Applicable Algebra in Engineering, Communication and Computing (2024) 35:821–832
https://doi.org/10.1007/s00200-022-00592-1

ORIGINAL PAPER

On a special type of permutation rational functions

Nurdagül Anbar[1]

Received: 20 August 2022 / Revised: 4 November 2022 / Accepted: 5 November 2022 /
Published online: 16 December 2022

Abstract

Let p be a prime and n be a positive integer. We consider rational functions $f_b(X) = X + 1/(X^p - X + b)$ over $\mathbb{F}_{p^n}$ with $\mathrm{Tr}(b) \neq 0$. In Hou and Sze (Finite Fields Appl 68, Paper No. 10175, 2020), it is shown that $f_b(X)$ is not a permutation for $p > 3$ and $n \geq 5$, while it is for $p = 2, 3$ and $n \geq 1$. It is conjectured that $f_b(X)$ is also not a permutation for $p > 3$ and $n = 3, 4$, which was recently proved sufficiently large primes in Bartoli and Hou (Finite Fields Appl 76, Paper No. 101904, 2021). In this note, we give a new proof for the fact that $f_b(X)$ is not a permutation for $p > 3$ and $n \geq 5$. With this proof, we also show the existence of many elements $b \in \mathbb{F}_{p^n}$ for which $f_b(X)$ is not a permutation for $n = 3, 4$.

Keywords Function fields/curves · Permutation polynomials · Rational places/points

Mathematics Subject Classification 11T06 · 14H05

1 Introduction

Let p be a prime, and let $\mathbb{F}_{p^n}$ be the finite field with p^n elements. A polynomial $P(X) \in \mathbb{F}_{p^n}[X]$ is called a *permutation polynomial* of $\mathbb{F}_{p^n}$ if the associated map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^n}$ defined by $\alpha \mapsto P(\alpha)$ is a bijection. For short we will say that $P(X)$ is a permutation of $\mathbb{F}_{p^n}$. Permutation polynomials over finite fields have been studied widely in the last decades, especially due to their applications in combinatorics, coding theory and symmetric cryptography, see [6, 7] and references therein.

The theory of algebraic curves is one of the main tools to show that $P(X)$ is not a permutation of certain finite fields, for instance, see [2]. The well-known approach can be summarized as follows:

For a given $P(X) \in \mathbb{F}_{p^n}[X]$, we define the bivariate polynomial

✉ Nurdagül Anbar
nurdagulanbar2@gmail.com

[1] Sabancı University, MDBF, Orhanlı, Tuzla, 34956 Istanbul, Turkey

$$g(X,Y)=\frac{P(X)-P(Y)}{X-Y}\in\mathbb{F}_{p^n}[X,Y]. \tag{1.1}$$

Suppose that $g(X, Y)$ in Equation (1.1) has an absolutely irreducible factor $f(X,Y)\in\mathbb{F}_{p^n}[X,Y]$. Let $\mathcal{X}$ be the absolutely irreducible curve defined by $f(X, Y)$. Then the Hasse-Weil bound [9, Theorem 5.2.3] together with Bezout's theorem implies that there exists an affine point $(x,y)\in\mathbb{F}_{p^n}\times\mathbb{F}_{p^n}$ of $\mathcal{X}$ with $x\neq y$ if p^n is sufficiently large compared to the degree of $f(X, Y)$. This proves that $P(x)=P(y)$ for some $x,y\in\mathbb{F}_{p^n}$ with $x\neq y$, hence P is not a permutation of $\mathbb{F}_{p^n}$. We remark that in this approach, we require $P(X)$ to have a small degree to guarantee that the absolutely irreducible factor $f(X, Y)$ has a sufficiently small degree compared to p^n.

Special interest is given to the polynomials of the form

$$P(X)=L(X)+G(X)^k$$

for a linearized polynomial $L(X)$ and a polynomial $G(X)$ over $\mathbb{F}_{p^n}$, see [1] and references therein. Particularly, the case $P(X)=X+(X^p-X+b)^k$, i.e., $L(X)=X$ and $G(X)=(X^p-X+b)$ with $\mathrm{Tr}(b)\neq 0$, where $\mathrm{Tr}(z)=z+z^p+\cdots+z^{p^{n-1}}$ the absolute trace from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$. There is a series of papers devoted to the classification of these permutation polynomials, see [5] and references therein. In the case $k=p^n-2$ the degree of the polynomial is large compared to the size of the finite field, hence one can not directly apply the above method. As $\mathrm{Tr}(b)\neq 0$, the polynomial X^p-X+b has no root in $\mathbb{F}_{p^n}$. Hence, for any $x\in\mathbb{F}_{p^n}$, we can denote the polynomial $P(X)=X+(X^p-X+b)^{p^n-2}$ as a rational function

$$f_b(x)=x+\frac{1}{x^p-x+b}. \tag{1.2}$$

We also refer to [5] and references therein for the recent work on $f_b(X)$ given in Equation (1.2). It is shown in [10] that $f_b(X)$ is a permutation of $\mathbb{F}_{p^n}$ for $p=2,3$ and any integer $n\geq 1$. Then Hou and Sze [5] have studied the polynomials $f_b(X)$ for $p>3$ and arrived at the following result.

