Finite Fields and Their Applications 18 (2012) 814–831

Contents lists available at SciVerse ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Dickson polynomials over finite fields

Qiang Wang [a,*,1], Joseph L. Yucas [b]

[a] *School of Mathematics and Statistics, Carleton University, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada*
[b] *Department of Mathematics, University of Southern Illinois, Carbondale, IL 62901, USA*

ARTICLE INFO

Article history:
Received 15 September 2011
Revised 23 January 2012
Accepted 7 February 2012
Available online 27 February 2012
Communicated by Rudolf Lidl

MSC:
11T06
13P10

Keywords:
Finite fields
Dickson polynomials
Permutation polynomials
Factorization

ABSTRACT

In this paper we introduce the notion of Dickson polynomials of the $(k+1)$-th kind over finite fields $\mathbb{F}_{p^m}$ and study basic properties of this family of polynomials. In particular, we study the factorization and the permutation behavior of Dickson polynomials of the third kind.

1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q = p^m$ elements. For any integer $n \geqslant 1$ and a parameter a in a field $\mathbb{F}_q$, we recall that the n-th Dickson polynomial of the first kind $D_n(x,a) \in \mathbb{F}_q[x]$ is defined by

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

[*] Corresponding author.
E-mail addresses: wang@math.carleton.ca (Q. Wang), jyucas@math.siu.edu (J.L. Yucas).

[1] Research of Qiang Wang is partially supported by NSERC of Canada.

1071-5797/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2012.02.001

Similarly, the n-th Dickson polynomial of the second kind $E_n(x,a) \in \mathbb{F}_q[x]$ is defined by

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

For $a \neq 0$, we write $x = y + a/y$ with $y \neq 0$ an indeterminate. Then Dickson polynomials can often be rewritten (also referred as functional expression) as

$$D_n(x,a) = D_n\left(y + \frac{a}{y}, a\right) = y^n + \frac{a^n}{y^n},$$

and

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

for $y \neq 0, \pm\sqrt{a}$; For $y = \pm\sqrt{a}$, we have $E_n(2\sqrt{a}, a) = (n+1)(\sqrt{a})^n$ and $E_n(-2\sqrt{a}, a) = (n+1)(-\sqrt{a})^n$. It is well known that $D_n(x,a) = xD_{n-1}(x,a) - aD_{n-2}(x,a)$ and $E_n(x,a) = xE_{n-1}(x,a) - aE_{n-2}(x,a)$ for any $n \geqslant 2$.

In the case $a = 1$, we denote the n-th Dickson polynomials of the first kind and the second kind by $D_n(x)$ and $E_n(x)$ respectively. It is well known that these Dickson polynomials are closely related to Chebyshev polynomials by the connections $D_n(2x) = 2T_n(x)$ and $E_n(2x) = U_n(x)$, where $T_n(x)$ and $U_n(x)$ are Chebyshev polynomials of degree n of the first kind and the second kind, respectively. More information on Dickson polynomials can be found in [8]. In the context of complex functions, Dickson polynomials of other kinds have already been introduced, see for example [6,9]. In the context of finite fields, some properties such as recursive relations remain the same but the emphases are rather different. For example, permutation property over finite fields is one of properties which have attract a lot of attention due to their applications in cryptography. In this paper, we study Dickson polynomials of the higher kinds over finite fields. For any $k < p$ and constant $a \in \mathbb{F}_q$, we define n-th Dickson polynomials $D_{n,k}(x,a)$ of the $(k+1)$-th kind and the n-th reversed Dickson polynomials $D_{n,k}(x,a)$ of the $(k+1)$-th kind in Section 2. Moreover, we give the relation between Dickson polynomials of the $(k+1)$-th kind and Dickson polynomials of the first two kinds, the recurrence relation of Dickson polynomials of the $(k+1)$-th kind in terms of degrees for a fixed k and its generating function, functional expressions, as well as differential recurrence relations. Some general results on functional expression reduction and permutation behavior of $D_{n,k}(x,a)$ are also obtained in Section 2. Then we focus on Dickson polynomials of the third kind. In Section 3, we show the relation between Dickson polynomials of the third kind and Dickson polynomials of the second kind and thus obtain the factorization of these polynomials. Finally, we study the permutation behavior of Dickson polynomials of the third kind $D_{n,2}(x,1)$ in Section 4. Our work is motivated by the study of Dickson polynomials of the second kind given by Cipu and Cohen (separately and together) in [3–5], which aimed to address conjectures of existence of nontrivial Dickson permutation polynomials of second kind other than several interesting exceptions when the characteristics is 3 or 5. We obtain some necessary conditions for $D_{n,2}(x,1)$ to be a permutation polynomial (PP) of any finite fields $\mathbb{F}_q$. We also completely describe Dickson permutation polynomials of the third kind over any prime field following the strategy of using Hermite's criterion and Gröbner basis over rings started in [3–5].

2. Dickson polynomial of the $(k+1)$-th kind

Definition 2.1. For $a \in \mathbb{F}_q$, and any positive integers n and k, we define the n-th *Dickson polynomial of the* $(k+1)$*-th kind* $D_{n,k}(x,a)$ over $\mathbb{F}_q$ by

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

Definition 2.2. For $a \in \mathbb{F}_q$, and any positive integers n and k, we define the n-th *reversed Dickson polynomial of the* $(k+1)$*-th kind* $D_{n,k}(a,x)$ over $\mathbb{F}_q$ by

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

Remark 2.3. For $n = 0$, we define $D_{n,k}(x,a) = 2-k = D_{n,k}(a,x)$. It is easy to see that $D_{n,0}(x,a) = D_n(x,a)$ and $D_{n,1}(x,a) = E_n(x,a)$. Moreover, we can have the following simple relation

$$D_{n,k}(x,a) = kD_{n,1}(x,a) - (k-1)D_{n,0}(x,a) = kE_n(x,a) - (k-1)D_n(x,a). \tag{2.1}$$

It is easy to see that if $char(\mathbb{F}_q) = 2$, then $D_{n,k}(x,a) = D_n(x,a)$ if k is even and $D_{n,k}(x,a) = E_n(x,a)$ if k is odd. So we can assume $char(\mathbb{F}_q)$ is odd and we can also restrict $k < p$ because $D_{n,k+p}(x,a) = D_{n,k}(x,a)$.

Remark 2.4. The fundamental functional equation is

$$\begin{aligned} D_{n,k}\big(y + ay^{-1}, a\big) &= \frac{y^{2n} + kay^{2n-2} + \cdots + ka^{n-1}y^2 + a^n}{y^n} \\ &= \frac{y^{2n} + a^n}{y^n} + \frac{ka}{y^n} \frac{y^{2n} - a^{n-1}y^2}{y^2 - a}, \quad \text{for } y \neq 0, \pm\sqrt{a}, \end{aligned}$$

where $D_{n,k}(\pm 2\sqrt{a}, a) = (\pm\sqrt{a})^n (kn - k + 2)$.

Remark 2.5. For a fixed k and any $n \geqslant 2$, we have the following recursion:

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

where $D_{0,k}(x,a) = 2-k$ and $D_{1,k}(x,a) = x$.

Using this recursion, we can obtain the generating function of these Dickson polynomials.

Lemma 2.6. *The generating function of* $D_{n,k}(x,a)$ *is*

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

Proof.

$$\begin{aligned}
&\bigl(1-xz+az^2\bigr)\sum_{n=0}^{\infty} D_{n,k}(x,a)z^n\\
&=\sum_{n=0}^{\infty} D_{n,k}(x,a)z^n - x\sum_{n=0}^{\infty} D_{n,k}(x,a)z^{n+1} + a\sum_{n=0}^{\infty} D_{n,k}(x,a)z^{n+2}\\
&=2-k+xz-(2-k)xz+\sum_{n=0}^{\infty}\bigl(D_{n+2,k}(x,a)-xD_{n+1,k}(x,a)+aD_{n,k}(x,a)\bigr)z^n\\
&=2-k+(k-1)xz. \qquad \square
\end{aligned}$$

Stoll [9] has studied these Dickson-type polynomials with coefficients over $\mathbb{C}$. We note that in our case all the coefficients of $D_{n,k}(x,a)$ are integers. Hence Lemma 17 in [9] can be modified to the following.

