Existence and nonexistence of permutation trinomials and quadrinomials

Zhiguo DING[1],* , **Michael E. ZIEVE**[2]

[1]Chengdu University of Technology, Chengdu, Sichuan, China

[2]Department of Mathematics, University of Michigan, Ann Arbor, MI, USA

Abstract: For each q of the form 4^k, we determine all $a \in \mathbb{F}_q$ for which $X + X^q + X^{2q-1} + aX^{q^2-q+1}$ permutes $\mathbb{F}_{q^2}$. We also construct a class of permutation trinomials over $\mathbb{F}_{q^2}$ in case $q \equiv 1 \pmod 3$.

Key words: Permutation polynomial, finite field, trinomial, quadrinomial

1. Introduction

For any prime power q, a polynomial $f(X) \in \mathbb{F}_q[X]$ is called a *permutation polynomial* if the function $\alpha \mapsto f(\alpha)$ induces a permutation of $\mathbb{F}_q$. Such polynomials have been intensively studied due to both their applications and their intrinsic interest. In particular, many authors have studied permutation polynomials with few terms.

The main result of the recent paper [2] is as follows, in which Tr_1^m is the trace function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_2$.

Theorem 1.1 (Theorem 3.2 of [2]) *Let* $q = 2^m$ *where* m *is an even integer with* $m > 2$. *If* $a, b \in \mathbb{F}_q$ *satisfy* $a + 1 \notin \{0, b\}$, $\mathrm{Tr}_1^m(\frac{1}{1+a}) = 0$, *and* $\mathrm{Tr}_1^m(1 + \frac{b}{(1+a+b)^2}) = 0$ *then* $f(X) := X + X^q + X^{2q-1} + aX^{q^2-q+1}$ *permutes* $\mathbb{F}_{q^2}$.

In this note, we show that Theorem 1.1 is false, in the following strong sense:

Theorem 1.2 *Let* $q = 2^m$ *where* $m > 0$ *is even, and pick* $a \in \mathbb{F}_q$. *Then* $f(X) := X + X^q + X^{2q-1} + aX^{q^2-q+1}$ *permutes* $\mathbb{F}_{q^2}$ *if and only if* $a = 0$.

In light of Theorem 1.2, it is easy to exhibit explicit counterexamples to Theorem 1.1, which may be verified independently of Theorem 1.2. For instance, one counterexample is $m = 4$, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2$, and $b = 0$.

This paper is organized as follows. After presenting some known results in the next section, we prove Theorem 1.2 in Section 3, after which we explain a mistake in the proof of [2, Thm. 3.2]. Then in Section 4, we present a class of permutation trinomials which generalizes [2, Thm. 3.1].

2. Background results

In this section, we present the known results which are used in our proof of Theorem 1.2. They rely on the following notation, which we use throughout this paper.

---

*Correspondence: ding8191@qq.com

Notation 2.1 *If q is a prime power then we write μ_{q+1} for the set of all $(q+1)$-th roots of unity in $\mathbb{F}_{q^2}$, and for any field K we define $\mathbb{P}^1(K) := K \cup \{\infty\}$ and let $\overline{K}$ be an algebraic closure of K.*

We begin with the following special case of [3, Lemma 2.1]:

Lemma 2.2 *Write $f(X) := X^r B(X^{q-1})$ where q is a prime power, r is a positive integer, and $B(X) \in \mathbb{F}_{q^2}[X]$. Then $f(X)$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(r, q-1) = 1$ and $g_0(X) := X^r B(X)^{q-1}$ permutes μ_{q+1}.*

The next lemma encodes a procedure introduced in [4]:

Lemma 2.3 *For $r > 0$ and $B(X) \in \mathbb{F}_q[X]$, the polynomial $g_0(X) := X^r B(X)^{q-1}$ permutes μ_{q+1} if and only if $B(X)$ has no roots in μ_{q+1} and $g(X) := X^r B(1/X)/B(X)$ permutes μ_{q+1}.*

Proof   Plainly, if $B(X)$ has roots in μ_{q+1}, then $g_0(X)$ does not permute μ_{q+1}. Henceforth, suppose that $B(X)$ has no roots in μ_{q+1}. Then for $\gamma \in \mu_{q+1}$ we have

$$B(\gamma)^{q-1} = \frac{B(\gamma)^q}{B(\gamma)} = \frac{B(\gamma^q)}{B(\gamma)} = \frac{B(\gamma^{-1})}{B(\gamma)},$$

so that $g_0(\gamma) = g(\gamma)$. The result follows.