Theorem A: Let $p>3$ and $b\in\mathbb{F}_{p^n}$ such that $\mathrm{Tr}(b)\neq 0$.

(i) $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$ if $n\geq 5$.
(ii) $f_b(X)$ is a permutation of $\mathbb{F}_{p^2}$ if and only if $\mathrm{Tr}(b)=\pm 1$.

Then according to MAGMA results, the authors conjectured that $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$ for $n=3,4$. Recently, it is shown in [3] that the conjecture is true for large primes p, namely $p\geq 1{,}734{,}097$ for $n=3$ and $p\geq 100{,}018{,}663$ for $n=4$.

In this paper, we represent a new proof for the result of Theorem A/(i). The proof depends on the theory of curves, their function fields and the correspondence between the rational points of curves and the rational places of their function fields. We relate the permutation property of $f_b(X)$ to the splitting property of special rational places. With the method of the proof, we also show the existence of many elements $b\in\mathbb{F}_{p^n}$ for which $f_b(X)$ is not a permutation for $n=3,4$. More precisely, we prove the following theorem.

Theorem 1.1 *Let $p > 3$ be a prime.*

(i) *If $n \geq 5$ then $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$ for any $b \in \mathbb{F}_{p^n}$ with* $\mathrm{Tr}(b) \neq 0$.

(ii) *For $n = 3$ (respectively, $n = 4$), there are at least $p^{n-1}(\sqrt{p} - 3)/2$ (respectively, $p^n/3$) elements $b \in \mathbb{F}_{p^n}$ for which $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$.*

The paper is organized as follows: In Sect. 2, we investigate two curves $\mathcal{X}$ and $\mathcal{E}_d$ and their function fields F and E_d. In Sect. 3, we relate splitting property of rational places of F in E_d with the permutation property of rational functions $f_b(X)$. Then we give the Proof of Theorem 1.1 by showing the existence of such a rational place.

2 Special curves and their function fields

In this section, we study function field extensions and their compositum. For the notations and well-known facts about function fields, as a general reference, we refer to [4, 9].

Let F be a function field over $\mathbb{F}_{p^n}$. We denote by $\bar{\mathbb{F}}$ the algebraic closure of $\mathbb{F}_{p^n}$. If $F \cap \bar{\mathbb{F}} = \mathbb{F}_{p^n}$ then $\mathbb{F}_{p^n}$ is called the full constant field of F. A place P of F is called rational if its residue field is $\mathbb{F}_{p^n}$. For a function field F with full constant field $\mathbb{F}_{p^n}$, the well-known Hasse-Weil bound [9, Theorem 5.2.3] states that the number $N(F)$ of rational places satisfies

$$p^n + 1 - 2g(F)p^{n/2} \leq N(F) \leq p^n + 1 + 2g(F)p^{n/2},$$

where $g(F)$ is the genus of F.

Let E/F be a finite separable extension of function fields of degree $[E : F] = r$. The extension E/F is called tame if there is no wild ramified place, i.e., the ramification index is not divisible by p. A place P of F splits completely in E if there are r distinct places $R_1, \ldots, R_r$ of E lying over P. By the Fundamental Equality [9, Theorem 3.1.11], if a rational place P splits completely in E then any place lying over P is rational.

From now on, we always suppose that p is a prime with $p > 3$.

2.1 The curve $\mathcal{X}$ and its function field F

Let $\mathcal{X}$ be the curve defined by the equation $g(Z, W) = Z(Z + W)(W^{p-1} - 1) - 1$ and F be the function field of $\mathcal{X}$. That is, $F = \mathbb{F}_{p^n}(w, z)$ with $z(z + w)(w^{p-1} - 1) = 1$. We continue with the analysis of the separability of some polynomials to calculate the genus of F.

Lemma 2.1 *Let* $h_\beta(T) = T^2 + \beta T - 1/(\beta^{p-1} - 1) \in \bar{\mathbb{F}}[T]$, *where* $\beta^{p-1} \neq 1$. *Then there exist* $p + 1$ *elements* $\beta \in \bar{\mathbb{F}}$ *for which* $h_\beta(T)$ *is not a separable polynomial.*

Proof We denote by $h'_\beta(T)$ the derivative of $h_\beta(T)$, i.e., $h'_\beta(T) = 2T + \beta$. The polynomial $h_\beta(T)$ is not separable if and only if $h_\beta(T)$ and $h'_\beta(T)$ have a common root in $\bar{\mathbb{F}}$, say $T = \gamma$. Note that $h'_\beta(\gamma) = 0$ if and only if $\gamma = -\beta/2$. Then

$$h_\beta(\gamma) = h_\beta(-\beta/2) = -\frac{\beta^2}{4} - \frac{1}{\beta^{p-1} - 1} = 0$$

if and only if $\beta^2(\beta^{p-1} - 1) + 4 = \beta^{p+1} - \beta^2 + 4 = 0$. That is, β is a root of the polynomial $f(T) = T^{p+1} - T^2 + 4$. We now observe that $f(T)$ is separable, i.e., $f(T)$ has exactly $p + 1$ distinct roots in $\bar{\mathbb{F}}$. This implies the existence of $p + 1$ elements β for which $h_\beta(T)$ is not separable. Note that β is a multiple root $f(T)$ if and only if β is also a root of the derivative $f'(T) = T^p - 2T$, i.e., $\beta^p = 2\beta$. Then we have

$$f(\beta) = \beta^{p+1} - \beta^2 + 4 = \beta^2 + 4 = 0,$$

i.e., $\beta^2 = -4$. Then we have the following equalities:

$$2 = \beta^{p-1} = (\beta^2)^{(p-1)/2} = (-4)^{(p-1)/2} = (-1)^{(p-1)/2} 2^{p-1} = (-1)^{(p-1)/2}. \qquad (2.1)$$

