Finite Fields and Their Applications 28 (2014) 148–165

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Some classes of monomial complete permutation polynomials over finite fields of characteristic two

Gaofei Wu [a], Nian Li [b], Tor Helleseth [c], Yuqing Zhang [d,*]

[a] *State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[b] *Information Security and National Computing Grid Laboratory, Southwest Jiaotong University, Chengdu 610031, China*
[c] *Department of Informatics, University of Bergen, N-5020 Bergen, Norway*
[d] *National Computer Network Intrusion Protection Center, UCAS, Beijing 100043, China*

ARTICLE INFO

Article history:
Received 26 October 2013
Received in revised form 14 January 2014
Accepted 19 January 2014
Available online 6 March 2014
Communicated by Rudolf Lidl

MSC:
05A05
11T06

Keywords:
Finite field
Complete permutation polynomials
Walsh transform
Dickson polynomials

ABSTRACT

In this paper, four classes of complete permutation polynomials over finite fields of characteristic two are presented. To consider the permutation property of the first three classes, Dickson polynomials play a key role. The fourth class is a generalization of a known result. In addition, we also calculate the inverses of these bijective monomials.

* Corresponding author.
E-mail addresses: gaofei_wu@qq.com (G. Wu), nianli.2010@gmail.com (N. Li), Tor.Helleseth@ii.uib.no (T. Helleseth), zhangyq@ucas.ac.cn (Y. Zhang).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2014.01.011

1. Introduction

Let $\mathbb{F}_q$ be a finite field of $q = p^n$ elements, where p is a prime number, and n is a positive integer. We denote by $\mathbb{F}_q^*$ the multiplication group of $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial (PP) if the associated polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a permutation over $\mathbb{F}_q$ [14]. Permutation polynomials over finite fields have important applications in cryptography, coding theory, and combinatorial design theory. In [12,13], Lidl and Mullen listed many open problems and one of them is to find more permutation polynomials. Recently, permutation polynomials have been studied extensively in the literature, see [1,3–5,7,8,10,11,15,19,24,25,27,29] for example.

A polynomial $f \in \mathbb{F}_q[x]$ is called a complete permutation polynomial (CPP) if both $f(x)$ and $f(x) + x$ are permutations over $\mathbb{F}_q$. CPPs are useful in the study of orthogonal Latin squares. In [17], Niederreiter and Robinson gave a detailed study of CPPs over $\mathbb{F}_q$. Dickson polynomials (see Section 2) are familiar examples of PPs. In [16], Mullen and Niederreiter studied under what conditions a Dickson polynomial can be a CPP. Although there are some results on CPPs over $\mathbb{F}_q$ [10,20,23,26], still very few classes of CPPs are known, even for monomial functions.

For a positive integer d and $a \in \mathbb{F}_q^*$, a monomial function ax^d is a CPP over $\mathbb{F}_q$ if and only if $\gcd(d, q-1) = 1$ and $ax^d + x$ is a PP over $\mathbb{F}_q$. We call such d a CPP exponent over $\mathbb{F}_q$. In [2], Charpin and Kyureghyan proved that $a^{-1}x^{2^k+2}$ is a CPP over $\mathbb{F}_{2^{2k}}$ for odd k and $a \in \beta\mathbb{F}_{2^k}$, where $\beta \in \mathbb{F}_{2^2} \backslash \mathbb{F}_2$. Very recently, Tu, Zeng, and Hu [21] gave three classes of CPP exponents over $\mathbb{F}_{2^n}$: (1) $d = 2^{2k} + 2^k + 2$, $n = 3k$, $\gcd(k, 3) = 1$; (2) $d = 2^{k+1} + 3$, $n = 2k$, k odd; and (3) $d = 2^{k-2}(2^k + 3)$, $n = 2k$, k odd. Some further results about CPPs can be found in [22,28].

In this paper, four more classes of monomial CPPs are studied:

(1) $n = 4k$ and $d = \frac{2^{4k}-1}{2^k-1} + 1$, where $\gcd(k, 4) = 1$.
(2) $n = 6k$ and $d = \frac{2^{6k}-1}{2^k-1} + 1$, where $\gcd(k, 6) = 1$.
(3) $n = 10k$ and $d = \frac{2^{10k}-1}{2^k-1} + 1$, where $\gcd(k, 10) = 1$.
(4) $n = 3k$ and $d = \frac{2^{3k}-1}{2^k-1} + 1$, where $\gcd(k, 9) = 3$.

In investigating the permutation behavior of the first three classes of CPPs, Dickson polynomials play an important role. The first three classes of CPP exponents are generalizations of two known results, namely, $d = \frac{2^{2k}-1}{2^k-1} + 1$ [2], and $d = \frac{2^{3k}-1}{2^k-1} + 1$ [21]. Note that for the exponent $d = \frac{2^{3k}-1}{2^k-1} + 1$, the case of $\gcd(k, 3) = 1$ has been discussed in [21], and in this paper we proved that d is also a CPP exponent over $\mathbb{F}_{2^{3k}}$ for $\gcd(k, 9) = 3$. In addition, the inverses of these CPP exponents are also given.