Annali di Matematica Pura ed Applicata (1923 -) (2023) 202:2767–2784
https://doi.org/10.1007/s10231-023-01339-6

Investigating rational perfect nonlinear functions

Daniele Bartoli[1] · **Marco Timpanella**[1]

Received: 10 December 2022 / Accepted: 11 April 2023 / Published online: 2 May 2023
© The Author(s) 2023

Abstract

Perfect nonlinear (PN) functions over a finite field, whose study is also motivated by practical applications to Cryptography, have been the subject of several recent papers where the main problems, such as effective constructions and non-existence results, are considered. So far, all contributions have focused on PN functions represented by polynomials, and their constructions. Unfortunately, for polynomial PN functions, the approach based on Hasse–Weil type bounds applied to function fields can only provide non-existence results in a small degree regime. In this paper, we investigate the non-existence problem of rational perfect nonlinear functions over a finite field. Our approach makes it possible to use deep results about the number of points of algebraic varieties over finite fields. Our main result is that no PN rational function f/g with $f, g \in \mathbb{F}_q[X]$ exists when certain mild arithmetical conditions involving the degree of $f(X)$ and $g(X)$ are satisfied.

Keywords Perfect nonlinear functions · Algebraic varieties over finite fields · Lang–Weil bound

Mathematics Subject Classification 06E30 · 11T06

1 Introduction

Since differential cryptanalysis [12, 13, 36] is an important cryptanalytic approach targeting symmetric-key primitives, perfect nonlinear (PN) and almost perfect nonlinear (APN) functions over finite fields and, more in general, functions with low differential uniformity, have been widely investigated in the last years due to their applications in cryptography. To mitigate the threat of differential cryptanalysis, derivatives of functions defined over finite fields have received a lot of interest.

In a discrete setting (usually finite groups), derivatives of functions can be defined as follows.

✉ Marco Timpanella
marco.timpanella@unipg.it

Daniele Bartoli
daniele.bartoli@unipg.it

[1] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Perugia, Italy

Definition 1.1 Let A and B be finite abelian groups and $F : A \to B$ be a function. Given $a \in A$, the function defined by $D_aF : A \to B$, with $D_aF(x) = F(x + a) - F(x)$, is called a derivative of F.

Usually, one is interested in bounding the number of solutions of the equation

$$D_aF(x) = b, \tag{1}$$

for any $a \in A$ and $b \in B$. In the late 1960s, functions $F : A \to B$, with $|A| = |B|$ and with bijective derivatives were studied in connection with projective planes; see [23].

Later on, differential cryptanalysis provided the motivation to study functions for which (1) has always the minimum number of solutions.

Definition 1.2 [37] Let $F : A \to B$ be a function and set

$$\delta(a, b) = \#\{x \in A : F(x + a) - F(x) = b\},$$

for $a \in A$ and $b \in B$. Then, the differential ΔF-uniformity of F is defined to be

$$\Delta F = \max_{a \in A, a \neq 0, b \in B} \delta(a, b).$$

Functions with ΔF equal to 1 or 2 are, respectively, called perfect nonlinear (PN for short) or almost perfect nonlinear (APN for short). Usually, $A = B$ are a finite field $\mathbb{F}_q$, where q is a prime power. Then, if F is a PN function all its derivatives are a bijection of $\mathbb{F}_q$. Permutations and PN functions have been widely investigated in the last years; see e.g., [7, 8, 16, 20–22, 26, 30, 39, 41, 42, 47–49]. Excellent surveys on this topic are [14, 18, 38].

An important subclass of PN functions is given by the so-called exceptional PN functions, i.e., functions which are PN over infinitely many finite fields $\mathbb{F}_q$; see for instance [27, 32, 51].

In the case $q = 2^n$ there are no PN functions, and APN functions have received a lot of attentions; see [1, 4, 9, 26]. Also, a slight modification to the definition of PN functions for the characteristic 2 case was proposed by Zhou [50]; see also [5, 6, 29, 33, 40, 43]. Interestingly, such functions have similar properties and applications as their counterparts in odd characteristic; see [43, 50]. Since in this paper we study PN functions, we will assume from now on $q = p^h$ odd.

Most of the PN or APN functions known so far have specific shapes: they consist of polynomials with few terms (monomials or binomials) or of particular degrees.

Let $\mathbb{A}^r(\mathbb{F}_q)$ and $\mathbb{P}^r(\mathbb{F}_q)$ denote the affine and the projective r-dimensional space over the finite field $\mathbb{F}_q$, respectively. In the polynomial case, a well-known approach to investigate whether $f(X) \in \mathbb{F}_q[X]$ is a PN function consists in attaching to f the surface $\mathcal{S}_f$ of $\mathbb{P}^3(\mathbb{F}_q)$ defined by

$$\mathcal{S}_f : \frac{f(X+Z) - f(X) - f(Y+Z) + f(Y)}{Z(X-Y)} = 0;$$

see [3, Section 10]. Then $f(X)$ is PN over $\mathbb{F}_q$ if and only if all the affine $\mathbb{F}_q$-rational points of $\mathcal{S}_f$ satisfy either $X = Y$ or $Z = 0$.

Note that if $f(X) = X^t$, then $f(X+Z) - f(X) - f(Y+Z) + f(Y)$ is homogenous of degree $t - 1$ and therefore $\mathcal{S}_f$ is actually the curve of affine equation

$$\mathcal{C}_t : \frac{(X+1)^t - X^t - (Y+1)^t + Y^t}{X-Y} = 0. \tag{2}$$

The investigation of $\mathcal{C}_t$ has been crucial to obtain the full classification of exceptional PN monomials; see [27, 32, 51]. As a (standard) terminology, if $f(X) = X^t$ is PN over $\mathbb{F}_q$ we will say that t is a PN exponent in $\mathbb{F}_q$. It is known that if t is an exceptional PN exponent then $t = p^i + p^j, i \geq j \geq 0$, or $t = (3^i + 3^j)/2, i > j \geq 0, i \not\equiv j \pmod 2$; see [27, 32, 51].

For polynomials $f(X)$ with more terms, the surface $\mathcal{S}_f$ is usually more complicated and sophisticated techniques must be employed.

The aim of this paper is to extend this connection between PN functions and algebraic varieties over finite fields to the investigation of rational PN functions.

On the one hand, it is well known that any function over finite fields can be expressed by a polynomial of degree at most $q-1$, although the shape of such a polynomial function can be rather involved. Also, non-existence results, proved by means of Hasse–Weil type bound, can be obtained only in a small degree regime; see [3] and the references therein.

On the other hand, the investigation of the existence of PN functions represented by rational functions instead of polynomials could expand the range of classification results while still manipulating polynomials (the numerator and the denominator of the rational function), and it is the main goal of this paper.

To the best of our knowledge, this problem has never been considered in the literature. In this scenario, a rational function

$$\alpha(X) = \frac{f(X)}{g(X)}, \tag{3}$$

with $f(X), g(X) \in \mathbb{F}_q[X]$, is PN over $\mathbb{F}_q$ if and only if

$$\alpha(X+a) - \alpha(X) = \frac{f(X+a)}{g(X+a)} - \frac{f(X)}{g(X)}$$

is a permutation of $\mathbb{F}_q$ for any $a \in \mathbb{F}_q^*$. Here, without loss of generality we can assume that $f(X)$ and $g(X)$ are coprime and in this case $g(x) \neq 0$ for each $x \in \mathbb{F}_q$ must hold.

The main tool in our investigation is the analysis of specific algebraic varieties over finite fields associated with the rational function $\alpha(X)$.

From now on we fix the following notations for $f(X)$ and $g(X)$:

$$f(X) = X^m + a_{m-1}X^{m-1} + a_{m-2}X^{m-2} + \cdots + a_1X + a_0, \tag{4}$$

$$g(X) = b_nX^n + b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_1X + b_0, \tag{5}$$

with $g(x) \neq 0$ for any $x \in \mathbb{F}_q$, $\gcd(f,g) = 1$, $a_i, b_j \in \mathbb{F}_q$, $b_n \neq 0$.

Note that $f(X)/g(X) - a_n/b_n$ is PN if and only if $f(X)/g(X)$ is PN. So, a_n can be assumed to be 0 (and in particular $\deg(f) \neq \deg(g)$). Also, since $\alpha(X)$ is PN if and only if $\alpha(X^p)$ is PN, we will always assume that $\alpha(X)$ is separable.