Then Equation (2.1) implies that $4 \equiv 1 \mod p$, which is not possible as $p > 3$. Also, any β satisfying $f(\beta) = 0$ can not satisfy $\beta^{p-1} = 1$; otherwise from $\beta^{p+1} = \beta^2$ we obtain

$$0 = f(\beta) = \beta^{p+1} - \beta^2 + 4 = 4,$$

which gives a contradiction. □

Theorem 2.2 *Let* $F = \mathbb{F}_{p^n}(w, z)$ *be the function field defined by* $z(z + w)(w^{p-1} - 1) = 1$. *Then* F *satisfies the following properties.*

(i) *F is a function field with the full constant field* $\mathbb{F}_{p^n}$.
(ii) $g(F) = p - 1$.

In particular, the number $N(F)$ of rational places of F satisfies

$$p^n + 1 - 2(p-1)p^{n/2} \leq N(F) \leq p^n + 1 + 2(p-1)p^{n/2}. \qquad (2.2)$$

Proof

(i) We consider the function field extension $F/\mathbb{F}_{p^n}(w)$. Then the element z satisfies the polynomial $h_w(T) = T^2 + wT - 1/(w^{p-1} - 1)$ over $\mathbb{F}_{p^n}(w)$. That is,

$[F : \mathbb{F}_{p^n}(w)] \leq 2 < p$. This implies that $F/\mathbb{F}_{p^n}(w)$ is a tame extension, i.e., there is no wild ramification. Let $(w = \alpha)$ be the place of $\mathbb{F}_{p^n}(w)$ corresponding to the zero of $w - \alpha$ such that $\alpha^{p-1} = 1$. Denote by v_α the corresponding valuation of $(w = \alpha)$. Note that $v_\alpha(1/(w^{p-1} - 1)) = -1$ and $v_\alpha(w) = 0$. Hence by the Eisenstein irreducibility criteria [9, Proposition 3.1.15], we conclude that $(w = \alpha)$ is totally ramified in F. This implies that $\mathbb{F}_{p^n}$ is the full constant field of F.

(ii) We consider the constant field extension to calculate the genus. Denote by $\bar{F} = F\bar{\mathbb{F}}$ the compositum of F and $\bar{\mathbb{F}}$. Let P be a place of $\mathbb{F}_{p^n}(w)$ corresponding to monic irreducible polynomial $p(T) \in \mathbb{F}_{p^n}[T]$ with $p(T) \neq T - \alpha$, where $\alpha^{p-1} = 1$. Let $(w = \beta)$ be the place of $\bar{\mathbb{F}}(w)$ lying over P, i.e., $\beta \in \bar{\mathbb{F}}$ is a root of $p(T)$. Recall that P is ramified in F if and only if $(w = \beta)$ is ramified in $\bar{F}$. Set $h_\beta(T) = T^2 + \beta T - 1/(\beta^{p-1} - 1)$. Note that $h_\beta(T)$ is obtained from $h_w(T)$ by taking coefficients residue class field of $(w = \beta)$. The place $(w = \beta)$ is ramified if and only if $h_\beta(T)$ has a multiple root, i.e., $h_\beta(T)$ is not separable. By Lemma 2.1, we conclude that there exist exactly $p + 1$ places of $\bar{\mathbb{F}}(w)$ ramified in $\bar{F}/\bar{\mathbb{F}}(w)$.

Now we consider the place $(w = \infty)$ of $\bar{\mathbb{F}}(w)$ corresponding the pole of w. For this, we consider the change of variable. Set $y = z/w$. Then $\bar{F} = \bar{\mathbb{F}}(w, z) = \bar{\mathbb{F}}(w, y)$, where the minimal polynomial of y over $\bar{\mathbb{F}}(w)$ is $g(T) = T^2 + T - 1/(w^2(w^{p-1} - 1))$. Then $g_\infty(T) = T^2 + T = T(T + 1)$, i.e., $(w = \infty)$ splits in $\bar{F}$. That is, $(w = \infty)$ is not ramified in $F/\mathbb{F}_{p^n}(w)$.

We also have observed in (i) that for all $\alpha \in \mathbb{F}_{p^n}$ with $\alpha^{p-1} = 1$, the place $(w = \alpha)$ is ramified. Therefore, there exist $2p$ ramified places. Since the constant field of $\bar{F}$ is algebraically closed and $\bar{F}/\bar{\mathbb{F}}_{p^n}(w)$ is of degree 2 extension, the degree of the different divisor is equal to the number of ramified places. Then by the Hurwitz genus formula [9, Theorem 3.4.13] we have

$$2g(F) - 2 = 2(-2) + 2p,$$

i.e., $g(F) = p - 1$.

