GANITA,Vol.75(1), 2025, 175-179

ON SOME TRINOMIALS IN CHARACTERISTIC 2

ZHIGUO DING ✉ **and MICHAEL E. ZIEVE**

Abstract

For each q of the form 4^k, we determine which of five trinomials permute $\mathbb{F}_q$. Our result corrects the results of a recent paper by Sharma, Gupta, and Kumar.

2010 *Mathematics subject classification:* primary 11T06; secondary 11C08, 11T55.

Keywords and phrases: Permutation polynomial, finite field.

1. Introduction

For any prime power q, a polynomial $f(X) \in \mathbb{F}_q[X]$ is called a *permutation polynomial* if the associated function $f\colon c \to f(c)$ from $\mathbb{F}_q$ to itself is bijective. The recent paper [4] includes five theorems, each of which asserts that certain polynomials permute $\mathbb{F}_{4^k}$ for either all k, all odd k, or all k not divisible by 4. In this note we show that these theorems are false, and that in fact none of the polynomials in these theorems permute $\mathbb{F}_{4^k}$ for any $k > 2$. To do this, we introduce a general procedure relying on simple computer calculations.

We now describe the polynomials in question. Write

$$B_1(X) := X^5 + X^2 + 1;$$
$$B_2(X) := X^5 + X^3 + 1;$$
$$B_3(X) := X^3 + X + 1.$$

The polynomials addressed in [4] are as follows, where $q := 2^k$:

$$f_1(X) := X^5 B_1(X^{q-1});$$
$$f_2(X) := X^5 B_2(X^{q-1});$$
$$f_3(X) := X^6 B_1(X^{q-1});$$
$$f_4(X) := X^4 B_2(X^{q-1});$$
$$f_5(X) := X^5 B_3(X^{q-1}).$$

The following result is the combination of Theorems 3.1–3.5 of [4].

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

Theorem 1.1. *Write $q = 2^k$ where k is a positive integer, and pick $i \in \{1, 2, 3, 4, 5\}$. Then $f_i(X)$ permutes $\mathbb{F}_{q^2}$ if and only if one of the following holds:*

- *$i \in \{1, 2, 5\}$ and $4 \nmid k$;*
- *$i = 3$ and $2 \nmid k$;*
- *$i = 4$.*

However, Theorem 1.1 is not true. In this paper we prove the following result, which determines when $f_i(X)$ permutes $\mathbb{F}_{q^2}$.

Theorem 1.2. *Write $q = 2^k$ where k is a positive integer, and pick $i \in \{1, 2, 3, 4, 5\}$. Then $f_i(X)$ permutes $\mathbb{F}_{q^2}$ if and only if one of the following holds:*

- *$i \in \{1, 2\}$ and $k \in \{1, 2\}$;*
- *$i \in \{4, 5\}$ and $k = 2$.*

We emphasize that Theorem 1.2 goes far beyond merely disproving the results of [4]. For instance, to disprove Theorem 1.1, it suffices to observe that if $q = 2$ then all three elements $c \in \mathbb{F}_{q^2}^*$ satisfy $f_3(c) = 1$. In order to prove Theorem 1.2, one must address all values k, rather than just a single k, and in fact the proof of Theorem 1.2 relies on some nontrivial tools from Galois theory and algebraic geometry.

2. Background material

In this section, we recall some previous results which are used in our proof of Theorem 1.2.

We use the following notation throughout this paper:

- q is a prime power;
- $\overline{\mathbb{F}}_q$ is an algebraic closure of $\mathbb{F}_q$;
- $\mathbb{P}^1(\mathbb{F}_q) := \mathbb{F}_q \cup \{\infty\}$;
- μ_{q+1} is the set of $(q+1)$-th roots of unity in $\mathbb{F}_{q^2}^*$.

We begin with the following special case of [5, Lemma 2.1].

Lemma 2.1. *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 result gives a useful reformulation of the condition in Lemma 2.1 that $g_0(X)$ permutes μ_{q+1}. This type of reformulation first appeared in [6].

Lemma 2.2. *For any integer r and any $B(X) \in \mathbb{F}_q[X]$ such that $B(X)$ and $B(1/X)$ have no common zeroes in μ_{q+1}, the function $g_0(X) := X^r B(X)^{q-1}$ permutes μ_{q+1} if and only if $g(X) := X^r B(1/X)/B(X)$ permutes μ_{q+1}.*

Proof. Since $B(X) \in \mathbb{F}_q[X]$, we have $B(X)^q = B(X^q)$. Thus, each $c \in \mu_{q+1}$ satisfies $B(c)^q = B(c^q) = B(1/c)$, so we must have $B(c) \neq 0$, since otherwise c would be a common zero of $B(X)$ and $B(1/X)$. Hence $g_0(X)$ and $g(X)$ induce the same function on μ_{q+1}, which implies the result. □

Definition 2.3. For any field K and any nonzero $f(X) \in K(X)$, by the numerator and denominator of $f(X)$ we mean the unique coprime $N(X), D(X) \in K[X]$ such that $D(X)$ is monic and $f(X) = N(X)/D(X)$, and then the *degree* of $f(X) \in K(X)$ is $\max(\deg(N), \deg(D))$.

