ACTA ARITHMETICA
166.3 (2014)

Determination of a type of permutation trinomials over finite fields

by

Xiang-dong Hou (Tampa, FL)

1. Introduction. Let $\mathbb{F}_q$ denote the finite field with q elements. A polynomial $f \in \mathbb{F}_q[\mathtt{x}]$ is called a *permutation polynomial* (PP) of $\mathbb{F}_q$ if the mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. Permutation polynomials over finite fields are studied for both theoretic [E, Hi1, Hi2, LN, NR] and practical [GM, L, LB, LC] reasons. PPs with few terms (excluding monomials) are particularly sought after [AW, LP, MPW, MZ, T, W1, W2, Z]

In the present paper we consider trinomials of the form $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$. Since $f \equiv (a+b+1)\mathtt{x} \pmod{\mathtt{x}^q - \mathtt{x}}$, f is a PP of $\mathbb{F}_q$ if and only if $a+b+1 \neq 0$. The question that we are interested in is when f is a PP of $\mathbb{F}_{q^2}$. This question will be completely answered in Theorem A (for odd q) and Theorem B (for even q). Partial solutions to the question appeared in two recent papers: PPs of $\mathbb{F}_{q^2}$ the form $t\mathtt{x} + \mathtt{x}^{2q-1}$ ($t \in \mathbb{F}_q^*$) and of the form $-\mathtt{x} + t\mathtt{x}^q + \mathtt{x}^{2q-1}$ ($t \in \mathbb{F}_q^*$) were determined in [Ho3] and [Ho4], respectively. For the proofs of Theorems A and B, we draw on the methods of [Ho3] and [Ho4], especially, the approach of [Ho4]. However, the proofs in the present paper are much more than a routine adaptation of the ones in [Ho3, Ho4]. We find a new method for proving the uniqueness of a solution $x \in \mathbb{F}_{q^2}$ of the equation $ax + bx^q + x^{2q-1} = y$, where $y \in \mathbb{F}_{q^2}$. A common theme throughout the proofs of Theorems A and B is that complicated computations that appear to be heading nowhere can produce surprisingly nice results. For example, a seemingly out-of-control polynomial of degree 4 not only factors but factors exactly the way we desire (see (3.13)).

Theorem A provides a solution to a related problem. For each integer $n \geq 0$, let $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ ($p = \operatorname{char} \mathbb{F}_q$) be the polynomial defined by the functional equation

$$\sum_{c \in \mathbb{F}_q} (\mathtt{x} + c)^n = g_{n,q}(\mathtt{x}^q - \mathtt{x}).$$

2010 *Mathematics Subject Classification*: Primary 11T06; Secondary 11T55.
Key words and phrases: discriminant, finite field, permutation polynomial.

DOI: 10.4064/aa166-3-3

The permutation property of the polynomial $g_{n,q}$ was the focus of several recent papers [FHL, Ho1, Ho2]. These studies have led to the discovery of many new interesting PPs including the ones in [Ho3, Ho4] and in the present paper. The ultimate goal concerning $g_{n,q}$ is to determine all triples of integers $(n, e; q)$ for which $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$; we call such triples *desirable.* While this goal may be out of reach for the time being, significant progress has been made. It was observed through computer search that many desirable triples appear in the form $(q^\alpha - q^\beta - 1, 2; q)$, where $\alpha > \beta \ge 0$. However, the chaotic values of those α and β were quite bewildering; see [FHL, Section 5 and Table 1]. In the present paper, we are able to determine all desirable triples of this form; the results are stated in Theorems C (for even q) and D (for odd q). Theorem C is an immediate consequence of some existing results. For Theorem D, we note that when $n = q^\alpha - q^\beta - 1$, the polynomial $g_{n,q}$, modulo $\mathtt{x}^{q^2} - \mathtt{x}$, can be transformed through an invertible change of variable into the form $A\mathtt{x} + B\mathtt{x}^q + C\mathtt{x}^{2q-1}$. Hence Theorem D follows from Theorem A.

2. Statements of Theorems A and B. The main results of the paper are the following theorems.

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

(i) *$a(a-1)$ is a square in $\mathbb{F}_q^*$, and $b^2 = a^2 + 3a$.*
(ii) *$a = 1$, and $b^2 - 4$ is a square in $\mathbb{F}_q^*$.*
(iii) *$a = 3$, $b = 0$, $q \equiv -1 \pmod 6$.*
(iv) *$a = b = 0$, $q \equiv 1, 3 \pmod 6$.*

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

(i) *$q > 2$, $a \ne 1$, $\mathrm{Tr}_{q/2}\big(\frac{1}{a+1}\big) = 0$, $b^2 = a^2 + a$.*
(ii) *$q > 2$, $a = 1$, $b \ne 0$, $\mathrm{Tr}_{q/2}\big(\frac{1}{b}\big) = 0$.*

In Theorem B(i), we can write $\frac{1}{a+1} = d^2 + d^4$, where $d \in \mathbb{F}_q \setminus \mathbb{F}_2$. Then $(a, b, 1) = \frac{1}{d^2+d^4}(1 + d^2 + d^4, 1 + d + d^2, d^2 + d^4)$. Similarly, in Theorem B(ii), we can write $\frac{1}{b} = d + d^2$, $d \in \mathbb{F}_q \setminus \mathbb{F}_2$. Then $(a, b, 1) = \frac{1}{d+d^2}(d + d^2, 1, d + d^2)$. Let $\mathrm{PG}(2, \mathbb{F}_q)$ denote the projective plane over $\mathbb{F}_q$ and define

$$\mathcal{X} = \{[a : b : c] \in \mathrm{PG}(2, \mathbb{F}_q) : a\mathtt{x} + b\mathtt{x}^q + c\mathtt{x}^{2q-1} \text{ is a PP of } \mathbb{F}_{q^2}\}.$$

Then for even q we have

$$\begin{aligned} \mathcal{X} = {} & \{[1 + d^2 + d^4 : 1 + d + d^2 : d^2 + d^4] : d \in \mathbb{F}_q \setminus \mathbb{F}_2\} \\ & \cup \{[d + d^2 : 1 : d + d^2] : d \in \mathbb{F}_q \setminus \mathbb{F}_2\} \\ & \cup \{[d : 1 : 0] : d \in \mathbb{F}_q \setminus \{1\}\} \cup \{[1 : 0 : 0]\}. \end{aligned}$$

3. Proof of Theorem A

3.1. The case $a(a-1)b=0$

CASE 1. Assume $a=b=0$. Then $f=\mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(2q-1,q^2-1)=1$, i.e., $q\equiv 1,3 \pmod 6$.

CASE 2. Assume $a\neq 0$, $b=0$. By [Ho3, Theorem 1.1], $f=a\mathtt{x}+\mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$ if and only if one of the following occurs:

(a) $a=1$, $q\equiv 1 \pmod 4$;
(b) $a=-3$, $q\equiv \pm 1 \pmod{12}$;
(c) $a=3$, $q\equiv -1 \pmod 6$.

Condition (c) is (iii) in Theorem A; condition (a) is equivalent to (ii) in Theorem A with $b=0$. Note that 3 is square in $\mathbb{F}_q^*$ if and only if $q\equiv\pm 1$ (mod 12) [IR, §5.2]. Hence condition (b) is equivalent to (i) in Theorem A with $b=0$.

CASE 3. Assume $a=0$, $b\neq 0$. For integers $\alpha,\beta\geq 0$ with $\alpha+\beta=q-1$, it follows from (3.17) below that

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+\beta q}=-\sum_{\substack{k,l\\ \alpha+1+k-l=0,\,q+1}}\binom{\alpha}{k}\binom{\beta}{l}b^{-(k+l)}.$$

Setting $\alpha=q-1$ and $\beta=0$, we have

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{q-1}=-\binom{q-1}{1}b^{-1}=b^{-1}\neq 0.$$

By Hermite's criterion [LN, Lemma 7.3], f cannot be a PP of $\mathbb{F}_{q^2}$ in this case.

CASE 4. Assume $a=1$. We show that $f=\mathtt{x}+b\mathtt{x}^q+\mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $f_1=\mathtt{x}^2+b\mathtt{x}+1$ has two distinct roots in $\mathbb{F}_q$.

($\Leftarrow$) Let $x,y\in\mathbb{F}_{q^2}$ be such that $f(x)=y$. We show that x is uniquely determined by y.

First assume $y\neq 0$. Let $t=xy=x^2+x^{2q}+bx^{q+1}\in\mathbb{F}_q$. Then

$$\frac{t}{y}+b\Big(\frac{t}{y}\Big)^q+\Big(\frac{t}{y}\Big)^{2q-1}=y,\quad \text{i.e.,}\quad t\Big(\frac{1}{y}+\frac{b}{y^q}+\frac{1}{y^{2q-1}}\Big)=y.$$

Hence t is unique. It follows that x is unique.

Next assume $y=0$. We claim that $x=0$. Assume to the contrary that $x\neq 0$. Then we have

$$1+bx^{q-1}+x^{2(q-1)}=0, \tag{3.1}$$

i.e., $f_1(x^{q-1})=0$. Thus $x^{q-1}\in\mathbb{F}_q$. Therefore $x^{2(1-q)}=x^{(q-1)^2}=1$, and hence $x^{q-1}=\pm 1$. It follows from (3.1) that $b=\pm 2$. Thus $f_1=(\mathtt{x}\pm 1)^2$, which is a contradiction.

($\Rightarrow$) Assume to the contrary that f_1 does not have two distinct roots in $\mathbb{F}_q$.

If f_1 is irreducible over $\mathbb{F}_q$, let $y \in \mathbb{F}_{q^2}$ be a root of f_1. Since $y^{1+q} = \mathrm{N}_{q^2/q}(y) = 1$, there exists an $x \in \mathbb{F}_{q^2}^*$ such that $y = x^{q-1}$. Then $f(x) = xf_1(y) = 0 = f(0)$, which is a contradiction.

If f_1 is not irreducible over $\mathbb{F}_q$, then $f_1 = (\mathtt{x} - \epsilon)^2$, where $\epsilon = 1$ or -1. Since $\epsilon^{1+q} = 1$, again there exists $x \in \mathbb{F}_{q^2}^*$ such that $\epsilon = x^{q-1}$. Then $f(x) = xf_1(\epsilon) = 0 = f(0)$, which is a contradiction.

