Cryptography and Communications
https://doi.org/10.1007/s12095-026-00880-4

RESEARCH

Non-existence of infinite APN families from patched monomials in odd characteristic

Daniele Bartoli[1] · **Pantelimon Stănică**[2]

Received: 4 October 2025 / Accepted: 6 March 2026

Abstract
In this paper we disprove a conjecture by Budaghyan and Pal (DCC, 2024) on the existence of an infinite family of APN permutations of the form $F(x) = x^{(q+3)/2} + ux^2$ over $\mathbb{F}_q$. Using function field theory and Hasse-Weil bounds, we prove that for $q \geq 2719$ and $u \notin \{0, \pm 1\}$, the function F is not APN. Combined with computational verification for $125 < q < 2719$, this establishes that no such infinite family exists beyond the finitely many known small-field examples. Moreover, we extend this negative result to related families including $F(x) = x^{(p^n-1)/2+3} + ux^3$ (for $q \equiv 1 \pmod 3$) and $F(x) = x^{(p^n-1)/2+p^k+1} + ux^{p^k+1}$, showing these "patched monomial" constructions $(\eta(x) + u)x^d$ systematically fail to produce infinite APN families as field size grows. Our methods combine algebraic geometry (Kummer extensions, genus calculations), character sum analysis, and computational techniques. We also investigate the permutation properties and value distributions of these functions, proving general non-permutation criteria and establishing differential uniformity bounds. This work demonstrates that while these constructions yield APN functions for small finite fields, they are fundamentally unsuitable for generating infinite APN families.

Keywords Finite fields · Permutation polynomials · Varieties · Irreducible components

Mathematics Subject Classification (2010) 11G20 · 11T06 · 12E20 · 14Q10

✉ Pantelimon Stănică
pstanica@nps.edu

Daniele Bartoli
daniele.bartoli@unipg.it

[1] Department of Mathematics and Computer Science, University of Perugia, Perugia 06123, Italy

[2] Applied Mathematics Department, Naval Postgraduate School, Monterey, CA 93943, USA

Published online: 31 March 2026

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^k$ elements, where k is a positive integer. We denote by $\mathbb{F}_q^*$ the multiplicative group of nonzero elements of $\mathbb{F}_q$ and by $\mathbb{F}_q[X]$ the polynomial ring in the indeterminate X over a finite field $\mathbb{F}_q$. A polynomial $f \in \mathbb{F}_q[X]$ is called a permutation polynomial if the equation $f(X) = a$ has exactly one solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$. Below, we let $\chi_1(a) = \exp\left(\frac{2\pi i \mathrm{Tr}_1^n(a)}{q}\right)$ be the principal additive character of $\mathbb{F}_q$, $q = p^n$.

Given a vectorial p-ary function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$, the derivative of f with respect to $a \in \mathbb{F}_{p^n}$ is the p-ary function $D_a f(x) = f(x + a) - f(x), \text{ for all } x \in \mathbb{F}_{p^n}$. For an (n, m)-function F, and $a \in \mathbb{F}_{p^n}, b \in \mathbb{F}_{p^m}$, we let $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x + a) - F(x) = b\}$. We call the quantity $\delta_F = \max\{\Delta_F(a, b) : a, b \in \mathbb{F}_{p^n}, a \neq 0\}$ the *differential uniformity* of F. If $\delta_F \leq \delta$, then we say that F is differentially δ-uniform. If $m = n$ and $\delta = 1$, then F is called a *perfect nonlinear* (*PN*) function, or *planar* function. If $m = n$ and $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function. It is well known that PN functions do not exist if $p = 2$.

We will denote by $\eta(\alpha)$ the quadratic character of α (that is, $\eta(\alpha) = 0$ if $\alpha = 0$, $\eta(\alpha) = 1$ if $0 \neq \alpha$ is a square, $\eta(\alpha) = -1$ if α is not a square).

2 Preliminaries from function field theory

In this paper we will make use of some concepts concerning Function Field Theory. This will yield a lower bound on the number of APN functions of the desired shape.

We recall that a *function field* over a perfect field $\mathbb{L}$ is an extension $\mathbb{F}$ of $\mathbb{L}$ such that $\mathbb{F}$ is a finite algebraic extension of $\mathbb{L}(\alpha)$, with α transcendental over $\mathbb{L}$. For basic definitions on function fields we refer to [15]. In particular, the (full) constant field of $\mathbb{F}$ is the set of elements of $\mathbb{F}$ that are algebraic over $\mathbb{L}$.

If $\mathbb{F}'$ is a finite extension of $\mathbb{F}$, then a place P' of $\mathbb{F}'$ is said to be *lying over* a place P of $\mathbb{F}$ if $P \subset P'$. This holds precisely when $P = P' \cap \mathbb{F}$. In this paper, $e(P'|P)$ will denote the ramification index of P' over P. A finite extension $\mathbb{F}'$ of a function field $\mathbb{F}$ is said to be *unramified* if $e(P'|P) = 1$ for every P' place of $\mathbb{F}'$ and every P place of $\mathbb{F}$ with P' lying over P. Since it is not needed here, we do not go into the tamely or totally ramification extensions' notions. Throughout the paper, we will refer to the following results.

Theorem 2.1 *[15, Cor. 3.7.4] Consider an algebraic function field $\mathbb{F}$ with constant field $\mathbb{L}$ containing a primitive n-th root of unity ($n > 1$ and n relatively prime to the characteristic of $\mathbb{L}$). Let $u \in \mathbb{F}$ be such that there is a place Q of $\mathbb{F}$ with $\gcd(v_Q(u), n) = 1$ (see [15, Definition 1.1.2] for the definition of the discrete valuation function v_Q). Let $\mathbb{F}' = \mathbb{F}(y)$ with $y^n = u$. Then:*

(1) *$\Phi(T) = T^n - u$ is the minimal polynomial of y over $\mathbb{F}$. The extension $\mathbb{F}' : \mathbb{F}$ is Galois of degree n and the Galois group of $\mathbb{F}' : \mathbb{F}$ is cyclic;*
(2) *We have*

$$e(P'|P) = \frac{n}{r_P} \quad \text{where} \quad r_P := GCD(n, v_P(u)) > 0\,;$$

(3) $\mathbb{L}$ *is the constant field of* $\mathbb{F}'$*;*
(4) *If* g' *(resp., g) is the genus of* $\mathbb{F}'$ *(resp.* $\mathbb{F}$*), then*

$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P\in\mathbb{P}(\mathbb{F})}(n - r_P)\deg P\,.$$

An extension such as $\mathbb{F}'$ in Theorem 2.1 is said to be a Kummer extension of $\mathbb{F}$.