The next result is a special case of [6, Lemma 3.1].

Lemma 2.4. *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 next result is well-known; for instance, cf. [2, Cor. 2.8].

Lemma 2.5. *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 $\rho^{-1}(X) = (dX - b)/(-cX + a)$.*

Definition 2.6. A polynomial $H(X, Y) \in \mathbb{F}_q[X, Y]$ is called *absolutely irreducible* if $H(X, Y)$ is irreducible in $\overline{\mathbb{F}}_q[X, Y]$.

Definition 2.7. A rational function $f(X) \in \mathbb{F}_q(X)$ is *exceptional* over $\mathbb{F}_q$ if the only absolutely irreducible polynomials in $\mathbb{F}_q[X, Y]$ which divide the numerator of $f(X) - f(Y)$ are the polynomials $c \cdot (X - Y)$ with $c \in \mathbb{F}_q^*$.

Definition 2.8. A rational function $f(X) \in \mathbb{F}_q(X)$ is *separable* if $f(X) \notin \mathbb{F}_q(X^p)$, where p is the characteristic of $\mathbb{F}_q$.

The following result is a special case of [3, Thm. 2.5].

Lemma 2.9. *Let q be a prime power, and let $n \geq 2$ be an integer such that $\sqrt{q} > 2(n-2)^2 + 1$. If $f(X) \in \mathbb{F}_q(X)$ is a separable rational function of degree n which permutes $\mathbb{P}^1(\mathbb{F}_q)$, then $f(X)$ is exceptional over $\mathbb{F}_q$.*

3. Proof of Theorem 1.2

It is routine to verify the result via computer when $k < 11$, so in what follows we assume $k \geq 11$. Writing $q := 2^k$, we must show that each $f_i(X)$ does not permute $\mathbb{F}_{q^2}$. In order to obtain a contradiction, assume that i has been chosen so that $f_i(X)$ permutes $\mathbb{F}_{q^2}$.

Pick $w \in \overline{\mathbb{F}}_q$ such that $w^q = w + 1$. Note that then $w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. Write $\rho(X) := (wX + w^q)/(X + 1)$ and $\rho^{-1}(X) := (X + w^q)/(X + w)$. By Lemmas 2.4 and 2.5, $\rho(X)$ induces a bijection from μ_{q+1} to $\mathbb{P}^1(\mathbb{F}_q)$ whose inverse is induced by $\rho^{-1}(X)$. By definition, $f_i(X) = X^r B_j(X^{q-1})$ for some $r \in \{4, 5, 6\}$ and some $j \in \{1, 2, 3\}$. Write $g_i(X) := X^r B_j(1/X)/B_j(X)$, and write $h_i(X) := \rho(X) \circ g_i(X) \circ \rho^{-1}(X)$.

We now show that $h_i(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$. To this end, we first show that $B_j(X)$ and $B_j(1/X)$ have no common zeroes in $\overline{\mathbb{F}}_q^*$. We have $B_3(X) + X^3 B_3(1/X) = X^2 + X$, and if $j \in \{1, 2\}$ then $B_j(X) + X^5 B_j(1/X) = X^3 + X^2$. Thus, regardless of the value of j, since $B_j(1) = 1 \neq 0$ it follows that $B_j(X)$ and $B_j(1/X)$ have no common zeroes in $\overline{\mathbb{F}}_q^*$. Since

$B_j(X) \in \mathbb{F}_q[X]$ and $f_i(X)$ permutes $\mathbb{F}_{q^2}$, Lemmas 2.1 and 2.2 imply that $g_i(X)$ permutes μ_{q+1}, so that $h_i(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$.

We have

$$g_1(X) := \frac{X^5+X^3+1}{X^5+X^2+1} = \frac{1}{g_2(X)},$$
$$g_3(X) := \frac{X^6+X^4+X}{X^5+X^2+1} = \frac{1}{g_4(X)},$$
$$g_5(X) := \frac{X^5+X^4+X^2}{X^3+X+1}.$$

Since $B_j(X)$ and $B_j(1/X)$ have no common zeroes in $\overline{\mathbb{F}}_q^*$, the polynomials displayed above whose ratio is $g_i(X)$ are in fact the numerator and denominator of $g_i(X)$. In particular, we have $\deg(h_i) = \deg(g_i) \in \{5, 6\}$, and by inspection we see that $g_i(X)$ is separable, which implies that $h_i(X)$ is separable as well.