This completes the proof of Theorem A for $a(a-1)b = 0$. In the next two subsections, we assume that $a(a-1)b \neq 0$ and we prove that f is a PP of $\mathbb{F}_{q^2}$ if and only if $a(a-1)$ is a square in $\mathbb{F}_q^*$ and $b^2 = a^2 + 3a$.

3.2. The case $a(a-1)b \neq 0$, sufficiency. Assume that $a(a-1)$ is a square in $\mathbb{F}_q^*$ and $b^2 = a^2 + 3a$.

1° We claim that $f(\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \subset \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

Assume to the contrary that there exists an $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ such that $f(x)^q = f(x)$. Then

$$ax^q + bx + x^{2-q} = ax + bx^q + x^{2q-1},$$

i.e.,

$$(a-b)(x^q - x) + \frac{x^3 - x^{3q}}{x^{1+q}} = 0.$$

Since $x^q - x \neq 0$, we have

$$a - b - \frac{x^2 + x^{1+q} + x^{2q}}{x^{1+q}} = 0,$$

i.e.,

$$x^{2(q-1)} - (a-b-1)x^{q-1} + 1 = 0. \tag{3.2}$$

Using the relation $b^2 = a^2 + 3a$, we find that

$$(a-b-1)^2 - 4 = \frac{a-1}{a}(a-b)^2,$$

which is a square in $\mathbb{F}_q^*$. So $\mathtt{x}^2 - (a-b-1)\mathtt{x} + 1$ is reducible over $\mathbb{F}_q$. Thus by (3.2), we have $x^{q-1} \in \mathbb{F}_q$. Then $1 = x^{(q-1)^2} = x^{q^2-2q+1} = x^{2(1-q)}$. Since $x \notin \mathbb{F}_q$, we must have $x^{1-q} = -1$. Then (3.2) becomes $a-b+1 = 0$. However,

$$(a+b+1)(a-b+1) = (a+1)^2 - b^2 = (a+1)^2 - (a^2+3a) = 1 - a \neq 0, \tag{3.3}$$

which is a contradiction.

2° Let $x, y \in \mathbb{F}_{q^2}$ be such that $f(x) = y$. We show that x is uniquely determined by y.

If $y \in \mathbb{F}_q$, by 1°, we have $x \in \mathbb{F}_q$, so $f(x) = (a+b+1)x$. By (3.3), $a+b+1 \neq 0$, so we must have $x = y/(a+b+1)$.

Therefore, we assume $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. It follows that $x \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$.

3° We write $\mathrm{T} = \mathrm{Tr}_{q^2/q}$ and $\mathrm{N} = \mathrm{N}_{q^2/q}$. It suffices to show that $\mathrm{T}(x)$ and $\mathrm{N}(x)$ are uniquely determined by y. (If $x_1 \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is such that $f(x_1) = y$ and $\mathrm{T}(x_1) = \mathrm{T}(x)$, $\mathrm{N}(x_1) = \mathrm{N}(x)$, then $x_1 = x$ or x^q. Since $f(x^q) = f(x)^q = y^q \neq y$, we must have $x_1 = x$.)

We observe that

$$\mathrm{T}(f(x)) = \mathrm{T}(y), \qquad \mathrm{N}(f(x)) = \mathrm{N}(y), \tag{3.4}$$

where

$$\mathrm{T}(f(x)) = (a+b)\mathrm{T}(x) + \mathrm{T}(x^{2q-1}), \tag{3.5}$$

$$\begin{aligned}\mathrm{N}(f(x)) &= (ax + bx^q + x^{2q-1})(ax^q + bx + x^{2-q}) \\ &= (a^2+b^2+1)\mathrm{N}(x) + (ab+b)\mathrm{T}(x^2) + a\mathrm{T}(x^{3-q}).\end{aligned} \tag{3.6}$$

We wish to express $\mathrm{T}(f(x))$ and $\mathrm{N}(f(x))$ in terms of $\mathrm{T}(x)$ and $\mathrm{N}(x)$. For this purpose, we need a few formulas: For $z \in \mathbb{F}_{q^2}^*$, we have

$$\begin{aligned}\mathrm{T}(z^2) &= \mathrm{T}(z)^2 - 2\mathrm{N}(z), \\ \mathrm{T}(z^3) &= \mathrm{T}(z)^3 - 2\mathrm{N}(z)\mathrm{T}(z),\end{aligned} \tag{3.7}$$

$$\mathrm{T}(z^{2q-1}) = \mathrm{T}(z^{3q} \cdot z^{-(1+q)}) = \frac{\mathrm{T}(z^3)}{\mathrm{N}(z)} = \frac{\mathrm{T}(z)^3}{\mathrm{N}(z)} - 3\mathrm{T}(z), \tag{3.8}$$

$$\begin{aligned}\mathrm{T}(z^{3-q}) &= \mathrm{T}(z^4 \cdot z^{-(1+q)}) = \frac{\mathrm{T}(z^4)}{\mathrm{N}(z)} = \frac{1}{\mathrm{N}(z)}[\mathrm{T}(z^2)^2 - 2\mathrm{N}(z^2)] \\ &= \frac{1}{\mathrm{N}(z)}[(\mathrm{T}(z)^2 - 2\mathrm{N}(z))^2 - 2\mathrm{N}(z^2)] \\ &= \frac{\mathrm{T}(z)^4}{\mathrm{N}(z)} - 4\mathrm{T}(z)^2 + 2\mathrm{N}(z).\end{aligned} \tag{3.9}$$

Put $t = \mathrm{T}(x)$, $n = \mathrm{N}(x)$, $\tau = \mathrm{T}(y)$, $\eta = \mathrm{N}(y)$. By (3.5)–(3.9), we have

$$\begin{aligned}\mathrm{T}(f(x)) &= (a+b)t + \frac{t^3}{n} - 3t = \frac{t^3}{n} + (a+b-3)t, \\ \mathrm{N}(f(x)) &= (a^2+b^2+1)n + (ab+b)(t^2-2n) + a\Big(\frac{t^4}{n} - 4t^2 + 2n\Big) \\ &= a\frac{t^4}{n} + (ab-4a+b)t^2 + (a-b+1)^2 n.\end{aligned}$$

Then (3.4) becomes

$$\begin{cases} \dfrac{t^3}{n} + (a+b-3)t = \tau, \\[2ex] a\dfrac{t^4}{n} + (ab-4a+b)t^2 + (a-b+1)^2 n = \eta. \end{cases} \tag{3.10}$$

We proceed to show that (3.10) has at most one solution $(t, n) \in \mathbb{F}_q \times \mathbb{F}_q$.

First assume $\tau = 0$. Since $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, q must be odd. We claim that $t = 0$. If, on the contrary, $t \neq 0$, then by the first equation of (3.10), we have $t^2/n = -(a+b-3)$. Using the relation $b^2 = a^2 + 3a$, we find that

$$\frac{t^2}{n}\left(\frac{t^2}{n} - 4\right) = (a+b+1)(a+b-3) = \frac{a-1}{a}(a+b)^2,$$

which is a square in $\mathbb{F}_q$. Then $x \in \mathbb{F}_q$, which is a contradiction. So the claim is proved. By the second equation of (3.10), we have $n = \eta/(a-b+1)^2$. Hence (t, n) is unique.

Now assume $\tau \neq 0$. It follows that $t \neq 0$. Put $s = t^2/n$ and $\sigma = \tau^2/\eta$, and write (3.10) as

$$\begin{cases} t(s+a+b-3) = \tau, \\ t^2\left(as + (ab-4a+b) + (a-b+1)^2\,\dfrac{1}{s}\right) = \dfrac{\tau^2}{\sigma}. \end{cases} \tag{3.11}$$

Eliminating t and τ in (3.11), we have

$$\frac{as + (ab-4a+b) + (a-b+1)^2\frac{1}{s}}{(s+a+b-3)^2} = \frac{1}{\sigma},$$

i.e.,

$$\begin{split} s^3 + (-a\sigma + 2a + 2b - 6)s^2 \\ + [(4a-b-ab)\sigma + (a+b-3)^2]s - (a-b+1)^2\sigma = 0. \end{split} \tag{3.12}$$

It suffices to show that (3.12) has at most one solution $s \in \mathbb{F}_q$.

Let $g(\mathtt{s}) \in \mathbb{F}_q[\mathtt{s}]$ denote the polynomial given by the left side of (3.12). We find that the discriminant of g is given by

$$D(g) = (a-1)^2\sigma(\sigma-4)h(\sigma), \tag{3.13}$$

where

$$\begin{split} h(\sigma) = a^2(b^2-4a)\sigma^2 - 2(ab(a+b)^2 - 8a^3 - 6a^2b - 2b^3 + 9ab)\sigma \\ + (a+b+1)(a+b-3). \end{split} \tag{3.14}$$

Here we emphasize that (3.13) and (3.14) hold with a and b treated as independent parameters. Using the relation $b^2 = a^2 + 3a$, we find that

$$h(\sigma) = a^3(a-1)\left(\sigma - \frac{2a^2 + 2ab - 3b}{a^2}\right)^2. \tag{3.15}$$

(Note: Equations (3.13) and (3.15), especially (3.13), are painful to compute by hand, but they are easily obtained using a symbolic computation program.) By (3.13) and (3.15),

$$D(g) = a^3(a-1)^3\sigma(\sigma-4)\left(\sigma - \frac{2a^2 + 2ab - 3b}{a^2}\right)^2. \tag{3.16}$$

In (3.16), $\sigma(\sigma-4)$ is a nonsquare in $\mathbb{F}_q^*$ because $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. If $\sigma \neq (2a^2+2ab-3b)/a^2$, then $D(g)$ is a nonsquare in $\mathbb{F}_q^*$. Therefore g has at most one root in $\mathbb{F}_q$, and we are done.

