2^e + 2^l + 1$ and $2^e + 2^k + 1$ are in the same 2^e-cyclotomic coset modulo $(2^{2e} - 1)$. Therefore, we may assume that $n = 2^e + 2^k + 1$ where $1 \leqslant k \leqslant e$. If $k = e$, then $n = 2^{e+1} + 1$ and $D_n(1, x)$ arises from an APN function. However, this is the only case in Theorem 5.3 where the reversed Dickson PP arises from an APN function.

Proposition 5.4. *Let $1 \leqslant k < e$ be integers and $n = 2^e + 2^k + 1$. Then x^n is not an APN function on $\mathbb{F}_{2^{2e}}$.*

Proof. Let $\epsilon \in \mathbb{F}_{2^e}$ such that $\mathrm{Tr}_{\mathbb{F}_{2^e}/\mathbb{F}_2}(\epsilon) = 1$ and let $a \in \mathbb{F}_{2^{2e}}$ such that $a^2 + a = \epsilon$. Choose $x_0 \in \mathbb{F}_{2^e}$ such that $x_0^{2^k-1} \neq 1$ and let $u = \frac{x_0^{2^{k-1}} + x_0}{x_0^{2^{k-1}+1}}$. For all $x \in \mathbb{F}_{2^e}$, similar to the computations in the proof of Theorem 5.3, we have

$$\begin{aligned}(x+ua)^n &= \left[x^{2^k}+(ua)^{2^k}\right](x+ua)\left(x+(ua)^{2^e}\right)\\ &= \left[x^{2^k}+(ua)^{2^k}\right](x+ua)\left(x+u(a+1)\right)\\ &= \left[x^{2^k}+(ua)^{2^k}\right]\left(x^2+ux+u^2\epsilon\right),\\ (x+1+ua)^n &= \left[(x+1)^{2^k}+(ua)^{2^k}\right]\left[(x+1)^2+u(x+1)+u^2\epsilon\right]\\ &= \left[x^{2^k}+1+(ua)^{2^k}\right]\left(x^2+ux+u^2\epsilon+u+1\right).\end{aligned}$$

Thus

$$\begin{aligned}&(x+ua+1)^n+(x+ua)^n\\ &= \left[x^{2^k}+(ua)^{2^k}\right]\left(x^2+ux+u^2\epsilon\right)+\left[x^{2^k}+(ua)^{2^k}+1\right]\left(x^2+ux+u^2\epsilon+u+1\right)\\ &= (u+1)\left[x^{2^k}+(ua)^{2^k}\right]+x^2+ux+u^2\epsilon+u+1\\ &= (u+1)x^{2^k}+x^2+ux+u^2\epsilon+(u+1)\left[(ua)^{2^k}+1\right].\end{aligned}$$

The linearized polynomial $(u+1)x^{2^k}+x^2+ux$ has at least three roots in $\mathbb{F}_{2^e}$: 0, 1 and x_0. Thus the mapping $x\mapsto (x+1)^n+x^n$ is not 2-to-1 on $ua+\mathbb{F}_{2^e}\subset\mathbb{F}_{2^{2e}}$. □

Lemma 5.5. *Let k be a positive odd integer and let $n=\frac{3^k+1}{2}$. Then in $\mathbb{F}_3[x]$,*

$$D_n\left(1,1-x^2\right)=-D_n(x,1).$$

Proof. Let $x=y^2+y^{-2}$. Then

$$\begin{aligned}D_n\left(1,1-x^2\right) &= D_n\left(1,(2+x)(2-x)\right)\\ &= (2+x)^n+(2-x)^n\\ &= \left(y+y^{-1}\right)^{2n}+\left(y-y^{-1}\right)^{2n}\quad\text{(since } n \text{ is even)}\\ &= \left(y+y^{-1}\right)^{3^k+1}+\left(y-y^{-1}\right)^{3^k+1}\\ &= 2y^{3^k+1}+2y^{-(3^k+1)}\\ &= -\left[\left(y^2\right)^n+\left(y^{-2}\right)^n\right]\\ &= -D_n(x,1).\qquad\square\end{aligned}$$

Let $n\geqslant 0$ be an integer and let $a\in\mathbb{F}_q$. By (2), we can write

$$D_{2n}(x,a)=F_n\left(x^2,a\right),\tag{7}$$

where

$$F_n(x,a)=\sum_{i=0}^{n}\frac{2n}{2n-i}\binom{2n-i}{i}(-a)^i x^{n-i}\in\mathbb{F}_q[x].$$

Lemma 5.6. *Let $n>0$ be an integer such that $(n,p^{4e}-1)=2$ and let $a\in\mathbb{F}_{p^e}^*$. Then $F_{\frac{n}{2}}(x,a)$ is a PP on $\mathbb{F}_{p^e}$.*

Proof. Assume $x_1, x_2 \in \mathbb{F}_{p^e}$ such that $F_{\frac{n}{2}}(x_1, a) = F_{\frac{n}{2}}(x_2, a)$. Write $x_1 = y_1^2$, $x_2 = y_2^2$ for some $y_1, y_2 \in \mathbb{F}_{p^{2e}}$. Further write $y_1 = z_1 + \frac{a}{z_1}$ and $y_2 = z_2 + \frac{a}{z_2}$ for some $z_1, z_2 \in \mathbb{F}_{p^{4e}}^*$. Then we have

$$z_1^n + \left(\frac{a}{z_1}\right)^n = D_n(y_1, a) = F_{\frac{n}{2}}(x_1, a) = F_{\frac{n}{2}}(x_2, a) = D_n(y_2, a) = z_2^n + \left(\frac{a}{z_2}\right)^n.$$

Thus $z_1^n = z_2^n$ or $z_1^n = (\frac{a}{z_2})^n$. Since $(n, p^{4e} - 1) = 2$, we have $z_1 = \pm z_2$ or $z_1 = \pm\frac{a}{z_2}$. It follows that $y_1 = \pm y_2$, so $x_1 = x_2$. □

Theorem 5.7. *Let $k > 0$ be an integer such that $(k, 2e) = 1$ and let $n = \frac{3^k+1}{2}$. Then $D_n(1, x)$ is a PP on $\mathbb{F}_{3^e}$.*

Proof. By [4, Lemma 2.6], $(n, 3^{4e} - 1) = 2$. So by Lemma 5.6, $F_{\frac{n}{2}}(x, 1)$ is a PP on $\mathbb{F}_{3^e}$. By (7) and Lemma 5.5, we have $F_{\frac{n}{2}}(x^2, 1) = D_n(x, 1) = -D_n(1, 1 - x^2)$. Hence $F_{\frac{n}{2}}(x, 1) = -D_n(1, 1 - x)$. Therefore $D_n(1, x)$ is a PP on $\mathbb{F}_{3^e}$. □

The reversed Dickson PP in Theorem 5.7 does not arise from an APN function since n is even.

6. Necessary conditions for $D_n(1, x)$ to be a PP

In this section we explore some necessary conditions on n for $D_n(1, x)$ to be a PP on $\mathbb{F}_{p^e}$.

First note that $D_n(1, 0) = 1$ for all $n \geqslant 1$. The values $D_n(1, 1)$, $n = 0, 1, \ldots$, can also be easily determined. From the recursive equation

$$\begin{cases} D_0(1, 1) = 2, \\ D_1(1, 1) = 1, \\ D_n(1, 1) = D_{n-1}(1, 1) - D_{n-2}(1, 1), \quad n \geqslant 2, \end{cases}$$

we have $(D_2(1, 1), \ldots, D_6(1, 1), D_7(1, 1)) = (-1, -2, -1, 1, 2, 1)$. So the sequence $\{D_n(1, 1): n = 0, 1, \ldots\}$ has period 6 and

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

Proposition 6.1. *Assume that $D_n(1, x)$ is a PP on $\mathbb{F}_{p^e}$. If $p = 2$, then $3 \mid n$. If $p = 3$ then $2 \mid n$. If $p > 3$, then $(n, 6) \neq 1$.*

Proof. Compare $D_n(1, 0)$ and $D_n(1, 1)$. □

Corollary 6.2. *Assume that x^n is an APN function on $\mathbb{F}_{p^{2e}}$. If $p = 2$, then $3 \mid n$. If $p = 3$ then $2 \mid n$. If $p > 3$, then $(n, 6) \neq 1$. In particular, x^n is not a permutation of $\mathbb{F}_{p^{2e}}$.*

Proposition 6.3. *Assume that $D_n(1, x)$ is a PP on $\mathbb{F}_{p^e}$. Then for every $a \in \mathbb{F}_{p^{2e}} \setminus \{0, 1\}$ such that $a(1 - a) \in \mathbb{F}_{p^e}$ and for every $k \geqslant 0$, we have*

$$n \not\equiv p^k \pmod{\operatorname{lcm}\big(o(a), o(1 - a)\big)},$$

where $o(a)$ is the multiplicative order of a in $\mathbb{F}_{p^{2e}}^*$.

