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

ARTICLE INFO

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

ABSTRACT

Let $f = a\mathbf{x} + \mathbf{x}^{3q-2} \in \mathbb{F}_{q^2}[\mathbf{x}]$, 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.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

A polynomial $f \in \mathbb{F}_q[\mathbf{x}]$ 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 ($a\mathbf{x}^n$, $a \in \mathbb{F}_q^*$, $\gcd(n, q-1) = 1$), 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
0022-314X/© 2014 Elsevier Inc. All rights reserved.

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

and sufficient. Zieve [18] considered $f = \mathtt{x}^m + a\mathtt{x}^n \in \mathbb{F}_q[\mathtt{x}]$, where $m > n > 0$ and $a \in \mathbb{F}_q^*$, under the assumption that $\{\eta + \frac{1}{\eta} : \eta \in \mu_{2d}\} \subset \mu_s$, where $s = \gcd(m-n, q-1)$, $d = \frac{q-1}{s}$ and $\mu_s = \{x \in \mathbb{F}_q : x^s = 1\}$. In this setting, it was shown that f is a PP of $\mathbb{F}_q$ if and only $-a \notin \mu_d$, $\gcd(n, s) = 1$ and $\gcd(2d, m+n) \leq 2$. (This characterization implies the aforementioned sufficient conditions in [1]; see [18].) We also refer the reader to a new survey [6] on permutation binomials and trinomials where more results and references on the topic can be found.

Recently, we determined all PPs of $\mathbb{F}_{q^2}$ of the form $a\mathtt{x} + \mathtt{x}^{2q-1}$ ($a \in \mathbb{F}_{q^2}^*$) [4,5]. The techniques introduced there are applicable to binomials of similar types. In the present paper, we determine all PPs of $\mathbb{F}_{q^2}$ of the form $a\mathtt{x} + \mathtt{x}^{3q-2}$. Our main result is the following.

Theorem 1.1. *Let $f = a\mathtt{x} + \mathtt{x}^{3q-2} \in \mathbb{F}_{q^2}[\mathtt{x}]$, where $a \in \mathbb{F}_{q^2}^*$. Then f is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs.*

(i) $q = 2^{2k+1}$ *and* $a^{\frac{q+1}{3}}$ *is a primitive 3rd root of unity.*
(ii) $q = 5$ *and* a^2 *is a root of* $(\mathtt{x}+1)(\mathtt{x}+2)(\mathtt{x}-2)(\mathtt{x}^2-\mathtt{x}+1)$.
(iii) $q = 2^3$ *and* a^3 *is a root of* $\mathtt{x}^3 + \mathtt{x} + 1$.
(iv) $q = 11$ *and* a^4 *is a root of* $(\mathtt{x}-5)(\mathtt{x}+2)(\mathtt{x}^2-\mathtt{x}+1)$.
(v) $q = 17$ *and* $a^6 = 4, 5$.
(vi) $q = 23$ *and* $a^8 = -1$.
(vii) $q = 29$ *and* $a^{10} = -3$.

Remark 1.2. Under the assumption that a is a $(q+1)$st root of unity, Theorem 1.1(i), which is the only relevant case under this assumption, follows from [19, Corollary 5.3]. If, in addition, q is assumed to be even, then [12, Theorem 1] also gives sufficiency part of Theorem 1.1(i).

2. Preliminaries

Let $f = a\mathtt{x} + \mathtt{x}^{3q-2} \in \mathbb{F}_{q^2}[\mathtt{x}]$, where $a \in \mathbb{F}_{q^2}^*$, and let $0 \leq \alpha, \beta \leq q-1$, $(\alpha, \beta) \neq (0,0)$. We have

$$\begin{aligned}\sum_{x \in \mathbb{F}_{q^2}} f(x)^{\alpha+\beta q} &= \sum_{x \in \mathbb{F}_{q^2}^*} \left(ax + x^{3q-2}\right)^{\alpha} \left(a^q x^q + x^{3-2q}\right)^{\beta} \\ &= \sum_{x \in \mathbb{F}_{q^2}^*} \sum_{i,j} \binom{\alpha}{i} (ax)^{\alpha-i} x^{(3q-2)i} \binom{\beta}{j} \left(a^q x^q\right)^{\beta-j} x^{(3-2q)j} \\ &= a^{\alpha+\beta q} \sum_{i,j} \binom{\alpha}{i}\binom{\beta}{j} a^{-i-jq} \sum_{x \in \mathbb{F}_{q^2}^*} x^{\alpha+\beta q+3(q-1)(i-j)}. \qquad (2.1)\end{aligned}$$

The inner sum is 0 unless $\alpha + \beta q \equiv 1 \pmod{q-1}$, i.e., $\alpha + \beta = q - 1$.

