Finite Fields and Their Applications 33 (2015) 198–211

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Permutation and complete permutation polynomials

L.A. Bassalygo, V.A. Zinoviev *

Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, GSP-4, 127994, Russia

A R T I C L E   I N F O

Article history:
Received 22 April 2014
Received in revised form 6 November 2014
Accepted 11 November 2014
Available online 14 January 2015
Communicated by Rudolf Lidl

MSC:
11T06
11T71
12Y05

Keywords:
Finite field
Permutation polynomial
Complete permutation polynomial
Exponential sum

A B S T R A C T

Polynomials of type $x^{q+2} + bx$ over the field $\mathbb{F}_{q^2}$ and of type $x^{q^2+q+2} + bx$ over $\mathbb{F}_{q^3}$, where $q = p^m > 2$ is a power of a prime p are considered. All cases when these polynomials are permutation polynomials are classified. Therefore, all cases when the polynomials $b^{-1}x^{q+2}$ over $\mathbb{F}_{q^2}$ and $b^{-1}x^{q^2+q+2}$ over $\mathbb{F}_{q^3}$ are the complete permutation polynomials are enumerated.

1. Introduction

The interest to a special case of the permutation polynomials – the complete permutation polynomials – has recently reappeared. A permutation polynomial $f(x)$ over a finite field $\mathbb{F}_q$ is called a *complete permutation polynomial* (see [2,6,9,11]), or a *complete*

* Corresponding author.
E-mail addresses: bass@iitp.ru (L.A. Bassalygo), zinov@iitp.ru (V.A. Zinoviev).

http://dx.doi.org/10.1016/j.ffa.2014.11.010
1071-5797/

mapping (see [5,7]), if $f(x) + x$ is also a permutation polynomial. We slightly generalize this definition: a permutation polynomial $f(x)$ over a finite field $\mathbb{F}_q$ is called a *b-complete permutation polynomial* if $f(x) + bx$ is also a permutation polynomial, $b \in \mathbb{F}_q^*$. Here and always later $b \neq 0$. Clearly, if $f(x)$ is a b-complete permutation polynomial then $b^{-1}f(x)$ is a complete permutation polynomial. Note that all complete permutation polynomials of degree at most 5 are listed in [7] and in [3], respectively.

We need the following result of [7].

Lemma 1. *(See [7].) The polynomial*

$$f(x) = x^{1+\frac{q-1}{n}} + bx, \quad n|(q-1),\ n > 1,$$

over $\mathbb{F}_q$ is a permutation polynomial if and only if the following conditions are satisfied:

(i) *the element b is such that $(-b)^n \neq 1$;*
(ii) *the inequality*

$$\left(\left(b + \omega^i\right)\left(b + \omega^j\right)^{-1}\right)^{\frac{q-1}{n}} \neq \omega^{j-i} \tag{1}$$

holds for all i, j, such that $0 \le i < j < n$, where ω is a fixed primitive root of the nth degree of 1 in the field $\mathbb{F}_q$.

Here, we use this lemma for certain special cases of $\mathbb{F}_q$ and the integer n. Throughout the paper, we assume that $q = p^m$, where p is the field characteristic and $p^m > 2$. For a field of any characteristic, we found all cases in which the polynomials $x^{q+2} + bx$ over the field $\mathbb{F}_{q^2}$ and the polynomials $x^{q^2+q+2} + bx$ over $\mathbb{F}_{q^3}$ are the permutation polynomials. In addition, for the fields of characteristic $p = 2$ and the polynomials $x^{q+2} + bx$ over $\mathbb{F}_{q^2}$ we give another proof of the results obtained in papers [2,8], and for the polynomials x^{q^2+q+2} over $\mathbb{F}_{q^3}$ we strengthen the previous results of [9,11] (see details below).

Thus, we answered the question of when the polynomials x^{q+2} over the fields $\mathbb{F}_{q^2}$ and the polynomials x^{q^2+q+2} over $\mathbb{F}_{q^3}$ are the b-complete permutation polynomials.[1]

2. The case of polynomial $x^{q+2} + bx$

Consider the field $\mathbb{F}_{q^2}$ and set $n = q - 1$. Then the condition $(-b)^n \neq 1$ implies that $b \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Set $x = \omega^i$ and $y = \omega^j$, and then the inequality (1) becomes the following inequality:

$$x(b + x)^{q+1} \neq y(b + y)^{q+1},$$

[1] The results of the paper are published without proofs in conference proceedings ACCT-2014 [1].