Journal of Number Theory 147 (2015) 14–23

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Determination of a type of permutation binomials over finite fields

Xiang-Dong Hou [*,1], Stephen D. Lappano

Department of Mathematics and Statistics, University of South Florida, Tampa, FL 33620, United States

A R T I C L E   I N F O

Article history:
Received 20 January 2014
Received in revised form 13 June 2014
Accepted 16 June 2014
Available online 8 August 2014
Communicated by D. Wan

MSC:
11T06
11T55

Keywords:
Binomial
Finite field
Hermite criterion
Permutation polynomial

A B S T R A C T

Let $f = a\mathtt{x} + \mathtt{x}^{3q-2} \in \mathbb{F}_{q^2}[\mathtt{x}]$, where $a \in \mathbb{F}_{q^2}^*$. We prove that f is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following occurs: (i) $q = 2^e$, e odd, and $a^{\frac{q+1}{3}}$ is a primitive 3rd root of unity. (ii) (q, a) belongs to a finite set which is determined in the paper.

1. Introduction

A polynomial $f \in \mathbb{F}_q[\mathtt{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if it induces a permutation of $\mathbb{F}_q$. While permutation monomials of $\mathbb{F}_q$ are obvious ($a\mathtt{x}^n$, $a \in \mathbb{F}_q^*$, $\gcd(n, q-1) = 1$), the situation for permutation binomials is much more interesting

* Corresponding author.
E-mail addresses: xhou@usf.edu (X.-D. Hou), slappano@mail.usf.edu (S.D. Lappano).

[1] Research partially supported by NSA Grant H98230-12-1-0245.

http://dx.doi.org/10.1016/j.jnt.2014.06.021

and challenging. The reason for a binomial to be a PP can be quite nontrivial despite the simple appearance of the binomial. In [3], Carlitz and Wells proved that for fixed integers $e > 1$ and $c > 0$, when q is large enough and satisfies the conditions $e \mid q-1$ and $\gcd(c, q-1) = 1$, there exists $a \in \mathbb{F}_q^*$ such that $\mathtt{x}^c(\mathtt{x}^{\frac{q-1}{e}} + a)^k$ is a PP of $\mathbb{F}_q$ for all $k \geq 0$. (Note that when $k = 1$, the PP is a binomial.) The special cases of this result with $c = k = 1$ and $e = 2, 3$ appeared in [2]. Carlitz and Wells' proof of the existence result relies on a bound on the Weil sum of a multiplicative character of $\mathbb{F}_q$ [17], [8, Theorem 5.39]. Using the Hasse–Weil bound on the number of degree one places of a function field over $\mathbb{F}_q$ [11, Theorem V.2.3], Masuda and Zieve [9] were able to make Carlitz–Wells' existence result (with $k = 1$) more precise. They proved that if $q \geq 4$ and $\frac{q-1}{e} > 2q(\log\log q)/\log q$, then there exists $a \in \mathbb{F}_q^*$ such that $\mathtt{x}^c(\mathtt{x}^{\frac{q-1}{e}} + a)$ is a PP of $\mathbb{F}_q$. Moreover, they obtained an estimate for the number of a's with this property.

There are also nonexistence results on permutation binomials. Niederreiter and Robinson [10] proved that if there is a PP of $\mathbb{F}_q$ of the form $\mathtt{x}^m + a\mathtt{x}$, where $m > 2$ and $a \in \mathbb{F}_q^*$, then either m is a power of p ($p = \operatorname{char}\mathbb{F}_q$) or $q < (m^2 - 4m + 6)^2$. An improvement of this result was obtained by Turnwald [13]: If there is a PP of $\mathbb{F}_q$ of the form $\mathtt{x}^m + a\mathtt{x}^n$, where $m > n > 0$ and $a \in \mathbb{F}_q^*$, then either $\frac{m}{n}$ is a power of p or $q \leq (m-2)^4 + 4m - 4$. For permutation binomials over prime fields, the nonexistence results are stronger. Wan [14] proved that if there is a PP of $\mathbb{F}_p$ of the form $\mathtt{x}^m + a\mathtt{x}$, where $m > 1$ and $a \in \mathbb{F}_p^*$, then $p - 1 \leq (m-1)\gcd(m-1, p-1)$. Turnwald [13] considered $f = \mathtt{x}^m + a\mathtt{x}^n \in \mathbb{F}_p[\mathtt{x}]$, where $m > n > 0$ and $a \in \mathbb{F}_p^*$, and proved that f is a PP of $\mathbb{F}_p$ implies $p < m \cdot \max(n, m-n)$. Masuda and Zieve [9] improved Turnwald's bound to $p - 1 < (m-1) \cdot \max\{n, \gcd(m-n, p-1)\}$.