Lemma 2.7. *The Dickson polynomial $D_{n,k}(x,a)$ satisfies the following difference equation*

$$\bigl(A_4x^4+aA_2x^2+a^2A_0\bigr)D''_{n,k}(x,a)+\bigl(B_3x^3+aB_1x\bigr)D'_{n,k}(x,a)-\bigl(C_2x^2+aC_0\bigr)D_{n,k}(x,a)=0,$$

where $A_4, A_2, A_0, B_3, B_1, C_2, C_0 \in \mathbb{Z}$ satisfy

$$\begin{aligned}
A_4&=B_3=n(1-k),\\
A_2&=-(n-1)(2-k)^2-2(2n+1)(2-k)+4n,\\
A_0&=4(n-1)(2-k)^2+8(2-k),\\
B_1&=-3(n-1)(2-k)^2+2(4n-3)(2-k)-8n,\\
C_2&=n^3(1-k),\\
C_0&=-n(n-1)(n-2)(2-k)^2-2n(3n-4)(2-k)-8n.
\end{aligned}$$

In particular, for $k=0,1,2$, we have

$$\begin{gathered}
\bigl(x^2-4a\bigr)D''_{n,0}(x,a)+xD'_{n,0}(x,a)-n^2D_{n,0}(x,a)=0,\\
\bigl(x^2-4a\bigr)D''_{n,1}(x,a)+3xD'_{n,1}(x,a)-n(n+2)D_{n,1}(x,a)=0,\\
x^2\bigl(x^2-4a\bigr)D''_{n,2}(x,a)+x\bigl(x^2+8a\bigr)D'_{n,2}(x,a)-\bigl(n^2x^2+8a\bigr)D_{n,2}(x,a)=0.
\end{gathered}$$

Theorem 2.8. *Suppose ab is a square in $\mathbb{F}_q{}^*$. Then $D_{n,k}(x,a)$ is a PP of $\mathbb{F}_q$ if and only if $D_{n,k}(x,b)$ is a PP of $\mathbb{F}_q$. Furthermore,*

$$D_{n,k}(\alpha,a)=(\sqrt{a/b})^nD_{n,k}\bigl((\sqrt{b/a})\alpha,b\bigr).$$

Proof.

$$\begin{aligned}
\sqrt{a/b}^{\,n}D_{n,k}(\sqrt{b/a}\alpha,b)&=(\sqrt{a/b})^n\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n-ki}{n-i}\binom{n-i}{i}(-b)^i(\sqrt{b/a}\alpha)^{n-2i}\\
&=(\sqrt{a/b})^n\sum_{i=0}^{\lfloor n/2\rfloor}\frac{n-ki}{n-i}\binom{n-i}{i}(-b)^i(\sqrt{b/a}\alpha)^{n-2i}
\end{aligned}$$

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

So we can focus on $a = \pm 1$. When $a = 1$, we denote by

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

Indeed, $D_{n,0}(x) = D_n(x)$ and $D_{n,1}(x) = E_n(x)$ are Dickson polynomial of the first kind and then second kind when $a = 1$ respectively.

Similarly, let $x = y + y^{-1}$, we obtain the functional expression of $D_{n,k}(x)$:

$$D_{n,k}\bigl(y + y^{-1}\bigr) = \frac{y^{2n} + ky^{2n-2} + \ldots + ky^2 + 1}{y^n}$$
$$= \frac{y^{2n}+1}{y^n} + \frac{k}{y^n} \frac{y^{2n} - y^2}{y^2 - 1}, \quad y \neq 0, \pm 1.$$

We remark that $D_{n,k}(\pm 2) = (\pm 1)^n (kn - k + 2)$ and $D_{n,k}(-x) = (-1)^n D_{n,k}(x)$. For a fixed k and any $n \geqslant 2$, we have the following recursion:

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

where $D_{0,k}(x) = 2 - k$ and $D_{1,k}(x) = x$.

For $\alpha \in \mathbb{F}_q$ there exists $u_\alpha \in \mathbb{F}_{q^2}$ with

$$\alpha = u_\alpha + \frac{1}{u_\alpha}.$$

The following property is well known.

Proposition 2.9. *For $u \in \mathbb{F}_{q^2}$ with $u + \frac{1}{u} \in \mathbb{F}_q$ we have $u^{q-1} = 1$ or $u^{q+1} = 1$.*

For positive integers n and r we use the notation $(n)_r$ to denote n (mod r), the smallest positive integer congruent to n modulo r. Let us also define S_{q-1}, S_{q+1}, and S_p by

$$S_{q-1} = \bigl\{\alpha \in \mathbb{F}_q \colon u_\alpha^{q-1} = 1\bigr\}, \qquad S_{q+1} = \bigl\{\alpha \in \mathbb{F}_q \colon u_\alpha^{q+1} = 1\bigr\}, \qquad S_p = \{\pm 2\}.$$

Then we can reduce the function $D_{n,k}(x)$ into step functions with smaller degrees.

Theorem 2.10. *As functions on $\mathbb{F}_q$, we have*

$$D_{n,k}(\alpha) = \begin{cases} D_{(n)_{2p},k}(\alpha) & \text{if } \alpha \in S_p, \\ D_{(n)_{q-1},k}(\alpha) & \text{if } \alpha \in S_{q-1}, \\ D_{(n)_{q+1},k}(\alpha) & \text{if } \alpha \in S_{q+1}. \end{cases}$$

Proof. If $\alpha \in S_p$ then $D_{n,k}(\alpha) = (\pm 1)^n(kn-k+2) = (\pm 1)^{(n)_{2p}}(k(n)_{2p}-k+2) = D_{(n)_{2p},k}(\alpha)$. If $\alpha \in S_{q-1}$ then $u_\alpha^n = u_\alpha^{(n)_{q-1}}$. Similarly, if $\alpha \in S_{q+1}$ then $u_\alpha^n = u_\alpha^{(n)_{q+1}}$. The rest of proof follows from the functional expression of Dickson polynomials. □

Define $c = \frac{p(q^2-1)}{4}$. By Proposition 2.9, we have $u_\alpha^{2c} = 1$. Therefore, using the functional expressions, we have $D_{n,k}(\alpha) = D_{(n)_{2c},k}(\alpha)$ as functions over $\mathbb{F}_q$. This means the sequence of Dickson polynomials of the $(k+1)$-th kind in terms of degrees modulo $x^q - x$ is a periodic function with period $2c$. Here we can obtain $(n)_{2c}$ in terms of $(n)_p$, $(n)_{q-1}$ and $(n)_{q+1}$.

Proposition 2.11. *Let $c = \frac{p(q^2-1)}{4}$. If n is a positive integer then we have*

$$(n)_{2c} = -(n)_p\left(q^2-1\right) + \frac{(n)_{q-1}q^2(q+1)}{2} - \frac{(n)_{q+1}q^2(q-1)}{2}.$$

Proof. If p is even, then both $q+1$ and $q-1$ are odd and thus $\frac{p}{2}$, $q+1$, $q-1$ are pairwise relatively prime. If p is odd, then both $q+1$ and $q-1$ are even. Hence p, $q+1$, $\frac{q-1}{2}$ are pairwise relatively prime if $q \equiv 3 \pmod 4$ and p, $\frac{q+1}{2}$, $q-1$ are pairwise relatively prime if $q \equiv 1 \pmod 4$. The rest of proof follows from Chinese Remainder Theorem. □

Let $\epsilon_\alpha = u_\alpha^c \in \{\pm 1\}$. Then we obtain the following.

Theorem 2.12. *Let $\alpha = u_\alpha + \frac{1}{u_\alpha}$ where $u_\alpha \in \mathbb{F}_{q^2}$ and $\alpha \in \mathbb{F}_q$. Let $\epsilon_\alpha = u_\alpha^c \in \{\pm 1\}$ where $c = \frac{p(q^2-1)}{4}$. As functions on $\mathbb{F}_q$ we have*

$$D_{c+n,k}(\alpha) = \epsilon_\alpha D_{n,k}(\alpha).$$

Moreover, $D_{n,k}(x)$ is a PP of $\mathbb{F}_q$ if and only if $D_{c+n,k}(x)$ is a PP of $\mathbb{F}_q$.