Assume $0 \le \alpha \le q-1$ and $\beta = q-1-\alpha$ in (2.1). We have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+(q-1-\alpha)q} \\
&\quad = a^{(\alpha+1)(1-q)} \sum_{i,j} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq} \sum_{x\in\mathbb{F}_{q^2}^*} x^{(q-1)[-\alpha-1+3(i-j)]} \\
&\quad = -a^{(\alpha+1)(1-q)} \sum_{-\alpha-1+3(i-j)\equiv 0 \,(\mathrm{mod}\, q+1)} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq}. \qquad (2.2)
\end{aligned}$$

As i runs over the interval $[0,\alpha]$ and j over the interval $[0, q-1-\alpha]$, the range of $-\alpha-1+3(i-j)$ is

$$I_\alpha := [2\alpha+2-3q, 2\alpha-1]. \qquad (2.3)$$

Thus we have

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+(q-1-\alpha)q} = -a^{(\alpha+1)(1-q)} S_q(\alpha, a), \qquad (2.4)$$

where

$$S_q(\alpha,a) = \sum_{-\alpha-1+3(i-j)\in I_\alpha \cap (q+1)\mathbb{Z}} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq}. \qquad (2.5)$$

By Hermite's criterion, f is a PP of $\mathbb{F}_{q^2}$ if and only if 0 is the only root of f and

$$S_q(\alpha,a) = 0 \quad \text{for all } 0 \le \alpha \le q-1. \qquad (2.6)$$

Lemma 2.1. *If f is a PP of $\mathbb{F}_{q^2}$, then $q+1 \equiv 0 \pmod 3$.*

Proof. Assume f is a PP of $\mathbb{F}_{q^2}$ and assume $q \ge 3$. If $q=3$, the only multiple of $q+1$ in $I_0 = [2-3q, -1]$ is $-(q+1)$. By (2.6) (with $\alpha = 0$), we have

$$0 = \sum_{-1-3j=-(q+1)} \binom{q-1}{j} a^{-jq} = -a^{-q},$$

which is a contradiction. Now assume $q \ge 4$. The multiples of $q+1$ in $I_0 = [2-3q, -1]$ are $-2(q+1)$ and $-(q+1)$. By (2.6) (with $\alpha = 0$),

$$0 = \sum_{-1-3j=-2(q+1),-(q+1)} \binom{q-1}{j} a^{-jq} = \binom{q-1}{\frac{2q+1}{3}}^* a^{-\frac{2q+1}{3}q} + \binom{q-1}{\frac{q}{3}}^* a^{-\frac{q}{3}}, \qquad (2.7)$$

where

$$\binom{m}{n}^* = \begin{cases} \binom{m}{n} & \text{if } n \in \mathbb{N}, \\ 0 & \text{otherwise.} \end{cases}$$

If, to the contrary, $q+1 \not\equiv 0 \pmod 3$, then exactly one of $\binom{q-1}{\frac{2q+1}{3}}^*$ and $\binom{q-1}{\frac{q}{3}}^*$ is nonzero, and hence (2.7) cannot hold. □

Remark 2.2. Assume $q+1 \equiv 0 \pmod 3$.

(i) 0 is the only root of f in $\mathbb{F}_{q^2}$ if and only if $a^{\frac{q+1}{3}} \neq 1$. (Note that $(-1)^{\frac{q+1}{3}} = 1$.)
(ii) For $b \in \mathbb{F}_{q^2}^*$, we have $f(b\mathtt{x}) = b^{3q-2}(b^{3(1-q)}a\mathtt{x} + \mathtt{x}^{3q-2})$. Thus if f is a PP of $\mathbb{F}_{q^2}$ for $a = a_0$, the same is true for $a = \epsilon a_0$, where $\epsilon \in \mathbb{F}_{q^2}$, $\epsilon^{\frac{q+1}{3}} = 1$.

