Designs, Codes and Cryptography (2023) 91:3167–3186
https://doi.org/10.1007/s10623-023-01246-0

# On the exceptionality of rational APN functions

Daniele Bartoli[1] · Giuliana Fatabbi[2] · Francesco Ghiandoni[3]

Received: 30 August 2022 / Revised: 20 February 2023 / Accepted: 6 May 2023 /
Published online: 31 May 2023
© The Author(s) 2023

**Abstract**
We investigate APN functions which can be represented as rational functions and we provide non-existence results exploiting the connection between these functions and specific algebraic varieties over finite fields. This approach allows to classify families of functions when previous approaches cannot be applied.

**Keywords** APN functions · Algebraic varieties · Finite fields

**Mathematics Subject Classification** 11T06

## 1 Introduction

Let $\mathbb{F}_q$ be the finite fields with $q = 2^n$ elements. APN functions in even characteristic, introduced by Nyberg in [27], were investigated not only for their theoretical interest but also in connection with their applications to cryptography [3].

**Definition 1.1** A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is **APN** (Almost Perfect Nonlinear) if

$$\forall \alpha \in \mathbb{F}_q^*, \forall \beta \in \mathbb{F}_q \Rightarrow \#\left\{x \in \mathbb{F}_q : f(x+\alpha) + f(x) = \beta\right\} \leq 2, \tag{1}$$

Moreover, $f$ is APN exceptional if there exist infinite extensions $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ where $f$ is APN.

APN functions have been constructed in connection with several combinatorial and geometrical objects, such as semi-biplanes [13] and dual-hyperovals [16]. In this context these

Communicated by A. Pott.

Daniele Bartoli
daniele.bartoli@unipg.it

Francesco Ghiandoni
francesco.ghiandoni@unifi.it

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

[2] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, Perugia, Italy

[3] Dipartimento di Matematica e Informatica Ulisse Dini, Università degli studi di Firenze, Firenze, Italy

mappings are also called semi-planar [15]. Another application of APN functions is related with the construction of error correcting codes, since each APN function yields a double error correcting BCH-like code.

Equivalence issues play an important role in the study of such functions. The above connection with BCH codes also provides an equivalence definition between APN functions: two APN functions are said to be inequivalent if the (extended) BCH-like codes obtained from them are inequivalent codes (see [4] for more details). This relation is called CCZ-equivalence [12], and it is the most general equivalence relation preserving the APN property.

In the last years, several families of APN functions (see [8] or [11] for a recent list of inequivalent APN families) were constructed. For some of these families the APN property is connected with the existence of polynomials having specific features; see i.e. [6, 7, 9, 31]. It is therefore crucial to understand whether APN functions coming from these constructions exist for infinitely many dimensions or do not.

It is well known that each function $f : \mathbb{F}_q \to \mathbb{F}_q$ can be represented as a polynomial function over $\mathbb{F}_q$ of degree at most $q - 1$.

The two most known families of exceptional APN functions, for each positive integer $k$, are the *Gold* functions $f(x) = x^{2^k+1}$ and the *Kasami-Welch* functions $f(x) = x^{4^k-2^k+1}$, which are APN on $\mathbb{F}_{2^n}$ for all positive integer $n$ that are coprime to $k$ (see [28], for example). The following conjecture was proposed by Aubry, McGuire and Rodier [1].

**Conjecture 1.2** [1]. *The only exceptional APN functions are, up to CCZ-equivalence (see* [5]*, for details), the Gold and Kasami–Welch functions.*

Conjecture 1.2 has been settled by Hernando and McGuire [21] in the case that $f$ is a monomial and many other special cases have been proved in several papers. We refer to [14] for a survey of the extensive recent literature on Conjecture 1.2.

APN functions, and the exceptional ones in particular, have been also investigated in connection with algebraic varieties over finite fields, whose degree strictly depends on the the degree of the corresponding polynomial; see e.g. [21]. In this direction, non-existence results were obtained by means of estimates on the number of $\mathbb{F}_q$-rational points of such varieties, as Hasse–Weil or Lang–Weil bounds, which can be applied only if the degree of the polynomial under investigation is small enough.

On the one hand, using such a machinery non-existence results were obtained only in small-degree regime or of so-called exceptional APN functions.

On the other hand, not all the examples of APN functions are described in the literature by polynomials. In fact, the inverse map $x \mapsto x^{-1}$ is known to be APN on $\mathbb{F}_{2^n}$ with $n$ odd, and thus it is also exceptional. Such a map, seen as a polynomial function, has large degree (the function coincides with $x^{q-2}$) and thus the previous machinery does not apply.

Inspired by this example, we start the investigation of functions which can be represented by rational maps. In a similar way (see Proposition 3.1 and Corollary 3.3), we attach to such a rational function a surface in the three-dimensional projective space and we investigate the number of its $\mathbb{F}_q$-rational points. The advantage of our approach is that functions whose corresponding polynomial has high degree and therefore is not treatable using the former machinery often can be described by a rational function of much smaller degree. In this case the investigation of its $\mathbb{F}_q$-rational points becomes feasible by means of Lang–Weil bound.

Our main achievement is the following.

**Main Theorem** *Let $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$ with $MCD(f, g) = 1$ in $\mathbb{F}_q[X]$, $g(x) \neq 0$ for all $x \in \mathbb{F}_q$, $deg(f) = m$, $deg(g) = d$. Then $\psi$ is not exceptional APN in the following cases.*

1. *$m - d > 0$ odd neither Gold nor Kasami-Welch;*

2. $(m-d)/2 > 0$ *odd, and* $f'/g \notin \mathbb{F}_q^*$ *or* $g' \neq 0$, $f'$ *and* $g'$ *denote the formal derivatives of* $f$ *and* $g$;
3. $d - m > 1$ *odd;*
4. $m = 1 < d$.

*In particular, if in addition* $m + 3d \geq 9$, $m + 3d < 0.45q^{\frac{1}{4}} + 0.5$, *then* $\psi$ *is not an APN function over* $\mathbb{F}_q$.

We want to point out that the above result allows to classify families of functions when previous approaches cannot be applied; see [29, Theorem 4.1]. Let us consider the following.

***Example 1.3*** Let $q = 2^{19}$ and $\psi : \mathbb{F}_q \to \mathbb{F}_q$, defined by $x \mapsto \frac{x}{x^3+x+1}$. It is well known that there exists a unique polynomial $h \in \mathbb{F}_q[X]$ of degree at most $q-1$ such that $\psi(x) = h(x)$ for any $x \in \mathbb{F}_q$. Such a polynomial $h$ can be found by the Lagrange Interpolation Formula, that is $h(X) = \sum_{a \in \mathbb{F}_q} \psi(a)(1-(X-a)^{q-1})$; see [26, Remark 8.1.3]. By computations with MAGMA, one gets that $\deg(f) = q - 1 > \sqrt[4]{q}$ so Rodier's results [29, Theorem 4.1] cannot be applied to establish the APN-ness of $\psi$. However, $9 \leq \deg(X) + 3\deg(X^3 + X + 1) \leq 0.45q^{\frac{1}{4}} + 0.5$, so Main Theorem implies that $\psi$ is not APN over $\mathbb{F}_q$.

## 2 General results

Let $F(X,Y) \in \mathbb{K}[X,Y]$, $\mathbb{K}$ a field, be a polynomial defining an affine plane curve $\mathcal{C} : F(X,Y) = 0$. A plane curve is absolutely irreducible if there are no non-trivial factorizations of its defining polynomial $F(X,Y)$ in $\overline{\mathbb{K}}[X,Y]$, where $\overline{\mathbb{K}}$ is the algebraic closure of $\mathbb{K}$. If $F(X,Y) = \prod_i F^{(i)}(X,Y)$, with $F^{(i)}(X,Y) \in \overline{\mathbb{K}}[X,Y]$ of positive degree, then $\mathcal{C}_i : F^{(i)}(X,Y) = 0$ are called components of $\mathcal{C}$. A component is $\mathbb{F}_q$-rational if it is fixed by the Frobenius morphism $\varphi$ or equivalently $\lambda F^{(i)}(X,Y) \in \mathbb{K}[X,Y]$ for some $\lambda \in \overline{\mathbb{K}}$.

Let $P = (u,v) \in \mathbb{A}^2(\mathbb{K})$ be a point in the plane, and write

$$F(X+u, Y+v) = F_0(X,Y) + F_1(X,Y) + F_2(X,Y) + \cdots,$$

where $F_i$ is either zero or homogeneous of degree $i$. The *multiplicity* of $P \in \mathcal{C}$, written as $m_P(\mathcal{C})$ or $m_P(F)$, is the smallest integer $m$ such that $F_m \neq 0$ and $F_i = 0$ for $i < m$; $F_m = 0$ is the *tangent cone* of $\mathcal{C}$ at $P$. A linear component of the tangent cone is called a *tangent* of $\mathcal{C}$ at $P$. The point $P$ is on the curve $\mathcal{C}$ if and only if $m_P(\mathcal{C}) \geq 1$. If $P$ is on $\mathcal{C}$, then $P$ is a *simple* point of $\mathcal{C}$ if $m_P(\mathcal{C}) = 1$, otherwise $P$ is a *singular* point of $\mathcal{C}$. It is possible to define in a similar way the multiplicity of an ideal point of $\mathcal{C}$, that is a point of the curve lying on the line at infinity. We denote by $Sing(\mathcal{C})$ the set of singular points of the curve $\mathcal{C}$.

