Finite Fields and Their Applications 50 (2018) 304–318

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

New permutation quadrinomials over $\mathbb{F}_{2^{2m}}$

Ziran Tu [a], Xiangyong Zeng [b,c,*], Tor Helleseth [d]

[a] *School of Mathematics and Statistics, Henan University of Science and Technology, Luoyang 471003, China*
[b] *Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan, 430062, China*
[c] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[d] *Department of Informatics, University of Bergen, Bergen N-5020, Norway*

ARTICLE INFO

Article history:
Received 2 February 2017
Accepted 29 November 2017
Available online xxxx
Communicated by Gary L. Mullen

MSC:
05A05
11T06
11T55

Keywords:
Permutation polynomial
Finite field
Permutation quadrinomial

ABSTRACT

In this paper, we propose a class of permutation polynomials over the finite field $\mathbb{F}_{2^{2m}}$ for odd m. These permutations are generally quadrinomials, and some permutation trinomials can also be obtained.

* Corresponding author at: Faculty of Mathematics and Statistics, Hubei Key Laboratory of Applied Mathematics, Hubei University, Wuhan, 430062, China.
E-mail addresses: naturetu@gmail.com (Z. Tu), xiangyongzeng@aliyun.com (X. Zeng), tor.helleseth@ii.uib.no (T. Helleseth).

https://doi.org/10.1016/j.ffa.2017.11.013
1071-5797/

1. Introduction

For a prime power q, let $\mathbb{F}_q$ denote the finite field of q elements and $\mathbb{F}_q^*$ denote its multiplicative group. A polynomial $f(x)$ over $\mathbb{F}_q$ is called a *permutation polynomial* if the induced mapping $f\colon c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a bijection. The study of permutation polynomials has a long history and dates back to Hermite [6] and Dickson [2]. Permutation polynomials have important applications in a wide range of areas such as coding theory, combinatorial designs and cryptography. In the last two decades, there is a wealth of results on permutation polynomials over finite fields, and most recent results are included in a survey by Hou [7].

Permutation polynomials with fewer terms attract researchers' attention due to their simple algebra representation and close connection with coding theory, combinatorial designs and cryptography. Recently, some permutation binomials and trinomials were found [3,4,8–11,13,14,19]. The permutation polynomials with the form $x^r f(x^{\frac{q-1}{d}})$ over the finite field $\mathbb{F}_q$ were investigated in [18], where the positive integers r, q and d satisfy $d \,|\, (q-1)$. By choosing certain values of parameters r, q and d, some explicit permutation binomials and trinomials can be constructed. Very recently, Hou determined all permutation trinomials $ax + bx^q + x^{2q-1} \in \mathbb{F}_{q^2}[x]$ of $\mathbb{F}_{q^2}$ [10]. Gupta and Sharma constructed four classes of permutation trinomials of the form $x^r f(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$ and proposed two conjectures [5], which were confirmed in [19] and six classes of new permutation trinomials were also found therein.

The main purpose of this paper is to construct new permutation quadrinomials of the form $x^r f(x^{2^m-1})$ over $\mathbb{F}_{2^{2m}}$ for a positive odd integer m. The technique is to transform the permutation problem to determine the number of solutions in the *unit circle* of certain equations, which can be reduced to a cubic equation over finite fields and it is the key to succeed.

The remainder of this paper is organized as follows. In Section 2, some basic concepts and related results are introduced. In Section 3, a family of permutation polynomials is presented.

2. Preliminaries

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

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

A criterion for permutation polynomials can be given by using additive characters of the underlying finite field [12].