Proof. Assume to the contrary that $n \equiv p^k \pmod{\operatorname{lcm}(o(a), o(1-a))}$ for some $k \geqslant 0$ and $a \in \mathbb{F}_{p^{2e}} \setminus \{0, 1\}$ such that $a(1-a) \in \mathbb{F}_{p^e}$. Then $a(1-a) \neq 0$ but

$$D_n\big(1, a(1-a)\big) = a^n + (1-a)^n = a^{p^k} + (1-a)^{p^k} = 1 = D_n(1, 0),$$

which is a contradiction. □

For each prime power p^e, we define

$$\mathcal{L}\big(p^e\big) = \big\{\operatorname{lcm}\big(o(a), o(1-a)\big) \colon a \in \mathbb{F}_{p^{2e}} \setminus \{0, 1\},\ a(1-a) \in \mathbb{F}_{p^e}\big\}.$$

Note that if $a \in \mathbb{F}_{p^{2e}} \setminus \mathbb{F}_{p^e}$ with $\operatorname{Tr}_{\mathbb{F}_{p^{2e}}/\mathbb{F}_{p^e}}(a) = a^{p^e} + a = 1$, then $a(1-a) \in \mathbb{F}_{p^e}$ and $o(a) = o(1-a)$, so that $o(a) \in \mathcal{L}(p^e)$. Also note that if p is odd, then $o(\frac{1}{2}) = o(2) \in \mathcal{L}(p^e)$. Consider $\mathcal{L}(p^e)$ as a partially ordered set with divisibility as the relation. Let $\mathcal{L}_0(p^e)$ denote the set of minimal elements in $\mathcal{L}(p^e)$. Then Proposition 6.3 can be restated as follows.

Proposition 6.3′. *Assume that $D_n(1, x)$ is a PP on $\mathbb{F}_{p^e}$. Then for every $l \in \mathcal{L}_0(p^e)$ and $k \geqslant 0$, $n \not\equiv p^k \pmod{l}$.*

The determination of the set $\mathcal{L}_0(p^e)$ seems to be an interesting problem. In Table 1 we list the elements of $\mathcal{L}_0(p^e)$ for $p^e < 200$.

7. Numerical results: Reversed Dickson PPs on $\mathbb{F}_{p^e}$ with $p^e < 200$

We did a computer search for all reversed Dickson PPs on $\mathbb{F}_{p^e}$ with $p^e < 200$. The results are compiled in Table 2. With only one exception, all entries in Table 2 are covered by Theorem 4.4, Corollary 5.2, Theorem 5.3 and Theorem 5.7. The exceptional entry has $p^e = 3^4$ and $n = 86$. Table 2 suggests that the occurrence of reversed Dickson PPs on $\mathbb{F}_{p^e}$ is highly predictable, especially when $e = 1$. We make the following conjecture based on the evidence in Table 2.

Conjecture 7.1. *Let $p > 3$ be a prime and let $1 \leqslant n \leqslant p^2 - 1$. Then $D_n(1, x)$ is a PP on $\mathbb{F}_p$ if and only if*

$$n = \begin{cases} 2, 2p, 3, 3p, p+1, p+2, 2p+1 & \text{if } p \equiv 1 \pmod{12}, \\ 2, 2p, 3, 3p, p+1 & \text{if } p \equiv 5 \pmod{12}, \\ 2, 2p, 3, 3p, p+2, 2p+1 & \text{if } p \equiv 7 \pmod{12}, \\ 2, 2p, 3, 3p & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

We note that if n is one of the above values, then our previous work shows that $D_n(1, x)$ is indeed a PP on the field $\mathbb{F}_p$. Moreover, from the discussion at the beginning of Section 6, we know that if $n \equiv 1, 5 \pmod 6$, then $D_n(1, 0) = D_n(1, 1) = 1$ so that $D_n(1, x)$ is not a PP on $\mathbb{F}_p$.

Appendix A. Proofs of Theorems 3.1 and 3.2

In the proofs that follow, we will frequently make use of Lucas's theorem on the congruence of binomial coefficients. Let p be a prime and let $\alpha, \beta \geqslant 0$ be two integers with p-adic expansions $\alpha = \alpha_0 p^0 + \alpha_1 p^1 + \cdots$, $\beta = \beta_0 p^0 + \beta_1 p^1 + \cdots$, $0 \leqslant \alpha_i, \beta_i \leqslant p - 1$. Lucas's theorem states that

$$\binom{\alpha}{\beta} \equiv \binom{\alpha_0}{\beta_0}\binom{\alpha_1}{\beta_1}\cdots \pmod{p}.$$

We start with a technical lemma.

Table 1
Elements of $\mathcal{L}_0(p^e)$, $p^e < 200$.

p^e	Elements of $\mathcal{L}_0(p^e)$	$p^{2e}-1$
2	3	3
2^2	3	$3\cdot 5$
2^3	3, 7	$3^2\cdot 7$
2^4	3, $5\cdot 17$	$3\cdot 5\cdot 17$
2^5	3, 31	$3\cdot 11\cdot 31$
2^6	3, 7	$3^3\cdot 5\cdot 7\cdot 13$
2^7	3, 127	$3\cdot 43\cdot 127$
3	2	2^3
3^2	2	$2^4\cdot 5$
3^3	2, 13	$2^3\cdot 7\cdot 13$
3^4	2	$2^5\cdot 5\cdot 41$
5	2^2, $2\cdot 3$	$2^3\cdot 3$
5^2	2^2, $2\cdot 3$	$2^4\cdot 3\cdot 13$
5^3	2^2, $2\cdot 3$, 31	$2^3\cdot 3^2\cdot 7\cdot 31$
7	3, 2^4	$2^4\cdot 3$
7^2	3, 2^4, $2^3\cdot 5^2$	$2^5\cdot 3\cdot 5^2$
11	5, $2\cdot 3$	$2^3\cdot 3\cdot 5$
11^2	5, $2\cdot 3$, $3\cdot 61$, $2^3\cdot 61$	$2^4\cdot 3\cdot 5\cdot 61$
13	$2\cdot 3$, $2^2\cdot 7$	$2^3\cdot 3\cdot 7$
13^2	$2\cdot 3$, $2^2\cdot 7$, $3\cdot 7\cdot 17$, $5\cdot 7\cdot 17$, $2^4\cdot 5\cdot 17$	$2^4\cdot 3\cdot 5\cdot 7\cdot 17$
17	$2\cdot 3$, 2^3	$2^5\cdot 3^2$
19	$2\cdot 3$, 3^2	$2^3\cdot 3^2\cdot 5$
23	$2\cdot 3$, 11	$2^4\cdot 3\cdot 11$
29	$2\cdot 3$, 7	$2^3\cdot 3\cdot 5\cdot 7$
31	5, $2\cdot 3$	$2^6\cdot 3\cdot 5$
37	$2\cdot 3$, 3^2, $3\cdot 19$, $2^2\cdot 19$	$2^3\cdot 3^2\cdot 19$
41	$2\cdot 3$, $2^2\cdot 5$, $5\cdot 7$, $2^3\cdot 7$	$2^4\cdot 3\cdot 5\cdot 7$
43	$2\cdot 3$, $2\cdot 7$, $3\cdot 7$, $3\cdot 11$, $7\cdot 11$, $2^3\cdot 11$	$2^3\cdot 3\cdot 7\cdot 11$
47	$2\cdot 3$, 23, 2^5	$2^5\cdot 3\cdot 23$
53	$2\cdot 3$, 13	$2^3\cdot 3^3\cdot 13$
59	$2\cdot 3$, 29	$2^3\cdot 3\cdot 5\cdot 29$
61	$2\cdot 3$, $3\cdot 5$, $2^2\cdot 5$, $3\cdot 31$, $5\cdot 31$, $2^3\cdot 31$	$2^3\cdot 3\cdot 5\cdot 31$
67	$2\cdot 3$, 11, $2^3\cdot 17$	$2^3\cdot 3\cdot 11\cdot 17$
71	$2\cdot 3$, $5\cdot 7$, $2^4\cdot 5$	$2^4\cdot 3^2\cdot 5\cdot 7$
73	$2\cdot 3$, 3^2, $2^2\cdot 37$	$2^4\cdot 3^2\cdot 37$
79	$2\cdot 3$, 13	$2^5\cdot 3\cdot 5\cdot 13$
83	$2\cdot 3$, 41	$2^3\cdot 3\cdot 7\cdot 41$
89	$2\cdot 3$, 11, $2^4\cdot 5$	$2^4\cdot 3^2\cdot 5\cdot 11$
97	$2\cdot 3$, 2^5, $2^2\cdot 7^2$	$2^6\cdot 3\cdot 7^2$
101	$2\cdot 3$, 5^2, $2^3\cdot 17$, $2\cdot 5\cdot 17$, $3\cdot 5\cdot 17$	$2^3\cdot 3\cdot 5^2\cdot 17$
103	$2\cdot 3$, 17, $3\cdot 13$, $2^4\cdot 13$	$2^4\cdot 3\cdot 13\cdot 17$
107	$2\cdot 3$, 53	$2^3\cdot 3^3\cdot 53$
109	$2\cdot 3$, 3^3, $2^3\cdot 5\cdot 11$, $3^2\cdot 5\cdot 11$	$2^3\cdot 3^3\cdot 5\cdot 11$
113	$2\cdot 3$, $2^2\cdot 7$, $2^2\cdot 19$, $2\cdot 7\cdot 19$, $3\cdot 7\cdot 19$	$2^5\cdot 3\cdot 7\cdot 19$
127	$2\cdot 3$, 7, 2^8	$2^8\cdot 3^2\cdot 7$
131	$2\cdot 3$, 13, $2\cdot 5\cdot 11$	$2^3\cdot 3\cdot 5\cdot 11\cdot 13$
137	$2\cdot 3$, 17	$2^4\cdot 3\cdot 17\cdot 23$
139	$2\cdot 3$, 23, $3\cdot 5\cdot 7$	$2^3\cdot 3\cdot 5\cdot 7\cdot 23$
149	$2\cdot 3$, 37	$2^3\cdot 3\cdot 5^2\cdot 37$
151	$2\cdot 3$, $3\cdot 5$, 5^2, $5\cdot 19$	$2^4\cdot 3\cdot 5^2\cdot 19$
157	$2\cdot 3$, $3\cdot 13$, $2^2\cdot 13$, $3\cdot 79$, $2^2\cdot 79$, $13\cdot 79$	$2^3\cdot 3\cdot 13\cdot 79$
163	$2\cdot 3$, 3^3, $2^3\cdot 41$, $3^2\cdot 41$	$2^3\cdot 3^4\cdot 41$
167	$2\cdot 3$, 83	$2^4\cdot 3\cdot 7\cdot 83$
173	$2\cdot 3$, 43, $2^3\cdot 29$	$2^3\cdot 3\cdot 29\cdot 43$
179	$2\cdot 3$, 89	$2^3\cdot 3^2\cdot 5\cdot 89$
181	$2\cdot 3$, $3^2\cdot 5$, $3^2\cdot 7$, $3\cdot 5\cdot 13$, $2^3\cdot 5\cdot 7$, $5\cdot 7\cdot 13$, $2^3\cdot 5\cdot 13$, $2^3\cdot 7\cdot 13$	$2^3\cdot 3^2\cdot 5\cdot 7\cdot 13$
191	$2\cdot 3$, 19, $2^6\cdot 5$	$2^7\cdot 3\cdot 5\cdot 19$
193	$2\cdot 3$, 2^5, $3\cdot 97$, $2^2\cdot 97$	$2^7\cdot 3\cdot 97$
197	$2\cdot 3$, $2^2\cdot 7$, 7^2, $3^2\cdot 7$	$2^3\cdot 3^2\cdot 7^2\cdot 11$
199	$2\cdot 3$, 11	$2^4\cdot 3^2\cdot 5^2\cdot 11$

