

DETERMINATION OF ALL COMPLETE MAPPINGS OF $\mathbb{F}_{q^2}$ OF THE FORM $aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3$

ZHIGUO DING, WEI XIONG, AND MICHAEL E. ZIEVE

ABSTRACT. For each prime power q , we determine all polynomials over $\mathbb{F}_{q^2}$ of the form $f(X) := aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3$ which induce complete mappings of $\mathbb{F}_{q^2}$, in the sense that each of the functions $x \mapsto f(x)$ and $x \mapsto f(x) + x$ permutes $\mathbb{F}_{q^2}$. This is the first result in the literature which classifies the complete mappings among some class of polynomials with arbitrarily large degree over finite fields of arbitrary characteristic. We also determine all permutation polynomials over $\mathbb{F}_{q^2}$ of the form $X^{q+2} + bX^q + cX$, and all permutations of $\mathbb{F}_q \times \mathbb{F}_q$ induced by maps of the form $(x, y) \mapsto (x^3 - exy^2 - ax - by, y^3 - cx - dy)$ where either $e = 0$ or $3 \mid q$. The latter results add to the small number of results in the literature classifying all permutations induced by maps of prescribed forms.

1. INTRODUCTION

A *complete mapping* of a group G is a permutation π of G for which the function $g \mapsto \pi(g) \cdot g$ permutes G . Complete mappings were introduced by Mann in his work on constructing orthogonal Latin squares [7]. They have been used in various ways in cryptography [9–11, 13], coding theory [12], and in the construction of quasigroups [8]. By a complete mapping of a field or of a vector space, we mean a complete mapping of the additive group of the relevant object.

There are only a few known classes of complete mappings of finite fields $\mathbb{F}_q$. Most of these come from one of two sources, namely additive homomorphisms of $\mathbb{F}_q$ or functions acting as scalar multiples on each coset of $\mathbb{F}_q^*/H$ for some low-index subgroup H of $\mathbb{F}_q^*$. There are simple conditions determining which functions of these two types are complete mappings.

In this paper we prove the first result classifying all complete mappings over finite fields of arbitrary characteristic among some class of polynomials other than the two just described. We give two descriptions of the relevant complete mappings, one providing simple representatives up to a natural equivalence relation, and one providing explicit conditions on the coefficients.

Date: October 21, 2025.

The second author was supported in part by the Natural Science Foundation of Hunan Province of China (No. 2020JJ4164). The third author was supported in part by Simons Travel Grant MPS-TSM-00007931.

We now define the equivalence relation we will use. We say that $f, g \in \mathbb{F}_{q^2}[X]$ are $\mathbb{F}_q$ -linearly conjugate if the induced functions on $\mathbb{F}_{q^2}$ satisfy $f = \rho^{-1} \circ g \circ \rho$ for some $\mathbb{F}_q$ -vector space automorphism ρ of $\mathbb{F}_{q^2}$. Equivalently, there exist $a, b \in \mathbb{F}_{q^2}$ such that $a^{q+1} \neq b^{q+1}$ and the polynomials $L(X) := aX^q + bX$ and $L^{-1}(X) := (aX^q - b^q X)/(a^{q+1} - b^{q+1})$ satisfy $f(X) \equiv L^{-1}(X) \circ g(X) \circ L(X) \pmod{X^{q^2} - X}$.

Our main result is as follows.

Theorem 1.1. *Let q be a power of a prime p , and pick any $a, b, c, d \in \mathbb{F}_{q^2}$. Then $f(X) := aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3$ is a complete mapping of $\mathbb{F}_{q^2}$ if and only if one of the following holds:*

- (1.1.1) $f(X)$ is $\mathbb{F}_q$ -linearly conjugate to γX^{q+2} for some $\gamma \in \mathbb{F}_{q^2}^*$ with $\gamma^{2q-2} - \gamma^{q-1} + 1 = 0$;
- (1.1.2) $q \equiv 0 \pmod{3}$ and $f(X) = aX^{3q} + dX^3$ where $a^{q+1} \neq d^{q+1}$ and $aX^{3q-1} + dX^2 + 1$ has no roots in $\mathbb{F}_{q^2}^*$.

Remark 1.2. The complete mappings γX^{q+2} in (1.1.1) first appeared in [16, Cor. 2.3]. A slightly weaker version of the special case $p = 2$ of Theorem 1.1 was proved in [1].

The complete mappings in (1.1.2) belong to the well-known class of additive polynomials (which are sometimes called linearized polynomials or p -polynomials), namely, polynomials of the form $\sum_{i=0}^m a_i X^{p^i}$ where p is the characteristic of $\mathbb{F}_q$. Such a polynomial $f(X)$ is a complete mapping of $\mathbb{F}_{q^2}$ if and only if both $f(X)$ and $f(X) + X$ have no roots in $\mathbb{F}_{q^2}^*$. We now determine explicit necessary and sufficient conditions on the coefficients of the non-additive complete mappings $f(X)$ in Theorem 1.1.

Theorem 1.3. *For any prime power q , and any $a, b, c, d \in \mathbb{F}_{q^2}$, the polynomial $f(X) := aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3$ is a complete mapping on $\mathbb{F}_{q^2}$ if and only if $q \not\equiv 1 \pmod{3}$ and either (1.1.2) holds or one of the following holds:*

- (1.3.1) $a = b = d = 0$ and $c^{2q-2} - c^{q-1} + 1 = 0$; or
- (1.3.2) all of these hold:
 - $3ac = b^2 \neq 9d^{2q}$,
 - $144a^{q+3} = -(b^2 + 3d^{2q})^2$,
 - $24a^2d = (b + d^q)(b^2 + 3d^{2q}) \neq 0$,
 - $24a^2b^q = -(b - 3d^q)(b^2 + 3d^{2q})$; or
- (1.3.3) $3 \mid q$ and all of these hold:
 - $b = d = 0$,
 - $c^{q-1} = -1$,
 - $(-a/c)^{(q+1)/2} = -1$; or
- (1.3.4) $3 \mid q$ and all of these hold:
 - $b = 0$,
 - $a^{q-1}d^{2q-2} = -1$,
 - $d^{4q+4} + a^4d^{q+5}$ is a square in $\mathbb{F}_q^*$,

- $acd^q + a^2d + d^{3q} = 0$; or
- (1.3.5) $2 \mid q$ and all of these hold:
- $a^{q+1} = c^{2q} + c^{q+1} + c^2$,
 - $ac = b^2$,
 - $d = b^q$,
 - $c \notin \mathbb{F}_q$; or
- (1.3.6) $q = 2$, $a = d$, $b = 0$, and $c \in \mathbb{F}_4 \setminus \mathbb{F}_2$.

Our proof of Theorem 1.1 uses a wide range of tools, including some intricate applications of Hermite's criterion, Weil's bound, results about primitive and doubly transitive permutation groups, and knowledge of all low-degree permutation rational functions. Our proof proceeds by first proving the following classifications of bijections of certain forms, which are of independent interest.

Theorem 1.4. *For any prime power q , and any $b, c \in \mathbb{F}_{q^2}$, the polynomial $f(X) := X^{q+2} + bX^q + cX$ permutes $\mathbb{F}_{q^2}$ if and only if one of the following holds:*

- (1.4.1) $q \not\equiv 1 \pmod{3}$, $b = 0$, and c^{q-1} is a root of $X^3 - X^2 + X$;
 (1.4.2) $q = 2$, $b \neq 0$, and $c = 1$.

Theorem 1.5. *For any prime power q , and any $a, b, c, d \in \mathbb{F}_q$, the map $\varphi: (x, y) \mapsto (x^3 - ax - by, y^3 - cx - dy)$ permutes $\mathbb{F}_q \times \mathbb{F}_q$ if and only if one of the following holds:*

- (1.5.1) $q \not\equiv 1 \pmod{3}$ and $a = d = bc = 0$;
 (1.5.2) $q \equiv 0 \pmod{3}$, $bc = 0$, and a and d are nonsquares in $\mathbb{F}_q$;
 (1.5.3) $q \equiv 0 \pmod{3}$, $bc \neq 0$, and no nonzero square in $\mathbb{F}_q$ is a root of the polynomial $X^4 - (a^3 + b^2d)X + b^2(ad - bc)$;
 (1.5.4) $q = 2$, $b = c = 1$, and $1 \in \{a, d\}$.

Theorem 1.6. *Let q be a power of 3, and pick $a, b, c, d, e \in \mathbb{F}_q$ with $e \neq 0$. Then $\varphi: (x, y) \mapsto (x^3 - exy^2 - ax - by, y^3 - cx - dy)$ permutes $\mathbb{F}_q \times \mathbb{F}_q$ if and only if $c = 0$, d is either zero or a nonsquare, and one of the following holds:*

- $a = 0$ and e is a nonsquare; or
- $q = 3$, $a = -1$, and $e = 1$.

Our final result relies on the following notion.

Definition 1.7. If U and V are $\mathbb{F}_q$ -vector spaces, then a function $f: U \rightarrow U$ is $\mathbb{F}_q$ -linearly equivalent to a function $g: V \rightarrow V$ if $f = \rho \circ g \circ \eta^{-1}$ for some $\mathbb{F}_q$ -vector space isomorphisms ρ and η from V to U .