Denote by $\mathbb{F}_q$ the finite field with q elements and let $\mathbb{K}$ be the algebraic closure of $\mathbb{F}_q$. A curve $\mathcal{C}$ in some affine or projective space over $\mathbb{K}$ is said to be defined over $\mathbb{F}_q$ if the ideal of $\mathcal{C}$ is generated by polynomials with coefficients in $\mathbb{F}_q$. Let $\mathbb{K}(\mathcal{C})$ denote the function field of $\mathcal{C}$. The subfield $\mathbb{F}_q(\mathcal{C})$ of $\mathbb{K}(\mathcal{C})$ consists of the rational functions on $\mathcal{C}$ defined over $\mathbb{F}_q$. The extension $\mathbb{K}(\mathcal{C}) : \mathbb{F}_q(\mathcal{C})$ is a constant field extension (see [15, Section 3.6]). In particular, $\mathbb{F}_q$ -rational places of $\mathbb{F}_q(\mathcal{C})$ can be viewed as the restrictions to $\mathbb{F}_q(\mathcal{C})$ of places of $\mathbb{K}(\mathcal{C})$ that are fixed by the Frobenius map on $\mathbb{K}(\mathcal{C})$. The center of an $\mathbb{F}_q$-rational place is an $\mathbb{F}_q$-rational point of $\mathcal{C}$; conversely, if P is a simple $\mathbb{F}_q$-rational point of $\mathcal{C}$, then the only place centered at P is $\mathbb{F}_q$-rational. Through the paper, we sometimes use concepts from both Function Field Theory and Algebraic Curves. Concepts such as the valuation of a function at a place can be also seen as multiplicity of intersections of fixed algebraic curves; see [15].

We now recall the well-known Hasse-Weil bound.

Theorem 2.2 *(Hasse-Weil bound, [15, Theorem 5.2.3]) The number* N_q *of* $\mathbb{F}_q$*-rational places of a function field* $\mathbb{F}$ *with constant field* $\mathbb{F}_q$ *and genus g satisfies*

$$|N_q - (q+1)| \le 2g\sqrt{q}.$$

In order to apply the Hasse-Weil bound, the following lemma will be useful.

Lemma 2.3 *[2, Lemma 1] Let* $\mathbb{F}_q(\beta_1,\ldots,\beta_n)$ *be a function field with constant field* $\mathbb{F}_q$*. Suppose that* $f \in \mathbb{F}_q(\beta_1,\ldots,\beta_n)[T]$ *is a polynomial which is irreducible over* $\mathbb{K}(\beta_1,\ldots,\beta_n)[T]$*. Then, for a root z of f, the field* $\mathbb{F}_q$ *is the constant field of* $\mathbb{F}_q(\beta_1,\ldots,\beta_n)(z)$*.*

3 A "potential" infinite class of APN functions

First, we prove the following result, which finds some low differential uniformity functions in odd characteristic. In our follow up result, we complete the proof for all the other cases and show that the conjecture of [4] is false. This result was independently obtained by Mesnager and Wu [11], reinforcing that the APN property of this function is a small finite field phenomenon.

Theorem 3.1 *Let* $F(x) = x^{\frac{p^n+3}{2}} + u\,x^2$ *on* $\mathbb{F}_{p^n}$*, where* $u \in \mathbb{F}_{p^n}$ *satisfies* $u \notin \{0, \pm 1\}$*. If* $u = -3$ *and* $p^n \equiv 5 \pmod 8$*, then the differential uniformity of F on* $\mathbb{F}_{p^n}$ *is* ≤ 4*.*

Proof For given $a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}$ we need to look at the differential equation $F(x+a) - F(x) = b$, that is,

$$(x+a)^{\frac{p^n+3}{2}} + u(x+a)^2 - x^{\frac{p^n+3}{2}} - ux^2 = b.$$

Denoting $t_{x+a} = \eta(x+a), t_x = \eta(x)$, and noting that $\frac{p^n+3}{2} = \frac{p^n-1}{2} + 2$, the equation above becomes

$$(x+a)^2(t_{x+a}+u) - x^2(t_x+u) = b. \tag{3.1}$$

We now distinguish four cases, which are displayed in (3.2), below.

Case	t_{x+a}	t_x	Equation (3.1)	x	$x+a$
$C_{1,1}$	1	1	$a^2(u+1)+2a(u+1)x = b$	$\frac{b-(u+1)a^2}{2a(u+1)}$	$\frac{b+(u+1)a^2}{2a(u+1)}$
$C_{-1,-1}$	−1	−1	$a^2(u-1)+2a(u-1)x = b$	$\frac{b-(u-1)a^2}{2a(u-1)}$	$\frac{b+(u-1)a^2}{2a(u-1)}$
$C_{-1,1}$	−1	1	$(u-1)a^2+2a(u-1)x-2x^2 = b$	$\frac{a(u-1)\pm\sqrt{a^2(u^2-1)-2b}}{2}$	$\frac{\left(a(u+1)\pm\sqrt{a^2(u^2-1)-2b}\right)}{2}$
$C_{1,-1}$	1	−1	$(u+1)a^2+2a(u+1)x+2x^2 = b$	$\frac{-a(u+1)\pm\sqrt{a^2(u^2-1)+2b}}{2}$	$\frac{-a(u-1)\pm\sqrt{a^2(u^2-1)+2b}}{2}$

(3.2)

For easy referral, we label the potential solutions as x_1 (Case $C_{1,1}$), x_2 (Case $C_{-1,-1}$), x_3, x_4 (Case $C_{1,-1}$), x_5, x_6 (Case $C_{-1,1}$).

In Case $C_{1,1}$ we must have $\eta\left(\frac{b}{2a(u+1)} - \frac{a}{2}\right) = \eta\left(\frac{b}{2a(u+1)} + \frac{a}{2}\right) = 1$, or equivalently,

$$\eta\left(\frac{b}{a^2(u+1)} - 1\right) = \eta\left(\frac{b}{a^2(u+1)} + 1\right) = \eta(2a). \tag{3.3}$$

For Case $C_{-1,-1}$ we need $\eta\left(\frac{b}{2a(u-1)} - \frac{a}{2}\right) = \eta\left(\frac{b}{2a(u-1)} + \frac{a}{2}\right) = -1$, or equivalently,

$$\eta\left(\frac{b}{a^2(u-1)} - 1\right) = \eta\left(\frac{b}{a^2(u-1)} + 1\right) = -\eta(2a). \tag{3.4}$$