Lemma 2.3. *Assume $q+1 \equiv 0 \pmod 3$, $\alpha > 0$, $\alpha+1 \equiv 0 \pmod 3$, $q \geq 2\alpha+4$. Then*

$$S_q(\alpha, a) = (-a)^{\frac{\alpha+1}{3}q} \sum_{i=0}^{\alpha} (-1)^i \binom{\alpha}{i} \left[\binom{i + \frac{2\alpha-1}{3}}{\alpha} v^{3i} + \binom{i+\frac{2\alpha}{3}}{\alpha} v^{3i+1} + \binom{i+\frac{2\alpha+1}{3}}{\alpha} v^{3i+2} \right], \tag{2.8}$$

where $S_q(\alpha, a)$ is defined in (2.5) and $v = a^{-\frac{q+1}{3}q}$.

Proof. Since $\alpha > 0$ and $q \geq 2\alpha+4$, the multiples of $q+1$ in $I_\alpha = [2\alpha+2-3q, 2\alpha-1]$ are $-2(q+1), -(q+1), 0$. We have

$$\begin{aligned} &\text{LHS of (2.8)} \\ &= \sum_{-\alpha-1+3(i-j) = -2(q+1), -(q+1), 0} \binom{\alpha}{i} \binom{q-1-\alpha}{j} a^{-i-jq} \\ &= \sum_{i=0}^{\alpha} \binom{\alpha}{i} \sum_{l=0}^{2} \binom{-1-\alpha}{\frac{1}{3}(l(q+1)-\alpha-1)+i} a^{-i-[\frac{1}{3}(l(q+1)-\alpha-1)+i]q}. \end{aligned}$$

By the fact that $\binom{-m}{n} = (-1)^n \binom{n+m-1}{m-1}$ for $m, n \in \mathbb{N}$ with $m > 0$, the above sum equals

$$\begin{aligned} &\sum_{i=0}^{\alpha} \binom{\alpha}{i} \sum_{l=0}^{2} (-1)^{\frac{1}{3}(l(q+1)-\alpha-1)+i} \binom{\frac{1}{3}(l(q+1)-\alpha-1)+i+\alpha}{\alpha} a^{\frac{\alpha+1}{3}q - \frac{q+1}{3}(l+3i)q} \\ &= (-a)^{\frac{\alpha+1}{3}q} \sum_{i=0}^{\alpha} (-1)^i \binom{\alpha}{i} \sum_{l=0}^{2} \binom{i+\frac{2\alpha-1+l}{3}}{\alpha} v^{3i+l}. \qquad \square \end{aligned}$$

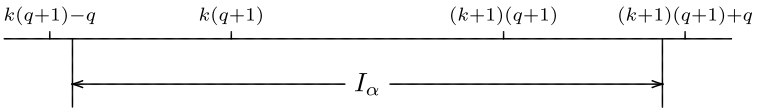


Fig. 1. Proof of (3.2).

3. Proof of Theorem 1.1

Lemma 3.1. *Assume* $q+1 \equiv 0 \pmod 3$ *and* $y := a^{\frac{q+1}{3}}$ *is a primitive* 3*rd root of unity. Then for* $1 \le s \le q^2-2$,

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = \begin{cases} a^{-\frac{1}{6}(q+1)(3q-2)}(1+y) & \text{if } q \text{ is odd and } s = \frac{q^2-1}{2}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Proof. By the observation after (2.1), we only have to consider $s = \alpha + (q-1-\alpha)q$, $0 \le \alpha \le q-1$. By (2.4), we may further assume $\alpha + 1 \equiv 0 \pmod 3$. There is nothing to prove if $q = 2$. Thus we assume $q > 3$.

1° We claim that $I_\alpha = [2\alpha+2-3q, 2\alpha-1]$ contains exactly three consecutive multiples of $q+1$ unless $\alpha = \frac{q-1}{2}$ (q odd); in the latter case, $I_\alpha = [-2q+1, q-2]$ contains exactly two multiples of $q+1$ which are $-(q+1)$ and 0.