Moreover, as $\mathbb{F}_{p^n}$ is the full constant field of F, we obtain the inequity given in (2.2) by the Hasse-Weil theorem. □

Corollary 2.3 *As the full constant field of* F *is* $\mathbb{F}_{p^n}$, *we conclude that* $g(Z, W) = Z(Z + W)(W^{p-1} - 1) - 1$ *is an absolutely irreducible polynomial, see* [9, *Corollary* 3.6.8].

We estimate the number $N_{aff}(\mathcal{X})$ of affine rational points of $\mathcal{X}$ by using the number of rational places of its function field F. For this, we first investigate the singular affine points of $\mathcal{X}$.

Lemma 2.4 *Let* $\mathcal{X}$ *be the curve defined by* $g(Z, W) = Z(Z + W)(W^{p-1} - 1) - 1$. *Then* $\mathcal{X}$ *has no affine singular points.*

Proof We recall that an affine point $(\alpha, \beta) \in \mathcal{X}$ is singular if and only if

$$g(\alpha, \beta) = \frac{\partial g(Z, W)}{\partial Z}(\alpha, \beta) = \frac{\partial g(Z, W)}{\partial W}(\alpha, \beta) = 0,$$

where $\partial g(Z, W)/\partial Z$ and $\partial g(Z, W)/\partial W$ are partial derivatives of g with respect to Z and W, respectively. Note that

$$\begin{aligned} \frac{\partial g(Z, W)}{\partial Z} &= (2Z + W)(W^{p-1} - 1), \text{ and} \\ \frac{\partial g(Z, W)}{\partial W} &= Z(W^{p-1} - 1) - Z(Z + W)W^{p-2} = -Z - Z^2 W^{p-2}. \end{aligned}$$

That is, if (α, β) is a singular point of $\mathcal{X}$ then α and β have to satisfy the following equalities.

$$\alpha(\alpha + \beta)(\beta^{p-1} - 1) - 1 = 0 \tag{2.3}$$

$$(2\alpha + \beta)(\beta^{p-1} - 1) = 0 \tag{2.4}$$

$$\alpha + \alpha^2 \beta^{p-2} = 0 \tag{2.5}$$

By Equation (2.3), we conclude that $\beta^{p-1} - 1 \neq 0$ and $\alpha \neq 0$, and hence we have $\beta = -2\alpha$ and $\alpha\beta^{p-2} = -1$ by Equations (2.4) and (2.5), respectively. By setting $\beta = -2\alpha$ in $\alpha\beta^{p-2} = -1$, we obtain $\alpha^{p-1} = 2$. Then $\beta = -2\alpha$ implies that $\beta^{p-1} = 2$. By Equation (2.3), we have

$$\alpha(\alpha + \beta)(\beta^{p-1} - 1) - 1 = -\alpha^2 - 1 = 0,$$

i.e., $\alpha^2 = -1$. Then we have the following equalities.

$$2 = \beta^{p-1} = (-2\alpha)^{p-1} = (\alpha^2)^{(p-1)/2} = (-1)^{(p-1)/2} = \pm 1 \tag{2.6}$$

However, Equation (2.6) is possible only for $p = 3$, which gives a contradiction. □

Theorem 2.5 *The number $N_{aff}(\mathcal{X})$ of affine rational points of $\mathcal{X}$ satisfies $N_{aff}(\mathcal{X}) = N(F) - (p + 1)$. In particular, we have*

$$p^n - 2(p-1)p^{n/2} - p \leq N_{aff}(\mathcal{X}) \leq p^n + 2(p-1)p^{n/2} - p.$$

Proof It is a well-known fact that each nonsingular rational point of a curve corresponds to a unique rational place of its function field, see [8, Section 3.1].

The points of $\mathcal{X}$ at infinity are the points $(Z : W : T)$ for which $g(Z : W : 0) = Z(Z + W)W^{p-1} = 0$. That is, they are $P_1 = (0 : 1 : 0)$, $P_2 = (1 : -1 : 0)$ and $P_3 = (1 : 0 : 0)$ with multiplicities $m_{P_1} = 1$, $m_{P_2} = 1$ and $m_{P_3} = p - 1$, respectively. Hence, there exits unique rational places of F corresponding to P_1 and P_2. Moreover, there are $p - 1$ distinct tangent lines of $\mathcal{X}$ at P_3, namely $W - \alpha T$ with $\alpha^{p-1} = 1$, corresponding to $p - 1$ distinct rational places of F. Hence, there are $p+1$ rational places corresponding to points of $\mathcal{X}$ at infinity. Moreover, each rational place of F which does not correspond to a point at infinity corresponds to a unique affine point of $\mathcal{X}$ since $\mathcal{X}$ has no affine singular points by Lemma 2.1. This proves the first assertion. Then by Eq. (2.2), we obtain the second assertion. □

2.2 The function field E_d

Now we consider the curve $\mathcal{Y}$ defined by the equation $f(Y,Z) = YZ(Y-Z)^{p-1} - YZ - 1$. Note that by setting $W = Y - Z$, we obtain $g(Z,W) = Z(Z+W)(W^{p-1}-1) - 1$. Therefore, the function field F of $\mathcal{Y}$ is the function field of $\mathcal{X}$.

