Finite Fields and Their Applications 49 (2018) 212–226

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Some permutation pentanomials over finite fields with even characteristic

Guangkui Xu [a,*], Xiwang Cao [b,c], Jingshui Ping [a]

[a] *Department of Applied Mathematics, Huainan Normal University, Huainan 232038, China*
[b] *Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China*
[c] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*

ARTICLE INFO

Article history:
Received 6 January 2017
Received in revised form 16 October 2017
Accepted 21 October 2017
Available online xxxx
Communicated by Rudolf Lidl

MSC:
11T06

Keywords:
Finite field
Permutation pentanomial
Permutation trinomial
Fractional polynomial

ABSTRACT

Six classes of permutation pentanomials are constructed from fractional polynomials which permute the set of $(2^m + 1)$-th roots of unity. Based on an approach which is a generalization of the work of Zha, Hu and Fan, some permutation pentanomials and trinomials are also obtained from known permutations of the set of $(2^m + 1)$-th roots of unity.

* Corresponding author.
E-mail addresses: xuguangkuiy@163.com (G. Xu), xwcao@nuaa.edu.cn (X. Cao), kepuduolong@163.com (J. Ping).

https://doi.org/10.1016/j.ffa.2017.10.005
1071-5797/

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements and $\mathbb{F}_q^*$ denote its multiplication group. 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 $\mathbb{F}_q$. Permutation polynomials have theoretical importance in finite fields and have wide applications in cryptography, coding theory, and combinatorial design theory. In general, finding new permutation polynomials of finite fields is not an easy task. For some constructions of permutation polynomials over finite fields, the reader is referred to [1,3,15,13,21,22, 24–31]. The most recent survey paper on permutation polynomials is [6].

Permutation polynomials with few terms have been extensively studied due to their simple algebraic form and some extraordinary properties. For some constructions of permutation polynomials with few terms, the reader is referred to [2,4,7–10,13,18,19,23]. Very recently, some constructions of permutation trinomials from fractional polynomials can be found in [12,14,16]. However, only a small number of classes of permutation pentanomials are known in the literature. To the best of our knowledge, Dobbertin [5] constructed a class of permutation pentanomials to prove Niho's conjecture. In this paper, we continue the work of [11,12,14,16,32] and construct several classes of permutation pentanomials over finite fields with even characteristic from fractional polynomials based on a powerful lemma which was proved in [20,33].

The paper is organized as follows. In Section 2, we give some notation and preliminaries. In Section 3, we present six classes of permutation pentanomials by determining the solutions of some quadratic or cubic equations over finite fields with even characteristic. In Section 4, we obtain some permutation pentanomials and trinomials over finite fields with even characteristic from known permutations of the set of (2^m+1)-th roots of unity.

2. Notation and preliminaries

Let $n = 2m$ be a positive integer and $q = 2^n$. Let $\mathbb{F}_q$ be the finite field with q elements. For any positive integer n, and for any positive integer k dividing n, the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$, denoted by Tr_k^n, is the mapping defined as

$$\mathrm{Tr}_k^n(x) = x + x^{2^k} + x^{2^{2k}} + \cdots + x^{2^{n-k}}.$$

For $k = 1$, the absolute trace function is simply denoted by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. For every integer k dividing n, the trace function satisfies the transitivity property, that is, for all $x \in \mathbb{F}_{2^n}$,

$$\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^k(\mathrm{Tr}_k^n(x)).$$

The permutation polynomials of the form $x^r h(x^{(q-1)/d})$ are interesting and have been paid attention, where $1 \le r < \frac{q-1}{d}$, $d|q-1$ and $h(x) \in \mathbb{F}_q[x]$. For a positive integer d,