Definition 2.4 *For any field K and any nonzero $h(X) \in K(X)$, by the numerator and denominator of $h(X)$, we mean the unique coprime $N, D \in K[X]$ such that $D(X)$ is monic and $h(X) = N(X)/D(X)$, and the degree of $h(X) \in K(X)$ is $\max(\deg(N), \deg(D))$.*

The following lemma is well-known and easy. It can be proved directly from the definitions, or as an immediate consequence of the first assertion in [1, Lemma 2.2].

Lemma 2.5 *For any field K, any nonconstant $h(X) \in K(X)$, and any degree-one $\rho, \eta \in K(X)$, the rational functions $h(X)$ and $\rho(X) \circ h(X) \circ \eta(X)$ have the same degree as one another.*

The following result is a special case of [4, Lemma 3.1].

Lemma 2.6 *For any prime power q, and any $c \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, the degree-one rational function $\rho(X) := (cX - c^q)/(X - 1)$ induces a bijection from μ_{q+1} to $\mathbb{P}^1(\mathbb{F}_q)$.*

The following result is well-known; for instance, cf. [1, Cor. 2.8]:

Lemma 2.7 *For any field K and any degree-one $\rho(X) \in K(X)$, there is a unique degree-one $\rho^{-1}(X) \in K(X)$ such that $\rho^{-1} \circ \rho = X = \rho \circ \rho^{-1}$. Explicitly, if $\rho(X) = (aX + b)/(cX + d)$ then $\rho^{-1}(X) = (dX - b)/(-cX + a)$.*

We will use the geometric description of all degree-three permutation rational functions over $\mathbb{F}_q$ from [1, Thm. 1.3], for which two very short proofs are given in [1]. The following is a consequence of that result:

Lemma 2.8 *Let q be a power of 2, and let $h(X) \in \mathbb{F}_q(X)$ have degree 3. If $h(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$ then there exist degree-one $\sigma, \tau \in \mathbb{F}_{q^2}(X)$ for which $h(X) = \sigma \circ X^3 \circ \tau$.*

3. Proof of Theorem 1.2

In this section, we prove Theorem 1.2. Throughout this section, we write $q := 2^m$ where $m > 0$ is even, and $f(X) := X + X^q + X^{2q-1} + aX^{q^2-q+1}$ for some $a \in \mathbb{F}_q$. We also use Notation 2.1 without further mention.

We may assume that $a \neq 1$, since if $a = 1$ then $f(1) = 0 = f(0)$ so that $f(X)$ does not permute $\mathbb{F}_{q^2}$. Note that

$$f(X) \equiv X^{q^2} + X^{q^2+q-1} + X^{q^2+2q-2} + aX^{q^2-q+1} \pmod{X^{q^2} - X},$$

so that $f(X)$ permutes $\mathbb{F}_{q^2}$ if and only if

$$f_1(X) := X^{q^2} + X^{q^2+q-1} + X^{q^2+2q-2} + aX^{q^2-q+1}$$

does. Here $f_1(X) = X^{q^2-q+1}B(X^{q-1})$ where $B(X) := X^3 + X^2 + X + a$. By Lemmas 2.2 and 2.3, $f_1(X)$ permutes $\mathbb{F}_{q^2}$ if and only if $B(X)$ has no roots in μ_{q+1} and $X^{q^2-q+1}B(1/X)/B(X)$ permutes μ_{q+1}. Since $q^2 - q + 1 \equiv 3 \pmod{q+1}$, it follows that $f(X)$ permutes $\mathbb{F}_{q^2}$ if and only if $B(X)$ has no roots in μ_{q+1} and $g(X) := X^3 B(1/X)/B(X)$ permutes μ_{q+1}.

First, suppose $a = 0$, so that $B(X) = X^3 + X^2 + X$ and

$$g(X) = \frac{X^2 + X + 1}{X^3 + X^2 + X} = \frac{1}{X}.$$

Then the roots of $B(X)$ are 0 and the primitive cube roots of unity. Since $q = 2^m$ with m even, we have $q \equiv 1 \pmod 3$ so that $q + 1 \equiv 2 \pmod 3$, whence $B(X)$ has no roots in μ_{q+1}. Since $g(X) = 1/X$ permutes μ_{q+1}, it follows that $f(X)$ permutes $\mathbb{F}_{q^2}$ in this case.

