Cryptography and Communications
https://doi.org/10.1007/s12095-020-00465-9

Permutations polynomials of the form $G(X)^k - L(X)$ and curves over finite fields

Nurdagül Anbar[1] · **Canan Kaşıkcı**[1]

Received: 3 August 2020 / Accepted: 3 December 2020 /

Abstract
For a positive integer k and a linearized polynomial $L(X)$, polynomials of the form $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$ are investigated. It is shown that when L has a non-trivial kernel and G is a permutation of $\mathbb{F}_{q^n}$, then $P(X)$ cannot be a permutation if $\gcd(k, q^n - 1) > 1$. Further, necessary conditions for $P(X)$ to be a permutation of $\mathbb{F}_{q^n}$ are given for the case that $G(X)$ is an arbitrary linearized polynomial. The method uses plane curves, which are obtained via the multiplicative and the additive structure of $\mathbb{F}_{q^n}$, and their number of rational affine points.

Keywords Curves/function fields · Permutation polynomials · Rational points/places

Mathematics Subject Classification (2010) 11T06 · 14H05

1 Introduction

Let q be a power of a prime p and let $\mathbb{F}_{q^n}$ be the finite field with q^n elements. A polynomial $P(X) \in \mathbb{F}_{q^n}[X]$ is called a *permutation polynomial* of $\mathbb{F}_{q^n}$ if the associated map from $\mathbb{F}_{q^n}$ to $\mathbb{F}_{q^n}$ defined by $x \mapsto P(x)$ is a bijection. For short we will say that $P(X)$ is a permutation of $\mathbb{F}_{q^n}$. 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 [7, 10] and references therein.

The theory of curves is one of the main tools to show that $P(X)$ is not a permutation of certain finite fields, see for instance [2, 6]. The usual approach can be summarized as follows.

✉ Nurdagül Anbar
nurdagulanbar2@gmail.com

Canan Kaşıkcı
canankasikci@sabanciuniv.edu

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

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

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

Suppose that $g(X, Y)$ in (1.1) has an absolutely irreducible factor $f(X, Y) \in \mathbb{F}_{q^n}[X, Y]$. Let $\mathcal{X}$ be the absolutely irreducible curve corresponding to $f(X, Y)$. Then the Hasse-Weil bound [12, Theorem 5.2.3] implies that there exists an affine point $(x, y) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$ of $\mathcal{X}$ with $x \neq y$ if q^n is sufficiently large compared to the degree of $f(X, Y)$. This proves that $P(x) = P(y)$ for some $x, y \in \mathbb{F}_{q^n}$ with $x \neq y$, hence P is not a permutation of $\mathbb{F}_{q^n}$. 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 q^n.

Polynomials of the form

$$P(X) = G(X)^k - L(X) \tag{1.2}$$

for a linearized polynomial $L(X)$ and a polynomial $G(X)$ over $\mathbb{F}_{q^n}$, have attracted a lot attention in recent literature on permutation polynomials. In [4, 16] research on permutation polynomials given as

$$P(X) = (X^{p^i} - X + \delta)^k - L(X) \tag{1.3}$$

for some positive integers i, k and an element $\delta \in \mathbb{F}_{q^n}$ was initiated. Meanwhile there is a series of papers devoted to the classification of permutation polynomials $P(X) \in \mathbb{F}_{q^n}[X]$ of the form (1.3), see for instance [8, 13–15, 17, 18] and references therein.

Polynomials of the form $P(X) = X^k - \gamma \mathrm{Tr}(X) \in \mathbb{F}_{q^n}[X]$, where $\mathrm{Tr} : \mathbb{F}_{q^n} \mapsto \mathbb{F}_q$ is the Trace function defined by

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

have been investigated intensively with the objective to determine values of k, γ, for which $P(X)$ is a permutation of $\mathbb{F}_{q^n}$, see [6, 9] and references therein. Recently, it has been shown in [1] and in [3] as a particular case that $P(X)$ is not a permutation of $\mathbb{F}_{q^n}$ if $\gcd(k, q^n - 1) > 1$. While finite fields arithmetic is used in [3], the approach in [1] uses absolutely irreducible curves over $\mathbb{F}_{q^n}$ in a different way, since the common approach, which we described above, is not applicable for these classes of polynomials as the degrees are quite large compared to the cardinality of the finite field. More precisely, the method in [1] relates the multiplicative and the additive structure of $\mathbb{F}_{q^n}$ via an absolutely irreducible curve.

In this article, we study polynomials $P(X)$ given as in (1.2). In Section 2, we investigate special function fields as a composition of rational function fields. In Section 3, we then relate the number of affine rational points of curves, whose function fields we analysed in Section 2, with the permutation property of our polynomials to prove our main results. We first show that for a permutation G and a linearized polynomial L with non-trival kernel, $P(X) = G(X)^k - L(X)$ cannot be a permutation if $\gcd(q^n - 1, k) > 1$. Although this has been recently presented in [3] by using the finite fields arithmetic, we apply the method in [1] as mentioned above. We then analyse general criteria for functions of the form (1.2), where $G(X)$ is an arbitrary linearized polynomial.

2 Compositum of rational function fields

In this section, we consider the function fields of the curves associated to polynomials $P(X) = X^k - L(X) \in \mathbb{F}_{q^n}[X]$, where k is a positive integer and $L(X)$ is a linearized polynomial, i.e.,

$$L(X) = a_m X^{p^m} + a_{m-1} X^{p^{m-1}} + \cdots + a_0 X \ . \tag{2.1}$$

Recall that a polynomial $L(X) \in \mathbb{F}_{q^n}[X]$ is separable if $L(X)$ and its derivative $L'(X)$ do not have any common factor of positive degree. This holds if and only if $L(X)$ has no multiple root in the algebraic closure $\bar{\mathbb{F}}_{q^n}$ of $\mathbb{F}_{q^n}$. Hence, $L(X)$ in (2.1) is separable if and only if $a_0 \neq 0$.

As the proof uses the compositum of rational function fields, we first recall some basic notions and facts about function fields. For details we refer to [12, Chapter 3].