Lemma 2.6 *Let $\mathcal{S}$ be the set of rational affine points of $\mathcal{Y}$ that do not lie on $Y=0$, $Z=0$ and $Y=Z$, i.e.,*

$$\mathcal{S} = \{(\alpha,\beta) \in \mathcal{Y} \ : \ \alpha,\beta \in \mathbb{F}_{p^n},\ \alpha\beta \neq 0,\ \alpha \neq \beta\}.$$

Then

$$|\mathcal{S}| \geq N_{aff}(\mathcal{X}) - 2 \geq p^n - 2(p-1)p^{n/2} - p - 2. \tag{2.7}$$

Proof As $W = Y - Z$, there exists one to one correspondence between the affine rational points of $\mathcal{Y}$ and the affine rational points of $\mathcal{X}$. Moreover, the points of $\mathcal{Y}$ lying on $Y=0$, $Z=0$ and $Y=Z$ correspond to the ones of $\mathcal{X}$ lying on $W+Z=0$, $Z=0$ and $W=0$, respectively.

From the defining equation $g(Z,W) = Z(Z+W)(W^{p-1}-1) - 1$ of $\mathcal{X}$, we conclude that $\mathcal{X}$ can not have any affine points on $W+Z=0$ and $Z=0$. If $(\alpha,0) \in \mathcal{X}$, then $\alpha^2 = -1$. That is, there are at most 2 rational affine points of $\mathcal{X}$ lying on the line $W=0$. Therefore, the cardinality of $\mathcal{S}$ satisfies $|\mathcal{S}| \geq N_{aff}(\mathcal{X}) - 2$, which gives the desired result by Theorem 2.5. □

Theorem 2.7 *Let $\mathcal{E}_d$ be the curve defined by*

$$\mathcal{E}_d = \begin{cases} C^p - C = Y^p - Y + 1/Y - d \\ YZ(Y-Z)^{p-1} - YZ - 1 = 0 \end{cases}$$

and E_d be its function field. Then E_d satisfies the following properties.

(i) *E_d is a function field with the full constant field $\mathbb{F}_{p^n}$.*
(ii) $g(E_d) \leq p(p-1)$

In particular, the number $N(E_d)$ of rational places of E_d satisfies

$$p^n + 1 - 2(p-1)p^{n/2+1} \leq N(E_d) \leq p^n + 1 + 2(p-1)p^{n/2+1}. \tag{2.8}$$

Proof Let F_d be the function field of the curve $\mathcal{Y}_d$ defined by $C^p - C = Y^p - Y + 1/Y - d$, i.e., F_d is $\mathbb{F}_{p^n}(c, y)$ with defining equation $c^p - c = y^p - y + 1/y - d$. Note that $F_d/\mathbb{F}_{p^n}(y)$ is an Artin-Schreier extension of degree p. We refer to [9, Proposition 3.7.8] for the properties of Artin-Schreier extensions. The zero $(y = 0)$ of y is the only ramified place of $\mathbb{F}_{p^n}(y)$ with the ramification index p and the different exponent $2(p-1)$. Then by the Hurwitz genus formula the genus $g(F_d) = 0$. That is, F_d is a rational function field with full constant field $\mathbb{F}_{p^n}$. In fact, we observe that $F_d = \mathbb{F}_{p^n}(y - c)$.

Let F be the function field of the curve $\mathcal{Y}$. Recall that F is the function field of $\mathcal{X}$ satisfying the properties in Theorem 2.2. That is, F is a function field of genus $g(F) = p - 1$ with the full constant field $\mathbb{F}_{p^n}$. Note that the minimal polynomial of z over $\mathbb{F}_{p^n}(y)$ is $M(T) = T(T-y)^{p-1} - T - \frac{1}{y}$. Hence by Kummer's theorem, we also conclude that the place $(y = 0)$ is totally ramified in F.

Note that the function field E_d of the curve $\mathcal{E}_d$ is the compositum of F and F_d over $\mathbb{F}_{p^n}(y)$, see Fig. 1. Therefore, either $E_d = F$ or E_d/F is a Galois extension of degree p. We will observe that the case $[E_d : F] = 1$ does not hold. Suppose that $[E_d : F] = 1$, equivalently $F = E_d$. Then we have $\mathbb{F}_{p^n}(y) \subseteq F_d \subseteq E_d = F$, which implies that

$$p = [F : \mathbb{F}_{p^n}(y)] = [F : F_d][F_d : \mathbb{F}_{p^n}(y)].$$

Since $[F_d : \mathbb{F}_{p^n}(y)] = p$, we have $F = F_d$. Therefore, we have $F = E_d = F_d$. This gives a contradiction as $g(F_d) = 0$ while $g(F) = p - 1$. Hence, we conclude that E_d/F is a Galois extension of degree p.

