AIMS Mathematics

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

AIMS Mathematics, 2(2): 244–259
DOI:10.3934/Math.2017.2.244
Received: 15 March 2017
Accepted: 18 April 2017
Published: 20 April 2017

Research article

Permutational behavior of reversed Dickson polynomials over finite fields

Kaimin Cheng

School of Mathematics and information, China west normal University, Nanchong 637009, P.R. China

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

Abstract: In this paper, we develop the method presented previously by Hong, Qin and Zhao to obtain several results on the permutational behavior of the reversed Dickson polynomial $D_{n,k}(1,x)$ of the $(k+1)$-th kind over the finite field $\mathbb{F}_q$. Particularly, we present the explicit evaluation of the first moment $\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)$. Our results extend the results of Hong, Qin and Zhao to the general $k \geq 0$ case.

Keywords: Permutation polynomial; Reversed Dickson polynomial of the $(k+1)$-th kind; Finite field; Generating function

1. Introduction

Permutation polynomials and Dickson polynomials are two of the most important topics in the area of finite fields. Let $\mathbb{F}_q$ be the finite field of characteristic p with q elements. Let $\mathbb{F}_q[x]$ be the ring of polynomials over $\mathbb{F}_q$ in the indeterminate x. If the polynomial $f(x) \in \mathbb{F}_q[x]$ induces a bijective map from $\mathbb{F}_q$ to itself, then $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of $\mathbb{F}_q$. Properties, constructions and applications of permutation polynomials may be found in [4], [5] and [6]. Associated to any integer $n \geq 0$ and a parameter $a \in \mathbb{F}_q$, the n-th *Dickson polynomials of the first kind and of the second kind*, denoted by $D_n(x,a)$ and $E_n(x,a)$, are defined for $n \geq 1$ by

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

and

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

respectively, and $D_0(x,a) := 2$, $E_0(x,a) := 1$. It is well known that $D_n(x,0)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$, and if $a \neq 0$, then $D_n(x,a)$ induces a permutation of $\mathbb{F}_q$ if and only if $\gcd(n, q^2 - 1) = 1$. There are lots of published results on permutational properties of Dickson polynomial $E_n(x, a)$ of the second kind (see, for example, [1]).

The *reversed Dickson polynomial of the first kind*, denoted by $D_n(a, x)$, was introduced in [3] and defined as follows

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

if $n \geq 1$ and $D_0(a, x) = 2$, where $[\frac{n}{2}]$ means the largest integer no more than $\frac{n}{2}$. Wang and Yucas [7] extended this concept to that of *the n-th reversed Dickson polynomial of* $(k+1)$*-th kind* $D_{n,k}(a, x) \in \mathbb{F}_q[x]$, which is defined for $n \geq 1$ by

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

and $D_{0,k}(a, x) = 2 - k$. Some families of permutation polynomials from the revered Dickson polynomials of the first kind were obtained in [3]. Hong, Qin and Zhao [2] studied the revered Dickson polynomial $E_n(a, x)$ of the second kind that is defined for $n \geq 1$ by

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

and $E_0(a, x) = 1$. In fact, they gave some necessary conditions for the revered Dickson polynomial $E_n(1, x)$ of the second kind to be a permutation polynomial of $\mathbb{F}_q$. Regarding the revered Dickson polynomial $D_{n,2}(a, x) \in \mathbb{F}_q[x]$ of the third kind, from its definition one can derive that

$$D_{n,2}(a, x) = aE_{n-1}(a, x) \tag{1.2}$$

for each $x \in \mathbb{F}_q$. Using (1.2), one can deduce immediately from [2] the similar results on the permutational behavior of the reversed Dickson polynomial $D_{n,2}(a, x)$ of the third kind.

In this paper, our main goal is to develop the method presented by Hong, Qin and Zhao in [2] to investigate the reversed Dickson polynomial $D_{n,k}(a, x)$ of the $(k+1)$-th kind which is defined by (1.1) if $n \geq 1$ and $D_{0,k}(a, x) := 2 - k$. For $a \neq 0$, we write $x = y(a - y)$ with an indeterminate $y \neq \frac{a}{2}$. Then one can rewrite $D_{n,k}(a, x)$ as

$$D_{n,k}(a, x) = \frac{((k-1)a - (k-2)y)y^n - (a + (k-2)y)(a-y)^n}{2y - a}. \tag{1.3}$$

We have

$$D_{n,k}\Big(a, \frac{a^2}{4}\Big) = \frac{(kn - k + 2)a^n}{2^n}. \tag{1.4}$$

In fact, (1.3) and (1.4) follow from Theorem 2.2 (i) and Theorem 2.4 (i) below. It is easy to see that if $\mathrm{char}(\mathbb{F}_q) = 2$, then $D_{n,k}(a, x) = E_n(a, x)$ if k is odd and $D_{n,k}(a, x) = D_n(a, x)$ if k is even. We also find that $D_{n,k}(a, x) = D_{n,k+p}(a, x)$, so we can restrict $p > k$. Thus we always assume $p = \mathrm{char}(\mathbb{F}_q) \geq 3$ in what follows.