Given two plane curves $\mathcal{A}$ and $\mathcal{B}$ and a point $P$ on the plane, the *intersection number* (or *intersection multiplicity*) $I(P, \mathcal{A} \cap \mathcal{B})$ of $\mathcal{A}$ and $\mathcal{B}$ at the point $P$ can be defined by seven axioms. We do not include its precise and long definition here. For more details, we refer to [18] and [22] where the intersection number is defined equivalently in terms of local rings and in terms of resultants, respectively.

For a given plane curve $\mathcal{C}$ and a point $P \in \mathcal{C}$, we denote by $I_{P,max}(\mathcal{C})$ the maximum possible intersection multiplicity of two components of $\mathcal{C}$ at $P \in Sing(\mathcal{C})$. Information on $I_{P,max}(\mathcal{C})$ will be crucial to prove the existence of suitable absolutely irreducible $\mathbb{F}_q$-rational components in $S_\psi$ via Criterion 2.3 (see below). We list here two useful results in this direction.

The first one follows directly from the fact that, given two curves $\mathcal{C}$ and $\mathcal{D}$ with no common tangents at a point $P$,

$$I(P,\mathcal{C}\cap\mathcal{D}) = m_P(\mathcal{C})m_P(\mathcal{D});$$

see e.g. [22, Theorem 3.7].

**Lemma 2.1** *Let $q$ be a prime power and $F(X,Y)\in\mathbb{F}_q[X,Y]$. Let $P=(\alpha,\beta)\in\mathbb{F}_q^2$ and write*

$$F(X+\alpha,Y+\beta)=F_m(X,Y)+F_{m+1}(X,Y)+\ldots,$$

*where $F_i\in\mathbb{F}_q[X,Y]$ is zero or homogeneous of degree $i$ and $F_m\neq 0$. If $F_m(X,Y)\neq 0$ is separable, then $I_{P,max}(\mathcal{C})\leq\lfloor m^2/2\rfloor$.*

**Lemma 2.2** [30, Lemma 4.3] [2, Lemma 2.5] *Let $q=2^n$ and $F(X,Y)\in\mathbb{F}_q[X,Y]$. Let $P=(\alpha,\beta)\in\mathbb{F}_q^2$ and write*

$$F(X+\alpha,Y+\beta)=F_m(X,Y)+F_{m+1}(X,Y)+\ldots,$$

*where $F_i\in\mathbb{F}_q[X,Y]$ is zero or homogeneous of degree $i$ and $F_m\neq 0$. Finally suppose that $F_m=L^m$ with $L$ a linear form. If $L\nmid F_{m+1}$ then $I_{P,max}(\mathcal{C})=0$. If $L^2\nmid F_{m+1}$ then $I_{P,max}(\mathcal{C})\leq m$.*

**Criterion 2.3** [24] *Let $\mathcal{C}: h(X,Y)=0$ be a curve of degree $n$ defined over $\mathbb{F}_q$. If*

$$\sum_{P\in Sing(h)} I_{P,max}(\mathcal{C}) < \frac{2}{9}deg^2(h)$$

*then $\mathcal{C}$ possesses at least one absolutely irreducible component defined over $\mathbb{F}_q$.*

In our approach we associate to a rational function $\psi$ an affine hypersurface, which is an affine variety of codimension one, described by $F(X_1,\ldots,X_r)=0$, where $F\in\mathbb{F}_q[X_1,\ldots,X_r]$. As a notation, $\mathbb{P}^r(\mathbb{F}_q)$ and $\mathbb{A}^r(\mathbb{F}_q)$ (or $\mathbb{F}_q^r$) denote the projective and the affine space of dimension $r\in\mathbb{N}$ over the finite field $\mathbb{F}_q$. We will consider the projective hyperplane $X_0=0$ as hyperplane at infinite and so a projective point is affine if $x_0\neq 0$ and the projective closure of the affine hypersurface $F(X_1,\ldots,X_r)=0$ is the projective one defined by $F^*(X_0,\ldots,X_r)=0$, where $F^*$ is the homogenization of $F$ with respect to $X_0$. A hypersurface is said to be absolutely irreducible if the corresponding polynomial $F(X_1,\ldots,X_r)$ is absolutely irreducible, i.e. it possesses no nontrivial factors over the algebraic closure of $\mathbb{F}_q$. The following result links varieties of different dimension.

**Lemma 2.4** [1, Lemma 2.1] *Let $\mathcal{X}\subseteq\mathbb{A}^N(\mathbb{F}_{2^n})$ be an affine hypersurface and let $\mathcal{H}\subseteq\mathbb{P}^N(\mathbb{F}_{2^n})$ be a projective hypersurface. If $\overline{\mathcal{X}}\cap\mathcal{H}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_{2^n}$, then $\overline{\mathcal{X}}$ has an absolutely irreducible component defined over $\mathbb{F}_{2^n}$.*

Lemma 2.4 yields the following.

**Criterion 2.5** *Let $F\in\mathbb{F}_q[X_1,\ldots,X_N]$ with*

$$F=F_m+F_{m+1}+\cdots+F_{d-1}+F_d,$$

*where $F_i\in\mathbb{F}_q[X_1,\ldots,X_N]$ is zero or a homogeneous polynomial of degree i and $F_mF_d\neq 0$. If $F_m$ or $F_d$ have a non-repeated absolutely irreducible component defined over $\mathbb{F}_q$ then $F$ has an absolutely irreducible component defined over $\mathbb{F}_q$.*

A crucial point in our investigation of rational APN functions is to prove the existence of suitable $\mathbb{F}_q$-rational points in algebraic hypersurfaces $\mathcal{H}$ attached to each rational function. This is reached by proving the existence of absolutely irreducible $\mathbb{F}_q$-rational components in $\mathcal{H}$ and estimates on the number of $\mathbb{F}_q$-rational points of an algebraic variety. We recall here the celebrated results by Lang and Weil [25].

**Theorem 2.6** (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*

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

Although the constant $C$ was not computed in [25], explicit estimates have been provided in the general shape $C = f(d)$ provided that $q > g(n, d)$, where $f$ and $g$ are polynomials of (usually) small degree. We refer to [10] for a survey on these bounds.

We will also frequently use the following corollary of Lucas's theorem (see [17], for example).

**Lemma 2.7** *The binomial coefficient $\binom{n}{m}$ is even if and only if al least one of the base-2 digits of $m$ is greater than the corresponding digit of $n$.*

## 3 APN rational functions

In this paper we consider rational functions over $\mathbb{F}_q$, i.e. elements of $\mathbb{F}_q(X)$, in order to face the exceptionality problem from another point of view.

From now on we will make the following assumptions for $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$:

(A.1) $g(x) \neq 0$ for all $x \in \mathbb{F}_q$;
(A.2) $GCD(f, g) = 1$;
(A.3) $f(X) = a_m X^m + \cdots + a_0$ and $g(X) = b_d X^d + \cdots + b_0$, with $a_m b_d \neq 0$ and $a_i, b_j \in \mathbb{F}_q$;
(A.4) $m \neq d$, since otherwise $\psi$ is CCZ-equivalent to $\frac{f}{g} - \frac{a_m}{b_d} = \frac{f'}{g}$, with $\deg(f') < \deg(g)$.

We will investigate the APN property of $\psi$ via a connection with the algebraic surface $S_\psi$ in $\mathbb{A}^3(\mathbb{F}_q)$ defined by

$$\varphi_\psi(X, Y, Z) := \frac{\theta_\psi(X, Y, Z)}{(X+Y)(X+Z)(Y+Z)} = 0,$$

where $\theta_\psi(X, Y, Z)$ has the following expression

$$f(X)g(Y)g(Z)g(X+Y+Z) + f(Y)g(X)g(Z)g(X+Y+Z) +$$
$$+ f(Z)g(X)g(Y)g(X+Y+Z) + f(X+Y+Z)g(X)g(Y)g(Z).$$

To this aim, it will also be useful to consider the projective closure of $S_\psi$ in $\mathbb{P}^3(\mathbb{F}_q)$, which will be denoted again by $S_\psi$.

Note that if $g(X) = 1$ then $S_\psi$ reads

$$\frac{f(X) + f(Y) + f(Z) + f(X+Y+Z)}{(X+Y)(X+Z)(Y+Z)} = 0,$$

and it coincides with the surface introduced in [23, 29].

As in the polynomial case, the connection between $S_\psi$ and the APN-ness of $\psi$ is straightforward.

**Proposition 3.1** *The rational function $\psi(X)$ is APN if and only if the surface $S_\psi$ has no affine $\mathbb{F}_q$-rational points off $X = Y$, $X = Z$ e $Y = Z$.*

***Proof*** Mimicking the proof in [29] we have that $\psi$ is APN over $\mathbb{F}_q$ if and only if the rational function

$$\eta := \frac{f}{g}(X) + \frac{f}{g}(Y) + \frac{f}{g}(Z) + \frac{f}{g}(X+Y+Z)$$

has no $\mathbb{F}_q$-rational zero off the planes $X = Y$, $X = Z$ and $Y = Z$. Since $g(x) \neq 0$ for all $x \in \mathbb{F}_q$, this holds if and only if $\theta_\psi(X, Y, Z) = \varphi_\psi(X, Y, Z)(X+Y)(X+Z)(Y+Z)$ also has no $\mathbb{F}_q$-rational zero off the planes $X = Y$, $X = Z$ and $Y = Z$, and so the same holds for $\varphi_\psi$.