(i) Now we observe that $\mathbb{F}_{p^n}$ is the full constant field of E_d. Suppose that $\mathbb{F}_{p^n}$ is a proper subfield of the full constant field $\mathbb{F}$ of E_d, i.e., $[\mathbb{F} : \mathbb{F}_{p^n}] > 1$. Note that we have $F \subsetneq \mathbb{F}F \subseteq E_d$, where $\mathbb{F}F$ is the compositum of $\mathbb{F}$ and F. Since $[F : E_d] = p$, we have $E_d = \mathbb{F}F$. In particular, E_d is a constant fields extension of F. Then by [9, Theorem 3.6.3], we have $g(E_d) = g(F) \geq 1$. Similarly, as $\mathbb{F}_{p^n}$ is the full constant field of F_d, we observe that E_d is a constant field extension of F_d. Therefore, $g(E_d) = g(F_d) = 0$, which gives a contradiction.

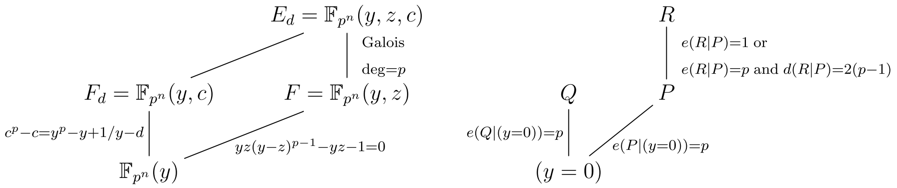
$E_d = \mathbb{F}_{p^n}(y, z, c)$
Galois
deg$=p$
$F_d = \mathbb{F}_{p^n}(y, c)$
$F = \mathbb{F}_{p^n}(y, z)$
$c^p - c = y^p - y + 1/y - d$
$yz(y-z)^{p-1} - yz - 1 = 0$
$\mathbb{F}_{p^n}(y)$
R
$e(R|P)=1$ or
$e(R|P)=p$ and $d(R|P)=2(p-1)$
Q
P
$e(Q|(y=0))=p$
$e(P|(y=0))=p$
$(y = 0)$

Fig. 1 E_d is the compositum of F_d and F over $\mathbb{F}_{p^n}(y)$

(*ii*) As $(y=0)$ is totally ramified in F and F_d, there are unique places of F and F_d lying over $(y=0)$, say P and Q, respectively. If E_d/F is a ramified extension, then the unique rational place P of F_d lying over $(y=0)$ is ramified with the ramification index $e(R|P)=p$ and the different exponent $d(R|P)=2(p-1)$, see Fig. 1. This comes from the fact that the only ramified place in $F_d/\mathbb{F}_{p^n}(y)$ is $(y=0)$. Then by the Hurwitz genus formula, we have

$$2g(E_d)-2 \le p(2g(F)-2)+2(p-1), \text{ i.e., } g(E_d) \le p(p-1).$$

Moreover, as $\mathbb{F}_{p^n}$ is the full constant field of E_d, we obtain the inequity given in Equation (2.8) by the Hasse-Weil theorem.

□

3 The proof of the main theorem

We recall our interest. We want to examine the permutation property of the rational functions

$$f_b(X)=X+\frac{1}{X^p-X+b},$$

where $b\in\mathbb{F}_{p^n}$ with $\mathrm{Tr}(b)\neq 0$. We set $\mathcal{Z}=\{c^p-c \mid c\in\mathbb{F}_{p^n}\}$, i.e., the inverse image of 0 under the absolute trace map. We first observe that the values of b for which $f_b(X)$ is a permutation depend on the cosets of $\mathcal{Z}$.

Remark 3.1 Let $b_1,b_2\in\mathbb{F}_{p^n}$ such that $\mathrm{Tr}(b_1)=\mathrm{Tr}(b_2)$, equivalently $b_1+\mathcal{Z}=b_2+\mathcal{Z}$. That is, $b_1=b_2+c^p-c$ for some $c\in\mathbb{F}_{p^n}$. Then

$$f_{b_1}(X)=X+\frac{1}{X^p-X+b_2+c^p-c}=Z+\frac{1}{Z^p-Z+b_2}-c=f_{b_2}(Z)-c,$$

where $Z=X+c$. Hence, we conclude that f_{b_1} is a permutation of $\mathbb{F}_{p^n}$ if and only if $f_{b_2}(X)$ is a permutation of $\mathbb{F}_{p^n}$ for any $b_2\in b_1+\mathcal{Z}$.

Proposition 3.2 *Let* $b\in\mathbb{F}_{p^n}$ *with* $b\notin\mathcal{Z}$, *equivalently* $\mathrm{Tr}(b)\neq 0$. *Then* $f_b(X)$ *is a permutation if and only if* $Y^p-Y+\frac{1}{Y}=d$ *has a unique solution in* $\mathbb{F}_{p^n}$ *for any* $d\in b+\mathcal{Z}$.

Proof Note that $f_b(X)$ is a permutation if and only if

$$\frac{1}{X^p-X+b}=-X+c \tag{3.1}$$

has a unique solution in $\mathbb{F}_{p^n}$ for each $c \in \mathbb{F}_{p^n}$. Since $x^p - x + b \neq 0$ for all $x \in \mathbb{F}_{p^n}$, Equation (3.1) has a unique solution in $\mathbb{F}_{p^n}$ if and only if $X^p - X + b = -1/(X - c)$ has a unique solution. By setting $Y = X - c$, we have the following equalities.

$$\begin{aligned} X^p - X + \frac{1}{X-c} + b &= (Y+c)^p - (Y+c) + \frac{1}{Y} + b \\ &= Y^p - Y + \frac{1}{Y} - d, \end{aligned}$$

where $-d = c^p - c + b$. Therefore, we conclude that if Equation (3.1) has a unique solution in $\mathbb{F}_{p^n}$ then $Y^p - Y + \frac{1}{Y} = d$ has a unique solution in $\mathbb{F}_{p^n}$ for $d \in b + \mathcal{Z}$.