The paper is organized as follows. First in section 2, we study the properties of the reversed Dickson polynomial $D_{n,k}(a, x)$ of the $(k+1)$-th kind. Subsequently, in Section 3, we prove a necessary condition for the reversed Dickson polynomial $D_{n,k}(1, x)$ of the $(k+1)$-th kind to be a permutation polynomial of $\mathbb{F}_q$ and then introduce an auxiliary polynomial to present a characterization for $D_{n,k}(1, x)$ to be a permutation of $\mathbb{F}_q$. From the Hermite criterion [4] one knows that a function $f : \mathbb{F}_q \to \mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$ if and only if the i-th moment

$$\sum_{a\in\mathbb{F}_q} f(a)^i = \begin{cases} 0, & \text{if } 0 \le i \le q-2, \\ -1, & \text{if } i = q-1. \end{cases}$$

Thus to understand well the permutational behavior of the reversed Dickson polynomial $D_{n,k}(1, x)$ of the $(k+1)$-th kind, we would like to know if the i-th moment $\sum_{a\in\mathbb{F}_q} D_{n,k}(1, a)^i$ is computable. We are able to treat with this sum when $i = 1$. The final section is devoted to the computation of the first moment $\sum_{a\in\mathbb{F}_q} D_{n,k}(1, a)$.

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

In this section, we study the properties of the reversed Dickson polynomials $D_{n,k}(a, x)$ of the $(k+1)$-th kind. Clearly, if $a = 0$, then

$$D_{n,k}(0, x) = \begin{cases} 0, & \text{if } n \text{ is odd}, \\ (-1)^{\frac{n}{2}+1}(k-2)x^{\frac{n}{2}}, & \text{if } n \text{ is even}. \end{cases}$$

Therefore, $D_{n,k}(0, x)$ is a PP (permutation polynomial) of $\mathbb{F}_q$ if and only if n is an even integer with $\gcd(\frac{n}{2}, q-1) = 1$. In what follows, we always let $a \in \mathbb{F}_q^*$. First, we give a basic fact as follows.

Lemma 2.1. *[4] Let $f(x) \in \mathbb{F}_q[x]$. Then $f(x)$ is a PP of $\mathbb{F}_q$ if and only if $cf(dx)$ is a PP of $\mathbb{F}_q$ for any given $c, d \in \mathbb{F}_q^*$.*

Then we can deduce the following result.

Theorem 2.2. *Let $a, b \in \mathbb{F}_q^*$. Then the following are true.*

(i). *One has $D_{n,k}(a, x) = \frac{a^n}{b^n} D_{n,k}(b, \frac{b^2}{a^2}x)$.*

(ii). *We have that $D_{n,k}(a, x)$ is a PP of $\mathbb{F}_q$ if and only if $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_q$.*

Proof. (i). By the definition of $D_{n,k}(a, x)$, we have

$$\begin{aligned}\frac{a^n}{b^n} D_{n,k}\Big(b, \frac{b^2}{a^2}x\Big) =& \frac{a^n}{b^n} \sum_{i=0}^{[\frac{n}{2}]} \frac{n-ki}{n-i} \binom{n-i}{i} (-1)^i b^{n-2i} \frac{b^{2i}}{a^{2i}} x^i \\ =& \sum_{i=0}^{[\frac{n}{2}]} \frac{n-ki}{n-i} \binom{n-i}{i} (-1)^i a^{n-2i} x^i \\ =& D_{n,k}(a, x)\end{aligned}$$

as required. Part (i) is proved.

(ii). Taking $b = 1$ in part (i), we have

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

It then follows from Lemma 2.1 that $D_{n,k}(a, x)$ is a PP of $\mathbb{F}_q$ if and only if $D_{n,k}(1, x)$ is a PP of $\mathbb{F}_q$. This completes the proof of part (ii). So Theorem 2.2 is proved. □

Theorem 2.2 tells us that to study the permutational behavior of $D_{n,k}(a,x)$ over $\mathbb{F}_q$, one only needs to consider that of $D_{n,k}(1,x)$. In the following, we supply several basic properties on the reversed Dickson polynomial $D_{n,k}(1,x)$ of the $(k+1)$-th kind. The following result is given in [2].

Lemma 2.3. *[2] Let $n \geq 0$ be an integer. Then*

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

and

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

if $x \neq \frac{1}{2}$.

Theorem 2.4. *Each of the following is true.*

(i). *For any integer $n \geq 0$, we have*

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

and

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

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

(ii). *If n_1 and n_2 are positive integers such that $n_1 \equiv n_2 \pmod{q^2-1}$, then one has $D_{n_1,k}(1,x_0) = D_{n_2,k}(1,x_0)$ for any $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$.*