Let E be a function field over $\mathbb{F}_{q^n}$ and let F/E be a finite separable extension of function fields, i.e., the minimal polynomial of any non-zero $y \in F$ over E is separable. Say the degree $[F : E]$ of the extension is 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 $e(Q|P) > 1$, then $Q|P$ is said to be ramified. If $e(Q|P) = [F : E]$, we say that $Q|P$ is totally ramified. In this case, Q is the unique place of F lying over P. Moreover, if the characteristic p of $\mathbb{F}_{q^n}$ 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 $Q_1, \dots, Q_r$ of F lying over P. Then by the fundamental equality [12, Theorem 3.1.11], we have $e(Q_i|P) = 1$ and $\deg(Q_i) = \deg(P)$ for all $i = 1, \dots, r$. A place P is called rational if $\deg(P) = 1$. Hence if P is a rational place of E splitting completely in F, then there are r rational places of F lying over P. For a rational function field $\mathbb{F}_{q^n}(z)$ and $\alpha \in \mathbb{F}_{q^n}$, we denote by $(z = \alpha)$ and by $(z = \infty)$ the places corresponding to the zero and to the pole of $z - \alpha$, respectively.

Let $k > 1$ be a divisor of $q^n - 1$, $c \in \mathbb{F}_{q^n}$ and $L(X) \in \mathbb{F}_{q^n}[X]$ be a separable linearized polynomial. We consider the following extensions of $\mathbb{F}_{q^n}(z)$.

(i) **$\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(z)$ defined by $z = x^k$:**

Since k is a divisor of $q^n - 1$, the extension $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(z)$ is a Kummer extension of degree k, see [12, Proposition 3.7.3]. The only ramified places are $(z = 0)$ and $(z = \infty)$, which are totally ramified. In particular, $(x = 0)$ and $(x = \infty)$ are the unique places lying over $(z = 0)$ and $(z = \infty)$, respectively. Hence,

$$e((x = 0)|(z = 0)) = e((x = \infty)|(z = \infty)) = k \ .$$

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

(ii) **$\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$ defined by $z = L(y) + c$:**

Since $L(X)$ is separable, $\mathbb{F}_{q^n}(x)/\mathbb{F}_{q^n}(z)$ is a separable extension of degree $\deg(L(X))$. Note that $(z = \infty)$ is totally ramified and $(y = \infty)$ is the unique place of $\mathbb{F}_{q^n}(y)$ lying over it. Also, the facts that $L(X)$ is separable and linearized imply that $L(X) + \beta$ has no multiple roots in $\bar{\mathbb{F}}_{q^n}$ for any $\beta \in \bar{\mathbb{F}}_{q^n}$, where $\bar{\mathbb{F}}_{q^n}$ is the algebraic closure of $\mathbb{F}_{q^n}$. Hence there is no other ramification in $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(z)$. Denote by $\mathrm{Im}(L)$ and $\mathrm{Ker}(L)$ the image and the kernel of $L(X)$ in $\mathbb{F}_{q^n}$, respectively. Then there exists a rational place of $\mathbb{F}_{q^n}(y)$ lying over $(z = \alpha)$ if and only if $\alpha \in (\mathrm{Im}(L) + c)$. In this case, the number of rational places lying over $(z = \alpha)$ is $|\mathrm{Ker}(L)|$.

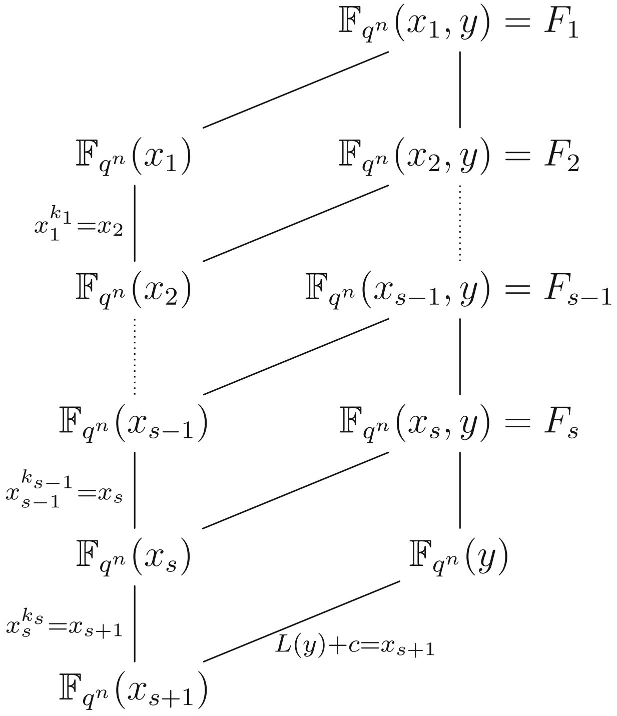
$\mathbb{F}_{q^n}(x_1, y) = F_1$
$\mathbb{F}_{q^n}(x_1)$
$\mathbb{F}_{q^n}(x_2, y) = F_2$
$x_1^{k_1}=x_2$
$\mathbb{F}_{q^n}(x_2)$
$\mathbb{F}_{q^n}(x_{s-1}, y) = F_{s-1}$
$\mathbb{F}_{q^n}(x_{s-1})$
$\mathbb{F}_{q^n}(x_s, y) = F_s$
$x_{s-1}^{k_{s-1}}=x_s$
$\mathbb{F}_{q^n}(x_s)$
$\mathbb{F}_{q^n}(y)$
$x_s^{k_s}=x_{s+1}$
$L(y)+c=x_{s+1}$
$\mathbb{F}_{q^n}(x_{s+1})$

Fig. 1 Compositum over Rational Function Fields

For $i = 1, \dots, s$, let $\mathbb{F}_{q^n}(x_i)/\mathbb{F}_{q^n}(x_{i+1})$ be the function field extension defined by $x_i^{k_i} = x_{i+1}$ for some positive integers k_i and let $\mathbb{F}_{q^n}(y)/\mathbb{F}_{q^n}(x_{s+1})$ be the extension defined by $L(y) + c = x_{s+1}$ for a separable linearized polynomial $L(X) \in \mathbb{F}_{q^n}[X]$. Now we consider the compositum F_i of $\mathbb{F}_{q^n}(x_i)$ and $\mathbb{F}_{q^n}(y)$ over $\mathbb{F}_{q^n}(x_{s+1})$ for $i = 1, \dots, s$, see Fig. 1.

Theorem 2.1 *Let k be a positive integer. Set*

$$k_1 := \gcd(q^n - 1, k) \quad \textit{and} \quad k_i := \gcd\left(q^n - 1, \frac{k}{k_{i-1} \cdots k_1}\right)$$

such that $k_i > 1$ for all $i = 2, \dots, s$ and $\gcd(q^n - 1, k/k_s \cdots k_1) = 1$. Let $F_i = \mathbb{F}_{q^n}(x_i, y)$ be the compositum of the rational function fields $\mathbb{F}_{q^n}(x_i)$ and $\mathbb{F}_{q^n}(y)$ given as above and let H_i be the subgroup generated by ζ^{k_i}, where ζ is a primitive element of $\mathbb{F}_{q^n}$. Then the following holds for all $i = 1, \dots, s$.