In Case $C_{-1,1}$, for at least a solution to exist, one needs the expression inside the root to be a square, and further $\eta(x_3x_4) = \eta((x_3+a)(x_4+a)) = 1$, so, $\eta\left(-2b + a^2\left(u^2-1\right)\right) = \eta\left(b-(u-1)a^2\right) = \eta\left(b+(u+1)a^2\right) = 1$, or equivalently,

$$\begin{aligned} \eta\left(\tfrac{-2b}{a^2(u^2-1)} + 1\right) &= \eta(u^2-1), \\ \eta\left(\tfrac{b}{(u-1)a^2} - 1\right) &= \eta(u-1), \\ \eta\left(\tfrac{b}{(u+1)a^2} + 1\right) &= \eta(u+1). \end{aligned} \tag{3.5}$$

Similarly, in Case $C_{1,-1}$, we must have $\eta\left(2b + a^2\left(u^2-1\right)\right) = \eta\left(-b-(u-1)a^2\right) = \eta\left(-b+(u+1)a^2\right) = 1$, or equivalently,

$$\begin{aligned} \eta\left(\tfrac{2b}{a^2(u^2-1)} + 1\right) &= \eta(u^2-1), \\ \eta\left(\tfrac{-b}{(u-1)a^2} - 1\right) &= \eta(u-1), \\ \eta\left(\tfrac{-b}{(u+1)a^2} + 1\right) &= \eta(u+1). \end{aligned} \tag{3.6}$$

We first take $p \equiv 5 \pmod 8$ and n odd (similarly, for the other cases). By Gauss' Reciprocity Law, we know that in these fields, 2 is a non-square (recall that 2 is a square in the field $\mathbb{F}_{p^n}$, p odd if and only if either $p \equiv \pm 1 \pmod 8$ or n is even) and -1 is a square (since $p^n \equiv 1 \pmod 4$ under our conditions). We shall be using that in the first part of our proof.

When $u = -3$, Case $C_{1,1}$ reduces to

$$\eta(b + 2a^2) = \eta(b - 2a^2) = \eta(a),$$

Case $C_{-1,-1}$ reduces to

$$\eta(b + 4a^2) = \eta(b - 4a^2) = \eta(a),$$

Case $C_{-1,1}$ implies

$$\eta(b - 2a^2) = 1 \text{ and } [\eta(b + 4a^2) = 1 \text{ or } \eta(b - 2a^2) = 1]$$

(it is inclusive or, since we might have one or two solutions satisfying the conditions, here and in the next case) and finally, Case $C_{1,-1}$ implies

$$\eta(b - 4a^2) = -1 \text{ and } [\eta(b - 4a^2) = 1 \text{ or } \eta(b + 2a^2) = 1].$$

We note that each case might contribute at most one solution. Summarizing,

$$\begin{aligned} C_{1,1} &: \eta(b + 2a^2) = \eta(b - 2a^2) = \eta(a) \\ C_{-1,-1} &: \eta(b + 4a^2) = \eta(b - 4a^2) = -\eta(a) \\ C_{-1,1} &: \eta(b - 2a^2) = -\eta(b + 4a^2) = 1 \\ C_{1,-1} &: \eta(b + 2a^2) = -\eta(b - 4a^2) = 1. \end{aligned}$$

Thus, the number of solutions is at most four, which is attained for some values of q, as one can quickly check for some primes (for example, $p = 461, n = 1$). Later, we shall show that, in fact, for $q > 125$, only the values 3, 4 are obtained. □

We now continue with the following observation. Combining the cases $C_{1,1}$ and $C_{1,-1}$, we are seeking to show that

$$(x + a)^{\frac{p^n+3}{2}} + u(x + a)^2 - x^{\frac{p^n+3}{2}} - ux^2 = b$$

has at least three solutions and thus the function F is not APN.

Consider a fixed $u \in \mathbb{F}_q \setminus \{0, \pm 1\}$ and let $\xi \in \mathbb{F}_q$ be a fixed non-square.

The case $C_{1,1}$ provides a solution if and only if there exist $a, b, X, Y \in \mathbb{F}_q$, $a \neq 0$, such that

$$\begin{cases} \frac{b}{2a(u+1)} - \frac{a}{2} = X^2 \\ \frac{b}{2a(u+1)} + \frac{a}{2} = Y^2. \end{cases}$$

On the other hand, the case $C_{-1,1}$ provides two solutions when there exist $a, b, Z, U, V, W, T \in \mathbb{F}_q$, $aZ \neq 0$, such that

$$\begin{cases} a^2(u^2-1) - 2b = Z^2 \\ a(u-1) + Z = 2U^2 \\ a(u-1) - Z = 2V^2 \\ a(u+1) + Z = 2\xi W^2 \\ a(u+1) - Z = 2\xi T^2. \end{cases}$$

Putting all together, we can observe that F is not APN if, for a fixed $u \in \mathbb{F}_q \setminus \{0, \pm 1\}$, there exist $a, b, X, Y, Z, U, V, W, T \in \mathbb{F}_q$, $aZ \neq 0$, satisfying the system

$$\begin{cases} \frac{b}{2a(u+1)} - \frac{a}{2} = X^2 \\ \frac{b}{2a(u+1)} + \frac{a}{2} = Y^2 \\ a^2(u^2-1) - 2b = Z^2 \\ a(u-1) + Z = 2U^2 \\ a(u-1) - Z = 2V^2 \\ a(u+1) + Z = 2\xi W^2 \\ a(u+1) - Z = 2\xi T^2 \end{cases}$$

and such that the three roots

$$\frac{b - (u+1)a^2}{2a(u+1)}, \quad \frac{a(u-1) \pm \sqrt{a^2(u^2-1) - 2b}}{2}$$

are all distinct. This is implied by $b + a^2(u+1) \neq 0$.

Note that the above system is equivalent to

$$\begin{cases} b = a(u+1)(2X^2 + a) \\ Y^2 = a + X^2 \\ Z^2 = a(u+1)((u-3)a - 4X^2) \\ U^2 = \frac{u-1}{2}a + \frac{Z}{2} \\ V^2 = \frac{u-1}{2}a - \frac{Z}{2} \\ W^2 = \frac{a(u+1)}{2\xi} + \frac{Z}{2\xi} \\ T^2 = \frac{a(u+1)}{2\xi} - \frac{Z}{2\xi}. \end{cases} \tag{3.7}$$

Our aim is to prove the existence of suitable solutions of the above system. To this end we will use an approach based on function fields over finite fields.