Proof. (i). First of all, it is easy to see that $D_{0,k}(1,\frac{1}{4}) = 2-k = \frac{k\times 0-k+2}{2^0}$ and $D_{1,k}(1,\frac{1}{4}) = 1 = \frac{k\times 1-k+2}{2^1}$. the first identity is true for the cases that $n=0$ and 1. Now let $n \geq 2$. Then one has

$$\begin{aligned} D_{n,k}\Big(1,\frac{1}{4}\Big) &= \sum_{i=0}^{[\frac{n}{2}]} \frac{n-ki}{n-i}\binom{n-i}{i}\Big(-\frac{1}{4}\Big)^i \\ &= \sum_{i=0}^{[\frac{n}{2}]} \frac{n-(k-1)i}{n-i}\binom{n-i}{i}\Big(-\frac{1}{4}\Big)^i + \sum_{i=0}^{[\frac{n}{2}]} \frac{-i}{n-i}\binom{n-i}{i}\Big(-\frac{1}{4}\Big)^i \\ &= D_{n,k-1}\Big(1,\frac{1}{4}\Big) + \frac{1}{4}\sum_{i=0}^{[\frac{n}{2}]-1}\binom{n-2-i}{i}\Big(-\frac{1}{4}\Big)^i \\ &= D_{n,k-1}\Big(1,\frac{1}{4}\Big) + \frac{1}{4}E_{n-2}\Big(1,\frac{1}{4}\Big), \end{aligned}$$

which follows from Theorem 2.2 (1) in [2] that

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

as desired. So the first identity is proved.

Now we turn our attention to the second identity. Let $x \neq \frac{1}{4}$, then there exists $y \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$ such that $x = y(1-y)$. So by the definition of the n-th reversed Dickson polynomial of the $(k+1)$-th kind, one has

$$\begin{aligned} D_{n,k}(1, y(1-y)) &= \sum_{i=0}^{[\frac{n}{2}]} \frac{n-ki}{n-i}\binom{n-i}{i}(-y(1-y))^i \\ &= \sum_{i=0}^{[\frac{n}{2}]} \frac{k(n-i)-kn}{n-i}\binom{n-i}{i}(-y(1-y))^i \\ &= k\sum_{i=0}^{[\frac{n}{2}]}\binom{n-i}{i}(-y(1-y))^i - (k-1)\sum_{i=0}^{[\frac{n}{2}]}\frac{n}{n-i}\binom{n-i}{i}(-y(1-y))^i \\ &= kE_n(1, y(1-y)) - (k-1)D_n(1, y(1-y)). \end{aligned} \tag{2.1}$$

But Lemma 2.3 gives us that

$$D_n(1, y(1-y)) = y^n + (1-y)^n \tag{2.2}$$

and

$$E_n(1, y(1-y)) = \sum_{i=0}^{n} y^{n-i}(1-y)^i = \frac{y^{n+1}-(1-y)^{n+1}}{2y-1}. \tag{2.3}$$

Thus it follows from (2.1) to (2.3) that

$$\begin{aligned} D_{n,k}(1, x) =& D_{n,k}(1, y(1-y)) \\ =& kE_n(1, y(1-y)) - (k-1)D_n(1, y(1-y)) \\ =& \frac{ky^{n+1} - k(1-y)^{n+1}}{2y-1} - (k-1)(y^n + (1-y)^n) \\ =& \frac{(k-1-(k-2)y)y^n - (1+(k-2)y)(1-y)^n}{2y-1} \end{aligned}$$

as required. So the second identity holds. Part (i) is proved.

(ii). For each $x_0 \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$, one can choose an element $y_0 \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$ such that $x_0 = y_0(1-y_0)$. Since $n_1 \equiv n_2 \pmod{q^2-1}$, one has $y_0^{n_1} = y_0^{n_2}$ and $(1-y_0)^{n_1} = (1-y_0)^{n_2}$. It then follows from part (i) that

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

as desired. This ends the proof of Theorem 2.4. □

Evidently, by Theorem 2.2 (i) and Theorem 2.4 (i) one can derive that (1.3) and (1.4) are true.

Proposition 2.5. *Let $n \geq 2$ be an integer. Then the recursion*

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

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

Proof. We consider the following two cases.

Case 1. $x \neq \frac{1}{4}$. For this case, one may let $x = y(1-y)$ with $y \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$. Then by Theorem 2.4 (i), we have

$$\begin{aligned} D_{n-1,k}(1,x) - xD_{n-2,k}(1,x) &= D_{n-1,k}(1,y(1-y)) - y(1-y)D_{n-2,k}(1,y(1-y)) \\ &= \frac{(k-1-(k-2)y)y^{n-1} - (1+(k-2)y)(1-y)^{n-1}}{2y-1} \\ &\quad - y(1-y)\frac{(k-1-(k-2)y)y^{n-2} - (1+(k-2)y)(1-y)^{n-2}}{2y-1} \\ &= \frac{(k-1-(k-2)y)y^{n} - (1+(k-2)y)(1-y)^{n}}{2y-1} \\ &= D_{n,k}(1,x) \end{aligned}$$

as required.

Case 2. $x = \frac{1}{4}$. Then by Theorem 2.4 (i), we have

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

This concludes the proof of Proposition 2.5. □

By Proposition 2.5, we can obtain the generating function of the reversed Dickson polynomial $D_{n,k}(1,x)$ of the $(k+1)$-th kind as follows.