Remark 1.8. It is easy to see that $\mathbb{F}_q$ -linear equivalence is an equivalence relation on the union of the sets of functions $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$ and $\mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{F}_q \times \mathbb{F}_q$, and that $\mathbb{F}_q$ -linear equivalence preserves the property of a function being bijective.

Remark 1.9. It is well-known that the $\mathbb{F}_q$ -vector space automorphisms of $\mathbb{F}_{q^2}$ are the functions induced by $aX^q + bX$ where $a, b \in \mathbb{F}_{q^2}$ satisfy $a^{q+1} \neq b^{q+1}$. Likewise, the $\mathbb{F}_q$ -vector space isomorphisms $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_q \times \mathbb{F}_q$ are the functions $x \mapsto (ax + (ax)^q, bx + (bx)^q)$ where $a, b \in \mathbb{F}_{q^2}^*$ satisfy $a^{q-1} \neq b^{q-1}$, and the $\mathbb{F}_q$ -vector space isomorphisms $\mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{F}_{q^2}$ are $(x, y) \mapsto ax + by$ where $a, b \in \mathbb{F}_{q^2}^*$ satisfy $a^{q-1} \neq b^{q-1}$.

Theorem 1.10. *Suppose q is a prime power and $a, b, c, d \in \mathbb{F}_{q^2}$. Write $f(X) := aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3 \in \mathbb{F}_{q^2}[X]$. Then $f(X)$ permutes $\mathbb{F}_{q^2}$ if and only if $f(X)$ is $\mathbb{F}_q$ -linearly equivalent to one of the following:*

- (1.10.1) X^{q+2} , where $q \not\equiv 1 \pmod{3}$;
- (1.10.2) (X^3, Y^3) , where $q \not\equiv 1 \pmod{3}$;
- (1.10.3) $(X^3 - eXY^2, Y^3)$ for some nonsquare $e \in \mathbb{F}_q^*$, where $q \equiv 0 \pmod{3}$.

Remark 1.11. It is not clear whether Theorem 1.10 can be used to obtain explicit necessary and sufficient conditions on the coefficients of $f(X)$ which do not involve the coefficients of the additive polynomials involved in the $\mathbb{F}_q$ -linear equivalence. However, we will determine such conditions via a different method in a forthcoming paper.

The interest of the above results about permutations is that there are only a handful of results determining all bijective functions having specified forms but with arbitrary coefficients and over an arbitrary (possibly square) finite field. For instance, the most general such result is [4, Thm. 1.1], which determines the members of a certain 4-parameter family of polynomials which permute $\mathbb{F}_{q^2}$.

This paper is organized as follows. Theorems 1.4, 1.5, 1.6 and 1.10 are proved in Sections 2, 3, 4 and 5, respectively. Then in Section 6 we prove Theorems 1.1 and 1.3.

2. BIJECTIONS INDUCED BY $X^{q+2} + bX^q + cX$

In this section we prove Theorem 1.4. Our proof uses the following result of Dickson [2, §14], which is a generalization to multinomial coefficients of Lucas's theorem on mod p reductions of binomial coefficients.

Lemma 2.1. *Let p be prime, let $m_1, m_2, \dots, m_k$ be nonnegative integers, and write $m := \sum_{i=1}^k m_i$. Write $m = \sum_{j=0}^{\ell} b_j p^j$ for integers b_j with $0 \leq b_j \leq p-1$, and for each i write $m_i = \sum_{j=0}^{\ell} a_{ij} p^j$ for integers a_{ij} with $0 \leq a_{ij} \leq p-1$. Then the multinomial coefficient $\binom{m}{m_1, m_2, \dots, m_k}$ is coprime to p if and only if for each j with $0 \leq j \leq \ell$ we have $b_j = \sum_{i=1}^k a_{ij}$.*

By a *term* of the base- p expansion of a nonnegative integer m , we mean some $b_j p^j$ as in the above result where $b_j > 0$. When we speak of the union of the base- p expansions of multiple integers, we mean the multiset of all terms of all the integers. In case $p = 2$, the above result can be written in the following simpler way.

Corollary 2.2. *In the situation of Lemma 2.1, if $p = 2$ then $\binom{m}{m_1, m_2, \dots, m_k}$ is odd if and only if the base-2 expansions of m_i and $m_{i'}$ have no common terms whenever $i \neq i'$.*

We also use Hermite's classical criterion for permutation polynomials, as generalized to possibly non-prime finite fields by Dickson [2, §11]:

Lemma 2.3. *Let q be a prime power, and pick $f(X) \in \mathbb{F}_q[X]$. Then $f(X)$ permutes $\mathbb{F}_q$ if and only if both of the following hold:*

- *for each integer m such that $0 < m < q - 1$ and $\gcd(m, q) = 1$, the reduction of $f(X)^m \bmod X^q - X$ has degree less than $q - 1$; and*
- *$f(X)$ has exactly one root in $\mathbb{F}_q$.*

When applying Lemma 2.3, it is convenient to observe that if $g(X)$ is the reduction of $f(X)^m \bmod X^q - X$ then the coefficient of X^{q-1} in $g(X)$ equals the sum of the coefficients of $X^{i(q-1)}$ in $f(X)^m$ for all positive integers i .

We now prove Theorem 1.4 in case $q > 2$ is even and $b \neq 0$. This was shown in [1], but the short proof below has some new features, so we include it for the reader's convenience.

Lemma 2.4. *If $q = 2^k$ with $k > 1$ then $f(X) := X^{q+2} + bX^q + cX$ does not permute $\mathbb{F}_{q^2}$ for any $b, c \in \mathbb{F}_{q^2}$ with $b \neq 0$.*

Proof. We may assume $k > 2$, since if $k = 2$ then the only term of $f(X)^5$ having degree divisible by $q^2 - 1$ is X^{30} , so Lemma 2.3 implies that $f(X)$ does not permute $\mathbb{F}_{q^2}$. We will show that the only term of $f(X)^{2q-1}$ having degree divisible by $q^2 - 1$ is $b^{3q/2} X^{2q^2-2}$. Since $2q - 1 < q^2 - 1$, it follows via Lemma 2.3 that $f(X)$ does not permute $\mathbb{F}_{q^2}$.

It remains to determine the terms of $f(X)^{2q-1}$ of degree divisible by $q^2 - 1$. By the multinomial theorem,

$$f(X)^{2q-1} = \sum_{i=0}^{2q-1} \sum_{j=0}^{2q-1-i} \binom{2q-1}{i, j, 2q-1-i-j} b^j c^{2q-1-i-j} X^{i(q+2)+jq+2q-1-i-j}.$$

The term corresponding to some choice of i and j has degree $i(q+1) + j(q-1) + 2q-1$. If this degree is divisible by $q^2 - 1$ then it is divisible by both $q-1$ and $q+1$, which says that

$$2i + 1 \equiv 0 \pmod{q-1} \quad \text{and} \quad -2j - 3 \equiv 0 \pmod{q+1}.$$

These conditions may be rewritten as

$$i \equiv \frac{q}{2} - 1 \pmod{q-1} \quad \text{and} \quad j \equiv \frac{q}{2} - 1 \pmod{q+1}.$$

If $i = j = q/2 - 1$ then the multinomial coefficient $\binom{2q-1}{i, j, 2q-1-i-j}$ is divisible by 2, by Corollary 2.2. Note that if $i = j = q/2 - 1$ then

$$i(q+1) + j(q-1) + 2q-1 = \left(\frac{q}{2} - 1\right) \cdot 2q + 2q-1 = q^2 - 1.$$

If we leave i fixed, and add $q+1$ to j , then we increase $i(q+1)+j(q-1)+2q-1$ by q^2-1 . Likewise, if we leave j fixed, and add $q-1$ to i , then we increase $i(q+1)+j(q-1)+2q-1$ by q^2-1 . Since $f(X)^{2q-1}$ has degree $(q+2)(2q-1) = 2q^2+3q-2 < 3q^2-3$, any term of $f(X)^{2q-1}$ with degree divisible by q^2-1 must have degree $2q^2-2$, and the coefficient of X^{2q^2-2} is the sum of the contributions from the pairs $(i, j) \in \{(q/2-1, 3q/2), (3q/2-2, q/2-1)\}$. Thus this coefficient is

$$\binom{2q-1}{\frac{q}{2}-1, \frac{3q}{2}} b^{3q/2} + \binom{2q-1}{\frac{3q}{2}-2, \frac{q}{2}-1, 2} b^{q/2-1} c^2.$$

By Corollary 2.2, the second multinomial coefficient in the above expression is even since the base-2 expansion of $q/2-1$ includes the term 2 (because $k > 2$), but the first multinomial coefficient in the above expression is odd since the base-2 expansions of $q/2-1$ and $3q/2 = q + q/2$ have no common terms. Thus the only term of $f(X)^{2q-1}$ with degree divisible by q^2-1 is $b^{3q/2} X^{2q^2-2}$, so Lemma 2.3 implies that $f(X)$ does not permute $\mathbb{F}_{q^2}$. $\square$

Next we prove Theorem 1.4 in case q is odd and $b \neq 0$.

