Curves over Finite Fields and Permutations of the Form $x^k - \gamma \mathrm{Tr}(x)$

Nurdagül ANBAR

Sabancı University,
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
email: nurdagulanbar2@gmail.com

Abstract

We consider the polynomials of the form $P(x) = x^k - \gamma \mathrm{Tr}(x)$ over $\mathbb{F}_{q^n}$ for $n \geq 2$. We show that $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$ in the case $\gcd(k, q^n - 1) > 1$. Our proof uses an absolutely irreducible curve over $\mathbb{F}_{q^n}$ and the number of rational points on it.

Keywords: function fields, permutation polynomials, rational places.
Mathematics Subject Classification(2010): 11T06, 14H05.

1 Introduction

Let q be a power of a prime p, and let $\mathbb{F}_q$ be the finite field with q elements. A polynomial $P(x) \in \mathbb{F}_q[x]$ is called a *permutation* of $\mathbb{F}_q$ if the associated map from $\mathbb{F}_q$ to $\mathbb{F}_q$ defined by $x \mapsto P(x)$ is a bijection, i.e., it permutes the elements of $\mathbb{F}_q$. 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, 8] and references therein.

One of the main approaches to show that $P(x)$ is not a permutation uses the theory of curves and their number of rational points, for instance see [1, 2]. The approach can be summarized as follows. For a given polynomial $P(x)$, one can consider the bivariate polynomial

$$\frac{P(X) - P(Y)}{X - Y} \tag{1.1}$$

over $\mathbb{F}_q$. Suppose that the polynomial in Equation (1.1) has an absolutely irreducible factor over $\mathbb{F}_q$. Then the corresponding curve $\mathcal{X}$ has a point $(x, y) \in \mathbb{F}_q^2$ with $x \neq y$ for all sufficiently large q. This proves that $P(x) = P(y)$ for $x, y \in \mathbb{F}_q$ with $x \neq y$, i.e., P is not a permutation of $\mathbb{F}_q$ for all sufficiently large q.

Let $n \geq 2$ be an integer and $\mathbb{F}_{q^n}$ be the extension of $\mathbb{F}_q$ of degree n. The topic of this paper is polynomials of the form $x^k - \gamma \mathrm{Tr}(x)$ over $\mathbb{F}_{q^n}$, where $\mathrm{Tr} : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q$ is the Trace function defined by

$$\mathrm{Tr}(x) = x + x^q + \cdots + x^{q^{n-1}} .$$

This is an interesting class of permutation polynomials that has been investigated intensively as it combines the multiplicative and the additive structure of $\mathbb{F}_{q^n}$, see [3, 4, 5, 7].

In this paper we show that $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$ in the case $\gcd(k, q^n - 1) > 1$ for all q and integer $n \geq 2$. Our main approach also uses absolutely irreducible curves over $\mathbb{F}_{q^n}$, but in a different way. More precisely, we relate the multiplicative and the additive structure of $\mathbb{F}_{q^n}$ via an absolutely irreducible curve. The paper is organized as follows. In Section 2 we investigate some rational function field extensions and their compositum, which we use in Section 3 to prove our main result.

2 Function Field Extensions

In this section we study some rational function field extensions and their compositum. For the notations and well-known facts about function fields, as a general reference, we refer to [10].

Let E be a function field over $\mathbb{F}_q$ and F/E be a finite separable extension of function fields of degree $[F : E] = r$. We write $Q|P$ for a place Q of F lying over a place P of E, and denote by $e(Q|P)$ the ramification index of $Q|P$. Recall that when the ramification index $e(Q|P) > 1$, it is said that $Q|P$ is ramified. Moreover, if the characteristic p of $\mathbb{F}_q$ does not divide $e(Q|P)$, then $Q|P$ is called tame; otherwise it is called wild. A place P of E splits completely in F if there are r distinct places $Q_1, \ldots, Q_r$ of F lying over P. Then by the Fundamental Equality [10, Theorem 3.1.11], we have $e(Q_i|P) = 1$ and $\deg(Q_i) = \deg(P)$ for all $i = 1, \ldots, r$. In particular, if P is a rational place of E splitting completely in F, then there are r rational places of F lying over P.