□

The next theorem is the analogous for rational functions of [29, Theorem 4.1], the proof is essentially the same and it relies on a refined version of the Lang–Weil Theorem proved by Ghorpade e Lachaud in [19]. We point this out here for the reader's convenience.

**Theorem 3.2** *Let $\psi : \mathbb{F}_q \to \mathbb{F}_q$, $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$. If $S_\psi$ has an absolutely irreducible component defined over $\mathbb{F}_q$ not contained in the surface $(X+Y)(X+Z)(Y+Z) = 0$ and $m + 3d \geq 9$, $m + 3d < 0.45q^{\frac{1}{4}} + 0.5$, then $\psi$ is not an APN function over $\mathbb{F}_q$.*

***Proof*** Let $\mathcal{V}$ be such an absolutely irreducible component of $S_\psi$. From a result of Ghorpade and Lachaud in [19], it follows that

$$\#\mathcal{V}(\mathbb{F}_q) \geq q^2 + q + 1 - (m+3d-4)(m+3d-5)q^{3/2} - 18(m+3d)^4 q.$$

Moreover, $\mathcal{V}$ intersects each of the planes $X = Y$, $X = Z$, $Y = Z$ and the plane at infinite in $\mathbb{P}^3(\mathbb{F}_q)$ in at most $q(m+3d-3)+1$ $\mathbb{F}_q$-rational points (see [29, Corollary 3.1]). Hence, by Proposition 3.1, if the inequality

$$q^2 + q + 1 - (m+3d-4)(m+3d-5)q^{3/2} - 18(m+3d)^4 q > 4((m+3d-3)q+1) \tag{3}$$

holds, $\psi$ is not APN on $\mathbb{F}_q$. Inequality (3) is equivalent to

$$q - (m+3d-4)(m+3d-5)q^{1/2} + (-18(m+3d)^4 - 4(m+3d) + 13) - 3/q > 0,$$

which is satisfied for $m + 3d \geq 9$ and $m + 3d < 0.45q^{\frac{1}{4}} + 0.5$ (see [29, Thm 4.1]).

□

**Corollary 3.3** *Let $\psi : \mathbb{F}_q \to \mathbb{F}_q$, $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$. If $S_\psi$ has an absolutely irreducible component defined over $\mathbb{F}_q$ distinct from $X = Y$, $X = Z$ e $Y = Z$, then $\psi$ is not exceptional APN.*

Our strategy in investigating the exceptionality of an APN rational functions consists in providing sufficient conditions on $S_\psi$ to possess suitable absolutely irreducible $\mathbb{F}_q$-rational components. First we focus on the intersection of $S_\psi$ with the hyperplane at infinity $H_\infty \subset \mathbb{P}^3(\mathbb{F}_q)$, which is provided by the curve whose homogeneous equation is defined by the homogeneous part in $\varphi_\psi$ of highest degree.

If $m-d$ is not a power of 2, then it is easy to see that the maximum degree homogeneous component of $\varphi_\psi$ is given by $a_m b_d^3 H_{m,d}$, where $H_{m,d}$ has the following expression

$$\frac{(X^mY^dZ^d+X^dY^mZ^d+X^dY^dZ^m)(X+Y+Z)^d+X^dY^dZ^d(X+Y+Z)^m}{(X+Y)(X+Z)(Y+Z)}. \tag{4}$$

Let us denote by $\mathcal{A}_{m,d}$ the curve of homogeneous equation $H_{m,d}=0$. In what follows, for the sake of convenience, we will also consider the polynomial $G_{m,d} := H_{m,d}(X+Y)(X+Z)(Y+Z)$.

We will consider separately the cases $m>d$ and $m<d$.

## 4 Investigation of rational functions $\psi = f/g$, with deg($f$) > deg($g$)

In this case $G_{m,d}$ and $H_{m,d}$ read as

$$G_{m,d} = X^dY^dZ^d(X+Y+Z)^d(X^{m-d}+Y^{m-d}+Z^{m-d}+(X+Y+Z)^{m-d}),$$
$$H_{m,d} = X^dY^dZ^d(X+Y+Z)^d\frac{X^{m-d}+Y^{m-d}+Z^{m-d}+(X+Y+Z)^{m-d}}{(X+Y)(X+Z)(Y+Z)}.$$

Note that $\dfrac{X^{m-d}+Y^{m-d}+Z^{m-d}+(X+Y+Z)^{m-d}}{(X+Y)(X+Z)(Y+Z)}$ defines the curve associated to the monomial function $x^{m-d}$.

The case $m-d$ odd can be easily investigated.

**Theorem 4.1** *Let $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$. If $m-d>0$ is odd and not Gold or Kasami-Welch, then $S_\psi$ has an absolutely irreducible component defined over $\mathbb{F}_q$ (hence $\psi$ is not an exceptional APN function ).*

***Proof*** Let $e := m-d$. By [21] we have that $\varphi_e = \dfrac{X^e+Y^e+Z^e+(X+Y+Z)^e}{(X+Y)(X+Z)(Y+Z)}$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_2$. Since the polynomial $X$, $Y$ e $X+Y+Z$ do not divide $\varphi_e$, this component is distinct from the lines $X=0$, $Y=0$ and $X+Y+Z=0$ and so $H_{m,d} = X^dY^dZ^d(X+Y+Z)^d\varphi_e$ has a non-repeated absolutely irreducible component defined over $\mathbb{F}_2$. The statement follows by Lemma 2.4 and Corollary 3.3. □

The case $m-d$ even is more complicated as the following remark shows.

***Remark 4.2*** Let $e=m-d=2^jl$, with $j\geq 1$ and $l>1$ odd. Then

$$\begin{aligned} H_{m,d} &= X^dY^dZ^d(X+Y+Z)^d\varphi_e \\ &= X^dY^dZ^d(X+Y+Z)^d((X+Y)(X+Z)(Y+Z))^{2^j-1}\varphi_l^{2^j}. \end{aligned}$$

If $j>1$ then all components of $\mathcal{A}_{d,m}$ are repeated (in fact $g(x)\neq 0$ for all $x\in\mathbb{F}_q$, implies $d=deg(g)\geq 2$), hence Lemma 2.4 cannot be applied.

If $j=1$ each of the three linear components of $(X+Y)(X+Z)(Y+Z)=0$ is a non-repeated absolutely irreducible component of $\mathcal{A}_{m,d}$; again by Lemma 2.4, $S_\psi$ has an absolutely irreducible component defined over $\mathbb{F}_q$. However such component may coincide with one of the three planes $X+Y=0$, $X+Z=0$, $Y+Z=0$. In this case the existence of $\mathbb{F}_q$-rational points of $S_\psi$ off the surface $(X+Y)(X+Z)(Y+Z)=0$ cannot be proved.

We continue our investigation of the case $m-d=2\ell$, $\ell$ odd, characterizing those rational functions $\psi$ for which $\varphi_\psi$ is divisible by $(X+Y)(X+Z)(Y+Z)$. In the following, for a polynomial $f(X)\in\mathbb{F}_q[X]$, we denote by $f'$ the formal derivative of $f$ with respect to $X$.

**Proposition 4.3** *Let $\psi=\frac{f}{g}\in\mathbb{F}_q(X)$. Then $(X+Y)(X+Z)(Y+Z)$ divides $\varphi_\psi$ if and only if $g'=0$ and $f'=\gamma g$, with $\gamma\in\mathbb{F}_q$. If this happens then $f=h^2+X\gamma g$, with $h\in\mathbb{F}_q[X]$.*

***Proof*** If $g'=0$ and $f'=\gamma g$ then there exists $h\in\mathbb{F}_q[X]$ such that $f=h^2+X\gamma g$; namely setting $r:=f+X\gamma g$ we have $r'=\gamma g+\gamma g=0$, hence all terms of $r$ have even degree. Therefore there exist $h,g_1\in\mathbb{F}_q[X]$ such that $r=h^2$ and $g=g_1^2$, so $\psi=\left(\frac{h}{g_1}\right)^2+\gamma X$, i.e. the function $\psi(x)$ is EA-equivalent to $\frac{h}{g_1}(x)$. From the definition of $\varphi_\psi$ it follows immediately that

$$\varphi_\psi=\varphi_{(\frac{h}{g_1})^2}=(\varphi_{\frac{h}{g_1}})^2(X+Y)(X+Z)(Y+Z).$$

Vice versa, suppose $(X+Y)(X+Z)(Y+Z)$ divides $\varphi_\psi$.