Conversely, suppose that $Y^p - Y + \frac{1}{Y} = d$ has a unique solution in $\mathbb{F}_{p^n}$ for any $d \in b + \mathcal{Z}$. For $c \in \mathbb{F}_{p^n}$, let $d = c^p - c + b$. By our assumption, there exists a solution y of $Y^p - Y + \frac{1}{Y} = d$. This implies that $x = y + c$ is a solution of $f_b(X) = c$. That is, $f_b(X)$ is onto, and hence it is a permutation. □

By Proposition 3.2, we consider the solutions of the following equation.

$$Y^p - Y + \frac{1}{Y} = Z^p - Z + \frac{1}{Z} \tag{3.2}$$

Equation (3.2) holds if and only if

$$(Y - Z)^p - (Y - Z) - \frac{Y - Z}{YZ} = 0.$$

Dividing by $Y - Z$ and setting $W = Y - Z$, we obtain the following equation:

$$Z(Z + W)(W^{p-1} - 1) - 1 = 0,$$

which is the defining equation of $\mathcal{X}$ studied in Sect. 2. Recall that the function field F of $\mathcal{X}$ is the same as the function field of $\mathcal{Y}$ given by $\mathbb{F}_{p^n}(y, z)$ with $yz(y - z)^{p-1} - yz - 1 = 0$. Also, we recall that the set $\mathcal{S}$ consists of the affine rational points (α, β) of $\mathcal{Y}$ satisfying $\alpha\beta \neq 0$ and $\alpha \neq \beta$, see Lemma 2.6.

We now relate the permutation property of $f_b(X)$ with the existence of the rational place of the function field E_d, which is the compositum of F and F_d, see Theorem 2.7.

Proposition 3.3 *E_d has a rational place Q lying over $P_{\alpha,\beta}$ of F corresponding to $(\alpha, \beta) \in \mathcal{S}$ if and only if $f_b(X)$ is not a permutation for $b \in d + \mathcal{Z}$.*

Proof From the defining equation $c^p - c = y^p - y + 1/y - d$ of the function field F_d, we conclude that the poles of c are the ones lying over $(y = 0)$ and $(y = \infty)$. In other words, the place Q is not a pole of c, which implies that $c(Q) = c_0$ lies in $\mathbb{F}_{p^n}$. As E_d is the compositum of F and F_d, we have $y(Q) = \alpha$ and $z(Q) = \beta$. Then from the defining equations of F_d and F we have

$$\alpha^p - \alpha + 1/\alpha = c_0^p - c_0 + d$$
$$\alpha^p - \alpha + 1/\alpha = \beta^p - \beta + 1/\beta,$$

which shows that α and β are two distinct solutions of the equation $Y^p - Y + 1/Y = c_0^p - c_0 + d$. Since $d + \mathcal{Z} = c_0^p - c_0 + d + \mathcal{Z}$, by Proposition 3.2 we conclude that $f_b(X)$ is not a permutation for $b \in d + \mathcal{Z}$.

Conversely, suppose that $f_b(X)$ is not a permutation for $b \in d + \mathcal{Z}$. Then by Proposition 3.2 there exist $\alpha, \beta \in \mathbb{F}_{p^n}$ with $\alpha \neq \beta$ such that

$$\alpha^p - \alpha + 1/\alpha = \beta^p - \beta + 1/\beta = d,$$

i.e., $(\alpha, \beta) \in \mathcal{Y}$. Note that $\alpha \neq 0$, $\beta \neq 0$ and $\alpha \neq \beta$, which implies that $(\alpha, \beta) \in \mathcal{S}$, see Lemma 2.6. Since $\mathrm{Tr}(\alpha^p - \alpha + 1/\alpha) = \mathrm{Tr}(d)$, i.e., $\mathrm{Tr}(\alpha^p - \alpha + 1/\alpha - d) = 0$, the place $(y = \alpha)$ of $\mathbb{F}_{p^n}(y)$ splits in F_d. Hence, the place $P_{\alpha,\beta}$ of F lying over $(y = \alpha)$ splits in E_d. That is, any place Q of E_d lying over $P_{\alpha,\beta}$ is rational. □

Now we give a Proof of Theorem 1.1. We first recall the statement of the theorem for the sake of the reader.