Let t and s be positive integers such that t is a divisor of $q^n - 1$ and s is relatively prime to $q^n - 1$. We consider the rational function field extensions

$\mathbb{F}_{q^n}(w)/\mathbb{F}_{q^n}(z)$, $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ and $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$ defined by the equations $z = (1/\gamma)w^s$, $w = x^t$ and $z = \mathrm{Tr}(y) + c$, respectively, and their compositum, where $\gamma, c \in \mathbb{F}_{q^n}$ with $\gamma \neq 0$, see Figure 1. For a rational function field $\mathbb{F}_{q^n}(z)$ and $\alpha \in \mathbb{F}_{q^n}$, we denote by $(z = \alpha)$ and $(z = \infty)$ the places corresponding the zero and the pole of $z - \alpha$, respectively.

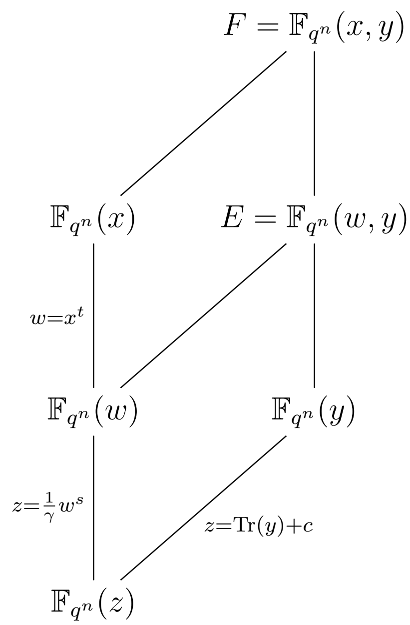

Figure 1: Compositum over Rational Function Fields

(i) **The extension $\mathbb{F}_{q^n}(w)/\mathbb{F}_{q^n}(z)$ defined by $z = (1/\gamma)w^s$:**
Note that $(z = 0)$ and $(z = \infty)$ are the only ramified places, which are totally ramified. In particular, $(w = 0)$ and $(w = \infty)$ are the unique places lying over $(z = 0)$ and $(z = \infty)$, respectively. Moreover, the fact that w^s permutes $\mathbb{F}_{q^n}$ implies that for any rational place of $\mathbb{F}_{q^n}(z)$ there exits a unique rational place of $\mathbb{F}_{q^n}(w)$ lying over it. In other words, $(w = \alpha)$ is the unique place of $\mathbb{F}_{q^n}(w)$ lying over $(z = (1/\gamma)\alpha^s)$.

(ii) **The extension $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ defined by $w = x^t$:**
Note that $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ is a Kummer extension as t is a divisor of $q^n - 1$, see [10, Proposition 3.7.3]. The only ramified places are $(w = 0)$ and $(w = \infty)$, which are totally ramified. In particular, $(x = 0)$ and $(x = \infty)$ are the unique places lying over $(w = 0)$ and $(w = \infty)$, respectively. The

place $(w = \alpha)$ splits completely in $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ if and only if α is a t-th power in $\mathbb{F}_{q^n}$. This shows that for $\alpha \in \langle \zeta^t \rangle$, where ζ is a primitive element of $\mathbb{F}_{q^n}$, there are t rational places of $\mathbb{F}_{q^n}(x)$ lying over $(w = \alpha)$.

(iii) **The extension $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$ defined by $z = \mathrm{Tr}(y) + c$:**
Note that $(z = \infty)$ is totally ramified and $(y = \infty)$ of $\mathbb{F}_{q^n}(y)$ is the unique place lying over it. Also, the fact that

$$z = \mathrm{Tr}(y) + c = y + y^q + \cdots + y^{q^{n-1}} + c$$

is a separable polynomial implies that there is no other ramification. Furthermore, the place $(z = \alpha)$ splits completely in $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$ if and only if $\alpha \in c + \mathbb{F}_q$.

To analyse the ramification structure of the compositum of function fields, we mainly use Abhyankar's Lemma [10, Theorem 3.9.1]. For convenience of the reader, we state the lemma as follows.

Lemma 2.1 (Abhyankar's Lemma)**.** *Let F/E be a finite separable extension. Suppose that $F = E_1 \cdot E_2$ is the compositum of the intermediate fields $E \subseteq E_1, E_2 \subseteq F$. Let $Q \in \mathbb{P}_F$ lying over $P \in \mathbb{P}_E$. We set $Q_i = Q \cap E_i$ for $i = 1, 2$. If at least one of $Q_1|P$ or $Q_2|P$ is tame, then*

$$e(Q|P) = \mathrm{lcm}\,\{e(Q_1|P), e(Q_2|P)\}\ ,$$

where lcm *denotes the least common multiple.*

Lemma 2.2. *Let $E = \mathbb{F}_{q^n}(w, y)$ be the compositum of the rational function fields $\mathbb{F}_{q^n}(w)$ and $\mathbb{F}_{q^n}(y)$ over $\mathbb{F}_{q^n}(z)$ defined as above, see Figure 1. Then E is a function field over $\mathbb{F}_{q^n}$ such that*

(i) $[E : \mathbb{F}_{q^n}(w)] = q^{n-1}$, $[E : \mathbb{F}_{q^n}(y)] = s$, and

(ii) there are q^{n-1} rational places of E lying over $(z = \alpha)$ for $\alpha \in c + \mathbb{F}_q$.

