Finite Fields and Their Applications 43 (2017) 69–85

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

New classes of permutation binomials and permutation trinomials over finite fields ☆

Kangquan Li, Longjiang Qu *, Xi Chen

College of Science, National University of Defense Technology, Changsha, 410073, China

ARTICLE INFO

Article history:
Received 13 October 2015
Received in revised form 3 August 2016
Accepted 1 September 2016
Available online xxxx
Communicated by Rudolf Lidl

MSC:
06E30
11T06
94A60

Keywords:
Finite field
Permutation polynomial
Permutation binomial
Permutation trinomial

ABSTRACT

Permutation polynomials over finite fields play important roles in finite fields theory. They also have wide applications in many areas of science and engineering such as coding theory, cryptography, combinatorial design, communication theory and so on. Permutation binomials and permutation trinomials attract people's interest due to their simple algebraic forms and additional extraordinary properties. In this paper, we find a new result about permutation binomials and construct several new classes of permutation trinomials. Some of them are generalizations of known ones.

☆ The research of this paper is supported by the NSFC of China under Grants 61272484, 61572026, the National Basic Research Program of China (Grant No. 2013CB338002), the Basic Research Fund of National University of Defense Technology (No. CJ 13-02-01) and the Program for New Century Excellent Talents in University (NCET).

* Corresponding author.
E-mail addresses: 940672099@qq.com (K. Li), ljqu_happy@hotmail.com (L. Qu), 1138470214@qq.com (X. Chen).

http://dx.doi.org/10.1016/j.ffa.2016.09.002
1071-5797/

1. Introduction

A polynomial $f \in \mathbb{F}_q[x]$ is called a permutation polynomial of $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ from $\mathbb{F}_q$ into $\mathbb{F}_q$ is a permutation. Permutation polynomials over finite fields play important roles in finite fields theory. They also have wide applications in coding theory, cryptography, combinational design, communication theory and so on. The study of permutation polynomial can date back to Hermite [16] and Dickson [11]. There are numerous books and survey papers on the subject covering different periods in the development of this active area [10, Ch. 18], [25, Ch. 7], [29, Ch. 8], [21,22], while the survey by Hou [21] in 2015 is the most recent one.

Permutation binomials and permutation trinomials attract people's interest due to their simple algebraic forms and additional extraordinary properties. Early works on permutation binomials can be traced to Carlitz [7] in 1962. Since then many existence and nonexistence results and new classes of permutation binomials have been discovered. For examples, Carlitz and Wells [8] claimed the existence of permutation polynomials $f = x\left(x^{\frac{q-1}{d}} + a\right)$ over $\mathbb{F}_q$ for each fixed d when q is sufficiently large. On the basis of Carlitz and Wells's works, Niederreiter and Robinson [30] gave a criterion for the polynomials with the aforementioned form to permute $\mathbb{F}_q$ and Wan and Lidl generalized these results in [35]. And Masuda and Zieve [27] gave a range of the number of $a \in \mathbb{F}_q$ such that $x^r\left(x^{\frac{q-1}{d}} + a\right)$ is a permutation binomial over $\mathbb{F}_q$. There are also numerous results about nonexistence of permutation binomials proved by several authors, such as Niederreiter and Robinson [30], Masuda and Zieve [27] and so on. Niederreiter and Robinson [30] proved that $f = x^m + ax \in \mathbb{F}_q[x]$, where $a \neq 0$ and $m > 0$ is not a power of $\mathrm{char}\mathbb{F}_q$, is not a permutation binomial over $\mathbb{F}_q$ if $q \geq \left(m^2 - 4m + 6\right)^2$. Later, Turnwald [33], Wan [34], Masuda and Zieve [27] improved and generalized this negative result. In recent years, the study about constructing new explicit permutation binomials is increasingly popular [5,17,23,24,32,36]. Wang [36] gave a necessary and sufficient condition for a polynomial with the form $x^n\left(x^{\frac{q-1}{d}} + 1\right)$ to be a permutation over $\mathbb{F}_q$ through exploring a connection between permutation polynomials of the form $x^n f\left(x^{\frac{q-1}{d}}\right)$ and cyclotomic mapping permutations over finite fields. Recently, Hou and Lappano [17,23,24] determined several explicit classes of permutation binomials with the form $ax + x^{2q-1}$, $ax + x^{3q-2}$, $ax + x^{5q-4}$ and $ax + x^{7q-6}$ over $\mathbb{F}_{q^2}$ by Hermite's Criterion [16] (cf. Lemma 2.3 in Section 2). The hard point to use Hermite's Criterion is to compute $\sum_{x \in \mathbb{F}_{q^2}} f(x)^s$ for $1 \leq s \leq 2^n - 1$ and $s \not\equiv 0 \bmod \mathrm{Char}\mathbb{F}_{q^2}$. Another way to obtain binomials is deducing from monomial complete permutation polynomials. A polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *complete permutation polynomial* over $\mathbb{F}_q$ if both $f(x)$ and $f(x)+x$ are permutation polynomials over $\mathbb{F}_q$. Therefore, if $f(x)$ is a monomial complete permutation polynomial, then $f(x)+x$ is a permutation binomial. Recently, there are many results about complete permutation monomials. Therefore, many permutation binomials are obtained in the meanwhile, such as [5,31,37–40,42]. Most proofs of these permutations utilized the method through computing the exponential sum $\sum_{x \in \mathbb{F}_q} (-1)^{\mathrm{Tr}_q(\gamma f(x))}, \gamma \in \mathbb{F}_q^*$, where Tr_q is the absolute trace function over $\mathbb{F}_q$.