Proposition 2.6. *The generating function of $D_{n,k}(1,x)$ is given by*

$$\sum_{n=0}^{\infty} D_{n,k}(1,x)t^n = \frac{(k-1)t-k+2}{1-t+xt^2}.$$

Proof. By the recursion presented in Proposition 2.5, we have

$$\begin{aligned} (1-t+xt^2)\sum_{n=0}^{\infty} D_{n,k}(1,x)t^n &= \sum_{n=0}^{\infty} D_{n,k}(1,x)t^n - \sum_{n=0}^{\infty} D_{n,k}(1,x)t^{n+1} + x\sum_{n=0}^{\infty} D_{n,k}(1,x)t^{n+2} \\ &= (k-1)t-k+2 + \sum_{n=0}^{\infty} (D_{n+2,k}(1,x) - D_{n+1,k}(1,x) + xD_{n,k}(1,x))t^{n+2} \\ &= (k-1)t-k+2. \end{aligned}$$

Thus the desired result follows immediately. □

Lemma 2.7. *[3] Let $x \in \mathbb{F}_{q^2}$. Then $x(1-x) \in \mathbb{F}_q$ if and only if $x^q = x$ or $x^q = 1-x$.*

Let V be defined by

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

Clearly, $\mathbb{F}_q \cap V = \{\frac{1}{2}\}$. Then we obtain a characterization for $D_{n,k}(1,x)$ to be a PP of $\mathbb{F}_q$ as follows.

Theorem 2.8. *Let $q = p^e$ with $p > 3$ being a prime and e being a positive integer. Let*

$$f : y \mapsto \frac{(k-1-(k-2)y)y^n - (1+(k-2)y)(1-y)^n}{2y-1}$$

be a mapping on $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$. Then $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if f is 2-to-1 and $f(y) \neq \frac{kn-k+2}{2^n}$ for any $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$.

Proof. First, we show the sufficiency part. Let f be 2-to-1 and $f(y) \neq \frac{kn-k+2}{2^n}$ for any $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$. Let $D_{n,k}(1,x_1) = D_{n,k}(1,x_2)$ for $x_1, x_2 \in \mathbb{F}_q$. To show that $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$, it suffices to show that $x_1 = x_2$, which will be done in what follows.

First of all, one can find $y_1, y_2 \in \mathbb{F}_{q^2}$ satisfying $x_1 = y_1(1-y_1)$ and $x_2 = y_2(1-y_2)$. By Lemma 2.7, we know that $y_1, y_2 \in \mathbb{F}_q \cup V$. We divide the proof into the following two cases.

Case 1. At least one of x_1 and x_2 is equal to $\frac{1}{4}$. Without loss of any generality, we may let $x_1 = \frac{1}{4}$. So by Theorem 2.4 (i), one derives that

$$D_{n,k}(1,x_2) = D_{n,k}(1,x_1) = D_{n,k}\Big(1, \frac{1}{4}\Big) = \frac{kn-k+2}{2^n}. \tag{2.4}$$

We claim that $x_2 = \frac{1}{4}$. Assume that $x_2 \neq \frac{1}{4}$. Then $y_2 \neq \frac{1}{2}$. Since $f(y) \neq \frac{kn-k+2}{2^n}$ for any $y \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$, by Theorem 2.4 (i), we get that

$$D_{n,k}(1,x_2) = \frac{(k-1-(k-2)y_2)y_2^n - (1+(k-2)y_2)(1-y_2)^n}{2y_2-1} = f(y_2) \neq \frac{kn-k+2}{2^n},$$

which contradicts to (2.4). Hence the claim is true, and so we have $x_1 = x_2$ as required.

Case 2. Both of x_1 and x_2 are not equal to $\frac{1}{4}$. Then $y_1 \neq \frac{1}{2}$ and $y_2 \neq \frac{1}{2}$. Since $D_{n,k}(1,x_1) = D_{n,k}(1,x_2)$, by Theorem 2.4 (i), one has

$$\frac{(k-1-(k-2)y_1)y_1^n - (1+(k-2)y_1)(1-y_1)^n}{2y_1-1} = \frac{(k-1-(k-2)y_2)y_2^n - (1+(k-2)y_2)(1-y_2)^n}{2y_2-1},$$

which is equivalent to $f(y_1) = f(y_2)$. However, f is a 2-to-1 mapping on $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$, and $f(y_2) = f(1-y_2)$ by the definition of f. It then follows that $y_1 = y_2$ or $y_1 = 1-y_2$. Thus $x_1 = x_2$ as desired. Hence the sufficiency part is proved.

Now we prove the necessity part. Let $D_{n,k}(1,x)$ be a PP of $\mathbb{F}_q$. Choose two elements $y_1, y_2 \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$ such that $f(y_1) = f(y_2)$, that is,

$$\frac{(k-1-(k-2)y_1)y_1^n - (1+(k-2)y_1)(1-y_1)^n}{2y_1-1} = \frac{(k-1-(k-2)y_2)y_2^n - (1+(k-2)y_2)(1-y_2)^n}{2y_2-1}. \tag{2.5}$$

Since $y_1, y_2 \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$, it follows from Lemma 2.7 that $y_1(1-y_1) \in \mathbb{F}_q$ and $y_2(1-y_2) \in \mathbb{F}_q$. So by Theorem 2.4 (i), (2.5) implies that

$$D_{n,k}(1, y_1(1-y_1)) = D_{n,k}(1, y_2(1-y_2)).$$

Thus $y_1(1-y_1) = y_2(1-y_2)$ since $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$, which infers that $y_1 = y_2$ or $y_1 = 1-y_2$. Since $y_2 \neq \frac{1}{2}$, one has $y_2 \neq 1-y_2$. Therefore f is a 2-to-1 mapping on $(\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$.