The length of I_α is $2\alpha - 1 - (2\alpha+2-3q) = 3(q-1)$. Since $2q < 3(q-1) < 3(q+1)$, there are at least 2 and at most 3 multiples of $q+1$ in I_α. Let $k(q+1), (k+1)(q+1) \in I_\alpha$. If $I_\alpha = [2\alpha+2-3q,\ 2\alpha-1]$ contains only two multiples of $q+1$, then

$$\begin{cases} 2\alpha + 2 - 3q \ge k(q+1) - q, \\ 2\alpha - 1 \le (k+1)(q+1) + q. \end{cases} \tag{3.2}$$

(See Fig. 1.)

Since $2\alpha+2-3q,\ 2\alpha-1 \equiv 0 \pmod 3$, we have

$$\begin{cases} 2\alpha + 2 - 3q \ge k(q+1) - q + 2, \\ 2\alpha - 1 \le (k+1)(q+1) + q - 2. \end{cases} \tag{3.3}$$

Taking the difference of the two inequalities in (3.3), we conclude that

$$\begin{cases} 2\alpha + 2 - 3q = k(q+1) - q + 2, \\ 2\alpha - 1 = (k+1)(q+1) + q - 2. \end{cases}$$

Since $0 \le \alpha \le q-1$, we must have $k = -1$. Thus $\alpha = \frac{q-1}{2}$.

2° First assume $\alpha \ne \frac{q-1}{2}$. Let $I_\alpha \cap (q+1)\mathbb{Z} = (q+1)L$, where L is a set of three consecutive integers. Then we have

$$S_q(\alpha, a) = \sum_{-\alpha-1+3(i-j)\in I_\alpha\cap(q+1)\mathbb{Z}} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq}$$

$$
\begin{aligned}
&= \sum_{l\in L} \sum_{-\alpha-1+3(i-j)=l(q+1)} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i-jq} \\
&= \sum_{l\in L} \sum_{i-j=\frac{1}{3}[\alpha+1+l(q+1)]} \binom{\alpha}{i}\binom{q-1-\alpha}{j} a^{-i+j} \quad \big(\text{since } a^{q+1}=1\big) \\
&= \sum_{l\in L} a^{-\frac{1}{3}[\alpha+1+l(q+1)]} \sum_{i-j=\frac{1}{3}[\alpha+1+l(q+1)]} \binom{\alpha}{\alpha-i}\binom{q-1-\alpha}{j} \\
&= a^{-\frac{1}{3}(\alpha+1)} \sum_{l\in L} y^{-l} \sum_{\alpha-i+j=\frac{1}{3}[2\alpha-1-l(q+1)]} \binom{\alpha}{\alpha-i}\binom{q-1-\alpha}{j} \\
&= a^{-\frac{1}{3}(\alpha+1)} \sum_{l\in L} y^{-l} \binom{q-1}{\frac{1}{3}[2\alpha-1-l(q+1)]} \\
&= -a^{-\frac{1}{3}(\alpha+1)} \sum_{l\in L} y^{-l} \\
&= 0. \qquad (3.4)
\end{aligned}
$$

In the next-to-last step, we have $\binom{q-1}{\frac{1}{3}[2\alpha-1-l(q+1)]} = (-1)^{\frac{1}{3}[2\alpha-1-l(q+1)]} = -1$ since $0 \le \frac{1}{3}[2\alpha-1-l(q+1)] \le \frac{1}{3}[2\alpha-1-(2\alpha+2-3q)] = q-1$. Combining (2.4) and (3.4) gives $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = 0$.

3° Now assume $\alpha = \frac{q-1}{2}$. By the calculation in (3.4), we have

$$S_q(\alpha, a) = -a^{-\frac{1}{3}(\alpha+1)} \sum_{l=-1,0} y^{-l} = -a^{-\frac{1}{6}(q+1)}(1+y). \qquad (3.5)$$

Combining (2.4) and (3.5) gives

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = a^{\frac{q+1}{2}(1-q)-\frac{q+1}{6}}(1+y) = a^{-\frac{1}{6}(q+1)(3q-2)}(1+y). \qquad \square$$

Proof of Theorem 1.1. ($\Leftarrow$) (ii)–(vii) are sporadic cases with small q. Using a computer, it is easy to verify that f is a PP in each of these cases. Now assume (i). By Lemma 3.1, we have $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = 0$ for all $1 \le s \le q^2-2$. Also note from Remark 2.2(i) that 0 is the only root of f in $\mathbb{F}_{q^2}$. Thus f is a PP of $\mathbb{F}_{q^2}$.