4° Now assume $\sigma = (2a^2+2ab-3b)/a^2$. We have

$$\begin{aligned}\sigma(\sigma-4) &= \left(2+\frac{b(2a-3)}{a^2}\right)\left(-2+\frac{b(2a-3)}{a^2}\right) = \frac{b^2(2a-3)^2}{a^4}-4\\ &= \frac{a(a+3)(2a-3)^2}{a^4}-4 = -\frac{27(a-1)}{a^3}.\end{aligned}$$

Since $\sigma(\sigma-4) \neq 0$ (a nonsquare in $\mathbb{F}_q^*$), we have $3 \nmid q$. Using the relations $\sigma = (2a^2+2ab-3b)/a^2$ and $b^2 = a^2+3a$, we find that

$$g(\mathtt{s}) = \mathtt{s}^3 + \frac{3(-2a+b)}{a}\mathtt{s}^2 + \frac{3(5a-4b+3)}{a}\mathtt{s} + \frac{-14a^2+13ab-18a+3b}{a^2}.$$

Then

$$g' = 3\mathtt{s}^2 + \frac{6(-2a+b)}{a}\mathtt{s} + \frac{3(5a-4b+3)}{a}.$$

The discriminant of g' is given by

$$D(g') = \left[\frac{2(-2a+b)}{a}\right]^2 - 4\frac{5a-4b+3}{a}.$$

Using the relation $b^2 = a^2+3a$, we find that

$$D(g') = 0.$$

Thus

$$g' = 3\left(\mathtt{s}+\frac{-2a+b}{a}\right)^2.$$

Since $D(g) = 0$, $\gcd(g, g') \neq 1$. Thus we must have

$$g = \left(\mathtt{s}+\frac{-2a+b}{a}\right)^3.$$

In particular, g has a unique root in $\mathbb{F}_q$. This completes the proof of the sufficiency part of Theorem A under the assumption $a(a-1)b \neq 0$.

3.3. The case $a(a-1)b \neq 0$, necessity. Recall that $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$. Let $0 \le s < q^2-1$ and write $s = \alpha+\beta q$, where $0 \le \alpha, \beta \le q-1$.

One has

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^2}} f(x)^s &= \sum_{x\in\mathbb{F}_{q^2}^*} (ax+bx^q+x^{2q-1})^{\alpha+\beta q}\\ &= \sum_{x\in\mathbb{F}_{q^2}^*} (ax+bx^q+x^{2q-1})^{\alpha}(ax^q+bx+x^{2-q})^{\beta}\\ &= \sum_{x\in\mathbb{F}_{q^2}^*}\sum_{i,j,k,l}\binom{\alpha}{i}\binom{i}{k}(ax)^{\alpha-i}(bx^q)^{i-k}(x^{2q-1})^k\binom{\beta}{j}\binom{j}{l}(ax^q)^{\beta-j}(bx)^{j-l}(x^{2-q})^l\\ &= \sum_{x\in\mathbb{F}_{q^2}^*}\sum_{i,j,k,l}\binom{\alpha}{i}\binom{i}{k}\binom{\beta}{j}\binom{j}{l}a^{\alpha+\beta-i-j}b^{i+j-k-l}x^{\alpha+\beta q+(q-1)(i+k-j-l)}.\end{aligned}$$

If $\alpha+\beta q\not\equiv 0 \pmod{q-1}$, then clearly $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s=0$. Assume $\alpha+\beta q\equiv 0 \pmod{q-1}$. Then one must have $\alpha+\beta=q-1$, and the above calculation becomes

$$\begin{aligned}&\sum_{x\in\mathbb{F}_{q^2}} f(x)^s\\ &\qquad= \sum_{x\in\mathbb{F}_{q^2}^*}\sum_{i,j,k,l}\binom{\alpha}{i}\binom{i}{k}\binom{\beta}{j}\binom{j}{l}a^{q-1-i-j}b^{i+j-k-l}x^{(q-1)(q-\alpha+i+k-j-l)}\\ &\qquad= -\sum_{\substack{i,j,k,l\\ q-\alpha+i+k-j-l\equiv 0 \,(\mathrm{mod}\, q+1)}}\binom{\alpha}{i}\binom{i}{k}\binom{\beta}{j}\binom{j}{l}a^{q-1-i-j}b^{i+j-k-l}.\end{aligned}$$

For $0\le k\le i\le\alpha$ and $0\le l\le j\le\beta$, one has

$$-(q+1)<q-\alpha+i+k-j-l<2(q+1).$$

Hence

$$\begin{aligned}(3.17)\qquad &\sum_{x\in\mathbb{F}_{q^2}} f(x)^s\\ &\qquad= -\sum_{q-\alpha+i+k-j-l=0,\,q+1}\binom{\alpha}{i}\binom{i}{k}\binom{\beta}{j}\binom{j}{l}a^{q-1-i-j}b^{i+j-k-l}.\end{aligned}$$

Now assume that $a(a-1)b\neq 0$ and f is a PP of $\mathbb{F}_{q^2}$. We proceed to prove that $a(a-1)$ is a square in $\mathbb{F}_q^*$ and $b^2=a^2+3a$. The proof relies on several lemmas which are provided afterwards.

Letting $\alpha = 0$ and $\beta = q-1$ in (3.17), one has

$$
\begin{aligned}
(3.18)\qquad 0 &= -\sum_{x\in\mathbb{F}_{q^2}} f(x)^{(q-1)q} = \sum_{q-j-l=0} \binom{q-1}{j}\binom{j}{l} a^{-j} b^{j-l} \\
&= \sum_{1\le l\le q/2} \binom{q-1}{q-l}\binom{q-l}{l} a^{-(q-l)} b^{q-2l} = \frac{b}{a}\sum_{1\le l\le q/2} (-1)^{q-l}\binom{-l}{l} a^l b^{-2l} \\
&= -\frac{b}{a}\sum_{1\le l\le q/2} \binom{-l}{l}\left(\frac{-a}{b^2}\right)^l = -\frac{b}{a}\biggl(\sum_{0\le l\le q/2}\binom{-l}{l}\left(\frac{-a}{b^2}\right)^l - 1\biggr).
\end{aligned}
$$

Thus $\sum_{0\le l\le q/2}\binom{-l}{l}(-a/b^2)^l = 1$. By Lemma 3.1, $1+4(-a/b^2)$ is a square in $\mathbb{F}_q^*$, i.e., b^2-4a is a square in $\mathbb{F}_q^*$. (Note that $b^2-4a = a(a-1)$ after we prove that $b^2 = a^2+3a$.)

Next we prove that $b^2 = a^2+3a$. Letting $\alpha = 1$ and $\beta = q-2$ in (3.17), one has

$$
\begin{aligned}
-\sum_{x\in\mathbb{F}_{q^2}} & f(x)^{1+(q-2)q} \\
&= \sum_{q-1-j-l=0}\binom{q-2}{j}\binom{j}{l} a^{-j} b^{j-l} + \sum_{q-j-l=0}\binom{q-2}{j}\binom{j}{l} a^{-1-j} b^{1+j-l} \\
&\quad + \sum_{q+1-j-l=0,\, q+1}\binom{q-2}{j}\binom{j}{l} a^{-1-j} b^{j-l} \\
&= \sum_{1\le l\le (q-1)/2}\binom{q-2}{q-1-l}\binom{q-1-l}{l} a^{-(q-1-l)} b^{q-1-2l} \\
&\quad + \sum_{2\le l\le q/2}\binom{q-2}{q-l}\binom{q-l}{l} a^{-1-(q-l)} b^{1+q-2l} \\
&\quad + \sum_{3\le l\le (q+1)/2}\binom{q-2}{q+1-l}\binom{q+1-l}{l} a^{-1-(q+1-l)} b^{q+1-2l} + a^{-1}.
\end{aligned}
$$

Since $\binom{-2}{k} = (-1)^k(k+1)$ for $k\ge 0$, the above calculation gives

$$
\begin{aligned}
-\sum_{x\in\mathbb{F}_{q^2}} f(x)^{1+(q-2)q} &= \sum_{1\le l\le (q-1)/2} (-1)^{q-1-l}(q-l)\binom{-1-l}{l} a^l b^{-2l} \\
&\quad + \sum_{2\le l\le q/2} (-1)^{q-l}(q-l+1)\binom{-l}{l} a^{l-2} b^{-2l+2} \\
&\quad + \sum_{3\le l\le (q+1)/2} (-1)^{q+1-l}(q+2-l)\binom{1-l}{l} a^{l-3} b^{-2l+2} + a^{-1}
\end{aligned}
$$

$$\begin{aligned}
&= \sum_{1\le l\le (q-1)/2} (l+1)\binom{-l}{l+1}(-1)^l a^l b^{-2l} \\
&\quad + \sum_{2\le l\le q/2} (l-1)\binom{-l}{l}(-1)^l a^{l-2} b^{-2l+2} \\
&\quad + \sum_{3\le l\le (q+1)/2} (l-2)\binom{-(l-1)}{l}(-1)^{l+1} a^{l-3} b^{-2l+2} + a^{-1}.
\end{aligned}$$

Put $z = -a/b^2$. Then one has

$$\begin{aligned}
(3.19)\qquad & -\sum_{x\in\mathbb{F}_{q^2}} f(x)^{1+(q-2)q} \\
&= \sum_{0\le l\le (q-1)/2} (l+1)\binom{-l}{l+1} z^l + \frac{b^2}{a^2}\sum_{0\le l\le q/2}(l-1)\binom{-l}{l} z^l + \frac{b^2}{a^2} \\
&\quad + \sum_{2\le l\le (q-1)/2} (l-1)\binom{-l}{l+1}(-1)^l a^{l-2} b^{-2l} + a^{-1} \\
&= \sum_{0\le l\le (q-1)/2} [l+1+(l-1)a^{-2}]\binom{-l}{l+1} z^l \\
&\quad + \frac{b^2}{a^2}\sum_{0\le l\le q/2}(l-1)\binom{-l}{l}(-1)^l z^l + \frac{b^2}{a^2} + \frac{1}{a} \\
&= (1+a^{-2})\sum_{0\le l\le (q-1)/2}(l+1)\binom{-l}{l+1} z^l - 2a^{-2}\sum_{0\le l\le (q-1)/2}\binom{-l}{l+1} z^l \\
&\quad + \frac{b^2}{a^2}\sum_{0\le l\le q/2}(l+1)\binom{-l}{l} z^l - 2\,\frac{b^2}{a^2}\sum_{0\le l\le q/2}\binom{-l}{l} z^l + \frac{b^2}{a^2} + \frac{1}{a} \\
&= (1+a^{-2})\frac{2z}{1+4z} - 2a^{-2} + \frac{b^2}{a^2}\,\frac{1+3z}{1+4z} - 2\,\frac{b^2}{a^2} + \frac{b^2}{a^2} + \frac{1}{a} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(by Lemmas 3.1–3.3)} \\
&= \frac{2(a-1)(b^2-a^2-3a)}{a^2(b^2-4a)}.
\end{aligned}$$

Since f is a PP of $\mathbb{F}_{q^2}$, one has $\sum_{x\in\mathbb{F}_{q^2}} f(x)^{1+(q-2)q} = 0$. Hence $b^2 - a^2 - 3a = 0$. This completes the proof of the necessity part of Theorem A under the assumption $a(a-1)b \neq 0$.