We have that $(X+Y)\mid\varphi_\psi$ if and only if $(X+Y)^2\mid\theta_\psi$. This implies $(X+Y)^2\mid\frac{\partial\theta_\psi}{\partial X}$ and in particular

$$\begin{aligned}\frac{\partial\theta_\psi}{\partial X}(X,X,Z)=0 \iff & [f'(X)g(X)+f(X)g'(X)]g^2(Z)\\ = & [f'(Z)g(Z)+f(Z)g'(Z)]g^2(X).\end{aligned}\tag{5}$$

Since $GCD(f,g)=1$, it follows that

$$g(X)\mid[f'(X)g(X)+f(X)g'(X)]\Rightarrow g(X)\mid f(X)g'(X)\Rightarrow g'=0,$$

Equality (5) reads

$$f'(X)g(X)g^2(Z)=f'(Z)g(Z)g^2(X),$$

that is

$$\frac{f'(X)}{g(X)}=\frac{f'(Z)}{g(Z)},$$

and so $\dfrac{f'(X)}{g(X)}=\gamma$ for some $\gamma\in\mathbb{F}_q$, i.e. $f'=\gamma g$ and the claim follows. □

**Theorem 4.4** *Let $\psi=\frac{f}{g}\in\mathbb{F}_q(X)$. Let $m-d=2\ell$ with $\ell>1$ odd. If $g'\neq 0$ or $f'\neq\gamma g$ for all $\gamma\in\mathbb{F}_q$ then $\psi$ is not an exceptional APN function.*

***Proof*** By Remark 4.2 it follows that $X+Y=0$ is a non-repeated absolutely irreducible component of $\mathcal{A}_{m,d}$ (maximum degree homogeneous component of $\varphi_\psi$) and therefore Lemma 2.4 guarantees the existence of an $\mathbb{F}_q$-rational absolutely irreducible component of $S_\psi$. Finally, by Proposition 4.3 we have that this component is different from $X=Y$, $X=Z$ e $Y=Z$, and so the statement follows from Corollary 3.3. □

We now briefly discuss the pending case.

***Remark 4.5*** Let $\psi=\frac{f}{g}$ be as in Proposition 4.3, with $g'=0$ and $f'=\gamma g$ with $\gamma\in\mathbb{F}_q$, $m-d=2\ell$, $\ell>0$ odd. As already noticed in the proof of Proposition 4.3, $\psi=(\frac{h}{g_1})^2+\gamma X$ with $g=g_1^2$ and so it is CCZ-equivalent to $\frac{h}{g_1}(x)$. Clearly, $\deg(h)-\deg(g_1)=\ell$ and this case can be studied via Theorem 4.1.

Theorem 4.4 and Remark 4.5 yields points 1. and 2. in Main Theorem.

## 5 Investigation of rational functions $\psi = f/g$, with $\deg(f) < \deg(g)$

We recall that the maximum degree homogeneous component of $\varphi_\psi$ is given by $a_m b_d^3 H_{m,d}$, where $H_{m,d}$ is as in (4). Direct computations show that, in this case, $H_{m,d}$ reads

$$H_{m,d} = X^m Y^m Z^m (X+Y+Z)^m \frac{F_{m,d}(X,Y,Z)}{(X+Y)(X+Z)(Y+Z)}, \tag{6}$$

where $F_{m,d}$ is

$$(Y^{d-m}Z^{d-m} + X^{d-m}Z^{d-m} + X^{d-m}Y^{d-m})(X+Y+Z)^{d-m} + X^{d-m}Y^{d-m}Z^{d-m}. \tag{7}$$

A first result can be easily obtained in the special case $m = 1$.

**Proposition 5.1** *Let $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$. If $m = 1 < d$ then $\psi$ is not an exceptional APN function.*

***Proof*** If $m = 1$ it is immediate to see that, $X+Y+Z$, $X$, $Y$ and $Z$ are non-repeated absolutely irreducible factors of (6) and so they are non-repeated absolutely irreducible factors of $H_{m,d}$. By Lemma 2.4 we have that $\varphi_\psi$ has a non-repeated absolutely irreducible defined over $\mathbb{F}_q$, off the surface $(X+Y)(X+Z)(Y+Z) = 0$ and so the conclusion follows from Corollary 3.3. □

For the case $m > 1$, we exploit a method introduced in [23] via the investigation of singular points of the curves

$$\mathcal{A}_{m,d} : \frac{F_{m,d}(X,Y,Z)}{(X+Y)(X+Z)(Y+Z)} = 0,$$

and

$$\mathcal{C}_{m,d} : F_{m,d}(X,Y,Z) = 0;$$

see Criterion 2.3.

In particular, our aim is to prove the existence of an absolutely irreducible $\mathbb{F}_q$-rational component of the curve $\mathcal{A}_e$. We proceed as follows.

1. We determine the set $Sing(\mathcal{A}_e)$ of singular points of $\mathcal{A}_e$; see below.
2. For each point $P \in Sing(\mathcal{A}_e)$ we provide upperbounds on $I_{P,max}(\mathcal{A}_e)$; see Propositions 5.3 and 5.8.
3. We compute an upper bound on $\sum_{P \in Sing(\mathcal{A}_e)} I_{P,max}(\mathcal{A}_e)$ and obtain the desired result via Criterion 2.3; see Theorem 5.9.

Consider the line $Z = 0$ as line at infinity in $\mathbb{P}^2(\mathbb{F}_q)$. In what follows we will make use of the following notation $e := d - m$, $F_e := F_{m,d}$, $f_e := (F_e)_* = (X^e + Y^e + X^eY^e)(X + Y + 1)^e + X^eY^e$,
$H_e := \dfrac{F_e}{(X+Y)(X+Z)(Y+Z)}$, $h_e := (H_e)_*$, $\mathcal{A}_e := \mathcal{A}_{m,d}$ and $\mathcal{C}_e := \mathcal{C}_{m,d}$.

Observe that $F_e, H_e, f_e, h_e$ are symmetric polynomials and that $deg(F_e) = deg(f_e) = 3e$, $deg(H_e) = deg(h_e) = 3(e-1)$.

***Remark 5.2*** Let $e = d - m = 2^j l$, with $l$ odd. The $\mathbb{F}_q$-automorphism given by $x \mapsto x^{2^j}$ induces an automorphism of $\mathbb{F}_q[X, Y, Z]$, so it immediately follows that

$$H_e = ((X+Y)(X+Z)(Y+Z))^{2^j-1} H_l(X,Y,Z)^{2^j},$$

where

$$H_l(X,Y,Z)=\frac{(Y^lZ^l+X^lZ^l+X^lY^l)(X+Y+Z)^l+X^lY^lZ^l}{(X+Y)(X+Z)(Y+Z)}.$$

If $j>1$, then $H_e$ has only repeated factors, therefore Lemma 2.4 cannot be applied.

Assume $e$ odd. By a direct computation we obtain that the points at infinity of $F_e=0$ are $[1:0:0]$, $[0:1:0]$ and $[1:1:0]$, and they all are singular points. The affine singular points of $F_e=0$ are the singular points of $f_e=0$. Also, a point $P=(\alpha,\beta)\in\mathbb{F}_q^2$ is singular for $f_e=0$ if and only if

$$\begin{cases} f_e(\alpha,\beta)=0\\ \frac{\partial f_e}{\partial X}(\alpha,\beta)=0\\ \frac{\partial f_e}{\partial Y}(\alpha,\beta)=0,\end{cases}$$

or equivalently, if and only if all the following equations hold

$$(\alpha^e+\beta^e)(\alpha+\beta+1)^e=\alpha^e\beta^e[(\alpha+\beta+1)^e+1]; \tag{8}$$

$$\beta^e[\alpha^{e-1}+(\alpha+\beta+1)^{e-1}]=\alpha^{e-1}(\alpha+\beta+1)^{e-1}(\beta+1)(\beta^e+1); \tag{9}$$

$$\alpha^e[\beta^{e-1}+(\alpha+\beta+1)^{e-1}]=\beta^{e-1}(\alpha+\beta+1)^{e-1}(\alpha+1)(\alpha^e+1). \tag{10}$$

Note that $f_e$ is symmetric, and thus $f_e|_Y(\alpha,\beta)=f_e|_X(\beta,\alpha)$. We now distinguish three cases:

(I) $\alpha=0$ or $\beta=0$. If $\alpha=0$, equation (8) yields $\beta^e(\beta+1)^e=0$ and so $\beta=0$ or $\beta=1$. By the symmetry of $f_e$ we have $\alpha=0$ or $\alpha=1$ for $\beta=0$,.

(II) $\alpha+\beta+1=0$. Equation (9) yields $\alpha^{e-1}\beta^e=0$ and so $\alpha=0$ or $\beta=0$.

(III) $\alpha\neq 0\neq\beta$ and $\alpha+\beta+1\neq 0$. Obviously if $P=(\alpha,\beta)$ satisfies (8)-(10), then $F_e|_Z(\alpha,\beta,1)=0$, i.e.

$$\alpha^e\beta^e[(\alpha+\beta+1)^{e-1}+1]+(\alpha+\beta+1)^{e-1}(\alpha+\beta)(\alpha^e+\beta^e)=0. \tag{11}$$

Multiplying (11) by $\alpha+\beta+1$ and replacing it in (8), we get

$$\alpha^e\beta^e(\alpha+\beta)[(\alpha+\beta+1)^e+1]=\alpha^e\beta^e(\alpha+\beta+1)[(\alpha+\beta+1)^{e-1}+1],$$

and therefore

$$(\alpha+\beta+1)^{e+1}=1. \tag{12}$$

Multiplying now Equations (9) and (10) by $(\alpha+\beta+1)^2$ and using (12), we obtain respectively

$$\beta^e[\alpha^{e-1}(\alpha+\beta+1)^2+1]=\alpha^{e-1}(\beta+1)(\beta^e+1),$$
$$\alpha^e[\beta^{e-1}(\alpha+\beta+1)^2+1]=\beta^{e-1}(\alpha+1)(\alpha^e+1),$$

from which we get

$$(\beta^{e+1}+1)(\beta+1)\alpha^{e-1}=(\alpha^{e+1}+1)\beta^e, \tag{13}$$

$$(\alpha^{e+1}+1)(\alpha+1)\beta^{e-1}=(\beta^{e+1}+1)\alpha^e. \tag{14}$$

Note that if $\alpha^{e+1}=1$ then necessarily $\beta^{e+1}=1$ and viceversa. Suppose that $(\alpha^{e+1}+1)(\beta^{e+1}+1)\neq 0$. Multiplying (13) by $\alpha$ and replacing (14) in (13), we have

$$(\beta^{e+1}+1)(\beta+1)(\alpha^{e+1}+1)(\alpha+1)\beta^{e-1}=\alpha(\alpha^{e+1}+1)(\beta^{e+1}+1)\beta^e, \tag{15}$$

and thus $(\alpha+1)(\beta+1)=\alpha\beta$, a contradiction to $\alpha+\beta+1\neq 0$.