In this paper, we investigate necessary conditions on $f(X)$ and $g(X)$ for which $\alpha(X)$ as in (3) is a PN function and our main result is the following; see Proposition 2.6, Theorems 3.3 and 5.5.

Main Theorem Let $\alpha(X) = f(X)/g(X) \in \mathbb{F}_q(X)$, where $f(X)$ and $g(X)$ are as in (4) and (5). Suppose that one of the following holds:

(i) $m < n$;
(ii) $p \nmid (m-n)$, $n < m$, $q > (m-n)^4$, and $m-n$ is not a PN exponent;
(iii) $m-n = p^k + 1$, for some positive integer k, and $2(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)$ is a nonzero square of $\mathbb{F}_q$.

Then $\alpha(X)$ is not PN exceptional.

2 Links with algebraic surfaces

First, we associate to the rational function $\alpha(X)$ the surface $S_\alpha : s_\alpha(X,Y,Z) = 0$, where

$$\begin{aligned} s_\alpha(X,Y,Z) = {} & (f(X+Z)g(X) - f(X)g(X+Z))g(Y+Z)g(Y) \\ & - (f(Y+Z)g(Y) - f(Y)g(Y+Z))g(X+Z)g(X). \end{aligned} \tag{6}$$

Clearly $Z(X-Y)$ divides $s_\alpha(X,Y,Z)$.

An analog of the link mentioned above between PN polynomials and points on algebraic surfaces can can straightforwardly obtained.

Proposition 2.1 *The rational function $\alpha(X)$ is PN over $\mathbb{F}_q$ if and only if S_α does not possess an $\mathbb{F}_q$-rational point (x_0, y_0, z_0) with $x_0 \neq y_0$, $z_0 \neq 0$.*

Proof It is enough to observe that a point $(x_0, y_0, z_0) \in S_\alpha$, with $x_0, y_0, z_0 \in \mathbb{F}_q$, $x_0 \neq y_0$, $z_0 \neq 0$, corresponds to a solution of

$$\alpha(X+Z) - \alpha(X) = \frac{f(X+Z)}{g(X+Z)} - \frac{f(X)}{g(X)} = \frac{f(Y+Z)}{g(Y+Z)} - \frac{f(Y)}{g(Y)} = \alpha(Y+Z) - \alpha(Y).$$

Denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$.

For a hypersurface $\mathcal{F} : F(X_1, \ldots, X_r) = 0$, $F \in \mathbb{F}_q[X_1, \ldots, X_r]$, a component of $\mathcal{F}$ is a hypersurface $\mathcal{G} : G(X_1, \ldots, X_r) = 0$ where $G(X_1, \ldots, X_r) \in \overline{\mathbb{F}}_q[X_1, \ldots, X_r]$ is a non-constant factor of $F(X_1, \ldots, X_r)$. If $\mathcal{F}$ possesses no components apart from itself, the hypersurface $\mathcal{F}$ is called absolutely irreducible. The component $\mathcal{G}$ is said to be $\mathbb{F}_q$-rational if there exists $\lambda \in \overline{\mathbb{F}}_q$ such that $\lambda G \in \mathbb{F}_q[X_1, \ldots, X_r]$.

The q-Frobenius $\phi_q : \overline{\mathbb{F}}_q[X_1, \ldots, X_r] \to \overline{\mathbb{F}}_q[X_1, \ldots, X_r]$ maps each polynomial F to the polynomial $\phi_q(F)$ raising all the coefficients of F to the power q. Clearly $F \in \mathbb{F}_q[X_1, \ldots, X_r]$ if and only if $\phi_q(F) = F$ and in this case we equivalently say that F is defined over $\mathbb{F}_q$.

Proposition 2.1 provides a strong motivation for studying the surface S_α and its $\mathbb{F}_q$ -rational points. In particular, to prove the existence of a suitable point of S_α, it is useful investigating the existence of an absolutely irreducible $\mathbb{F}_q$-rational component of S_α.

In the next sections, we will provide sufficient conditions on the polynomials (4) and (5) to ensure the existence of an absolutely irreducible component defined over $\mathbb{F}_q$ of S_α, distinct from $Z = 0$ and $X - Y = 0$. For a comprehensive introduction on the methods and the basic notions on algebraic varieties and related topics we refer to [28]. In what follows, we list only a few results we will make use in the sequel, whose proofs can be found, for instance, in [3].

The following is a particular case of [1, Lemma 2.1].

Proposition 2.2 *Let H be a hyperplane of $\mathbb{P}^3(\mathbb{F}_q)$ such that $S_\alpha \cap H$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$. Then S_α possesses a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$.*

In the small-degree regime (usually when $\max\{\deg(f), \deg(g)\} \lesssim \sqrt[4]{q}$), the existence of such a component yields the existence of suitable $\mathbb{F}_q$-rational points of S_α, due to estimates on the number of $\mathbb{F}_q$-rational points of an algebraic variety such as the Lang–Weil bound [31] and its generalizations.

Theorem 2.3 (Lang–Weil Theorem) *Let $\mathcal{V} \subset \mathbb{P}^N(\mathbb{F}_q)$ be an absolutely irreducible variety of dimension n and degree d. Then there exists a constant C depending only on N, n, and d such that*

$$\left| \#(\mathcal{V} \cap \mathbb{P}^N(\mathbb{F}_q)) - \sum_{i=0}^{n} q^i \right| \leq (d-1)(d-2)q^{n-1/2} + Cq^{n-1}.$$

Although the constant C was not computed in [31], explicit estimates have been provided for instance in [15, 17, 24, 25, 34, 44] and they have the general shape $C = r(d)$ provided that $q > s(n, d)$, where r and s are polynomials of (usually) small degree. We refer to [17] for a survey on these bounds. We only include the following result due to Cafure and Matera.

Theorem 2.4 [17, Theorem 7.1] *Let $\mathcal{V} \subset \mathbb{A}^N(\mathbb{F}_q)$ be an absolutely irreducible variety defined over $\mathbb{F}_q$ of dimension n and degree d. If $q > 2(n+1)d^2$, then the following estimate holds*:

$$|\#(\mathcal{V} \cap \mathbb{A}^N(\mathbb{F}_q)) - q^n| \leq (d-1)(d-2)q^{n-1/2} + 5d^{13/3}q^{n-1}.$$

In most of the cases, due to Theorem 2.3 and its generalizations, results on PN functions obtained investigating algebraic varieties are presented in terms of exceptional PN functions. In terms of non-exceptional functions, non-existence results can be obtained via Theorem 2.4. Summing up, one of our key tools will be the following.

Theorem 2.5 *Suppose that S_α possesses an absolutely irreducible component defined over $\mathbb{F}_q$ different from $Z = 0$ and $X = Y$. Then $\alpha(X)$ is not exceptional PN. Also, if $q > (3n+m)^{13/3}$ then $\alpha(X)$ is not PN.*

We conclude this section with this observation that proves case (i) of Main Theorem.

Proposition 2.6 *Let $\alpha(X) = f(X)/g(X) \in \mathbb{F}_q(X)$, where f and g are as in* (4) *and* (5). *Suppose that $m < n$. Then $\alpha(X)$ is not PN exceptional.*

Proof In this case $F(X) := \alpha(X+a) - \alpha(X)$ is a rational function whose denominator has degree larger than the one of the numerator. If $F(X)$ permutes $\mathbb{F}_q$, then there exists a unique $\overline{x} \in \mathbb{F}_q$ such that $F(\overline{x}) = 0$. On the other hand, when $F(X)$ is seen as a function on $\mathbb{P}^1(\mathbb{F}_q)$, $F(\infty) = 0$. Thus, ∞ does not belong to the value set of $F(X)$. When q is large enough, this contradicts [19, Theorem 1.2]. □

In view of the previous result, we will focus on rational functions whose denominator has degree smaller than the degree of the numerator, and we will assume, throughout the paper, $m > n$.

3 Necessary conditions from homogeneous parts of high degree in S_α

For $h \in \mathbb{F}_q[X_1, \dots, X_r]$, with the symbol $h^{(i)}$ we denote the homogeneous part of degree i in h. In particular, $h^{(\mathrm{MAX})}$ and $h^{(\min)}$ denote the homogeneous parts of highest and smallest degree, respectively.

