Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The first and second moments of reversed Dickson polynomials over finite fields

Kaimin Cheng[a,b], Shaofang Hong[a,*,1]

[a] *Mathematical College, Sichuan University, Chengdu 610064, PR China*
[b] *School of Mathematics and Information, China West Normal University, Nanchong 637009, PR China*

ARTICLE INFO

Article history:
Received 4 September 2017
Received in revised form 7 October 2017
Accepted 7 October 2017
Available online xxxx
Communicated by D. Wan

MSC:
11T06
11T55
11C08

Keywords:
Permutation polynomial
Reversed Dickson polynomial of $(k+1)$-th kind
Moment
Lucas' congruence
Hermite criterion

ABSTRACT

Let n and k be nonnegative integers. In 2010, Hou and Ly evaluated the first and second moments of the n-th reversed Dickson polynomial of the first kind. In 2016, Hong, Qin and Zhao presented a recursive formula for the first moment of the n-th reversed Dickson polynomial of the second kind. In this paper, we introduce a new method to investigate the moments of the n-th reversed Dickson polynomial of $(k+1)$-th kind. In fact, we first show an extension of the famous Lucas' congruence and then study arithmetic properties of some two-variable linear congruences. Finally, with more efforts, we arrive at the explicit formulas for the first and second moments of the n-th reversed Dickson polynomial of the $(k+1)$-th kind.

[*] Corresponding author.
E-mail addresses: ckm20@126.com, chengkaimin@yahoo.com (K.M. Cheng), sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com (S.F. Hong).

[1] Hong was supported partially by National Science Foundation of China Grants # 11371260 and # 11771304.

https://doi.org/10.1016/j.jnt.2017.10.021
0022-314X/© 2017 Elsevier Inc. All rights reserved.

Please cite this article in press as: K.M. Cheng, S.F. Hong, The first and second moments of reversed Dickson polynomials over finite fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.10.021

1. Introduction

Permutation polynomial is an important subject in the area of finite fields and has many applications in coding theory, cryptography and combinatorial design theory (see [9,13,15] for reviews and [1,10–12] for recent developments). Dickson polynomial is another significant topic of finite fields (see [3,9]). Let $n \geq 0$ be an integer and $\mathbb{F}_q$ be the finite field of characteristic p and with q elements. Let $D_n(x,y) \in \mathbb{Z}[x]$ be defined by the following functional equation

$$D_n(x+y, xy)) = x^n + y^n.$$

Clearly, the well-known *Dickson polynomial*, denoted by $D_n(x,a)$, and the reversed Dickson polynomial, denoted by $D_n(a,x)$, with $a \in \mathbb{F}_q^*$ being the parameters, are the descendants of $D_n(x,y)$. In the past decade, the reversed Dickson polynomials received attentions from many authors. Hou, Mullen, Sellers and Yucas [8] introduced the definition of *the reversed Dickson polynomial of the first kind*, denoted by $D_n(a,x)$, as follows

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

and $D_n(a,x) := 2$. Let $k \geq 0$ be an integer. To extend the definition of reversed Dickson polynomials, Wang and Yucas [14] defined *the n-th reversed Dickson polynomial of $(k+1)$-th kind* $D_{n,k}(a,x) \in \mathbb{F}_q[x]$, which is defined by

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

if $n \geq 1$, and $D_{0,k}(a,x) := 2-k$. It is clear that if $\mathrm{char}(\mathbb{F}_q) = 2$, then $D_{n,k}(a,x) = D_{n,1}(a,x)$ if k is odd and $D_{n,k}(a,x) = D_n(a,x)$ if k is even. So throughout this paper, we always assume that $p = \mathrm{char}(\mathbb{F}_q) \geq 3$.

The permutational behavior of $D_{n,k}(a,x)$ is an interesting topic. Hou, Mullen, Sellers and Yucas [8] considered the permutational behavior of reversed Dickson polynomial $D_n(a,x)$ of the first kind. In fact, they showed that $D_n(a,x)$ is closely related to almost perfect nonlinear functions, and obtained some families of permutation polynomials from the reversed Dickson polynomials of the first kind. In [7], Hou and Ly found several necessary conditions for the reversed Dickson polynomials $D_n(a,x)$ of the first kind to be a permutation polynomial. In 2016, Hong, Qin and Zhao [5] studied the reversed Dickson polynomial $D_{n,1}(a,x)$ of the second kind. In fact, they gave some necessary conditions for the reversed Dickson polynomial $D_{n,1}(a,x)$ to be a permutation polynomial of $\mathbb{F}_q$. It is natural to ask the following interesting question: When does $D_{n,k}(a,x)$ permute the finite field $\mathbb{F}_q$? It is hard to answer this problem in general.

Please cite this article in press as: K.M. Cheng, S.F. Hong, The first and second moments of reversed Dickson polynomials over finite fields, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.10.021