Let a be such that $a(u+1)$ is a square in $\mathbb{F}_q$. The solutions of the following system

$$\begin{cases} b = a(u+1)(2X^2+a) \\ Z^2 = a(u+1)((u-3)a - 4X^2) \\ U^2 = \dfrac{u-1}{2}a + \frac{Z}{2} \\ V^2 = \dfrac{u-1}{2}a - \frac{Z}{2} \\ W^2 = \dfrac{a(u+1)}{2\xi} + \frac{Z}{2\xi} \\ T^2 = \dfrac{a(u+1)}{2\xi} - \frac{Z}{2\xi} \\ Y = \dfrac{\xi}{\sqrt{a(u+1)}}TW \end{cases} \tag{3.8}$$

are also solutions of System (3.7).

We are now ready to put these together as a first step in the completion of our disproof of the conjecture.

Theorem 3.2 *Let q be an odd prime power, $u \in \mathbb{F}_q \setminus \{0, \pm 1, 3\}$, $a \in \mathbb{F}_q^*$ such that $a(u+1)$ is a square in $\mathbb{F}_q$, ξ a fixed nonsquare in $\mathbb{F}_q$, that is, $\eta(a(u+1)) = 1, \eta(\xi) = -1$. The function field $\mathbb{K}(X, Y, Z, W, T)$ defined by*

$$\begin{cases} Z^2 = a(u+1)((u-3)a - 4X^2) \\ W^2 = \dfrac{a(u+1)}{2\xi} + \frac{Z}{2\xi} \\ T^2 = \dfrac{a(u+1)}{2\xi} - \frac{Z}{2\xi} \\ Y = \dfrac{\xi}{\sqrt{a(u+1)}}TW \\ U^2 = \dfrac{u-1}{2}a + \frac{Z}{2} \\ V^2 = \dfrac{u-1}{2}a - \frac{Z}{2} \end{cases} \tag{3.9}$$

has $\mathbb{F}_q$ as a field of constants.

Proof We rewrite the system above as

$$\begin{cases} Z = 2\xi W^2 - a(u+1) \\ X^2 = -\dfrac{\xi^2}{a(u+1)}W^4 + \xi W^2 - a \\ T^2 = \dfrac{a(u+1)}{\xi} - W^2 \\ Y = \dfrac{\xi}{\sqrt{a(u+1)}}TW \\ U^2 = \xi W^2 - a \\ V^2 = -\xi W^2 + au. \end{cases}$$

Consider $\mathbb{K}_0 := \mathbb{K}(W)$. Clearly, $Z \in \mathbb{K}(W)$. We consider now $\mathbb{K}_1 := \mathbb{K}(X, W)$, where $X^2 = -\frac{\xi^2}{a(u+1)}W^4 + \xi W^2 - a$. It is readily seen that $-\frac{\xi^2}{a(u+1)}W^4 + \xi W^2 - a$ is not a square

in $\mathbb{K}_0$ and thus $\mathbb{K}_1$ is a Kummer extension of $\mathbb{K}_0$ with field of constants $\mathbb{F}_q$ by Theorem 2.1 and Lemma 2.3. Let $\mathbb{K}_2 := \mathbb{K}(X, T, W)$, where $T^2 = \frac{a(u+1)}{\xi} - W^2$. Since $\pm\sqrt{\frac{a(u+1)}{\xi}}$ are simple zeros of $\frac{a(u+1)}{\xi} - W^2$, which are not zeros of $-\frac{\xi^2}{a(u+1)}W^4 + \xi W^2 - a$, we conclude that above the places $P_{\pm\sqrt{\frac{a(u+1)}{\xi}}} \in \mathbb{K}_0$ there are exactly 4 places in $\mathbb{K}_1$ which are simple zeros of $-\frac{\xi^2}{a(u+1)}W^4 + \xi W^2$ and thus this function cannot be a square in $\mathbb{K}_1$. Again by Theorem 2.1 and Lemma 2.3 we conclude that $\mathbb{K}_2$ is a Kummer extension of $\mathbb{K}_1$ and its field of constants $\mathbb{F}_q$.

Consider now $\mathbb{K}_3 := \mathbb{K}(X, T, U, W)$, where $U^2 = \xi W^2 - a$. The zeros of $\xi W^2 - a$ in $\mathbb{K}_2$ are not zeros of X nor of T and thus they lie over unramified places in the extension $\mathbb{K}_2 : \mathbb{K}_0$. This shows that they are simple zeros for $\xi W^2 - a$ and thus $\xi W^2 - a$ is not a square in $\mathbb{K}_2$. By Theorem 2.1 and Lemma 2.3 we conclude that $\mathbb{K}_3$ is a Kummer extension of $\mathbb{K}_2$ and its field of constants $\mathbb{F}_q$.

Let $\mathbb{K}_4 := \mathbb{K}(X, T, U, V, W)$, where $V^2 = -\xi W^2 + au$. The zeros of $-\xi W^2 + au$ in $\mathbb{K}_3$ are not zeros of X, nor of T, nor of U and thus they lie over unramified places in the extension $\mathbb{K}_3 : \mathbb{K}_0$. Arguing as before, we conclude that $\mathbb{K}_4$ is a Kummer extension of $\mathbb{K}_3$ and its field of constants $\mathbb{F}_q$.

To conclude the proof it is sufficient to note that $\mathbb{K}_5 := \mathbb{K}(X, Y, T, U, V, W)$ coincides with $\mathbb{K}_4$. □

We now show that the conjecture of [4] is false, and not only there is no infinite family of APN functions, but in fact there are no APN functions besides those listed in [4, Table 5].

Theorem 3.3 *Let q be an odd prime power, $q > 125$, and select $u \in \mathbb{F}_q \setminus \{0, \pm 1\}$. The polynomial $F(x) = x^{(q+3)/2} + ux^2$ is not APN.*

Proof We first let $u = 3$. Although, one can also infer it from (3.2), if $q \equiv 1 \pmod 4$, our treatment of System 3.9 requires $a(u+1)$ and $-4a(u+1)$ to be squares concurrently, which can happen for $q \equiv 1 \pmod 4$, since $\eta(-1) = 1$. We removed $u = 3$ from the statement of Theorem 3.2 (and even below), since we wanted to treat the system globally, but the arguments also hold for $u = 3, q \equiv 1 \pmod 4$.