Lemma 2.5. *If q is an odd prime power then $f(X) := X^{q+2} + bX^q + cX$ does not permute $\mathbb{F}_{q^2}$ for any $b, c \in \mathbb{F}_{q^2}$ with $b \neq 0$.*

Proof. We will show that $f(X)^{q-1}$ is congruent mod $X^{q^2}-X$ to a polynomial of degree q^2-1 . By Hermite's criterion (Lemma 2.3), it follows that $f(X)$ does not permute $\mathbb{F}_{q^2}$.

By the multinomial theorem,

$$f(X)^{q-1} = \sum_{i=0}^{q-1} \sum_{j=0}^{q-1-i} \binom{q-1}{i, j, q-1-i-j} b^j c^{q-1-i-j} X^{i(q+2)+jq+q-1-i-j}.$$

Since $f(X)^{q-1}$ has degree $(q+2)(q-1) = q^2-1+q-1 < 2q^2-2$, any term of $f(X)^{q-1}$ with degree divisible by q^2-1 must have degree equal to q^2-1 . The summand corresponding to some choice of i and j has degree $i(q+1) + (j+1)(q-1)$. If this degree equals q^2-1 then it is divisible by both $q-1$ and $q+1$, so that $i = r(q-1)/2$ and $j+1 = s(q+1)/2$ for some integers $r \geq 0$ and $s > 0$. Conversely, for such i and j we have $i(q+1) + (j+1)(q-1) = (r+s)(q^2-1)/2$, which equals q^2-1 if and only if $r+s=2$. Moreover, for such i and j the hypothesis $q-1-i \geq j$ says that $q-1 \geq i+j = r(q-1)/2-1+s(q+1)/2 = (r+s)(q-1)/2-1+s = q-2+s$, so that $s \leq 1$. Thus $i(q+1) + (j+1)(q-1)$ equals q^2-1 if and only if $r=s=1$, so that $i = (q-1)/2$ and $j+1 = (q+1)/2$. Hence the coefficient of X^{q^2-1} in $f(X)^{q-1}$ is

$$\binom{q-1}{\frac{q-1}{2}, \frac{q-1}{2}} b^{(q-1)/2}.$$

Writing $q = p^k$ where p is prime, the base- p expansions of $q-1$ and $(q-1)/2$ are $\sum_{i=0}^{k-1} (p-1)p^i$ and $\sum_{i=0}^{k-1} \frac{p-1}{2} p^i$, respectively. By Lemma 2.1, it follows

that $\left(\frac{q-1}{2}, \frac{q-1}{2}\right)$ is coprime to p , so the coefficient of X^{q^2-1} in $f(X)^{q-1}$ is the product of $b^{(q-1)/2}$ with an element of $\mathbb{F}_q^*$. Hence if $b \neq 0$ then the reduction of $f(X)^{q-1} \bmod (X^{q^2} - X)$ has degree $q^2 - 1$, which by Lemma 2.3 implies that $f(X)$ does not permute $\mathbb{F}_{q^2}$. $\square$

We now prove Theorem 1.4.

Proof of Theorem 1.4. If $b = c = 0$ then $f(X) = X^{q+2}$ permutes $\mathbb{F}_{q^2}$ if and only if $\gcd(q+2, q^2-1) = 1$; since plainly $\gcd(q+2, q+1) = 1$, we have $\gcd(q+2, q^2-1) = \gcd(q+2, q-1) = \gcd(3, q-1)$, so that $f(X)$ permutes $\mathbb{F}_{q^2}$ if and only if $q \not\equiv 1 \pmod{3}$. If $b = 0 \neq c$ then the result is [16, Cor. 2.3]. Henceforth suppose $b \neq 0$. If q is odd then the result is Lemma 2.5. If q is even and $q > 2$ then the result is Lemma 2.4. Finally, if $q = 2$ and $b \neq 0$ then $f(X) \equiv bX^2 + (c+1)X \pmod{X^{q^2} - X}$, so that $f(X)$ induces a homomorphism φ from the additive group of $\mathbb{F}_{q^2}$ to itself, and any such φ is bijective if and only if its kernel is trivial, or equivalently $c = 1$. $\square$

3. BIJECTIONS INDUCED BY $(X^3 - aX - bY, Y^3 - cX - dY)$

In this section we prove Theorem 1.5. We begin with some terminology and tools used in our proofs. Let $f(X) \in \mathbb{F}_q[X]$ have degree $n > 0$, and assume that $\gcd(n, q) = 1$. If t is transcendental over $\overline{\mathbb{F}}_q$ then $f(X) - t$ has no multiple roots in $\overline{\mathbb{F}}_q(t)$, since its derivative is a nonzero polynomial in $\overline{\mathbb{F}}_q[X]$ and hence has no common roots with $f(X) - t$. The *geometric monodromy group* of $f(X)$ is the Galois group of $f(X) - t$ over $\overline{\mathbb{F}}_q(t)$, viewed as a group of permutations of the roots of $f(X) - t$. Recall that a subgroup G of S_n is *primitive* if the only partitions of $\{1, 2, \dots, n\}$ which are preserved by G are the trivial partitions consisting of either one n -element set or n one-element sets. Also, a subgroup G of S_n is *doubly transitive* if it is transitive on the set of ordered pairs of distinct elements of $\{1, 2, \dots, n\}$. The following translations between properties of $f(X)$ and properties of G are well known; see for instance [6, Thms. 6.10–6.12].

Lemma 3.1. *Let $f(X) \in \mathbb{F}_q[X]$ have degree $n > 0$, where $\gcd(n, q) = 1$, and let G be the geometric monodromy group of $f(X)$. Then the following hold:*

- G contains an n -cycle;
- G is primitive if and only if $f(X)$ cannot be written as $g(h(X))$ for any $g, h \in \overline{\mathbb{F}}_q[X]$ of degree less than n ;
- G is doubly transitive if and only if $(f(X) - f(Y))/(X - Y)$ is irreducible in $\overline{\mathbb{F}}_q[X, Y]$.

The following result is a special case of [5, Thm. 4], in light of the discussion about equivalent definitions in [5, §2]. The main ingredient in its proof is Weil's bound.

Lemma 3.2. *Let $f(X) \in \mathbb{F}_q[X]$ have degree $n > 0$. If $(f(X) - f(Y))/(X - Y)$ is irreducible in $\overline{\mathbb{F}_q}[X, Y]$ and*

$$q > \left(\frac{(n-2)(n-3) + \sqrt{(n-2)^2(n-3)^2 + 8n-12}}{2} \right)^2$$

then $f(X)$ does not permute $\mathbb{F}_q$.

Finally, we use the following simple result [2, §18, 22, and 57].

Lemma 3.3. *Let q be a prime power, n a positive integer, and $a \in \mathbb{F}_q^*$. Then X^n permutes $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$, and $X^3 - aX$ permutes $\mathbb{F}_q$ if and only if $3 \mid q$ and a is a nonsquare in $\mathbb{F}_q$.*

With these ingredients in hand, we now prove Theorem 1.5.

Proof of Theorem 1.5. First assume $bc = 0$. Since the hypothesis and conclusion are unchanged by interchanging the pairs (a, b) and (d, c) when $bc = 0$, we may assume that $b = 0$. Then φ is bijective if and only if both $X^3 - aX$ and $X^3 - dX$ permute $\mathbb{F}_q$, which by Lemma 3.3 says that either (1.5.1) and (1.5.2) holds.

Henceforth assume $bc \neq 0$. Then the first coordinate of $\varphi(x, y)$ takes value u if and only if $y = (x^3 - ax - u)/b$, in which case the second coordinate of $\varphi(x, y)$ is $H_u(x)$ where

$$H_u(X) := \left(\frac{X^3 - aX - u}{b} \right)^3 - cX - d \cdot \frac{X^3 - aX - u}{b}.$$

Therefore φ is bijective if and only if $H_u(X)$ permutes $\mathbb{F}_q$ for all $u \in \mathbb{F}_q$. If $q \equiv 0 \pmod{3}$ then

$$H_u(X) = b^{-3}X^9 - (a^3b^{-3} + db^{-1})X^3 - (c - dab^{-1})X - u^3b^{-3} + dub^{-1},$$

so that $H_u(X) - H_u(0)$ induces a homomorphism from the additive group of $\mathbb{F}_q$ to itself, and hence is bijective if and only if its kernel is trivial, which yields (1.5.3). Henceforth assume $q \not\equiv 0 \pmod{3}$.

We now prove the result for $q \leq 1793$. If $q = 2$ then $\varphi(x, y) = ((1+a)x + by, cx + (1+d)y)$ is a linear transformation of the $\mathbb{F}_2$ -vector space $\mathbb{F}_2^2$, and hence is bijective if and only if its determinant is nonzero, which yields (1.5.4). If $2 < q \leq 1793$ (and $3 \nmid q$) then we check via Magma that there are no $a, b, c, d \in \mathbb{F}_q$ for which $bc \neq 0$ and every $H_u(X)$ permutes $\mathbb{F}_q$. To speed up this program, we first compose on both sides with scalar multiples in order to reduce to the case that $b = 1$ and a is either 0, 1, or (for odd q) a prescribed nonsquare in $\mathbb{F}_q$.