(i) $[F_i : \mathbb{F}_{q^n}(x_i)] = \deg(L(X))$ *and* $[F_i : \mathbb{F}_{q^n}(y)] = k_s \cdots k_i$.
(ii) *F_i is a function field over $\mathbb{F}_{q^n}$ defined by $x_i^{k_s \cdots k_i} = L(y) + c$.*
(iii) *The number $N(F_i)$ of rational places of F_i satisfies*

$$N(F_i) = \begin{cases} |H_i \cap (\mathrm{Im}(L) + c)|\ |\mathrm{Ker}(L)|\ k_i + |\mathrm{Ker}(L)| + 1, & \textit{if } -c \in \mathrm{Im}(L), \\ |H_i \cap (\mathrm{Im}(L) + c)|\ |\mathrm{Ker}(L)|\ k_i + 1, & \textit{otherwise.} \end{cases} \tag{2.2}$$

Proof (i) Note that

$$[\mathbb{F}_{q^n}(x_i):\mathbb{F}_{q^n}(x_{s+1})]=k_s\cdots k_i \quad \text{and} \quad [\mathbb{F}_{q^n}(y):\mathbb{F}_{q^n}(x_{s+1})]=\deg(L(X))\ .$$

Since $k_s\cdots k_i$ and $\deg(L(X))$ are relatively prime, F_i is the compositum of $\mathbb{F}_{q^n}(x_i)$ and $\mathbb{F}_{q^n}(y)$, which is linearly disjoint over $\mathbb{F}_{q^n}(x_{s+1})$. That is, any linearly independent subset of $\mathbb{F}_{q^n}(y)$ (resp., $\mathbb{F}_{q^n}(x_i)$) over $\mathbb{F}_{q^n}(x_{s+1})$ is also linearly independent over $\mathbb{F}_{q^n}(x_i)$ (resp., $\mathbb{F}_{q^n}(y)$), which proves (i).

(ii) The facts that $[F_i:\mathbb{F}_{q^n}(x_i)]=\deg(L(X))$ and $x_\ell^{k_\ell}=x_{\ell+1}$ for $\ell=i,\dots,s$ imply that $x_i^{k_s\cdots k_i}=L(y)+c$ is a defining equation for F_i. Observe that the pole of $x_{\ell+1}$ is totally ramified in F_ℓ, i.e., $(x_\ell=\infty)$ is the unique place of F_ℓ lying over $(x_{\ell+1}=\infty)$. Then the transitivity of the ramification indices implies that $e((x_i=\infty)|(x_{s+1}=\infty))=k_s\cdots k_i$. Hence we have

$$e((x_i=\infty)|(x_{s+1}=\infty))=k_s\cdots k_i \quad \text{and} \quad e((y=\infty)|(x_{s+1}=\infty))=\deg(L(X))\ .$$

By Abhyankar's Lemma [12, Theorem 3.9.1], we then conclude that $(x_{s+1}=\infty)$ is totally ramified in F_i; hence, F_i is a function field over $\mathbb{F}_{q^n}$.

(iii) Note that the unique place of F_i lying over $(x_{s+1}=\infty)$ is rational as $(x_{s+1}=\infty)$ is totally ramified in F_i. Set $\zeta_i=\zeta^{(q^n-1)/k_i}$ for $i=1,\dots,s$, i.e., ζ_i is a primitive k_i-th root of unity. Let P be a rational place of F_i lying over $(x_{s+1}=\alpha_{s+1})$ for a non-zero $\alpha_{s+1}\in\mathbb{F}_{q^n}$. Set $Q:=P\cap\mathbb{F}_{q^n}(y)$ and $P_\ell:=P\cap\mathbb{F}_{q^n}(x_\ell)$ for $\ell=i,\dots,s+1$, i.e., we have $(x_{s+1}=\alpha_{s+1})=P_{s+1}$ and

$$P\mid Q\mid(x_{s+1}=\alpha_{s+1}) \quad \text{and} \quad P\mid P_\ell\mid(x_{s+1}=\alpha_{s+1})\ .$$

Note that Q and P_ℓ are rational places of $\mathbb{F}_{q^n}(y)$ and $\mathbb{F}_{q^n}(x_\ell)$ for $\ell=i,\dots,s+1$, respectively. Let $P_\ell=(x_\ell=\alpha_\ell)$ for some non-zero $\alpha_\ell\in\mathbb{F}_{q^n}$. Then we have $\alpha_\ell^{k_\ell}=\alpha_{\ell+1}$ for $\ell=i,\dots,s$. Recall that, as $\mathbb{F}_{q^n}(x_\ell)/\mathbb{F}_{q^n}(x_{\ell+1})$ is a Kummer extension, P_ℓ is rational if and only if $P_{\ell+1}$ splits completely in $\mathbb{F}_{q^n}(x_\ell)$ for $\ell=i,\dots,s$.

Now we show that $(x_\ell=\alpha_\ell)$ is the only rational place of $\mathbb{F}_{q^n}(x_\ell)$ lying over $(x_{\ell+1}=\alpha_{\ell+1})$ and splitting in $\mathbb{F}_{q^n}(x_{\ell-1})$ for $\ell=2,\dots,s$. This means that all rational places of $\mathbb{F}_{q^n}(x_i)$ lying over $(x_{s+1}=\alpha_{s+1})$ are the ones lying over $(x_{i+1}=\alpha_{i+1})$. Therefore, there are exactly k_i rational places of $\mathbb{F}_{q^n}(x_i)$ lying over $(x_{s+1}=\alpha_{s+1})$, namely $(x_i=\alpha_i\zeta_i^j)$ for $j=0,\dots,k_i-1$. The places lying over $(x_{\ell+1}=\alpha_{\ell+1})$ are $(x_\ell=\alpha_\ell\zeta_\ell^j)$ for $j=0,\dots,k_\ell-1$. Since $\alpha_\ell=\alpha_{\ell-1}^{k_{\ell-1}}$, the place $(x_\ell=\alpha_\ell\zeta_\ell^j)$ splits in $F(x_{\ell-1})$ if and only if ζ_ℓ^j is a $k_{\ell-1}$-th power in $\mathbb{F}_{q^n}$. Note that

$$\zeta_\ell^j=\zeta^{\frac{q^n-1}{k_\ell}j} \quad \text{for } j=0,\dots,k_\ell-1\ ,$$

i.e., ζ_ℓ^j is a $k_{\ell-1}$-th power if and only if $k_{\ell-1}$ divides $j(q^n-1)/k_\ell$. Since

$$\gcd\left(\frac{q^n-1}{k_\ell},k_{\ell-1}\right)=\frac{1}{k_\ell}\gcd\left(q^n-1,k_{\ell-1}k_\ell\right)\le\frac{1}{k_\ell}\gcd\left(q^n-1,k_{\ell-1}\cdots k_s\right)=\frac{k_{\ell-1}}{k_\ell}\ ,$$

for a positive integer $j\le k_\ell-1$, we have

$$\gcd\left(\frac{q^n-1}{k_\ell}j,k_{\ell-1}\right)\le j\gcd\left(\frac{q^n-1}{k_\ell},k_{\ell-1}\right)\le j\frac{k_{\ell-1}}{k_\ell}<k_{\ell-1}\ .$$