Summing up, the affine singular points of $f_e = 0$ are:

1. $(0, 0)$;
2. $(0, 1)$;
3. $(1, 0)$;
4. $(\alpha, \beta)$, with $\alpha^{e+1} = \beta^{e+1} = (\alpha + \beta + 1)^{e+1} = 1$.

In the following we provide upper bounds for each singular point $P$ of $\mathcal{A}_e$ on $I_{P,max}(\mathcal{A}_e)$ in order to apply Criterion 2.3. First, we deal with the ideal points of $\mathcal{A}_e$ and the affine points $(0, 0)$, $(1, 0)$, $(0, 1)$.

**Proposition 5.3** *Let $\mathcal{A}_e : H_e = 0$, with e odd. Then*

$$max \left\{I_{(0,0),max}(h_e = 0),\, I_{(0,1),max}(h_e = 0),\, I_{(1,0),max}(h_e = 0)\right\} \leq \frac{(e-1)^2}{4},$$

$$max \left\{I_{[1:0:0],max}(H_e = 0),\, I_{[0:1:0],max}(H_e = 0),\, I_{[1:1:0],max}(H_e = 0)\right\} \leq \frac{(e-1)^2}{4}.$$

***Proof*** We will discuss each case separately.

1. $P = (0, 0)$. We have

$$f_e = (X^e + Y^e + X^eY^e)(X + Y + 1)^e + X^eY^e = (X + Y)(X + 1)(Y + 1)h_e,$$

so the tangent cone of $f_e = 0$ at $P$ is $X^e + Y^e = 0$. Moreover, $e$ odd implies that all the factors of $X^e + Y^e$ are distinct. Since $f_e = (X + Y)(X + 1)(Y + 1)h_e$, the tangent cone of $h_e = 0$ cannot have repeated factors and by Lemma 2.1

$$I_{(0,0),max}(h_e = 0) \leq \frac{(e-1)^2}{4}.$$

2. $P = (1, 0)$ or $P = (0, 1)$. Consider now

$$\begin{aligned} f_e(X + 1, Y) &= [(X + 1)^e + Y^e + (X + 1)^eY^e](X + Y)^e + (X + 1)^eY^e \\ &= (X + Y)^e + Y^e + f'_e(X, Y), \end{aligned}$$

where $f'_e(X, Y)$ contains terms of degree larger than $e$. Since $(X+Y)^e+Y^e$ is separable, we deduce by Lemma 2.1

$$I_{(1,0),max}(h_e = 0) \leq \frac{(e-1)^2}{4}.$$

From the symmetry of $f_e$ and $h_e$ we deduce that

$$I_{(0,1),max}(h_e = 0) \leq \frac{(e-1)^2}{4}.$$

3. $P = [1 : 0 : 0]$, $P = [0 : 1 : 0]$ or $P = [1 : 1 : 0]$. If we denote by $j_i : \mathbb{F}_q^2 \to \mathbb{P}^2(\mathbb{F}_q)\setminus H_{\infty,i}$, $i = 1, 2, 3$, the embedding of the affine plane into the projective plane with respect to $x_i$ (where $H_{\infty,i}$ denotes the hyperplane $x_i = 0$ ),we have that $j_1^{-1}([1 : 0 : 0]) = (0, 0)$, $j_2^{-1}([0 : 1 : 0]) = (0, 0)$ e $j_1^{-1}([1 : 1 : 0]) = (1, 0)$. By the symmetry of $F_e$ e $H_e$ we finally get

$$max \left\{I_{[1:0:0],max}(H_e = 0),\, I_{[0:1:0],max}(H_e = 0),\, I_{[1:1:0],max}(H_e = 0)\right\} \leq \frac{(e-1)^2}{4}.$$

□

We now investigate the singular points $(\alpha, \beta)$, with $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$, of the curve $f_e = 0$. Note that any upper bound on $I_{P,max}(f_e = 0)$ is also an upper bound for $I_{P,max}(h_e = 0)$, since the curve $h_e = 0$ is a component of the curve $f_e = 0$.

Recall that

$$f_e(X+\alpha, Y+\beta) = C_r + C_{r+1} + \cdots = \sum_{\mu,\nu \geq 0} B_{\mu\nu} X^{\mu} Y^{\nu},$$

where

$$C_k = \sum_{n+m=k} \left[ \left( \binom{e}{n} (X^n \alpha^{e-n} + Y^n \beta^{e-n}) + \sum_{i+j=n} \binom{e}{i}\binom{e}{j} X^i Y^j \alpha^{e-i} \beta^{e-j} \right) \cdot \right.$$
$$\left. \cdot \binom{e}{m} (X+Y)^m (\alpha+\beta+1)^{e-m} \right] + \sum_{i+j=k} \binom{e}{i}\binom{e}{j} X^i Y^j \alpha^{e-i} \beta^{e-j}. \tag{16}$$

The next few propositions deal with singular points $P = (\alpha, \beta)$, with $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$. In particular, in order to provide upper bounds on $I_{P,max}(\mathcal{A}_e)$, we need to determine the two first nonzero polynomials $C_k$.

**Proposition 5.4** *Let $e$ be odd, $e \equiv 2^N - 1 \pmod{2^{N+1}}$, $f_e = (X^e + Y^e + X^e Y^e)(X+Y+1)^e + X^e Y^e$ and consider $P = (\alpha, \beta)$ with $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$. Then $C_k = 0$ for all $k = 0, \ldots, 2^N - 1$.*

***Proof*** First observe that, by Lemma 2.7, $\binom{e}{k} = 1$ for all $k = 0, \ldots, 2^N - 1$. We will proceed by induction on $k$. If $k = 0$ then $C_0 = 0$ since the curve passes through the origin. By direct computations it follows that

$$C_k = \left( \alpha^{e-k} X^k + \beta^{e-k} Y^k + \sum_{i+j=k} \alpha^{e-i} \beta^{e-j} X^i Y^j \right) (\alpha+\beta+1)^e$$
$$+ \frac{X+Y}{\alpha+\beta+1} \left( C_{k-1} + \sum_{i+j=k-1} \alpha^{e-i} \beta^{e-j} X^i Y^j \right) + \sum_{i+j=k} \alpha^{e-i} \beta^{e-j} X^i Y^j.$$

By induction $C_{k-1} = 0$, and therefore

$$C_k = \left( \alpha^{e-k} X^k + \beta^{e-k} Y^k + \sum_{i+j=k} \alpha^{e-i} \beta^{e-j} X^i Y^j \right) (\alpha+\beta+1)^e$$
$$+ \left( \sum_{i+j=k-1} \alpha^{e-i} \beta^{e-j} X^{i+1} Y^j + \sum_{i+j=k-1} \alpha^{e-i} \beta^{e-j} X^i Y^{j+1} \right) (\alpha+\beta+1)^e$$
$$+ \sum_{i+j=k} \alpha^{e-i} \beta^{e-j} X^i Y^j.$$

Note that

$$\sum_{i+j=k-1} \alpha^{e-i} \beta^{e-j} X^{i+1} Y^j = \alpha^{e-k+1} \beta^e X^k + \sum_{\substack{i+j=k \\ i,j \geq 1}} \alpha^{e-i+1} \beta^{e-j} X^i Y^j,$$

$$\sum_{i+j=k-1} \alpha^{e-i} \beta^{e-j} X^i Y^{j+1} = \alpha^e \beta^{e-k+1} Y^k + \sum_{\substack{i+j=k \\ i,j \geq 1}} \alpha^{e-i} \beta^{e-j+1} X^i Y^j,$$

$$\sum_{i+j=k} \alpha^{e-i}\beta^{e-j}X^iY^j = \alpha^{e-k}\beta^e X^k + \alpha^e\beta^{e-k}Y^k + \sum_{\substack{i+j=k\\ i,j\geq 1}} \alpha^{e-i}\beta^{e-j}X^iY^j.$$

Thus

$$\sum_{\substack{i+j=k\\ i,j\geq 1}} \alpha^{e-i+1}\beta^{e-j}X^iY^j + \sum_{\substack{i+j=k\\ i,j\geq 1}} \alpha^{e-i}\beta^{e-j+1}X^iY^j = (\alpha+\beta)\sum_{\substack{i+j=k\\ i,j\geq 1}} \alpha^{e-i}\beta^{e-j}X^iY^j.$$

and finally we obtain

$$\begin{aligned} C_k &= (\alpha+\beta+1)^e\Big(\alpha^{e-k}(1+\beta^e)X^k + \beta^{e-k}(1+\alpha^e)Y^k + \alpha^{e-k+1}\beta^e X^k \\ &\quad +\alpha^e\beta^{e-k+1}Y^k + (\alpha+\beta+1)(\alpha^{e-k}\beta^e X^k + \alpha^e\beta^{e-k}Y^k)\Big) \\ &= 0. \end{aligned}$$

□

In the following we use the notation $B(i,j)$ to denote the coefficient of $X^iY^j$ in $f_e(X+\alpha, Y+\beta)$.