Henceforth suppose, for the sake of obtaining a contradiction, that $a \neq 0$ and $f(X)$ permutes $\mathbb{F}_{q^2}$. Then $g(X)$ permutes μ_{q+1}. We first show that $\deg(g) = 3$. Write $N(X) := X^3 B(1/X)$, so that $N(X) = aX^3 + X^2 + X + 1$ and $g(X) = N(X)/B(X)$. Then $N(X) + B(X) = (a+1)(X^3+1)$, so since $a \neq 1$ it follows that any common root of $N(X)$ and $B(X)$ would be a root of $X^3 + 1$. However, $N(1) = a + 1 \neq 0$ and each $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$ satisfies $N(\omega) = a \neq 0$, so $N(X)$ and $B(X)$ have no common roots. Thus, $\gcd(N(X), B(X)) = 1$, which since $\deg(N) = \deg(B) = 3$ implies that $\deg(g) = 3$.

Next, we show that $g(X)$ is the composition of X^3 with degree-one rational functions over $\mathbb{F}_{q^2}$. To this end, first pick $s \in \overline{\mathbb{F}}_q$ satisfying $s^q + s = 1$. Then $s \notin \mathbb{F}_q$, and since $s^q + s = 1 = 1^q = s^{q^2} + s^q$, we conclude that $s^{q^2} = s$, so that $s \in \mathbb{F}_{q^2}$. Write $\rho(X) := (sX + s^q)/(X+1)$ and $\rho^{-1}(X) := (X + s^q)/(X + s)$, so that $\rho(X)$ maps μ_{q+1} bijectively onto $\mathbb{P}^1(\mathbb{F}_q)$ (by Lemma 2.6) and $\rho^{-1}(X)$ induces the inverse bijection (by Lemma 2.7). Since $g(X)$ permutes μ_{q+1}, we see that $h(X) := \rho(X) \circ g(X) \circ \rho^{-1}(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$. The rational function $h(X)$ is in $\mathbb{F}_{q^2}(X)$; we now show that in fact it is in $\mathbb{F}_q(X)$. Writing $t := s^2 + s$, a routine computation yields

$$h(X) := \rho \circ g \circ \rho^{-1} = \frac{X^3 + tX + t + \frac{1}{a+1}}{X^2 + X + t + 1}.$$

Note that $t^q = (s+1)^2 + (s+1) = s^2 + s = t$ so that $t \in \mathbb{F}_q$, whence $h(X) \in \mathbb{F}_q(X)$. Thus, $h(X)$ is a rational function in $\mathbb{F}_q(X)$ which permutes $\mathbb{P}^1(\mathbb{F}_q)$, and $\deg(h) = 3$ by Lemma 2.5, so by Lemma 2.8, we see

that $h(X) = \sigma \circ X^3 \circ \tau$ for some degree-one $\sigma, \tau \in \mathbb{F}_{q^2}(X)$. Thus,

$$g(X) = \rho^{-1} \circ \sigma \circ X^3 \circ \tau \circ \rho$$

can be written as $g(X) = \widehat{\sigma} \circ X^3 \circ \widehat{\rho}$ where $\widehat{\sigma} := \rho^{-1} \circ \sigma$ and $\widehat{\tau} := \tau \circ \rho$ are degree-one rational functions in $\mathbb{F}_{q^2}(X)$.

Finally, we obtain a contradiction by examining the numbers of g-preimages in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ of certain elements of $\mathbb{P}^1(\overline{\mathbb{F}}_q)$. Note that each element of $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ has either 1 or 3 preimages under X^3. Since $\widehat{\sigma}$ and $\widehat{\tau}$ induce bijections on $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, it follows that each element of $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ has either 1 or 3 preimages under $g(X) = \widehat{\sigma} \circ X^3 \circ \widehat{\tau}$. Let $\beta \in \overline{\mathbb{F}}_q$ be a root of $X^2 + (a+1)X + 1$, so that $\beta \notin \mathbb{F}_2$ since $a \neq 1$. Then