Hence, we conclude that $k_{\ell-1}$ divides $j(q^n-1)/k_\ell$ if and only if $j=0$, which gives the desired conclusion.

Note that if P is a rational place of F_i lying over $(x_{s+1} = \alpha_{s+1})$, then α_{s+1} is a $(k_s \cdots k_i)$-th power, i.e.,

$$\alpha_{s+1} \in \langle \zeta^{k_s \cdots k_i} \rangle = \langle \zeta^{\gcd(q^n-1, k_s \cdots k_i)} \rangle = \langle \zeta^{k_i} \rangle = H_i \ .$$

Furthermore, Q is rational if and only if $\alpha_{s+1} \in (\mathrm{Im}(L) + c)$. Set $m := |\mathrm{Ker}(L)|$. Since the minimal polynomial of y over $\mathbb{F}_{q^n}(x_i)$ is $L(X) + c = x_i^{k_s \cdots k_i}$, there are exactly m rational places lying over $(x_i = \alpha_i)$ by Kummer's Theorem, see [12, Theorem 3.3.7]. Hence, by above argument, we conclude that there are mk_i rational places of F_i lying over $(x_{s+1} = \alpha_{s+1})$ for each $\alpha_{s+1} \in H_i \cap (\mathrm{Im}(L) + c)$. Moreover, if $L(X) + c$ has a root in $\mathbb{F}_{q^n}$, i.e., $-c \in \mathrm{Im}(L)$, then there are m rational places of $\mathbb{F}_{q^n}(y)$ lying over $(x_{s+1} = 0)$. By Abhyankar's Lemma, each place of $\mathbb{F}_{q^n}(y)$ lying over $(x_{s+1} = 0)$ is totally ramified in F_i. Therefore, there are exactly m rational places of F_i lying over $(x_{s+1} = 0)$. This gives the desired result. □

Corollary 2.2 *Let k be a positive integer such that $\gcd(q^n - 1, k) > 1$, and let $L(X) \in \mathbb{F}_{q^n}[X]$ be separable and linearized. Then $f(X, Y) = X^k - L(Y) - c$ is absolutely irreducible over $\mathbb{F}_{q^n}$ for all $c \in \mathbb{F}_{q^n}$. Therefore, $f(X, Y)$ defines an absolutely irreducible curve over $\mathbb{F}_{q^n}$.*

We can generalize the result on the absolute irreducibility of $X^k - L(Y) - c$ to $G(X)^k - L(Y) - c$. In this case, we need the intersection theory of plane curves. We hence recall some basic facts related to plane curves over finite fields. For details, we refer to [5, Chapter 3]. Let $\mathcal{X}$ be the curve defined by $f(X, Y)$. Then the degree of $\mathcal{X}$ is the degree of $f(X, Y)$. A component of $\mathcal{X}$ is a curve $\mathcal{Y}$ for which the defining polynomial $g(X, Y)$ of $\mathcal{Y}$ divides $f(X, Y)$.

Let $\mathcal{X}$ be a curve with the defining equation $f(X, Y)$ and ℓ be a line with the defining equation $bX - aY + c$, which is not a component of $\mathcal{X}$. We can parametrize ℓ as follows:

$$x = x_0 + at \quad y = y_0 + bt \ \text{ for } t \in \bar{\mathbb{F}}_{q^n} \ .$$

As ℓ is not a factor of $f(X, Y)$, we have

$$f(x, y) = f(x_0 + at, y_0 + bt) = f_m t^m + \cdots + f_d t^d \in \bar{\mathbb{F}}_{q^n}[t] \quad \text{with} \quad f_m \neq 0 \ .$$

Then $m := m(P, \mathcal{X} \cap \ell)$ is called the intersection multiplicity of $\mathcal{X}$ and ℓ at P. For $P \in \mathcal{X}$,

$$m_P(\mathcal{X}) := \min\{m(P, \mathcal{X} \cap \ell) \mid P \in \ell\}$$

is called the multiplicity of $\mathcal{X}$ at P. If $m_P(\mathcal{X}) = 1$, then P is called a non-singular point; otherwise it is called singular. The point $P = (x_0, y_0)$ is a singular point of $\mathcal{X}$ if and only if

$$\frac{\partial f(X, Y)}{\partial X}(x_0, y_0) = \frac{\partial f(X, Y)}{\partial Y}(x_0, y_0) = 0 \ ,$$

where $\partial f / \partial X$ and $\partial f / \partial Y$ are the partial derivatives of $f(X, Y)$ with respect to X and Y, respectively.

Let $\mathcal{X}$ and $\mathcal{Y}$ be two plane curves such that $P \in \mathcal{X} \cap \mathcal{Y}$. Then $\mathcal{X}$ and $\mathcal{Y}$ intersect at P with multiplicity

$$m(P, \mathcal{X} \cap \mathcal{Y}) \geq m_P(\mathcal{X}) m_P(\mathcal{Y}) \ ,$$

and equality holds if and only if they do not have a common tangent line at P, see [5, Theorem 3.7]. Moreover we have the following well-known result, see [5, Theorem 3.13].