The following lemmas, used in the above proof, hold for all (odd and even) q.

Lemma 3.1 ([Ho4, Lemma 5.1]). *Let $z \in \mathbb{F}_q^*$ and write $\mathtt{x}^2 + \mathtt{x} - z = (\mathtt{x} - r_1)(\mathtt{x} - r_2)$, $r_1, r_2 \in \mathbb{F}_{q^2}$. Then*

$$\sum_{0 \le l \le \frac{q}{2}} \binom{-l}{l} z^l = \begin{cases} 1/2 & \text{if } r_1 = r_2 \in \mathbb{F}_q, \\ 1 & \text{if } r_1, r_2 \in \mathbb{F}_q,\ r_1 \neq r_2, \\ 0 & \text{if } r_1, r_2 \notin \mathbb{F}_q. \end{cases}$$

Lemma 3.2. *Let $z \in \mathbb{F}_q^*$ be such that $\mathtt{x}^2 + \mathtt{x} - z$ has two distinct roots in $\mathbb{F}_q$. Then*

$$\sum_{0 \le l \le q/2} (l+1) \binom{-l}{l} z^l = \frac{1+3z}{1+4z}.$$

Proof. We denote the constant term of a Laurent series in x by ct( ). We have

$$\begin{aligned} \sum_{0 \le l \le q/2} (l+1) \binom{-l}{l} z^l &= \sum_{0 \le l \le q-2} (l+1) \binom{-l}{l} z^l \\ &= \sum_{0 \le l \le q-2} (l+1) \cdot \mathrm{ct}\Big(\frac{1}{\mathtt{x}^l (1+\mathtt{x})^l} \Big) \cdot z^l \\ &= \mathrm{ct}\Big[\sum_{0 \le l \le q-2} (l+1) \Big(\frac{z}{\mathtt{x}(1+\mathtt{x})} \Big)^l \Big]. \end{aligned}$$

Since

$$\sum_{1 \le l \le q-1} l \mathtt{y}^{l-1} = \frac{d}{d\mathtt{y}} \Big(\frac{1-\mathtt{y}^q}{1-\mathtt{y}} \Big) = \frac{1-\mathtt{y}^q}{(1-\mathtt{y})^2},$$

we have

$$\begin{aligned} \sum_{0 \le l \le q-2} (l+1) \Big(\frac{z}{\mathtt{x}(1+\mathtt{x})} \Big)^l &= \frac{1 - \big(\frac{z}{\mathtt{x}(1+\mathtt{x})}\big)^q}{\big(1 - \frac{z}{\mathtt{x}(1+\mathtt{x})}\big)^2} \\ &= \Big(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x}) - z} \Big)^2 \Big(1 - \frac{z}{\mathtt{x}^q} + \frac{z}{(1+\mathtt{x})^q} \Big). \end{aligned}$$

Thus

$$\begin{aligned} \sum_{0 \le l \le q/2} (l+1) \binom{-l}{l} z^l &= \mathrm{ct}\Big[-\frac{z}{\mathtt{x}^q} \Big(\frac{\mathtt{x}(1+\mathtt{x})}{\mathtt{x}(1+\mathtt{x}) - z} \Big)^2 \Big] \\ &= \mathrm{ct}\Big[-\frac{z}{\mathtt{x}^q} \Big(1 + \frac{z}{\mathtt{x}^2 + \mathtt{x} - z} \Big)^2 \Big]. \end{aligned}$$

The rest of the calculation is almost identical to that in [Ho4, proof of Lemma 5.3]. We omit the details. ∎

Lemma 3.3 ([Ho4, Lemmas 5.2 and 5.3]). *Let $z \in \mathbb{F}_q^*$ be such that $\mathtt{x}^2 + \mathtt{x} - z$ has two distinct roots in $\mathbb{F}_q$. Then*

$$\sum_{0\le l\le (q-1)/2} \binom{-l}{l+1} z^l = 1, \qquad \sum_{0\le l\le (q-1)/2} (l+1)\binom{-l}{l+1} z^l = \frac{2z}{1+4z}.$$

4. Proof of Theorem B. We follow the same outline of the proof of Theorem A. However, certain critical arguments in that proof fail in characteristic 2, and they have to be replaced with new approaches. First, in Subsection 3.2, the discriminant $D(g)$ in (3.13), which was at the heart of the proof there, is rendered useless in characteristic 2. Second, in Subsection 3.3, the calculation in (3.19) does not produce any useful information, again because of the even characteristic.

4.1. The case $a(a-1)b = 0$

Case 1. Assume $a = b = 0$. Then $f = \mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$ if and only if $\gcd(2q-1, q^2-1) = 1$, i.e., $q = 2^{2k}$, which is equivalent to (i) in Theorem B with $a = b = 0$.

Case 2. Assume $a \ne 0$, $b = 0$. By [Ho3, Theorem 1.1], $f = a\mathtt{x} + \mathtt{x}^{2q-1}$ is never a PP of $\mathbb{F}_{q^2}$.

Case 3. Assume $a = 0$, $b \ne 0$. By Case 3 in Subsection 3.1, f cannot be a PP of $\mathbb{F}_{q^2}$.

Case 4. Assume $a = 1$. The conclusion in Case 4 of Subsection 3.1 also holds for characteristic 2: f is a PP of $\mathbb{F}_{q^2}$ if and only if $\mathtt{x}^2 + b\mathtt{x} + 1$ has two distinct roots in $\mathbb{F}_q$, i.e., $b \ne 0$ and $\mathrm{Tr}_{q/2}(1/b) = 0$, which is (ii) in Theorem B. (Note: Theorem B with $a = 1$ also appeared as [Ho4, Theorem 1.2].)

4.2. The case $a(a-1)b \ne 0$, sufficiency. We are given that q (> 2) is even, $a \in \mathbb{F}_q \setminus \mathbb{F}_2$, $\mathrm{Tr}_{q/2}(\frac{1}{a+1}) = 0$, and $b^2 = a^2 + a$. The goal is to show that f is a PP of $\mathbb{F}_{q^2}$.

For each $y \in \mathbb{F}_{q^2}$, we show that there is at most one $x \in \mathbb{F}_{q^2}$ such that $f(x) = y$. We only have to consider the case $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. (We have $\mathrm{Tr}_{q/2}\big(\frac{1}{(a+b+1)^2}\big) = \mathrm{Tr}_{q/2}\big(\frac{1}{a+1}\big) = 0$. Thus $\mathtt{x}^2 + (a+b+1)\mathtt{x} + 1$ has two distinct roots in $\mathbb{F}_q$. By the argument in Subsection 3.2, 1°, $f(\mathbb{F}_{q^2} \setminus \mathbb{F}_q) \subset \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. By Subsection 3.2, 2°, if $y \in \mathbb{F}_q$, there is precisely one $x \in \mathbb{F}_{q^2}$ such that $f(x) = y$.)

Put $\tau = \mathrm{Tr}_{q^2/q}(y)$, $\eta = \mathrm{N}_{q^2/q}(y)$, $\sigma = \tau^2/\eta$. Then $\mathrm{Tr}_{q/2}(1/\sigma) = 1$ since $y \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. By (3.12) and the argument of Subsection 3.2, 3°, it suffices to show that the equation

$$s^3 + a\sigma s^2 + (a+1)(b\sigma + 1)s + (a+1)\sigma = 0 \tag{4.1}$$

has at most one solution $s \in \mathbb{F}_q$. Let $u = 1/\sigma$ and rewrite (4.1) as

$$\frac{1}{s^3} + (b+u)\frac{1}{s^2} + \frac{a}{a+1}\,\frac{1}{s} + \frac{u}{a+1} = 0.$$

So it suffices to show that

$$g := \mathtt{x}^3 + (b+u)\mathtt{x}^2 + \frac{a}{a+1}\mathtt{x} + \frac{u}{a+1}$$

has at most one root in $\mathbb{F}_q$. Put $A = b+u$, $B = a/(a+1)$, $C = u/(a+1)$. Assume to the contrary that g has at least two distinct roots in $\mathbb{F}_q$. Then g splits in $\mathbb{F}_q$. By a theorem of K. Conrad, stated as Theorem 4.1 at the end of this subsection, we conclude that

$$\mathtt{x}^2 + (AB+C)\mathtt{x} + (A^3C + B^3 + C^2)$$

is reducible over $\mathbb{F}_q$.

First assume $AB + C \neq 0$. Then

$$\mathrm{Tr}_{q/2}\biggl(\frac{A^3C + B^3 + C^2}{(AB+C)^2}\biggr) = 0. \tag{4.2}$$

We have

$$AB + C = \frac{(a+1)u + ab}{a+1}, \tag{4.3}$$

$$A^3C + B^3 + C^2 = \frac{1}{(a+1)^3}[(a+1)^2(b+u)^3u + a^3 + (a+1)u^2].$$

Hence

$$\frac{A^3C + B^3 + C^2}{(AB+C)^2} = \frac{(a+1)^2(b+u)^3u + a^3 + (a+1)u^2}{(a+1)[(a+1)u+ab]^2}.$$

Using the relation $b^2 = a^2 + a$ in the above equation, we find that

$$\frac{A^3C + B^3 + C^2}{(AB+C)^2} \tag{4.4}$$

$$= u^2 + \frac{1}{a+1} + \frac{bu}{a+1} + \biggl(\frac{bu}{a+1}\biggr)^2 + \frac{a^2}{(a+1)(bu+a^2)} + \biggl[\frac{a^2}{(a+1)(bu+a^2)}\biggr]^2.$$

It follows from (4.4) that

$$\mathrm{Tr}_{q/2}\biggl(\frac{A^3C + B^3 + C^2}{(AB+C)^2}\biggr) = \mathrm{Tr}_{q/2}(u^2) = 1,$$

which contradicts (4.2). It took some effort to find the desirable expression in (4.4). But the verification of (4.4) should be straightforward.