Thus, we next let $u = 3, q \equiv 3 \pmod 4$, and so, $\eta(-1) = -1$. Further, if n is even, then regardless of p, 2, 3 are quadratic residues and we get at least three viable solutions by taking $\eta(a) = 1$, $b = -4a^2$, as we see from (3.2). If n is odd, $p \equiv 3, 11 \pmod{24}$, again, 2, 3 are quadratic residues and the same argument applies. If n is odd, $p \equiv 23 \pmod{24}$ (we removed $p \equiv 9 \pmod{24}$, since we are in the case of $q \equiv 3 \pmod 4$; similarly, we will also remove, from the next discussion, the cases $p \equiv 5, 21 \pmod{24}$), then $\eta(2) = 1, \eta(3) = -1$. Taking $b = -4a^2$ with $\eta(a) = 1$, at least three solutions of (3.2) survive. If n is odd, and $p \equiv 11 \pmod{24}$, then $\eta(2) = -1, \eta(3) = 1$, taking again, $b = -4a^2$, with $\eta(a) = -1$, exactly three solutions survive. If n is odd, and $p \equiv 19 \pmod{24}$, then $\eta(2) = \eta(3) = -1$, and $b = 4a^2$, at least three solutions survive. Therefore, even when $u = 3$, the function is not APN, for p larger than 29 (see [4, Table 5], for small cases).

We now let $u \neq \pm 1, 3$. Select $a \in \mathbb{F}_q^*$ such that $a(u+1)$ is a square in $\mathbb{F}_q$ and consider a fixed nonsquare $\xi \in \mathbb{F}_q$. By Theorem 3.2, System (3.9) defines a function field whose field of constants is $\mathbb{F}_q$. By direct checking, following the same notation as in the proof of Theorem

3.2, Theorem 2.1 yields that the genus of $\mathbb{K}_i$, $i = 0, \ldots, 5$, is 0, 1, 3, 9, 25, 25 respectively. There are at most 2^4 places lying over P_∞. Since we need the three roots to be distinct, $b + a^2(u+1) \neq 0$, together with $Z \neq 0$. Recalling that $b = a(u+1)(2X^2 + a)$, the first above condition is equivalent to $X^2 \neq -a$ and thus $-\frac{\xi^2}{a(u+1)}W^4 + \xi W^2 = 0$. There are at most 2^6 places in $\mathbb{K}_5$ satisfying this constraint. Finally, $Z = 0$ corresponds to $W^2 = \frac{a(u+1)}{2\xi}$ and again there are at most 2^5 places in $\mathbb{K}_5$ satisfying this constraint. Thus, the polynomial F is not APN whenever the lower bound given by the Hasse-Weil bound exceeds $2^4 + 2^5 + 2^6$, that is

$$q - 50\sqrt{q} - 111 > 0 \iff \sqrt{q} \geq 52.13, \text{ so }, q \geq 2719.$$

For the cases when $125 < q = p^n < 2719$ (that is, outside [4, Table 5], which lists $q = 5^3$ as the highest cardinality when the function is APN, for some specific values of u), we used Magma [3] and found no other cases when the function is APN. The claim follows. □

Remark 3.4 Via Magma [3], we found that, in addition to [4, Table 5], there are other interesting examples of functions of best/optimal differential uniformity. For example, if $p = 3$, $n = 1$, $u = -1$, the function is PN; if $p = 3$, $n = 2$, $u = g, g^3, g^5, g^7$, the function is PN.

In the appendix (Tables 2-6) we display more computational data to display the differential spectrum for various dimensions and parameters u.

4 A related class of potential APNs

Let $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ on $\mathbb{F}_{p^n}$ with $p > 3$, $q = p^n$. Computationally, we observed that, for some u values, F is APN for $p = 5, 7, 11, 13, 19, 23$ and $n = 1$, as well as $p = 5, n = 2$, and has mostly low differential uniformity, for other small dimensions.

One surely wonders if there are infinitely many pairs (p, n) for which F is APN. We shall show that that is not the case (at least when $q \equiv 1 \pmod 3$).

Lemma 4.1 *Let $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ on $\mathbb{F}_{p^n}$ with $p > 3$, $q = p^n$, and $u \notin \{\pm 1\}$. Fix $a \in \mathbb{F}_q^*$ and $b \in \mathbb{F}_q$. Then:*

(1) *If $t_{x+a} = t_x = \epsilon \in \{\pm 1\}$, then the differential equation $F(x+a) - F(x) = b$ has two solutions for some (a, b).*
(2) *If $t_{x+a} = -t_x = \epsilon \in \{\pm 1\}$, the differential equation is equivalent to a cubic $G_{a,b}(x) = 0$, where $G_{a,b}(x) = 0$ is defined in (4.1).*
(3) *When $q \equiv 1 \pmod 3$, the cubic $G_{a,b}(x) = 0$ from part (2) possesses three distinct solutions in $\mathbb{F}_q$ if and only if $\delta(a, b) \in \square_q$ and $G_{a,b}(\beta_1)/G_{a,b}(\beta_2)$ is a cube in $\mathbb{F}_q$, where β_1, β_2 are the roots of the Hessian H(T) of $G_{a,b}$ and $\Delta \neq 0$.*

Proof First, note that the differential equation of F at $a \in \mathbb{F}_q^*, b \in \mathbb{F}_q$ is equivalent to

$$(x+a)^3(u + t_{x+a}) - x^3(u + t_x) = b.$$

For part (1): when $t_{x+a} = t_x = \epsilon$, the differential equation becomes $(x+a)^3(u+\epsilon) - x^3(u+\epsilon) = b$, and since $u+\epsilon \neq 0$ we may divide to get $(x+a)^3 - x^3 = \frac{b}{u+\epsilon}$. Expanding the left side gives $3x^2a + 3xa^2 + a^3 = \frac{b}{u+\epsilon}$, which rearranges to

$$x^2 + ax + \frac{a^2}{3} - \frac{b}{3(u+\epsilon)} = 0,$$

of discriminant $\Delta = -\frac{a^2}{3} + \frac{4b}{3(u+\epsilon)}$, which is linear in b. It is known that in $\mathbb{F}_{p^n}$ half of all nonzero elements are squares and half are non-squares. Regardless, since Δ is linear in b, then we conclude that one can always find b to force Δ to be a nonzero square and hence our differential equation has two solutions, for some a, b.