Proof. For $\alpha = \pm 2$, we have $u_\alpha = \pm 1$. Moreover, $p \mid c$. Hence

$$\begin{aligned} D_{c+n,k'}(\pm 2) &= (\pm 1)^{c+n}\big(k(c+n)-k+2\big) \\ &= (\pm 1)^c(\pm 1)^n(kn-k+2) \\ &= \epsilon_\alpha D_{n,k}(\pm 2). \end{aligned}$$

If $\alpha \neq \pm 2, 0$, we have $u_\alpha^c = u_\alpha^{-c}$ and thus

$$\begin{aligned} D_{c+n,k}(\alpha) &= \frac{u_\alpha^{2(c+n)}+1}{u_\alpha^{c+n}} + \frac{k}{u_\alpha^{c+n}}\frac{u_\alpha^{2(c+n)}-u_\alpha^2}{u_\alpha^2-1} \\ &= \frac{u_\alpha^{2c}u_\alpha^{2n}+1}{u_\alpha^c u_\alpha^n} + \frac{k}{u_\alpha^c u_\alpha^n}\frac{u_\alpha^{2c}u_\alpha^{2n}-u_\alpha^2}{u_\alpha^2-1} \\ &= \frac{u_\alpha^c u_\alpha^{2n}+u_\alpha^{-c}}{u_\alpha^n} + \frac{k}{u_\alpha^n}\frac{u_\alpha^c u_\alpha^{2n}-u_\alpha^{-c}u_\alpha^2}{u_\alpha^2-1} \\ &= u_\alpha^c\left(\frac{u_\alpha^{2n}+1}{u_\alpha^n} + \frac{k}{u_\alpha^n}\frac{u_\alpha^{2n}-u_\alpha^2}{u_\alpha^2-1}\right) \\ &= u_\alpha^c D_{n,k}(\alpha). \end{aligned}$$

If q is even, then $D_{c+n,k}(x) = D_{n,k}(x)$. Hence we assume q is odd for the rest of the proof. If $D_{n,k}(x)$ is a PP of $\mathbb{F}_q$, then n must be odd because $D_{n,k}(\pm 2) = (\pm 1)^n(kn - k + 2)$ and $D_{n,k}(2) \neq D_{n,k}(-2)$. Therefore $D_{n,k}(-\alpha) = -D_{n,k}(\alpha)$ for any $\alpha \in \mathbb{F}_q$. Since c is even, $c + n$ is odd and $D_{c+n,k}(-\alpha) = -D_{c+n,k}(\alpha)$. Suppose $D_{c+n,k}(\alpha_1) = D_{c+n,k}(\alpha_2)$ for some $\alpha_1, \alpha_2 \in \mathbb{F}_q$. Then there are $\epsilon_{\alpha_1}, \epsilon_{\alpha_2} \in \{\pm 1\}$ such that $\epsilon_{\alpha_1} D_{n,k}(\alpha_1) = \epsilon_{\alpha_2} D_{n,k}(\alpha_2)$. Therefore we either have $D_{n,k}(\alpha_1) = D_{n,k}(\alpha_2)$ or $D_{n,k}(\alpha_1) = -D_{n,k}(\alpha_2)$. In the latter case, $D_{n,k}(-\alpha_2) = -D_{n,k}(\alpha_2) = D_{n,k}(\alpha_1)$ implies that $\alpha_1 = -\alpha_2$. Then $D_{c+n,k}(\alpha_1) = D_{c+n,k}(-\alpha_2) = -D_{c+n,k}(\alpha_2)$, which contradicts to $D_{c+n,k}(\alpha_1) = D_{c+n,k}(\alpha_2)$ and q is odd. Hence $D_{n,k}(\alpha_1) = D_{n,k}(\alpha_2)$ and thus $\alpha_1 = \alpha_2$. Therefore $D_{c+n,k}(x)$ is also a PP of $\mathbb{F}_q$. The converse follows similarly. □

We remark that $D_{2c+n,k}(\alpha) = \epsilon_\alpha^2 D_{n,k}(\alpha) = D_{n,k}(\alpha)$ and thus $D_{n,k}(x) \equiv D_{(n)_{2c},k}(x) \pmod{x^q - x}$. This implies that the sequence of Dickson polynomials of the $(k+1)$-th kind in terms of degrees is a periodic function with period $2c$.

Finally we give the following result which relates a Dickson polynomial of one kind to a Dickson polynomial of another kind.

Theorem 2.13. *Let $q = p^m$ be an odd prime power. For $k \neq 1$, let $k' = \frac{k}{k-1} \pmod p$ and $\epsilon_\alpha = u_\alpha^c \in \{\pm 1\}$ where $c = \frac{p(q^2-1)}{4}$. For $n < c$, as functions on $\mathbb{F}_q$ we have*

$$D_{c-n,k'}(\alpha) = \frac{-\epsilon_\alpha}{k-1} D_{n,k}(\alpha).$$

Moreover, $D_{n,k}(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $D_{c-n,k'}(x)$ is a permutation polynomial of $\mathbb{F}_q$.

Proof. For $\alpha = \pm 2$, we have $u_\alpha = \pm 1$. Hence

$$\begin{aligned} D_{c-n,k'}(\pm 2) &= (\pm 1)^{c-n}\big(k'(c-n) - k' + 2\big) \\ &= (\pm 1)^c (\pm 1)^n \left(\frac{k(c-n)}{k-1} - \frac{k}{k-1} + \frac{2(k-1)}{k-1}\right) \\ &= \frac{u_\alpha^c}{k-1}(\pm 1)^n \big(k(c-n) - k + 2(k-1)\big) \\ &= -\frac{u_\alpha^c}{k-1}(\pm 1)^n (kn - k + 2) \\ &= \frac{-\epsilon_\alpha}{k-1} D_{n,k}(\pm 2). \end{aligned}$$

If $\alpha \neq \pm 2, 0$, then $u_\alpha^c = u_\alpha^{-c}$ and thus

$$\begin{aligned} D_{c-n,k'}(\alpha) &= \frac{u_\alpha^{2(c-n)} + 1}{u_\alpha^{c-n}} + \frac{k'}{u_\alpha^{c-n}} \frac{u_\alpha^{2(c-n)} - u_\alpha^2}{u_\alpha^2 - 1} \\ &= \frac{u_\alpha^{2c} u_\alpha^{-2n} + 1}{u_\alpha^c u_\alpha^{-n}} + \frac{k}{(k-1) u_\alpha^c u_\alpha^{-n}} \frac{u_\alpha^{2c} u_\alpha^{-2n} - u_\alpha^2}{u_\alpha^2 - 1} \\ &= \frac{u_\alpha^c u_\alpha^{-2n} + u_\alpha^{-c}}{u_\alpha^{-n}} + \frac{k}{(k-1) u_\alpha^{-n}} \frac{u_\alpha^c u_\alpha^{-2n} - u_\alpha^{-c} u_\alpha^2}{u_\alpha^2 - 1} \\ &= u_\alpha^c \left(\frac{u_\alpha^{-2n} + 1}{u_\alpha^{-n}} + \frac{k}{(k-1) u_\alpha^{-n}} \frac{u_\alpha^{-2n} - u_\alpha^2}{u_\alpha^2 - 1}\right) \end{aligned}$$

$$
\begin{aligned}
&= \frac{u_\alpha^c}{k-1}\left(\frac{(k-1)(u_\alpha^{-2n}+1)}{u_\alpha^{-n}} + \frac{k}{u_\alpha^{-n}}\frac{u_\alpha^{-2n}-u_\alpha^2}{u_\alpha^2-1}\right)\\
&= \frac{u_\alpha^c}{k-1}\left(\frac{-1(u_\alpha^{-2n}+1)}{u_\alpha^{-n}} + \frac{k}{u_\alpha^{-n}}\frac{u_\alpha^{-2n+2}-1}{u_\alpha^2-1}\right)\\
&= \frac{u_\alpha^c}{k-1}\left(\frac{-1(u_\alpha^{-2n}+1)}{u_\alpha^{-n}} + \frac{k}{u_\alpha^{-n}}\frac{u_\alpha^{-2n}-u_\alpha^{-2}}{1-u_\alpha^{-2}}\right)\\
&= \frac{-u_\alpha^c}{k-1}D_{n,k}(\alpha).
\end{aligned}
$$

The rest of proof is similar to that of Theorem 2.12. □

3. Dickson polynomial of the 3rd kind

First we recall

$$D_{n,k}(x,a) = kD_{n,1}(x,a) - (k-1)D_{n,0}(x,a) = kE_n(x,a) - (k-1)D_n(x,a). \tag{3.1}$$

It is easy to see that if $char(\mathbb{F}_q) = 2$, then $D_{n,k}(x,a) = D_n(x,a)$ if k is even and $D_{n,k}(x,a) = E_n(x,a)$ if k is odd. Hence it is more interesting to study $D_{n,k}(x)$ when $char(\mathbb{F}_q) > 2$.