Proof. As $(z = 0)$ is totally ramified in $\mathbb{F}_{q^n}(w)/\mathbb{F}_{q^n}(z)$, and it is not ramified in $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$, by Abhyankar's Lemma, any place P of $\mathbb{F}_{q^n}(y)$ lying over $(z = 0)$ is ramified in $E/\mathbb{F}_{q^n}(y)$ with ramification index $e((w = 0)|(z = 0)) = s$. This shows that

$$[E : \mathbb{F}_{q^n}(y)] = s, \quad [E : \mathbb{F}_{q^n}(w)] = q^{n-1}$$

and E is a function field over $\mathbb{F}_{q^n}$, i.e., $\mathbb{F}_{q^n}$ is the full constant field of E.

A place $(z = \alpha)$ splits completely in $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$ if and only if $\alpha \in c+\mathbb{F}_q$. Recall that there exists a unique rational place of $\mathbb{F}_{q^n}(w)$ lying over $(z = \alpha)$ for $\alpha \in \mathbb{F}_{q^n}$. Therefore, the place lying over $(z = \alpha)$ splits completely in $E/\mathbb{F}_{q^n}(w)$ for $\alpha \in \mathbb{F}_{q^n}$, see [10, Proposition 3.9.6]. □

Lemma 2.3. *Let $F = \mathbb{F}_{q^n}(x, y)$ be the compositum of the rational function fields $\mathbb{F}_{q^n}(x)$ and $E = \mathbb{F}_{q^n}(w, y)$ over $\mathbb{F}_{q^n}(w)$ defined as above, see Figure 1. Let H be the subgroup of the multiplicative group of $\mathbb{F}_{q^n}$ generated by ζ^t, where ζ is a primitive element of $\mathbb{F}_{q^n}$. Then F is a function field over $\mathbb{F}_{q^n}$ such that*

- *(i) $[F : \mathbb{F}_{q^n}(x)] = q^{n-1}$, $[F : E] = t$, and*
- *(ii) there are tq^{n-1} rational places of F lying over $(w = \alpha)$ for all $(1/\gamma)\alpha^s \in (1/\gamma)H \cap c + \mathbb{F}_q$.*

Proof. As $[E : \mathbb{F}_{q^n}(w)] = q^{n-1}$ and $[\mathbb{F}_{q^n}(x) : \mathbb{F}_{q^n}(w)] = t$ are relatively prime, we have $[F : \mathbb{F}_{q^n}(x)] = q^{n-1}$ and $[F : E] = t$. Note that $(w = 0)$ is totally ramified in $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$, and by Lemma 2.2 it is not ramified in $E/\mathbb{F}_{q^n}(w)$. Therefore, a place P of E lying over $(w = 0)$ is totally ramified in F/E. This shows that F is a function field with full constant field $\mathbb{F}_{q^n}$.

Note that $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ and $E/\mathbb{F}_{q^n}(w)$ are Galois extensions. For a nonzero $\alpha \in \mathbb{F}_{q^n}$, the place $(w = \alpha)$ is not ramified in both extensions, and hence a place P of F lying over $(w = \alpha)$ is rational if and only if $(w = \alpha)$ splits completely in both extensions. We have seen in Lemma 2.2 that $(w = \alpha)$ splits in $E/\mathbb{F}_{q^n}(w)$ if and only if $(1/\gamma)\alpha^s \in c + \mathbb{F}_q$. Furthermore, $(w = \alpha)$ splits in $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(w)$ if and only if $\alpha \in H$. Since $\gcd(s, q^n - 1) = 1$, this holds if and only if $\alpha^s \in H$, i.e. $(1/\gamma)\alpha^s \in (1/\gamma)H$. Therefore, P is a rational place lying over $(w = \alpha)$ if and only if $(1/\gamma)\alpha^s \in (1/\gamma)H \cap (c + \mathbb{F}_q)$. In this case, since $(w = \alpha)$ splits completely in F, and there are tq^{n-1} rational places lying over $(w = \alpha)$.