Now take $y' \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$. Then from Lemma 2.7 it follows that $y'(1-y') \in \mathbb{F}_q$ and

$$y'(1-y') \neq \frac{1}{2}\Big(1-\frac{1}{2}\Big).$$

Notice that $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$. Hence one has

$$D_{n,k}(1, y'(1-y')) \neq D_{n,k}\Big(1, \frac{1}{2}\Big(1-\frac{1}{2}\Big)\Big).$$

But Theorem 2.4 (i) tells us that

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

Then by Theorem 2.4 (i) and noting that $y' \neq \frac{1}{2}$, we have

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

which infers that $f(y') \neq \frac{kn-k-2}{2^n}$ for any $y' \in (\mathbb{F}_q \cup V) \setminus \{\frac{1}{2}\}$. So the necessity part is proved.

The proof of Theorem 2.8 is complete. □

Now we can use Theorem 2.4 to present an explicit formula for $D_{n,k}(1,x)$ when n is a power of the characteristic p. Then we derive the detailed characterization for $D_{n,k}(1,x)$ being a PP of $\mathbb{F}_q$ in this case.

Proposition 2.9. *Let $p = \mathrm{char}(\mathbb{F}_q) \geq 3$ and $s \geq 0$ be an integer. Then*

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

Proof. We consider the following two cases.

Case 1. $x \neq \frac{1}{4}$. For this case, putting $x = y(1-y)$ in Theorem 2.4 (i) gives us that

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

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

where $u=2y-1$. So we obtain that

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

which infers that

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

as desired.

Case 2. $x=\frac{1}{4}$. By Theorem 2.4 (i), one has

$$2D_{p^s,k}(1,\frac{1}{4})+k-2=2\times\frac{kp^s-k+2}{2^{p^s}}+k-2=0=k(1-4\times\frac{1}{4})^{\frac{p^s-1}{2}}$$

as required. So Proposition 2.9 is proved. □

It is well known that every linear polynomial over $\mathbb{F}_q$ is a PP of $\mathbb{F}_q$ and that the monomial x^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n,q-1)=1$. Then by Proposition 2.9, we have the following result.

Corollary 2.10. *Let $p\geq 3$ be a prime, $q=p^e$ with $e\geq 1$ and $s\geq 0$ be an integer. Then $D_{p^s,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $k\geq 1, p=3,$ s is odd and* $\gcd(s,e)=1$.

Proof. First assume that $D_{p^s,k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$. It then follows from Proposition 2.9 that $D_{p^s,k}(1,x)$ is a PP of $\mathbb{F}_{p^e}$ if and only if

$$k(1-4x)^{\frac{p^s-1}{2}} \tag{2.6}$$

is a PP of $\mathbb{F}_{p^e}$. Clearly, $k\geq 1$ and $s>0$ in this case. Suppose $p>3$, then (2.6) is a PP of $\mathbb{F}_{p^e}$ if and only if

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

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

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

So $p=3,k\geq 1$ and $s>0$ in what following. Now Suppose $s>0$ is even, then it is easy to see that $2|\gcd(\frac{3^s-1}{2},3^e-1)$ which is a contradiction. This means that s must be an odd integer and then so is $\frac{3^s-1}{2}$. Thus we have that (2.6) is a PP of $\mathbb{F}_{p^e}$ if and only if

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

which is equivalent to that s is odd and $\gcd(s,e)=1$. So Corollary 2.10 is proved. □

3. A necessary condition for $D_{n,k}(1,x)$ to be permutational and an auxiliary polynomial

In this section, we study a necessary condition on n for $D_{n,k}(1,x)$ to be a PP of $\mathbb{F}_q$. On one hand, it is easy to check that

$$D_{0,k}(1,0) = 2-k, D_{n,k}(1,0) = 1$$

for any $n \geq 1$ and $D_{0,k}(1,1) = 2-k, D_{1,k}(1,1) = 1$. On the other hand, Proposition 2.5 tells us that

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

for $n \geq 0$. Then one can easily show that the sequence $\{D_{n,k}(1,1)|n \in \mathbb{N}\}$ is periodic with the smallest positive periods 6. In fact, one has

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

So we have the following result.

Theorem 3.1. *Assume that $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ with $q = p^e$ and $p > 3$. Then $n \not\equiv 1 \pmod 6$.*

Proof. Let $D_{n,k}(1,x)$ be a PP of $\mathbb{F}_q$. Then $D_{n,k}(1,0)$ and $D_{n,k}(1,1)$ are distinct. Then by the above results, the desired result $n \not\equiv 1 \pmod 6$ follows immediately. □

Let n, k be nonnegative integers. We define the following auxiliary polynomial $p_{n,k}(x) \in \mathbb{Z}[x]$ by

$$p_{n,k}(x) := k \sum_{j \geq 0} \binom{n}{2j+1} x^j - (k-2) \sum_{j \geq 0} \binom{n}{2j} x^j$$

for $n \geq 1$, and

$$p_{0,k}(x) := 2^n(2-k).$$

Then we have the following relation between $D_{n,k}(1,x)$ and $p_{n,k}(x)$.