$$g(X) + \beta = \frac{N(X) + \beta B(X)}{B(X)}$$

$$= \frac{(a+\beta)X^3 + (1+\beta)(X^2 + X) + 1 + \beta a}{B(X)}$$

$$= (a+\beta)\frac{(X^2 + \beta)(X + \beta)}{B(X)},$$

where it is easy to check that the numerators of the last two rational functions have the same terms of degree X^i for $i \in \{1,2,3\}$, and then one can conclude that they also have the same constant term since the constant term of $(a+\beta)(X^2+\beta)(X+\beta)$ is β times the coefficient of X, and hence is $\beta(1+\beta) = 1 + \beta a$. Since $g(X)$ is nonconstant, we have $\deg(g(X)+\beta) = \deg(g) = 3$, so that $B(X)$ and $(X^2+\beta)(X+\beta)$ are coprime. Since $\beta \neq a = g(\infty)$, it follows that the only g-preimages of β in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ are β and $\sqrt{\beta}$. Since $\beta \notin \mathbb{F}_2$, we conclude that β has exactly two g-preimages in $\mathbb{P}^1(\overline{\mathbb{F}}_q)$, which contradicts what we showed above. This contradiction implies that if $a \neq 0$ then $f(X)$ does not permute $\mathbb{F}_{q^2}$, which concludes the proof of Theorem 1.2.

Remark 3.1 *One mistake in the proof of [2, Thm. 3.2] occurs in the last displayed equation on page 927 of [2], where the author claims that*

$$\mathrm{Tr}_1^m\left(1 + \frac{\mu}{1 + a^2 + a\mu + \mu} + \frac{(1+a)\mu^2}{(1+a^2+a\mu+\mu)^2}\right) = \mathrm{Tr}_1^m\left(1 + \frac{\mu}{(1+a+\mu)^2}\right).$$

This equality is false in general, and no justification for this equality is given in the paper [2].

4. Another class of permutation polynomials

The second theorem in [2] is as follows:

Theorem 4.1 (Theorem 3.1 of [2]) *If $q = 2^m$ for some positive integer m then $f(X) := X + X^{q^3-q+1} + X^{q^4-q^3+q}$ permutes $\mathbb{F}_{q^4}$.*

In this section, we construct some classes of permutation polynomials which include Theorem 4.1 as a very special case. Throughout this section, we use Notation 2.1.

We begin with the following general result.

Theorem 4.2 (Theorem 5.1 of [4]) *Let Q be a prime power, let r and d be positive integers, and let β be a $(Q+1)$-th root of unity in $\mathbb{F}_{Q^2}$. Let $B(X) := \sum_{i=0}^{d} a_i X^i$ where $a_0 \neq 0$ and, for $0 \leq i \leq d/2$, we have $a_i \in \mathbb{F}_{Q^2}$ and $a_{d-i} = (\beta a_i)^Q$. Then $f(X) := X^r B(X^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if all of the following hold:*

(4.2.1) $\gcd(r, Q-1) = 1$;

(4.2.2) $\gcd(r-d, Q+1) = 1$;

(4.2.3) $B(X)$ *has no roots in* μ_{Q+1}.

In order to produce explicit classes of permutation polynomials using Theorem 4.2, one must exhibit explicit situations in which (4.2.3) holds. Here is one such situation:

Corollary 4.3 *Let Q be a power of a prime p, and let r, k, v be positive integers with $k > 1$. Let $B(X) := \sum_{i=0}^{k-1} X^{iv}$. Then $f(X) := X^r B(X^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if all of the following hold:*

(4.3.1) $\gcd(r, Q-1) = 1$;

(4.3.2) $\gcd(r - kv + v, Q+1) = 1$;

(4.3.3) $\gcd(p \frac{Q+1}{\gcd(Q+1, v)}, k) = 1$.