Proposition 2.3 (Bezout's theorem) *Let $\mathcal{X}$ and $\mathcal{Y}$ be two projective plane curves of degree d_1 and d_2, respectively. If $\mathcal{X}$ and $\mathcal{Y}$ do not have a common component then*

$$\sum_{P \in \mathcal{X} \cap \mathcal{Y}} m(P, \mathcal{X} \cap \mathcal{Y}) = d_1 d_2 \,.$$

Theorem 2.4 *Let k be a positive integer such that $\gcd(q^n - 1, k) > 1$ and $L(X)$ be a separable linearized polynomial. Then $f(X, Y) = G(X)^k - L(Y) - c \in \mathbb{F}_{q^n}[X, Y]$ is absolutely irreducible for any $c \in \mathbb{F}_{q^n}$.*

Proof Let $\mathcal{X}$ be the curve defined by the equation $f(X, Y)$. Note that $\deg G(T)^k \neq \deg L(T)$; hence, there is a unique point P at infinity of multiplicity $d = \deg f(X, Y)$, namely $P = (1 : 0 : 0)$ if $\deg G(T)^k > \deg L(T)$ and $P = (0 : 1 : 0)$ if $\deg G(T)^k < \deg L(T)$. In both cases, the line at infinity is the unique tangent line at P. Since $L(Y)$ is separable and linearized, $\partial f(X, Y)/\partial Y = \alpha$ for some non-zero $\alpha \in \mathbb{F}_{q^n}$. Therefore, $\mathcal{X}$ has no singular affine points.

Suppose that $f(X, Y)$ is not absolutely irreducible. Then $\mathcal{X} = \mathcal{X}_1 \cup \mathcal{X}_2$ for some curves $\mathcal{X}_1$ and $\mathcal{X}_2$ of degree d_1 and d_2, respectively. As $\mathcal{X}$ has no affine singular point, $\mathcal{X}_1$ and $\mathcal{X}_2$ have no intersection in the affine plane. In particular, $\mathcal{X}_1$ and $\mathcal{X}_2$ do not have a common component and intersect only at the unique point P at infinity. As $m_P(\mathcal{X}_i) \le d_i$ and

$$d_1 + d_2 = d = m_P(\mathcal{X}) = m_P(\mathcal{X}_1) + m_P(\mathcal{X}_2) \,,$$

we conclude that $m_P(\mathcal{X}_i) = d_i$ for $i = 1, 2$. Then the intersection multiplicity $m(P, \mathcal{X}_1 \cap \mathcal{X}_2)$ of $\mathcal{X}_1$ and $\mathcal{X}_2$ at P satisfies

$$m(P, \mathcal{X}_1 \cap \mathcal{X}_2) \ge m_P(\mathcal{X}_1) m_P(\mathcal{X}_2) = d_1 d_2 \,. \tag{2.3}$$

Since the line at infinity is the common tangent at P, the equality in (2.3) cannot hold, i.e., we have

$$m(P, \mathcal{X}_1 \cap \mathcal{X}_2) > d_1 d_2 \,.$$

However, by Bezout's Theorem, we have $m(P, \mathcal{X}_1 \cap \mathcal{X}_2) = d_1 d_2$, which is a contradiction. □

3 Curves over finite fields and permutation polynomials

Let $P(X) = G(X)^k - L(X)$ for some $G(X) \in \mathbb{F}_{q^n}[X]$ and a linearized polynomial $L(X) \in \mathbb{F}_{q^n}[X]$. For $c \in \mathbb{F}_{q^n}$, we consider the curve $\mathcal{X}_c$ defined by the equation $G(X)^k = L(Y) + c$. Recall that an affine point $(x, y) \in \mathcal{X}_c$ is called rational if $x, y \in \mathbb{F}_{q^n}$. We denote by $N(\mathcal{X}_c)$ the number of affine rational points of $\mathcal{X}_c$.

The following result relates the number of affine rational points of curves $\mathcal{X}_c$ with the permutation property of polynomials $P(X)$. The proof is similar to the proof of [1, Theorem 3.1]. We present it here for the sake of convenience of the reader.

Proposition 3.1 *If there exists $c \in \mathbb{F}_{q^n}$ such that $N(\mathcal{X}_c) > q^n$, then $P(X)$ is not a permutation of $\mathbb{F}_{q^n}$.*

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

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

Note that $\mathcal{L}$ covers all affine rational points in the plane; hence, it covers all affine rational points on $\mathcal{X}_c$. Since $N(\mathcal{X}_c) > q^n$ and $|\mathcal{L}| = q^n$, there exists $d \in \mathbb{F}_{q^n}$ such that ℓ_d intersects with $\mathcal{X}_c$ at least in two distinct affine rational points P_1 and P_2. Note that $P_1 = (x_1, x_1 + d)$, $P_2 = (x_2, x_2 + d)$ for some $x_1, x_2 \in \mathbb{F}_{q^n}$ since $P_1, P_2 \in \ell_d$. Then $P_1 \neq P_2$ implies that $x_1 \neq x_2$. Furthermore, we have

$$G(x_1)^k - L(x_1 + d) = G(x_2)^k - L(x_2 + d) = c$$

since $P_1, P_2 \in \mathcal{X}_c$, which is defined by the equation $G(X)^k = L(Y) + c$. Since L is a linearized polynomial, i.e., $L(x_i + d) = L(x_i) + L(d)$ for $i = 1, 2$, we have

$$P(x_1) = G(x_1)^k - L(x_1) = G(x_2)^k - L(x_2) = P(x_2) = L(d) + c$$

for $x_1, x_2 \in \mathbb{F}_{q^n}$ with $x_1 \neq x_2$. □

Theorem 3.2 *Let $P(X) = G(X)^k - L(X)$ for a linearized polynomial $L(X) \in \mathbb{F}_{q^n}[X]$ and a polynomial $G(X) \in \mathbb{F}_{q^n}[X]$. If $P(X)$ is a permutation of $\mathbb{F}_{q^n}$, then the curve $\mathcal{X}_c$ defined by $G(X)^k = L(Y) + c$ has exactly q^n affine rational points for all $c \in \mathbb{F}_{q^n}$.*

Proof By Proposition 3.1, it is enough to show that $N(\mathcal{X}_{c_1}) > q^n$ for some $c_1 \in \mathbb{F}_{q^n}$ if and only if $N(\mathcal{X}_{c_2}) < q^n$ for some $c_2 \in \mathbb{F}_{q^n}$. For given $(x, y) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$, there exists a unique $c \in \mathbb{F}_{q^n}$ such that $(x, y) \in \mathcal{X}_c$, namely $c = G(x)^k - L(y)$. Then the fact that there exist q^{2n} pairs (x, y) and q^n curves of the form $\mathcal{X}_c$ gives the desired conclusion. □

We are now ready to show a main result on polynomials of the form $X^k - L(X)$. It generalizes to a large extent earlier results on the case that $L(X) = \gamma \mathrm{Tr}(X)$, see for instance [6, 9] and [1].