($\Rightarrow$) Assume that f is a PP of $\mathbb{F}_{q^2}$. By Lemma 2.1, we have $q+1 \equiv 0 \pmod 3$. Let $y = a^{\frac{q+1}{3}q}$. If y is a primitive 3rd root of unity, by Lemma 3.1, q must be even, i.e., $q = 2^{2k+1}$, and we have case (i). Now assume that $y^2+y+1 \neq 0$. We show that one of the cases (ii)–(vii) occurs.

The sum in the right side of (2.8) is a polynomial in y^{-1} $(= v)$ which can be easily computed for small α with computer assistance. For $\alpha = 2, 5, 8, 11, 14$, we find that

$$S_q(\alpha,a)=(-a)^{\frac{\alpha+1}{3}q}y^{-3\alpha-2}\big(y^2+y+1\big)\begin{cases}3^{-2}g_2(y) & \text{if } \alpha=2,\ q\geq 8,\\ 3^{-6}g_5(y) & \text{if } \alpha=5,\ q\geq 14,\\ 3^{-10}g_8(y) & \text{if } \alpha=8,\ q\geq 20,\\ 3^{-15}g_{11}(y) & \text{if } \alpha=11,\ q\geq 26,\\ 3^{-19}g_{14}(y) & \text{if } \alpha=14,\ q\geq 32,\end{cases} \tag{3.6}$$