Consider the following polynomials

$$\begin{aligned} h_{1,a}(X,Y,Z) &:= (X+Z)^a - (Y+Z)^a + Y^a - X^a,\\ h_{2,a,b}(X,Y,Z) &:= \left((X+Z)^a X^b - X^a(X+Z)^b\right)\left(Y^b + (Y+Z)^b\right)\\ &\quad + ((X+Z)^a - X^a)(Y+Z)^b Y^b\\ &\quad - \left((Y+Z)^a Y^b - Y^a(Y+Z)^b\right)\left(X^b + (X+Z)^b\right)\\ &\quad - ((Y+Z)^a - Y^a)(X+Z)^b X^b. \end{aligned}$$

From now on, let T be the homogeneous coordinate and $\pi_\infty : T = 0$ be the plane at infinity of $\mathbb{P}^3(\mathbb{F}_q)$, and consider $\mathcal{C}_\infty : h^{(\mathrm{MAX})}(X, Y, 1) = 0$ the affine chart of the algebraic curve $S_\alpha \cap \pi_\infty : h^{(\mathrm{MAX})}(X, Y, Z) = 0$, obtained by de-homogenizing with respect to Z. The next result is easily obtained from (6) by direct computation.

Proposition 3.1 *The homogeneous part of highest degree in s_α is*

$$X^n Y^n (X+Z)^n (Y+Z)^n h_{1,m-n}(X,Y,Z).$$

The following fact will be used in the proof of Theorem 3.3.

Remark 3.2 [35, Theorem 8.4.19] Suppose that d is not a PN exponent. If $q > d^4$, then $(X+1)^d - X^d$ is not a permutation and therefore the curve $\mathcal{C}_d : h_{1,d}(X, Y, Z) = 0$ (see (2)) contains an absolutely irreducible component defined over $\mathbb{F}_q$ and distinct from $X = Y$ and $Z = 0$.

We are now in position to prove (*ii*) of Main Theorem.

Theorem 3.3 *Assume that $p \nmid (m-n)$, and $q > (m-n)^4$. If $m-n$ is not a PN exponent, then S_α possesses an absolutely irreducible component defined over $\mathbb{F}_q$ and distinct from $X - Y = 0$ and $Z = 0$. If in addition $q > (3n+m)^{13/3}$, then $\alpha(X)$ is not PN over $\mathbb{F}_q$.*

Proof Since $m-n$ is not a PN exponent, the function X^{m-n} is not PN. Now the curve $\mathcal{C}_\infty = S_\alpha \cap \pi_\infty$ has equation $X^n Y^n (X+Z)^n (Y+Z)^n h_{1,m-n}(X, Y, Z) = 0$ by Proposition 3.1. Also, $h_{1,m-n}(X, Y, Z) = 0$ defines precisely the curve $\mathcal{C}_{m-n}$ as in (2) and thus by Remark 3.2 it possesses an $\mathbb{F}_q$-rational component distinct from $X = Y$ and $Z = 0$. Since $p \nmid m-n$, such a component, which is clearly distinct from $X = 0$, $Y = 0$, $X + Z = 0$, $Y + Z = 0$, is non-repeated in $\mathcal{C}_\infty$. Therefore, by Proposition 2.2, the claim follows. The last part of the claim follows by Theorem 2.5. □

Now, we provide the following general criterion. It will be crucial in the proof of Theorem 3.5. As a notation, for two polynomials F and G, we write $F^k \mid\mid G$ if $F^k \mid G$ and $F^{k+1} \nmid G$. Also, for a prime p and an integer ℓ, $p^k \mid\mid \ell$ if $p^k \mid \ell$ and $p^{k+1} \nmid \ell$.

Proposition 3.4 *Let*

$$s(X,Y,Z) = s^{(M)}(X,Y,Z) + s^{(M-1)}(X,Y,Z) + s^{(M-2)}(X,Y,Z) + \cdots,$$

where each $s^{(i)}$ is either homogeneous of degree i or the zero polynomial, and $s^{(M)} \neq 0$. Let $t(X, Y, Z)$ be a non-constant absolutely irreducible factor of $s^{(M)}(X,Y,Z)$ defined over $\mathbb{F}_q$. Suppose that one of the following holds.

1. $t(X,Y,Z) \nmid s^{(M-1)}(X,Y,Z)$;
2. $s^{(M-1)}(X,Y,Z) = 0$, $t(X,Y,Z)^{2\beta+1} \mid\mid s^{(M)}(X,Y,Z)$ *for some* $\beta \geq 0$, $t(X,Y,Z) \nmid s^{(M-2)}(X,Y,Z)$;
3. $s^{(M-1)}(X,Y,Z) = s^{(M-2)}(X,Y,Z) = 0$, $t(X,Y,Z)^{2\beta+1} \mid\mid s^{(M)}(X,Y,Z)$ *for some* $\beta \geq 0$ *such that* $3 \nmid 2\beta + 1$, $t(X,Y,Z) \nmid s^{(M-3)}(X,Y,Z)$.

Then $s(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

Proof

1. Let $u(X, Y, Z)$ and $v(X, Y, Z)$ be such that $u(X,Y,Z)v(X,Y,Z) = s(X,Y,Z)$. Suppose by the way of contradiction that $t(X,Y,Z) \mid u^{(N)}(X,Y,Z)$ and $t(X,Y,Z) \mid v^{(M-N)}(X,Y,Z)$, where $u^{(N)}(X,Y,Z)$ and $v^{(M-N)}(X,Y,Z)$ are the homogeneous parts of the highest degree in u and v. Then

   $$\begin{aligned} t \mid s^{(M-1)}(X,Y,Z) = u^{(N)}(X,Y,Z)v^{(M-N-1)}(X,Y,Z) \\ + u^{(N-1)}(X,Y,Z)v^{(M-N)}(X,Y,Z), \end{aligned}$$

   a contradiction. This shows that there exists a unique absolutely irreducible factor of $s(X, Y, Z)$ whose highest homogeneous part is divisible by $t(X, Y, Z)$. Such a factor is therefore fixed by the q-Frobenius ϕ_q and thus is defined over $\mathbb{F}_q$.
2. With the same notations as Case 1, assume again by absurd that $t(X, Y, Z)$ divides both $u^{(N)}(X,Y,Z)$ and $v^{(M-N)}(X,Y,Z)$. Since $t(X,Y,Z)^{2\beta+1} \mid\mid s^{(M)}(X,Y,Z)$, without loss of generality we can suppose that $t(X,Y,Z)^{\beta+1} \mid u^{(N)}(X,Y,Z)$. By

   $$\begin{aligned} 0 = s^{(M-1)}(X,Y,Z) = u^{(N)}(X,Y,Z)v^{(M-N-1)}(X,Y,Z) \\ + u^{(N-1)}(X,Y,Z)v^{(M-N)}(X,Y,Z), \end{aligned}$$

   $t(X,Y,Z) \mid u^{(N-1)}(X,Y,Z)$. Therefore

   $$\begin{aligned} t \mid s^{(M-2)}(X,Y,Z) = u^{(N)}(X,Y,Z)v^{(M-N-2)}(X,Y,Z) \\ + u^{(N-1)}(X,Y,Z)v^{(M-N-1)}(X,Y,Z) \\ + u^{(N-2)}(X,Y,Z)v^{(M-N)}(X,Y,Z), \end{aligned}$$

   a contradiction. Arguing as before, this shows that $s(X, Y, Z)$ contains an absolutely irreducible factor defined over $\mathbb{F}_q$.

3. Assume, by absurd, that no absolutely irreducible factor of $s(X, Y, Z)$ is defined over $\mathbb{F}_q$. Then
$$s(X,Y,Z) = \prod_i u_i(X,Y,Z),$$
with u_i absolutely irreducible of degree M_i and such that $t^{\beta_i} \mid\mid u_i^{(M_i)}(X,Y,Z)$. Then $2\beta + 1 = \sum_i \beta_i$. Note that, since no $u_i(X,Y,Z)$ is defined over $\mathbb{F}_q$, for each β_i such that $t^{\beta_i} \mid\mid u_i^{(M_i)}(X,Y,Z)$, there exists at least another $u_{i'}(X,Y,Z)$ (namely $u_{i'}(X,Y,Z) = \phi_q(u_i(X,Y,Z)))$ such that $t^{\beta_i} \mid\mid u_{i'}^{(M_{i'})}(X,Y,Z)$. This also means that $2\beta + 1 \neq \beta_i$ for each i.