Theorem 3.1. *For any $n \geqslant 1$, we have*

$$D_{n,k}(x,a) = D_{n,k-1}(x,a) + aE_{n-2}(x,a).$$

In particular,

$$D_{n,2}(x,a) = xE_{n-1}(x,a)$$

and

$$D_{n,3}(x,a) = xE_{n-1}(x,a) + aE_{n-2}(x,a).$$

Proof. Indeed, we have

$$
\begin{aligned}
D_{n,k}(x,a) &= kE_n(x,a) - (k-1)D_n(x,a)\\
&= D_{n,k-1}(x,a) + \bigl(E_n(x,a) - D_n(x,a)\bigr)\\
&= D_{n,k-1}(x,a) + aE_{n-2}(x,a),
\end{aligned}
$$

where the last identity holds because $E_n(x,a) - aE_{n-2}(x,a) = D_n(x,a)$. In particular, when $k = 2$, then

$$
\begin{aligned}
D_{n,2}(x,a) &= D_{n,1}(x,a) + aE_{n-2}(x,a)\\
&= E_n(x,a) + aE_{n-2}(x,a)\\
&= xE_{n-1}(x,a). \qquad \square
\end{aligned}
$$

Since the factorization of $E_n(x,a)$ over a finite field $\mathbb{F}_q$ is well known (see for example, [1] or [2]), we can obtain the factorization of $D_{n+1,2}(x,a) = xE_n(x,a)$ over $\mathbb{F}_q$ as well. Of course, it is enough to give the result for the case that $\gcd(n+1,p) = 1$. Indeed, if $n+1 = p^r(t+1)$ where $\gcd(t+1,p) = 1$, then it is straightforward to obtain $E_n(x,a) = E_t(x,a)^{p^r}(x^2-4a)^{\frac{p^r-1}{2}}$ by using the functional expression of $E_t(x,a)$.

Corollary 3.2. *Let $\mathbb{F}_q$ be a finite field with char$(\mathbb{F}_q) = p$, $\gcd(n+1, p) = 1$, and ϕ be Euler's totient function. Let $a \neq 0$.*

(i) *If q is even, then $D_{n+1,2}(x,a)$ is a product of irreducible polynomials in $\mathbb{F}_q[x]$ which occur in cliques corresponding to the divisors d of $n+1$. The irreducible factor corresponding to $d = 1$ is x. To each such $d > 1$ there correspond $\phi(d)/2k_d$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1}\left(x - \sqrt{a}\left(\zeta_d^{q^i} + \zeta_d^{-q^i}\right)\right),$$

where ζ_d is a primitive d-th root of unity and k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$.

(ii) *If q is odd, then $D_{n+1,2}(x,a)$ is a product of irreducible polynomials in $\mathbb{F}_q[x]$ which occur in cliques corresponding to the divisors d of $4n+2$ with $d > 2$ and $d = 1$. The irreducible factor corresponding to $d = 1$ is x. To each such $d > 2$ there corresponds $\phi(d)/2N_d$ irreducible factors, each of which has the form*

$$\prod_{i=0}^{k_d-1}\left(x - \sqrt{a}^{q^i}\left(\zeta_d^{q^i} + \zeta_d^{-q^i}\right)\right),$$

where ζ_d is a primitive d-th root of unity, unless a is non-square in $\mathbb{F}_q$ and $4 \nmid d$; in this exceptional case there are $\phi(d)/N_d$ factors corresponding to each $d = d_0$ and $d = 2d_0$, where $d_0 > 1$ is an odd divisor of $k+1$, and the factors corresponding to d_0 are identical to the factors corresponding to $2d_0$. Here k_d is the least positive integer such that $q^{k_d} \equiv \pm 1 \pmod{d}$, and

$$N_d = \begin{cases} k_d/2 & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } d \equiv 0 \pmod{2} \text{ and } k_d \equiv 2 \pmod{4} \\ & \text{and } q^{k_d/2} \equiv \frac{d}{2} \pm 1 \pmod{d}; \\ 2k_d & \text{if } \sqrt{a} \notin \mathbb{F}_q \text{ and } k_d \text{ is odd}; \\ k_4 & \text{otherwise}. \end{cases}$$

4. Permutation behavior of Dickson polynomials of the 3rd kind

Let $f_n(x) := D_{n,2}(x) = xE_{n-1}(x)$. The functional expression of $f_n(x)$ is given as follows:

$$f_n\left(y + y^{-1}\right) = \left(y + y^{-1}\right)\frac{y^n - y^{-n}}{y - y^{-1}} \quad \text{for } y \neq 0, \pm 1, \tag{4.1}$$

where $f_n(0) = 0$, $f_n(2) = 2n$, and $f_n(-2) = (-1)^n 2n$. If q is even then $D_{n,2}(x)$ is the Dickson polynomial of the first kind as explained earlier.

So we assume q is odd in this section. Let ξ be a primitive $(q-1)$-th root of unity and η be a primitive $(q+1)$-th root of unity in $\mathbb{F}_{q^2}$. Then $S_{q-1} = \{x = \xi^i + \xi^{-i} \in \mathbb{F}_q\colon\ 1 \leqslant i \leqslant (q-3)/2\}$ and $S_{q+1} = \{x = \eta^j + \eta^{-j} \in \mathbb{F}_q\colon\ 1 \leqslant j \leqslant (q-1)/2\}$. We note that $-S_{q-1} = S_{q-1}$ and $-S_{q+1} = S_{q+1}$. Using the functional expression, one can also easily obtain the following sufficient conditions for $f_n(x)$ to be a permutation polynomial of $\mathbb{F}_q$.

Theorem 4.1. *Let q be an odd prime power. Suppose $n \pmod{p}$, $n \pmod{(q-1)/2}$ and $n \pmod{(q+1)/2}$ are all equal to ± 1. Then $f_n(x)$ is a permutation polynomial of $\mathbb{F}_q$.*

Proof. Because one of $(q-1)/2$ and $(q+1)/2$ is even, both $n \equiv \pm 1 \pmod{(q-1)/2}$ and $n \equiv \pm 1 \pmod{(q+1)/2}$ imply that n must be odd. Therefore $n \equiv \pm 1 \pmod{p}$ implies that $n \equiv \pm 1 \pmod{2p}$.

The rest of proof follows directly from Theorem 2.10 and Eq. (4.1). Indeed, $f_n(x)$ permutes each subset S_p, S_{q-1} and S_{q+1} of $\mathbb{F}_q$ in the same way as linear polynomial $\pm x$ (but $f_n(x)$ is not necessarily equal to $\pm x$). □

We are interested in the necessary conditions when $f_n(x)$ is a PP of $\mathbb{F}_q$.

Proposition 4.2. *Let q be an odd prime power. If $f_n(x)$ is a permutation polynomial of $\mathbb{F}_q$, then*

(i) *n is odd.*
(ii) *$p \nmid 2n$.*
(iii) *$\gcd(n, q^2 - 1) = 1$.*
(iv) *$n \equiv \pm 1 \pmod p$.*

Proof. (i) and (ii) are obvious because $f_n(0) = 0$, $f_n(2) = 2n$, $f_n(-2) = (-1)^n 2n$ and $f_n(x)$ is a permutation polynomial of $\mathbb{F}_q$.

(iii) Because $f_n(x)$ is a permutation polynomial of $\mathbb{F}_q$ and $f_n(0) = 0$, there does not exist $x_0 \neq 0 \in S_{q-1} \cup S_{q+1}$ such that $f_n(x_0) = 0$. Let $x = y + y^{-1}$ where $y = \xi^i$ for some $1 \leqslant i \leqslant (q-3)/2$ or η^j for some $1 \leqslant j \leqslant (q-1)/2$. Then either $\xi^i + \xi^{-i} = 0$ if $i = \frac{q-1}{4}$ or $\eta^j + \eta^{-j} = 0$ if $j = \frac{q+1}{4}$.