□

Corollary 2.4. *For a nonzero $\gamma \in \mathbb{F}_{q^n}$ and an integer $k \geq 1$, the polynomial $f(X, Y) = (1/\gamma)X^k - \mathrm{Tr}(Y) - c \in \mathbb{F}_{q^n}$ is an absolutely irreducible polynomial. Therefore, the zero set defines an absolutely irreducible curve over $\mathbb{F}_{q^n}$.*

3 Main Result

In this section we investigate the permutation polynomials of the type $P(x) = x^k - \gamma\mathrm{Tr}(x)$. A well-known fact is that a monomial x^k is a permutation if and only if k is relatively prime to q^n-1. Therefore, $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$ if $\gcd(k, q^n-1)>1$ in the case $\gamma=0$. From now on, we assume that γ is a nonzero element of $\mathbb{F}_{q^n}$.

As mentioned in the introduction, we consider the multiplicative and the additive structure of $\mathbb{F}_{q^n}$ to investigate the image of $P(x)$ on $\mathbb{F}_{q^n}$. In particular, for some $c \in \mathbb{F}_{q^n}$ we consider the solution set of

$$\frac{1}{\gamma}x^k = \mathrm{Tr}(x) + c \ , \tag{3.1}$$

and by Equation (3.1), we investigate the rational points of the curve $\mathcal{X}_c$ over $\mathbb{F}_{q^n}$ defined by

$$f_c(X,Y) = \frac{1}{\gamma}X^k - \mathrm{Tr}(Y) - c = 0 \ . \tag{3.2}$$

Theorem 3.1. *Let $P(x) = x^k - \gamma\mathrm{Tr}(x)$ be polynomial, where γ is a nonzero element in $\mathbb{F}_{q^n}$ and k is a positive integer. If $t = \gcd(k, q^n-1) > 1$, then $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$.*

Proof. We will show that there exist $x_1, x_2 \in \mathbb{F}_{q^n}$ with $x_1 \neq x_2$ such that $P(x_1) = P(x_2)$.

As in the previous section we denote by H the subgroup generated by ζ^t, where ζ is a primitive element of $\mathbb{F}_{q^n}$, i.e., H is a subgroup of order $(q^n-1)/t$. Note that the image $\mathrm{Im}(\mathrm{Tr}(\mathbb{F}_{q^n})) = \mathbb{F}_q$ is an additive subgroup of $\mathbb{F}_{q^n}$, i.e., $\mathbb{F}_{q^n}$ is the disjoint union of q^{n-1} cosets of $\mathbb{F}_q$. In particular, there exists $c \in \mathbb{F}_{q^n}$ such that we have

$$|(1/\gamma)H \cap (c + \mathbb{F}_q)| \geq \left\lceil \frac{q^n-1}{tq^{n-1}} \right\rceil \ ,$$

where $\lceil x \rceil$ denotes the least integer greater than or equal to the real number x. Note that we have

$$\frac{q^n-1}{t} = bq^{n-1} + i \quad \text{for some } 1 \leq i < q^{n-1} - 1 \ . \tag{3.3}$$

Then we have $\lceil (q^n-1)/tq^{n-1} \rceil = b+1$, i.e., there exists c such that

$$|(1/\gamma)H \cap (c + \mathbb{F}_q)| \geq b + 1 \ .$$

For this value of c, we consider the curve $\mathcal{X}_c$ defined by $f_c(X,Y)=0$, where f_c is the bivariate polynomial defined as in Equation (3.2). By Corollary 2.4,

$\mathcal{X}_c$ is an absolutely irreducible curve defined over $\mathbb{F}_{q^n}$. Let $F = \mathbb{F}_{q^n}(x, y)$ be the function field of $\mathcal{X}_c$. By Lemma 2.3, for each $\alpha \in (1/\gamma)H \cap (c + \mathbb{F}_q)$ there are tq^{n-1} distinct rational places of F. Note that these are the places lying over $(z = \alpha)$ for $\alpha \in (1/\gamma)H \cap (c + \mathbb{F}_q)$, i.e., all of them correspond to affine points of $\mathcal{X}_c$.