Let $\gamma = \min\{\beta_i > 0\}$ and denote by $u(X,Y,Z) = u_{i_\gamma}(X,Y,Z)$, so γ is the highest power of t dividing $u_{i_\gamma}^{(M_{i_\gamma})}(X,Y,Z)$. By the above consideration $\gamma \neq 2\beta + 1$. Also, since $2\beta + 1$ is an odd number not divisible by 3, we are able to rule out the cases $2\beta + 1 \in \{2\gamma, 3\gamma, 4\gamma\}$. Either $\beta_i = \gamma$ for each i and then $2\beta + 1 \geq 5\gamma$ or there exists at least a β_i such that $\beta_i = \gamma' > \gamma$ and
$$2\beta + 1 \geq 2\gamma + 2\gamma' \geq 2\gamma + 2(\gamma + 1) = 4\gamma + 2,$$
which yields $\gamma \leq (\beta - 1)/2$.

Now, let
$$s(X,Y,Z) = u(X,Y,Z)v(X,Y,Z),$$
where $v(X,Y,Z) = \prod_{i \neq i_\gamma} u_i(X,Y,Z)$. As above,
$$\begin{aligned} u(X,Y,Z) &:= u^{(N)}(X,Y,Z) + u^{(N-1)}(X,Y,Z) + u^{(N-2)}(X,Y,Z) + \cdots \\ v(X,Y,Z) &:= v^{(M-N)}(X,Y,Z) + v^{(M-N-1)}(X,Y,Z) + v^{(M-N-2)}(X,Y,Z) + \cdots . \end{aligned}$$

If $t \mid u^{(N-1)}(X,Y,Z)$ and $t \mid v^{(M-N-1)}(X,Y,Z)$, then t divides $s^{(M-3)}(X,Y,Z)$, a contradiction.

Since $s^{(M-1)}(X,Y,Z) = 0$, $t \mid v^{(M-N-1)}(X,Y,Z)$. So we can suppose that $t \nmid u^{(N-1)}(X,Y,Z)$ and $t^{2\beta+1-2\gamma} \mid v^{(M-N-1)}(X,Y,Z)$.

Since $s^{(M-2)}(X,Y,Z) = 0$, $t^{2\beta+1-3\gamma>0} \mid v^{(M-N-2)}(X,Y,Z)$. This yields a contradiction to $t \nmid s_\alpha^{(M-3)}(X,Y,Z)$.

□

Theorem 3.5 *Let* $q > (m-n)^4$, $(m-n)$ *be not a PN exponent, and* $\bar{r}$ *be such that* $p^{\bar{r}} \mid\mid (m-n)$. *Suppose that* f *is not a monomial and define* $\bar{i} = \max\{i \in \{0, \ldots, m-1\} : a_i \neq 0\}$, $\bar{j} = \max\{j \in \{0, \ldots, n-1\} : b_j \neq 0\}$.

Assume that one of the following cases holds.

1. $0 < m - \bar{i} \leq 2,\ n < \bar{i},\ n - \bar{j} > m - \bar{i},\ \gcd((m-n)/p^{\bar{r}} - 1, (\bar{i} - n)/p^k - 1) = 1,$ *where* $p^k \mid\mid (\bar{i} - n)$;
2. $m = \bar{i} + 3, n < \bar{i}, n - \bar{j} > 3, \gcd((m-n)/p^{\bar{r}} - 1, (\bar{i} - n)/p^k - 1) = 1,$ *where* $p^k \mid\mid (\bar{i} - n)$, *and* $p \neq 3$;
3. $0 < n - \bar{j} \leq 2, m - \bar{i} > n - \bar{j}, \gcd((m-n)/p^{\bar{r}} - 1, m + \bar{j} - 2n - 1) = 1, p \nmid (m - \bar{j})$;

4. $n = \bar{j} + 3$, $m - \bar{i} > 3$, $\gcd((m-n)/p^{\bar{r}} - 1, m + \bar{j} - 2n - 1) = 1$, $p \nmid (m - \bar{j})$, *and* $p \neq 3$.

Then $S_\alpha(X, Y, Z)$ possesses an absolutely irreducible component defined over $\mathbb{F}_q$ distinct from $X = Y$ and $Z = 0$. Thus $\alpha(X)$ is not PN exceptional. If in addition $q > (3n + m)^{13/3}$, then $\alpha(X)$ is not PN over $\mathbb{F}_q$.

Proof Since $m > n$,

$$s_\alpha(X, Y, Z)^{(\mathrm{MAX})} = X^n Y^n (X + Z)^n (Y + Z)^n h_{1,m-n}(X, Y, Z).$$

By Remark 3.2, $h_{1,(m-n)/p^{\bar{r}}}(X, Y, Z)$ possesses an absolutely irreducible factor $\bar{h}(X, Y, Z)$ defined over $\mathbb{F}_q$ and different from $X - Y$ and Z, and therefore

$$\bar{h}(X, Y, Z)^{(\mathrm{MAX})} \mid h_{1,(m-n)/p^{\bar{r}}}(X, Y, Z)/(X - Y).$$

We will prove that such a factor is not a factor of $s_\alpha(X, Y, Z)^{(N)}$, the second highest homogeneous part in $s_\alpha(X, Y, Z)$. Note that

$$s_\alpha^{(N)}(X, Y, Z) = \begin{cases} X^n Y^n (X + Z)^n (Y + Z)^n h_{1,\bar{i}-n}(X, Y, Z), & \text{if Cases 1–2 hold;} \\ X^{\bar{j}} Y^{\bar{j}} (X + Z)^{\bar{j}} (Y + Z)^{\bar{j}} h_{2,m-\bar{j},n-\bar{j}}(X, Y, Z), & \text{if Cases 3–4 hold.} \end{cases}$$

Recall that k is such that $p^k \mid\mid (\bar{i} - n)$. Then

$$h^{(\mathrm{MAX})}_{1,(m-n)/p^{\bar{r}}}(X, Y, 1) = X^{(m-n)/p^{\bar{r}}-1} - Y^{(m-n)/p^{\bar{r}}-1},$$
$$h^{(\mathrm{MAX})}_{1,\bar{i}-n}(X, Y, 1) = X^{(\bar{i}-n)/p^k-1} - Y^{(\bar{i}-n)/p^k-1},$$

, whereas $h^{(\mathrm{MAX})}_{2,m-\bar{j},n-\bar{j}}(X, Y, 1)$ equals

$$\begin{cases} (m - \bar{j}) X^{2(n-\bar{j})} Y^{2(n-\bar{j})} (X^{m-\bar{j}-1-2(n-\bar{j})} - Y^{m-\bar{j}-1-2(n-\bar{j})}), & \text{if } m - \bar{j} - 1 > 2(n - \bar{j}); \\ (m - \bar{j}) X^{m-\bar{j}-1} Y^{m-\bar{j}-1} (X^{2(n-\bar{j})-m+\bar{j}+1} - Y^{2(n-\bar{j})-m+\bar{j}+1}), & \text{if } m - \bar{j} - 1 < 2(n - \bar{j}). \end{cases}$$

By our assumptions,

$$\gcd\left(h^{(\mathrm{MAX})}_{2,m-\bar{j},n-\bar{j}}, h^{(\mathrm{MAX})}_{1,(m-n)/p^{\bar{r}}}\right) = (X - Y),$$

and

$$\gcd\left(h^{(\mathrm{MAX})}_{1,\bar{i}-n}(X, Y, Z), h^{(\mathrm{MAX})}_{1,(m-n)/p^{\bar{r}}}\right) = (X - Y),$$

and therefore $\bar{h}(X, Y, Z) \nmid s_\alpha^{(N)}(X, Y, Z)$. Finally, Proposition 3.4 yields the first part of the claim. The final claims follow from Theorem 2.5. □

4 Necessary conditions from homogeneous parts of low degree in S_α

Other necessary conditions for $\alpha(X)$ to be a PN rational function can be obtained by looking at low degree terms of $f(X)$ and $g(X)$. Our approach is summarized in the following remark.

Remark 4.1 Consider the algebraic curve $\mathcal{C}_0$ with homogeneous equation $s_\alpha^{(\min)}(X,Y,Z)=0$. Assume there exists a simple $\mathbb{F}_q$-rational point P of $\mathcal{C}_0$ off $X=Y$ and $Z=0$. By [11, Lemma 2.9] then there exists an $\mathbb{F}_q$-rational plane π such that $\pi \cap S_\alpha$ possesses a non-repeated absolutely irreducible $\mathbb{F}_q$-rational component. By Proposition 2.2 this yields the existence of an absolutely irreducible component of S_α defined over $\mathbb{F}_q$ distinct from $X-Y=0$ and $Z=0$.