**Proposition 5.5** *Let $e$ be odd, $e \equiv 2^N - 1 \pmod{2^{N+1}}$. Suppose $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$. Then*

- $C_{2^N} = B(2^N,0)X^{2^N} + B(0,2^N)Y^{2^N}$,
- $C_{2^N+1} = B(2^N+1,0)X^{2^N+1} + B(2^N,1)X^{2^N}Y + B(1,2^N)XY^{2^N} + B(0,2^N+1)Y^{2^N+1}$.

***Proof*** By Lemma 2.7 we have $\binom{e}{2^N} = \binom{e}{2^N+1} = 0$ so, from (16), we obtain

$$\begin{aligned} C_{2^N} &= \sum_{\substack{n+m=2^N\\ n,m\geq 1}} \left[\left(X^n\alpha^{e-n} + Y^n\beta^{e-n} + \sum_{i+j=n} X^iY^j\alpha^{e-i}\beta^{e-j}\right)\cdot (X+Y)^m(\alpha+\beta+1)^{e-m}\right] \\ &\quad + \sum_{\substack{i+j=2^N\\ i,j\geq 1}} X^iY^j\alpha^{e-i}\beta^{e-j} + (\alpha+\beta+1)^e \sum_{\substack{i+j=2^N\\ i,j\geq 1}} X^iY^j\alpha^{e-i}\beta^{e-j} \\ &= \frac{X+Y}{\alpha+\beta+1}\left[\sum_{i+j=2^N-1} X^iY^j\alpha^{e-i}\beta^{e-j} + C_{2^N-1} + \frac{\alpha^e+\beta^e+\alpha^e\beta^e}{(\alpha+\beta+1)^{2^N}}(X+Y)^{2^N-1}\right] \\ &\quad + \frac{\alpha+\beta}{\alpha+\beta+1}\sum_{\substack{i+j=2^N\\ i,j\geq 1}} X^iY^j\alpha^{e-i}\beta^{e-j} \\ &= (\alpha+\beta+1)^{e-2^N}(\alpha^e+\beta^e+\alpha^e\beta^e)(X+Y)^{2^N} + (\alpha+\beta+1)^e\left(\frac{\beta^e}{\alpha^{2^N}}X^{2^N} + \frac{\alpha^e}{\beta^{2^N}}Y^{2^N}\right) \\ &= B(2^N,0)X^{2^N} + B(0,2^N)Y^{2^N}, \end{aligned}$$

where

$$B(2^N,0) = \frac{\alpha^{2^N-1} + (\alpha+\beta+1)^{2^N-1}}{\alpha^{2^N}\beta(\alpha+\beta+1)^{2^N}}; \tag{17}$$

$$B(0,2^N) = \frac{\beta^{2^N-1} + (\alpha+\beta+1)^{2^N-1}}{\alpha\beta^{2^N}(\alpha+\beta+1)^{2^N}}. \tag{18}$$

Concerning $C_{2^N+1}$, we get

$$\begin{aligned} C_{2^N+1} = (\alpha+\beta+1)^e & \sum_{\substack{i+j=2^N+1\\ i,j\geq 2}} X^iY^j\alpha^{e-i}\beta^{e-j}\\ & +(X+Y)(\alpha+\beta+1)^{e-1}\sum_{\substack{i+j=2^N\\ i,j\geq 1}} X^iY^j\alpha^{e-i}\beta^{e-j}\\ & +\sum_{\substack{n+m=2^N+1\\ n,m\geq 2}}\Bigg[\Bigg(X^n\alpha^{e-n}+Y^n\beta^{e-n}+\sum_{i+j=n} X^iY^j\alpha^{e-i}\beta^{e-j}\Bigg)\\ & \times(X+Y)^m(\alpha+\beta+1)^{e-m}\Bigg]+\sum_{\substack{i+j=2^N+1\\ i,j\geq 2}} X^iY^j\alpha^{e-i}\beta^{e-j} \end{aligned}$$

From (16), it follows that

$$\sum_{\substack{n+m=2^N+1\\ n,m\geq 2}}\Bigg[\Bigg(X^n\alpha^{e-n}+Y^n\beta^{e-n}+\sum_{i+j=n} X^iY^j\alpha^{e-i}\beta^{e-j}\Bigg)\cdot(X+Y)^m(\alpha+\beta+1)^{e-m}\Bigg]$$

equals $\frac{(X+Y)^2}{(\alpha+\beta+1)^2}G$, where

$$\begin{aligned} G = C_{2^N-1} & +(\alpha^e+\beta^e+\alpha^e\beta^e)(\alpha+\beta+1)^{-2^N}(X+Y)^{2^N-1}\\ & +(\alpha^{e-1}(1+\beta^e)X+\beta^{e-1}(1+\alpha^e)Y)(\alpha+\beta+1)^{1-2^N}(X+Y)^{2^N-2}\\ & +\sum_{i+j=2^N-1} X^iY^j\alpha^{e-i}\beta^{e-j}. \end{aligned}$$

Denote $\sum_{\substack{i+j=2^N+1\\ i,j\geq 2}} X^iY^j\alpha^{e-i}\beta^{e-j}$ by $\theta$. So

$$\begin{aligned} C_{2^N+1} & = \frac{\theta}{\alpha+\beta+1}+\frac{(\alpha+\beta)\theta+\alpha^{-2^N}\beta^{e-1}X^{2^N}Y+\alpha^{e-1}\beta^{-2^N}XY^{2^N}}{\alpha^2+\beta^2+1}+\theta\\ & \quad +\frac{(X+Y)^2}{(\alpha+\beta+1)^2}G\\ & = \frac{\theta}{\alpha+\beta+1}+\frac{(\alpha+\beta)\theta+\alpha^{-2^N}\beta^{e-1}X^{2^N}Y+\alpha^{e-1}\beta^{-2^N}XY^{2^N}}{\alpha^2+\beta^2+1}+\theta\\ & \quad +\frac{\alpha^e+\beta^e+\alpha^e\beta^e}{(\alpha+\beta+1)^{2^N+2}}(X+Y)^{2^N+1}\\ & \quad +\frac{(\alpha^{e-1}(1+\beta^e)X+\beta^{e-1}(1+\alpha^e)Y)}{(\alpha+\beta+1)^{2^N+1}}(X+Y)^{2^N}\\ & \quad +\frac{(\alpha+\beta)^2\theta+\alpha^e\beta^{-2^N}Y^{2^N+1}+\alpha^{e-1}\beta^{1-2^N}XY^{2^N}+\alpha^{-2^N}\beta^eX^{2^N+1}+\alpha^{1-2^N}\beta^{e-1}X^{2^N}Y}{\alpha^2+\beta^2+1}. \end{aligned}$$

Since

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

$$
\begin{aligned}
C_{2^N+1} &= \frac{\alpha^{-2^N}X^{2^N+1}+\beta^{-2^N}Y^{2^N+1}}{\alpha^2+\beta^2+1}+\frac{(\alpha^e+\beta^e+\alpha^e\beta^e)}{(\alpha+\beta+1)^{2^N+2}}(X+Y)^{2^N+1}\\
&\quad+\frac{(\alpha^{e-1}(1+\beta^e)X+\beta^{e-1}(1+\alpha^e)Y)}{(\alpha+\beta+1)^{2^N+1}}(X+Y)^{2^N}\\
&\quad+\frac{+\alpha\beta^{-2^N-2}Y^{2^N+1}+\beta^{-2^N-1}XY^{2^N}+\beta\alpha^{-2^N-2}X^{2^N+1}+\alpha^{-2^N-1}X^{2^N}Y}{\alpha^2+\beta^2+1}\\
&= B(2^N+1,0)X^{2^N+1}+B(2^N,1)X^{2^N}Y+B(1,2^N)XY^{2^N}+B(0,2^N+1)Y^{2^N+1},
\end{aligned}
$$

where

$$
\begin{aligned}
B(2^N+1,0) &= \frac{\alpha^{2^N-2}+(\alpha+\beta+1)^{2^N-2}}{\alpha^{2^N}\beta(\alpha+\beta+1)^{2^N}},\\
B(2^N,1) &= \frac{\alpha^{2^N-1}+(\alpha+1)(\alpha+\beta+1)^{2^N-2}}{\beta^2\alpha^{2^N}(\alpha+\beta+1)^{2^N}},\\
B(1,2^N) &= \frac{\beta^{2^N-1}+(\beta+1)(\alpha+\beta+1)^{2^N-2}}{\alpha^2\beta^{2^N}(\alpha+\beta+1)^{2^N}},\\
B(0,2^N+1) &= \frac{\beta^{2^N-2}+(\alpha+\beta+1)^{2^N-2}}{\alpha\beta^{2^N}(\alpha+\beta+1)^{2^N}}.
\end{aligned}
$$

□

***Remark 5.6*** Suppose $\alpha^{e+1}=\beta^{e+1}=(\alpha+\beta+1)^{e+1}=1$. Then $C_{2^N}=0$ if and only if $B(2^N,0)=B(0,2^N)=0$, that is

$$
\begin{cases}
\alpha^{2^N-1}+(\alpha+\beta+1)^{2^N-1}=0\\
\beta^{2^N-1}+(\alpha+\beta+1)^{2^N-1}=0.
\end{cases}
$$

It follows that $\alpha^{2^N-1}=\beta^{2^N-1}$. Also, multiply by $\alpha+\beta+1\neq 0$ one gets $\alpha^{2^N-1}=\beta^{2^N-1}=(\alpha+\beta+1)^{2^N-1}=1$.

