Journal of Number Theory 133 (2013) 3549–3558

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A class of permutation binomials over finite fields

Xiang-dong Hou [1]

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

ARTICLE INFO

Article history:
Received 9 October 2012
Revised 1 March 2013
Accepted 16 April 2013
Available online 19 June 2013
Communicated by D. Wan

MSC:
11T06
11T55
33C05

Keywords:
Finite field
Hypergeometric sum
Permutation polynomial

ABSTRACT

Let q be a prime power and $f = tx + x^{2q-1}$, where $t \in \mathbb{F}_q^*$. It was recently conjectured that f is a permutation polynomial of $\mathbb{F}_{q^2}$ if and only if one of the following holds: (i) $t = 1$, $q \equiv 1 \pmod 4$; (ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$; (iii) $t = 3$, $q \equiv -1 \pmod 6$. We confirm this conjecture in the present paper.

1. Introduction

Let q be a prime power and $\mathbb{F}_q$ the finite field with q elements. A polynomial $f \in \mathbb{F}_q[x]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Nontrivial PPs in simple algebraic forms are rare. Such PPs are sometimes the result of the mysterious interplay between the algebraic and combinatorial structures of the finite field. Permutation *binomials* over finite fields are particularly interesting for this reason, and they have attracted the attention of many researchers over decades; see [1,3,10–12,15–19]. In these references, the reader will find not only many interesting results on permutation binomials but also plenty challenges that remain.

The main result of the present paper is the following theorem:

Theorem 1.1. *Let $f = tx + x^{2q-1} \in \mathbb{F}_q[x]$, where $t \in \mathbb{F}_q^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:*

E-mail address: xhou@usf.edu.

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

http://dx.doi.org/10.1016/j.jnt.2013.04.011

(i) $t = 1$, $q \equiv 1 \pmod 4$;
(ii) $t = -3$, $q \equiv \pm 1 \pmod{12}$;
(iii) $t = 3$, $q \equiv -1 \pmod 6$.

In fact, an equivalent form of Theorem 1.1 was conjectured in [4], where the polynomial is $\mathtt{x}^{q-2} + t\mathtt{x}^{q^2-q-1}$, which is $f(\mathtt{x}^{q^2-q-1})$ modulo $\mathtt{x}^{q^2} - \mathtt{x}$ for $q > 2$. (Note that $\mathtt{x}^{q^2-q-1}$ is a PP of $\mathbb{F}_{q^2}$.) The conjecture originated from a recent study of certain permutation polynomials over finite fields defined by a functional equation. We will briefly describe this connection in Section 4.

The attempt to prove Theorem 1.1 has led to the discovery of a curious hypergeometric identity stated in Theorem 1.2. In return, Theorem 1.2 clears the last hurdle in the proof of Theorem 1.1.

Theorem 1.2. *Let $n \geqslant 0$ be an integer. Then we have*

$$\sum_{k \leqslant 2n+1} \binom{2n+1}{k} \left(\prod_{j=1}^{2n+1} (6n - 2k + 4 - 2j) \right) (-1)^k 3^{2k+1} + \sum_{k \leqslant 2n+1} \binom{2n+1}{k} \left(\prod_{j=1}^{2n+1} (6n - 2k + 5 - 2j) \right) (-1)^k 3^{2k} = 0. \tag{1.1}$$

The proofs of Theorems 1.2 and 1.1 are given in Sections 2 and 3, respectively.

Remarks.

(i) There are criteria for a polynomial of the form $\mathtt{x}^r h(\mathtt{x}^{\frac{q-1}{d}})$ to be a PP of $\mathbb{F}_q$, where $d, r > 0$, $d \mid q-1$, and $h \in \mathbb{F}_q[\mathtt{x}]$; see [1,2,18–20]. We can write the polynomial f in Theorem 1.1 as $f = \mathtt{x}h(\mathtt{x}^{q-1})$, where $h(\mathtt{x}) = \mathtt{x}^2 + t$. According to [20, Lemma 2.1], f is a PP of $\mathbb{F}_{q^2}$ if and only if $\mathtt{x}(\mathtt{x}^2 + t)^{q-1}$ permutes the $(q-1)$st powers in $\mathbb{F}_{q^2}^*$. This observation, though interesting in its own right, does not seem to be useful in our approach.
(ii) The following related result is a special case of [20, Theorem 1.1]: Assume that q is odd and $a \in \mathbb{F}_{q^2}^*$ such that $(-a)^{\frac{q+1}{2}} \neq 1$ and $(\eta + \frac{a}{\eta})^{2(q-1)} = 1$ for every $\eta \in \mathbb{F}_{q^2}^*$ with $\eta^{q+1} = 1$. Then $a\mathtt{x} + \mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$.
(iii) In [19], necessary and sufficient conditions are given for the polynomial $\mathtt{x}^r(\mathtt{x}^{es} + 1)$ to be a PP of $\mathbb{F}_q$, where q is odd, $s \mid q-1$, and $\gcd(2e, \frac{q-1}{s}) = 1$. However, the conditions there are not explicit enough for one to derive Theorem 1.1 with $t = 1$, or equivalently, $t = a^{2(q-1)}$ for some $a \in \mathbb{F}_{q^2}^*$.

2. Proof of Theorem 1.2

Let

$$F_1(n,k) = \binom{2n+1}{k} \left(\prod_{j=1}^{2n+1} (6n - 2k + 4 - 2j) \right) (-1)^k 3^{2k+1},$$

$$F_2(n,k) = \binom{2n+1}{k} \left(\prod_{j=1}^{2n+1} (6n - 2k + 5 - 2j) \right) (-1)^k 3^{2k},$$

$$S_1(n) = \sum_k F_1(n,k),$$

$$S_2(n) = \sum_k F_2(n,k).$$