Now assume $AB + C = 0$. By (4.3), $u = ab/(a+1)$. Using this and the relation $b^2 = a^2 + a$, we see that $B^3 = C^2$. Thus

$$g = \mathtt{x}^3 + A\mathtt{x}^2 + B\mathtt{x} + C = \mathtt{x}^3 + \frac{C}{B}\mathtt{x}^2 + B\mathtt{x} + C = \biggl(\mathtt{x} + \frac{C}{B}\biggr)(\mathtt{x}^2 + B) = \biggl(\mathtt{x} + \frac{C}{B}\biggr)^3,$$

which is again a contradiction.

This completes the proof of the sufficiency part of Theorem B under the assumption $a(a-1)b \neq 0$.

Theorem 4.1 ([Co, Theorem 2.1]). *Let K be any field and $f = \mathrm{x}^3 + A\mathrm{x}^2 + B\mathrm{x} + C \in K[\mathrm{x}]$ have roots r_1, r_2, r_3 in a splitting field. Then*

$$\begin{aligned}(4.5)\qquad &\big(\mathrm{x} - (r_1^2r_2 + r_2^2r_3 + r_3^2r_1)\big)\big(\mathrm{x} - (r_2^2r_1 + r_1^2r_3 + r_3^2r_2)\big)\\ &\qquad = \mathrm{x}^2 + (AB-3C)\mathrm{x} + (A^3C + B^3 + 9C^2 - 6ABC),\end{aligned}$$

and the above quadratic polynomial has the same discriminant as f.

Theorem 4.1, proved by direct computation, was used in [Co] to obtain a criterion that determines whether the Galois group of a separable irreducible cubic polynomial f over K (of any characteristic) is S_3 or A_3: the Galois group is S_3 (resp. A_3) if the quadratic polynomial in (4.5) is irreducible (resp. reducible) over K.

4.3. The case $a(a-1)b \neq 0$, necessity. Assume that q is even and $f = a\mathrm{x} + b\mathrm{x}^q + \mathrm{x}^{2q-1} \in \mathbb{F}_q[\mathrm{x}]$ is a PP of $\mathbb{F}_{q^2}$, where $a(a-1)b \neq 0$. The goal is to prove that $\mathrm{Tr}_{q/2}\big(\frac{1}{a+1}\big) = 0$ and $b^2 = a^2 + a$.

Let $z = a/b^2$. By (3.18), $\sum_{0\le l\le q/2} \binom{-l}{l} z^l = 1$. It follows from Lemma 3.1 that $\mathrm{x}^2 + \mathrm{x} + z$ is reducible over $\mathbb{F}_q$. Hence $\mathrm{Tr}_{q/2}(z) = 0$. (Note that $z = a/b^2 = 1/(a+1)$ after we prove that $b^2 = a^2 + a$.)

It remains to show that $b^2 = a^2 + a$. Since $z \neq 0$ and $\mathrm{Tr}_{q/2}(z) = 0$, we must have $q > 2$. Letting $\alpha = 2$ and $\beta = q-3$ in (3.17), we have

$$\begin{aligned}&\sum_{x\in\mathbb{F}_{q^2}} f(x)^{2+(q-3)q}\\ &= \sum_{q-2+i+k-j-l=0,\,q+1} \binom{2}{i}\binom{i}{k}\binom{q-3}{j}\binom{j}{l} a^{-i-j} b^{i+j-k-l}\\ &= \sum_{q-2-j-l=0,\,q+1} \binom{q-3}{j}\binom{j}{l} a^{-j} b^{j-l} + \sum_{q-j-l=0,\,q+1} \binom{q-3}{j}\binom{j}{l} a^{-2-j} b^{2+j-l}\\ &\quad + \sum_{q+2-j-l=0,\,q+1} \binom{q-3}{j}\binom{j}{l} a^{-2-j} b^{j-l}\\ &= \sum_{q-2-j-l=0} \binom{q-3}{j}\binom{j}{l} a^{-j} b^{j-l} + \sum_{q-j-l=0} \binom{q-3}{j}\binom{j}{l} a^{-2-j} b^{2+j-l}\\ &\quad + \sum_{q+2-j-l=0} \binom{q-3}{j}\binom{j}{l} a^{-2-j} b^{j-l} + \sum_{j+l=1} \binom{q-3}{j}\binom{j}{l} a^{-2-j} b^{j-l}\end{aligned}$$

$$
\begin{aligned}
&= \sum_{1\le l\le q/2-1} \binom{q-3}{q-2-l}\binom{q-2-l}{l} a^{-(q-2-l)} b^{q-2-2l} \\
&\quad + \sum_{3\le l\le q/2} \binom{q-3}{q-l}\binom{q-l}{l} a^{-2-(q-l)} b^{2+q-2l} \\
&\quad + \sum_{5\le l\le q/2+1} \binom{q-3}{q+2-l}\binom{q+2-l}{l} a^{-2-(q+2-l)} b^{q+2-2l} + a^{-3}b.
\end{aligned}
$$

Since $\binom{-3}{k} = (-1)^k\binom{k+2}{2}$ for all integers $k \ge 0$, the above computation continues as

$$
\begin{aligned}
&\sum_{x\in\mathbb{F}_{q^2}} f(x)^{2+(q-3)q} \\
&\qquad = \sum_{1\le l\le q/2-1} \binom{q-l}{2}\binom{-2-l}{l} a^{1+l} b^{-1-2l} \\
&\qquad\quad + \sum_{3\le l\le q/2} \binom{q-l+2}{2}\binom{-l}{l} a^{-3+l} b^{3-2l} \\
&\qquad\quad + \sum_{5\le l\le q/2+1} \binom{q+4-l}{2}\binom{2-l}{l} a^{-5+l} b^{3-2l} + a^{-3}b \\
&\qquad = \frac{a}{b} \sum_{1\le l\le q/2-1} \binom{-l}{2}\binom{-l-2}{l} z^l + \frac{b^3}{a^3} \sum_{3\le l\le q/2} \binom{-l+2}{2}\binom{-l}{l} z^l \\
&\qquad\quad + \frac{b^3}{a^5} \sum_{5\le l\le q/2+1} \binom{-l+4}{2}\binom{-l+2}{l} z^l + \frac{b}{a^3}.
\end{aligned}
$$

Note that in the first sum on the right,

$$\binom{-l-2}{l} = -\binom{-l-1}{l+1},$$

and in the third sum,

$$
\begin{aligned}
\binom{-l+4}{2}\binom{-l+2}{l} &= \frac{(l-4)(l-3)}{2}\binom{-l+2}{l} \\
&\equiv \frac{(l-3)l}{2}\binom{-l+2}{l} \pmod 2 \\
&= \frac{(l-3)(-l+2)}{2}\binom{-l+1}{l-1}.
\end{aligned}
$$

Therefore we have

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_{q^2}} f(x)^{2+(q-3)q}\\
&\qquad= \frac{a}{b}\sum_{1\le l\le q/2-1}\binom{-l}{2}\binom{-l-1}{l+1}z^l+\frac{b^3}{a^3}\sum_{3\le l\le q/2}\binom{-l+2}{2}\binom{-l}{l}z^l\\
&\qquad\quad+\frac{b^3}{a^5}\sum_{5\le l\le q/2+1}\frac{(l-3)(l-2)}{2}\binom{-l+1}{l-1}z^l+\frac{b}{a^3}\\
&\qquad= \frac{a}{b}\sum_{0\le l\le q/2}\binom{-l+1}{2}\binom{-l}{l}z^{l-1}\\
&\qquad\quad+\frac{b^3}{a^3}\Bigg[\sum_{0\le l\le q/2}\binom{-l+2}{2}\binom{-l}{l}z^l+1\Bigg]\\
&\qquad\quad+\frac{b^3}{a^5}\Bigg[\sum_{0\le l\le q/2}\frac{(l-2)(l-1)}{2}\binom{-l}{l}z^{l+1}+z\Bigg]+\frac{b}{a^3}\\
&\qquad= \sum_{0\le l\le q/2}\binom{-l}{l}z^l\Bigg[b\binom{-l+1}{2}+\frac{b^3}{a^3}\binom{-l+2}{2}+\frac{b}{a^4}\cdot\frac{(l-2)(l-1)}{2}\Bigg]\\
&\qquad\quad+\frac{b^3}{a^3}+\frac{b}{a^4}+\frac{b}{a^3}\\
&\qquad= \sum_{0\le l\le q/2}\binom{-l}{l}z^l\Bigg[\Big(b+\frac{b^3}{a^3}+\frac{b}{a^4}\Big)\binom{l+2}{2}\\
&\qquad\quad+\Big(\frac{b^3}{a^3}+\frac{b}{a^4}\Big)(l+1)+\Big(b+\frac{b^3}{a^3}+\frac{b}{a^4}\Big)\Bigg]\\
&\qquad\quad+\frac{b^3}{a^3}+\frac{b}{a^4}+\frac{b}{a^3}.
\end{aligned}$$

Using the formulas

$$\sum_{0\le l\le q/2}\binom{-l}{l}z^l=1 \qquad \text{(Lemma 3.1),}$$

$$\sum_{0\le l\le q/2}(l+1)\binom{-l}{l}z^l=1+z \qquad \text{(Lemma 3.2),}$$

$$\sum_{0\le l\le q/2}\binom{l+2}{2}\binom{-l}{l}z^l=1+z^2 \qquad \text{(Lemma 4.2, to be proved),} \tag{4.6}$$

we have

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^2}} f(x)^{2+(q-3)q} &= \Big(b+\frac{b^3}{a^3}+\frac{b}{a^4}\Big)(1+z^2)+\Big(\frac{b^3}{a^3}+\frac{b}{a^4}\Big)(1+z)\\ &\quad +b+\frac{b^3}{a^3}+\frac{b}{a^4}+\frac{b^3}{a^3}+\frac{b}{a^4}+\frac{b}{a^3}\\ &=\Big(b+\frac{b^3}{a^3}+\frac{b}{a^4}\Big)\frac{a^2}{b^4}+\Big(\frac{a^3}{b^3}+\frac{b}{a^4}\Big)\frac{a}{b^2}+\frac{b}{a^3}\\ &=\frac{(a+1)(a+b+1)^2(a^2+b^2+a)}{a^3b^3}.\end{aligned}$$

Since f is a PP of $\mathbb{F}_{q^2}$, the above expression equals 0. Since $a+b+1\neq 0$ ($f(x)=(a+b+1)x$ for all $x\in\mathbb{F}_q$), we must have $b^2=a^2+a$.