Because n is odd, we let $\gcd(n, q-1) = \gcd(n, (q-1)/2) = d_1$ and $\gcd(n, q+1) = \gcd(n, (q+1)/2) = d_2$. If either $d_1 > 1$ or $d_2 > 1$ then we have either

$$f_n\big(\xi^{(q-1)/d_1} + \xi^{-(q-1)/d_1}\big) = \big(\xi^{(q-1)/d_1} + \xi^{-(q-1)/d_1}\big)\frac{\xi^{n(q-1)/d_1} - \xi^{-n(q-1)/d_1}}{\xi^{(q-1)/d_1} - \xi^{-(q-1)/d_1}} = 0,$$

or

$$f_n\big(\eta^{(q+1)/d_2} + \eta^{-(q+1)/d_2}\big) = \big(\eta^{(q+1)/d_2} + \eta^{-(q+1)/d_2}\big)\frac{\eta^{n(q+1)/d_2} - \eta^{-n(q+1)/d_2}}{\eta^{(q+1)/d_2} - \eta^{-(q+1)/d_2}} = 0.$$

Because n is odd, $d_1 > 1$ implies $d_1 \geqslant 3$ and $d_2 > 1$ implies $d_2 \geqslant 3$. Hence $(q-1)/d_1 < (q-1)/2$ and $(q+1)/d_2 < (q+1)/2$. However, that d_1 and d_2 are both odd implies that $\xi^i + \xi^{-i} \neq 0$ and $\eta^j + \eta^{-j} \neq 0$, a contradiction. Hence $d_1 = d_2 = 1$ and thus $\gcd(n, q^2 - 1) = \gcd(n, (q^2-1)/4) = 1$.

(iv) By Wilson's theorem, we have

$$\prod_{x \in \mathbb{F}_q,\, x \neq 0} f_n(x) = -1.$$

Similar to the proof of Lemma 5 in [5], we expand the product on the left-hand side and obtain some relations in terms of n.

We note that if $q \equiv 1 \pmod 4$ then $\xi^{(q-1)/4} + \xi^{-(q-1)/4} = 0 \in S_{q-1}$, and if $q \equiv 3 \pmod 4$ then $\eta^{(q+1)/4} + \eta^{-(q+1)/4} = 0 \in S_{q+1}$.

Let us consider $q \equiv 1 \pmod 4$ first. So $0 \in S_{q-1}$. Then

$$\begin{aligned}\prod_{x \in \mathbb{F}_q, x \neq 0} f_n(x) &= f(2)f(-2) \prod_{\substack{x \in S_{q-1} \cup S_{q+1} \\ x \neq 0}} f_n(x) \\ &= f(2)f(-2) \prod_{\substack{x \in S_{q-1} \\ x \neq 0}} f_n(x) \prod_{x \in S_{q+1}} f_n(x)\end{aligned}$$

$$= f(2)f(-2)\prod_{\substack{i=1\\ i\neq(q-1)/4}}^{(q-3)/2}\left(\xi^i+\xi^{-i}\right)\frac{\xi^{in}-\xi^{-in}}{\xi^i-\xi^{-i}}\prod_{j=1}^{(q-1)/2}\left(\eta^j+\eta^{-j}\right)\frac{\eta^{jn}-\eta^{-jn}}{\eta^j-\eta^{-j}}$$

$$= f(2)f(-2)\prod_{\substack{i=1\\ i\neq(q-1)/4}}^{(q-3)/2}\left(\xi^i+\xi^{-i}\right)\prod_{j=1}^{(q-1)/2}\left(\eta^j+\eta^{-j}\right),$$

the last equation holds because $\gcd(n, q-1) = 1$ and $\gcd(n, q+1) = 1$. Hence

$$\prod_{x\in\mathbb{F}_q, x\neq 0} f_n(x) = f(2)f(-2)\prod_{\substack{x\in S_{q-1}\cup S_{q+1}\\ x\neq 0}} x.$$

By Wilson's theorem again, we have

$$\prod_{\substack{x\in S_{q-1}\cup S_{q+1}\\ x\neq 0}} x = \frac{1}{4}.$$

Then we obtain

$$-1 = \prod_{x\in\mathbb{F}_q,\, x\neq 0} f_n(x) = f(2)f(-2)\frac{1}{4} = (-1)^n n^2 = -n^2.$$

Therefore, $n \equiv \pm 1 \pmod p$.

Similarly, if $q \equiv 3 \pmod 4$ then $0 \in S_{q+1}$. Because $\gcd(n, q^2-1) = 1$, we have

$$\prod_{x\in\mathbb{F}_q, x\neq 0} f_n(x) = f(2)f(-2)\prod_{\substack{x\in S_{q-1}\cup S_{q+1}\\ x\neq 0}} f_n(x)$$

$$= f(2)f(-2)\prod_{x\in S_{q-1}} f_n(x)\prod_{\substack{x\in S_{q+1}\\ x\neq 0}} f_n(x)$$

$$= f(2)f(-2)\prod_{i=1}^{(q-3)/2}\left(\xi^i+\xi^{-i}\right)\frac{\xi^{in}-\xi^{-in}}{\xi^i-\xi^{-i}}\prod_{\substack{j=1\\ j\neq(q+1)/4}}^{(q-1)/2}\left(\eta^j+\eta^{-j}\right)\frac{\eta^{jn}-\eta^{-jn}}{\eta^j-\eta^{-j}}$$

$$= f(2)f(-2)\prod_{i=1}^{(q-3)/2}\left(\xi^i+\xi^{-i}\right)\prod_{\substack{j=1\\ j\neq(q+1)/4}}^{(q-1)/2}\left(\eta^j+\eta^{-j}\right)$$

$$= f(2)f(-2)\prod_{\substack{x\in S_{q-1}\cup S_{q+1}\\ x\neq 0}} x.$$

Therefore we obtain $n \equiv \pm 1 \pmod p$ in this case as well. □

Denote $n_1 = (n)_{q-1}$ and $n_2 = (n)_{q+1}$. Because n is odd, n_1 and n_2 are odd. Then we can present the permutation polynomial $f_n(x)$ of $\mathbb{F}_q$ as

$$f_n(x) = \begin{cases} 2n & \text{if } x = 2; \\ -2n & \text{if } x = -2; \\ f_{n_1}(x) & \text{if } x \in S_{q-1}; \\ f_{n_2}(x) & \text{if } x \in S_{q+1}. \end{cases}$$

Let m be the unique integer such that $1 \leqslant m \leqslant (q-3)/4$ and $n_1 \equiv \pm m \pmod{\frac{q-1}{2}}$. Then $f_{n_1}(x) = \pm f_m(x)$ if $x \in S_{q-1}$. Indeed, if $n_1 < (q-1)/2$, then $n_1 = m$. If $n_1 > (q-1)/2$, then $y^{(q-1)/2+m} - y^{-((q-1)/2+m)} = \pm(y^m - y^{-m})$ and thus $f_{n_1+\frac{q-1}{2}}(x) = \pm f_m(x)$. Similarly, Let ℓ be unique integer such that $1 \leqslant \ell \leqslant (q-1)/4$ and $n_2 \equiv \pm \ell \pmod{\frac{q+1}{2}}$. Then $f_{n_2}(x) = \pm f_\ell(x)$ if $x \in S_{q+1}$.

Note that if $f_n(x)$ is a PP then $m \neq 0$ and $\ell \neq 0$. In the following we want to show that $m = \ell = 1$ when $q = p$ by using the similar arguments as in [3–5].

Because $n \equiv \pm 1 \pmod{p}$, using Hermite's criterion, we now deduce the following result similar to the key lemma in [4] or [5].