Theorem 4.2 *Suppose that f is not a monomial and define* $\underline{i}=\min\{i \in \{1,\dots,m-1\} : a_i \neq 0\}$, $\underline{j}=\min\{j \in \{1,\dots,n-1\} : b_j \neq 0\}$ *Assume that one of the following cases holds.*

- $a_0 \neq 0$, $\underline{j} < \underline{i}$, $q > \underline{j}^4$, $p \nmid \underline{j}$, and $\underline{j}$ not a PN exponent; or
- $a_0 \neq 0$, $\underline{j} > \underline{i}$, $q > \underline{i}^4$, $p \nmid \underline{i}$, and $\underline{i}$ not a PN exponent; or
- $a_0 = 0$, $q > \underline{i}^4$, $p \nmid \underline{i}$, and $\underline{i}$ not a PN exponent.

Then S_α possesses an absolutely irreducible component defined over $\mathbb{F}_q$ distinct from $X-Y=0$ and $Z=0$. Thus $\alpha(X)$ is not PN exceptional. If in addition $q > (3n+m)^{13/3}$, then $\alpha(X)$ is not PN over $\mathbb{F}_q$.

Proof Assume first $a_0 \neq 0$ and $\underline{j} < \underline{i}$. Then by a straightforward computation

$$s_\alpha^{(\min)}(X,Y,Z) = a_0 b_0^2 b_{\underline{j}}(X^{\underline{j}} - (X+Z)^{\underline{j}} - Y^{\underline{j}} + (Y+Z)^{\underline{j}}).$$

Note that, since $p \nmid \underline{j}$, $s_\alpha^{(\min)}(X,Y,Z)$ does not have repeated factors (to see this it is enough to observe that the number of singular points of $s_\alpha^{(\min)}(X,Y,Z)=0$ in the algebraic closure is finite).

Since $\underline{j}$ is not a PN exponent, the function $X^{\underline{j}}$ is not PN and hence, by Remark 3.2, the algebraic curve $\mathcal{C}_0 : s_\alpha^{(\min)}(X,Y,Z)=0$ possesses an absolutely irreducible component defined over $\mathbb{F}_q$ and distinct from $X=Y$ and $Z=0$. Since such a component is non-repeated and $q > \underline{j}^4$, this component possesses a non-singular $\mathbb{F}_q$-rational point not lying on $X=Y$ and $Z=0$ by the Aubry-Perret Bound (see Theorem 5.2 below). This, together with Remark 4.1, yields the existence of an $\mathbb{F}_q$-rational absolutely irreducible component of S_α distinct from $X=Y$ and $Z=0$. In the remaining cases, the same arguments applied to

$$s_\alpha^{(\min)}(X,Y,Z) = b_0^3 a_{\underline{i}}(X^{\underline{i}} - (X+Z)^{\underline{i}} - Y^{\underline{i}} + (Y+Z)^{\underline{i}}),$$

prove the first claim. The final claims follow from Theorem 2.5. □

5 Links with algebraic curves

Recall that if $p \nmid (m-n)$ and $m-n$ is not a PN exponent, then Theorems 2.5 and 3.3 yield that $\alpha(X)$ is not an exceptional PN rational function. In this section, we want to investigate the case where $m-n$ is a PN exponent. Recall that in this case $m-n = p^i + p^j$, $i \geq j \geq 0$, or $m-n = (3^i+3^j)/2$, $i > j \geq 0$, $i \not\equiv j \pmod 2$; see [27, 32, 51].

In what follows we investigate the case $m-n = p^k+1$. Again, we consider a variety $\mathcal{C}_\alpha^{(a)}$ attached to the rational function $\alpha(X) = f(X)/g(X)$, but this time we see a as a parameter. In this case $\mathcal{C}_\alpha^{(a)}$ is a curve defined by $F_a(X,Y)=0$, where

$$F_a(X,Y) := (f(X+a)g(X) - f(X)g(X+a))g(Y+a)g(Y) \tag{7}$$

$$- (f(Y+a)g(Y) - f(Y)g(Y+a))g(X+a)g(X). \tag{8}$$

Note that the curve $\mathcal{C}_\alpha^{(a)}$ has no affine $\mathbb{F}_q$-rational points off $X-Y=0$ if and only if $\alpha(X+a)-\alpha(X)$ permutes $\mathbb{F}_q$.

A result similar to Proposition 2.1 can be easily obtained.

Proposition 5.1 *The rational function $\alpha(X) \in \mathbb{F}_q(X)$ is a PN function if and only if for any $a \in \mathbb{F}_q^*$ the curve $\mathcal{C}_\alpha^{(a)}$ has no affine $\mathbb{F}_q$-rational points off $X-Y=0$.*

Now, we want to obtain non-existence results for PN rational functions $\alpha(X)$ via an investigation of putative absolutely irreducible $\mathbb{F}_q$-rational components in the curves $\mathcal{C}_\alpha^{(a)}$.

In fact, by the Hasse–Weil Bound [46], absolutely irreducible $\mathbb{F}_q$-rational components provide the existence of $\mathbb{F}_q$-rational points in a small degree regime.

We include here a refined version of Hasse–Weil Bound given by Aubry and Perret, and independently by Leep and Yeomans.

Theorem 5.2 (Aubry-Perret bound) [2, *Corollary* 2.5] *Let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve of degree d. Then*

$$q+1-(d-1)(d-2)\sqrt{q} \leq \#(\mathcal{C} \cap \mathbb{P}^2(\mathbb{F}_q)) \leq q+1+(d-1)(d-2)\sqrt{q}. \tag{9}$$

As a corollary, in a small degree regime we obtain the following.

Corollary 5.3 *Let $\mathcal{C} \subset \mathbb{P}^2(\mathbb{F}_q)$ be an absolutely irreducible curve. If* $\deg(\mathcal{C}) < \sqrt[4]{q}$ *then $\mathcal{C}$ possesses affine $\mathbb{F}_q$-rational points out of $X-Y=0$.*

In order to prove the existence of suitable absolutely irreducible $\mathbb{F}_q$-rational components in $\mathcal{C}_\alpha^{(a)}$, we will make use of the so called local quadratic transformations to deal with resolutions of singularities and branch analysis. Note that local quadratic transformations (see [28, Section 4] and [10, Section 2]) are in particular $\mathbb{F}_q$-birational transformations.

First, we can suppose that the singular point under examination is the origin $O=(0,0)$. Thus, consider a plane curve $\mathcal{C}$ defined by

$$F(X,Y) = F_r(X,Y) + F_{r+1}(X,Y) + \cdots = 0,$$

where each $F_i(X, Y)$ is zero or homogeneous in X and Y and of degree i and $F_r(X, Y) \neq 0$. We can also suppose that $X = 0$ is not a tangent line at O, i.e., $X \nmid F_r(X, Y)$. Clearly, r is the multiplicity of (0, 0). The *geometric transform* of the curve $\mathcal{C}$ is the curve $\mathcal{C}'$ given by $F'(X, Y) = F(X, XY)/X^r$. Note that if $Y = 0$ is not a tangent line at O then we can also consider $\mathcal{C}'$ defined by $F'(X, Y) = F(XY, Y)/Y^r$. By [28, Theorem 4.44], there exists a bijection between the branches of $\mathcal{C}$ centered at the origin and the branches of $\mathcal{C}'$ centered at an affine point on $X = 0$. A finite number of local quadratic transformations can be be performed to determine the total number of branches centered at a point. In particular, if r is coprime with the characteristic and the tangent cone $F_r(X, Y)$ at O splits into non-repeated linear factors (over the algebraic closure) distinct from X then there are precisely r distinct branches centered at O. In fact, distinct linear factors of $F_r(X, Y)$ correspond to distinct affine points of $\mathcal{C}'$ on $X = 0$.

We refer to [28] for a more comprehensive introduction to local quadratic transformations and branches.

In our investigation we will make use of the following result.