Theorem 3.3 *Let k be a positive integer and $L(X) \in \mathbb{F}_{q^n}[X]$ be a linearized polynomial. If* $\gcd(q^n - 1, k) > 1$ *and the kernel* $\mathrm{Ker}(L)$ *of L is non-trivial, then $P(X) = X^k - L(X)$ is not a permutation of $\mathbb{F}_{q^n}$.*

Proof For $c \in \mathbb{F}_{q^n}$, we define $f_c(X, Y) := X^k - L(Y) - c$. We set

$$k_1 := \gcd(q^n - 1, k) \quad \text{and} \quad k_i := \gcd\left(q^n - 1, \frac{k}{k_{i-1} \cdots k_1}\right) \quad \text{for } i \geq 2 .$$

We can write $q^n - 1 = k_s \cdots k_1 \ell$ such that ℓ is relatively prime to $q^n - 1$ and $k_i > 1$ for all $i = 1, \ldots, s$. If $L(Y)$ is not separable, then we can write $L(Y) = \tilde{L}(Y^{p^s})$ for some positive integer s and a separable linearized polynomial $\tilde{L}$. Note that the kernel of $\tilde{L}$ is non-trivial as the kernel of L is non-trivial. Since the maps $X \mapsto X^\ell$ and $Y \mapsto Y^{p^s}$ are permutations of $\mathbb{F}_{q^n}$, there is a one-to-one correspondence between the affine rational points of the curves defined by f_c and $\tilde{f}_c(X, Y) := X^{k_1 \cdots k_s} - \tilde{L}(Y) - c$. Therefore, we can without loss of generality assume that L is separable and $k = k_1 \cdots k_s$.

Denote by $\mathcal{X}_c$ the curve defined by $f_c(X, Y)$. By Theorem 3.2, it is sufficient to show that there exists $c \in \mathbb{F}_{q^n}$ such that the number $N(\mathcal{X}_c)$ of affine rational points of $\mathcal{X}_c$ is not equal to q^n. By Corollary 2.2, we know that $\mathcal{X}_c$ is an absolutely irreducible curve over $\mathbb{F}_{q^n}$. Moreover, by Theorem 2.4, there is a unique point of $\mathcal{X}_c$ at infinity, which is the only singular point of $\mathcal{X}_c$. Let F_c be the function field of $\mathcal{X}_c$. By Theorem 2.1, $F_c = \mathbb{F}_{q^n}(x, y)$ is a function field over $\mathbb{F}_{q^n}$ defined by $x^k = L(y) + c$. It is a well-known fact that each non-singular rational point of $\mathcal{X}_c$ corresponds to a unique rational place of F_c, see [11, Section 3.1]. Moreover, there is a unique place corresponding to the point at infinity, namely the unique place P lying over $(x = \infty)$, see the proof of Theorem 2.1(ii). That is, there is one to one correspondence between the set of affine rational points of $\mathcal{X}_c$ and the set of rational places of F_c except P. As $\mathrm{Ker}(L)$ is non-trivial, there exists $c \in \mathbb{F}_{q^n}$ such that $-c$ does not lie in the image of L. By Theorem 2.1(iii), for this element c we have

$$N(\mathcal{X}_c) = |H \cap (\mathrm{Im}(L) + c)|\ |\mathrm{Ker}(L)|\ k_1\ ,$$

where H be the subgroup generated by ζ^{k_1} for a primitive element ζ of $\mathbb{F}_{q^n}$. In particular, $N(\mathcal{X}_c)$ is divisible by $k_1 > 1$. Since $\gcd(k_1, q^n) = 1$, we conclude that $N(\mathcal{X}_c) \neq q^n$. □

Remark 3.4 The idea to associate a polynomial to an absolutely irreducible curve via the multiplicative and the additive structure of $\mathbb{F}_{q^n}$ is taken from [1], where the permutation property of the polynomials $P(X) = X^k - \gamma\mathrm{Tr}(X)$ is investigated. We remark that in the main result of [1] instead of $\gcd(q^n - 1, k) > 1$, the stronger condition that k divides $q^n - 1$ is imposed.

Note that the curves defined by $X^k - L(Y) - c$ and $G(X)^k - L(Y) - c$ have the same number of affine rational points when G is a permutation of $\mathbb{F}_{q^n}$. As a result, we obtain the following conclusion, which is presented in [3] by using the finite fields arithmetic.

Corollary 3.5 *Let $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$, where G is a permutation of $\mathbb{F}_{q^n}$ and L is a linearized polynomial of non-trival kernel. If $\gcd(q^n - 1, k) > 1$, then $P(X)$ is not a permutation of $\mathbb{F}_{q^n}$.*

In what follows, we deduce conditions on $P(X) = G(X)^k - L(X)$ for which P is, or is not a permutation, where now $G(X)$ is a polynomial of the form

$$G(X) = b_t X^{p^t} + b_{t-1} X^{p^{t-1}} + \cdots + b_0 X + b \in \mathbb{F}_{q^n}[X]\ .$$

This may pave the way for further analysis on polynomials of such forms.

Theorem 3.6 *Let $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$ for linearized polynomials $L(X)$, $G(X) - G(0)$ and a positive integer k such that $\gcd(k, q^n - 1) > 1$. Assume that $|\mathrm{Ker}(G - G(0))| = q^m$ and $|\mathrm{Ker}(L)| = q^s$. Set*

$$S_c = \{\ \eta \in \mathrm{Im}(G)\ |\ \eta^k \in \mathrm{Im}(L + c)\ \}\ . \tag{3.1}$$

If there exists $c \in \mathbb{F}_{q^n}$ such that $|S_c| \neq q^{n-m-s}$, then $P(X)$ is not a permutation of $\mathbb{F}_{q^n}$.

Proof Let $\mathcal{X}_c$ be the curve defined by the equation $f_c(X, Y) = G(X)^k - L(Y) - c$. As in the proof of Theorem 3.3, we can assume that L, $G - G(0)$ are separable linear polynomials and $k = k_1 \cdots k_s$, where k_i, $i = 1, \ldots, s$, are positive integers defined as before. Recall from the proof of Theorem 2.1 that for any rational place P of $F(x_1)$ lying over $(x_{s+1} = \alpha_{s+1})$, the function field $F(x_\ell)$ has a unique rational place lying over $(x_{s+1} = \alpha_{s+1})$ splitting in $F(x_{\ell-1})$ for all $\ell = 2, \ldots, s$. Hence, the number of rational places of $F(x_1)$ is determined by the extension $F(x_1)/F(x_2)$. Therefore, we can without loss of generality assume that $k = k_1$, i.e., k is a divisor of $q^n - 1$.