Proof Writing $d := (k-1)v$, we have $B(X) = \sum_{i=0}^{d} a_i X^i$ where $a_i = 1$ when $v \mid d$ and $a_i = 0$ otherwise. Thus, $a_0 \neq 0$, each a_i is in $\mathbb{F}_Q$, and $a_{d-i} = a_i$ for each i (since $v \mid d$ implies that $v \mid i$ if and only if $v \mid (d-i)$). Thus, for each i, we have $a_{d-i} = (\beta a_i)^Q$ with $\beta := 1$. Hence, Q, r, d, β, and $B(X)$ satisfy the hypotheses of Theorem 4.2, so by Theorem 4.2, we see that $f(X)$ permutes $\mathbb{F}_{Q^2}$ if and only if conditions (4.2.1)–(4.2.3) hold. Plainly, (4.2.1) and (4.3.1) are identical, and since $d = kv - v$, we see that (4.3.2) is a reformulation of (4.2.2). Next, note that $B(X) = (X^{kv} - 1)/(X^v - 1)$. If p divides k, then $X^{kv} - 1$ is divisible by $X^{pv} - 1$, which equals $(X^v - 1)^p$, so that $B(X)$ is a polynomial times $(X^v - 1)^{p-1}$, and thus, $B(1) = 0$. Hence, if $p \mid k$, then (4.2.3) does not hold, and plainly, in this case, (4.3.3) does not hold either. Finally, assume that $p \nmid k$. Then the roots of $(X^k - 1)/(X - 1)$ are the nontrivial k-th roots of unity in $\overline{\mathbb{F}}_p$, so the roots of $B(X)$ are the elements of $\overline{\mathbb{F}}_p^*$ whose order divides kv but does not divide v. There are no such elements in μ_{Q+1} if and only if $\gcd(kv, Q+1) = \gcd(v, Q+1)$, or equivalently $\gcd(k, \frac{Q+1}{\gcd(Q+1, v)}) = 1$. Thus, (4.2.3) is equivalent to (4.3.3), which concludes the proof of Corollary 4.3.

In the special case where $k = 3$ and $Q \equiv 1 \pmod{3}$, Corollary 4.3 becomes the following.

Corollary 4.4 *Let Q be a prime power with $Q \equiv 1 \pmod{3}$, and let r and v be positive integers. Let $B(X) := 1 + X^v + X^{2v}$. Then $f(X) := X^r B(X^{Q-1})$ permutes $\mathbb{F}_{Q^2}$ if and only if $\gcd(r, Q-1) = 1 = \gcd(r - 2v, Q+1)$.*

There are many choices of r and v which satisfy the gcd conditions in Corollary 4.4. For instance, we obtain the following result from the choices $v = \sqrt{Q}$ and $r = v^4 - v^3 + v$.

Corollary 4.5 *Let q be a power of a prime p. Then $f(X) := X + X^{q^3 - q + 1} + X^{q^4 - q^3 + q}$ permutes $\mathbb{F}_{q^4}$ if and only if $p \neq 3$.*

Proof First, note that if $p = 3$, then $f(X)$ does not permute $\mathbb{F}_{q^4}$ since $f(1) = 0 = f(0)$. Henceforth, assume $p \neq 3$, and write $v := q$, $Q := q^2$, $r := q^4 - q^3 + q$, and $B(X) := 1 + X^v + X^{2v}$. Then Q is a prime power with $Q \equiv 1 \pmod{3}$, and r and v are positive integers. Moreover, since $r + v(Q-1) = v^4 = r - 2v + v(Q+1)$, we have $\gcd(r, Q-1) = \gcd(v^4, v^2-1) = 1$ and likewise $\gcd(r - 2v, Q+1) = 1$. Thus, Corollary 4.4 implies that $\widehat{f}(X) := X^r B(X^{Q-1})$ permutes $\mathbb{F}_{q^4}$. We have

$$\widehat{f}(X) = X^{q^4 - q^3 + q} + X^{q^4 - q^3 + q + q(q^2 - 1)} + X^{q^4 - q^3 + q + 2q(q^2 - 1)}$$

$$= X^{q^4 - q^3 + q} + X^{q^4} + X^{q^4 + q^3 - q},$$

so that $\widehat{f}(X)$ induces the same function on $\mathbb{F}_{q^4}$ as does $f(X)$. Thus, $f(X)$ permutes $\mathbb{F}_{q^4}$, which concludes the proof. $\qquad\blacksquare$

Theorem 4.1 is the special case of Corollary 4.5 in which $p = 2$. Thus, Corollary 4.5 is a vast generalization of Theorem 4.1, while Corollary 4.4 is much more general than Corollary 4.5, and Corollary 4.3 is enormously more general than Corollary 4.4, and finally Corollary 4.3 is one very special case of Theorem 4.2.

A different type of generalization of the permutation polynomials in Theorem 4.1 is provided by the following result.