When this happens, $B(2^N+1,0)=\frac{\beta+1}{\alpha^2(\alpha+\beta+1)^2}$ and $B(2^N+1,0)=\frac{\alpha+1}{\beta^2(\alpha+\beta+1)^2}$ which is never 0 unless $(\alpha,\beta)=(1,1)$. In this case $B(2^N,1)=B(1,2^N)=1$ and therefore $C_{2^N+1}$ never vanishes.

We are interested in singular points for which $C_{2^N+1}$ and $C_{2^N}$ share a factor. The following lemma will be crucial to this aim.

**Lemma 5.7** *Let $\alpha^{e+1}=\beta^{e+1}=(\alpha+\beta+1)^{e+1}=1$. Let $C_{2^N+1}$ and $C_{2^N}$ be as in Proposition 5.5 and suppose that $(B(2^N,0),B(0,2^N))\neq(0,0)$. If they share a factor then such a factor is not repeated.*

***Proof*** By Proposition 5.5,

$$
\begin{aligned}
C_{2^N} &= \left(\sqrt[2^N]{B(2^N,0)}X+\sqrt[2^N]{B(0,2^N)}Y\right)^{2^N},\\
C_{2^N+1} &= B(2^N+1,0)X^{2^N+1}+B(1,2^N)XY^{2^N}+B(2^N,1)X^{2^N}Y+B(0,2^N+1)Y^{2^N+1}.
\end{aligned}
$$

If $B(2^N,0)=0$, then the only possibility is $B(2^N+1,0)=B(2^N,1)=0$ and thus $\alpha^{2^N-1}+(\alpha+1)\alpha^{2^N-2}=\alpha^{2^N-2}=0$, a contradiction to $\alpha \neq 0$. Analogously, a contradiction arises if $B(0,2^N)=0$.

Now we assume $B(2^N,0)B(0,2^N)\neq 0$. We have that $\sqrt[2^N]{B(2^N,0)}X+\sqrt[2^N]{B(0,2^N)}Y$ is a repeated factor of $C_{2^N+1}$ if and only there exists a non-trivial solution of

$$\begin{cases} \sqrt[2^N]{B(2^N,0)}X+\sqrt[2^N]{B(0,2^N)}Y=0\\ B(2^N+1,0)X^{2^N+1}+B(1,2^N)XY^{2^N}+B(2^N,1)X^{2^N}Y+B(0,2^N+1)Y^{2^N+1}=0\\ B(2^N+1,0)X^{2^N}+B(1,2^N)Y^{2^N}=0. \end{cases}$$

This is equivalent to

$$\begin{cases} B(2^N,0)X^{2^N}+B(0,2^N)Y^{2^N}=0\\ B(2^N,1)X^{2^N}+B(0,2^N+1)Y^{2^N}=0\\ B(2^N+1,0)X^{2^N}+B(1,2^N)Y^{2^N}=0, \end{cases}$$

and thus

$$\begin{cases} B(2^N+1,0)B(0,2^N+1)+B(2^N,1)B(1,2^N)=0\\ B(2^N+1,0)B(0,2^N)+B(2^N,0)B(1,2^N)=0\\ B(2^N,1)B(0,2^N)+B(2^N,0)B(0,2^N+1)=0. \end{cases}$$

From the first equation we obtain

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

and thus

$$(\alpha+\beta+1)^{2^N-2}\Big(\alpha^{2^N-1}+\beta^{2^N-1}+(\alpha+\beta+1)^{2^N-1}\Big)=0. \tag{19}$$

The second equation yields

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

and therefore

$$(\alpha+\beta+1)^{2^N-2}(\alpha^{2^N}+\beta^{2^N}+\beta^{2^N-1}+(\alpha+\beta+1)^{2^N})=0. \tag{20}$$

Analogously, from the third equation we get

$$(\alpha+\beta+1)^{2^N-2}(\alpha^{2^N}+\beta^{2^N}+\alpha^{2^N-1}+(\alpha+\beta+1)^{2^N})=0. \tag{21}$$

Since $\alpha+\beta+1\neq 0$, from Equations (20) and (21) $\alpha^{2^N-1}=\beta^{2^N-1}$. Finally, (19) yields $(\alpha+\beta+1)^{2^N-1}=0$, a contradiction. □

We are in position now to provide the desired upper bounds on $I_{P,max}(\mathcal{A}_e)$, where $P=(\alpha,\beta)$, $\alpha^{e+1}=\beta^{e+1}=(\alpha+\beta+1)^{e+1}=1$.

**Proposition 5.8** *Let $e$ odd, $e \equiv 2^N - 1 \pmod{2^{N+1}}$, and $f_e = (X^e + Y^e + X^eY^e)(X + Y + 1)^e + X^eY^e$. Let $P = (\alpha, \beta)$, $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$, be such that $f_e(\alpha, \beta) = 0$. Then,*

1. *$I_{P,max}(f_e = 0) \leq \frac{(2^N+1)^2}{4}$ if $\alpha^{2^N-1} = \beta^{2^N-1} = (\alpha + \beta + 1)^{2^N-1} = 1$;*
2. *$I_{P,max}(f_e = 0) \leq 2^N$ otherwise.*

***Proof*** If $\alpha^{2^N-1} = \beta^{2^N-1} = (\alpha + \beta + 1)^{2^N-1} = 1$, then $C_{2^N} = 0$ and

$$C_{2^N+1} = \frac{1}{\alpha\beta(\alpha + \beta + 1)^2} \left( \frac{\beta + 1}{\alpha} X^{2^N+1} + X^{2^N} Y + XY^{2^N} + \frac{\alpha + 1}{\beta} Y^{2^N+1} \right) \not\equiv 0$$

is separable by direct checking and thus $I_{P,max}(f_e = 0) \leq \frac{(2^N+1)^2}{4}$ by Lemma 2.1. In the other cases, $C_{2^N} \neq 0$ and $GCD(C_{2^N}, C_{2^N+1}) = 1$ or $\sqrt[2^N]{B(2^N, 0)}X + \sqrt[2^N]{B(0, 2^N)}Y$ by Proposition 5.7 and, by Lemma 2.2, $I_{P,max}(f_e = 0) \leq 2^N$.

□

The following is the main result of this section.

**Theorem 5.9** *If $e > 1$ is odd, then $h_e$ has an absolutely irreducible factor over $\mathbb{F}_2$.*

***Proof*** Let $\mathcal{A}_e : h_e = 0$. We want to prove that $\sum\limits_{P \in Sing(\mathcal{A}_e)} I_{P,max}(\mathcal{A}_e) < \frac{2}{9} deg^2(h_e) = 2(e - 1)^2$; the statement will then follow by Criterion 2.3.

Recall that any upper bound on $I_{P,max}(f_e = 0)$ is also an upper bound for $I_{P,max}(h_e = 0)$, since the curve $h_e = 0$ is a component of the curve $f_e = 0$.

Let $e \equiv 2^N - 1 \pmod{2^{N+1}}$, $e + 1 = 2^N m$, $m$ odd. Points $P = (\alpha, \beta)$ with $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$ are at most $m^2$ while the number of singular points $P = (\alpha, \beta)$ of $\mathcal{A}_e$ with $\alpha^{2^N-1} = \beta^{2^N-1} = (\alpha+\beta+1)^{2^N-1} = 1$ is at most $d^2$, where $d := GCD(2^N - 1, m)$. Let

$$\begin{aligned}
\Omega &:= \{(0, 0), (1, 0), (0, 1), [1 : 0 : 0], [0 : 1 : 0], [1 : 1 : 0]\},\\
\Theta &:= \{(\alpha, \beta) : \alpha^{e+1} = \beta^{e+1} = (\alpha + \beta + 1)^{e+1} = 1\},\\
\Sigma &:= \{(\alpha, \beta) \in \Theta : \alpha^{2^N-1} = \beta^{2^N-1} = (\alpha + \beta + 1)^{2^N-1} = 1\}.
\end{aligned}$$

We have that $\#\Omega = 6$, $\#\Theta \leq m^2 = \frac{(e+1)^2}{2^{2N}}$, $\#\Sigma \leq d^2$, and by Proposition 5.3, Proposition 5.8.

$$I_{P,\max}(\mathcal{A}_e) \leq \begin{cases} \frac{(e-1)^2}{4} & P \in \Omega;\\ 2^N & P \in \Theta \setminus \Sigma;\\ \frac{(2^N+1)^2}{4} & P \in \Sigma. \end{cases}$$

Thus

$$\sum_{P \in Sing(\mathcal{A}_e)} I_{P,max}(\mathcal{A}_e) \leq \frac{6}{4}(e - 1)^2 + \frac{(e + 1)^2}{2^N} + d^2 \left( \frac{(2^N + 1)^2}{4} - 2^N \right).$$

Noting that $d^2(\frac{(2^N+1)^2}{4} - 2^N) \leq m^2(\frac{(2^N+1)^2}{4} - 2^N) = \frac{1}{4}(e + 1 + \frac{e+1}{2^N})^2 - \frac{(e+1)^2}{2^N} = \frac{(2^N+1)^2}{2^{2N+2}}(e + 1)^2 - \frac{(e+1)^2}{2^N}$, we get

$$\sum_{P \in Sing(\mathcal{A}_e)} I_{P,max}(\mathcal{A}_e) \leq \frac{3}{2}(e - 1)^2 + \frac{(2^N + 1)^2}{2^{2N+2}}(e + 1)^2.$$

Therefore

$$\frac{3}{2}(e-1)^2+\frac{(2^N+1)^2}{2^{2N+2}}(e+1)^2<2(e-1)^2$$

is equivalent to

$$\frac{(e+1)^2}{(e-1)^2}<\frac{2^{2N+1}}{(2^N+1)^2}, \tag{22}$$

i.e

$$\frac{e+1}{e-1}<\sqrt{2}\cdot\frac{2^N}{2^N+1}. \tag{23}$$

Inequality (23) is satisfied for any pair $(N, e)$ with $N \geq 2$ and $e \geq 17$ or $(N, e) = (4, 15)$ (recall that $e+1 = 2^N m$, $m$ odd).