Proposition 5.4 ([45, Lemma 7] and [3, Theorem 4.4]) *Suppose that there exists an $\mathbb{F}_q$-rational branch centered at an $\mathbb{F}_q$-rational point of a curve $\mathcal{C}$. Then there exists an absolutely irreducible component of $\mathcal{C}$ which is defined over $\mathbb{F}_q$.*

Since the term of the highest degree in $F_a(X, Y)$ (see (8)) is $aX^{2n}Y^{2n}(X - Y)^{p^k}$, the curve $\mathcal{C}_\alpha^{(a)}$ has three points at infinity. We will investigate the point $(1 : 1 : 0)$ in order to determine conditions for which there exists an $\mathbb{F}_q$-rational branch centered at it. To this aim, we need to consider a change of variables to send $(1 : 1 : 0)$ to the origin $(0 : 0 : 1)$. Let $f(X, T)$ and $g(X, T)$ be the homogenization of f and g and consider the homogenization $F_a(X, Y, T)/T$ of $F_a(X, Y)$, where

$$\begin{aligned} F_a(X, Y, T) := &(f(X + aT, T)g(X, T) - f(X, T)g(X + aT, T))g(Y + aT, T)g(Y, T)\\ &- (f(Y + aT, T)g(Y, T) - f(Y, T)g(Y + aT, T))g(X + aT, T)g(X, T). \end{aligned}$$

Note that $F_a(X, Y, T)$ is actually divisible by T.

Consider now $G_a(X, Y) := F_a(X + 1, 1, Y)$, where $G_a(X, Y)$ reads

$$\begin{aligned} &(f(X + 1 + aY, Y)g(X + 1, Y) - f(X + 1, Y)g(X + 1 + aY, Y))g(1 + aY, Y)g(1, Y)\\ &\quad - (f(1 + aY, Y)g(1, Y) - f(1, Y)g(1 + aY, Y))g(X + 1 + aY, Y)g(X + 1, Y) \qquad (10)\\ &= c_0(X) + c_1(X)Y + c_2(X)Y^2 + c_3(X)Y^3 + \dots . \end{aligned}$$

Note that the origin (0, 0) belongs to $\mathcal{D}_\alpha^{(a)} : G_a(X, Y) = 0$ and that $\mathcal{D}_\alpha^{(a)}$ and $\mathcal{C}_\alpha^{(a)}$ are projectively equivalent. This means that any $\mathbb{F}_q$-rational component of $\mathcal{D}_\alpha^{(a)}$ different from $X = 0$ is mapped into an $\mathbb{F}_q$-rational component of $\mathcal{C}_\alpha^{(a)}$ distinct from $X - Y = 0$.

In order to deal with $G_a(X, Y)$, it is useful to consider the following polynomials

$$\begin{aligned}
f(X+1+aY,Y) &= (X+1)^m + m(X+1)^{m-1}aY + \binom{m}{2}(X+1)^{m-2}a^2Y^2 + \cdots \\
&\quad + a_{m-1}Y\Big((X+1)^{m-1} + (m-1)(X+1)^{m-2}aY \\
&\quad + \binom{m-1}{2}(X+1)^{m-3}a^2Y^2 + \cdots\Big) + a_{m-2}Y^2\Big((X+1)^{m-2} \\
&\quad + (m-2)(X+1)^{m-3}aY + \binom{m-2}{2}(X+1)^{m-4}a^2Y^2 + \cdots\Big) + \cdots, \\
f(X+1,Y) &= (X+1)^m + a_{m-1}Y(X+1)^{m-1} + a_{m-2}Y^2(X+1)^{m-2} + \cdots, \\
f(1+aY,Y) &= 1 + maY + \binom{m}{2}a^2Y^2 + \cdots \\
&\quad + a_{m-1}Y\Big(1 + (m-1)aY + \binom{m-1}{2}a^2Y^2 + \cdots\Big) \\
&\quad + a_{m-2}Y^2\Big(1 + (m-2)aY + \binom{m-2}{2}a^2Y^2 + \cdots\Big) + \cdots, \\
f(1,Y) &= 1 + a_{m-1}Y + a_{m-2}Y^2 + \cdots,
\end{aligned}$$

and

$$\begin{aligned}
g(X+1+aY,Y) &= b_n\Big((X+1)^n + n(X+1)^{n-1}aY + \binom{n}{2}(X+1)^{n-2}a^2Y^2 + \cdots\Big) + \\
&\quad + b_{n-1}Y\Big((X+1)^{n-1} + (n-1)(X+1)^{n-2}aY \\
&\quad + \binom{n-1}{2}(X+1)^{n-3}a^2Y^2 + \cdots\Big) \\
&\quad + b_{n-2}Y^2\Big((X+1)^{n-2} + (n-2)(X+1)^{n-3}aY \\
&\quad + \binom{n-2}{2}(X+1)^{n-4}a^2Y^2 + \cdots\Big) + \cdots, \\
g(X+1,Y) &= b_n(X+1)^n + b_{n-1}Y(X+1)^{n-1} + b_{n-2}Y^2(X+1)^{n-2} + \cdots, \\
g(1+aY,Y) &= b_n\Big(1 + naY + \binom{n}{2}a^2Y^2 + \cdots\Big) + \\
&\quad + b_{n-1}Y\Big(1 + (n-1)aY + \binom{n-1}{2}a^2Y^2 + \cdots\Big) \\
&\quad + b_{n-2}Y^2\Big(1 + (n-2)aY + \binom{n-2}{2}a^2Y^2 + \cdots\Big) + \cdots, \\
g(1,Y) &= b_n + b_{n-1}Y + b_{n-2}Y^2 + \cdots.
\end{aligned}$$

We already know that $G_a(X,Y)$ is divisible by XY, since $F_a(X,Y,T)$ is divisible by $T(X-Y)$, so in Equation (10) the polynomial $c_0(X)$ vanishes. Now, we are interested in the coefficients $c_1(X)$, $c_2(X)$, $c_3(X)$ of Y, Y^2, and Y^3.

By a MAGMA aided computation, recalling that $m = p^k + 1 + n \equiv 1 + n \pmod{p}$, we obtain

$$\begin{aligned}
c_1(X) &= b_n^3a(m-n)(X+1)^{2n}(1-(X+1)^{m-n-1}) = \ b_n^3a(X+1)^{2n}X^{p^k},\\
c_2(X) &= b_n^2a(nab_n+2b_{n-1})(X+2)(X+1)^{2n-1}((X+1)^{m-n-1}-1)\\
&= b_n^2a(nab_n+2b_{n-1})(X+2)(X+1)^{2n-1}X^{p^k},\\
c_3(X) &= \alpha(X+1)^{2n-2}(1-(X+1)^{p^k+2}) + \beta(X+1)^{2n-1}X^{p^k}-\\
&\quad \gamma(X+1)^{2n}(1-(X+1)^{p^k-2}),
\end{aligned} \tag{11}$$

where

$$\begin{aligned}
\alpha &:= -\frac{1}{2}b_na(n^2a^2b_n^2 - na^2b_n^2 + 4nab_{n-1}b_n - 2ab_{n-1}b_n + 2b_{n-1}^2 + 4b_{n-2}b_n),\\
\beta &:= b_na(nab_n+2b_{n-1})^2,\\
\gamma &:= -\frac{1}{2}b_n^2a(n^2a^2b_n - na^2b_n + 4nab_{n-1} - 2ab_{n-1} + 2a_{m-1}b_{n-1} - 2a_{m-2}b_n + 6b_{n-2}).
\end{aligned}$$

We are now in position to prove the main result of this section.

Theorem 5.5 *Let $m-n=p^k+1$ such that $(4n+p^k-1)^4 < q$. If $2(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)$ is a non-zero square of $\mathbb{F}_q$, then $\alpha(X+a)-\alpha(X)$ is not a permutation of $\mathbb{F}_q$ for any $a \in \mathbb{F}_q^*$ and $\alpha(X)$ is not PN. In particular, $\alpha(X)$ is not PN exceptional.*

Proof From (11), the lowest degree parts in $c_1(X)$, $c_2(X)$, $c_3(X)$ are

$$b_n^3aX^{p^k}, \quad 2b_n^2a(nab_n+2b_{n-1})X^{p^k}, \quad -2b_na(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)X,$$

, respectively. Therefore,

$$\begin{aligned}
\frac{G_a(X,Y)}{XY} =& -2b_na(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)Y^2\\
&+ 2b_n^2a(nab_n+2b_{n-1})X^{p^k-1}Y + b_n^3aX^{p^k-1} + \cdots.
\end{aligned}$$