Theorem 4.6 (Proposition 1.1 of [3]) *Let Q be a power of a prime p, and let r, k, v, t be positive integers. Write $s := \gcd(v, Q-1)$, $d := (Q-1)/s$, and $e := v/s$, and let S be the set of d-th roots of unity in $\mathbb{F}_Q$ which do not equal 1. Then $X^r(\sum_{i=0}^{k-1} X^{iv})^t$ permutes $\mathbb{F}_Q$ if and only if all of the following hold:*

(4.6.1) $\gcd(r, s) = \gcd(d, k) = 1$;

(4.6.2) $\gcd(d, 2r + vt(k-1)) \leq 2$;

(4.6.3) $k^{st} \equiv (-1)^{(d+1)(r+1)} \pmod{p}$;

(4.6.4) $g(X) := X^r \left(\frac{1 - X^{ke}}{1 - X^e}\right)^{st}$ *is injective on S;*

(4.6.5) $(-1)^{(d+1)(r+1)} \notin g(S)$.

Proof that Theorem 4.6 implies Corollary 4.5 Let q be a power of a prime p, and write $f(X) := X + X^{q^3 - q + 1} + X^{q^4 - q^3 + q}$. Plainly, if $p = 3$, then $f(1) = 0 = f(0)$, so that $f(X)$ does not permute $\mathbb{F}_{q^4}$. Henceforth, suppose $p \neq 3$, and write $Q := q^4$, $r := q^4 - q^3 + q$, $k := 3$, $v := q^3 - q$, and $t := 1$. Define s, d, e, S as in Theorem 4.6, so that $s = q^2 - 1$, $d = q^2 + 1$, $e = q$, and S is the set of nontrivial $(q^2 + 1)$-th roots of unity in $\mathbb{F}_{q^4}^*$. By Theorem 4.6, $\widehat{f}(X) := X^r(\sum_{i=0}^{k-1} X^{iv})^t$ permutes $\mathbb{F}_Q$ if and only if (4.6.1)–(4.6.5) hold. We now verify each of these conditions. Since $r + qs = q^4$, we have $\gcd(r, s) = \gcd(q^4, s) = \gcd(q^4, q^2 - 1) = 1$. Since -1 is a nonsquare in $\mathbb{F}_3^*$, we have $\gcd(d, k) = \gcd(q^2 + 1, 3) = 1$, which implies (4.6.1). We compute $\gcd(d, 2r + vt(k-1)) = \gcd(q^2 + 1, 2q^4) \leq 2$, so that (4.6.2) holds. Condition (4.6.3) holds because $3^{p-1} \equiv 1 \pmod{p}$ and $(-1)^{r+1} = 1$. We have $g(X) = X^r(1 + X^q + X^{2q})^{q^2 - 1}$. Since $r \equiv 2q + 1 \pmod{q^2 + 1}$ and

$3 \nmid (q^2 + 1)$, each $\gamma \in S$ satisfies $1 + \gamma^q + \gamma^{2q} \neq 0$, and thus,

$$g(\gamma) = \gamma^{2q+1}(1 + \gamma^q + \gamma^{2q})^{q^2-1}$$

$$= \gamma^{2q+1}\frac{(1 + \gamma^q + \gamma^{2q})^{q^2}}{1 + \gamma^q + \gamma^{2q}}$$

$$= \gamma^{2q+1}\frac{1 + \gamma^{-q} + \gamma^{-2q}}{1 + \gamma^q + \gamma^{2q}}$$

$$= \gamma.$$

Therefore, $g(X)$ induces the identity function on S, so that (4.6.4) holds, and also (4.6.5) holds since $1 \notin S = g(S)$. We have verified (4.6.1)–(4.6.5), so that $\widehat{f}(X)$ permutes $\mathbb{F}_{q^4}$. Finally, we compute $\widehat{f}(X) = X^{q^4-q^3+q} + X^{q^4} + X^{q^4+q^3-q}$, so that $\widehat{f}(X)$ induces the same function on $\mathbb{F}_{q^4}$ as does $f(X)$. It follows that $f(X)$ permutes $\mathbb{F}_{q^4}$, which yields Corollary 4.5.

Acknowledgment

References

[1] Ding Z, Zieve M. Low-degree permutation rational functions over finite fields. Acta Arithmetica 2022; 202 (3): 253–280. https://doi.org/10.4064/aa210521-12-11

[2] Liu Q. Two classes of permutation polynomials with Niho exponents over finite fields with even characteristic. Turkish Journal of Mathematics 2022; 46 (3): 919–928. https://doi.org/10.55730/1300-0098.3132

[3] Zieve M. Some families of permutation polynomials over finite fields. International Journal of Number Theory 2008; 4 (5): 851–857. https://doi.org/10.1142/S1793042108001717

[4] Zieve M. Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$. https://doi.org/10.48550/arXiv.1310.0776