Finite Fields and Their Applications 31 (2015) 228–240

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Complete permutation polynomials over finite fields of odd characteristic

Xu Guangkui [a,b], Xiwang Cao [a,*]

[a] School of Mathematical Sciences, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China
[b] Department of Mathematics and Computational Science, Huainan Normal University, Huainan 232038, China

ARTICLE INFO

Article history:
Received 1 December 2013
Received in revised form 23 August 2014
Accepted 24 August 2014
Available online 10 November 2014
Communicated by Rudolf Lidl

MSC:
05A05
11T06
11T55

Keywords:
Complete permutation polynomial
Permutation polynomial
Dickson polynomial
Finite fields

ABSTRACT

In this paper, we present three classes of complete permutation monomials over finite fields of odd characteristic. Meanwhile, the compositional inverses of these polynomials are also investigated.

* Corresponding author.
E-mail addresses: xuguangkuis@gmail.com (X. Guangkui), xwcao@nuaa.edu.cn (X. Cao).

http://dx.doi.org/10.1016/j.ffa.2014.08.002
1071-5797/

1. Introduction

Let p be a prime number and $q = p^n$. Let $\mathbb{F}_q$ denote the finite field of order q and $\mathbb{F}_q^*$ the set of all nonzero elements of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the associated polynomial function $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. For a permutation polynomial $f(x) \in \mathbb{F}_q[x]$ there exists (a unique) $f^{-1}(x) \in \mathbb{F}_q[x]$ such that $f(f^{-1}(x)) \equiv f^{-1}(f(x)) \equiv x (\mathrm{mod}\ x^q - x)$. We call $f^{-1}(x)$ the *compositional inverse* of $f(x)$. Permutation polynomials were studied first by Hermite [8] and later by Dickson [5]. Permutation polynomials have been an active topic of study in recent years due to their important applications in cryptography, coding theory, and combinatorial designs theory. A permutation polynomial $f(x) \in \mathbb{F}_q[x]$ is a *complete permutation polynomial* (CPP) over $\mathbb{F}_q$ if $f(x) + x$ permutes $\mathbb{F}_q$ as well. The study of complete permutation polynomials started with the work of Niederreiter and Robinson [14]. Finding new PPs and CPPs of finite fields is a difficult problem and there are rare classes of CPPs known. For more study of PPs and CPPs can be found in [1–4,6,9,10, 15,17,19,20].

Our interest in complete permutation polynomials arises from a recent paper by Tu et al. [16] in which several classes of complete permutation polynomials over finite fields of even characteristic were constructed. More precisely, they considered three classes of monomial complete permutation polynomials and a class of trinomial complete permutation polynomials. In [14], Niederreiter and Robinson pointed out that the compositional inverse of a complete permutation polynomial is also a complete permutation polynomial. As part of our main results in this correspondence we present three new classes of monomial complete permutations (see Theorem 3.1, Theorem 3.3 and Theorem 3.5) over finite fields of odd characteristic, not corresponding to any known monomial complete permutation. The proofs of Theorem 3.1 and Theorem 3.3 are based on the methods used by Dobbertin [7], Leander [11] and Tu et al. [16]. Furthermore, we find that the complete permutation polynomials in the second class (see Theorem 3.3) are related to Dickson polynomials. Inspired by the work of Wan and Lidl [18], we obtain the third class of complete permutation monomials (see Theorem 3.5) over finite fields of odd characteristic. In addition, the compositional inverses of these polynomials are also investigated.

The rest of this paper is organized as follows. Necessary basic concepts and related results are given in Section 2. In Section 3, we propose three classes of monomial complete permutations over finite fields of odd characteristic and give their compositional inverses.

2. Preliminaries

For every prime p, the residue class ring $\mathbb{Z}/(p)$ forms a finite filed with p elements. Let p be the characteristic of $\mathbb{F}_{p^n}$; then the prime field contained in $\mathbb{F}_{p^n}$ is $\mathbb{F}_p$, which we identify with $\mathbb{Z}/(p)$. For any positive integer n with a divisor $m \geq 1$, the trace function, denoted by $\mathrm{Tr}_m^n(x)$, from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$ is defined as