Finite Fields and Their Applications 25 (2014) 182–193

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Several classes of complete permutation polynomials

Ziran Tu [a], Xiangyong Zeng [b,c,*], Lei Hu [c]

[a] School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471003, China
[b] Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China
[c] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 9 July 2013
Received in revised form 21 September 2013
Accepted 23 September 2013
Available online 9 October 2013
Communicated by Rudolf Lidl

MSC:
05A05
11T06
11T55

Keywords:
Permutation polynomial
Complete permutation polynomial
Trace function
Walsh spectrum

ABSTRACT

In this paper, three classes of monomials and one class of trinomials over finite fields of even characteristic are proposed. They are proved to be complete permutation polynomials.

1. Introduction

For a prime power q, let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ denote its multiplicative group. A polynomial $f \in \mathbb{F}_q[x]$ is called *a permutation polynomial* (PP) if its associated polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a bijection. Permutation polynomials over finite fields have important applications in cryptography, coding theory and combinatorial design theory [1,3,5,6,10–12,15,16,22,26–28,31]. Finding new PPs is of great interest in both theoretical and applied aspects.

A polynomial $f(x) \in \mathbb{F}_q[x]$ is *a complete permutation polynomial* (CPP) if both $f(x)$ and $f(x) + x$ are permutations of $\mathbb{F}_q$. These polynomials were introduced by Niederreiter and Robinson in [19].

* Corresponding author at: Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China.
E-mail addresses: naturetu@gmail.com (Z. Tu), xyzeng@hubu.edu.cn (X. Zeng), hu@is.ac.cn (L. Hu).

1071-5797/$ – see front matter
http://dx.doi.org/10.1016/j.ffa.2013.09.007

Further study of CPPs can be found in [13,18,24]. Recently, several classes of CPPs were obtained in [29], and some examples of CPPs over the finite field $\mathbb{F}_{16}$ were discussed in [30]. The purpose of this paper is to find more CPPs. The simplest polynomials are monomials, and for a positive integer d and $\alpha \in \mathbb{F}_q^*$, the monomial αx^d over $\mathbb{F}_q$ is a CPP if and only if d satisfies $\gcd(d, q-1) = 1$ and the binomial $\alpha x^d + x$ is a PP. For example, the monomial x^{2^m+2} is a CPP over $\mathbb{F}_q$ [2], where $q = 2^{2m}$ for a positive odd integer m. In this paper, we find other three classes of monomial CPPs over finite fields of even characteristic. The proofs of our main results are based on a criterion for PPs given by using additive characters of the underlying finite fields [16], and the technique in [4,14] to represent the elements of finite fields and the so-called polar coordinate representation [20] are also needed in the proofs. To investigate the permutation behavior of the second class of monomial CPPs proposed in this paper, a crucial problem is to determine the number of solutions to an equation over finite fields (see Lemma 2 (1) for details). The problem is related to a characterization of monomial hyperovals [17], and it can be solved with the corresponding property of Segre hyperoval [23]. In addition, a class of trinomial CPPs is also proposed in this paper.

The remainder of this paper is organized as follows. In Section 2, we introduce some basic concepts and related results. In Section 3, three classes of monomial CPPs are given. A class of trinomial CPPs is also presented in Section 4.

2. Preliminaries

For two positive integers m and n with $m \mid n$, we use $\mathrm{Tr}_m^n(\cdot)$ to denote the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, i.e.,

$$\mathrm{Tr}_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}}.$$

For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, the *Walsh spectrum* of f at $a \in \mathbb{F}_{2^n}$ is defined by

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + \mathrm{Tr}_1^n(ax)}.$$

A criterion for PPs can be given by using additive characters of the underlying finite field [16]. This can also be characterized by judging whether the Walsh spectra of some Boolean functions at 0 are equal to zero.

Lemma 1. *(See [16].) A mapping $g : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a permutation polynomial of $\mathbb{F}_{2^n}$ if and only if for every nonzero $\gamma \in \mathbb{F}_{2^n}$,*

$$\sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(\gamma g(x))} = 0.$$

Let q be a prime power, and we recall some results about the finite projective plane $PG(2, q)$ over $\mathbb{F}_q$. A *k-arc* of $PG(2, q)$ is a set of k distinct points, any three of which are never collinear. The maximum value for k is $q+1$ or $q+2$, according as q is odd or even. When q is odd, $(q+1)$-arcs are called *ovals*, and in the even case, $(q+2)$-arcs are called *hyperovals*. For more details, we refer the reader to [25].

Proposition 1. *(See [9,25].) For even q, every hyperoval of $PG(2, q)$ can be transformed under projective transformations to the following form*:

$$D(f) = \{(1, t, f(t)) : t \in \mathbb{F}_q\} \cup \{(0, 1, 0), (0, 0, 1)\},$$

where $f(x) \in \mathbb{F}_q$ is such that