Note that the origin is a double point for $\overline{\mathcal{D}_\alpha^{(a)}} : \frac{G_a(X,Y)}{XY} = 0$ since the smallest degree term in the polynomial defining $\overline{\mathcal{D}_\alpha^{(a)}}$ is Y^2. Now, we apply $(p^k-3)/2$ times the local quadratic transformation $\psi : H(X,Y) \mapsto H(X,XY)/X^2$, obtaining, at the end of this process, the polynomial

$$\overline{G_a}(X,Y) = -2b_na(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)Y^2 + b_n^3aX^2 + \overline{H_a}(X,Y),$$

where $\overline{H_a}(X,Y)$ has only terms of degree larger than 2. By assumption $2(a_{m-1}b_{n-1}b_n - b_{n-1}^2 - a_{m-2}b_n^2 + b_{n-2}b_n)$ is a nonzero square of $\mathbb{F}_q$, then the homogeneous part of the smallest degree in $\overline{G_a}(X,Y)$ factorizes into two distinct linear factors defined over $\mathbb{F}_q$. This means that the origin is the center of two distinct $\mathbb{F}_q$-rational branches of $\overline{\mathcal{D}_\alpha^{(a)}}$ and thus in view of Proposition 5.4, there exists an absolutely irreducible $\mathbb{F}_q$-rational component of $\overline{\mathcal{D}_\alpha^{(a)}}$ which is clearly different from $X=0$ and $Y=0$. This shows that $\mathcal{C}_\alpha^{(a)}$ contains an absolutely irreducible $\mathbb{F}_q$-rational component distinct from $X-Y=0$ and by Proposition 5.1, together with Corollary 5.3, the claim follows. □

6 PN functions on the projective line

It is worth mentioning that another possible environment for PN rational functions could be the projective line $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$. As a notation, $\infty + x = \infty$ for any $x \in \mathbb{F}_q$. In this context, we can give the following definition.

Definition 6.1 Let $F : \mathbb{P}^1(\mathbb{F}_q) \to \mathbb{P}^1(\mathbb{F}_q)$ be a function and set

$$\delta(a,b) = \#\{x \in \mathbb{P}^1(\mathbb{F}_q) \,:\, F(x+a) - F(x) = b\}$$

for $a \in \mathbb{F}_q$, $b \in \mathbb{P}^1(\mathbb{F}_q)$. As usual we denote

$$\Delta F = \max_{a \in \mathbb{F}_q^*, b \in \mathbb{P}^1(\mathbb{F}_q)} \delta(a,b),$$

and F is said to PN (resp. APN) over $\mathbb{P}^1(\mathbb{F}_q)$ if ΔF equals 1 (resp. 2).

Remark 6.2 The equation $F(x+a) - F(x) = b$ always makes sense in $\mathbb{P}^1(\mathbb{F}_q)$, as one can first compute the rational function $G(X) := F(X+a) - F(X) = N(X)/D(X)$, where $N(X), D(X) \in \mathbb{F}_q[X]$, $\gcd(N(X), D(X)) = 1$, $N_{\max}$ and $D_{\max}$ are the leading coefficients of $N(X)$ and $D(X)$, and then consider

$$G(u) := \begin{cases} N(u)/D(u), & \text{if } u \neq \infty, D(u) \neq 0; \\ \infty, & \text{if } u \neq \infty, D(u) = 0; \\ \infty, & \text{if } u = \infty, \deg D < \deg N; \\ 0, & \text{if } u = \infty, \deg D > \deg N; \\ N_{\max}/D_{\max}, & \text{if } u = \infty, \deg D = \deg N. \end{cases}$$

Note that for PN rational functions over $\mathbb{P}^1(\mathbb{F}_q)$, Proposition 2.1 does not hold. However, the following remark holds.

Remark 6.3 If S_α possesses an $\mathbb{F}_q$-rational point (x_0, y_0, z_0) with $x_0 \neq y_0$, $z_0 \neq 0$, then α is neither PN over $\mathbb{F}_q$ nor over $\mathbb{P}^1(\mathbb{F}_q)$. In fact, we deduce that $\alpha(x_0 + z_0) - \alpha(x_0) = \alpha(y_0 + z_0) - \alpha(y_0)$ and thus $\alpha(X+a) - \alpha(X)$ is not a permutation over $\mathbb{F}_q$ nor over $\mathbb{P}^1(\mathbb{F}_q)$.

Proposition 6.4 *Let $\alpha(X) = f(X)/g(X)$ be a PN rational function over $\mathbb{F}_q$. Then $\alpha(X)$ is a PN rational function over $\mathbb{P}^1(\mathbb{F}_q)$ if and only if*

$$\deg(f(X+a)g(X) - f(X)g(X+a)) > \deg(g(X+a)g(X)),$$

for any $a \in \mathbb{F}_q^*$.

Proof The rational function $\alpha(X)$ is PN over $\mathbb{P}^1(\mathbb{F}_q)$ if and only if for every $a \in \mathbb{F}_q$

$$\alpha(x+a) - \alpha(x) = \frac{f(x+a)}{g(x+a)} - \frac{f(x)}{g(x)},$$

permutes $\mathbb{P}^1(\mathbb{F}_q)$ for x ranging in $\mathbb{F}_q$. Since $\alpha(X)$ is a PN rational function over $\mathbb{F}_q$, then $g(x) \neq 0$ for every $x \in \mathbb{F}_q$, and for every $a \in \mathbb{F}_q^*$

$$\alpha(x+a)-\alpha(x)=\frac{f(x+a)}{g(x+a)}-\frac{f(x)}{g(x)},$$

permutes $\mathbb{F}_q$ as x ranges in $\mathbb{F}_q$. Therefore, $\alpha(X)$ is a PN function over $\mathbb{P}^1(\mathbb{F}_q)$ if and only if the function $\frac{f(X+a)}{g(X+a)}-\frac{f(X)}{g(X)}$ takes ∞ to ∞ for every $a \in \mathbb{F}_q^*$, which proves the claim. □

As a corollary, the following holds.

Corollary 6.5 *If* $\alpha(X)$ *is a PN rational function over* $\mathbb{F}_q$ *and* $\deg(f) < \deg(g)$, *then* $\alpha(X)$ *is not PN over* $\mathbb{P}^1(\mathbb{F}_q)$.

Finally, we note that there exist no PN rational functions over $\mathbb{P}^1(\mathbb{F}_q)$ if $\deg(f) < \deg(g) < q$, as it happens for PN exceptional rational functions over $\mathbb{F}_q$; see Proposition 2.6.

Proposition 6.6 *Let* $\alpha(X) = f(X)/g(X) \in \mathbb{F}_q(X)$, *where* $f, g \in \mathbb{F}_q[X]$ *and* $\gcd(f, g) = 1$. *Suppose that* $\deg(f) < \deg(g) < q$. *Then* $\alpha(X)$ *cannot be PN over* $\mathbb{P}^1(\mathbb{F}_q)$.

Proof In this case $F(X) := \alpha(X+a)-\alpha(X)$ is a rational function whose denominator has degree larger than the one of the numerator. Since $F(X)$ maps ∞ to 0, there must exist $x_0 \in \mathbb{F}_q$ such that $g(x_0) = 0$, so that $F(x_0) = \infty$. Now, for each $a \in \mathbb{F}_q^*$ we have that $g(x_0 - a) = 0$ otherwise $F(x_0 - a) = \infty$ since its denominator vanishes at $x_0 - a$ and f and g are coprime. This means that $(X - (x_0 - a)) \mid g(X)$ for each $a \in \mathbb{F}_q^*$ and so $X^q - X \mid g(X)$, a contradiction to $\deg(g) < q$. □

7 Conclusions and open problems

The main aim of this paper is to provide constraints on the structure of PN rational functions. This investigation could be useful in the search for new PN functions with prescribed shape. Since we did not provide examples of PN rational functions, it would be interesting to search for infinite families. Another possible direction is the investigation of APN rational functions.

Acknowledgements The research of D. Bartoli and M. Timpanella was partially supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM). The second author was funded by the project ”VALERE: VAnviteLli pEr la RicErca” of the University of Campania ”Luigi Vanvitelli”, and by the project “Metodi matematici per la firma digitale ed il cloud computing" (Programma Operativo Nazionale (PON) “Ricerca e Innovazione” 2014-2020, University of Perugia). We thank the anonymous referee for her/his helpful suggestions.