Henceforth assume $q > 1793$. We now show that $H_u(X)$ is not the composition of two degree-3 polynomials in $\overline{\mathbb{F}_q}[X]$. Suppose to the contrary that $H_u(X) = g(h(X))$ for some $g, h \in \overline{\mathbb{F}_q}[X]$ of degree 3. By replacing $g(X)$ and $h(X)$ by $g(\rho(X))$ and $\rho^{-1}(h(X))$ for a suitably chosen degree-1 $\rho(X) \in \overline{\mathbb{F}_q}[X]$, we may assume that $h(X)$ is monic and $h(0) = 0$. Equating leading terms in $H_u(X) = g(h(X))$ shows that the leading coefficient of

$g(X)$ is b^{-3} . Equating terms of degrees 8 and 7 shows that $h(X) = X^3 - aX$. But this is impossible, since plainly $H_u(X) + cX$ is in $\overline{\mathbb{F}}_q[X^3 - aX]$, so that $H_u(X)$ cannot also be in $\overline{\mathbb{F}}_q[X^3 - aX]$.

We have shown that $H_u(X)$ is not the composition of two degree-3 polynomials in $\overline{\mathbb{F}}_q[X]$. Since $H_u(X)$ has degree 9, it follows that $H_u(X)$ is not the composition of two lower-degree polynomials in $\overline{\mathbb{F}}_q[X]$. By Lemma 3.1, the geometric monodromy group of $H_u(X)$ is a primitive subgroup of S_9 which contains a 9-cycle. But any such group is doubly transitive: this can be shown by directly checking all such groups, or alternately it is a special case of Schur's theorem (e.g., cf. [6, Thm. 6.5]). By Lemma 3.1, it follows that $(H_u(X) - H_u(Y))/(X - Y)$ is irreducible in $\overline{\mathbb{F}}_q[X, Y]$. Since $q > 1793$, Lemma 3.2 implies that $H_u(X)$ does not permute $\mathbb{F}_q$, which concludes the proof. $\square$

4. BIJECTIONS INDUCED BY $(X^3 - eXY^2 - aX - bY, Y^3 - cX - dY)$

In this section we prove Theorem 1.6. We begin with the following elementary lemmas.

Lemma 4.1. *Write $Q := 3^\ell$ for some $\ell \geq 3$. Let n_1, n_2, n_3, n_5, n_9 be non-negative integers for which $n_1 + 2n_2 + 3n_3 + 5n_5 + 9n_9 = Q - 1$ and the union of the base-3 expansions of the n_j 's consists of one copy of each 3^i with $1 \leq i \leq \ell - 2$ along with some partition of 2. Then the base-3 expansion of n_5 contains $Q/9$, and the base-3 expansion of n_9 contains $Q/27$.*

Proof. The sum of the n_j 's is $1 + (Q/3 - 1)/2 = (Q + 3)/6$. Since $Q - 1 \geq 9n_9$, we have $n_9 < Q/9$. It follows that the base-3 expansion of n_5 includes $Q/9$, since otherwise we obtain the contradiction

$$Q - 1 \leq 2\frac{Q}{9} + 9\left(\frac{Q + 3}{6} - \frac{Q}{9}\right) = \frac{13Q + 81}{18} < Q - 1.$$

Next, if $Q > 27$ then the base-3 expansion of n_9 includes $Q/27$, since otherwise we obtain the contradiction

$$\begin{aligned} Q - 1 &\leq 5\left(\frac{Q}{9} + \frac{Q}{27}\right) + 9\left(\frac{Q + 3}{6} - \frac{Q}{9} - \frac{Q}{27}\right) \\ &= \frac{49Q + 243}{54} \\ &< Q - 1. \end{aligned}$$

Finally, if $Q = 27$ then $Q - 1 - 5Q/9 = 11$ equals $n_1 + 2n_2 + 3n_3 + 5(n_5 - 3) + 9n_9$ where $n_1, n_2, n_3, n_5 - 3, n_9$ are nonnegative integers whose sum is 2. It follows that $n_2 = n_9 = 1$, so that $n_9 = Q/27$. $\square$

Lemma 4.2. *Write $Q := 3^\ell$ with $\ell \geq 5$. Let n_1, n_2, n_5, n_9 be nonnegative integers for which $n_1 + 2n_2 + 5n_5 + 9n_9 = Q - 1$ and the union of the base-3 expansions of the n_j 's consists of one copy of each 3^i with $0 \leq i \leq \ell - 2$ and $i \neq 2$, along with either one copy of $2 \cdot 9$ or two copies of 9. Then the base-3*

expansion of n_5 contains $Q/9$, and if $\ell \geq 6$ then the base-3 expansion of n_9 contains $Q/27$.

We omit the proof of Lemma 4.2, since it is nearly identical to that of Lemma 4.1.

We now use the above lemmas to prove the following result, which is of some interest for its own sake.

Proposition 4.3. *Let $q = 3^k$ for some $k \geq 1$, and pick $a, b, c, d \in \mathbb{F}_q$ with $ac \neq 0$. Then $f(X) := X^9 + aX^5 + bX^3 + cX^2 + dX$ does not permute $\mathbb{F}_q$.*

Proof. Suppose to the contrary that $f(X)$ permutes $\mathbb{F}_q$. We first apply Hermite's criterion (Lemma 2.3) with exponent $(q+3)/6$, noting that this exponent is a positive integer which is less than $q-1$. If $q = 3$ then we obtain the contradiction $c = 0$. If $q = 9$ then we obtain $-ab = 0$, so that $b = 0$; then Lemma 2.3 with exponents 4 and 5 yield $a^3(d+1) + a(d+1)^3 + c^4 = 0$ and $c^3(a^2 + (d+1)^2) = 0$, so that $a^2 = -(d+1)^2$ and thus $c^4 = 0$, contradiction. Henceforth assume $q > 9$. Then $g(X) := f(X)^{(q+3)/6}$ has degree $9(q+3)/6$, which is less than $2q-2$. Thus Lemma 2.3 implies that the coefficient of X^{q-1} in $g(X)$ is zero. Letting S be the set of all tuples of nonnegative integers $(n_1, n_2, n_3, n_5, n_9)$ such that $n_1 + n_2 + n_3 + n_5 + n_9 = (q+3)/6$ and $n_1 + 2n_2 + 3n_3 + 5n_5 + 9n_9 = q-1$, it follows that

$$(4.4) \quad \sum_{(n_1, n_2, n_3, n_5, n_9) \in S} \binom{\frac{q+3}{6}}{n_1, n_2, n_3, n_5, n_9} a^{n_5} b^{n_3} c^{n_2} d^{n_1} = 0.$$

Let T be the set of tuples $(n_1, n_2, n_3, n_5, n_9)$ in S for which $\binom{(q+3)/6}{n_1, n_2, n_3, n_5, n_9}$ is coprime to 3. Note that $(q+3)/6 = 1 + \sum_{i=0}^{k-2} 3^i$. By Lemma 2.1, T consists of the tuples $(n_1, n_2, n_3, n_5, n_9)$ in S for which the union of the base-3 expansions of the n_j 's consists of a single copy of each 3^i with $1 \leq i \leq k-2$ together with some partition of 2. Pick any $(n_1, n_2, n_3, n_5, n_9) \in T$. We prove by induction on i that if $0 < 2i \leq k-1$ then 3^{k-2i} is a term in the base-3 expansion of n_5 and 3^{k-1-2i} is a term in the base-3 expansion of n_9 . The base case $i = 1$ follows from Lemma 4.1. Now suppose $2 < 2i \leq k-1$. By the inductive hypothesis, we know that if $1 \leq j \leq i-1$ then the base-3 expansion of n_5 includes 3^{k-2j} and the base-3 expansion of n_9 includes 3^{k-1-2j} . Let n'_z be the least nonnegative residue of $n_z \bmod 3^{k-2i+1}$. Then $n'_1 + 2n'_2 + 3n'_3 + 5n'_5 + 9n'_9 = q-1 - 5 \sum_{j=1}^{i-1} 3^{k-2j} - 9 \sum_{j=1}^{i-1} 3^{k-1-2j} = q/3^{2i-2} - 1$, and the union of the base-3 expansions of the various n'_z consists of one copy of each 3^ℓ with $1 \leq \ell \leq k-2i$ along with some partition of 2. Also the hypothesis $2i \leq k-1$ says that $3 \leq k-2i+2$. Hence by Lemma 4.1 we conclude that the base-3 expansions of n_5 and n_9 include 3^{k-2i} and 3^{k-1-2i} , respectively. This concludes the induction.

If k is odd then, writing n'_5 and n'_9 for the least nonnegative residues of n_5 and $n_9 \bmod 3$, we have $n_1 + 2n_2 + 3n_3 + 5n'_5 + 9n'_9 = 11$ and $n_1 + n_2 + n_3 + n'_5 + n'_9 = 2$. Thus $n_2 = n'_9 = 1$ and $n_1 = n_3 = n'_5 = 0$. We have shown

that $n_1 = n_3 = 0$, $n_2 = 1$, $n_5 = \sum_{i=1}^{(k-1)/2} 3^{2i-1}$, and $n_9 = \sum_{i=0}^{(k-3)/2} 3^{2i}$. Conversely, it is easy to check that these n_j 's indeed yield a tuple in T . Thus (4.4) implies that $a^{n_5}c = 0$, contradiction.