Table 2
Reversed Dickson PPs $D_n(1, x)$ on $\mathbb{F}_{p^e}$, $p^e < 200$.

p^e	n	Cyclotomic coset mod $p^{2e} - 1$	Reference
2	3	3	Theorem 4.4.I(i)
2^2	3	3, 6, 12, 9	Theorem 4.4.I(i)
2^3	3	3, 6, 12, 24, 48, 33	Theorem 4.4.I(i)
2^4	3	3, 6, 12, 24, 48, 96, 192, 129	Theorem 4.4.I(i)
	9	9, 18, 36, 72, 144, 33, 66, 132	Theorem 4.4.I(i)
	21	21, 42, 84, 168, 81, 162, 69, 138	Theorem 5.3
	39	39, 78, 156, 57, 114, 228, 201, 147	Theorem 4.4.I(ii)
2^5	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 513	Theorem 4.4.I(i)
	9	9, 18, 36, 72, 144, 288, 576, 129, 258, 516	Theorem 4.4.I(i)
	57	57, 114, 228, 456, 912, 801, 579, 135, 270, 540	Theorem 4.4.I(ii)
	213	213, 426, 825, 681, 339, 678, 333, 666, 309, 618	Theorem 4.4.I(iii)
2^6	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 1563, 3072, 2049	Theorem 4.4.I(i)
	33	33, 66, 132, 264, 528, 1056, 2112, 129, 258, 516, 1032, 2064	Theorem 4.4.I(i)
	69	69, 138, 276, 552, 1104, 2208, 321, 642, 1284, 2568, 1041, 2082	Theorem 5.3
	159	159, 318, 636, 1272, 2544, 993, 1986, 3972, 3849, 3603, 3111, 2127	Theorem 4.4.I(ii)
2^7	3	3, 6, 12, 24, 48, 96, 192, 384, 768, 1563, 3072, 6144, 12288, 8193	Theorem 4.4.I(i)
	9	9, 18, 36, 72, 144, 288, 576, 1152, 2304, 4608, 9216, 2049, 4098, 8196	Theorem 4.4.I(i)
	33	33, 66, 132, 264, 528, 1056, 2112, 4224, 8448, 513, 1026, 2052, 4104, 8208	Theorem 4.4.I(i)
	57	57, 114, 228, 456, 912, 1824, 3648, 7296, 14592, 12801, 9219, 2055, 4110, 8220	Theorem 4.4.I(ii)
	543	543, 1086, 2172, 4344, 8688, 993, 1986, 3972, 7944, 15888, 15393, 14403, 12423, 8463	Theorem 4.4.I(ii)
3	2	2, 6	Corollary 5.2(i)
3^2	2	2, 6, 18, 54	Corollary 5.2(i)
	10	10, 30	Corollary 5.2(i)
	14	14, 42, 46, 58	Theorem 5.7
3^3	2	2, 6, 18, 54, 162, 486	Corollary 5.2(i)
	10	10, 30, 90, 270, 82, 246	Corollary 5.2(i)
	122	122, 366, 370, 382, 418, 526	Theorem 5.7
3^4	2	2, 6, 18, 54, 162, 486, 1458, 4374	Corollary 5.2(i)
	14	14, 42, 126, 378, 1134, 3402, 3646, 4378	Theorem 5.7
	82	82, 246, 738, 2214	Corollary 5.2(i)
	86	86, 258, 774, 2322, 406, 1218, 3654, 4402	?
	122	122, 366, 1098, 3294, 3322, 3406, 3658, 4414	Theorem 5.7
	1094	1094, 3282, 3286, 3298, 3334, 3442, 3766, 4738	Theorem 5.7
5	2	2, 10	Corollary 5.2(i)
	3	3, 15	Theorem 4.4.II(i)
	6	6	Corollary 5.2(i)
5^2	2	2, 10, 50, 250	Corollary 5.2(i)
	3	3, 15, 75, 375	Theorem 4.4.II(i)
	26	26, 130	Corollary 5.2(i)
	27	27, 135, 51, 255	Theorem 4.4.II(ii)
	63	63, 315, 327, 387	Theorem 4.4.II(iii)
5^3	2	2, 10, 50, 250, 1250, 6250	Corollary 5.2(i)
	3	3, 15, 75, 375, 1875, 9375	Theorem 4.4.II(i)
	6	6, 30, 150, 750, 3750, 3126	Corollary 5.2(i)
	26	26, 130, 650, 3250, 626, 3130	Corollary 5.2(i)
	126	126, 630, 3150	Corollary 5.2(i)
	1536	1563, 7815, 7827, 7887, 8187, 9687	Theorem 4.4.II(iii)
7	2	2, 14	Corollary 5.2(i)
	3	3, 21	Theorem 4.4.II(i)
	9	9, 15	Theorem 4.4.II(ii)
7^2	2	2, 14, 98, 686	Corollary 5.2(i)
	3	3, 21, 147, 1029	Theorem 4.4.II(i)
	50	50, 350	Corollary 5.2(i)
	51	51, 357, 99, 693	Theorem 4.4.II(ii)

Table 2 (*continued*)

p^e	n	Cyclotomic coset mod $p^{2e}-1$	Reference
11	2	2, 22	Corollary 5.2(i)
	3	3, 33	Theorem 4.4.II(i)
11^2	2	2, 22, 242, 2662	Corollary 5.2(i)
	3	3, 33, 363, 3993	Theorem 4.4.II(i)
	122	122, 1342	Corollary 5.2(i)
	123	123, 1353, 243, 2673	Theorem 4.4.II(i)
13	2	2, 26	Corollary 5.2(i)
	3	3, 39	Theorem 4.4.II(i)
	14	14	Corollary 5.2(i)
	15	15, 17	Theorem 4.4.II(ii)
13^2	2	2, 26, 338, 4394	Corollary 5.2(i)
	3	3, 39, 507, 6591	Theorem 4.4.II(i)
	170	170, 2210	Corollary 5.2(i)
	171	171, 2223, 339, 4407	Theorem 4.4.II(ii)

$e = 1$, $17 \leqslant p \leqslant 199$

p	n	Cyclotomic coset mod p^2-1	Reference
$p \equiv -1 \pmod{12}$	2	2, $2p$	Corollary 5.2(i)
	3	3, $3p$	Theorem 4.4.II(i)
$p \equiv 5 \pmod{12}$	2	2, $2p$	Corollary 5.2(i)
	3	3, $3p$	Theorem 4.4.II(i)
	$p+1$	$p+1$	Corollary 5.2(i)
$p \equiv 7 \pmod{12}$	2	2, $2p$	Corollary 5.2(i)
	3	3, $3p$	Theorem 4.4.II(i)
	$p+2$	$p+2$, $2p+1$	Theorem 4.4.II(ii)
$p \equiv 1 \pmod{12}$	2	2, $2p$	Corollary 5.2(i)
	3	3, $3p$	Theorem 4.4.II(i)
	$p+1$	$p+1$	Corollary 5.2(i)
	$p+2$	$p+2$, $2p+1$	Theorem 4.4.II(ii)

