Journal of Number Theory 172 (2017) 234–255

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Reversed Dickson polynomials of the $(k+1)$-th kind over finite fields

Neranga Fernando

Department of Mathematics, Northeastern University, Boston, MA 02115, United States

A R T I C L E I N F O

Article history:
Received 24 May 2016
Accepted 10 August 2016
Available online 8 October 2016
Communicated by D. Goss

MSC:
11T06
11T55

Keywords:
Finite field
Permutation polynomial
Dickson polynomial
Reversed Dickson polynomial

A B S T R A C T

We discuss the properties and the permutation behavior of the reversed Dickson polynomials of the $(k+1)$-th kind $D_{n,k}(1,x)$ over finite fields. The results in this paper unify and generalize several recently discovered results on reversed Dickson polynomials over finite fields.

1. Introduction

Let p be a prime and q a power of p. Let $\mathbb{F}_q$ be the finite field with q elements. A polynomial $f \in \mathbb{F}_q[\mathrm{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the associated mapping $x \mapsto f(x)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Permutation polynomials over finite fields have important applications in Coding Theory, Cryptography, Finite Geometry, Combinatorics and Computer Science, among other fields.

E-mail address: w.fernando@neu.edu.

http://dx.doi.org/10.1016/j.jnt.2016.08.018
0022-314X/

Recently, reversed Dickson polynomials over finite fields have been studied extensively by many for their general properties and permutation behavior. The concept of the reversed Dickson polynomial $D_n(a,x)$ was first introduced by Hou, Mullen, Sellers and Yucas in [5] by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(x,a)$.

The n-th reversed Dickson polynomial of the first kind $D_n(a,x)$ is defined by

$$D_n(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}, \tag{1.1}$$

where $a \in \mathbb{F}_q$ is a parameter.

In [5], it was shown that the reversed Dickson polynomials of the first kind are closely related to Almost Perfect Nonlinear (APN) functions which have applications in cryptography. Hou and Ly found more properties of the reversed Dickson polynomials of the first kind and necessary conditions for them to be a permutation of $\mathbb{F}_q$; see [4].

By reversing the roles of the variable and the parameter in the Dickson polynomial of the second kind $E_n(x,a)$, the n-th reversed Dickson polynomial of the second kind $E_n(a,x)$ can be defined by

$$E_n(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-i}{i} (-x)^i a^{n-2i}, \tag{1.2}$$

where $a \in \mathbb{F}_q$ is a parameter.

In [2], Hong, Qin, and Zhao explored the reversed Dickson polynomials of the second kind and found many of their properties and necessary conditions for them to be a permutation of $\mathbb{F}_q$.

For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i}, \tag{1.3}$$

and $D_{0,k}(a,x) = 2-k$; see [8].

Note that $D_{n,0}(a,x) = D_n(a,x)$ and $D_{n,1}(a,x) = E_n(a,x)$. Also note that we only need to consider $0 \le k \le p-1$. It follows from (1.1), (1.2), and (1.3) that

$$D_{n,k}(a,x) = kE_n(a,x) - (k-1)D_n(a,x). \tag{1.4}$$

The author of the current paper surveyed the properties and the permutation behavior of the reversed Dickson polynomials of the third kind over finite fields in [3]. Most recently, Cheng, Hong, and Qin studied the reversed Dickson polynomials of the fourth kind over finite fields; see [1].