Henceforth suppose k is even. Writing n'_5 and n'_9 for the least nonnegative residues of n_5 and n_9 mod 3, we have $n_1 + 2n_2 + 3n_3 + 5n'_5 + 9n'_9 = 8$ and $n_1 + n_2 + n_3 + n'_5 + n'_9 = 2$. Thus $n_3 = n'_5 = 1$ and $n_1 = n_2 = n'_9 = 0$, so $n_1 = n_2 = 0$, $n_3 = 1$, $n_5 = \sum_{i=0}^{k/2-1} 3^{2i}$, and $n_9 = \sum_{i=1}^{k/2-1} 3^{2i-1}$. Conversely, it is easy to check that this tuple of n_j 's yields an element of T . Thus (4.4) implies that $a^{n_5}b = 0$, so that $b = 0$.

Next, in case $k > 2$ is even and $b = 0$, we apply Lemma 2.3 with exponent $(q + 51)/6$, noting that this is a positive integer less than $q - 1$. In case $k = 4$, this yields the contradiction $-a^{12}c^{10} = 0$, so we assume henceforth that $k \geq 6$. Then $g(X) := f(X)^{(q+51)/6}$ has degree less than $2q - 2$, so Lemma 2.3 implies that the coefficient of X^{q-1} in $g(X)$ is zero. Letting S be the set of all tuples of nonnegative integers (n_1, n_2, n_5, n_9) such that $n_1 + n_2 + n_5 + n_9 = (q + 51)/6$ and $n_1 + 2n_2 + 5n_5 + 9n_9 = q - 1$, it follows that

$$(4.5) \quad \sum_{(n_1, n_2, n_5, n_9) \in S} \binom{\frac{q+51}{6}}{n_1, n_2, n_5, n_9} a^{n_5} c^{n_2} d^{n_1} = 0.$$

Let T be the set of tuples (n_1, n_2, n_5, n_9) in S for which $\binom{(q+51)/6}{n_1, n_2, n_5, n_9}$ is coprime to 3. Note that $(q + 51)/6 = 9 + \sum_{i=0}^{k-2} 3^i$. By Lemma 2.1, T consists of the tuples (n_1, n_2, n_5, n_9) in S for which the union of the base-3 expansions of the n_j 's consists of a single 3^i for each i with $0 \leq i \leq k - 2$ and $i \neq 2$, along with either one copy of $2 \cdot 9$ or two copies of 9. Now suppose that $(n_1, n_2, n_5, n_9) \in T$. Arguing as above, but now using Lemma 4.2, we conclude that the base-3 expansion of n_5 includes $3^{k-2}, 3^{k-4}, \dots, 3^4$, and the base-3 expansion of n_9 includes $3^{k-3}, 3^{k-5}, \dots, 3^5$. Writing n'_j for the least nonnegative residue of n_j mod 81, we have $n'_1 + 2n'_2 + 5n'_5 + 9n'_9 = 323$ and $n'_1 + n'_2 + n'_5 + n'_9 = 49$, where we know that for each $i \in \{0, 1, 3\}$ there is a unique j for which the base-3 expansion of n'_j includes 3^i , and moreover there is no j for which the base-3 expansion of n'_j includes $2 \cdot 3^i$. The unique solution is $(n'_1, n'_2, n'_5, n'_9) = (0, 10, 12, 27)$. Thus $n_1 = 0$, $n_2 = 10$, $n_5 = 3 + \sum_{i=1}^{k/2-1} 3^{2i}$, and $n_9 = \sum_{i=2}^{k/2-1} 3^{2i-1}$. Conversely, it is easy to check that these n_j 's yield an element of T , so that (4.5) gives the contradiction $a^{10}c^{n_5} = 0$. $\square$

We now prove Theorem 1.6.

Proof of Theorem 1.6. First suppose $c = 0$. The projection of the image of φ onto the second coordinate is surjective if and only if $Y^3 - dY$ permutes $\mathbb{F}_q$, which holds if and only if either $d = 0$ or d is a nonsquare in $\mathbb{F}_q$. Suppose that $Y^3 - dY$ permutes $\mathbb{F}_q$. Then φ is bijective if and only if, for each $y \in \mathbb{F}_q$, the polynomial $X^3 - (ey^2 + a)X$ permutes $\mathbb{F}_q$. By Lemma 3.3, this says that

$ey^2 + a$ is either zero or a nonsquare in $\mathbb{F}_q$ for each $y \in \mathbb{F}_q$. If $a = 0$ then this condition holds if and only if e is a nonsquare. Now assume $a \neq 0$. If $q = 3$ then $\{ey^2 + a : y \in \mathbb{F}_q\} = \{a, e + a\}$, so that φ is bijective if and only if both a and $e + a$ are in $\{0, -1\}$, which holds if and only if $a = -1$ and $e = 1$. We show now that φ is not bijective when $a \neq 0 = c$ and $q > 3$. Suppose otherwise. Since $a \neq 0$, the curve $X^2 = eY^2 + a$ is irreducible over $\overline{\mathbb{F}}_q$. The closure C of this curve in $\mathbb{P}^2$ is nonsingular, and has at most two $\mathbb{F}_q$ -rational points with $Y = \infty$. For any $x, y \in \mathbb{F}_q$ with $x^2 = ey^2 + a$, the hypothesis that $ey^2 + a$ is either zero or a nonsquare implies that $x = 0$. Since at most two elements $y \in \mathbb{F}_q$ satisfy $ey^2 + a = 0$, we conclude that C has at most four $\mathbb{F}_q$ -rational points. But C has genus 0, so it has $q + 1$ $\mathbb{F}_q$ -rational points, which is impossible since $q > 3$.

Henceforth suppose $c \neq 0$. For any $v \in \mathbb{F}_q$, the second coordinate of $\varphi(x, y)$ equals v if and only if $y^3 - cy - dy = v$, or equivalently $x = (y^3 - dy - v)/c$. Thus if the second coordinate of $\varphi(x, y)$ equals v then the first coordinate of $\varphi(x, y)$ is

$$c^{-3}(y^3 - dy - v)^3 - ec^{-1}(y^3 - dy - v)y^2 - ac^{-1}(y^3 - dy - v) - by.$$

Therefore φ is bijective if and only if, for each $v \in \mathbb{F}_q$, the polynomial $H_v(Y) := (Y^3 - dY - v)^3 - ec^2(Y^3 - dY - v)Y^2 - ac^2(Y^3 - dY - v) - bc^3Y$ permutes $\mathbb{F}_q$. We compute

$$H_v(Y) - H_v(0) = Y^9 - ec^2Y^5 + (edc^2 - ac^2 - d^3)Y^3 + ec^2vY^2 + (adc^2 - bc^3)Y.$$

Since c and e are nonzero, Proposition 4.3 implies that $H_v(Y)$ does not permute $\mathbb{F}_q$ for any $v \in \mathbb{F}_q^*$. Therefore φ is not bijective. $\square$

5. BIJECTIONS INDUCED BY $aX^{3q} + bX^{2q+1} + cX^{q+2} + dX^3$

In this section we prove Theorem 1.10. We first present the notation, terminology, and previous results we will use.

- q is a fixed prime power;
- μ_{q+1} denotes the set of $(q+1)$ -th roots of unity in $\mathbb{F}_{q^2}$;
- $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$ is the set of $\mathbb{F}_q$ -rational points on $\mathbb{P}^1$;
- for any $g(X) \in \overline{\mathbb{F}}_q(X)$, we write $g^{(q)}(X)$ for the rational function obtained from $g(X)$ by replacing each coefficient by its q -th power;
- the *degree* of a nonzero rational function $g(X)$ is the maximum of the degrees of $N(X)$ and $D(X)$, for any prescribed choice of coprime polynomials $N(X)$ and $D(X)$ such that $g(X) = N(X)/D(X)$.

The following result is a special case of [14, Lemma 2.1].

Lemma 5.1. *Write $f(X) = X^r B(X^{q-1})$ where r is a positive integer, q is a prime power, 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 following result encodes a procedure introduced in [15], which is spelled out in [17, Lemma 2.2].

Lemma 5.2. *Let q be a prime power, and write $g_0(X) = X^r B(X)^{q-1}$ where $r \in \mathbb{Z}$ and $B(X) \in \mathbb{F}_{q^2}[X]$. Then $g_0(X)$ permutes μ_{q+1} if and only if $B(X)$ has no roots in μ_{q+1} and $g(X) := X^r B^{(q)}(1/X)/B(X)$ permutes μ_{q+1} .*

The next two results are immediate consequences of [15, Lemmas 2.1 and 3.1].