Lemma A.1. *Let* $n_1 = \alpha_1 + \beta_1 p^e$, $n_2 = \alpha_2 + \beta_2 p^e$, $0 \leqslant \alpha_1, \alpha_2, \beta_1, \beta_2 \leqslant p^e - 1$. *Then*

$$D_{n_1}(1, x) \equiv D_{n_2}(1, x) \pmod{x^{p^e} - x} \tag{8}$$

if and only if

$$x^{\alpha_1+\beta_1} + (1-x)^{\alpha_1+\beta_1} \equiv x^{\alpha_2+\beta_2} + (1-x)^{\alpha_2+\beta_2} \pmod{x^{p^e} - x} \tag{9}$$

and

$$x^{\alpha_1}(1-x)^{\beta_1} + x^{\beta_1}(1-x)^{\alpha_1} \equiv x^{\alpha_2}(1-x)^{\beta_2} + x^{\beta_2}(1-x)^{\alpha_2} \pmod{x^{p^e} + x - 1}. \tag{10}$$

Moreover, (9) *holds if and only if*

(i) $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 0$ *or*
(ii) $\alpha_1 + \beta_1 > 0$, $\alpha_2 + \beta_2 > 0$ *and* $\alpha_1 + \beta_1 \equiv \alpha_2 + \beta_2 \pmod{p^e - 1}$ *or*
(iii) $\alpha_1 + \beta_1 > 0$, $\alpha_2 + \beta_2 > 0$, $\alpha_1 + \beta_1 \equiv p^k$, $\alpha_2 + \beta_2 \equiv p^l \pmod{p^e - 1}$ *for some* $0 \leqslant k, l \leqslant e-1$, $k \neq l$;

(10) *holds if and only if*

$$(-1)^{\beta_1}\binom{\alpha_1}{\alpha_1+\beta_1} + (-1)^{\alpha_1}\binom{\beta_1}{\alpha_1+\beta_1} - (-1)^{\beta_1}\binom{\alpha_1}{\alpha_1+\beta_1-p^e} - (-1)^{\alpha_1}\binom{\beta_1}{\alpha_1+\beta_1-p^e}$$

$$\equiv (-1)^{\beta_2}\binom{\alpha_2}{\alpha_2+\beta_2}+(-1)^{\alpha_2}\binom{\beta_2}{\alpha_2+\beta_2}$$
$$-(-1)^{\beta_2}\binom{\alpha_2}{\alpha_2+\beta_2-p^e}-(-1)^{\alpha_2}\binom{\beta_2}{\alpha_2+\beta_2-p^e} \pmod p \tag{11}$$

and

$$(-1)^{\beta_1}\binom{\alpha_1}{\alpha_1+\beta_1-i}+(-1)^{\alpha_1}\binom{\beta_1}{\alpha_1+\beta_1-i}$$
$$-(-1)^{\beta_1}\binom{\alpha_1+1}{\alpha_1+\beta_1+1-p^e-i}-(-1)^{\alpha_1}\binom{\beta_1+1}{\alpha_1+\beta_1+1-p^e-i}$$
$$\equiv (-1)^{\beta_2}\binom{\alpha_2}{\alpha_2+\beta_2-i}+(-1)^{\alpha_2}\binom{\beta_2}{\alpha_2+\beta_2-i}$$
$$-(-1)^{\beta_2}\binom{\alpha_2+1}{\alpha_2+\beta_2+1-p^e-i}-(-1)^{\alpha_2}\binom{\beta_2+1}{\alpha_2+\beta_2+1-p^e-i} \pmod p,$$
$$1\leqslant i\leqslant p^e-1. \tag{12}$$

Proof. 1° Let $x\in\mathbb{F}_{p^{2e}}$. By Lemma 4.1, $x(1-x)\in\mathbb{F}_{p^e}$ if and only if $x^{p^e}=x$ or $x^{p^e}=1-x$. For $s=1,2$, we have

$$D_{n_s}\big(1,x(1-x)\big)=x^{n_s}+(1-x)^{n_s}=\begin{cases}x^{\alpha_s+\beta_s}+(1-x)^{\alpha_s+\beta_s} & \text{if } x^{p^e}=x,\\ x^{\alpha_s}(1-x)^{\beta_s}+x^{\beta_s}(1-x)^{\alpha_s} & \text{if } x^{p^e}=1-x.\end{cases}$$

Hence (8) holds if and only if both (9) and (10) hold.

2° Obviously, any of (i), (ii), (iii) implies (9). Now assume that none of (i), (ii), (iii) is satisfied. We show that (9) fails. If $\alpha_1+\beta_1=0$ but $\alpha_2+\beta_2>0$, then $x^{\alpha_1+\beta_1}+(1-x)^{\alpha_1+\beta_1}=2$ but $x^{\alpha_2+\beta_2}+(1-x)^{\alpha_2+\beta_2}\equiv 1\not\equiv 2 \pmod x$, so (9) fails. Assume $\alpha_1+\beta_1>0$ and $\alpha_2+\beta_2>0$. Write $\alpha_s+\beta_s\equiv\gamma_s \pmod{p^e-1}$ with $1\leqslant\gamma_s\leqslant p^e-1$, $s=1,2$. If γ_1 is a power of p but γ_2 is not a power of p, then

$$x^{\gamma_1}+(1-x)^{\gamma_1}=1\not\equiv x^{\gamma_2}+(1-x)^{\gamma_2} \quad \big(\mathrm{mod}\, x^{p^e}-x\big),$$

so (9) fails. If both γ_1 and γ_2 are not powers of p, write $\gamma_s=a_0^{(s)}p^0+\cdots+a_{e-1}^{(s)}p^{e-1}$, $0\leqslant a_t^{(s)}\leqslant p-1$. Since $\gamma_1\neq\gamma_2$, we have $a_t^{(1)}\neq a_t^{(2)}$ for some $0\leqslant t\leqslant e-1$. The coefficient of x^{p^t} in $x^{\gamma_s}+(1-x)^{\gamma_s}$ is $-a_t^{(s)}$, $s=1,2$. So (9) also fails.

3° For $0\leqslant\alpha,\beta\leqslant p^e-1$, we have

$$x^\alpha(1-x)^\beta$$
$$=x^\alpha\sum_{i=0}^{\beta}(-1)^i\binom{\beta}{i}x^i$$
$$\equiv\sum_{i=0}^{p^e-\alpha-1}(-1)^i\binom{\beta}{i}x^{\alpha+i}+\sum_{i=p^e-\alpha}^{\beta}(-1)^i\binom{\beta}{i}x^{\alpha+i-p^e}(1-x) \quad \big(\mathrm{mod}\, x^{p^e}+x-1\big)$$
$$=\sum_{i=\alpha}^{p^e-1}(-1)^{i-\alpha}\binom{\beta}{i-\alpha}x^i+(1-x)\sum_{i=0}^{\alpha+\beta-p^e}(-1)^{i+p^e-\alpha}\binom{\beta}{i+p^e-\alpha}x^i$$

$$
\begin{aligned}
&= \sum_{i=0}^{p^e-1} (-1)^{i-\alpha} \binom{\beta}{i-\alpha} x^i + \sum_{i=0}^{p^e-2} (-1)^{i+1-\alpha} \binom{\beta}{i+p^e-\alpha} x^i - \sum_{i=1}^{p^e-1} (-1)^{i-\alpha} \binom{\beta}{i+p^e-\alpha-1} x^i \\
&= \sum_{i=0}^{p^e-1} (-1)^{i-\alpha} \binom{\beta}{i-\alpha} x^i + \sum_{i=1}^{p^e-1} (-1)^{i+1-\alpha} \left[\binom{\beta}{i+p^e-\alpha} + \binom{\beta}{i+p^e-\alpha-1} \right] x^i \\
&\quad + (-1)^{1-\alpha} \binom{\beta}{p^e-\alpha} \\
&= (-1)^{-\alpha} \binom{\beta}{-\alpha} + (-1)^{1-\alpha} \binom{\beta}{p^e-\alpha} + \sum_{i=1}^{p^e-1} (-1)^{i-\alpha} \left[\binom{\beta}{i-\alpha} - \binom{\beta+1}{i+p^e-\alpha} \right] x^i \\
&= (-1)^{-\alpha} \binom{\beta}{\alpha+\beta} - (-1)^{-\alpha} \binom{\beta}{\alpha+\beta-p^e} \\
&\quad + \sum_{i=1}^{p^e-1} (-1)^{i-\alpha} \left[\binom{\beta}{\alpha+\beta-i} - \binom{\beta+1}{\alpha+\beta+1-p^e-i} \right] x^i.
\end{aligned}
$$

Hence (10) holds if and only if both (11) and (12) do. □

Proof of Theorem 3.1. The subsets listed in Theorem 3.1 form a partition of $\{0, 1, \ldots, 2^{2e}-1\}$; they will be referred to as "parts". Clearly, if n_1, n_2 belong to the same part, then $n_1 \sim n_2$. Now assume that $n_1 \sim n_2$. We want to show that n_1 and n_2 belong to the same part.