Lemma 4.3. *Assume that $f_n(x)$ is a PP of $\mathbb{F}_q$. Let m, ℓ be defined as above. Let $\xi = \zeta_{q-1}$ and $\eta = \zeta_{q+1}$, where ζ_d is a primitive d-th root of unity in $\mathbb{F}_{q^2}$. Then for each $r = 1, \ldots, (q-3)/2$,*

$$\sum_{i=0}^{q-2} \bigl(f_m(\xi^i + \xi^{-i})\bigr)^{2r} + \sum_{j=0}^{q} \bigl(f_\ell(\eta^j + \eta^{-j})\bigr)^{2r} + 2^{2r+2} = 2\bigl((2m)^{2r} + (2\ell)^{2r}\bigr). \tag{4.2}$$

Proof.

$$\begin{aligned} \sum_{i=0}^{q-2} \bigl(f_m(\xi^i + \xi^{-i})\bigr)^{2r} &= \sum_{\substack{i=1 \\ i \neq (q-1)/2}}^{q-2} \bigl(f_m(\xi^i + \xi^{-i})\bigr)^{2r} + \bigl(f_m(2)\bigr)^{2r} + \bigl(f_m(-2)\bigr)^{2r} \\ &= 2 \sum_{x \in S_{q-1}} \bigl(f_m(\xi^i + \xi^{-i})\bigr)^{2r} + 2(2m)^{2r}. \end{aligned}$$

Similarly,

$$\sum_{j=0}^{q} \bigl(f_\ell(\eta^j + \eta^{-j})\bigr)^{2r} = 2 \sum_{x \in S_{q+1}} \bigl(f_\ell(\eta^j + \eta^{-j})\bigr)^{2r} + 2(2\ell)^{2r}.$$

Because $n \equiv \pm 1 \pmod{p}$, Hermite's criterion gives

$$\sum_{x \in S_{q-1}} \bigl(f_m(\xi^i + \xi^{-i})\bigr)^{2r} + \sum_{x \in S_{q+1}} \bigl(f_\ell(\eta^j + \eta^{-j})\bigr)^{2r} + 2^{2r+1} = 0,$$

and the result follows. □

Again we will apply Lemma 4.3 together with basic properties of roots of unity such as

$$\sum_{i=0}^{q-2} \xi^{is} = \begin{cases} 0, & (q-1) \nmid s; \\ -1, & (q-1) \mid s; \end{cases} \qquad \sum_{j=0}^{q} \eta^{js} = \begin{cases} 0, & (q+1) \nmid s; \\ 1, & (q+1) \mid s. \end{cases} \tag{4.3}$$

Because $f_n(x) = xE_{n-1}(x)$, using Eq. (2.5) in [4], we obtain

$$\left[f_n\left(u^i + u^{-i}\right)\right]^{2r} = \sum_{v=0}^{2r} \sum_{k=0}^{2r(n-1)} \left(\sum_{j \geqslant 0} (-1)^j \binom{2r}{j} \binom{k - jn + 2r - 1}{2r - 1} \right) \binom{2r}{v} u^{2i(nr-k-v)}. \tag{4.4}$$

From Eqs. (4.3) and (4.4) each identity (4.2) gives an equation in terms of m and ℓ over prime field $\mathbb{F}_p$. As in [4,5], for $r \leqslant 2$, since m and ℓ are less than $q/4$, one needs evaluate only the constant term in the expansion of $f_m(\xi^i + \xi^{-i})^{2r}$ for $i \leqslant q-2$ and $f_\ell(\eta^j + \eta^{-j})^{2r}$ for $j \leqslant q$. For $r \geqslant 3$, the ranges have to be subdivided because in some cases the coefficients of $u^{q\pm 1}$ may have to be considered.

Let $h_r := h_r(m, \ell) = 0$ be the series of polynomial identities obtained from Eq. (4.2) by setting $r = 1, 2, \ldots$. Without loss of generality, we can assume the coefficients are integers.

Lemma 4.4. (i) $h_1 = 2m^2 + 2\ell^2 + m - \ell - 4$.
(ii) $h_2 = 3m^4 + 3\ell^4 + m^3 - \ell^3 - m + \ell - 6$.

Proof. (i) For $r = 1$, the constant term of $[f_n(u^i + u^{-i})]^2$ happens when $n = k + v$ where $0 \leqslant v \leqslant 2$. Hence $k = n - v$ and the constant term is

$$\sum_{v=0}^{2} \sum_{j \geqslant 0} (-1)^j \binom{2}{j} \binom{n - v - jn + 1}{1} \binom{2}{v} = (n + 1 - 2) + 2n + (n - 1) = 4n - 2.$$

Plug $r = 1$ into Eq. (4.2), we obtain

$$-(4m - 2) + 4\ell - 2 + 16 = 2\left(4m^2 + 4\ell^2\right).$$

Hence $h_1 = 2m^2 + 2\ell^2 + m - \ell - 4$.

(ii) For $r = 2$, the constant term of $[f_n(u^i + u^{-i})]^4$ happens when $2n = k + v$ where $0 \leqslant v \leqslant 4$. Hence $k = 2n - v$ and the constant term is

$$\sum_{v=0}^{4} \sum_{j \geqslant 0} (-1)^j \binom{4}{j} \binom{2n - v - jn + 3}{3} \binom{4}{v}.$$

This expands to $(\binom{2n+3}{3} - 4\binom{n+3}{3} + 6) + 4(\binom{2n+2}{3} - 4\binom{n+2}{3}) + 6(\binom{2n+1}{3} - 4\binom{n+1}{3}) + 4(\binom{2n}{3} - 4\binom{n}{3}) + (\binom{2n-1}{3} - 4\binom{n-1}{3}) = (32n^3 - 32n)/3 + 6$.

Plug $r = 2$ into Eq. (4.2), we obtain

$$-\left(\left(32m^3 - 32m\right)/3 + 6\right) + \left(32\ell^3 - 32\ell\right)/3 + 6 + 64 = 2\left(16m^4 + 16\ell^4\right).$$

Hence $h_2 = 3m^4 + 3\ell^4 + m^3 - \ell^3 - m + \ell - 6$. □

Let $D := m - \ell$ and $P := m\ell$. We have $m^2 + \ell^2 = D^2 + 2P$, $m^3 - \ell^3 = D^3 + 3PD$, and $m^4 + \ell^4 = D^4 + 4PD^2 + 2P^2$. Using h_1 we obtain $P = 1 - D/4 - D^2/2$. Plug it into h_2, we obtain

$$3D^4 - 14D^3 + 71D^2 - 16D = 0.$$

Obviously $D = 0$ is a solution. We need to whether there is a solution for

$$3D^3 - 14D^2 + 71D - 16 = 0.$$

As in [5], there are infinity prime numbers such that $3D^3 - 14D^2 + 71D - 16 = 0$ has nonzero solutions. Thus we need to take $r = 3$ and we have to consider different cases.

Lemma 4.5. *We have the following expressions for* h_3:

- *if* $m < \frac{q-1}{6}$ *and* $\ell < \frac{q+1}{6}$, *then*

$$h_3 = h_{3a} := 80\big(m^6 + \ell^6\big) + 22\big(m^5 - \ell^5\big) - 20\big(m^3 - \ell^3\big) + 23(m - \ell) - 160;$$

- *if* $\frac{q-1}{6} \leqslant m \leqslant \frac{q-3}{4}$ *and* $\frac{q+1}{6} \leqslant \ell \leqslant \frac{q+1}{4}$ *(hence* $q \geqslant 11$*), then*

$$h_3 = h_{3b} := 8\left(h_{3a} + 80\sum_{v=0}^{6}\binom{6}{v}\binom{3m - v + \frac{11}{2}}{5} - 80\sum_{v=0}^{6}\binom{6}{v}\binom{3\ell - v + \frac{9}{2}}{5}\right);$$

- *if* $\frac{q-1}{6} \leqslant m \leqslant \frac{q-3}{4}$ *and* $\ell < \frac{q+1}{6}$ *(hence* $q \geqslant 11$*), then*

$$h_3 = h_{3c} := 16\left(h_{3a} + 80\sum_{v=0}^{6}\binom{6}{v}\binom{3m - v + \frac{11}{2}}{5}\right);$$

- *if* $m < \frac{q-1}{6}$ *and* $\frac{q+1}{6} \leqslant \ell \leqslant \frac{q+1}{4}$, *then*

$$h_3 = h_{3d} := 16\left(h_{3a} - 80\sum_{v=0}^{6}\binom{6}{v}\binom{3\ell - v + \frac{9}{2}}{5}\right).$$

Proof. Take $r = 3$, we need to consider coefficients in Eq. (4.4) such that $3m - k - v \equiv 0 \pmod{q-1}$ and $3\ell - k - v \equiv 0 \pmod{q+1}$. Then the result follows from a case analysis and a computer calculation. □

We observe that $h_{3d}(m, \ell) = h_{3c}(-\ell, -m)$. In the expanded form, we have $h_{3b} = 640(m^6 + \ell^6) + 1472(m^5 - \ell^5) + 1080(m^4 + l^4) + 1640(m^3 - l^3) + 780(m^2 + l^2) + 493(m - \ell) - 1205$ and $h_{3c} = 1280\ell^6 - 352\ell^5 + 320\ell^3 - 368\ell + 1280m^6 + 2944m^5 + 2160m^4 + 3280m^3 + 1560m^2 + 986m - 2485$.

