Finite Fields and Their Applications 41 (2016) 89–96

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Some new classes of permutation trinomials over finite fields with even characteristic

Rohit Gupta *, R.K. Sharma

Department of Mathematics, Indian Institute of Technology, Delhi, New Delhi 110016, India

ARTICLE INFO

Article history:
Received 7 March 2016
Received in revised form 26 April 2016
Accepted 23 May 2016
Available online 8 June 2016
Communicated by Xiang-dong Hou

MSC:
11T06
11T55

Keywords:
Finite field
Permutation polynomial
Permutation trinomial

ABSTRACT

Let $\mathbb{F}_q$ denote the finite field of order q. In this paper, we present four new classes of permutation trinomials of the form $x^r h(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$.

1. Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is said to be a *permutation polynomial* over $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation of $\mathbb{F}_q$. Recently, permutation

* Corresponding author.
E-mail addresses: rohittgupta20@gmail.com (R. Gupta), rksharmaiitd@gmail.com (R.K. Sharma).

http://dx.doi.org/10.1016/j.ffa.2016.05.004
1071-5797/

polynomials have been an interesting area of research. They have applications in various areas such as coding theory [1,7], cryptography [11,13] and combinatorial designs [3]. Some recent progress on permutation polynomials can be found in [9,14,4,15,16,12,6].

The simplest type of polynomials are monomials. A monomial x^n permutes $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$. But for binomials and trinomials the situation is not so easy. Only a few classes of permutation binomials and trinomials are known. We are particularly interested in classes of permutation trinomials over finite fields with even characteristic. It is known that there are no permutation binomials with both nonzero coefficients equal to 1 over finite fields with even characteristic. This motivates us to find new classes of permutation trinomials with trivial coefficients over finite fields with even characteristic. However, a handful of classes of permutation trinomials over $\mathbb{F}_{2^n}$ are known so far. In [8], Lee and Park characterize permutation trinomials of the form $x^r(h(x^{\frac{q-1}{3}}))$ over $\mathbb{F}_q$ where $q \equiv 1 \pmod 3$. In this paper, we present four new classes of permutation trinomials of the form $x^r(h(x^{\frac{q-1}{d}}))$ with trivial coefficients, where $q = 2^{2m}$ and $d = 2^m + 1$. To the best of the authors' knowledge, the classes of permutation trinomials presented in this paper are new. For a brief survey on known classes of permutation trinomials, we refer to [5,2,10].

2. Preliminaries

Throughout this paper, μ_d denotes the set of d-th roots of unity in the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$. For $m \in \mathbb{N}$, we use $Tr_1^m(\cdot)$ to denote the *trace function* from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, i.e.,

$$Tr_1^m(\alpha) = \alpha + \alpha^2 + \cdots + \alpha^{2^{m-1}}.$$

It is easy to verify that $Tr_1^m(\cdot)$ is a linear function and for $i \in \mathbb{N}$, $Tr_1^m(\alpha^{2^i}) = Tr_1^m(\alpha)$.

Now we present few auxiliary results that will be needed in the next sections.

Lemma 2.1. [17, Lemma 2.1] *Let $d, r > 0$ with $d \mid (q-1)$, and let $h(x) \in \mathbb{F}_q[x]$. Then $f(x) = x^r h(x^{(q-1)/d})$ permutes $\mathbb{F}_q$ if and only if the following two conditions hold:*

(i) $\gcd(r, (q-1)/d) = 1$.
(ii) $x^r h(x)^{(q-1)/d}$ *permutes* μ_d.

Lemma 2.2. *For $m \in \mathbb{N}$, each of the polynomials $1 + x + x^3$, $1 + x^2 + x^3$, $1 + x + x^4$ and $1 + x^3 + x^4$ have no roots in μ_{2^m+1}.*

Proof. Suppose $\alpha \in \mu_{2^m+1}$ is a root of $1 + x + x^3$, i.e.,

$$1 + \alpha + \alpha^3 = 0. \tag{1}$$

Raising both sides of (1) to the power 2^m and multiplying by α^3, we get