Theorem 1.1 *Let $p > 3$ be a prime.*

(i) *If $n \geq 5$ then $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$ for any $b \in \mathbb{F}_{p^n}$ with* $\mathrm{Tr}(b) \neq 0$.
(ii) *For $n = 3$ (respectively, $n = 4$), there are at least $p^{n-1}(\sqrt{p} - 3)/2$ (respectively, $p^n/3$) elements $b \in \mathbb{F}_{p^n}$ for which $f_b(X)$ is not a permutation of $\mathbb{F}_{p^n}$.*

Proof of Theorem 1.1 (i) By Proposition 3.3, it is sufficient to show that E_d has a rational place lying over $P_{\alpha,\beta}$ for some $(\alpha, \beta) \in S$. By Theorem 2.5 and Lemma 2.6, we have $|S| \geq N(F) - (p + 3)$, i.e., there are at most $p + 3$ rational places of F not corresponding a point in S. As there are at most p places of E_d lying over a place P of F, it is sufficient to show that $N(E_d) - p(p + 3) > 0$. By Equation (2.8) we have

$$N(E_d) - p(p + 3) \geq p^n + 1 - 2(p - 1)p^{n/2+1} - p(p + 3).$$

This implies that $N(E_d) - p(p + 3) > 0$ for all $n \geq 5$.

(ii) Recall that the place $P_{\alpha,\beta}$ corresponding to $(\alpha, \beta) \in \mathcal{S}$ splits completely in E_d if and only if $\mathrm{Tr}(\alpha^p - \alpha + 1/\alpha) = \mathrm{Tr}(d)$. Since $\mathrm{Tr}(d) = \mathrm{Tr}(b)$ for any $b \in d + \mathcal{Z}$, the place $P_{\alpha,\beta}$ splits completely in E_b for any $b \in d + \mathcal{Z}$. Hence, we only consider the representatives of the cosets of $\mathcal{Z}$. Let $\mathcal{R}$ be the set of representatives of distinct cosets of $\mathcal{Z}$. Then for any $(\alpha, \beta) \in \mathcal{S}$ there exits unique $d \in \mathcal{R}$ such that $P_{\alpha,\beta}$ splits completely in E_d. We set $\tilde{\mathcal{R}} \subseteq \mathcal{R}$ such that $d \in \tilde{\mathcal{R}}$ if and only if there exists $P_{\alpha,\beta}$ of F splits completely in E_d for some $(\alpha, \beta) \in \mathcal{S}$. We have observed that any place Q of E_d lying over $P_{\alpha,\beta}$ is not a pole of c, i.e., $c(Q) \in \mathbb{F}_{p^n}$. That is, a splitting place $P_{\alpha,\beta}$ gives p distinct affine rational points on the curve $\mathcal{E}_d$, namely $(\alpha, \beta, c(Q) + i)$ for $i \in \mathbb{F}_p$. Then by Eq. (2.7) we have

$$p(p^n - 2(p-1)p^{n/2} - p - 2) \le p|\mathcal{S}| \le \sum_{d\in\tilde{\mathcal{R}}} N(E_d). \tag{3.3}$$

Set $k = |\tilde{\mathcal{R}}|$. Then by the Pigeonhole principle and Eqs. (2.8) and (3.3), there exists $d \in \mathcal{R}$ such that

$$\frac{1}{k}p(p^n - 2(p-1)p^{n/2} - p - 2) \le N(E_d) \le p^n + 1 + 2(p-1)p^{n/2+1},$$

i.e.,

$$p(p^n - 2(p-1)p^{n/2} - p - 2) \le k(p^n + 1 + 2(p-1)p^{n/2+1}). \tag{3.4}$$

Hence, if $n = 3$ (respectively, $n = 4$) then we get a contradiction with $k < (\sqrt{p} - 3)/2$ (respectively, $k < p/3$) by Equation (3.4). □

Remark 3.4 Note that Eq. (3.4) shows that $k = p$ for $n \ge 5$. Hence, (ii) also proves the fact that $f_b(X)$ is not a permutation for any $b \in \mathbb{F}_{p^n}$ in the case $n \ge 5$ and $p > 3$.

Acknowledgements N. Anbar is supported by TÜBİTAK Project under Grant 120F309.

References

1. Anbar, N., Kaşıkcı, C.: Permutations polynomials of the form $G(X)^k - L(X)$ and curves over finite fields. Cryptogr. Commun. **13**(2), 283–294 (2021)
2. Anbar, N., Odžak, A., Patel, V., Quoos, L., Somoza, A., Topuzoğlu, A.: On the difference between permutation polynomials over finite fields. Finite Fields Appl. **49**, 132–142 (2018)
3. Bartoli, D., Hou, X.D.: On a conjecture on permutation rational functions over finite fields. Finite Fields Appl. 76, Paper No. 101904 (2021)
4. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves Over a Finite Field. Princeton University Press, New Jersey (2013)
5. Hou, X.D., Sze, C.: On a type of permutation rational functions over finite fields. Finite Fields Appl. **68**, Paper No. 10175 (2020)
6. Lidl, R., Niederreiter, H.: Finite fields. With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, vol. 20. Cambridge University Press, Cambridge (1997)
7. Mullen, G.L., Panario, D.: Handbook of Finite Fields. Chapman and Hall, London (2013)
8. Niederreiter, H., Xing, C.P.: Algebraic Geometry in Coding Theory and Cryptography. Princeton University Press, Princeton, NJ (2009)
9. Stichtenoth, H.: Algebraic Function Fields and Codes. Graduate Texts in Mathematics, vol. 254, 2nd edn. Springer-Verlag, Berlin (2009)
10. Yuan, J., Ding, C., Wang, H., Pieprzyk, J.: Permutation polynomials of the form $(x^p - x + \delta)^s + L(X)$. Finite Fields Appl. **14**(2), 482–493 (2008)