Funding Open access funding provided by Università degli Studi di Perugia within the CRUI-CARE Agreement.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Aubry, Y., McGuire, G., Rodier, F.: A few more functions that are not APN infinitely often. In finite fields: theory and applications. Contemp. Math. Amer. Math. Soc. **518**, 23–31 (2010)
2. Aubry, Y., Perret, M.: A Weil theorem for singular curves. In: Arithmetic Geometry and Coding theory (Luminy, 1993), pp. 1–7. de Gruyter, Berlin (1996)
3. Bartoli, D.: Hasse-weil type theorems and relevant classes of polynomial functions. London Mathematical Society Lecture Note Series. In: Proceedings of 28th British Combinatorial Conference, Cambridge University Press, to appear
4. Bartoli, D., Calderini, M., Timpanella, M.: Exceptional crooked functions. Finite Fields Appl. **84**(102109), 12 (2022)
5. Bartoli, D., Schmidt, K.-U.: Low-degree planar polynomials over finite fields of characteristic two. J. Algebra **535**, 541–555 (2019)
6. Bartoli, D., Timpanella, M.: A family of planar binomials in characteristic 2. Finite Fields Appl. **63**, 101651 (2020)
7. Bartoli, D., Timpanella, M.: A family of permutation trinomials over $\mathbb{F}_{q^2}$. Finite Fields Appl. **70**, 101781 (2021)
8. Bartoli, D., Timpanella, M.: On trinomials of type $X^{n+m}(1 + AX^{m(q-1)} + BX^{n(q-1)})$, n, m odd, over $\mathbb{F}_{q^2}$, $q = 2^{2s+1}$. Finite Fields Appl. **72**, 101816 (2021)
9. Bartoli, D., Timpanella, M.: On a conjecture on APN permutations. Cryptogr. Commun. **14**(4), 925–931 (2022)
10. Bartoli, D., Zhou, Y.: Exceptional scattered polynomials. J. Algebra **509**, 507–534 (2018)
11. Bartoli, D., Zhou, Y.: Asymptotics of Moore exponent sets. J. Combin. Theory Ser. A **175**, 105281 (2020)
12. Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
13. Biham, E., Shamir, A.: Differential Cryptanalysis of the Data Encryption Standard. Springer-Verlag, Berlin, Heidelberg (1993)
14. Blondeau, C., Nyberg, K.: Perfect nonlinear functions and cryptography. Finite Fields Appl. **32**, 120–147 (2015)
15. Bombieri, E.: Counting points on curves over finite fields. In: Séminaire Bourbaki : vol. 1972/73, exposés 418-435, number 15 in Séminaire Bourbaki. Springer-Verlag, (1974)
16. Budaghyan, L., Helleseth, T.: New perfect nonlinear multinomials over $\mathbf{F}_{p^{2k}}$ for any odd prime p. In: Sequences and their applications—SETA 2008, volume 5203 of Lecture Notes in Computer Science, pp. 403–414. Springer, Berlin (2008)
17. Cafure, A., Matera, G.: Improved explicit estimates on the number of solutions of equations over a finite field. Finite Fields Appl. **12**(2), 155–185 (2006)
18. Carlet, C., Ding, C.: Highly nonlinear mappings. J. Complex. **20**(2), 205–244 (2004)
19. Cohen, S.D.: Value sets of functions over finite fields. Acta Arith. **39**(4), 339–359 (1981)
20. Coulter, R.S.: The classification of planar monomials over fields of prime square order. Proc. Am. Math. Soc. **134**(11), 3373–3378 (2006)
21. Coulter, R.S., Lazebnik, F.: On the classification of planar monomials over fields of square order. Finite Fields Appl. **18**(2), 316–336 (2012)
22. Coulter, R.S., Matthews, R.W.: Planar functions and planes of Lenz-Barlotti class II. Des. Codes Cryptogr. **10**(2), 167–184 (1997)
23. Dembowski, P., Ostrom, T.G.: Planes of order n with collineation groups of order n^2. Math. Z. **103**, 239–258 (1968)
24. Ghorpade, S.R., Lachaud, G.: Étale cohomology, Lefschetz theorems and number of points of singular varieties over finite fields. Mosc. Math. J. **2**(3), 589–631 (2002)
25. Ghorpade, S.R., Lachaud, G.: Number of solutions of equations over finite fields and a conjecture of Lang and Weil. In: Number theory and discrete mathematics (Chandigarh, 2000). Trends Math., pp. 269–291. Birkhäuser, Basel (2002)
26. Hernando, F., McGuire, G.: On the classification of perfect nonlinear (PN) and almost perfect nonlinear (APN) monomial functions. In: Finite fields and their applications, volume 11 of Radon Ser. Comput. Appl. Math., pp. 145–168. De Gruyter, Berlin (2013)
27. Hernando, F., Mcguire, G., Monserrat, F.: On the classification of exceptional planar functions over $\mathbb{F}_p$. Geom. Dedicata **173**, 1–35 (2014)
28. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over a Finite Field. Princeton University Press, stu - student edition edition (2008)

29. Hu, S., Li, S., Zhang, T., Feng, T., Ge, G.: New pseudo-planar binomials in characteristic two and related schemes. Des. Codes Cryptogr. **76**(2), 345–360 (2015)
30. Kyureghyan, G.M., Pott, A.: Some theorems on planar mappings. In: Arithmetic of finite fields, volume 5130 of Lecture Notes in Comput. Sci., pp. 117–122. Springer, Berlin (2008)
31. Lang, S., Weil, A.: Number of points of varieties in finite fields. Am. J. Math. **76**, 819–827 (1954)
32. Leducq, E.: Functions which are PN on infinitely many extensions of $\mathbb{F}_p$, p odd. Des. Codes Cryptogr. **75**(2), 281–299 (2015)
33. Li, Y., Li, K., Longjiang, Q., Li, C.: Further study of planar functions in characteristic two. J. Algebra **573**, 712–740 (2021)
34. Lidl, R., Niederreiter, H.: Finite fields, volume 20 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, second edition, (1997)
35. Mullen, G.L.: (ed). Handbook of finite fields. Discrete Mathematics and its Applications (Boca Raton). CRC Press, Boca Raton, FL (2013)
36. Murphy, S.: The cryptanalysis of FEAL-4 with 20 chosen plaintexts. J. Cryptol. **2**(3), 145–154 (1990)
37. Nyberg, K.: Differentially uniform mappings for cryptography. In: Advances in cryptology—EUROCRYPT ’93 (Lofthus, 1993), volume 765 of Lecture Notes in Comput. Sci., pp. 55–64. Springer, Berlin (1994)
38. Pott, A.: Almost perfect and planar functions. Des. Codes Cryptogr. **78**(1), 141–195 (2016)
39. Pott, A., Zhou, Y.: A character theoretic approach to planar functions. Cryptogr. Commun. **3**(4), 293–300 (2011)
40. Qu, L.: A new approach to constructing quadratic pseudo-planar functions over $\mathbb{F}_{2^n}$. IEEE Trans. Inform. Theory **62**(11), 6644–6658 (2016)
41. Rónyai, L., Szőnyi, T.: Planar functions over finite fields. Combinatorica **9**(3), 315–320 (1989)
42. Scherr, Z., Zieve, M.E.: Some planar monomials in characteristic 2. Ann. Comb. **18**(4), 723–729 (2014)
43. Schmidt, K.-U., Zhou, Y.: Planar functions over fields of characteristic two. J. Algebraic Combin. **40**(2), 503–526 (2014)
44. Schmidt, W.: Equations Over Finite Fields: An Elementary Approach. Kendrick Press, Heber City (2004)
45. Segre, B., Bartocci, U.: Ovali ed altre curve nei piani di Galois di caratteristica due. Acta Arith. **18**, 423–449 (1971)
46. Weil, A.: On the Riemann hypothesis in functionfields. Proc. Nat. Acad. Sci. U.S.A. **27**, 345–347 (1941)
47. Weng, G., Zeng, X.: Further results on planar DO functions and commutative semifields. Des. Codes Cryptogr. **63**(3), 413–423 (2012)
48. Zha, Z., Kyureghyan, G.M., Wang, X.: Perfect nonlinear binomials and their semifields. Finite Fields Appl. **15**(2), 125–133 (2009)
49. Zha, Z., Wang, X.: New families of perfect nonlinear polynomial functions. J. Algebra **322**(11), 3912–3918 (2009)
50. Zhou, Y.: $(2^n, 2^n, 2^n, 1)$-relative difference sets and their representations. J. Combin. Des. **21**(12), 563–584 (2013)
51. Zieve, M.E.: Planar functions and perfect nonlinear monomials over finite fields. Des. Codes Cryptogr. **75**(1), 71–80 (2015)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.