Let $r \geq 2$. In [2], Carlitz proved that the binomial $\mathtt{x}^{1+\frac{q-1}{2}} + a\mathtt{x}$ (q odd, $a \neq 0$) cannot be a PP of $\mathbb{F}_{q^r}$, and he raised the same question for $\mathtt{x}^{1+\frac{q-1}{3}} + a\mathtt{x}$ ($q \equiv 1 \pmod 3$, $a \neq 0$). Wan [14,15] answered Carlitz's question by showing that $\mathtt{x}^{1+\frac{q-1}{3}} + a\mathtt{x}$ ($q \equiv 1 \pmod 3$, $a \neq 0$) cannot be a PP of $\mathbb{F}_{p^r}$. Kim and Lee [7] proved that $\mathtt{x}^{1+\frac{q-1}{5}} + a\mathtt{x}$ ($q \equiv 1 \pmod 5$, $a \neq 0$) cannot be a PP of $\mathbb{F}_{q^r}$ for $p \neq 2$. More generally, one may consider $\mathtt{x}^{1+\frac{q-1}{m}} + a\mathtt{x} \in \mathbb{F}_q[\mathtt{x}]$, where $q \equiv 1 \pmod m$, $m \geq 2$, $a \neq 0$. Clearly, if $m = \frac{q-1}{p^i-1}$, where $\mathbb{F}_{p^i} \subset \mathbb{F}_q$, then $\mathtt{x}^{1+\frac{q-1}{m}} + a\mathtt{x} = \mathtt{x}^{p^i} + a\mathtt{x}$, which is a PP of $\mathbb{F}_{q^r}$ if and only if $(-a)^{(q^r-1)/(p^i-1)} \neq 1$. When $1 + \frac{q-1}{m}$ is not a power of p, it is not known if the binomial can be a PP of $\mathbb{F}_{q^r}$.

Let $f = \mathtt{x}^m + a\mathtt{x}^n \in \mathbb{F}_q[\mathtt{x}]$, where $m > n > 0$ and $a \in \mathbb{F}_q^*$. The conditions that make f a PP of $\mathbb{F}_q$ are encoded in a simple set of parameters m, n, q, a in a mysterious way that is not well understood on the whole. However, when m and n take certain particular forms, necessary and sufficient conditions for f to be a PP of $\mathbb{F}_q$ have been found. Niederreiter and Robinson [10] proved that $\mathtt{x}^{\frac{q+1}{2}} + a\mathtt{x} \in \mathbb{F}_q[x]$ (q odd, $a \in \mathbb{F}_q^*$) is a PP of $\mathbb{F}_q$ if and only if $a^2 - 1$ is a square in $\mathbb{F}_q^*$; also see [2]. Akbary and Wang [1] considered binomials of the form $f = \mathtt{x}^r(1 + \mathtt{x}^{es})$, where e, r, s are positive integers such that $s \mid q-1$, $\gcd(r, s) = 1$, $\gcd(2e, \frac{q-1}{s}) = 1$. They found sufficient conditions for f to be a PP of $\mathbb{F}_q$ in terms of the period of the generalized Lucas sequence. The conditions are not entirely explicit, but their special cases do give explicit classes of permutation binomials of $\mathbb{F}_q$. The sufficient conditions in [1] were later weakened by Wang [16] to conditions that are both necessary