Finite Fields and Their Applications 50 (2018) 178–195

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

A class of new permutation trinomials

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

[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] Department of Informatics, University of Bergen, Bergen N-5020, Norway

ARTICLE INFO

Article history:
Received 10 June 2017
Received in revised form 29 September 2017
Accepted 21 November 2017
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
05A05
11T06
11T55

Keywords:
Permutation polynomial
Finite field
Permutation trinomial

ABSTRACT

In this paper, we characterize the coefficients of $f(x) = x + a_1x^{q(q-1)+1} + a_2x^{2(q-1)+1}$ in $\mathbb{F}_{q^2}[x]$ for even q that lead $f(x)$ to be a permutation of $\mathbb{F}_{q^2}$. We transform the problem into studying some low-degree equations with variable in the unit circle, which are intensively investigated with some parameterization techniques. From the numerical results, the coefficients that lead $f(x)$ to be a permutation appear to be completely characterized in this paper. It is also demonstrated that some permutations proposed in this paper are quasi-multiplicative (QM) inequivalent to the previously known permutation trinomials.

1. Introduction

For a prime power q, denote by $\mathbb{F}_q$ the finite field with q elements. A polynomial $f(x)$ over $\mathbb{F}_q$ is called a *permutation polynomial* if the induced mapping $f: c \mapsto f(c)$ from $\mathbb{F}_q$ to

* Corresponding author.
E-mail addresses: naturetu@gmail.com (Z. Tu), xzeng@hubu.edu.cn (X. Zeng), chunlei.li@uib.no (C. Li), tor.helleseth@uib.no (T. Helleseth).

https://doi.org/10.1016/j.ffa.2017.11.009
1071-5797/

itself is a bijection. The study of permutation polynomials has a long history and dates back to Hermite [13] and Dickson [7]. Permutation polynomials have important applications in a wide range of areas such as coding theory [9,18], combinatorial designs [10] and cryptography [28,29]. In the last two decades, there is a wealth of results on permutation polynomials over finite fields, and many recent results are surveyed by Hou in [14].

Permutations with a few terms have attracted researchers' attention due to their simple algebraic expressions. So far a number of permutation binomials and trinomials have been found in the literatures [8,11,12,15–17,19–22,24,32,36,38]. Among the known results, the trinomials defined from Niho exponents [26] over $\mathbb{F}_{q^2}$, namely

$$f(x) = x + a_1 x^{s_1(q-1)+1} + a_2 x^{s_2(q-1)+1}, \quad a_1, a_2 \in \mathbb{F}_{q^2}, \tag{1}$$

where s_1 and s_2 are two integers, have been intensively studied [8,12,17,19–21,36]. In fact, the trinomials of the form in (1) belong to a class of polynomials with a more generalized form $x^r h(x^{\frac{q-1}{d}})$ [31]. In some special cases, permutation polynomials of this form have been investigated in [4,5,25], and Wan and Lidl characterized them in terms of the primitive roots [31]. A necessary and sufficient condition for these polynomials to be permutations is summarized later in [27,37].

Lemma 1. ([27,37]) *Let q be a prime power and let r, d be two positive integers, then $x^r h(x^{\frac{q-1}{d}})$ permutes $\mathbb{F}_q$ if and only if*

(i) $\gcd\left(r, \frac{q-1}{d}\right) = 1$;
(ii) $x^r h(x)^{\frac{q-1}{d}}$ *permutes the d-th roots of unity in $\mathbb{F}_q$.*

Verifying the second condition in Lemma 1 is generally challenging, so many authors have chosen the coefficients a_1 and a_2 in (1) to be 1 [8,12,19–21,36]. In the case of $(s_1, s_2) = (1, 2)$, Hou determined all the coefficients a_1 and a_2 for $f(x)$ in (1) to be a permutation [17]. To the best of our knowledge, this is the first and unique instance that all possible coefficients of a permutation trinomial in (1) are completely determined. The AGW criterion [1,34,35] is a more general criterion that has been used to examine whether polynomials of certain forms are permutations, e.g., the form as given in (1). Other methods like the multivariate method, linear fractional polynomials, Hermite's criterion and some properties of finite fields are employed to investigate the permutation behaviors of the polynomials proposed in [8,12,19–21,36].

The purpose of this paper is to find new permutation trinomials $f(x)$ as in (1) over $\mathbb{F}_{2^{2m}}$ with more general coefficients a_1 and a_2, where m is a positive integer. To this end, we investigate the coefficients a_1 and a_2 for the case $(s_1, s_2) = (2^m, 2)$. Different from the methods used in [8,12,19–21,36], we introduce a substitution based on the fact that $f(x)$ in (1) has all terms with Niho exponents and then we transform the general equation $f(x) = b$ for any b in $\mathbb{F}_{2^{2m}}$ into quadratic and cubic equations of variable in the unit