Write $n_s = \alpha_s + \beta_s 2^e$, $0 \leqslant \alpha_s, \beta_s \leqslant 2^e - 1$, $s = 1, 2$. Then one of the conditions (i)–(iii) in Lemma A.1 holds.

Case 1. $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 0$, and we are done.

Case 2. $\alpha_1 + \beta_1 > 0$, $\alpha_2 + \beta_2 > 0$ and $\alpha_1 + \beta_1 \equiv \alpha_2 + \beta_2 \pmod{2^e - 1}$.

Case 2.1. Assume that $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$. Without loss of generality, assume $\alpha_1 = \min\{\alpha_1, \beta_1, \alpha_2, \beta_2\}$. Then by (10), we have

$$
(1-x)^{\beta_1-\alpha_1} + x^{\beta_1-\alpha_1} \equiv x^{\alpha_2-\alpha_1}(1-x)^{\beta_2-\alpha_1} + x^{\beta_2-\alpha_1}(1-x)^{\alpha_2-\alpha_1} \pmod{x^{2^e} + x - 1}.
$$

In the above equation, both sides have degree $\leqslant \beta_1 - \alpha_1 < 2^e$. Thus

$$
(1-x)^{\beta_1-\alpha_1} + x^{\beta_1-\alpha_1} = x^{\alpha_2-\alpha_1}(1-x)^{\beta_2-\alpha_1} + x^{\beta_2-\alpha_1}(1-x)^{\alpha_2-\alpha_1}. \tag{13}
$$

Comparing the x-adic orders of the terms in (13), one can easily see that $(\alpha_1, \beta_1) = (\alpha_2, \beta_2)$ or (β_2, α_2).

Case 2.2. Assume that $\alpha_1 + \beta_1 \neq \alpha_2 + \beta_2$. Without loss of generality, assume $\alpha_1 + \beta_1 = \alpha_2 + \beta_2 + 2^e - 1$. Let $i = \alpha_1 + \beta_1 - 2^e = \alpha_2 + \beta_2 - 1$. Then $0 \leqslant i \leqslant 2^e - 2$. If $i = 0$, then $\alpha_1 + \beta_1 = 2^e$ and $\alpha_2 + \beta_2 = 1$. Then both sides of (10) have degree $< 2^e$. So (10) becomes

$$
x^{\alpha_1}(1-x)^{\beta_1} + x^{\beta_1}(1-x)^{\alpha_1} = x^{\alpha_2}(1-x)^{\beta_2} + x^{\beta_2}(1-x)^{\alpha_2}.
$$

One of α_2 and β_2 is 0 (since $\alpha_2+\beta_2=1$). It follows (by comparing the x-adic orders of the terms in the above equation) that one of α_1 and β_1 is 0, say $\alpha_1=0$. Then $\beta_1=2^e>2^e-1$, which is a contradiction. So $i\geqslant 1$. By (12), we have

$$\binom{\alpha_1+1}{1}+\binom{\beta_1+1}{1}\equiv\binom{\alpha_2}{1}+\binom{\beta_2}{1}\pmod 2,$$

i.e., $\alpha_1+\beta_1\equiv\alpha_2+\beta_2 \pmod 2$, which is a contradiction.

Case 3. $\alpha_1+\beta_1>0$, $\alpha_2+\beta_2>0$, $\alpha_1+\beta_1\equiv 2^k$, $\alpha_2+\beta_2\equiv 2^l \pmod{2^e-1}$ for some $0\leqslant k,l\leqslant e-1$, $k\neq l$.

By considering $2^{e-k}n_1$ and $2^{e-k}n_2$ (modulo $2^{2e}-1$) instead of n_1 and n_2 we may assume $k=0$. (See Proposition 2.1(ii), (iii).) Therefore $\alpha_1+\beta_1=1$ or 2^e.

Case 3.1. Assume $\alpha_1+\beta_1=1$. Then $n_1=1$ or 2^e; in both cases, $D_{n_1}(1,x)=1$. Thus

$$\begin{aligned}D_{n_2 2^{e-l}}(1,x)&=\big[D_{n_2}(1,x)\big]^{2^{e-l}}\\&\equiv\big[D_{n_1}(1,x)\big]^{2^{e-l}}\pmod{x^{2^{2e}}-x}\\&=1\\&=D_{n_1}(1,x).\end{aligned}$$

Note that $n_2 2^{e-l}\equiv\alpha_2'+\beta_2' 2^e \pmod{2^e-1}$, where $0\leqslant\alpha_2',\beta_2'\leqslant 2^e-1$ and $\alpha_2'+\beta_2'\equiv 1 \pmod{2^e-1}$. Thus by Case 2, $n_2 2^{e-l} \pmod{2^e-1}$ and n_1 ($=1$ or 2^e) are in the same part. So $n_2 p^{e-l} \pmod{2^e-1}$ is a power of 2, hence n_2 is a power of 2. Therefore n_2 and n_1 are in the same part.

Case 3.2. Assume $\alpha_1+\beta_1=2^e$. Then $\alpha_2+\beta_2=2^l$ or 2^l+2^e-1.

If $\alpha_2+\beta_2=2^l$, then both sides of (10) have degree $<2^e$, so (10) becomes

$$x^{\alpha_1}(1-x)^{\beta_1}+x^{\beta_1}(1-x)^{\alpha_1}=x^{\alpha_2}(1-x)^{\beta_2}+x^{\beta_2}(1-x)^{\alpha_2}. \tag{14}$$

Without loss of generality, assume $\alpha_2=\min\{\alpha_1,\beta_1,\alpha_2,\beta_2\}$. By comparing the x-adic orders of the terms in (14), we see that $\min\{\alpha_1,\beta_1,\beta_2\}=\alpha_2$. If $\alpha_2=\beta_2$, then (14) becomes $x^{\alpha_1}(1-x)^{\beta_1}+x^{\beta_1}(1-x)^{\alpha_1}=0$, which forces $\alpha_1=\beta_1$. Then $n_1=(2^e+1)2^{e-1}$ and $n_2=(2^e+1)2^{l-1}$, which belong to the same part. If $\alpha_2=\alpha_1$ or β_1, say $\alpha_2=\alpha_1$, then (14) gives

$$(1-x)^{\beta_1-\alpha_1}+x^{\beta_1-\alpha_1}=(1-x)^{\beta_2-\alpha_1}+x^{\beta_2-\alpha_1}.$$

By Lemma A.1(i)–(iii), we have $\beta_1-\alpha_1=\beta_2-\alpha_1$ or both $\beta_1-\alpha_1$ and $\beta_2-\alpha_1$ are powers of 2. If $\beta_1=\beta_2$, then $\alpha_1+\beta_1=\alpha_2+\beta_2$, which is a contradiction. If $\beta_1-\alpha_1=2^u$, $\beta_2-\alpha_1=2^v$, $0\leqslant u,v\leqslant e-1$, $u\neq v$, then

$$2^e-2^u=\alpha_1+\beta_1-(\beta_1-\alpha_1)=2\alpha_1=\alpha_2+\beta_2-(\beta_2-\alpha_1)=2^l-2^v,$$

which is impossible.

So we may assume $\alpha_2+\beta_2=2^l+2^e-1$.

We claim that $\alpha_2<2^e-1$ and $\beta_2<2^e-1$. Assume to the contrary that $\alpha_2=2^e-1$ and $\beta_2=2^l$. Then by (11), we have

$$0 \equiv \binom{2^e-1}{2^l-1} + \binom{2^l}{2^l-1} \pmod 2,$$

which is a contradiction. So the claim is proved.

Letting $i = 2^l$ in (12), we get

$$\binom{\alpha_1}{2^e-2^k} + \binom{\beta_1}{2^e-2^l} \equiv 0 \pmod 2. \tag{15}$$

Letting $i = 2^l - 1$ in (12), we have

$$\binom{\alpha_1}{2^e-2^l+1} + \binom{\beta_1}{2^e-2^l+1} \equiv \binom{\alpha_2+1}{1} + \binom{\beta_2+1}{1} \equiv 1 \pmod 2.$$

Without loss of generality, assume $\binom{\alpha_1}{2^e-2^l+1} \equiv 1 \pmod 2$.

In the following, the notation 0 under 1 denotes the fact that 1 is the coefficient of 2^0 and similarly, and l under 1 denotes the fact that 1 is the coefficient of 2^l.