Lemma 5.3. *The degree-one rational functions in $\overline{\mathbb{F}}_q(X)$ which permute μ_{q+1} are precisely the functions $\rho(X) = (\beta^q X + \alpha^q)/(\alpha X + \beta)$ where $\alpha, \beta \in \mathbb{F}_{q^2}$ satisfy $\alpha^{q+1} \neq \beta^{q+1}$.*

Lemma 5.4. *The degree-one rational functions in $\overline{\mathbb{F}}_q(X)$ which map $\mathbb{P}^1(\mathbb{F}_q)$ bijectively onto μ_{q+1} are $(\beta^q X + \alpha^q)/(\beta X + \alpha)$ with $\beta \in \mathbb{F}_{q^2}^*$ and $\alpha \in \mathbb{F}_{q^2}$ such that $\alpha/\beta \notin \mathbb{F}_q$. The degree-one rational functions in $\overline{\mathbb{F}}_q(X)$ which map μ_{q+1} bijectively onto $\mathbb{P}^1(\mathbb{F}_q)$ are $(\gamma X + \gamma^q)/(\delta X + \delta^q)$ with $\delta \in \mathbb{F}_{q^2}^*$ and $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma/\delta \notin \mathbb{F}_q$.*

The following result is [3, Thm. 1.3].

Lemma 5.5. *A degree-three $h(X) \in \mathbb{F}_q(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$ if and only if there exist degree-one $\rho, \eta \in \mathbb{F}_q(X)$ for which $\rho(h(\eta(X)))$ is one of the following:*

(5.5.1) X^3 where $q \not\equiv 1 \pmod{3}$;

(5.5.2) $\nu^{-1} \circ X^3 \circ \nu$ where $q \equiv 1 \pmod{3}$ and for some $\delta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ we have $\nu(X) = (X - \delta^q)/(X - \delta)$ and $\nu^{-1}(X) = (\delta X - \delta^q)/(X - 1)$;

(5.5.3) $X^3 - \alpha X$ where $3 \mid q$ and α is a nonsquare in $\mathbb{F}_q$.

Proof of Theorem 1.10. The “if” implication follows from Lemma 3.3. It remains to prove the “only if” implication. Thus, we assume in what follows that $f(X)$ permutes $\mathbb{F}_{q^2}$, so in particular a, b, c, d are not all zero. Write $B(X) := aX^3 + bX^2 + cX + d$, and write $\widehat{B}(X) := d^q X^3 + c^q X^2 + b^q X + a^q$, so that $\widehat{B}(X) = X^3 B^{(q)}(X^{-1})$. Let $C(X) := \gcd(B(X), \widehat{B}(X))$, where we may assume that $C(X)$ is monic. Write $g(X) := \widehat{B}(X)/B(X)$. By Lemmas 5.1 and 5.2, the hypothesis that $f(X)$ permutes $\mathbb{F}_{q^2}$ implies that $q \not\equiv 1 \pmod{3}$, $B(X)$ has no roots in μ_{q+1} , and $g(X)$ permutes μ_{q+1} . Since $B(X)$ has no roots in μ_{q+1} , also $C(X)$ has no roots in μ_{q+1} .

First suppose that $C(X)$ has a root $\gamma \in \overline{\mathbb{F}}_q^*$. Then $0 = B(\gamma)^q = B^{(q)}(\gamma^q) = \gamma^{3q} \widehat{B}(\gamma^{-q})$, so that $\widehat{B}(\gamma^{-q}) = 0$, and likewise $0 = \widehat{B}(\gamma)^q = \gamma^{3q} B(\gamma^{-q})$ implies $B(\gamma^{-q}) = 0$. Thus $C(\gamma^{-q}) = 0$, and we must have $\gamma^{-q} \neq \gamma$ since $C(X)$ has no roots in μ_{q+1} . Hence γ and γ^{-q} are distinct roots of $C(X)$. Since $\deg(g) = \max(\deg(B), \deg(\widehat{B})) - \deg(C) \leq 3 - \deg(C)$, and $g(X)$ must be nonconstant because it permutes μ_{q+1} , we conclude that $C(X) = (X - \gamma)(X - \gamma^{-q})$.

Now suppose that $\deg(g) < 3$. We claim that $B(X) = (\alpha X + \beta)(X - \gamma)(\gamma^q X - 1)$ for some $\alpha, \beta, \gamma \in \mathbb{F}_{q^2}$ with $\gamma \notin \mu_{q+1}$. If $\{a, d\} = \{0\}$ then the claim holds with $\alpha := -b$, $\beta := -c$, and $\gamma := 0$. If $\{a, d\} \neq \{0\}$ then $C(0) \neq 0$ and $\max(\deg(B), \deg(\widehat{B})) = 3$, so that $C(X)$ has a root $\gamma \in \overline{\mathbb{F}}_q^*$

and thus the previous paragraph yields $C(X) = (X - \gamma)(X - \gamma^{-q})$ and $\gamma \notin \mu_{q+1}$, which implies the claim since $C(X)$ divides $B(X)$. Thus the claim holds in every case. It is easy to check that $f(X) \equiv M(X) \circ X^{q+2} \circ L(X) \pmod{X^{q^2} - X}$ where $L(X) := X^q - \gamma X$ and $M(X) := ((\alpha\gamma + \beta)X^q + (\alpha + \gamma^q\beta)X)/(\gamma^{q+1} - 1)$. Plainly $L(X)$ and $M(X)$ are $\mathbb{F}_q$ -linear maps $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_{q^2}$, and they are bijective since $f(X)$ is bijective. Thus (1.10.1) holds.

Henceforth suppose that $\deg(g) = 3$. Pick any $z \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. By Lemma 5.4, $\theta(X) := (zX - z^q)/(X - 1)$ defines a bijection from μ_{q+1} onto $\mathbb{P}^1(\mathbb{F}_q)$, and $\theta^{-1}(X) := (X - z^q)/(X - z)$ defines the inverse bijection from $\mathbb{P}^1(\mathbb{F}_q)$ onto μ_{q+1} . Write $h(X) := \theta(X) \circ g(X) \circ \theta^{-1}(X)$, so that $\deg(h) = 3$ and $h(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$. It is easy to check that $h^{(q)}(X) = h(X)$, so that $h(X) \in \mathbb{F}_q(X)$. Since $q \not\equiv 1 \pmod{3}$, by Lemma 5.5 there exist degree-one $\hat{\rho}, \hat{\eta} \in \mathbb{F}_q(X)$ for which $\hat{\rho}(h(\hat{\eta}(X)))$ is either (5.5.1) or (5.5.3). It follows that there exist degree-one $\rho, \eta \in \mathbb{F}_{q^2}(X)$ such that $\rho^{-1}(g(\eta^{-1}(X)))$ is either (5.5.1) or (5.5.3), where in addition $\rho(\mathbb{P}^1(\mathbb{F}_q)) = \mu_{q+1}$ and $\eta(\mu_{q+1}) = \mathbb{P}^1(\mathbb{F}_q)$. By Lemma 5.4, we have $\rho(X) = (\beta^q X + \alpha^q)/(\beta X + \alpha)$ and $\eta(X) = (\gamma X + \gamma^q)/(\delta X + \delta^q)$ for some $\alpha, \beta, \gamma, \delta \in \mathbb{F}_{q^2}$ such that $\beta, \delta \neq 0$ and $\alpha\beta^{-1}, \gamma\delta^{-1} \notin \mathbb{F}_q$. Let $\tilde{\rho}: \mathbb{F}_q \times \mathbb{F}_q \rightarrow \mathbb{F}_{q^2}$ and $\tilde{\eta}: \mathbb{F}_{q^2} \rightarrow \mathbb{F}_q \times \mathbb{F}_q$ map $\tilde{\rho}: (x, y) \mapsto \beta x + \alpha y$ and $\tilde{\eta}: x \mapsto (\gamma x^q + \gamma^q x, \delta x^q + \delta^q x)$, so that $\tilde{\rho}$ and $\tilde{\eta}$ are $\mathbb{F}_q$ -linear. We have $g(X) = \rho(X) \circ (X^3 - eX) \circ \eta(X)$, where if $e \neq 0$ then $3 \mid q$ and e is a nonsquare in $\mathbb{F}_q$. Then it is easy to check that there is some $\varepsilon \in \mathbb{F}_{q^2}^*$ for which $\varepsilon \cdot f(X)$ induces the same function on $\mathbb{F}_{q^2}$ as does $\tilde{\rho} \circ (X^3 - eXY^2, Y^3) \circ \tilde{\eta}$. Since bijectivity of $f(X)$ implies bijectivity of $\varepsilon^{-1}\tilde{\rho}$ and $\tilde{\eta}$, this yields (1.10.2) if $e = 0$ and (1.10.3) if $e \neq 0$. $\square$

6. COMPLETE MAPPINGS

In this section we prove Theorems 1.1 and 1.3.

