Finite Fields and Their Applications 52 (2018) 30–50

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On a conjecture about a class of permutation trinomials

Daniele Bartoli

ARTICLE INFO

Article history:
Received 28 December 2017
Received in revised form 3 March 2018
Accepted 13 March 2018
Available online xxxx
Communicated by Xiang-dong Hou

MSC:
11T06

Keywords:
Permutation polynomials
Finite fields
Algebraic curves

ABSTRACT

We prove a conjecture by Tu, Zeng, Li, and Helleseth concerning trinomials $f_{\alpha,\beta}(x) = x+\alpha x^{q(q-1)+1}+\beta x^{2(q-1)+1} \in \mathbb{F}_{q^2}[x]$, $\alpha\beta \neq 0$, q even, characterizing all the pairs $(\alpha, \beta) \in \mathbb{F}_{q^2}^2$ for which $f_{\alpha,\beta}(x)$ is a permutation of $\mathbb{F}_{q^2}$.

1. Introduction

Let $q = p^h$ be a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a *permutation polynomial* (PP for short) if it is a bijection of the finite field $\mathbb{F}_q$ into itself. On the other hand, each permutation of $\mathbb{F}_q$ can be expressed as a polynomial over $\mathbb{F}_q$.

Permutation polynomials have nice connections with applied areas of mathematics, such as cryptography, coding theory, and combinatorial designs. Random PP for a given field $\mathbb{F}_q$ can be easily constructed. In many applications, however, simple structures or additional extraordinary properties on PPs are usually required and PPs meeting these

E-mail address: daniele.bartoli@unipg.it.

https://doi.org/10.1016/j.ffa.2018.03.003

criteria are usually difficult to find. For a deeper treatment of the connections of PPs with other fields of mathematics we refer to [7,6] and the references therein.

In this work we deal with a particular class of PPs introduced in [10], that is polynomials $f_{\alpha,\beta}(x) \in \mathbb{F}_{q^2}$ of type

$$x + \alpha x^{q(q-1)+1} + \beta x^{2(q-1)+1}, \tag{1}$$

with $\alpha, \beta \in \mathbb{F}_{q^2}^*$, $q = 2^m$. The authors prove that if

1. $\beta = \alpha^{q-1}$ and $Tr\left(1 + \frac{1}{\alpha^{q+1}}\right) = 0$ or
2. $\beta(1 + \alpha^{q+1} + \beta^{q+1}) + \alpha^{2q} = 0$, $\beta^{q+1} \neq 1$, and $Tr\left(\frac{\beta^{q+1}}{\alpha^{q+1}}\right) = 0$

then $f_{\alpha,\beta}(x)$ permutes $\mathbb{F}_{q^2}$; see [10, Theorem 1]. Due to some experimental results, the authors state the following conjecture.

Conjecture 1.1. *If $f_{\alpha,\beta}(x)$ permutes $\mathbb{F}_{q^2}$ then 1 or 2 holds.*

In this work we prove the above conjecture, using the well known connection between permutation polynomials and algebraic curves over finite fields.

First of all, let us remark that the polynomials $f_{\alpha,\beta}(x)$ belong to the more general class of polynomials

$$f_{r,d,h}(x) = x^r h\left(x^{\frac{q-1}{d}}\right),$$

where $h(x)$ is a polynomial over $\mathbb{F}_q$, $q = p^m$, d a divisor of $q-1$, r an integer with $1 \leq r < (q-1)/d$.

A useful criterion to decide weather $f_{r,d,h}$ permutes $\mathbb{F}_q$ was established in [8,13].

Theorem 1.2. *The polynomial $f_{r,d,h}(x)$ is a PP of $\mathbb{F}_q$ if and only if $gcd(r,(q-1)/d) = 1$ and $x^r h(x)^{(q-1)/d}$ permutes the set μ_d of the d-th roots of unity in $\mathbb{F}_q$.*

The above theorem can be seen as an application of the AGW criterion; see [1,11,12].

By Theorem 1.2, the polynomial $f_{\alpha,\beta}(x)$ in (1) permutes $\mathbb{F}_{q^2}$ if and only if

$$x(1 + \alpha x^q + \beta x^2)^{q-1}$$

permutes μ_{q+1}. Recalling that for $x \in \mu_{q+1}$ we have that $x^q = 1/x$, this is equivalent to

$$g_{\alpha,\beta}(x) = \frac{\alpha^q x^3 + x^2 + \beta^q}{\beta x^3 + x + \alpha}$$

permuting μ_{q+1}.