Theorem 3.2. *Let $p > 3$ be a prime and $n \geq 0$ be an integer. Then each of the following is true.*

(i). *One has*

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

(ii). *We have that $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $p_{n,k}(x)$ is a PP of $\mathbb{F}_q$.*

Proof. (i). Clearly, (3.1) follows from the definitions of $p_{0,k}(x)$ and $D_{0,k}(1,x)$ if $n = 0$. Then we assume that $n \geq 1$ in what follows.

First, let $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$. Then there exists $y \in \mathbb{F}_{q^2} \setminus \{\frac{1}{2}\}$ such that $x = y(1-y)$. Let $u = 2y - 1$. It then follows from Theorem 2.4 (i) that

$$\begin{aligned}
D_{n,k}(1,x) &= D_{n,k}(1,y(1-y)) \\
&= \frac{(k-1-(k-2)y)y^n-(1+(k-2)y)(1-y)^n}{2y-1} \\
&= \frac{1}{u}\Big(\frac{-(k-2)u+k}{2}(\frac{u+1}{2})^n-\frac{(k-2)u+k}{2}(\frac{1-u}{2})^n\Big) \\
&= \frac{1}{2^{n+1}u}\Big(k((u+1)^n-(1-u)^n)-(k-2)u((u+1)^n+(1-u)^n)\Big) \\
&= \frac{1}{2^n}\left(k\sum_{j\geq 0}\binom{n}{2j+1}x^j-(k-2)\sum_{j\geq 0}\binom{n}{2j}u^{2j}\right) \\
&= \frac{1}{2^n}p_{n,k}(u^2) \\
&= \frac{1}{2^n}p_{n,k}(1-4y(1-y)) \\
&= \frac{1}{2^n}p_{n,k}(1-4x)
\end{aligned}$$

as desired. So (3.1) holds in this case.

Consequently, we let $x=\frac{1}{4}$. Then by Theorem 2.4 (i), we have

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

On the other hand, we can easily check that

$$p_{n,k}(0)=kn-k+2.$$

Therefore

$$D_{n,k}\Big(1,\frac{1}{4}\Big)=\frac{1}{2^n}p_{n,k}(0)=\frac{1}{2^n}p_{n,k}\Big(1-4\times\frac{1}{4}\Big)$$

as one desires. So (3.1) is proved.

(ii). Notice that $\frac{1}{2^n}\in\mathbb{F}_q^*$ and $1-4x$ is linear. So $D_{n,k}(1,x)$ is a PP of $\mathbb{F}_q$ if and only if $p_{n,k}(x)$ is a PP of $\mathbb{F}_q$. This ends the proof of Theorem 3.2. □

4. The first moment $\sum_{a\in\mathbb{F}_q}D_{n,k}(1,a)$

In this section, we compute the first moment $\sum_{a\in\mathbb{F}_q}D_{n,k}(1,a)$. By Proposition 2.6, one has

$$\begin{aligned}
\sum_{n=0}^{\infty}D_{n,k}(1,x)t^n &= \frac{(k-1)t-k+2}{1-t+xt^2}=\frac{(k-1)t-k+2}{1-t}\frac{1}{1-\frac{t^2}{t-1}x} \\
&= \frac{(k-1)t-k+2}{1-t}\Big(1+\sum_{m=1}^{q-1}\sum_{\ell=0}^{\infty}\Big(\frac{t^2}{t-1}\Big)^{m+\ell(q-1)}x^{m+\ell(q-1)}\Big) \\
&\equiv \frac{2t-1}{1-t}\Big(1+\sum_{m=1}^{q-1}\sum_{\ell=0}^{\infty}\Big(\frac{t^2}{t-1}\Big)^{m+\ell(q-1)}x^{m}\Big) \pmod{x^q-x}
\end{aligned}$$

$$= \frac{(k-1)t-k+2}{1-t}\Big(1+\sum_{m=1}^{q-1}\frac{(\frac{t^2}{t-1})^m}{1-(\frac{t^2}{t-1})^{q-1}}x^m\Big)$$

$$= \frac{(k-1)t-k+2}{1-t}\Big(1+\sum_{m=1}^{q-1}\frac{(t-1)^{q-1-m}t^{2m}}{(t-1)^{q-1}-t^{2(q-1)}}x^m\Big). \tag{4.1}$$

Moreover, by Theorem 2.4 (ii), it follows that for any $x \in \mathbb{F}_q \setminus \{\frac{1}{4}\}$, one has

$$D_{n_1,k}(1,x) = D_{n_2,k}(1,x)$$

when $n_1 \equiv n_2 \pmod{q^2-1}$. Thus if $x \neq \frac{1}{4}$, one has

$$\begin{aligned}\sum_{n=0}^{\infty} D_{n,k}(1,x)t^n &= 1+\sum_{n=1}^{q^2-1}\sum_{\ell=0}^{\infty} D_{n+\ell(q^2-1),k}(1,x)t^{n+\ell(q^2-1)}\\ &= 1+\sum_{n=1}^{q^2-1} D_{n,k}(1,x)\sum_{\ell=0}^{\infty} t^{n+\ell(q^2-1)}\\ &= 1+\frac{1}{1-t^{q^2-1}}\sum_{n=1}^{q^2-1} D_{n,k}(1,x)t^n. \end{aligned}\tag{4.2}$$