Proof of Theorem 1.1. We first prove the “if” implication. If $\gamma \in \mathbb{F}_{q^2}^*$ satisfies $\gamma^{2q-2} - \gamma^{q-1} + 1 = 0$ then $q \not\equiv 1 \pmod{3}$, and γX^{q+2} is a complete mapping of $\mathbb{F}_{q^2}$ by [16, Cor. 3.4]. Since $\mathbb{F}_q$ -linear conjugacy preserves the complete mapping property, it follows that the polynomials $f(X)$ in (1.1.1) are complete mappings. If (1.1.2) holds then both $f(X)$ and $f(X) + X$ induce homomorphisms from the additive group of $\mathbb{F}_{q^2}$ to itself, so that they permute $\mathbb{F}_{q^2}$ if and only if these homomorphisms have trivial kernel. The kernel of $f(X)$ is trivial because $a^{q+1} \neq d^{q+1}$, and the kernel of $f(X) + X$ is trivial because $(f(X) + X)/X$ has no roots in $\mathbb{F}_{q^2}^*$ by hypothesis. Thus $f(X)$ is a complete mapping of $\mathbb{F}_{q^2}$.

It remains to prove the “only if” implication. Henceforth we suppose that $f(X)$ is a complete mapping of $\mathbb{F}_{q^2}$. In particular, $f(X)$ permutes $\mathbb{F}_{q^2}$, so Theorem 1.10 implies that $f(X)$ is $\mathbb{F}_q$ -linearly equivalent to one of (1.10.1)–(1.10.3).

First suppose that $f(X)$ is (1.10.1) up to $\mathbb{F}_q$ -linear equivalence. Thus $q \not\equiv 1 \pmod{3}$ and $\rho \circ f(X) \circ \eta = X^{q+2}$ as maps on $\mathbb{F}_{q^2}$ for some automorphisms

ρ and η of $\mathbb{F}_{q^2}$ as an $\mathbb{F}_q$ -vector space. Since $\rho \circ \eta$ is an $\mathbb{F}_q$ -vector space automorphism of $\mathbb{F}_{q^2}$, there are $\alpha, \beta \in \mathbb{F}_{q^2}$ with $\alpha^{q+1} \neq \beta^{q+1}$ such that $\rho \circ \eta = \alpha X^q + \beta X$ as maps on $\mathbb{F}_{q^2}$. It follows that $\rho \circ (f(X) + X) \circ \eta = X^{q+2} + \alpha X^q + \beta X$ as maps on $\mathbb{F}_{q^2}$. Since $f(X) + X$ permutes $\mathbb{F}_{q^2}$, also $X^{q+2} + \alpha X^q + \beta X$ permutes $\mathbb{F}_{q^2}$, which by Theorem 1.4 implies that one of the following holds:

- (1) $q \not\equiv 1 \pmod{3}$, $\alpha = 0$, and β^{q-1} is a root of $X^3 - X^2 + X$;
- (2) $q = 2$, $\alpha \neq 0$, and $\beta = 1$.

Since $\alpha^{q+1} \neq \beta^{q+1}$, it follows that (1) holds and $\beta \neq 0$. Thus β^{q-1} is a root of $X^2 - X + 1$. Since $\rho = \beta \eta^{-1}$, it follows that $\eta^{-1} \circ f(X) \circ \eta = \beta^{-1} X^{q+2}$ as maps on $\mathbb{F}_{q^2}$, which gives (1.1.1).

Next suppose that $f(X)$ is (1.10.2) up to $\mathbb{F}_q$ -linear equivalence. Thus $q \not\equiv 1 \pmod{3}$ and $\rho \circ f(X) \circ \eta^{-1} = (X^3, Y^3)$ as maps on $\mathbb{F}_q \times \mathbb{F}_q$ for some $\mathbb{F}_q$ -vector space isomorphisms ρ and η from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q \times \mathbb{F}_q$. Since $\rho \circ \eta^{-1}$ is an $\mathbb{F}_q$ -vector space automorphism of $\mathbb{F}_q \times \mathbb{F}_q$, there exists $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \text{GL}_2(\mathbb{F}_q)$ such that $\rho \circ \eta^{-1}$ sends (x, y) to $(\alpha x + \beta y, \gamma x + \delta y)$ for any $x, y \in \mathbb{F}_q$. It follows that $\rho \circ (f(X) + X) \circ \eta^{-1} = (X^3 + \alpha X + \beta Y, Y^3 + \gamma X + \delta Y)$ as maps on $\mathbb{F}_q \times \mathbb{F}_q$. Since $f(X) + X$ permutes $\mathbb{F}_{q^2}$, also $(X^3 + \alpha X + \beta Y, Y^3 + \gamma X + \delta Y)$ permutes $\mathbb{F}_q \times \mathbb{F}_q$, so Theorem 1.5 implies that one of the following holds:

- (1) $q \equiv 0 \pmod{3}$, $\beta\gamma = 0$, and $-\alpha$ and $-\delta$ are nonsquares in $\mathbb{F}_q$;
- (2) $q \equiv 0 \pmod{3}$, $\beta\gamma \neq 0$, and no square in $\mathbb{F}_q$ is a root of the polynomial $X^4 + (\alpha^3 + \beta^2\delta)X + \beta^2(\alpha\delta - \beta\gamma)$;
- (3) $q = 2$, $\beta = \gamma = 1$, and $\alpha + \delta = 1$.

If (3) holds then it is easy to check that $f(X)$ is $\mathbb{F}_q$ -linearly conjugate to wX with $w \in \mathbb{F}_4 \setminus \mathbb{F}_2$, so that (1.1.1) holds. Henceforth we suppose that either (1) or (2) holds. Then $q \equiv 0 \pmod{3}$, so the map $\rho^{-1} \circ (X^3, Y^3) \circ \eta$ on $\mathbb{F}_{q^2}$ is the cube of an $\mathbb{F}_q$ -linear automorphism of $\mathbb{F}_{q^2}$, and hence is induced by a polynomial whose terms have degrees in $\{3, 3q\}$. Thus $f(X) = aX^{3q} + dX^3$. Since $f(X)$ permutes $\mathbb{F}_{q^2}$, we have $a^{q+1} \neq d^{q+1}$. Since $f(X) + X$ permutes $\mathbb{F}_{q^2}$, the polynomial $(f(X) + X)/X = aX^{3q-1} + dX^2 + 1$ has no roots in $\mathbb{F}_{q^2}^*$, so that (1.1.2) holds.

Finally, suppose that $f(X)$ is (1.10.3) up to $\mathbb{F}_q$ -linear equivalence. Thus $q \equiv 0 \pmod{3}$ and $\rho \circ f(X) \circ \eta^{-1} = (X^3 - eXY^2, Y^3)$ as maps on $\mathbb{F}_q \times \mathbb{F}_q$, where e is a nonsquare in $\mathbb{F}_q^*$ and ρ and η are $\mathbb{F}_q$ -vector space isomorphisms $\mathbb{F}_{q^2} \rightarrow \mathbb{F}_q \times \mathbb{F}_q$. Since $\rho \circ \eta^{-1}$ is an $\mathbb{F}_q$ -vector space automorphism of $\mathbb{F}_q \times \mathbb{F}_q$, there exists $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \text{GL}_2(\mathbb{F}_q)$ such that $\rho \circ \eta^{-1}$ sends (x, y) to $(\alpha x + \beta y, \gamma x + \delta y)$ for any $x, y \in \mathbb{F}_q$. It follows that $\rho \circ (f(X) + X) \circ \eta^{-1} = (X^3 - eXY^2 + \alpha X + \beta Y, Y^3 + \gamma X + \delta Y)$ as maps on $\mathbb{F}_q \times \mathbb{F}_q$. Since $f(X) + X$ permutes $\mathbb{F}_{q^2}$, also $(X^3 - eXY^2 + \alpha X + \beta Y, Y^3 + \gamma X + \delta Y)$ permutes $\mathbb{F}_q \times \mathbb{F}_q$, which is impossible by Theorem 1.6 since e is a nonsquare in $\mathbb{F}_q$ and $\alpha\delta \neq \beta\gamma$. $\square$

We conclude this paper by proving Theorem 1.3.

Proof of Theorem 1.3. First we prove the result when $q = 2$. If $q = 2$ then $f(X) \equiv (a + d)X^3 + bX^2 + cX \pmod{X^4 + X}$; since the only permutation polynomials over $\mathbb{F}_4$ of degree at most 3 which have a degree-1 term are the degree-1 polynomials, we see that $f(X)$ is a complete mapping over $\mathbb{F}_4$ if and only if (1.3.6) holds. If $q = 2$ then (1.3.2), (1.3.3), and (1.3.4) do not hold, and each of (1.3.1) and (1.3.5) implies (1.3.6). Thus the result is true when $q = 2$, so we assume henceforth that $q > 2$.