To complete the proof of the necessity part of Theorem B under the assumption $a(a-1)b\neq 0$, we only need to establish (4.6). The following lemma, which gives (4.6), holds in all characteristics.

Lemma 4.2. *Let $\mathbb{F}_q$ be any finite field. Let $z\in\mathbb{F}_q^*$ be such that $\mathtt{x}^2+\mathtt{x}-z$ has two distinct roots in $\mathbb{F}_q$. Then*

$$\sum_{0\le l\le q/2}\binom{l+2}{2}\binom{-l}{l}z^l=\begin{cases}1+z & \text{if } q=2,\\ \dfrac{1+6z+11z^2}{(1+4z)^2} & \text{if } q>2.\end{cases}\tag{4.7}$$

Proof. When $q=2$, (4.7) is easily verified. Assume $q>2$. Recall that ct( ) denotes the constant term of a Laurent series in $\mathtt{x}$. We have

$$\begin{aligned}S:=\sum_{0\le l\le q/2}\binom{l+2}{2}\binom{-l}{l}z^l &= \sum_{0\le l\le q-3}\binom{l+2}{2}\binom{-l}{l}z^l\\ &=\sum_{0\le l\le q-3}\binom{l+2}{2}\cdot\operatorname{ct}\Big(\frac{1}{\mathtt{x}^l(1+\mathtt{x})^l}\Big)\cdot z^l\\ &=\operatorname{ct}\Big[\sum_{0\le l\le q-3}\binom{l+2}{2}\Big(\frac{z}{\mathtt{x}(1+\mathtt{x})}\Big)^l\Big].\end{aligned}$$

Let ∂^2 denote the second order Hasse derivative with respect to $\mathtt{y}$ [Ha]. Since

$$\sum_{2\le l\le q-1}\binom{l}{2}\mathtt{y}^{l-2}=\partial^2\sum_{0\le l\le q-1}\mathtt{y}^k=\partial^2[(1-\mathtt{y}^q)(1-\mathtt{y})^{-1}]=\frac{1-\mathtt{y}^q}{(1-\mathtt{y})^3},$$

we have

$$\sum_{0\le l\le q-3}\binom{l+2}{2}\left(\frac{z}{\mathrm{x}(1+\mathrm{x})}\right)^{l}=\frac{1-\left(\frac{z}{\mathrm{x}(1+\mathrm{x})}\right)^{q}}{\left(1-\frac{z}{\mathrm{x}(1+\mathrm{x})}\right)^{3}}$$
$$=\left(\frac{\mathrm{x}(1+\mathrm{x})}{\mathrm{x}^2+\mathrm{x}-z}\right)^{3}\left(1-\frac{z}{\mathrm{x}^q}+\frac{z}{(1+\mathrm{x})^q}\right).$$

Thus

$$S=\mathrm{ct}\left[\left(\frac{\mathrm{x}(1+\mathrm{x})}{\mathrm{x}^2+\mathrm{x}-z}\right)^{3}\left(1-\frac{z}{\mathrm{x}^q}+\frac{z}{(1+\mathrm{x})^q}\right)\right]\tag{4.8}$$
$$=\mathrm{ct}\left[-\frac{z}{\mathrm{x}^q}\left(\frac{\mathrm{x}(1+\mathrm{x})}{\mathrm{x}^2+\mathrm{x}-z}\right)^{3}\right]$$
$$=-z\cdot\mathrm{ct}\left[\mathrm{x}^{-q}\left(1+\frac{z}{\mathrm{x}^2+\mathrm{x}-z}\right)^{3}\right].$$

Write $\mathrm{x}^2+\mathrm{x}-z=(\mathrm{x}-r_1)(\mathrm{x}-r_2)$. Using the substitution

$$\frac{1}{(\mathrm{x}-r_1)(\mathrm{x}-r_2)}=\frac{1}{r_1-r_2}\left(\frac{1}{\mathrm{x}-r_1}-\frac{1}{\mathrm{x}-r_2}\right)$$

repeatedly, we find that

$$\left(1+\frac{z}{(\mathrm{x}-r_1)(\mathrm{x}-r_2)}\right)^{3}\tag{4.9}$$
$$=1+(3zc-6z^2c^3+6z^3c^5)\left(\frac{1}{\mathrm{x}-r_1}-\frac{1}{\mathrm{x}-r_2}\right)$$
$$+(3z^2c^2-3z^3c^4)\left(\frac{1}{(\mathrm{x}-r_1)^2}-\frac{1}{(\mathrm{x}-r_2)^2}\right)$$
$$+z^3c^3\left(\frac{1}{(\mathrm{x}-r_1)^3}-\frac{1}{(\mathrm{x}-r_2)^3}\right),$$

where $c=1/(r_1-r_2)$. Note that for $r\neq 0$ (in any field) and integer k, we have

$$(\mathrm{x}-r)^k=(-r)^k\left(1-\frac{\mathrm{x}}{r}\right)^{k}=(-r)^k\sum_{l\ge 0}\binom{k}{l}(-r)^{-l}\mathrm{x}^l.\tag{4.10}$$

Combining (4.8)–(4.10) gives

$$
\begin{aligned}
(4.11)\qquad S = -z\Big[&(3zc - 6z^2c^3 + 6z^3c^5)\big((-r_1)^{-1-q} - (-r_2)^{-1-q}\big)\binom{-1}{q}\\
&+ (3z^2c^2 - 3z^3c^4\big((-r_1)^{-2-q} + (-r_2)^{-2-q}\big)\binom{-2}{q}\\
&+ z^3c^3\big((-r_1)^{-3-q} - (-r_2)^{-3-q}\big)\binom{-3}{q}\Big]\\
= -z\big[&(3z - 6z^2c^2 + 6z^3c^4)\cdot c\cdot(-r_1^{-2} + r_2^{-2})\\
&+ (3z^2c^2 - 3z^3c^4)(r_1^{-3} + r_2^{-3}) + z^3c^2\cdot c\cdot(-r_1^{-4} + r_2^{-4})\big].
\end{aligned}
$$

In the above

$$
\begin{aligned}
c^2 &= \frac{1}{(r_1 - r_2)^2} = \frac{1}{(r_1 + r_2)^2 - 4r_1r_2} = \frac{1}{1 + 4z},\\
c(-r_1^{-2} + r_2^{-2}) &= \frac{1}{r_1 - r_2}\cdot\frac{r_1^2 - r_2^2}{(r_1r_2)^2} = \frac{r_1 + r_2}{z^2} = -\frac{1}{z^2},\\
r_1^{-3} + r_2^{-3} &= \frac{r_1^3 + r_2^3}{(r_1r_2)^3} = \frac{(r_1 + r_2)^3 - 3r_1r_2(r_1 + r_2)}{-z^3}\\
&= \frac{-1 - 3z}{-z^3} = \frac{1 + 3z}{z^3},\\
c(-r_1^{-4} + r_2^{-4}) &= \frac{1}{r_1 - r_2}\cdot\frac{r_1^4 - r_2^4}{(r_1r_2)^4} = \frac{(r_1 + r_2)(r_1^2 + r_2^2)}{z^4} = \frac{-(1 + 2z)}{z^4}.
\end{aligned}
$$

Making the above substitutions in (4.11), we get

$$S = \frac{1 + 6z + 11z^2}{(1 + 4z)^2}. \quad ■$$

5. The polynomial $g_{n,q}$. The trinomial $a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1}$ owes its origin to a class of seemingly unrelated polynomials.

It is known [Ca, HHM] that

$$(5.1)\qquad \sum_{c\in\mathbb{F}_q}\frac{1}{\mathtt{x} + c} = \frac{1}{\mathtt{x} - \mathtt{x}^q}.$$

We have

$$
\begin{aligned}
\sum_{n\ge 0}\sum_{c\in\mathbb{F}_q}(\mathtt{x} + c)^n\mathtt{t}^n &= \sum_{c\in\mathbb{F}_q}\frac{1}{1 - (\mathtt{x} + c)\mathtt{t}} = \frac{1}{\mathtt{t}}\sum_{c\in\mathbb{F}_q}\frac{1}{\frac{1}{\mathtt{t}} - \mathtt{x} - c}\\
&= \frac{1}{\mathtt{t}}\,\frac{1}{(1/\mathtt{t} - \mathtt{x}) - (1/\mathtt{t} - \mathtt{x})^q} \qquad \text{(by (5.1))}\\
&= \frac{-\mathtt{t}^{q-1}}{1 - \mathtt{t}^{q-1} - (\mathtt{x}^q - \mathtt{x})\mathtt{t}^q} = \sum_{n\ge 0} g_{n,q}(\mathtt{x}^q - \mathtt{x})\mathtt{t}^n,
\end{aligned}
$$

where $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ (with $p = \operatorname{char} \mathbb{F}_q$) is the polynomial defined by

$$\frac{-\mathtt{t}^{q-1}}{1-\mathtt{t}^{q-1}-\mathtt{x}\mathtt{t}^{q}} = \sum_{n\ge 0} g_{n,q}\mathtt{t}^n.$$

Thus

$$\sum_{c\in\mathbb{F}_q} (\mathtt{x}+c)^n = g_{n,q}(\mathtt{x}^q-\mathtt{x}),$$

which can also be viewed as the definition of the polynomial $g_{n,q}$. Recent studies show that the class $g_{n,q}$ contains many new and interesting PPs [FHL, Ho1, Ho2, Ho3, Ho4]. When $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$, we call the triple $(n,e;q)$ *desirable*. All desirable triples with $e=1$ are known [FHL, Theorem 2.1]. The complete determination of all desirable triples is a challenging unsolved problem. One of the mysterious phenomena observed in the study of the polynomial $g_{n,q}$ is that among the known desirable triples $(n,e;q)$, n frequently appears in the form $q^\alpha - q^\beta - 1$. Here is a summary of the previous state of knowledge of the desirable triples $(n,e;q)$ with $n = q^\alpha - q^\beta - 1$.