Next we show that $h_i(X)$ is in $\mathbb{F}_q(X)$. To this end, note that $v := w^2 + w$ is in $\mathbb{F}_q$, since $v = w(w+1)$ so that $v^q = w^q(w^q+1) = (w+1)w = v$. Now a simple computation shows that $h_i(X) \in \mathbb{F}_2(v)(X)$, so that $h_i(X) \in \mathbb{F}_q(X)$. This computation can be done by hand, or by the following program using the computer algebra package Magma [1].

```
K<w>:=FunctionField(GF(2));
wq:=w+1;
v:=w^2+w;
_<x>:=FunctionField(K);
rho:=(w*x+wq)/(x+1);
rhoinv:=(x+wq)/(x+w);
H:={0,1,v,v+1,v^2,v^2+1,v^2+v,v^2+v+1,v^3,v^3+v+1};
for g in [(x^5+x^3+1)/(x^5+x^2+1), (x^5+x^2+1)/(x^5+x^3+1),
          (x^6+x^4+x)/(x^5+x^2+1), (x^5+x^2+1)/(x^6+x^4+x),
          (x^5+x^4+x^2)/(x^3+x+1)]
   do h:=Evaluate(rho,Evaluate(g,rhoinv));
      {i in H: i in Coefficients(Numerator(h)) cat
                    Coefficients(Denominator(h))};
end for;
```

We have shown that $h_i(X)$ is a separable rational function in $\mathbb{F}_q(X)$ of degree n, where $n \in \{5, 6\}$, and that $h_i(X)$ permutes $\mathbb{P}^1(\mathbb{F}_q)$. Since $q = 2^k$ with $k \geq 11$, Lemma 2.9 implies that $h_i(X)$ is exceptional over $\mathbb{F}_q$. Since $n > 2$, it follows that the numerator of $(h_i(X) - h_i(Y))/(X - Y)$ is not absolutely irreducible. Thus the numerator of $(g_i(X) - g_i(Y))/(X - Y)$ also cannot be irreducible in $\overline{\mathbb{F}}_q[X, Y]$. However, this contradicts the output of the following Magma program, which shows that the numerator of $(g_i(X)-g_i(Y))/(X-Y)$ is an absolutely irreducible polynomial in $\mathbb{F}_2[X, Y]$.

```
P<x,y>:=AffineSpace(GF(2),2);
```

```
for g in [(x^5+x^3+1)/(x^5+x^2+1), (x^6+x^4+x)/(x^5+x^2+1),
          (x^5+x^4+x^2)/(x^3+x+1)] do
   g2:=(g-Evaluate(g,[y,y]))/(x-y);
   IsAbsolutelyIrreducible(Curve(P,Numerator(g2)));
end for;
```

This contradiction concludes the proof of Theorem 1.2.

REMARK 3.1. *Our proof of Theorem 1.2 relies on two Magma programs. If one preferred, one could replace these programs with theoretical arguments. However, such arguments would require significantly more space than the short proof in the present paper, and also would require introducing additional concepts and background results.*

Author contributions:
Conceptualisation: Z. Ding, M. E. Zieve ; *Software:* M. E. Zieve ; *Writing-Original Draft:* Z. Ding, M. E. Zieve

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997) 235–265.

[2] Z. Ding and M. E. Zieve, *Low-degree permutation rational functions over finite fields*, Acta Arith. **202** (2022) 253–280.

[3] R. M. Guralnick, T. J. Tucker, and M. E. Zieve, *Exceptional covers and bijections on rational points*, Int. Math. Res. Notices **2007** (2007) Art. ID rnm004, 20 pp.

[4] P. L. Sharma, S. Gupta, and S. Kumar, *Some new classes of permutation trinomials over* $\mathbb{F}_{2^{2m}}$, GANITA **73** (2023) 141–147.

[5] M. E. Zieve, *Some families of permutation polynomials over finite fields*, Int. J. Number Theory **4** (2008) 851–857.

[6] M. E. Zieve, *Permutation polynomials on* $\mathbb{F}_q$ *induced from Rédei function bijections on subgroups of* $\mathbb{F}_q^*$, arXiv:1310.0776v2, 7 Oct 2013.

Zhiguo Ding, School of Mathematics and Statistics, Central South University, Changsha, 410075 China
e-mail: ding8191@csu.edu.cn

Michael E. Zieve, Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043 USA
e-mail: zieve@umich.edu