Since

$$2^e - 2^l + 1 = (\underset{0}{1}\ 0 \cdots 0\ \underset{l}{1} \cdots 1)P,$$

where

$$P = \begin{bmatrix} 2^0 \\ \vdots \\ 2^{e-1} \end{bmatrix},$$

we must have

$$\alpha_1 = (\underset{0}{1}, a_1, \ldots, a_{l-1}, \underset{l}{1}, \ldots, 1)P, \quad a_1, \ldots, a_{l-1} \in \{0, 1\}. \tag{16}$$

Since $\alpha_1 + \beta_1 = 2^e$, we have

$$\beta_1 = (\underset{0}{1}, 1 - a_1, \ldots, 1 - a_{l-1}, \underset{l}{0}, \ldots, 0)P. \tag{17}$$

Since

$$2^e - 2^l = (\underset{0}{0} \cdots 0\ \underset{l}{1} \cdots 1)P,$$

it follows from (16) and (17) that

$$\binom{\alpha_1}{2^e-2^l} + \binom{\beta_1}{2^e-2^l} \equiv 1 \pmod 2,$$

which is a contradiction to (15). □

Proof of Theorem 3.2. The subsets listed in Theorem 3.2 form a partition of $\{0, 1, \ldots, p^{2e} - 1\}$; they will be referred to as "parts". Clearly, if n_1, n_2 belong the same part, then $n_1 \sim n_2$. Now assume that $n_1 \sim n_2$. We want to show that n_1 and n_2 belong to the same part.

Write $n_s = \alpha_s + \beta_s p^e$, $0 \leqslant \alpha_s, \beta_s \leqslant p^e - 1$. Then one of the conditions (i)–(iii) in Lemma A.1 holds.

Case 1. $\alpha_1 = \beta_1 = \alpha_2 = \beta_2 = 0$, and we are done.

Case 2. $\alpha_1 + \beta_1 > 0$, $\alpha_2 + \beta_2 > 0$ and $\alpha_1 + \beta_1 \equiv \alpha_2 + \beta_2 \pmod{p^e - 1}$.

Case 2.1. Assume that $\alpha_1 + \beta_1 = \alpha_2 + \beta_2$. The proof is the same as in the $p = 2$ case (proof of Theorem 3.1, Case 2.1).

Case 2.2. Assume that $\alpha_1 + \beta_1 \neq \alpha_2 + \beta_2$. Without loss of generality, assume $\alpha_1 + \beta_1 = \alpha_2 + \beta_2 + p^e - 1$. Let $i_0 = \alpha_1 + \beta_1 - p^e = \alpha_2 + \beta_2 - 1$. Then $0 \leqslant i_0 \leqslant p^e - 2$. By the same argument in the $p = 2$ case (proof of Theorem 3.1, Case 2.2), we have $i_0 > 0$. Letting $i = i_0$ in (12), we have

$$-(-1)^{\beta_1}(\alpha_1 + 1) - (-1)^{\alpha_1}(\beta_1 + 1) \equiv (-1)^{\beta_2}\alpha_2 + (-1)^{\alpha_2}\beta_2 \pmod{p}. \tag{18}$$

Letting $i = i_0 + 1$ in (12), we have

$$(-1)^{\beta_1}\binom{\alpha_1}{p^e - 1} + (-1)^{\alpha_1}\binom{\beta_1}{p^e - 1} - (-1)^{\beta_1} - (-1)^{\alpha_1} \equiv (-1)^{\beta_2} + (-1)^{\alpha_2} \pmod{p}. \tag{19}$$

We claim that $\alpha_1 < p^e - 1$ and $\beta_1 < p^e - 1$. Assume to the contrary that $\alpha_1 = p^e - 1$. If $\beta_1 = p^e - 1$, then $\alpha_2 + \beta_2 = \alpha_1 + \beta_1 - (p^e - 1) = p^e - 1$ is even. By (18), we have $\alpha_2 + \beta_2 \equiv 0 \pmod{p}$, which is false since $\alpha_2 + \beta_2 = p^e - 1$. So $\beta_1 < p^e - 1$. Now (19) gives

$$-1 \equiv (-1)^{\beta_2} + (-1)^{\alpha_2} \pmod{p}.$$

Thus $p = 3$ and both α_2 and β_2 are even. Since $\alpha_2 + \beta_2 = \beta_1 < p^e - 1$, we have $\alpha_2 + \beta_2 \leqslant p^e - 3$. We have

$$\begin{aligned}
&(1 - x)^{\alpha_2+\beta_2+2} + x^{\alpha_2+\beta_2+2} \\
&\quad \equiv x^{p^e}(1 - x)^{\alpha_2+\beta_2+1} + x^{\alpha_2+\beta_2+1}(1 - x)^{p^e} \pmod{x^{p^e} + x - 1} \\
&\quad = x(1 - x)\left[x^{\alpha_1}(1 - x)^{\beta_1} + x^{\beta_1}(1 - x)^{\alpha_1}\right] \\
&\quad \equiv x(1 - x)\left[x^{\alpha_2}(1 - x)^{\beta_2} + x^{\beta_2}(1 - x)^{\alpha_2}\right] \pmod{x^{p^e} + x - 1} \quad (\text{by } (10)) \\
&\quad = x^{\alpha_2+1}(1 - x)^{\beta_2+1} + x^{\beta_2+1}(1 - x)^{\alpha_2+1}.
\end{aligned}$$

Since $\alpha_2 + \beta_2 + 2 \leqslant p^e - 1$, we must have

$$(1 - x)^{\alpha_2+\beta_2+2} + x^{\alpha_2+\beta_2+2} = x^{\alpha_2+1}(1 - x)^{\beta_2+1} + x^{\beta_2+1}(1 - x)^{\alpha_2+1},$$

which is clearly false. Thus the claim is proved.

Now Eq. (19) becomes

$$-(-1)^{\beta_1} - (-1)^{\alpha_1} \equiv (-1)^{\beta_2} + (-1)^{\alpha_2} \pmod{p}. \tag{20}$$

We claim that $\alpha_1+\beta_1$ is odd. Assume to the contrary that $\alpha_1+\beta_1$ is even. Then by (20), we have $\beta_2=\alpha_2\equiv\beta_1+1 \pmod 2$. Thus we have

$$\begin{aligned}\alpha_1+\beta_1+2&\equiv\alpha_2+\beta_2 \pmod p \quad \big(\text{by (18)}\big)\\ &=\alpha_1+\beta_1-p^e+1,\end{aligned}$$

which is a contradiction. So the claim is proved. It follows from (20) that $\alpha_2+\beta_2$ is also odd.

Now Eq. (18) becomes

$$-(-1)^{\beta_1}\alpha_1-(-1)^{\alpha_1}\beta_1\equiv(-1)^{\beta_2}\alpha_2+(-1)^{\alpha_2}\beta_2 \pmod p. \tag{21}$$

Let $i=i_0-1$ in (12). (Note that $i_0-1\geqslant 1$ since $i_0=\alpha_2+\beta_2-1$ is positive and even.) We have

$$-(-1)^{\beta_1}\binom{\alpha_1+1}{2}-(-1)^{\alpha_1}\binom{\beta_1+1}{2}\equiv(-1)^{\beta_2}\binom{\alpha_2}{2}+(-1)^{\alpha_2}\binom{\beta_2}{2} \pmod p,$$

i.e.,

$$\begin{aligned}&-(-1)^{\beta_1}(\alpha_1+1)\alpha_1-(-1)^{\alpha_1}(\beta_1+1)\beta_1\\ &\quad\equiv(-1)^{\beta_2}\alpha_2(\alpha_2-1)+(-1)^{\alpha_2}\beta_2(\beta_2-1) \pmod p.\end{aligned} \tag{22}$$

We claim that $\alpha_1\equiv\beta_1 \pmod p$ and $\alpha_2\equiv\beta_2 \pmod p$. In (21) and (22), we may assume without loss of generality that $\beta_1\equiv\alpha_2 \pmod 2$. Then (21) becomes $\alpha_1-\beta_1\equiv\alpha_2-\beta_2 \pmod p$. On the other hand, $\alpha_1+\beta_1\equiv\alpha_2+\beta_2-1 \pmod p$. So $2\alpha_1\equiv 2\alpha_2-1 \pmod p$, i.e., $\alpha_1+\frac{1}{2}\equiv\alpha_2 \pmod p$. It follows that $\beta_1+\frac{1}{2}\equiv\beta_2 \pmod p$. Meanwhile, Eq. (22) gives

$$\left(\alpha_1+\frac{1}{2}\right)^2-\left(\beta+\frac{1}{2}\right)^2\equiv\alpha_2^2-\alpha_2-\beta_2^2+\beta_2 \pmod p.$$

Thus we have $\alpha_2\equiv\beta_2 \pmod p$, from which we also have $\alpha_1\equiv\beta_1 \pmod p$. For $s=1,2$, write

$$\begin{aligned}\alpha_s&=a_0^{(s)}+a_1^{(s)}p+\cdots+a_{e-1}^{(s)}p^{e-1},\\ \beta_s&=b_0^{(s)}+b_1^{(s)}p+\cdots+b_{e-1}^{(s)}p^{e-1},\end{aligned}$$

where $a_j^{(s)},b_j^{(s)}\in\{0,\ldots,p-1\}$, $1\leqslant s\leqslant 2$, $0\leqslant j\leqslant e-1$. Then we have

$$a_0^{(s)}=b_0^{(s)},\quad s=1,2. \tag{23}$$

Now consider $n_1'=n_1p$ and $n_2'=n_2p$ instead of n_1 and n_2. Note that for $s=1,2$, $n_s'\equiv\alpha_s'+\beta_s'p^e \pmod{p^{2e}-1}$, where

$$\begin{aligned}\alpha_s'&=b_{e-1}^{(s)}+a_0^{(s)}p+\cdots+a_{e-2}^{(s)}p^{e-1},\\ \beta_s'&=a_{e-1}^{(s)}+b_0^{(s)}p+\cdots+b_{e-2}^{(s)}p^{e-1}.\end{aligned}$$

Clearly, n_1' and n_2' are still in Case 2. If they are in Case 2.1, then they are in the same part. It follows that n_1 and n_2 are in the same part and we are done. So we may assume that n_1' and n_2' are in

Case 2.2. By (23) (applied to n_1' and n_2'), we have $a_{e-1}^{(s)} = b_{e-1}^{(s)}$, $s = 1, 2$. Continuing this way, we have $a_j^{(s)} = b_j^{(s)}$ for all $0 \leqslant j \leqslant e-1$, $s = 1, 2$, i.e., $\alpha_s = \beta_s$, $s = 1, 2$. Since $\alpha_1 + \beta_1 = \alpha_2 + \beta_2 + p^e - 1$, we must have $\alpha_1 = \beta_1 = \alpha_2 + \frac{p^e-1}{2} = \beta_2 + \frac{p^e-1}{2}$.