Assume that $e \ge 2$, $n > 0$, and $n \equiv q^\alpha - q^\beta - 1 \pmod{q^{pe}-1}$, where $0 \le \alpha, \beta < pe$. (By [Ho2, Proposition 2.4], it suffices to consider n modulo $q^{pe}-1$, hence it suffices to consider $0 \le \alpha, \beta < pe$.)

(1) If $\alpha < \beta$, then $(n,e;q)$ is desirable if and only if $(n',e;q)$ is desirable, where $n' = q^{\alpha'} - q^{\beta'} - 1$, $\alpha' = pe - \alpha - \beta$, $\beta' = pe - \beta$. (So we may assume $\beta \le \alpha$.) [FHL, §5]

(2) If $\beta = \alpha$, then $(n,e;q)$ is desirable if and only if $q > 2$. [FHL, §5]

(3) If $0 = \beta < \alpha$ and q is even, then $(n,e;q)$ is desirable if and only if $\alpha = 3$ and $q = 2$, or $\alpha = 2$ and $\gcd(q-2, q^e-1) = 1$. [FHL, §5]

(4) Assume $0 = \beta < \alpha$ and q is odd. If $\alpha \le 2$, $(n,e;q)$ is desirable if and only if $\alpha = 2$ and $\gcd(q-2, q^e-1) = 1$; if $\alpha > 2$, it was conjectured that $(n,e;q)$ is not desirable. [FHL, §5]

(5) If $(\beta,\alpha) = (1,2)$, then $(n,e;q)$ is desirable if and only if $\gcd(q-2, q^e-1) = 1$. [FHL, Corollary 5.2]

(6) If $0 < \beta < \alpha$ and $\alpha \equiv \beta \equiv 0 \pmod{e}$, then $(n,e;q)$ is desirable. [FHL, Theorem 5.3]

(7) Assume $e \ge 3$ and $0 < \beta < \alpha$. It was conjectured that the only desirable triples are those in (5) and (6). [FHL, Conjecture 5.5]

(8) Assume that $e = 2$, $0 < \beta < \alpha$, and β is even. Then $(n,2;q)$ is desirable if and only if α is even. [FHL, Remark 5.4]

(9) Assume that $e = 2$, q is odd, and $\beta = p$. If $\alpha = p + 2i$, $0 < i \le \frac{1}{2}(p-1)$, then $(n,2;q)$ is desirable if and only if $4i \not\equiv 1 \pmod{p}$; if $\alpha = p + 2i - 1$, $0 < i \le \frac{1}{2}(p-1)$, then $(n,2;q)$ is desirable if and only if $4i \not\equiv 3 \pmod{p}$. [FHL, Theorems 5.6, 5.7]

(10) If $e = 2$, q is even, and $(\beta, \alpha) = (1, 3)$, then $(n, 2; q)$ is desirable if and only $q \equiv 1 \pmod 3$. [FHL, Theorem 5.9]

(11) Assume that $e = 2$, $q > 2$, $(\beta, \alpha) = (1, 2i)$, $i > 0$. Then $(n, 2; q)$ is desirable if and only if one of the following holds.

 (i) $2i \equiv 1 \pmod p$ and $q \equiv 1 \pmod 4$;
 (ii) $2i \equiv -1 \pmod p$ and $q \equiv \pm 1 \pmod{12}$;
 (iii) $4i \equiv 1 \pmod p$ and $q \equiv -1 \pmod 6$.

 [Ho3, Theorem 4.1]

(12) Assume that $e = 2$, q is odd, $(\beta, \alpha) = (1, 2i + 1)$, $i > 0$. Then $(n, e; q)$ is desirable if and only $p \equiv 1$ or $3 \pmod 8$, $q \equiv 1 \pmod 8$, and $i^2 = -1/2$. [Ho4, Corollary 6.1]

For $e \geq 3$, there was little activity as indicated by statement (7). For $e = 2$, the situation appeared to be chaotic. In fact, our computer search produced many desirable triples with $e = 2$ (and $n = q^\alpha - q^\beta - 1$) that are not covered by the above results; see [FHL, Table 1]. The case $(q^\alpha - q^\beta - 1, 2; q)$, which seemed hopeless till now, will be completely resolved in the next section. When $n = q^\alpha - q^\beta - 1$, $0 \leq \beta < \alpha$, the polynomial function $g_{n,q}(x)$ on $\mathbb{F}_{q^2}$ can be transformed into the form $Ax + Bx^q + Cx^{2q-1}$ through an invertible change of variable. Thus Theorems A and B allow us to determine all desirable triples of the form $(q^\alpha - q^\beta - 1, 2; q)$, $0 \leq \beta < \alpha$. We note that for even q, all desirable triples $(q^\alpha - q^\beta - 1, 2; q)$ are already determined by a combination of some of the above statements, so Theorem B is not necessary for this purpose.

6. Theorems C and D

Lemma 6.1. *Assume $q > 2$. Let $n = q^\alpha - q^\beta - 1$, where $0 < \beta < \alpha < 2p$, β is odd, and $\beta \neq p$. Write $\alpha - \beta = a_0 + 2a_1$, $0 \leq a_0 \leq 1$, and $\beta = 1 + 2b_1$. Then*

$$g_{n,q}(x) = A\phi(x) + B\phi(x)^q + C\phi(x)^{2q-1} \quad \textit{for all } x \in \mathbb{F}_{q^2}, \tag{6.1}$$

where ϕ is a permutation of $\mathbb{F}_{q^2}$ and

$$\begin{cases} A = \dfrac{1}{\beta}(-a_0 b_1 + b_1 + a_1), \\ B = a_0 - \dfrac{b_1 + 1}{\beta}, \\ C = -\dfrac{1}{\beta}(a_0 b_1 + a_0 + a_1). \end{cases} \tag{6.2}$$

Proof. For every integer $a \geq 0$, define $S_a = \mathtt{x} + \mathtt{x}^q + \cdots + \mathtt{x}^{q^{a-1}} \in \mathbb{F}_p[\mathtt{x}]$. Let $x \in \mathbb{F}_{q^2}^*$. By [FHL, (5.3)],

$$\begin{aligned} g_{n,q}(x) &= -x^{q^2-2} - x^{q^2-q-2}(a_1 S_2(x) + S_{a_0}(x)^q)((b_1 S_2(x) + S_1(x))^{q-1} - 1) \\ &= -x^{-1} - x^{-q-1}\big(a_1 x + (a_0 + a_1)x^q\big)[((b_1+1)x + b_1 x^q)^{q-1} - 1] \\ &= -y - (a_1 y^q + (a_0 + a_1)y)[((b_1+1)y^q + b_1 y)^{q-1} - 1], \end{aligned}$$

where $y = x^{-1}$. Note that $(b_1+1)\mathtt{x}^q + b_1\mathtt{x}$ is a PP of $\mathbb{F}_{q^2}$ whose inverse on $\mathbb{F}_{q^2}$ is given by $\frac{1}{\beta}((b_1+1)\mathtt{x}^q - b_1\mathtt{x})$.

Let $z = (b_1+1)y^q + b_1 y$. Then $y = \frac{1}{\beta}((b_1+1)z^q - b_1 z)$. We have

$$\begin{aligned} g_{n,q}(x) &= -\frac{1}{\beta}((b_1+1)z^q - b_1 z) \\ &\quad - \left[a_1\frac{1}{\beta}((b_1+1)z - b_1 z^q) + (a_0+a_1)\frac{1}{\beta}((b_1+1)z^q - b_1 z)\right](z^{q-1}-1) \\ &= Az + Bz^q + Cz^{2q-1}. \end{aligned}$$

Extend the mapping $x \mapsto z$ to a bijection $\phi : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ by setting $\phi(0) = 0$. Then (6.1) holds. ∎

Theorem C. *Let q be even and $n = q^\alpha - q^\beta - 1$, where $0 \leq \beta < \alpha < 2\cdot 2$. Then $(n, 2; q)$ is desirable if and only if one of the following occurs:*

(i) *$q \equiv 1 \pmod 3$, $(\beta, \alpha) = (0, 2), (1, 2), (1, 3)$.*
(ii) *$q = 2$, $(\beta, \alpha) = (0, 3)$.*

Proof. The conclusion follows from statements (3), (5), (8), (10) in Section 5. ∎

Theorem D. *Let q be odd and $n = q^\alpha - q^\beta - 1$, where $0 \leq \beta < \alpha < 2p$. Then $(n, 2; q)$ is desirable if and only if one of the following occurs:*

(i) *$q \equiv 1 \pmod 3$, $(\beta, \alpha) = (0, 2)$.*
(ii) *$\beta > 0$, $\beta \equiv \alpha \equiv 0 \pmod 2$.*
(iii) *$(\beta, \alpha) = (p, p+i)$, $0 < i < p$, $2i \not\equiv (-1)^i \pmod p$.*
(iv) *$\beta \neq p$, $\beta = 1 + 2b_1$, $\alpha - \beta = a_0 + 2a_1$, $a_0, a_1, b_1 \in \mathbb{N}$, $0 \leq a_0 \leq 1$, and one of the following is satisfied.*

(iv.1) *$(a_1 + b_1)(2a_1 + b_1) + a_0(a_1 - 2a_1 b_1 - b_1^2)$ is a square in $\mathbb{F}_q^*$ and*

$$1 + 2b_1 + 2a_1^2 + a_1 b_1 + a_0\big(-1 - 2b_1 + b_1^2 + a_1(3 + 2b_1)\big) \equiv 0 \pmod p.$$

$$\text{(iv.2)} \qquad \begin{cases} a_0 + 2a_1 + b_1 \equiv 0 \pmod p, \\ (1+b_1)^2 - 4a_1^2 - a_0\big(5 + 10b_1 + 4b_1^2 + 8a_1(1+b_1)\big) \\ \qquad\qquad \equiv 0 \pmod p. \end{cases}$$

$$\text{(iv.3)} \qquad \begin{cases} a_0 = 1,\ b_1 = 0, \\ 4a_1 + 3 \equiv 0 \pmod{p}, \\ q \equiv -1 \pmod{6}. \end{cases}$$

$$\text{(iv.4)} \qquad \begin{cases} a_0 = 1,\ a_1 = 0,\ b_1 = 0, \\ q \equiv 1, 3 \pmod{6}. \end{cases}$$

Proof. CASE 1. Assume $\beta = 0$. We show that $(n, 2; q)$ is desirable if and only if $\alpha = 2$ and $q \equiv 1 \pmod{3}$. The "if" part follows from statement (4) in Section 5. To prove the "only if" part, by the same statement, it suffices to show that $(n, 2; q)$ is not desirable for $\alpha > 2$.