Then (4.1) together with (4.2) gives that for any $x \neq \frac{1}{4}$, we have

$$\begin{aligned}&\sum_{n=1}^{q^2-1} D_{n,k}(1,x)t^n = \Big(\sum_{n=0}^{\infty} D_{n,k}(1,x)t^n - 1\Big)(1-t^{q^2-1})\\ \equiv&\Big(\frac{(k-1)t-k+2}{1-t}-1\Big)(1-t^{q^2-1})+\frac{(1-t^{q^2-1})((k-1)t-k+2)}{1-t}\sum_{m=1}^{q-1}\frac{(t-1)^{q-1-m}t^{2m}}{(t-1)^{q-1}-t^{2(q-1)}}x^m \pmod{x^q-x}\\ =&\frac{(kt+1-k)(1-t^{q^2-1})}{1-t}+h(t)\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}x^m, \end{aligned}\tag{4.3}$$

where

$$h(t) := \frac{(t^{q^2-1}-1)((k-1)t-k+2)}{(t-1)^q-(t-1)t^{2(q-1)}}.$$

Lemma 4.1. *[4] Let $u_0, u_1, \cdots, u_{q-1}$ be the list of the all elements of $\mathbb{F}_q$. Then*

$$\sum_{i=0}^{q-1} u_i^k = \begin{cases} 0, & \text{if } 0 \le k \le q-2,\\ -1, & \text{if } k = q-1.\end{cases}$$

Now by Theorem 2.4 (i), Lemma 4.1 and (4.3), we derive that

$$\sum_{n=1}^{q^2-1}\sum_{a\in\mathbb{F}_q} D_{n,k}(1,a)t^n = \sum_{n=1}^{q^2-1} D_{n,k}\Big(1,\frac{1}{4}\Big)t^n + \sum_{n=1}^{q^2-1}\sum_{a\in\mathbb{F}_q\setminus\{\frac{1}{4}\}} D_{n,k}(1,a)t^n$$

$$
\begin{aligned}
&=\sum_{n=1}^{q^2-1}\frac{kn-k+2}{2^n}t^n+\sum_{a\in\mathbb{F}_q\setminus\{\frac14\}}\frac{(kt+1-k)(1-t^{q^2-1})}{1-t}+h(t)\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}\sum_{a\in\mathbb{F}_q\setminus\{\frac14\}}a^m\\
&=\sum_{n=1}^{q^2-1}\frac{kn-k+2}{2^n}t^n+(q-1)\frac{(kt+1-k)(1-t^{q^2-1})}{1-t}+h(t)\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}\sum_{a\in\mathbb{F}_q}a^m\\
&\quad-h(t)\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}\Big(\frac14\Big)^m\\
&=\sum_{n=1}^{q^2-1}\frac{kn-k+2}{2^n}t^n-\frac{(kt+1-k)(1-t^{q^2-1})}{1-t}-h(t)t^{2(q-1)}-h(t)\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}\Big(\frac14\Big)^m. \qquad (4.4)
\end{aligned}
$$

Since $(t-1)^q = t^q - 1$ and q is odd, one has

$$
\begin{aligned}
h(t)=&\frac{(t^{q^2-1}-1)(2t-1)}{(t-1)^q-(t-1)t^{2(q-1)}}\\
=&\frac{(t^{q^2-1}-1)(2t-1)}{(1-t^{q-1})(t^q-t^{q-1}-1)}\\
=&\frac{(t^{q^2}-t)(2t-1)}{(t-t^q)(t^q-t^{q-1}-1)}\\
=&\frac{(t^q-t)^q+t^q-t}{t-t^q}\cdot\frac{2t-1}{t^q-t^{q-1}-1}\\
=&\frac{(-1-(t-t^q)^{q-1})(2t-1)}{t^q-t^{q-1}-1}\\
=&\frac{(2t-1)\sum_{i=0}^{q^2-q}b_it^i}{t^q-t^{q-1}-1}, \qquad (4.5)
\end{aligned}
$$

where

$$
\sum_{i=0}^{q^2-q}b_it^i := -1-(t-t^q)^{q-1}.
$$

Then by the binomial theorem applied to $(t-t^q)^{q-1}$, we can derive the following expression for the coefficient b_i.

Proposition 4.2. *For each integer i with* $0 \le i \le q^2-q$, *write* $i=\alpha+\beta q$ *with* α *and* β *being integers such that* $0\le\alpha,\beta\le q-1$. *Then*

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

For convenience, let

$$
a_n := \sum_{a\in\mathbb{F}_q}D_{n,k}(1,a).
$$

Then by (4.4) and (4.5), we arrive at

$$\sum_{n=1}^{q^2-1}\Big(a_n-\frac{kn-k+2}{2^n}\Big)t^n=-\frac{(kt+1-k)(1-t^{q^2-1})}{1-t}-\frac{(2t-1)\sum_{i=0}^{q^2-q}b_it^i}{t^q-t^{q-1}-1}\Big(t^{2(q-1)}+\sum_{m=1}^{q-1}(t-1)^{q-1-m}t^{2m}\Big(\frac{1}{4}\Big)^m\Big),$$

which implies that

$$\begin{aligned}&(t^q-t^{q-1}-1)\sum_{n=1}^{q^2-1}\Big(a_n-\frac{kn-k+2}{2^n}\Big)t^n\\ =&-(t^q-t^{q-1}-1)(kt+1-k)\sum_{i=0}^{q^2-2}t^i-(2t-1)\Big(t^{2(q-1)}+\sum_{k=1}^{q-1}(t-1)^{q-1-k}t^{2k}\Big(\frac{1}{4}\Big)^k\Big)\sum_{i=0}^{q^2-q}b_it^i.\end{aligned} \tag{4.6}$$