Now consider the remaining cases, i.e. $N = 1$, or $e = 3, 7, 11$.

- $N = 1$ (i.e. $e \equiv_4 1$). Let $P = (\alpha, \beta)$ with $\alpha^{e+1} = \beta^{e+1} = (\alpha+\beta+1)^{e+1} = 1$; we want to prove that $I_{P,max}(\mathcal{A}_e) = 0$.
  - If $P = (1, 1)$, by Remark 5.6 we have that $m_P(f_e) = 3$, $P \notin \mathcal{A}_e$, and thus $I_{P,max}(\mathcal{A}_e) = 0$.
  - If $P \neq (1, 1)$ belongs to the curve defined by $(X+Y)(X+1)(Y+1) = 0$, by Remark 5.6 and Proposition 5.8 it follows that $m_P(h_e) = 1$, i.e. $P$ is a regular point of $h_e$ and thus $I_{P,max}(\mathcal{A}_e) = 0$.
  - If $\alpha \neq 1 \neq \beta$ and $\alpha \neq \beta$, from Proposition 5.5 we obtain

    $$C_2 = \frac{\beta+1}{\alpha^2\beta(\alpha+\beta+1)^2}X^2+\frac{\alpha+1}{\alpha\beta^2(\alpha+\beta+1)^2}Y^2,$$
    $$C_3 = \frac{XY(X+Y)}{\alpha^2\beta^2(\alpha+\beta+1)^2}.$$

    Since $B(2, 0) \neq B(0, 2)$, $GCD(C_2, C_3) = 1$ and by Lemma 2.2 $I_{P,max}(\mathcal{A}_e) = 0$.

  we conclude that

  $$\sum_{P\in Sing(\mathcal{A}_e)} I_{P,max}(\mathcal{A}_e) \leq \frac{6}{4}(e-1)^2 < 2(e-1)^2 = \frac{2}{9}deg(h_e)^2,$$

  and therefore the claim follows.
- $e = 3, 7$. In this case $e+1$ is a power of 2, so there are no $(e+1)$-roots of unity different from 1. From Remark 5.6 and Proposition 5.8 we deduce $m_{(1,1)}(h_3) = m_{(1,1)}(f_3) - 3$ equals 2 (resp. $m_{(1,1)}(h_7) = 6$) and since the tangent cone is separable $I_{P,max}(h_3) \leq 1$ (resp. $I_{P,max}(h_7) \leq 9$). Summing up

  $$\sum_{P\in Sing(\mathcal{A}_3)} I_{P,max}(\mathcal{A}_3) \leq \frac{6}{4}(e-1)^2+1 = 7 < 8 = 2(e-1)^2,$$
  $$\sum_{P\in Sing(\mathcal{A}_7)} I_{P,max}(\mathcal{A}_7) \leq \frac{6}{4}(e-1)^2+9 = 63 < 72 = 2(e-1)^2,$$

  and the claim follows.

- $e = 11$. In this case $N = 2$ and $m = 3$. Thus

$$\Theta = \Sigma = \{(1, 1), (1, \omega), (1, \omega^2), (\omega, \omega), (\omega^2, \omega^2), (\omega, 1), (\omega^2, 1)\}.$$

Also, $I_{(1,1),max}(h_3) \leq 1$ and $I_{P,max}(h_3) \leq 6$ for any $P \in \Sigma \setminus \{(1, 1)\}$. Thus

$$\sum_{P \in Sing(\mathcal{A}_{11})} I_{P,max}(\mathcal{A}_{11}) \leq \frac{6}{4}(e-1)^2 + 1 + 36 = 187 < 200 = 2(e-1)^2,$$

and the claim follows.

□

We summarize the results of this section in the following theorem (see also point 3. in Main Theorem.)

**Theorem 5.10** *Let $\psi = \frac{f}{g} \in \mathbb{F}_q(X)$. If $d - m > 1$ is odd then $\psi$ is not an exceptional APN function.*

**Acknowledgements** This research was supported by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INdAM).

**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, finite fields theory and applications. Contemp. Math. **518**, 23–31 (2010).
2. Bartoli D., Zhou Y.: Exceptional scattered polynomials. J. Algebra **509**, 507–534 (2018).
3. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems, finite fields: theory and applications. Contemp. Math. **4**, 3–72 (1991).
4. Browning K.A., Dillon J., Kibler R., McQuistan M.T.: APN polynomials and related codes. J. Combin. Inf. Syst. Sci. **34**(1–4), 135–159 (2009).
5. Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Tran. Inf. Theory **52**, 1141–1152 (2006).
6. Budaghyan L., Carlet C.: Classes of quadratic APN trinomials and hexanomials and related structures. IEEE Tran. Inf. Theory **54**(5), 2354–2357 (2008).
7. Budaghyan L., Calderini M., Carlet C., Coulter R.S., Villa I.: Constructing APN functions through isotopic shifts. IEEE Tran. Inf. Theory **66**(8), 5299–5309 (2020).
8. Budaghyan L., Calderini M., Villa I.: On equivalence between known families of quadratic APN functions. Finite Fields Appl. **66**, 101704 (2020).
9. Budaghyan L., Calderini M., Carlet C., Coulter R., Villa I.: Generalized isotopic shift construction for APN functions. Des. Codes Cryptogr. **89**(1), 19–32 (2021).
10. 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).
11. Carlet C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021).

12. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998).
13. Coulter R.S., Henderson M.: A class of functions and their application in constructing semi-biplanes and association schemes. Discret. Math. **202**(1–3), 21–31 (1999).
14. Delgado M.: The state of the art on the conjecture of exceptional APN functions. Note Mat. **37**(1), 41–51 (2017).
15. Dembowski P., Ostrom T.G.: Planes of order $n$ with collineation groups of order $n^2$. Math. Z. **103**(3), 239–258 (1968).
16. Dempwolff U., Edel Y.: Dimensional dual hyperovals and APN functions with translation groups. J. Algebraic Combin. **39**(2), 457–496 (2014).
17. Fine N.J.: Binomial coefficients modulo a prime. Am. Math. Mon. **54**, 589–592 (1947).
18. Fulton W.: Algebraic Curves. Advanced Book Classics. Addison-Wesley Publishing Company Advanced Book Program, Redwood City (1989).
19. Ghorpade S., Lachaud G.: Etale cohomology, Lefschetz theorem and number of points of singular varieties over finite fields. Mosc. Math. J. **2**, 589–631 (2002).
20. Hartshorne, R.: Algebraic Geometry. Graduate Texts in Mathematics. Springer, New York. (1977)
21. Hernando F., McGuire G.: Proof of a conjecture on the sequence of exceptional numbers classifying cyclic codes and APN functions. J. Algebra **343**, 78–92 (2011).
22. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic Curves over a Finite Field. Princeton Series in Applied Mathematics, Princeton (2008)
23. Janwa H., McGuire G., Wilson R.: Double-error correcting cyclic codes and absolutely irreducible polynomials over $GF(2)$. J. Algebra **178**, 665–676 (1995).
24. Jedlicka D.: APN monomials over $GF(2^n)$ for infinitely many $n$. Finite Fields Appl. **13**, 1006–1028 (2007).
25. Lang S., Weil A.: Number of points of varieties in finite fields. Am. J. Math. **76**, 819–827 (1954).
26. Mullen G.L., Panario D.: Handbook of Finite Fields. Chapman and Hall/CRC, Boca Raton (2013).
27. Nyberg K.: Differentially uniform mappings for cryptography. In: Advances in Cryptography, EUROCRYPT'93. Lecture Notes in Computer Science, vol. 765, pp. 55–64. Springer, New York (1994).
28. Pott A.: Almost perfect and planar functions. Des. Codes Cryptogr. **78**(1), 141–195 (2016).
29. Rodier F.: Bornes sur le degré des polynômes presque parfaitement non-linéaires. Contemp. Math. **487**, 169–181 (2009).
30. Schmidt K.-U., Zhou Y.: Planar functions over fields of characteristic two. J. Algebraic Combin. **40**, 503–526 (2014).
31. Taniguchi H.: On some quadratic APN functions. Des. Codes Cryptogr. **87**(9), 1973–1983 (2019).

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