where

$$\begin{aligned}
g_2(\mathtt{x}) &= 2\mathtt{x}^5+3\mathtt{x}^4-23\mathtt{x}^3-8\mathtt{x}^2-9\mathtt{x}+44,\\
g_5(\mathtt{x}) &= -14\mathtt{x}^{14}-8\mathtt{x}^{13}+22\mathtt{x}^{12}-469\mathtt{x}^{11}-1093\mathtt{x}^{10}+8852\mathtt{x}^9+6801\mathtt{x}^8+10\,527\mathtt{x}^7\\
&\quad -61\,068\mathtt{x}^6-18\,619\mathtt{x}^5-25\,033\mathtt{x}^4+120\,197\mathtt{x}^3+13\,516\mathtt{x}^2+16\,822\mathtt{x}-71\,162,\\
g_8(\mathtt{x}) &= 130\mathtt{x}^{23}+57\mathtt{x}^{22}-187\mathtt{x}^{21}+4082\mathtt{x}^{20}+3585\mathtt{x}^{19}-7667\mathtt{x}^{18}+156\,234\mathtt{x}^{17}\\
&\quad +453\,573\mathtt{x}^{16}-3\,916\,551\mathtt{x}^{15}-4\,144\,622\mathtt{x}^{14}-7\,594\,467\mathtt{x}^{13}+48\,939\,959\mathtt{x}^{12}\\
&\quad +25\,221\,008\mathtt{x}^{11}+39\,342\,423\mathtt{x}^{10}-213\,366\,911\mathtt{x}^9-61\,811\,112\mathtt{x}^8-88\,032\,825\mathtt{x}^7\\
&\quad +422\,650\,317\mathtt{x}^6+66\,303\,028\mathtt{x}^5+88\,882\,095\mathtt{x}^4-389\,019\,163\mathtt{x}^3-25\,886\,212\mathtt{x}^2\\
&\quad -33\,211\,905\mathtt{x}+135\,094\,180,\\
g_{11}(\mathtt{x}) &= -3952\mathtt{x}^{32}-1522\mathtt{x}^{31}+5474\mathtt{x}^{30}-139\,802\mathtt{x}^{29}-89\,324\mathtt{x}^{28}+229\,126\mathtt{x}^{27}\\
&\quad -3\,943\,602\mathtt{x}^{26}-4\,392\,909\mathtt{x}^{25}+8\,336\,511\mathtt{x}^{24}-180\,820\,302\mathtt{x}^{23}-605\,825\,169\mathtt{x}^{22}\\
&\quad +5\,521\,784\,781\mathtt{x}^{21}+7\,111\,655\,988\mathtt{x}^{20}+14\,607\,372\,831\mathtt{x}^{19}-101\,269\,369\,227\mathtt{x}^{18}\\
&\quad -69\,095\,625\,624\mathtt{x}^{17}-119\,477\,261\,853\mathtt{x}^{16}+705\,650\,100\,129\mathtt{x}^{15}\\
&\quad +303\,870\,716\,124\mathtt{x}^{14}+475\,920\,749\,355\mathtt{x}^{13}-2\,503\,382\,174\,319\mathtt{x}^{12}\\
&\quad -706\,243\,777\,836\mathtt{x}^{11}-1\,034\,492\,806\,725\mathtt{x}^{10}+4\,972\,469\,163\,636\mathtt{x}^9\\
&\quad +898\,579\,001\,889\mathtt{x}^8+1\,253\,008\,322\,595\mathtt{x}^7-5\,598\,768\,742\,164\mathtt{x}^6\\
&\quad -591\,556\,509\,206\mathtt{x}^5-794\,043\,854\,630\mathtt{x}^4+3\,339\,003\,167\,188\mathtt{x}^3\\
&\quad +157\,572\,058\,982\mathtt{x}^2+205\,140\,400\,010\mathtt{x}-819\,352\,075\,360,\\
g_{14}(\mathtt{x}) &= 41800\mathtt{x}^{41}+14\,895\mathtt{x}^{40}-56\,695\mathtt{x}^{39}+1\,691\,000\mathtt{x}^{38}+905\,631\mathtt{x}^{37}-2\,596\,631\mathtt{x}^{36}\\
&\quad +47\,250\,150\mathtt{x}^{35}+37\,894\,401\mathtt{x}^{34}-85\,144\,551\mathtt{x}^{33}+1\,395\,800\,990\mathtt{x}^{32}\\
&\quad +1\,826\,164\,521\mathtt{x}^{31}-3\,221\,965\,511\mathtt{x}^{30}+75\,566\,097\,190\mathtt{x}^{29}+281\,332\,431\,561\mathtt{x}^{28}\\
&\quad -2\,683\,745\,985\,685\mathtt{x}^{27}-3\,976\,231\,919\,076\mathtt{x}^{26}-8\,901\,790\,877\,799\mathtt{x}^{25}\\
&\quad +65\,232\,090\,577\,890\mathtt{x}^{24}+53\,701\,334\,712\,609\mathtt{x}^{23}+100\,487\,514\,543\,597\mathtt{x}^{22}\\
&\quad -632\,854\,611\,825\,486\mathtt{x}^{21}-347\,885\,978\,019\,711\mathtt{x}^{20}-586\,551\,837\,541\,203\mathtt{x}^{19}\\
&\quad +3\,307\,822\,221\,633\,594\mathtt{x}^{18}+1\,283\,881\,108\,529\,889\mathtt{x}^{17}+2\,015\,859\,062\,567\,817\mathtt{x}^{16}\\
&\quad -10\,419\,893\,389\,315\,746\mathtt{x}^{15}-2\,892\,546\,806\,289\,271\mathtt{x}^{14}\\
&\quad -4\,307\,726\,185\,011\,783\mathtt{x}^{13}+20\,728\,564\,105\,915\,330\mathtt{x}^{12}+4\,054\,215\,382\,726\,378\mathtt{x}^{11}
\end{aligned}$$

$$+ 5\,793\,391\,583\,605\,092\mathtt{x}^{10} - 26\,245\,535\,590\,106\,350\mathtt{x}^9 - 3\,451\,745\,974\,770\,042\mathtt{x}^8$$
$$- 4\,770\,402\,189\,292\,728\mathtt{x}^7 + 20\,520\,594\,631\,893\,930\mathtt{x}^6 + 1\,634\,454\,816\,505\,198\mathtt{x}^5$$
$$+ 2\,197\,118\,421\,394\,272\mathtt{x}^4 - 9\,034\,762\,128\,135\,730\mathtt{x}^3 - 330\,180\,086\,243\,950\mathtt{x}^2$$
$$- 433\,563\,200\,685\,120\mathtt{x} + 1\,713\,531\,735\,146\,800.$$

Combining (2.6) and (3.6), we have

$$\begin{cases} g_2(y) = 0 & \text{if } q \geq 8, \\ g_5(y) = 0 & \text{if } q \geq 14, \\ g_8(y) = 0 & \text{if } q \geq 20, \\ g_{11}(y) = 0 & \text{if } q \geq 26, \\ g_{14}(y) = 0 & \text{if } q \geq 32. \end{cases} \tag{3.7}$$

When $q < 14$, a quick computer search produces cases (ii)–(iv). So we assume $q \geq 14$. Next we compute the resultant of g_2 and g_5:

$$R(g_2, g_5) = 2^5 \cdot 3^{35} \cdot 17^2 \cdot 23 \cdot 29 \cdot 103 \cdot 16\,069.$$

By (3.7) and the fact that $q+1 \equiv 0 \pmod 3$, we must have $p = \operatorname{char} \mathbb{F}_q \in \{2, 17, 23, 29\}$.