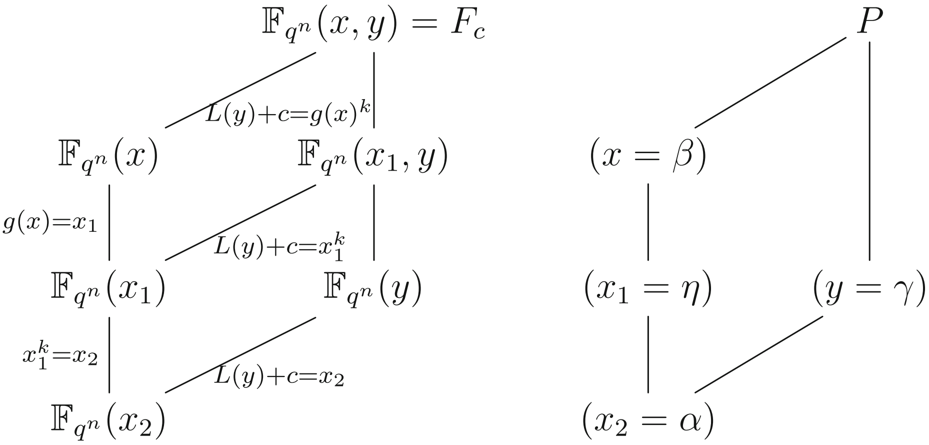

Fig. 2 The function field F_c of $\mathcal{X}_c$

Let F_c be the function field of $\mathcal{X}_c$, see Fig. 2. By Theorem 2.4, we know that F_c is a function field over $\mathbb{F}_{q^n}$. Note that the poles of x and y are the ones lying over $(x_2 = \infty)$. Moreover, $\mathcal{X}_c$ has no singular affine point. Hence there is a one-to-one correspondence between the set of affine rational points of $\mathcal{X}_c$ and the set of rational places of F_c not lying over $(x_2 = \infty)$. Let P be a rational place of F_c lying over $(x_2 = \alpha)$ for some $\alpha \in \mathbb{F}_{q^n}$. Suppose that we have

$$P \mid (x = \beta) \mid (x_1 = \eta) \mid (x_2 = \alpha) \quad \text{and} \quad P \mid (y = \gamma) \mid (x_2 = \alpha)\,.$$

Then $\eta = G(\beta)$ and $\alpha = G(\beta)^k$, see Fig. 2. Since $(y = \gamma)$ is rational, $\alpha = G(\beta)^k$ lies in $\mathrm{Im}(L + c)$. We observe from the defining equation that if there is a rational place of $\mathbb{F}_{q^n}(x)$ lying over $(x_1 = \eta)$, then there are exactly $|\mathrm{Ker}(G - G(0))| = q^m$ rational places of $\mathbb{F}_{q^n}(x)$ lying over $(x_1 = \eta)$, see Kummer's Theorem [12, Theorem 3.3.7]. Similarly, if there exists a rational place P of F_c lying over $(x = \beta)$, then there are exactly $|\mathrm{Ker}(L)| = q^s$ rational places lying over $(x = \beta)$. Therefore, there are exactly q^{m+s} rational places of F_c lying over $(x_1 = \eta)$.

If $P(X)$ is a permutation of $\mathbb{F}_{q^n}$, by Theorem 3.2, the curve $\mathcal{X}_c$ has exactly q^n affine rational points for all $c \in \mathbb{F}_{q^n}$. As for each $G(\beta)$ such that $G(\beta)^k \in \mathrm{Im}(L + c)$, there are exactly q^{m+s} rational places of F_c lying over $(x_1 = G(\beta))$, the set S_c must have cardinality q^{n-m-s}, which gives the desired result. □

Remark 3.7 Note that if $P(X)$ given as in Theorem 3.6 is a permutation polynomial, then $|H \cap \mathrm{Im}(L + c)| \geq \lceil q^{n-m-s}/\gcd(q^n - 1, k)\rceil$ for any $c \in \mathbb{F}_{q^n}$, where $\lceil x \rceil$ denotes the smallest integer bigger than or equal to x.

Corollary 3.8 *Let $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$ be a permutation given as above. If $m + s = n$ and G has no root in $\mathbb{F}_{q^n}$, then* $\gcd(q^n - 1, k) < q^m$.

Proof As in the proof of Theorem 3.6, we can assume that k is a divisor of $q^n - 1$. Let H be the subgroup generated by ζ^k for a primitive element ζ of $\mathbb{F}_{q^n}$. Then the assumption that

G has no root in $\mathbb{F}_{q^n}$ implies that

$$\{G(\beta)^k \mid \beta \in \mathbb{F}_{q^n}\} \subseteq H \ .$$

As $m + s = n$, by Theorem 3.6, we conclude that $|S_c| = 1$ for any $c \in \mathbb{F}_{q^n}$. Hence, each coset of $\mathrm{Im}(L)$ contains exactly one k-th power from the image of G. This implies that X^k is a one-to-one mapping on the image $\mathrm{Im}(G)$ of G. As a result, $|\mathrm{Im}(G^k)| = |\mathrm{Im}(G)| \le |H|$; and hence, we have $q^{n-m} \le (q^n - 1)/k$. In particular, $kq^{n-m} \le q^n - q^{n-m}$, which implies the desired result. ☐

Next we observe that the condition in Corollary 3.8 that $G(X)$ has no root in $\mathbb{F}_{q^n}$ holds, if the degree of G is sufficiently small compared to q^n.

Theorem 3.9 *Let* $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$ *for linearized polynomials* $L(X)$, $G(X) - G(0)$ *and a positive integer* k *such that* $\gcd(k, q^n - 1) > 1$. *Assume that* $|\mathrm{Ker}(G - G(0))| = q^m$ *and* $|\mathrm{Ker}(L)| = q^s$ *with* $m + s = n$. *If* $P(X)$ *is a permutation of* $\mathbb{F}_{q^n}$ *and* $\deg(G) \le q^{n/4}$, *then* $G(X)$ *has no zero in* $\mathbb{F}_{q^n}$.

Proof As in the proof of Theorem 3.6, we can assume that L and G are separable polynomials and k is a divisor of $q^n - 1$. We suppose that G has a root in $\mathbb{F}_{q^n}$. By change of variables, we can assume that 0 is a root of $G(X)$. If $\mathrm{Ker}(G) = \{0\}$, then $L(X)$ is the zero polynomial and $P(X) = G(X)^k$. Then $P(X)$ is not a permutation of $\mathbb{F}_{q^n}$ as X^k is not a permutation.