By Theorem 1.1, $f(X)$ is a complete mapping of $\mathbb{F}_{q^2}$ if and only if either (1.1.1) or (1.1.2) holds. Since (1.1.2) appears in the conclusion of Theorem 1.3, it remains to determine the possibilities for a, b, c, d when (1.1.1) holds. By definition, (1.1.1) holds if and only if

$$f(X) \equiv \frac{\lambda X^q - \beta^q X}{\lambda^{q+1} - \beta^{q+1}} \circ \gamma X^{q+2} \circ (\lambda X^q + \beta X) \pmod{X^{q^2} - X}$$

for some $\lambda, \beta, \gamma \in \mathbb{F}_{q^2}$ such that $\lambda^{q+1} \neq \beta^{q+1}$ and $\gamma^{2q-2} - \gamma^{q-1} + 1 = 0$. Since $q > 2$, the monomials X^{3q} , X^{2q+1} , X^{q+2} , and X^3 are pairwise incongruent mod $X^{q^2} - X$. Thus (1.1.1) holds if and only if there exist $\lambda, \beta, \gamma \in \mathbb{F}_{q^2}$ such that all of the following hold:

- (1) $\lambda^{q+1} \neq \beta^{q+1}$,
- (2) $\omega := -\gamma^{q-1}$ satisfies $\omega^2 + \omega + 1 = 0$,
- (3) $a(\lambda^{q+1} - \beta^{q+1}) = \lambda^2 \beta^{2q} (\gamma^q - \gamma)$,
- (4) $b(\lambda^{q+1} - \beta^{q+1}) = \lambda \beta^{2q+1} (\gamma^q - 2\gamma) + \lambda^{q+2} \beta^q (2\gamma^q - \gamma)$,
- (5) $c(\lambda^{q+1} - \beta^{q+1}) = 2\lambda^{q+1} \beta^{q+1} (\gamma^q - \gamma) + \lambda^{2q+2} \gamma^q - \beta^{2q+2} \gamma$,
- (6) $d(\lambda^{q+1} - \beta^{q+1}) = \lambda^{2q+1} \beta \gamma^q - \lambda^q \beta^{q+2} \gamma$.

We may assume that $q \not\equiv 1 \pmod{3}$, since this condition follows from (2) and also appears in the conclusion of Theorem 1.3. If $\lambda = 0$ and (2) holds then (1)–(6) hold if and only if $\beta \neq 0 = a = b = d$ and $c = \beta^{q+1} \gamma$. If $\beta = 0$ and (2) holds then (1)–(6) hold if and only if $\lambda \neq 0 = a = b = d$ and $c = \lambda^{q+1} \gamma^q$. Thus (1)–(6) hold with $\lambda\beta = 0$ if and only if (1.3.1) holds.

We now show that (1.3.2) holds if and only if $\gcd(q, 6) = 1$ and (1)–(6) hold with $\lambda\beta \neq 0$. It is straightforward to check that if $\gcd(q, 6) = 1$ and (1)–(6) hold with $\lambda\beta \neq 0$ then (1.3.2) holds. Conversely, suppose (1.3.2) holds. Then $24a^2d \neq 0$, so that $\gcd(q, 6) = 1$. Pick any $\gamma \in \mathbb{F}_{q^2}^*$ for which $\omega := -\gamma^{q-1}$ has order 3. Then it is routine to verify that

$$\delta := \frac{-\omega^2(b + 3d^q) \cdot (b + (1 + 2\omega)d^q)}{12a\gamma}$$

is in $\mathbb{F}_q^*$. Let β be any element of $\mathbb{F}_{q^2}^*$ such that $\beta^{q+1} = \delta$, and put

$$\lambda := \frac{2(1 - \omega)a\beta}{b + (1 + 2\omega)d^q}.$$

Then $\lambda \in \mathbb{F}_{q^2}^*$, and it is routine to verify that (1)–(6) hold.

Now suppose that $3 \mid q$. Then (1)–(6) imply $b = 0$, and also each of (1.3.3) and (1.3.4) implies $b = 0$. If (1)–(6) hold with $\lambda, \beta \neq 0$ then $\gamma^{q-1} = -1$, and d equals 0 if and only if $\lambda^{q+1} = -\beta^{q+1}$, in which case it is easy to check that (1.3.3) holds. Conversely, if (1.3.3) holds then $\gamma := c$ satisfies $\gamma^{q-1} = -1$, so (2) holds. Pick any $\beta \in \mathbb{F}_{q^2}^*$ with $\beta^{q+1} = -1$. By hypothesis, $(-a/c)^{(q^2-1)/2} = 1$, so that $-a/c$ is a square in $\mathbb{F}_{q^2}^*$ and thus we may choose $\lambda \in \mathbb{F}_{q^2}^*$ with $(\lambda/\beta)^2 = -a/c$. Then it is easy to check that (1)–(6) hold. If (1)–(6) hold with $\lambda, \beta, d \neq 0$ then it is easy to check that (1.3.4) holds, where $d^{4q+4} + a^4 d^{q+5}$ is the square of $\gamma^4 (\lambda\beta)^{2q+2} (\beta^{q+1} + \lambda^{q+1})^3 / (\beta^{q+1} - \lambda^{q+1})^3$. Conversely, if (1.3.4) holds then put $\gamma := 1/(ad^2)$, so that (2) holds. Let α be a square root of $d^{4q+4} + a^4 d^{q+5}$, and put $\delta := c\gamma^{-1} + \alpha$. Then $\delta \in \mathbb{F}_q^*$, so we may choose $\lambda \in \mathbb{F}_{q^2}^*$ with $\lambda^{q+1} = \delta$, and then put $\beta := \lambda(acd^2 - \delta - d^{2q+2})/(ad^{q+2})$. It is easy to check that (1)–(6) hold.

Finally, suppose q is even. It is routine to verify that (1)–(6) imply (1.3.5). Conversely, suppose (1.3.5) holds. If $b = 0$ then one can check that (1)–(6) hold for $\lambda = 0$, $\beta = 1$, and $\gamma = c$. Finally, if $b \neq 0$ then pick any $\omega \in \mathbb{F}_4 \setminus \mathbb{F}_2$. It is easy to check that (1)–(6) hold for $\gamma^2 = \omega c^{2q} + \omega^2 c^{q+1} + c^2$, $\beta = 1$, and $\lambda = (c + \gamma)/b^q$. This concludes the proof. $\square$

REFERENCES

- [1] C. H. Chan, Z. Ding, N. Li, X. Xie, M. Xiong, and M. E. Zieve, *On a class of complete permutation quadrinomials*, Finite Fields Appl. **110** (2026), Paper No. 102734, 19 pp. [2](#), [5](#)
- [2] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*, Ann. of Math. **11** (1897), 65–120. [4](#), [5](#), [8](#)
- [3] Z. Ding and M. E. Zieve, *Low-degree permutation rational functions over finite fields*, Acta Arith. **202** (2022), 253–280. [13](#)
- [4] Z. Ding and M. E. Zieve, *Determination of a class of permutation quadrinomials*, Proc. London Math. Soc. (3) **127** (2023), 221–260. [4](#)
- [5] X. Fan, *The Weil bound and non-exceptional permutation polynomials over finite fields*, arXiv:1811.12631v2, 6 Dec 2018. [7](#)
- [6] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Pitman Monogr. Surveys Pure Appl. Math. **65**, Longman Sci. & Tech., Harlow, 1993. [7](#), [9](#)
- [7] H. B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Stat. **13** (1942), 418–423. [1](#)
- [8] S. Markovski and A. Mileva, *Generating huge quasigroups from small non-linear bijections via extended Feisten function*, Quasigroups and related systems **17** (2009), 91–106. [1](#)
- [9] L. Mittenenthal, *Block substitutions using orthomorphic mapping*, Adv. Applied Math. **16** (1995), 59–71. [1](#)
- [10] L. Mittenenthal, *Nonlinear dynamic substitution devices and methods for block substitutions employing coset decompositions and direct geometric generation*, US Patent 5647001, 1997. [1](#)
- [11] C. P. Schnorr and S. Vaudenay, *Black box cryptanalysis of Hash networks based on multipermutations*, in: Advances in Cryptology—EUROCRYPT '94, Springer, Berlin, 1995, pp. 47–57. [1](#)

- [12] R. Shaheen and A. Winterhof, *Permutations of finite fields for check digit systems*, Des. Codes Cryptogr. **57** (2010), 361–371. [1](#)
- [13] S. Vaudenay, *On the Lai–Massey scheme*, in: Advances in Cryptology—ASIACRYPT ’99, Springer, Berlin, 1999, pp. 8–19. [1](#)
- [14] M. E. Zieve, *Some families of permutation polynomials over finite fields*, Int. J. Number Theory **4** (2008), 851–857. [12](#)
- [15] M. E. Zieve, *Permutation polynomials on $\mathbb{F}_q$ induced from Rédei function bijections on subgroups of $\mathbb{F}_q^*$* , Monatsh. Math., to appear. arXiv:1310.0776v2, 7 Oct 2013. [12](#), [13](#)
- [16] M. E. Zieve, *Permutation polynomials induced from permutations of subfields, and some complete sets of mutually orthogonal latin squares*, arXiv:1312.1325v3, 9 Dec 2013. [2](#), [7](#), [14](#)
- [17] M. E. Zieve, *A note on the paper* arXiv:2112.14547, arXiv:2201.01106v2, 2 Aug 2022. [12](#)

SCHOOL OF MATHEMATICS AND STATISTICS, HUNAN NORMAL UNIVERSITY, CHANGSHA 410081, CHINA

Email address: ding8191@qq.com

SCHOOL OF MATHEMATICS, HUNAN UNIVERSITY, CHANGSHA 410082, CHINA

Email address: weixiong@amss.ac.cn

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, 530 CHURCH STREET, ANN ARBOR, MI 48109-1043 USA

Email address: zieve@umich.edu

URL: <https://dept.math.lsa.umich.edu/~zieve/>