For part (2): when $t_{x+a} = -t_x = \epsilon$, we have $t_x = -\epsilon$, so the differential equation is $(x+a)^3(u+\epsilon) - x^3(u-\epsilon) = b$. Expanding and collecting,

$$\begin{aligned}(u+\epsilon)(x^3 + 3x^2a + 3xa^2 + a^3) - (u-\epsilon)x^3 &= b,\\ 2\epsilon x^3 + (u+\epsilon)(3x^2a + 3xa^2 + a^3) &= b,\end{aligned}$$

and dividing through by 2ϵ yields the cubic

$$G_{a,b}(x) := x^3 + \frac{3a(u+\epsilon)}{2\epsilon}\,x^2 + \frac{3a^2(u+\epsilon)}{2\epsilon}\,x + \frac{a^3(u+\epsilon) - b}{2\epsilon} = 0. \tag{4.1}$$

For part (3): the three-roots criterion follows from [7, Theorem 1.34]. The Hessian of $G_{a,b}(x)$ is

$$H(T) := \frac{-9}{4}\left((-a^2u^2 + a^2)T^2 + (-a^3u^2 + a^3 - 2b)T + (-abu - ab)\right),$$

whose discriminant is

$$\delta(a,b) := \frac{81}{16}\left(a^6u^4 - 2a^6u^2 + a^6 - 4a^3bu^3 + 4a^3bu + 4b^2\right). \tag{4.2}$$

The roots $\beta_{1,2}$ of $H(T)$ are given by the quadratic formula:

$$\beta_{1,2} = \frac{a^3u^2 - a^3 + 2b \pm X}{2a^2(1-u^2)}, \quad X^2 = \delta(a,b).$$

Let η be a fixed third root of unity in $\mathbb{F}_q$, and $e \in \mathbb{F}_q$ fixed with $e^3 = G_{a,b}(\beta_1)/G_{a,b}(\beta_2)$. The three roots of $G_{a,b}(x)$ are the standard Lagrange resolvent expressions

$$x_1 := \frac{\beta_2 e - \beta_1}{e-1}, \quad x_2 := \frac{\beta_2\eta e - \beta_1}{\eta e - 1}, \quad x_3 := \frac{\beta_2\eta^2 e - \beta_1}{\eta^2 e - 1}. \tag{4.3}$$

Finally, by substituting β_1 and β_2 into $G_{a,b}(T)$ and simplifying, one obtains

$$\frac{G_{a,b}(\beta_1)}{G_{a,b}(\beta_2)} = \frac{a^3u^3 - a^3u - 2b - 4X/9}{a^3u^3 - a^3u - 2b + 4X/9}. \tag{4.4}$$

□

Lemma 4.2 *Let $q \equiv 1 \pmod 3$, $u \notin \{\pm 1, \pm\sqrt{3}, \pm 2\}$, and let $\xi \in \mathbb{F}_q$ be a fixed non-square. With the notation of Lemma 4.1, $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ possesses at least three solutions to $F(x+a) - F(x) = b$ satisfying $t_x = 1 = -t_{x+a}$ if the following system*

$$\begin{cases} (uY^2 + uY + u + Y^2 + 3Y + 1)(u-1)a^2 - 4YW_0^2(u-1)a - 4W_0^4Y = 0, \\ Z_0^2 = \frac{-a + W_0^2}{\xi}, \\ Z_1^2 = -\frac{(2\eta+4)auY + (-2\eta+2)au - 2\eta aY + (2\eta+2)a + (4\eta+4)W_0^2Y - 4\eta W_0^2}{4(Y+1)}, \\ W_1^2 = -\frac{(2\eta+4)\xi auY + (-2\eta+2)\xi au - 2\eta\xi aY - 4aY + (2\eta+2)a\xi - 4a + (4\eta+4)\xi W_0^2Y - 4\eta\xi W_0^2}{4(Y+1)}, \\ Z_2^2 = \frac{(2\eta-2)auY + (-2\eta-4)au + (-2\eta-2)aY + 2\eta a + 4\eta W_0^2Y + (-4\eta-4)W_0^2}{4\xi(Y+1)}, \\ W_2^2 = \frac{(2\eta-2)\xi auY + (-2\eta-4)\xi au + (-2\eta+2)\xi aY + (2\eta+4)a\xi + 4\eta\xi W_0^2Y + (-4\eta-4)\xi W_0^2}{4\xi(Y+1)}, \end{cases} \tag{4.5}$$

has a solution $(a, Y, Z_0, Z_1, Z_2, W_0, W_1, W_2) \in \mathbb{F}_q^8$ with $a \neq 0$, $(Y^3 - 1)Y(Y+1) \neq 0$, and $(u+1)Y^2 + (3-2u)Y + u + 1 \neq 0$, where η denotes a primitive cube root of unity in $\mathbb{F}_q$. The condition $(u+1)Y^2 + (3-2u)Y + u + 1 \neq 0$ together with $Y(Y+1) \neq 0$ ensures $X \in \mathbb{F}_q^*$.

Proof In what follows we want to prove that if $q \equiv 1 \pmod 3$ there exist $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$ such that $G_{a,b}(x)$ has three distinct roots in $\mathbb{F}_q$, all of them satisfying $t_x = 1 = -t_{x+a}$.

We will make use of a direct expression for the three roots. Let η be a fixed third root of unity in $\mathbb{F}_q$, and $e \in \mathbb{F}_q$ fixed with $e^3 = G_{a,b}(\beta_1)/G_{a,b}(\beta_2)$. By Lemma 4.1(3), the three roots of $G_{a,b}(x)$ are the x_1, x_2, x_3 given in (4.3).

Let $\xi \in \mathbb{F}_q$ be a fixed nonsquare. The function $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ possesses at least three solutions (with $t_{x_i} = 1$ and $t_{x_i+a} = -1$) if the system

$$\begin{cases} a^6u^4 - 2a^6u^2 + a^6 - 4a^3bu^3 + 4a^3bu + 4b^2 = \frac{16X^2}{81}, \\ \frac{a^3u^3 - a^3u - 2b - 4X/9}{a^3u^3 - a^3u - 2b + 4X/9} = Y^3, \\ \frac{\beta_2\eta^i e - \beta_1}{\eta^i e - 1} = \xi Z_i^2, \quad i = 0, 1, 2, \\ \frac{\beta_2\eta^i e - \beta_1}{\eta^i e - 1} + a = W_i^2, \quad i = 0, 1, 2, \end{cases}$$

has nontrivial solutions $(X, Y, Z_0, Z_1, Z_2, W_0, W_1, W_2, a, b)$ with $aXY \neq 0, Y \neq 1$.

Note that $\frac{\beta_2\eta^i e - \beta_1}{\eta^i e - 1} + a = W_i^2$ can be rewritten as $\xi Z_i^2 + a = W_i^2$, $i = 0, 1, 2$.