Let

$$\sum_{i=1}^{q^2+q-1}c_it^i$$

denote the right-hand side of (4.6) and let

$$d_n:=a_n-\frac{kn-k+2}{2^n}$$

for each integer n with $1\le n\le q^2-1$. Then (4.6) can be reduced to

$$(t^q-t^{q-1}-1)\sum_{n=1}^{q^2-1}d_nt^n=\sum_{i=1}^{q^2+q-1}c_it^i. \tag{4.7}$$

Then by comparing the coefficient of t^i with $1\le i\le q^2+q-1$ of the both sides in (4.7), we derive the following relations:

$$\begin{cases}c_j=-d_j, & \text{if } 1\le j\le q-1,\\ c_q=-d_1-d_q, & \\ c_{q+j}=d_j-d_{j+1}-d_{q+j}, & \text{if } 1\le j\le q^2-q-1,\\ c_{q^2+j}=d_{q^2-q+j}-d_{q^2-q+j+1}, & \text{if } 0\le j\le q-2,\\ c_{q^2+q-1}=d_{q^2-1}, & \end{cases}$$

from which we can deduce that

$$\begin{cases}d_j=-c_j, & \text{if } 1\le j\le q-1,\\ d_q=c_1-c_q, & \\ d_{\ell q+j}=d_{(\ell-1)q+j}-d_{(\ell-1)q+j+1}-c_{\ell q+j}, & \text{if } 1\le \ell\le q-2 \ \text{ and } \ 1\le j\le q-1,\\ d_{\ell q}=d_{(\ell-1)q}-d_{(\ell-1)q+1}-c_{\ell q}, & \text{if } 2\le \ell\le q-2,\\ d_{q^2-q+j}=\sum_{i=j}^{q-1}c_{q^2+i}, & \text{if } 0\le j\le q-1.\end{cases} \tag{4.8}$$

Finally, (4.8) together with the following identity

$$\sum_{a\in\mathbb{F}_q}D_{n,k}(1,a)=d_n+\frac{kn-k+2}{2^n}$$

shows that the last main result of this paper is true:

Theorem 4.3. *Let c_i be the coefficient of t^i in the right-hand side of (4.6) with i being an integer such that $1 \le i \le q^2 + q - 1$. Then we have*

$$\sum_{a\in\mathbb{F}_q} D_{j,k}(1,a) = -c_j + \frac{kj-k+2}{2^j} \quad if \ \ 1 \le j \le q-1,$$

$$\sum_{a\in\mathbb{F}_q} D_{q,k}(1,a) = c_1 - c_q - \frac{k-2}{2},$$

$$\sum_{a\in\mathbb{F}_q} D_{\ell q+j,k}(1,a) = \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+j,k}(1,a) - \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+j+1,k}(1,a) - c_{\ell q+j} + \frac{k}{2^{\ell+j}}$$

$$if \ \ 1 \le \ell \le q-2 \text{ and } 1 \le j \le q-1,$$

$$\sum_{a\in\mathbb{F}_q} D_{\ell q,k}(1,a) = \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q,k}(1,a) - \sum_{a\in\mathbb{F}_q} D_{(\ell-1)q+1,k}(1,a) - c_{\ell q} + \frac{k}{2^{\ell}} \quad if \ \ 2 \le \ell \le q-2$$

and

$$\sum_{a\in\mathbb{F}_q} D_{q^2-q+j,k}(1,a) = \sum_{i=j}^{q-1} c_{q^2+i} + \frac{kj-k+2}{2^j} \quad if \ \ 0 \le j \le q-1.$$

Acknowledgement

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

Conflict of Interest

The author declares no conflicts of interest in this paper.

References

1. S. D. Cohen, *Dickson polynomials of the second kind that are permutations,* Canad. J. Math., **46** (1994), 225-238.
2. S. Hong, X. Qin and W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational,* Finite Fields Appl., **37** (2016), 54-71.
3. X. Hou, G. L. Mullen, J.A. Sellers and J.L. Yucas, *Reversed Dickson polynomials over finite fields,* Finite Fields Appl., **15** (2009), 748-773.
4. R. Lidl and H. Niederreiter, *Finite Fields, second ed., Encyclopedia of Mathematics and its Applications,* Cambridge University Press, Cambridge, **20** 1997.
5. X. Qin and S. Hong, *Constructing permutation polynomials over finite fields,* Bull. Aust. Math. Soc., **89** (2014), 420-430.

6. X. Qin, G. Qian and S. Hong, *New results on permutation polynomials over finite fields,* Int. J. Number Theory, **11** (2015), 437-449.

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