Now (10) gives

$$\left[x(1-x)\right]^{\frac{p^e-1}{2}} \equiv 1 \pmod{x^{p^e} + x - 1},$$

which is impossible.

Case 3. $\alpha_1 + \beta_1 > 0$, $\alpha_2 + \beta_2 > 0$, $\alpha_1 + \beta_1 \equiv p^k \pmod{p^e - 1}$, $\alpha_2 + \beta_2 \equiv p^l \pmod{p^e - 1}$ for some $0 \leqslant k, l \leqslant e-1$, $k \neq l$.

By considering $p^{e-i}n_1$ and $p^{e-i}n_2$ (modulo $p^{2e}-1$) instead of n_1 and n_2, we may assume $\alpha_1 + \beta_1 \equiv 1 \pmod{p^e - 1}$. So $\alpha_1 + \beta_1 = 1$ or p^e.

Case 3.1. $\alpha_1 + \beta_1 = 1$. The proof is identical to the $p = 2$ case (proof of Theorem 3.1, Case 3.1).

Case 3.2. $\alpha_1 + \beta_1 = p^e$. Then $\alpha_2 + \beta_2 = p^l$ or $p^l + p^e - 1$ for some $0 < l \leqslant e-1$. We claim that $\alpha_2 + \beta_2 = p^l + p^e - 1$. The proof of this claim is almost identical to the proof in the $p = 2$ case (proof of Theorem 3.1, Case 3.1) and is thus omitted. (We remind the reader that the possibility that $\alpha_2 = \beta_2$ in the $p = 2$ case does not occur in the current situation since $\alpha_2 + \beta_2$ is odd.)

We further claim that $\alpha_2 < p^e - 1$ and $\beta_2 < p^e - 1$. Again, the proof is the same as in the $p = 2$ case (proof of Theorem 3.1, Case 3.2).

Letting $i = p^l$ in (12), we obtain

$$(-1)^{\beta_1}\binom{\alpha_1}{p^e - p^l} + (-1)^{\alpha_1}\binom{\beta_1}{p^e - p^l} \equiv 0 \pmod{p},$$

i.e.,

$$\binom{\alpha_1}{p^e - p^l} \equiv \binom{\beta_1}{p^e - p^l} \pmod{p}. \tag{24}$$

Letting $i = p^l - 1$ in (12), we have

$$(-1)^{\beta_1}\binom{\alpha_1}{p^e - p^l + 1} + (-1)^{\alpha_1}\binom{\beta_1}{p^e - p^l + 1} \equiv -(-1)^{\beta_2}\alpha_2 - (-1)^{\alpha_2}\beta_2 \pmod{p},$$

i.e.,

$$\pm(\alpha_2 - \beta_2) \equiv \binom{\alpha_1}{p^e - p^l + 1} - \binom{\beta_1}{p^e - p^l + 1} \pmod{p}. \tag{25}$$

We claim that in (25),

$$\binom{\alpha_1}{p^e - p^l + 1} \equiv \binom{\beta_1}{p^e - p^l + 1} \equiv 0 \pmod{p}. \tag{26}$$

Note that

$$p^e - p^l + 1 = (\underset{0}{1}, 0, \ldots, 0, \underset{l}{p-1}, \ldots, p-1)P,$$

where

$$P = \begin{bmatrix} p^0 \\ \vdots \\ p^{e-1} \end{bmatrix}.$$

To prove (26), it suffices to show that

$$\alpha_1 \neq (*, \ldots, *, \underset{l}{p-1}, \ldots, p-1)P, \qquad \beta_1 \neq (*, \ldots, *, \underset{l}{p-1}, \ldots, p-1)P. \tag{27}$$

Assume to the contrary that

$$\alpha_1 = (*, \ldots, *, \underset{l}{p-1}, \ldots, p-1)P.$$

Since $\alpha_1 + \beta_1 = p^e$,

$$\beta_1 \neq (*, \ldots, *, \underset{l}{p-1}, \ldots, p-1)P.$$

Then $\binom{\alpha_1}{p^e - p^l} \equiv 1 \pmod p$ and $\binom{\beta_1}{p^e - p^l} \equiv 0 \pmod p$, which is a contradiction to (24). So (26) is proved. Now (25) gives $\alpha_2 \equiv \beta_2 \pmod p$. Since $\alpha_2 + \beta_2 \equiv -1 \pmod p$, we must have $\alpha_2 \equiv \beta_2 \equiv \frac{p-1}{2} \pmod p$, i.e.,

$$\alpha_2 = \left(\frac{p-1}{2}, *, \ldots, *\right)P,$$
$$\beta_2 = \left(\frac{p-1}{2}, *, \ldots, *\right)P.$$

We now use induction to prove that

$$\begin{cases} \alpha_2 = \left(\dfrac{p-1}{2}, \ldots, \overset{l-1}{\dfrac{p-1}{2}}, *, \ldots, *\right)P, \\ \beta_2 = \left(\dfrac{p-1}{2}, \ldots, \underset{l-1}{\dfrac{p-1}{2}}, *, \ldots, *\right)P. \end{cases} \tag{28}$$

Let $0 < t < l$ and let $i = p^l - p^t$ in (12). We have

$$\begin{aligned} &(-1)^{\beta_1}\binom{\alpha_1}{p^e - p^l + p^t} + (-1)^{\alpha_1}\binom{\beta_1}{p^e - p^l + p^t} \\ &\quad \equiv -(-1)^{\beta_2}\binom{\alpha_2 + 1}{p^t} - (-1)^{\alpha_2}\binom{\beta_2 + 1}{p^t} \pmod p. \end{aligned} \tag{29}$$

Note that

$$p^e - p^l + p^t = (0, \ldots, 0, \underset{t}{1}, 0, \ldots, 0, \underset{l}{p-1}, \ldots, p-1)P.$$

So by (27),

$$\binom{\alpha_1}{p^e - p^l + p^t} \equiv \binom{\beta_1}{p^e - p^l + p^t} \equiv 0 \pmod{p}.$$

Thus (29) gives

$$\binom{\alpha_2 + 1}{p^t} \equiv \binom{\beta_2 + 1}{p^t} \pmod{p},$$

i.e.,

$$\binom{\alpha_2}{p^t} + \binom{\alpha_2}{p^t - 1} \equiv \binom{\beta_2}{p^t} + \binom{\beta_2}{p^t - 1} \pmod{p}.$$

By the induction hypothesis,

$$\alpha_2 = \left(\frac{p-1}{2}, \ldots, \overset{t-1}{\frac{p-1}{2}}, *, \ldots, *\right)P,$$
$$\beta_2 = \left(\frac{p-1}{2}, \ldots, \underset{t-1}{\frac{p-1}{2}}, *, \ldots, *\right)P,$$

which implies

$$\binom{\alpha_2}{p^t - 1} \equiv \binom{\beta_2}{p^t - 1} \equiv 0 \pmod{p}.$$

So we have

$$\binom{\alpha_2}{p^t} \equiv \binom{\beta_2}{p^t} \pmod{p}. \tag{30}$$

Write

$$\alpha_2 = \left(\frac{p-1}{2}, \ldots, \overset{t-1}{\frac{p-1}{2}}, a, *, \ldots, *\right)P,$$
$$\beta_2 = \left(\frac{p-1}{2}, \ldots, \underset{t-1}{\frac{p-1}{2}}, b, *, \ldots, *\right)P.$$

We have

$$\begin{cases} a = b & \big(\text{by (30)}\big), \\ a + b = p - 1 & \big(\text{since } \alpha_2 + \beta_2 = p^l - 1 + p^e\big). \end{cases}$$

So $a = b = \frac{p-1}{2}$ and the induction is complete.