From the second equation one gets

$$b = \frac{9a^3u^3Y^3 - 9a^3u^3 - 9a^3uY^3 + 9a^3u + 4Y^3X + 4X}{18(Y^3-1)}.$$

Combining with the other equations one obtains

$$\begin{cases} -81(Y^3-1)^2(u^2-1)^3a^6 + 64Y^3X^2 = 0, \\ (Y-1)\big(9(u^2-1)a^2(au+a+2\xi Z_0^2)Y^3 - 8XY^2 - 8XY - 9(u^2-1)a^2(au+a+2\xi Z_0^2)\big) = 0, \\ \xi Z_0^2 + a = W_0^2, \\ (Y-\eta^2)\big(9(u^2-1)a^2(au+a+2Z_1^2)Y^3 - 8\eta^2XY^2 - 8\eta XY - 9(u^2-1)a^2(au+a+2Z_1^2)\big) = 0, \\ \xi Z_1^2 + a = W_1^2, \\ (Y-\eta)\big(9(u^2-1)a^2(au+a+2\xi Z_2^2)Y^3 - 8\eta XY^2 - 8\eta^2XY - 9(u^2-1)a^2(au+a+2\xi Z_2^2)\big) = 0, \\ \xi Z_2^2 + a = W_2^2. \end{cases}$$

Let us discard the factors $(Y-1)$, $(Y-\eta)$, $(Y-\eta^2)$. From the second equation we obtain

$$X = \frac{9(au+a+2\xi Z_0^2)a^2(u^2-1)(Y^3-1)}{8Y(Y+1)},$$

and thus the system above, using also $\xi Z_0^2 = -a + W_0^2$, reads (after discarding factors such as a, Y, $Y+1$, and (Y^3-1))

$$\begin{cases} \xi Z_0^2 = -a + W_0^2, \\ (uY^2 + uY + u + Y^2 + 3Y + 1)(u-1)a^2 - 4YW_0^2(u-1)a - 4W_0^4Y = 0, \\ 3auY - 3\eta au + (-2\eta - 1)aY + (\eta+2)a + (2\eta+4)W_0^2Y + (-4\eta-2)W_0^2 + (-2\eta+2)(Y+1)Z_1^2 = 0, \\ W_1^2 = a + \xi Z_1^2, \\ 3auY + (3\eta+3)au + (2\eta+1)aY + (-\eta+1)a + (-2\eta+2)W_0^2Y + (4\eta+2)W_0^2 + (2\eta+4)(Y+1)\xi Z_2^2Y = 0, \\ W_2^2 = \xi Z_2^2 + a. \end{cases}$$

Finally we can combine the fourth and the third, and the sixth and fifth equations to get System (4.5), where the constraints $a \neq 0$, $(Y^3-1)Y(Y+1) \neq 0$, and $(u+1)Y^2 + (3-2u)Y + u + 1 \neq 0$ ensure $X \in \mathbb{F}_q^*$. □

We now use these two lemmas to prove the main result of this section.

Theorem 4.3 *Let $q \equiv 1 \pmod 3$. Consider $u \notin \{\pm 1, \pm\sqrt{3}, \pm 2\}$. If q is large enough then $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ is not APN.*

Proof By Lemma 4.2, it suffices to find $(a, Y, Z_0, Z_1, Z_2, W_0, W_1, W_2) \in \mathbb{F}_q^8$ satisfying System (4.5) with $a \neq 0$, $(Y^3-1)Y(Y+1) \neq 0$, and $(u+1)Y^2 + (3-2u)Y + u + 1 \neq 0$. We show that such solutions exist for q sufficiently large by proving System (4.5) defines a function field with constant field $\mathbb{F}_q$, and then applying the Hasse-Weil bound.

Consider first the case where u is not a root of

$$\begin{aligned} h(u) :=& (u^2-4)\Big((\xi^2-\xi)u + \xi^2 - \xi + 2/3\Big)\Big(\xi^2u^2 + (-\xi^2+\xi)u - 2\xi^2 + \xi - 2\Big) \\ &\cdot (u-1)(u^2-3)(\xi u + \xi - 1)\Big(\xi u - 2/3\xi^2 + 1/3\xi - 2/3\Big) \\ &\cdot \Big(\xi^2u^2 + \xi u - 3\xi^2 + 3\xi - 2\Big)\Big(\xi^2u^2 + (2\xi - \xi^2)u - 2\xi^2 + 2\xi - 2\Big). \end{aligned}$$

To this end, fix an element $W_0 \neq 0$ in $\mathbb{F}_q$.

We will show that System (4.5) defines a function field whose field of constants is $\mathbb{F}_q$. This will provide, asymptotically, a negative answer for the APN-ness of the function $F(x)$.

Consider first the equation

$$(uY^2 + uY + u + Y^2 + 3Y + 1)(u-1)a^2 - 4YW_0^2(u-1)a - 4W_0^4Y = 0.$$

The discriminant with respect to a is

$$64Y(Y+1)^2W_0^4(u^2-1),$$

and it is, clearly, a nonsquare in $\mathbb{K}_0 := \mathbb{K}(Y)$. Thus, by Theorem 2.1 and Lemma 2.3, the field of constants of $\mathbb{K}_1 = \mathbb{K}_0(a)$ is $\mathbb{F}_q$. We want now to prove that the other 5 equations define Kummer extensions with field of constants $\mathbb{F}_q$.

To this end, consider the subsequent equations written as

$$Z_0^2 = \phi_1(a,Y), \quad Z_1^2 = \phi_2(a,Y), \quad W_1^2 = \phi_3(a,Y), \quad Z_2^2 = \phi_4(a,Y), \quad W_2^2 = \phi_5(a,Y),$$

and denote by $\mathbb{K}_2 \subset \cdots \subset \mathbb{K}_6$ the corresponding function fields.

It is sufficient to show that for each $i = 1, \ldots, 5$ there exists at least one place in $\mathbb{K}_1$ which is a simple zero for ϕ_i and a nonzero for each ϕ_j, $j \neq i$. This will ensure the existence of a place in $\mathbb{K}_{i+1}$ which is a simple zero for ϕ_i.

Thus we check the resultant between the numerators of the functions $\phi_i(a,Y)$ and $(uY^2 + uY + u + Y^2 + 3Y + 1)(u-1)a^2 - 4YW_0^2(u-1)a - 4W_0^4Y$ with respect to a. We want to prove that each of them has a nonrepeated linear factor in Y (different from Y and $(Y+1)$), which is not a factor of any other resultant.

We list below the factorizations of these resultants:

$$(u+1)W_0^4\Big((u-1)Y^2 + (u-3)Y + u - 1\Big),$$

$$(Y+1)^4W_0^4(u+1)\Big((u-1)Y^2 + (-\eta-1)uY + \eta u + (3\eta+3)Y - \eta\Big),$$

$$(Y+1)^4W_0^4\Big(\xi^2(u^2-1)Y^2 - (\eta+1)(\xi^2u^2 - 2\xi^2u + 4\xi u - 3\xi^2 + 4\xi - 4)Y + \eta\xi^2(u^2-1)\Big),$$

$$\xi^2(Y+1)^4W_0^4(u+1)\Big((u-1)Y^2 + (\eta u - 3)Y + (-\eta-1)u + \eta + 1\Big),$$

$$\xi^4(Y+1)^4W_0^4(u-1)\Big((u+1)Y^2 + (\eta u + 3)Y + (-\eta-1)u - \eta - 1\Big).$$

As can be easily checked, there is a common zero among them (apart from -1) only if u is a root of $h(u)$. If u is not a root of $h(u)$, none of the degree-2 factors above has $Y = -1$ as a root.