Now we suppose that $\mathrm{Ker}(G)$ is non-trivial. Hence there exist $\beta_1, \beta_2 \in \mathbb{F}_{q^n}$ with $\beta_1 \ne \beta_2$ such that $G(\beta_1) = G(\beta_2) = 0$. For a k-th root of unity $\zeta_k \ne 1$, we consider $h(X, Y) = G(X) - \zeta_k G(Y)$. Note that we have $G(\beta_1) = \zeta_k G(\beta_2)$, i.e., (β_1, β_2) is a point on the curve $\mathcal{X}_h$ defined by h. By our assumption on separability of G, any affine point of $\mathcal{X}_h$ is non-singular, i.e., (β_1, β_2) is a non-singular rational point of $\mathcal{X}_h$. Then by [2, Lemma 2.1], the factor $\tilde{h} \in \mathbb{F}_{q^n}[X, Y]$ of h passing through (β_1, β_2) is absolutely irreducible. Let $\mathcal{X}_{\tilde{h}}$ be the absolutely irreducible curve over $\mathbb{F}_{q^n}$ defined by $\tilde{h}$. Note that $\tilde{h} \ne X - Y$ as $\beta_1 \ne \beta_2$. By the Hasse-Weil theorem [5, Theorem 9.57], the number $N(\mathcal{X}_{\tilde{h}})$ of rational points of $\mathcal{X}_{\tilde{h}}$ satisfies

$$N(\mathcal{X}_{\tilde{h}}) \ge q^n + 1 - (d - 1)(d - 2)q^{n/2} \ ,$$

where d is the degree of $\tilde{h}$. As $d \le \deg(h(X, Y)) = \deg(G(X)) = q^\ell$ for some $\ell \le n/4$, we have

$$N(\mathcal{X}_{\tilde{h}}) \ge q^n + 1 - (q^\ell - 1)(q^\ell - 2)q^{n/2} \ .$$

Note that $\mathcal{X}_{\tilde{h}}$ has a unique point at infinity, namely $(\eta : 1 : 0)$ such that $\eta^{q^\ell} = \beta$. Moreover, $|\mathcal{X}_{\tilde{h}} \cap (X = Y)| \le \deg(G(X)) = q^\ell$ as $X - Y$ is not a component of $\mathcal{X}_{\tilde{h}}$. Therefore, the number N of affine rational points (β_1, β_2) on $\mathcal{X}_{\tilde{h}}$ with $\beta_1 \ne \beta_2$ satisfies

$$N \ge N(\mathcal{X}_{\tilde{h}}) - (q^\ell + 1) \ge q^n - (q^\ell - 1)(q^\ell - 2)q^{n/2} - q^\ell \ . \tag{3.2}$$

Recall that there are $q^m(q^m - 1)$ pairs (β_1, β_2) with $\beta_1 \ne \beta_2$ and $G(\beta_1) = G(\beta_2)$. If $\ell \le n/4$, then we have $q^m(q^m - 1) \le q^\ell(q^\ell - 1) < N$ by (3.2). This implies that there exists a pair (β_1, β_2) with $\beta_1 \ne \beta_2$ such that $G(\beta_1) \ne G(\beta_2)$ and $G(\beta_1)^k = G(\beta_2)^k$. However, by Theorem 3.6, we know that X^k has to permute the image of G. Hence, we obtain a contradiction. ☐

Corollary 3.10 *Let* $P(X) = G(X)^k - L(X) \in \mathbb{F}_{q^n}[X]$ *be a permutation given as in Theorem 3.6. If* $m + s = n$ *and* $\deg(G) \le q^{n/4}$, *then* $\gcd(q^n - 1, k) < q^m$.

Acknowledgements N.A. is supported by B.A.CF-19-01967.

We would like to thank Wilfried Meidl for his useful comments, which helped to improve the presentation of the manuscript considerably.

References

1. Anbar, N.: Curves over finite fields and permutations of the form $x^k - \gamma \mathrm{Tr}(x)$. Turkish J. Math. **43**(1), 533–538 (2019)
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. Gerike, D., Kyureghyan, G.: Results on permutation polynomials of shape $x^t + \gamma \mathrm{Tr}_{q^n/q}(x^d)$. Combinatorics and Finite Fields, Radon Ser. Comput. Appl. Math., De Gruyter. Berlin **23**, 67–78 (2019)
4. Helleseth, T., Zinoviev, V.: New Kloosterman sums identities over $\mathbb{F}_{2^m}$ for all m. Finite Fields Appl. **9**(2), 187–193 (2003)
5. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over a Finite Field. Princeton University Press (2013)
6. Kyureghyan, G., Zieve, M.: Permutation Polynomials of the Form $X + \gamma \mathrm{Tr}(X^k)$. Contemporary Developments in Finite Fields and Applications, pp. 178–194. World Sci. Publ., Hackensack (2016)
7. 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)
8. Liu, Q., Sun, Y., Zhang, W.G.: Some classes of permutation polynomials over finite fields with odd characteristic. Appl. Algebra Engrg. Comm. Comput. **29**(5), 409–431 (2018)
9. Ma, J., Ge, G.: A note on permutation polynomials over finite fields. Finite Fields Appl. **48**, 261–270 (2017)
10. Mullen, G.L., Panario, D.: Handbook of Finite Fields. Chapman and Hall (2013)
11. Niederreiter, H., Xing, C.P.: Algebraic Geometry in Coding Theory and Cryptography. Princeton University Press, Princeton (2009)
12. Stichtenoth, H.: Algebraic Function Fields and Codes. Second edition Graduate Texts in Mathematics, vol. 254. Springer, Berlin (2009)
13. Tu, Z., Zeng, X., Li, C., Helleseth, T.: Permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over the finite field $\mathbb{F}_{p^{2m}}$ of odd characteristic. Finite Fields Appl. **34**, 20–35 (2015)
14. Wang, L., Wu, B., Liu, Z.: Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2m}}$. Finite Fields Appl. **44**, 92–112 (2017)
15. Xu, G., Cao, X., Xu, S.: Further results on permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$ over $\mathbb{F}_{p^{2m}}$. J. Algebra Appl. **15**(5), 1650098 (2016). 13 pp
16. Yuan, J., Ding, C.: Four classes of permutation polynomials of $\mathbb{F}_{2^m}$. Finite Fields Appl. **13**(4), 869–876 (2007)
17. 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)
18. Zheng, D., Chen, Z.: More classes of permutation polynomials of the form $(x^{p^m} - x + \delta)^s + L(x)$. Appl. Algebra Engrg. Comm. Comput. **28**(3), 215–223 (2017)