Finite Fields and Their Applications 52 (2018) 137–155

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

General constructions of permutation polynomials of the form $(x^{2^m} + x + \delta)^{i(2^m-1)+1} + x$ over $\mathbb{F}_{2^{2m}}$

Libo Wang [a], Baofeng Wu [b,*]

[a] College of Information Science and Technology, Jinan University, Guangzhou 510632, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 15 January 2018
Received in revised form 28 March 2018
Accepted 7 April 2018
Available online xxxx
Communicated by Steven Wang

MSC:
05A05
11T06
11T55

Keywords:
Finite field
Permutation polynomial
Niho exponent

ABSTRACT

Recently, there has been a lot of work on constructions of permutation polynomials of the form $(x^{2^m} + x + \delta)^s + x$ over the finite field $\mathbb{F}_{2^{2m}}$, especially in the case when s is of the form $s = i(2^m - 1) + 1$ (Niho exponent). In this paper, we further investigate permutation polynomials with this form. Instead of seeking for sporadic construction of the parameter i, we give two general sufficient conditions on i such that $(x^{2^m} + x + \delta)^{i(2^m-1)+1} + x$ permutes $\mathbb{F}_{2^{2m}}$: (i) $(2^k + 1)i \equiv 1$ or $2^k \pmod{2^m + 1}$; (ii) $(2^k - 1)i \equiv -1$ or $2^k \pmod{2^m + 1}$, where $1 \leq k \leq m - 1$ is any integer. It turns out that most of previous constructions of the parameter i are covered by our results, and they yield many new classes of permutation polynomials as well.

* Corresponding author.
E-mail address: wubaofeng@iie.ac.cn (B. Wu).

https://doi.org/10.1016/j.ffa.2018.04.003

1. Introduction

Let q be a power of a prime p, and $\mathbb{F}_q$ be the finite field with q elements. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) if its associated polynomial mapping $f : c \mapsto f(c)$ from $\mathbb{F}_q$ to itself is a bijection. PPs over finite fields have important applications in cryptography, coding and combinatorial design. Classical results on properties, constructions and applications of PPs may be found in [5,6]. For some recent advances and contributions to this area, we refer to [3,6] and the references therein.

Helleseth and Zinoviev [2] first investigated PPs of the form

$$\left(\frac{1}{x^2+x+\delta}\right)^{2^\ell} + x$$

for the goal of deriving new identities on Kloosterman sums over $\mathbb{F}_{2^n}$, where $\delta \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(\delta) = 1$, $\ell = 0$ or 1. This motivated Yuan and Ding [10], Yuan, Ding, Wang and Pieprzyk [11] to investigate the permutation behavior of polynomials having the form

$$(x^{p^k} - x + \delta)^s + L(x)$$

over $\mathbb{F}_{p^n}$, where $k,\ s$ are integers, $\delta \in \mathbb{F}_{p^n}$ and $L(x)$ is a linearized polynomial. An extension of the above work and some new classes of PPs were found in [4,12,13,15]. Specially, Tu et al. [8] proposed two classes of PPs over $\mathbb{F}_{2^{2m}}$ of the form

$$(x^{2^m} + x + \delta)^s + x \tag{1}$$

for some s satisfies either

$$s(2^m + 1) \equiv 2^m + 1 \pmod{2^{2m} - 1}$$

or

$$s(2^m - 1) \equiv 2^m - 1 \pmod{2^{2m} - 1}.$$

For these exponents, Zeng et al. [14] further investigated the permutation behavior of the polynomials having the form

$$(\mathrm{Tr}_m^n(x) + \delta)^s + L(x)$$

over finite field $\mathbb{F}_{2^n}$, where $m \mid n$ and $L(x) = x$ or $\mathrm{Tr}_m^n(x) + x$, and "$\mathrm{Tr}_m^n(\cdot)$" is the *trace function* from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ defined by

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