It is a well-known fact that each non-singular rational point of $\mathcal{X}_c$ corresponds to a unique rational place of F, see [9, 10]. Recall that an affine point (x_0, y_0) on $\mathcal{X}_c$ is singular if and only if we have

$$f(x_0, y_0) = \frac{df(X,Y)}{dX}(x_0, y_0) = \frac{df(X,Y)}{dY}(x_0, y_0) = 0 \ ,$$

where df/dX and df/dY denotes the partial derivatives of f with respect to X and Y, respectively. Since $df(X,Y)/dY = -1$, we conclude that $\mathcal{X}$ has no singular affine point. That is, each rational place of F lying over $(z = \alpha)$ for $\alpha \in (1/\gamma)H \cap (c+\mathbb{F}_q)$ corresponds to a unique rational point of $\mathcal{X}_c$. Therefore, the number $N(\mathcal{X}_c)$ of affine rational points of $\mathcal{X}_c$ satisfies

$$N(\mathcal{X}_c) \geq (b + 1)\, tq^{n-1} = btq^{n-1} + tq^{n-1} \ . \tag{3.4}$$

By Equation (3.3), we have $btq^{n-1} = q^n - 1 - it \geq q^n - 1 - (q^{n-1} - 1)t$. Hence by Equation (3.4) we have

$$N(\mathcal{X}_c) \geq q^n + (t - 1) > q^n \ .$$

Let ℓ_d be the line defined by the equation $Y = X + d$ for $d \in \mathbb{F}_{q^n}$. Then the set

$$\mathcal{L} = \{\ell_d \mid d \in \mathbb{F}_{q^n}\}$$

covers all affine points in the projective plane, and hence it covers all affine points on $\mathcal{X}_c$. Since $N(\mathcal{X}_c) > q^n$, there exists ℓ_d intersect $\mathcal{X}_c$ at least two rational points. That is, there exist distinct elements $x_1, x_2 \in \mathbb{F}_{q^n}$ such that $(x_1, x_1 + d), (x_2, x_2 + d) \in \mathcal{X}_c \cap \ell_d$. Then the defining equation f_c, see Equation (3.2), implies that

$$x_1^k - \gamma \mathrm{Tr}(x_1) = x_2^k - \gamma \mathrm{Tr}(x_2) = \gamma(c + \mathrm{Tr}(d)) \ ,$$

which gives the desired result. □

Corollary 3.2. *Let $\mathbb{F}_{q^n}$ be the finite field of characteristic $p > 2$ and $n \geq 2$. Then for any $\gamma \in \mathbb{F}_{q^n}$ the polynomial $P(x) = x^{2r} - \gamma \mathrm{Tr}(x)$ is not a permutation of $\mathbb{F}_{q^n}$.*

Remark 3.3. Let $P(x) = x^k - \gamma \mathrm{Tr}(x^d)$ for some integers k, d such that d is relatively prime to $q^n - 1$. We recall that a polynomial $P(x)$ is a permutation of $\mathbb{F}_{q^n}$ if and only if $P(x^r)$ is a permutation of $\mathbb{F}_{q^n}$ for any integer r relatively prime to $q^n - 1$. Let r be the integer with $rd \equiv 1 \mod (q^n - 1)$. We set

$$\tilde{P}(x) = P(x^r) = x^{rk} - \gamma \mathrm{Tr}(x^{rd}) = x^{rk} - \gamma \mathrm{Tr}(x) \ . \tag{3.5}$$

Then by Theorem 3.1, we conclude that $P(x)$ is not a permutation of $\mathbb{F}_{q^n}$ if $\gcd(k, q^n - 1) > 1$.

Acknowledgement

The author would like to thank Prof. Gohar Kyureghyan for pointing out the problem and helpful discussions. The author is partially supported by the Austrian Science Fund (FWF): Project F5505–N26 and Project F5511–N26, which is a part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications".

References

[1] 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 (2018), 132–142.

[2] Hou X. Applications of the Hasse–Weil bound to permutation polynomials. Finite Fields Appl. 54 (2018), 113–132.

[3] Charpin P, Kyureghyan G. Monomial functions with linear structure and permutation polynomials. Finite fields: theory and applications, 99–111, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

[4] Kyureghyan G. Constructing permutations of finite fields via linear translators. J. Combin. Theory Ser. A 118 (2011), no. 3, 1052–1061.

[5] Kyureghyan G, Zieve M. Permutation polynomials of the form $X + \gamma \mathrm{Tr}(X^k)$. Contemporary developments in finite fields and applications, 178–194, World Sci. Publ., Hackensack, NJ, 2016.

[6] Lidl R, Niederreiter H. Finite fields. With a foreword by P. M. Cohn. Second edition. Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.

[7] Ma J, Ge G. A note on permutation polynomials over finite fields. Finite Fields Appl. 48 (2017), 261–270.

[8] Mullen GL, Panario D. Handbook of finite fields. Chapman and Hall, 2013.

[9] Niederreiter H, Xing CP. Algebraic geometry in coding theory and cryptography. Princeton University Press, Princeton, NJ, 2009.

[10] Stichtenoth H. Algebraic function fields and codes. Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.