For $r = 4$ we define

$$C_{q-1,4}(m) = \sum_{v=0}^{8}\binom{4m - v + \frac{15}{2}}{7}\binom{8}{v}, \qquad C_{q-1,3}(m) = \sum_{v=0}^{8}\binom{3m - v + \frac{15}{2}}{7}\binom{8}{v},$$

$$C_{q+1,4}(\ell) = \sum_{v=0}^{8}\binom{4\ell - v + \frac{13}{2}}{7}\binom{8}{v}, \qquad C_{q+1,3}(\ell) = \sum_{v=0}^{8}\binom{3\ell - v + \frac{13}{2}}{7}\binom{8}{v}.$$

Then we obtain h_4 similarly. We note that one can also get the symbolic expressions from Eq. (4.4) and Lemma 4.3 using a computer package like MAGMA or SAGE.

Lemma 4.6. *We have the following expressions for* h_4:

- *if* $m \leqslant \frac{q-3}{8}$ *and* $1 \leqslant \ell \leqslant \frac{q-1}{8}$ *then*

$$\begin{aligned} h_{4a} &= \frac{315}{2^8}\left(2(2m)^8 + 2(2\ell)^8 - 2^{10} + \sum_{v=0}^{8}\sum_{k=0}^{8(m-1)}\sum_{t\geqslant 0}(-1)^t\binom{8}{t}\binom{4m-v-tm+7}{7}\binom{8}{v}\right. \\ &\quad \left. - \sum_{v=0}^{8}\sum_{k=0}^{8(\ell-1)}\sum_{t\geqslant 0}(-1)^t\binom{8}{t}\binom{4\ell-v-t\ell+7}{7}\binom{8}{v}\right) \\ &= 630\big(m^8+\ell^8\big) + 151\big(m^7-\ell^7\big) + 140\big(m^5+\ell^5\big) + 154\big(m^3-\ell^3\big) + 165(m-\ell) - 1260; \end{aligned}$$

- *if* $m \leqslant \frac{q-3}{8}$ *and* $\frac{q-1}{8} < \ell \leqslant \frac{q+1}{6}$ *then*

$$h_{4b} = 1260\left(\frac{2^8}{315}h_{4a} - 2C_{q+1,4}(\ell)\right);$$

- *if* $m \leqslant \frac{q-3}{8}$ *and* $\frac{q+1}{6} < \ell \leqslant \frac{q-1}{4}$ *then*

$$h_{4c} = 1260\left(\frac{2^8}{315}h_{4a} - 2C_{q+1,4}(\ell) + 16C_{q+1,3}(\ell)\right);$$

- *if* $\frac{q-3}{8} < m \leqslant \frac{q+1}{6}$ *and* $1 \leqslant \ell \leqslant \frac{q-1}{8}$ *then*

$$h_{4d} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m)\right);$$

- *if* $\frac{q-3}{8} < m \leqslant \frac{q+1}{6}$ *and* $\frac{q-1}{8} < \ell \leqslant \frac{q+1}{6}$ *then*

$$h_{4e} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m) - 2C_{q+1,4}(\ell)\right);$$

- *if* $\frac{q-3}{8} < m \leqslant \frac{q+1}{6}$ *and* $\frac{q+1}{6} < \ell \leqslant \frac{q-1}{4}$ *then*

$$h_{4f} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m) - 2C_{q+1,4}(\ell) + 16C_{q+1,3}(\ell)\right);$$

- *if* $\frac{q-1}{6} < m \leqslant \frac{q-3}{4}$ *and* $1 \leqslant \ell \leqslant \frac{q-1}{8}$ *then*

$$h_{4g} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m) - 16C_{q-1,3}(m)\right);$$

- *if* $\frac{q-1}{6} < m \leqslant \frac{q-3}{4}$ *and* $\frac{q-1}{8} < \ell \leqslant \frac{q+1}{6}$ *then*

$$h_{4h} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m) - 16C_{q-1,3}(m) - 2C_{q+1,4}(\ell)\right);$$

- *if* $\frac{q-1}{6} < m \leqslant \frac{q-3}{4}$ *and* $\frac{q+1}{6} \leqslant \ell \leqslant \frac{q-1}{4}$ *then*

$$h_{4i} = 1260\left(\frac{2^8}{315}h_{4a} + 2C_{q-1,4}(m) - 16C_{q-1,3}(m) - 2C_{q+1,4}(\ell) + 16C_{q+1,3}(\ell)\right).$$

Table 1
The third and fourth generator of the ideal I.

	$m \leqslant \frac{q-3}{8}$	$m \leqslant \frac{q-3}{6}$	$m = \frac{q-1}{6}$	$m \leqslant \frac{q-3}{4}$
$\ell \leqslant \frac{q-1}{8}$	h_{3a}, h_{4a} (case I)	h_{3a}, h_{4d} (case II)	h_{3c}, h_{4d} (case III)	h_{3c}, h_{4g} (case IV)
$\ell \leqslant \frac{q-1}{6}$	h_{3a}, h_{4b} (case V)	h_{3a}, h_{4e} (case VI)	h_{3c}, h_{4e} (case VII)	h_{3c}, h_{4h} (case VIII)
$\ell = \frac{q+1}{6}$	h_{3d}, h_{4b} (case IX)	h_{3d}, h_{4e} (case X)	h_{3b}, h_{4e} (case XI)	h_{3b}, h_{4h} (case XII)
$\ell \leqslant \frac{q-1}{4}$	h_{3d}, h_{4c} (case XIII)	h_{3d}, h_{4f} (case XIV)	h_{3b}, h_{4f} (case XV)	h_{3b}, h_{4i} (case XVI)

Table 2
Leading coefficients in bivariate Gröbner bases over $\mathbb{Z}$.

Case	Leading coefficients > 1	Prime divisors
I	2, 4, 6, 12	2, 3
II, V	3, 315, 152073086445	3, 5, 7, 19, 73, 157, 739
III, IV, VII, VIII, IX, X, XIII, XIV,	3, 15, 315	3, 5, 7
VI	2, 3, 6, 9658530	2, 3, 5, 7, 15331
XI, XII, XV, XVI	3, 15	3, 5

Now we have the following 16 cases in Table 1. We number with Roman digits the 16 cases described Table 1, starting from the upper-left corner and going right and down. Using MAGMA, the idea I generated by h_1, h_2, h_{3a}, h_{4a} in the polynomial ring $\mathbb{Z}[m, \ell]$ in Case I has Gröbner basis as follows:

$$m^2 + 2 * m + 7 * l^2 - 2 * l - 8,$$

$$m * l + 2 * m + 4 * l^3 + 15 * l^2 - 6 * l - 16,$$

$$3 * m + 12 * l^2 - 3 * l - 12,$$

$$2 * l^4 + 16 * l^2 - 18,$$

$$8 * l^3 - 8 * l,$$

$$24 * l^2 - 24.$$

This means that in this case $m = \ell = 1$ for $p \geqslant 5$.

In each of Cases II–XVI the ideal I generated by h_1, h_2 and corresponding h_3 and h_4 contains a constant polynomial. We collect all the leading coefficients of the polynomials in each basis in Table 2.

For each prime $p \geqslant 5$ appearing in the last column of Table 2 we computed a Gröbner basis of the image of the ideal I in the polynomial ring $\mathbb{F}_p[m, \ell]$ using MAGMA.

A synopsis of the output is given in Table 3. They all turn out to be special cases of $m \equiv \ell \equiv \pm 1 \pmod{p}$. Hence $m = \ell = 1$. In the same way as in [3–5] we conclude with the following theorem.

Theorem 4.7. *Let $q = p \geqslant 5$. Then $f_n(x)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $n \equiv \pm 1 \pmod{p}$, $n \equiv \pm 1 \pmod{(q-1)/2}$, and $n \equiv \pm 1 \pmod{(q+1)/2}$.*

We expect the result works for $q = p^2$ as well, which involves further computation for $r = 5$, and thus decide not to pursue it further.