Write $\alpha = a_0 + 2a_1$, $a_0, a_1 \in \mathbb{N}$, $0 \le a_0 \le 1$. By [FHL, (5.1)], for all $x \in \mathbb{F}_{q^2}$ we have

$$\begin{aligned} g_{n,q}(x) &= x^{q-2} + x^{q^2-2} + \cdots + x^{q^{\alpha-1}-2} \\ &= a_1(x^{q-2} + x^{q^2-2}) + (a_0 - 1)x^{q^2-2} \\ &= a_1 x^{q-2} + (a_0 + a_1 - 1)x^{q^2-2} \\ &= (a_0 + a_1 - 1)y^q + a_1 y^{2q-1}, \end{aligned}$$

where $y^q = x^{q^2-2}$. Note that $0 < a_1 < p$ and $0 < a_0 + a_1 - 1 < p$, so $a_1 \not\equiv 0 \pmod{p}$ and $a_0 + a_1 - 1 \not\equiv 0 \pmod{p}$. By Theorem A, $(a_0 + a_1 - 1)\mathtt{x}^q + a_1\mathtt{x}^{2q-1}$ is not a PP of $\mathbb{F}_{q^2}$. So $g_{n,q}$ is not a PP of $\mathbb{F}_{q^2}$ either.

CASE 2. Assume $\beta > 0$ and $\beta \equiv 0 \pmod{2}$. By statement (8) in Section 5, $(n, 2; q)$ is desirable if and only if (ii) holds.

CASE 3. Assume $\beta = p$. By statement (9) in Section 5, $(n, 2; q)$ is desirable if and only if (iii) holds.

CASE 4. Assume $\beta \not\equiv 0 \pmod{2}$ and $\beta \ne p$. Write $\beta = 1 + 2b_1$ and $\alpha - \beta = a_0 + 2a_1$, $a_0, a_1, b_1 \in \mathbb{N}$, $0 \le a_0 \le 1$. By Lemma 6.1, $(n, 2; q)$ is desirable if and only if $A\mathtt{x} + B\mathtt{x}^q + C\mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$, where A, B, C are given by (6.2). We claim that $C \ne 0$ in $\mathbb{F}_p$, i.e., $a_0 b_1 + a_0 + a_1 \not\equiv 0 \pmod{p}$. In fact,

$$0 < a_0 b_1 + a_0 + a_1 \le a_1 + b_1 + 1 = \tfrac{1}{2}(1 + 2a_1 + 1 + 2b_1) \le \tfrac{1}{2}(\alpha - \beta + \beta) = \tfrac{1}{2}\alpha < p.$$

Thus $(n, 2; q)$ is desirable if and only if $(A/C)\mathtt{x} + (B/C)\mathtt{x}^q + \mathtt{x}^{2q-1}$ is a PP of $\mathbb{F}_{q^2}$, which happens if and only if one of the conditions in Theorem A holds with $a = A/C$ and $b = B/C$. Let

$$a = \frac{A}{C} = \frac{a_0 b_1 - b_1 - a_1}{a_0 b_1 + a_0 + a_1}, \qquad b = \frac{B}{C} = \frac{-2a_0 b_1 - a_0 + b_1 + 1}{a_0 b_1 + a_0 + a_1}$$

in Theorem A; then conditions (i)–(iv) in Theorem A become (iv.1)–(iv.4) in Theorem D. ∎

7. A final remark. Let $f = a\mathtt{x} + b\mathtt{x}^q + \mathtt{x}^{2q-1} \in \mathbb{F}_q[\mathtt{x}]$, $ab \neq 0$. For $0 \le s < q^2-1$, we saw in Section 3.3 that $\sum_{x\in\mathbb{F}_{q^2}} f(x)^s = 0$ unless $s = \alpha+\beta q$, $0 \le \alpha, \beta \le q-1$, $\alpha+\beta = q-1$.

Let $z = -a/b^2$ and assume that $\mathtt{x}^2 + \mathtt{x} - z$ has two distinct roots in $\mathbb{F}_q$. By (3.18) and (3.19), which hold for both odd and even q, we have

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{0+(q-1)q} = 0, \tag{7.1}$$

$$\sum_{x\in\mathbb{F}_{q^2}} f(x)^{1+(q-2)q} = \frac{2(1-a)(b^2-a^2-3a)}{a^2(b^2-4a)}. \tag{7.2}$$

The sum $\sum_{x\in\mathbb{F}_{q^2}} f(x)^{2+(q-3)q}$ was computed in Section 4.3 for even $q \ge 4$. That computation can be adapted for an arbitrary q resulting in the following formula:

$$\begin{aligned}\sum_{x\in\mathbb{F}_{q^2}} & f(x)^{2+(q-3)q} \\ &= \frac{3b(1-a)(b^2-a^2-3a)(9a-6a^2+a^3-2b^2+ab^2)}{a^4(b^2-4a)^2}, \qquad q \ge 3.\end{aligned} \tag{7.3}$$

(The computation of (7.3), which is quite lengthy and tedious, is given in the appendix of [Ho5].) Note that the sums (7.1)–(7.3) are rational functions in a, b, independent of q, with coefficients in $\mathbb{Z}$. Moreover, the factor b^2-a^2-3a appears in the numerator of each these three rational functions. In fact, this is true in general. Following the idea behind the computations in Sections 3.3 and 4.3, it is not difficult to be convinced that for every $0 \le \alpha \le q-1$, the sum $\sum_{x\in\mathbb{F}_{q^2}} f(x)^{\alpha+(q-1-\alpha)q}$ should be a rational function $R_\alpha(a,b)$ in a, b, independent of q, with coefficients in $\mathbb{Z}$, although we do not know the explicit expression of $R_\alpha(a,b)$ for a general α. Since we already assumed that $\mathtt{x}^2+\mathtt{x}-z$ has two distinct roots in $\mathbb{F}_q$, by Theorems A and B, the condition $b^2-a^2-3a = 0$ implies that f is a PP of $\mathbb{F}_{q^2}$, which further implies that $R_\alpha(a,b) = 0$ for all $0 \le \alpha \le q-1$. Hence b^2-a^2-3a is a factor of the numerator of the reduced form of $R_\alpha(a,b)$. Two questions arise: Is it possible to compute $R_\alpha(a,b)$ explicitly for all $0 \le \alpha \le q-1$? If $R_\alpha(a,b)$ is too complicated to compute, is there any more direct explanation why b^2-a^2-3a always appears in the numerator of $R_\alpha(a,b)$?

Acknowledgements. This research was partly supported by NSA (grant no. H98230-12-1-0245).

References

[AW] A. Akbary and Q. Wang, *A generalized Lucas sequence and permutation binomials*, Proc. Amer. Math. Soc. 134 (2006), 15–22.

[Ca] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. 1 (1935), 139–158.

[Co] K. Conrad, *Galois groups of cubics and quartics in all characteristics*, unpublished.

[E] A. B. Evans, *Orthomorphism Graphs of Groups*, Lecture Notes in Math. 1535, Springer, Berlin, 1992.

[FHL] N. Fernando, X. Hou and S. D. Lappano, *A new approach to permutation polynomials over finite fields, II*, Finite Fields Appl. 22 (2013), 122–158.

[GM] S. W. Golomb and O. Moreno, *On periodicity properties of Costas arrays and a conjecture on permutation polynomials*, IEEE Trans. Inform. Theory 42 (1996), 2252–2253.

[Ha] H. Hasse, *Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik*, J. Reine Angew. Math. 175 (1936), 50–54.

[HHM] K. Hicks, X. Hou and G. L. Mullen, *Sums of reciprocals of polynomials over finite fields*, Amer. Math. Monthly 119 (2012), 313–317.

[Hi1] J. W. P. Hirschfeld, *Rational curves on quadrics over finite fields of characteristic two*, Rend. Mat. (6) 4 (1971), 773–795.

[Hi2] J. W. P. Hirschfeld, *Ovals in desarguesian planes of even order*, Ann. Mat. Pura Appl. (4) 102 (1975), 79–89.

[Ho1] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory Ser. A 118 (2011), 448–454.

[Ho2] X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. 18 (2012), 492–521.

[Ho3] X. Hou, *A class of permutation binomials over finite fields*, J. Number Theory 133 (2013), 3549–3558.

[Ho4] X. Hou, *A class of permutation trinomials over finite fields*, Acta Arith. 162 (2014), 51–64.

[Ho5] X. Hou, *Determination of a type of permutation trinomials over finite fields*, arXiv:1309.3530.

[IR] K. F. Ireland and M. I. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1982.

[L] Y. Laigle-Chapuy, *Permutation polynomials and applications to coding theory*, Finite Fields Appl. 13 (2007), 58–70.

[LP] J. B. Lee and Y. H. Park, *Some permuting trinomials over finite fields*, Acta Math. Sci. (English Ed.) 17 (1997), 250–254.

[LB] J. Levine and J. V. Brawley, *Some cryptographic applications of permutation polynomials*, Cryptologia 1 (1977), 76–92.

[LC] J. Levine and R. Chandler, *Some further cryptographic applications of permutation polynomials*, Cryptologia 11 (1987), 211–218.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[MPW] A. Masuda, D. Panario and Q. Wang, *The number of permutation binomials over $\mathbb{F}_{4p+1}$ where p and $4p+1$ are primes*, Electron. J. Combin. 13 (2006), R65.

[MZ] A. M. Masuda and M. E. Zieve, *Permutation binomials over finite fields*, Trans. Amer. Math. Soc. 361 (2009), 4169–4180.

[NR] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser. A 33 (1982), 197–212.

[T] G. Turnwald, *Permutation polynomials of binomial type*, in: Contributions to General Algebra 6, Hölder-Pichler-Tempsky, Wien, 1988, 281–286.

[W1] D. Wan, *Permutation polynomials over finite fields*, Acta Math. Sinica (N.S.) 3 (1987), 1–5.

[W2] D. Wan, *Permutation binomials over finite fields*, Acta Math. Sinica (N.S.) 10 (1994), Special Issue, 30–35.

[Z] 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.

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida
Tampa, FL 33620, U.S.A.
E-mail: xhou@usf.edu

Received on 18.12.2013 (7683)