Discrete Mathematics 341 (2018) 3010–3020

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

A class of permutation quadrinomials

Ziran Tu [a,d], Xiangyong Zeng [b,*], 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
[d] College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, 266590, China

ARTICLE INFO

Article history:
Received 31 October 2017
Received in revised form 17 May 2018
Accepted 18 July 2018

Keywords:
Permutation polynomial
Finite field
Permutation quadrinomial
Trace function

ABSTRACT

In this paper, we investigate the permutation behavior of a class of quadrinomials. Each term of these quadrinomials has a Niho-type exponent, and two sets of coefficient triples making the quadrinomials to be permutations are obtained. We use a substitution to transform the permutation problem into the root distribution problem in the unit circle of certain quadratic and cubic equations.

1. Introduction

Let q be a prime power and $\mathbb{F}_q$ denote a finite field with q elements. The so-called *permutation polynomial* (PP), i.e., a polynomial in $\mathbb{F}_q[x]$ which induces a bijective mapping over $\mathbb{F}_q$, has attracted people's attentions for a rather long period. From [6] and [11], many new methods and results have been introduced, and some known permutation polynomials can be found in a survey [14] by Hou.

Permutation polynomials, especially those with fewer terms, have important applications in various fields like coding, cryptography and combinatorics. Some known permutation binomials and trinomials can be referred to [7,9,10,12,13,15–19,21,27,28], and a detailed list on trinomials is given in [19]. Many of the results focus on polynomials with Niho exponents [22], i.e., polynomials over $\mathbb{F}_{q^2}$ having the form

$$f(x) = x + \sum_{i=1}^{l} a_i x^{s_i(q-1)+1}. \tag{1}$$

Actually, such kind of polynomials belong to the family of polynomials having a generalized form $x^r h(x^{\frac{q-1}{d}})$ [25], where the permutation property was characterized in terms of primitive roots, and this kind of permutation polynomials was also studied later in [2,16,29]. A more generalized framework to discuss such kind of polynomial is the AGW criterion [1]. However, even with the help of these characterizations, determining the permutation property of polynomials in (1) remains difficult. When $l = 2$, the coefficients $(a_1, a_2) = (1, 1)$ were investigated in [7,10,17–19,28]. By further study, more possible pairs (s_1, s_2) making (1) to be permutations were discussed. When $(s_1, s_2) = (1, 2)$, Hou determined all the coefficients a_1 and a_2 such that the polynomial in (1) is a permutation [13] by using complicated techniques in combinatorics. To the best

* Corresponding author.
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.disc.2018.07.021
0012-365X/

of our knowledge, this is the first and unique instance that all possible coefficients of a permutation trinomial in (1) are completely determined. In [24], when q is even and $(s_1, s_2) = (q, 2)$, through a substitution, the permutation problem in the finite field $\mathbb{F}_{q^2}$ is transformed to determine the root distribution in the unit circle of some parameterized cubic equations. The authors found two sets of coefficient pairs (a_1, a_2) making (1) to be permutations, and based on numerical experiments, they also conjectured that all possible coefficients have been covered by these two sets.

The purpose of this paper is to characterize new quadrinomial permutations in (1) with $l = 3$. Inspired by the parameter pairs $(s_1, s_2) = (1, 2)$ in [13] and $(s_1, s_2) = (q, 2)$ in [24], we investigate the case that $(s_1, s_2, s_3) = (q, 1, 2)$ and q is even (the same type quadrinomials with odd q was discussed in [4]). Two sets of coefficient triples making the quadrinomial to be permutations are proposed with the restriction $a_3 = a_2^2$. By the similar substitution as in [24], we reduce the problem of determining the solutions in $\mathbb{F}_{q^2}$ of the equation $f(x) = b$ to that of the root distribution in the unit circle of certain related quadratic and cubic equations. Some techniques are used to determine the values of certain kinds of *absolute trace*.

The remainder of this paper is organized as follows: In Section 2, some basic concepts and results are introduced. Section 3 presents the main theorem and the proof. Section 4 concludes this study.

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 $\mathbb{F}_{2^m}$ [20], i.e.,

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

For each element x in the finite field $\mathbb{F}_{2^{2m}}$, define $\overline{x} = x^{2^m}$. The *unit circle* of $\mathbb{F}_{2^{2m}}$ is defined as the set

$$U = \left\{ \eta \in \mathbb{F}_{2^{2m}} : \eta^{2^m+1} = \eta\overline{\eta} = 1 \right\}. \tag{2}$$

Lemma 1 ([23]). *Let $A \in \mathbb{F}_{2^{2m}} \setminus \mathbb{F}_{2^m}$ be fixed. Then*

$$U \setminus \{1\} = \left\{ \frac{u + \bar{A}}{u + A} : u \in \mathbb{F}_{2^m} \right\},$$

where U is given in (2).

Lemma 2 ([5]). *For a positive integer n, the quadratic equation $x^2 + ax + b = 0$, $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$.*

When n is even and $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$, the following lemma describes the root distribution in U of the equation $x^2+ax+b = 0$, while case (i) has been discussed in [3,8].

Lemma 3 ([24]). *Let $n = 2m$ be an even positive integer and $a, b \in \mathbb{F}_{2^n}^*$ satisfy $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$. Then for the quadratic equation $x^2 + ax + b = 0$, we have*

(i) *both two solutions are in the unit circle, if and only if $b = \frac{a}{\bar{a}}$ and*

$$\mathrm{Tr}_1^m\left(\frac{b}{a^2}\right) = \mathrm{Tr}_1^m\left(\frac{1}{a\bar{a}}\right) = 1;$$

(ii) *there is exactly one solution in the unit circle, if and only if $b \neq \frac{a}{\bar{a}}$ and*

$$(1 + b\bar{b})(1 + a\bar{a} + b\bar{b}) + a^2\bar{b} + \bar{a}^2 b = 0.$$

Lemma 4 ([26]). *For a positive integer n, let $a, b \in \mathbb{F}_{2^n}$ with $b \neq 0$. The cubic equation $x^3 + ax + b = 0$ has exactly one solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(\frac{a^3}{b^2}) \neq \mathrm{Tr}_1^n(1)$.*

For later convenience we give a corollary as follows:

Corollary 1. *Let m be a positive integer, $B_1, B_2, B_3, B_4 \in \mathbb{F}_{2^m}$ and $B_1(B_2B_3 + B_1B_4) \neq 0$. Then the cubic equation*

$$B_1x^3 + B_2x^2 + B_3x + B_4 = 0$$

has a unique solution in $\mathbb{F}_{2^m}$ if and only if one of the following two conditions holds:

(i) $B_2^2 + B_1B_3 = 0$ *and m is odd;*

(ii) $B_2^2 + B_1B_3 \neq 0$ *and* $\mathrm{Tr}_1^m\left(1 + \frac{(B_2^2+B_1B_3)(B_3^2+B_2B_4)}{(B_2B_3+B_1B_4)^2}\right) = 1.$