5. Conclusions

In this paper we introduced the notion of n-th Dickson polynomials $D_{n,k}(x, a)$ of the $(k+1)$-th kind and n-th reversed Dickson polynomials $D_{n,k}(x, a)$ of the $(k+1)$-th kind in Section 2. We studied basic properties of Dickson polynomials of the $(k+1)$-th kind and their relations to Dickson

Table 3
Gröbner bases over $\mathbb{F}_p$ where $p \geqslant 5$.

Case	Polynomials
II	$m \equiv \ell \equiv \pm 1 \pmod{p}$ where $p = 5, 7$ $m \equiv \ell \equiv 1 \pmod{p}$ where $p = 19, 739$ $m \equiv \ell \equiv -1 \pmod{p}$ where $p = 73, 157$
III, IV, VII, VIII	$m \equiv \ell \equiv \pm 1 \pmod{5}$, $m \equiv \ell \equiv 1 \pmod{7}$
V	$m \equiv \ell \equiv \pm 1 \pmod{p}$ where $p = 5, 7$ $m \equiv \ell \equiv 1 \pmod{p}$ where $p = 73, 157$ $m \equiv \ell \equiv -1 \pmod{p}$ where $p = 19, 739$
VI	$m \equiv \ell \equiv \pm 1 \pmod{p}$ where $p = 5, 7, 15331$
IX, X, XIII, XIV	$m \equiv \ell \equiv \pm 1 \pmod{5}$, $m \equiv \ell \equiv -1 \pmod{7}$
XI, XII, XV, XVI	$m \equiv \ell \equiv \pm 1 \pmod{p}$ where $p = 5$

polynomials of the first two kinds, the recurrence relation of Dickson polynomials of the $(k+1)$-th kind in terms of degrees for a fixed k and its generating function, functional expressions and their reductions, as well as differential recurrence relations. Finally we considered the factorization and the permutation behavior of Dickson polynomials of the third kind. Here, we only completely described the permutation behavior of the Dickson polynomial of the third kind over any prime field. Similar result is expected to be true over $\mathbb{F}_{q^2}$, however, it seems that it is necessary to invent more tools to deal with arbitrary extension fields. For the reversed Dickson polynomials of the $(k+1)$-th kind, it would be more interesting to study further in a similar way as that of the reversed Dickson polynomial of the first kind started in [7].

Acknowledgments

Qiang Wang wants to thank Stephen D. Cohen for kindly sending him papers [3–5]. We also want to thank Stephen D. Cohen and Gary L. Mullen for spending some time on reading a draft of this paper and suggesting some future directions. Finally we thank the anonymous referees for their helpful suggestions.

Appendix A. Numeric expression for h_3 and h_4

$h3a := 160 * l^6 - 44 * l^5 + 40 * l^3 + 160 * m^6 + 44 * m^5 - 40 * m^3 - 46 * l + 46 * m - 320;$

$h3b := 640 * l^6 - 1472 * l^5 + 1080 * l^4 - 1640 * l^3 + 780 * l^2 + 640 * m^6 + 1472 * m^5 + 1080 * m^4 + 1640 * m^3 + 780 * m^2 - 493 * l + 493 * m - 1205;$

$h3c := 1280 * l^6 - 352 * l^5 + 320 * l^3 + 1280 * m^6 + 2944 * m^5 + 2160 * m^4 + 3280 * m^3 + 1560 * m^2 - 368 * l + 986 * m - 2485;$

$h3d := 1280 * l^6 - 2944 * l^5 + 2160 * l^4 - 3280 * l^3 + 1560 * l^2 + 1280 * m^6 + 352 * m^5 - 320 * m^3 - 986 * l + 368 * m - 2485;$

$h4a := 630 * l^8 - 151 * l^7 + 140 * l^5 - 154 * l^3 + 630 * m^8 + 151 * m^7 - 140 * m^5 + 154 * m^3 + 165 * l - 165 * m - 1260;$

$h4b := 645120 * l^8 - 2251776 * l^7 + 1835008 * l^6 - 4214784 * l^5 + 2437120 * l^4 - 2010624 * l^3 + 546112 * l^2 + 645120 * m^8 + 154624 * m^7 - 143360 * m^5 + 157696 * m^3 + 37704 * l - 168960 * m - 1279215;$

$h4c := 645120 * l^8 - 12288 * l^7 - 777728 * l^6 + 4058880 * l^5 - 3731840 * l^4 + 4243008 * l^3 - 1911392 * l^2 + 645120 * m^8 + 154624 * m^7 - 143360 * m^5 + 157696 * m^3 + 825240 * l - 168960 * m - 1367415;$

$h4d := 645120 * l^8 - 154624 * l^7 + 143360 * l^5 - 157696 * l^3 + 645120 * m^8 + 2251776 * m^7 + 1835008 * m^6 + 4214784 * m^5 + 2437120 * m^4 + 2010624 * m^3 + 546112 * m^2 + 168960 * l - 37704 * m - 1279215;$

$h4e := 645120 * l^8 - 2251776 * l^7 + 1835008 * l^6 - 4214784 * l^5 + 2437120 * l^4 - 2010624 * l^3 + 546112 * l^2 + 645120 * m^8 + 2251776 * m^7 + 1835008 * m^6 + 4214784 * m^5 + 2437120 * m^4 + 2010624 * m^3 + 546112 * m^2 + 37704 * l - 37704 * m - 1268190;$

$h4f := 645120 * l^8 - 12288 * l^7 - 777728 * l^6 + 4058880 * l^5 - 3731840 * l^4 + 4243008 * l^3 - 1911392 * l^2 + 645120 * m^8 + 2251776 * m^7 + 1835008 * m^6 + 4214784 * m^5 + 2437120 * m^4 + 2010624 * m^3 + 546112 * m^2 + 825240 * l - 37704 * m - 1356390;$

$h4g := 645120 \ast l^8 - 154624 \ast l^7 + 143360 \ast l^5 - 157696 \ast l^3 + 645120 \ast m^8 + 12288 \ast m^7 - 777728 \ast m^6 - 4058880 \ast m^5 - 3731840 \ast m^4 - 4243008 \ast m^3 - 1911392 \ast m^2 + 168960 \ast l - 825240 \ast m - 1367415;$

$h4h := 645120 \ast l^8 - 2251776 \ast l^7 + 1835008 \ast l^6 - 4214784 \ast l^5 + 2437120 \ast l^4 - 2010624 \ast l^3 + 546112 \ast l^2 + 645120 \ast m^8 + 12288 \ast m^7 - 777728 \ast m^6 - 4058880 \ast m^5 - 3731840 \ast m^4 - 4243008 \ast m^3 - 1911392 \ast m^2 + 37704 \ast l - 825240 \ast m - 1356390;$

$h4i := 645120 \ast l^8 - 12288 \ast l^7 - 777728 \ast l^6 + 4058880 \ast l^5 - 3731840 \ast l^4 + 4243008 \ast l^3 - 1911392 \ast l^2 + 645120 \ast m^8 + 12288 \ast m^7 - 777728 \ast m^6 - 4058880 \ast m^5 - 3731840 \ast m^4 - 4243008 \ast m^3 - 1911392 \ast m^2 + 825240 \ast l - 825240 \ast m - 1444590.$

References

[1] M. Bhargava, M.E. Zieve, Factorizing Dickson polynomials over finite fields, Finite Fields Appl. 5 (1999) 103–111.

[2] W.S. Chou, The factorization of Dickson polynomials over finite fields, Finite Fields Appl. 3 (1997) 84–96.

[3] M. Cipu, Dickson polynomials that are permutations, Serdica Math. J. 30 (2004) 177–194.

[4] M. Cipu, S.D. Cohen, Dickson polynomial permutations and Gröbner bases, Contemp. Math. 461 (2008) 79–90.

[5] S.D. Cohen, Dickson polynomials of the second kind that are permutations, Canad. J. Math. 46 (2) (1994) 225–238.

[6] A. Dujella, I. Gusić, Decomposition of a recursive family of polynomials, Monatsh. Math. 152 (2007) 97–104.

[7] X.D. Hou, G.L. Mullen, J. A Sellers, J.L. Yucas, Reversed Dickson polynomials over finite fields, Finite Fields Appl. 15 (6) (2009) 748–773.

[8] R. Lidl, G.L. Mullen, G. Turnwald, Dickson Polynomials, Longman Scientific and Technical, 1993.

[9] T. Stoll, Complete decomposition of Dickson-type polynomials and related Diophantine equations, J. Number Theory 128 (5) (2008) 1157–1181.