Next, we consider $n_1 p^{e-l}$ and $n_2 p^{e-l}$. Write $n_1 p^{e-l} \equiv \alpha_1' + \beta_1' p^e \pmod{p^{2e} - 1}$ and $n_2 p^{e-l} \equiv \alpha_2' + \beta_2' p^e \pmod{p^{2e} - 1}$, where $0 \leqslant \alpha_s', \beta_s' \leqslant p^e - 1$, $s = 1, 2$. It is easy to see that $\alpha_2' + \beta_2' = p^e$ and

$\alpha_1' + \beta_1' \equiv p^{e-l} \pmod{p^e - 1}$. By the remark at the beginning of Case 3.2, we have $\alpha_1' + \beta_1' = p^{e-l} + p^e - 1$. Therefore, by (28) (applied to $n_2 p^{e-l}$ and $n_1 p^{e-l}$), we have

$$\alpha_1' = \left(\frac{p-1}{2}, \ldots, \underset{e-l-1}{\frac{p-1}{2}}, *, \ldots, *\right)P,$$
$$\beta_1' = \left(\frac{p-1}{2}, \ldots, \underset{e-l-1}{\frac{p-1}{2}}, *, \ldots, *\right)P,$$

which imply that

$$\begin{cases} \alpha_1 = \left(*, \ldots, *, \underset{l}{\frac{p-1}{2}}, \ldots, \frac{p-1}{2}\right)P, \\ \beta_1 = \left(*, \ldots, *, \underset{l}{\frac{p-1}{2}}, \ldots, \frac{p-1}{2}\right)P. \end{cases} \tag{31}$$

Let $l < t \leqslant e-1$ and let $i = p^e - 1 + p^l - p^t$ in (12). We have

$$(-1)^{\beta_1}\binom{\alpha_1}{1+p^t-p^l} + (-1)^{\alpha_1}\binom{\beta_1}{1+p^t-p^l} \equiv (-1)^{\beta_2}\binom{\alpha_2}{p^t} + (-1)^{\alpha_2}\binom{\beta_2}{p^t} \pmod{p}. \tag{32}$$

Note that

$$1 + p^t - p^l = (1, 0, \ldots, 0, \underset{l}{p-1}, \ldots, \underset{t-1}{p-1}, 0, \ldots, 0)P.$$

It follows from (31) that

$$\binom{\alpha_1}{1+p^t-p^l} \equiv \binom{\beta_1}{1+p^t-p^l} \pmod{p}. \tag{33}$$

Write

$$\alpha_2 = \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \underset{l}{*}, \ldots, \underset{t}{a}, \ldots, *\right)P,$$
$$\beta_2 = \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \underset{l}{*}, \ldots, \underset{t}{b}, \ldots, *\right)P.$$

Then (32) and (33) give $a = b$. Since $\alpha_2 + \beta_2 = p^l - 1 + p^e$, we have $a + b = p - 1$ or p, so we must have $a = b = \frac{p-1}{2}$. Therefore we have proved that

$$\begin{cases} \alpha_2 = \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \underset{l}{w}, \frac{p-1}{2}, \ldots, \frac{p-1}{2}\right)P, \\ \beta_2 = \left(\frac{p-1}{2}, \ldots, \frac{p-1}{2}, \underset{l}{z}, \frac{p-1}{2}, \ldots, \frac{p-1}{2}\right)P \end{cases}$$

for some $w, z \in \{0, \ldots, p-1\}$. By considering $n_1 p^{e-l}$ and $n_2 p^{e-l}$, we also have

$$\begin{cases} \alpha_1 = \left(u, \dfrac{p-1}{2}, \ldots, \dfrac{p-1}{2}\right)P, \\ \beta_1 = \left(v, \dfrac{p-1}{2}, \ldots, \dfrac{p-1}{2}\right)P \end{cases}$$

for some $u, v \in \{0, \ldots, p-1\}$.

Letting $i = p^e - 1$ in (12), we have

$$(-1)^{\beta_1}\alpha_1 + (-1)^{\alpha_1}\beta_1 \equiv (-1)^{\beta_2}\binom{\alpha_2}{p^l} + (-1)^{\alpha_2}\binom{\beta_2}{p^l} \pmod{p},$$

i.e.,

$$u - v \equiv \pm(w - z) \pmod{p}.$$

We also have $u + v = p = w + z$ (since $\alpha_1 + \beta_1 = p^e$ and $\alpha_2 + \beta_2 = p^l - 1 + p^e$). Thus

$$\begin{cases} u = w, \\ v = z = p - u, \end{cases} \quad \text{or} \quad \begin{cases} u = z, \\ v = w = p - u. \end{cases} \tag{34}$$

The proof will be complete if we can show that $u = \frac{p-1}{2}$ or $\frac{p+1}{2}$. With this claim, we have $\{\alpha_1, \beta_1\} = \{\frac{p^e-1}{2}, \frac{p^e-1}{2} + 1\}$ and $\{\alpha_2, \beta_2\} = \{\frac{p^e-1}{2}, \frac{p^e-1}{2} + p^l\}$. Then $n_1 = \frac{p^{2e}-1}{2} + 1$ or $\frac{p^{2e}-1}{2} + p^e$ and $n_2 = \frac{p^{2e}-1}{2} + p^l$ or $\frac{p^{2e}-1}{2} + p^{e+l}$, so n_1 and n_2 belong to the same part.

First note that by (10) and (34), we have

$$\begin{aligned} &x^{u-\frac{p-1}{2}}(1-x)^{-u+\frac{p+1}{2}} + x^{-u+\frac{p+1}{2}}(1-x)^{u-\frac{p-1}{2}} \\ &\quad\equiv \left[x^{u-\frac{p-1}{2}}(1-x)^{-u+\frac{p+1}{2}} + x^{-u+\frac{p+1}{2}}(1-x)^{u-\frac{p-1}{2}}\right]^{p^l} \pmod{x^{p^e} + x - 1}. \end{aligned} \tag{35}$$

(Since $(x(1-x), x^{p^e} + x - 1) = 1$, possible negative exponents in the above do not cause any problem.) Assume to the contrary that $u < \frac{p-1}{2}$ or $u > \frac{p+1}{2}$, say, $u < \frac{p-1}{2}$. Rewrite (35) as

$$\begin{aligned} &\left[x^{u-\frac{p-1}{2}}(1-x)^{-u+\frac{p+1}{2}} + x^{-u+\frac{p+1}{2}}(1-x)^{u-\frac{p-1}{2}}\right]\left[x(1-x)\right]^{(\frac{p-1}{2}-u)p^l} \\ &\quad\equiv \left[(1-x)^{p-2u} + x^{p-2u}\right]^{p^l} \pmod{x^{p^e} + x - 1}. \end{aligned} \tag{36}$$

Both sides of (36) are polynomials of degree $< p^e$, hence they are equal, i.e.,

$$\begin{aligned} &x^{(\frac{p-1}{2}-u)(p^l-1)}(1-x)^{(\frac{p-1}{2}-u)(p^l+1)+1} + x^{(\frac{p-1}{2}-u)(p^l+1)+1}(1-x)^{(\frac{p-1}{2}-u)(p^l-1)} \\ &\quad= (1-x)^{(p-2u)p^l} + x^{(p-2u)p^l}. \end{aligned}$$

The above equation implies that $x \mid (1-x)$, which is a contradiction. This completes the proof of the theorem. □

References

[1] L. Budaghyan, C. Carlet, G. Leander, Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inform. Theory 54 (2008) 4218–4229.
[2] W.-S. Chou, J. Gomez-Calderon, G.L. Mullen, Value sets of Dickson polynomials over finite fields, J. Number Theory 30 (1988) 334–344.
[3] S.D. Cohen, R.W. Matthews, A class of exceptional polynomials, Trans. Amer. Math. Soc. 345 (1994) 897–909.
[4] R.S. Coulter, Explicit evaluation of some Weil sums, Acta Arith. 83 (1998) 241–251.
[5] L.E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, Ann. of Math. 11 (1896/1897) 65–120, 161–183.
[6] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: The Welsh case, IEEE Trans. Inform. Theory 45 (1999) 1271–1275.
[7] H. Dobbertin, Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5, in: Finite Fields and Applications, Springer, Berlin, 2001, pp. 113–121.
[8] T. Helleseth, C. Rong, D. Sandberg, New families of almost perfect nonlinear power mappings, IEEE Trans. Inform. Theory 45 (1999) 474–485.
[9] S.W. Kang, Remarks on finite fields, Bull. Korean Math. Soc. 20 (2) (1983) 81–85.
[10] S.W. Kang, Remarks on finite fields II, Bull. Korean Math. Soc. 22 (1) (1985) 37–41.
[11] S.W. Kang, Remarks on finite fields III, Bull. Korean Math. Soc. 23 (2) (1986) 103–111.
[12] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Longman Scientific and Technical, Essex, United Kingdom, 1993.
[13] R. Lidl, H. Niederreiter, Finite Fields, second ed., Cambridge Univ. Press, Cambridge, 1997.
[14] I.G. Macdonald, Symmetric Functions and Orthogonal Polynomials, Amer. Math. Soc., Providence, RI, 1998.
[15] K. Nyberg, Differentially uniform mappings for cryptography, in: Advances in Cryptology—EUROCRYPT '93, Lofthus, 1993, in: Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 55–64.
[16] I. Schur, Über den Zusammenhang zwischen einen Problem der Zahlentheorie und einen Satz über algebraische Funktionen, in: Sitzungsber. Preuss. Akad. Wiss. Berlin, 1923, pp. 123–134.