Finite Fields and Their Applications 51 (2018) 1–16

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Permutation polynomials, fractional polynomials, and algebraic curves

Daniele Bartoli *, Massimo Giulietti

Department of Mathematics and Computer Science, University of Perugia, 06123 Perugia, Italy

ARTICLE INFO

Article history:
Received 16 August 2017
Received in revised form 28 November 2017
Accepted 6 January 2018
Available online xxxx
Communicated by Stephen D. Cohen

MSC:
11T06

Keywords:
Permutation polynomials
Fractional permutation polynomials

ABSTRACT

In this note we prove a conjecture by Li, Qu, Li, and Fu on permutation trinomials over $\mathbb{F}_{3^k}^2$. In addition, new examples and generalizations of some families of permutation polynomials of $\mathbb{F}_{3^k}$ and $\mathbb{F}_{5^k}$ are given. We also study permutation quadrinomials of type $Ax^{q(q-1)+1}+Bx^{2(q-1)+1}+Cx^q+x$. Our method is based on the investigation of an algebraic curve associated with a fractional polynomial over a finite field.

1. Introduction

Let $q = p^h$ be a prime power. A polynomial $f(x) \in \mathbb{F}_q[x]$ is a *permutation polynomial* (PP) 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 were first studied by Hermite and Dickson; see [5,8].

* Corresponding author.
E-mail addresses: daniele.bartoli@unipg.it (D. Bartoli), massimo.giulietti@unipg.it (M. Giulietti).

https://doi.org/10.1016/j.ffa.2018.01.001
1071-5797/

In general it is not difficult to construct a random PP for a given field $\mathbb{F}_q$. Particular, simple structures or additional extraordinary properties are usually required by applications of PPs in other areas of mathematics and engineering, such as cryptography, coding theory, or combinatorial designs. Permutation polynomials meeting these criteria are usually difficult to find. For a deeper introduction on the connections of PPs with other fields of mathematics we refer to [14,9] and the references therein.

In this work we deal with a particular class of PPs. For a prime p and a positive integer m, let $\mathbb{F}_{p^m}$ be the finite field with p^m elements. Given a polynomial $h(x)$ over $\mathbb{F}_{p^m}$, a divisor d of p^m-1, and an integer r with $1 \le r < (p^m-1)/d$, let

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

A useful criterion to decide weather $f_{r,d,h}$ permutes $\mathbb{F}_{p^m}$ is the following.

Theorem 1.1. [15,19] *The polynomial $f_{r,d,h}(x)$ is a PP of $\mathbb{F}_{p^m}$ if and only if $gcd(r,(p^m-1)/d)=1$ and $x^r h(x)^{(p^m-1)/d}$ permutes the set μ_d of the d-th roots of unity in $\mathbb{F}_{p^m}$.*

Let $q=p^n$. For $h(x)=\sum_{i=0}^{\ell} a_i x^i$ a polynomial over $\mathbb{F}_{q^2}$, by Theorem 1.1 $x^r h\left(x^{q-1}\right)$ permutes $\mathbb{F}_{q^2}$ if and only if $x^r h\left(x\right)^{q-1}$ permutes μ_{q+1}. If this is the case and in addition $h(x) \in \mathbb{F}_q[x]$, then for each $z \in \mu_{q+1}$ we have that

$$z^r h\left(z\right)^{q-1} = z^r \frac{(h(z))^q}{h(z)} = z^r \frac{h(1/z)}{h(z)} = z^{r-\ell}\frac{\widetilde{h}(z)}{h(z)},$$

where $\deg(h)=\ell$ and $\widetilde{h}(x)=\sum_{i=0}^{\ell} a_{\ell-i}x^i$. We call the rational function $x^{r-\ell}\frac{\widetilde{h}(x)}{h(x)}$ the *fractional polynomial* associated with the PP $x^r h\left(x^{q-1}\right)$. Conversely, given a fractional polynomial $x^{r-\ell}\frac{\widetilde{h}(x)}{h(x)}$ which permutes μ_{q+1} we call $x^r h\left(x^{q-1}\right)$ the associated permutation polynomial.

A standard approach to the problem of deciding whether a polynomial $f(x)$ is a PP is the investigation of the plane algebraic curve

$$\mathcal{C}_f : \frac{f(x)-f(y)}{x-y} = 0;$$

in fact, f is a PP over $\mathbb{F}_{p^m}$ if and only if $\mathcal{C}_f$ has no $\mathbb{F}_{p^m}$-rational point (a,b) with $a \neq b$. In the case where $p^m=q^2$ and f is of type $f_{r,q+1,h}$ with $h \in \mathbb{F}_q[x]$, it can be more effective to study the curve, with degree lower than $\mathcal{C}_f$, defined by the equation

$$x^{r-\ell}\frac{\widetilde{h}(x)}{h(x)} - y^{r-\ell}\frac{\widetilde{h}(y)}{h(y)} = 0$$

and check whether it has some $\mathbb{F}_{q^2}$-rational points (a,b) with $a \neq b$ and $a^{q+1}=b^{q+1}=1$.