When $p = 2$, we have $q \geq 32$. In this case, $\gcd(g_2, g_5, g_8) = \mathtt{x}$, which is a contradiction to (3.7).

When $p = 17$, we find that $\gcd(g_2, g_5, g_8) = 1$. By (3.7), we must have $q = 17$. A computer search results in case (v).

When $p = 23$, $\gcd(g_2, g_5, g_8) = \mathtt{x} + 1$, and $g_{11}(-1) = 12 \neq 0$. By (3.7), we must have $q = 23$. A computer search results in case (vi).

When $p = 29$, $\gcd(g_2, g_5, g_8) = \mathtt{x} + 10$, and $g_{11}(-10) = 0$, $g_{14}(-10) = 2 \neq 0$. By (3.7), we must have $q = 29$. A computer search results in case (vii). □

References

[1] A. Akbary, Q. Wang, A generalized Lucas sequence and permutation binomials, Proc. Amer. Math. Soc. 134 (2006) 15–22.
[2] L. Carlitz, Some theorems on permutation polynomials, Bull. Amer. Math. Soc. (N.S.) 68 (1962) 120–122.
[3] L. Carlitz, C. Wells, The number of solutions of a special system of equations in a finite field, Acta Arith. 12 (1966/1967) 77–84.
[4] X. Hou, A class of permutation binomials over finite fields, J. Number Theory 133 (2013) 3549–3558.
[5] X. Hou, Determination of a type of permutation trinomials over finite fields, II, arXiv:1404.1822, 2014.
[6] X. Hou, A survey of permutation binomials and trinomials over finite fields, in: Proceedings of the 11th International Conference on Finite Fields and Their Applications, in press.
[7] S.Y. Kim, J.B. Lee, Permutation polynomials of the type $x^{1+((q-1)/m)} + ax$, Commun. Korean Math. Soc. 10 (1995) 823–829.
[8] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
[9] A.M. Masuda, M.E. Zieve, Permutation binomials over finite fields, Trans. Amer. Math. Soc. 361 (2009) 4169–4180.

[10] H. Niederreiter, K.H. Robinson, Complete mappings of finite fields, J. Austral. Math. Soc. Ser. A 33 (1982) 197–212.
[11] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer-Verlag, Berlin, 1993.
[12] Z. Tu, X. Zeng, L. Hu, C. Li, A class of binomial permutation polynomials, arXiv:1310.0337, 2013.
[13] G. Turnwald, Permutation Polynomials of Binomial Type, Contrib. Gen. Algebra, vol. 6, Hölder–Pichler–Tempsky, Vienna, 1988, pp. 281–286.
[14] D. Wan, Permutation polynomials over finite fields, Acta Math. Sin. (N.S.) 3 (1987) 1–5.
[15] D. Wan, Permutation binomials over finite fields, Acta Math. Sin. (N.S.) 10 (1994) 30–35, Special Issue.
[16] Q. Wang, Cyclotomic mapping permutation polynomials over finite fields, in: S.W. Golomb, G. Gong, T. Helleseth, H.-Y. Song (Eds.), Sequences, Subsequences, and Consequences, in: Lecture Notes in Comput. Sci., vol. 4893, Springer, Berlin, 2007, pp. 119–128.
[17] A. Weil, On the Riemann hypothesis in function fields, Proc. Natl. Acad. Sci. USA 27 (1941) 345–347.
[18] M.E. Zieve, On some permutation polynomials over $\mathbb{F}_q$ of the form $x^r h(x^{(q-1)/d})$, Proc. Amer. Math. Soc. 137 (2009) 2209–2216.
[19] M.E. Zieve, Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$, arXiv:1310.0776, 2013.