Thus, there exists a simple zero of each ϕ_i which is not a zero (nor a pole) of ϕ_j, $j \neq i$, for each $i = 1, \ldots, 5$. By Theorem 2.1 and Lemma 2.3, each extension $\mathbb{K}_{i+1} : \mathbb{K}_i$ is a Kummer extension with field of constants $\mathbb{F}_q$. Therefore, $\mathbb{K}_6$ has field of constants $\mathbb{F}_q$ and genus bounded by Theorem 2.1.

By the Hasse-Weil bound (Theorem 2.2), for q sufficiently large, there exist $\mathbb{F}_q$-rational places of $\mathbb{K}_6$ satisfying all the required conditions, which correspond to solutions of System (4.5). Hence $F(x)$ is not APN for large q.

Case when u is a root of $h(u)$: Suppose that u is a zero of $h(u)$ distinct from $\pm 1, \pm\sqrt{3}, \pm 2$. We now show that we can choose a different nonsquare $\xi \in \mathbb{F}_q$ to make the argument work.

The polynomial $h(u)$ involves the parameter ξ. For a fixed $u \in \mathbb{F}_q \setminus \{0, \pm 1, \pm\sqrt{3}, \pm 2\}$, viewing $h(u)$ as a polynomial in ξ, we can write

$$h(u) = c(u) \cdot \prod_{i=1}^{m} (\xi - \xi_i(u))^{e_i},$$

where $c(u) \in \mathbb{F}_q[u]$ is the leading coefficient with respect to ξ, and $\xi_i(u) \in \overline{\mathbb{F}_q}$ are the roots. By examining the factorization of $h(u)$, the total degree in ξ satisfies $\sum_{i=1}^{m} e_i \leq 10$.

Since there are $(q-1)/2$ nonsquares in $\mathbb{F}_q^*$, and at most 10 of them can be roots of $h(u)$ (only counting those in $\mathbb{F}_q$), for $q \geq 23$ we can always find a nonsquare $\xi \in \mathbb{F}_q$ such that $h(u) \neq 0$. For such a choice of ξ, the resultant computations above show that there are no common zeros (apart from $Y = -1$) among the five degree-2 polynomials in Y, and thus the Kummer extension argument proceeds as before.

For the finitely many small values $q < 23$, we handle each case individually via direct computation or by using the explicit structure of $h(u)$ to verify that at least one suitable ξ exists for each relevant u. □

Remark 4.4 Presumably, the same outcome will happen for $q \equiv 2 \pmod 3$. Recall (see [13, Theorem 1, Corollary 2.9], or [7]) that if $\mathbb{F}_q$ is a field of characteristic different from 3, then $f(x) = ax^3 + bx^2 + cx + d, a \neq 0$, permutes $\mathbb{F}_q$ if and only if $b^2 = 3ac$, and $q \equiv 2 \pmod 3$. Thus, the case of $q \equiv 2 \pmod 3$ will be slightly more involved (though, doable), since one needs several cases necessary to handle the roots of a cubic under this modularity condition on q.

5 Character (Weil) sum analysis of the difference distribution table

Since determining the differential spectrum of a function theoretically or computationally can be quite difficult, character-based methods offer significant advantages. The approach proposed in [14] achieves speeds of more than ten times the classical method. We further develop this for our families of functions.

Theorem 5.1 *Let $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^j+1}$, $0 \leq j \leq k < n$, on $\mathbb{F}_{p^n}$. The number of solutions to $F(x+a) - F(x) = b$ for $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$ is given by*

$$\mathcal{N}_{a,b} = p^{-n} \sum_{\epsilon,\mu \in \{\pm 1\}} \sum_{\alpha,x \in \mathbb{F}_{p^n}} \chi_1 \Big(\alpha(u+\epsilon)x^{p^k+1} - \alpha(u+\epsilon\mu)x^{p^j+1} + \Big((\alpha a(u+\epsilon))^{p^{n-k}} + \alpha a^{p^k}(u+\epsilon) \Big) x + \alpha \Big((u+\epsilon)a^{p^k+1} - b \Big) \Big),$$

where the outer sum is over the four combinations of $\epsilon = \eta(x+a), \mu = \eta(x)$.

Proof As before, we let $\eta(x) = t_x$ and $\eta(x+a) = t_{x+a}$. The differential equation becomes

$$(x+a)^{p^k+1}(u+t_{x+a}) - x^{p^j+1}(u+t_x) = b,$$

and with notations $t_{x+a} = \epsilon, t_x = \epsilon\mu$, where $\mu, \epsilon \in \{\pm 1\}$, we obtain

$$(u+\epsilon)x^{p^k+1} - (u+\epsilon\mu)x^{p^j+1} + (u+\epsilon)(ax^{p^k} + a^{p^k}x) + (u+\epsilon)a^{p^k+1} - b = 0. \quad (5.1)$$

The number $\mathcal{N}_{a,b}$ of solutions is given by the standard character sum formula [10]:

$$\begin{aligned}\mathcal{N}_{a,b} &= \frac{1}{p^n}\sum_{x\in\mathbb{F}_{p^n}}\sum_{\alpha\in\mathbb{F}_{p^n}}\chi_1\left(\alpha\left((u+\epsilon)x^{p^k+1} - (u+\epsilon\mu)x^{p^j+1} + (u+\epsilon)(ax^{p^k} + a^{p^k}x) + (u+\epsilon)a^{p^k+1} - b\right)\right)\\ &= \sum_{\alpha\in\mathbb{F}_{p^n}}\chi_1\left(\alpha\left((u+\epsilon)a^{p^k+1} - b\right)\right)\sum_{x\in\mathbb{F}_{p^n}}\chi_1\left(\alpha\left((u+\epsilon)x^{p^k+1} - (u+\epsilon\mu)x^{p^j+1} + (u+\epsilon)(ax^{p^k} + a^{p^k}x)\right)\right).\end{aligned}$$

We now simplify the linear term. Applying the Frobenius automorphism p^k times to $\alpha a(u+\epsilon)x^{p^k}$ gives

$$\left(\alpha a(u+\epsilon)x^{p^k}\right)^{p^k} = \alpha^{p^k}a^{p^k}(u+\epsilon)^{p^k}x^{p^{2k}}.$$

Since $u, \epsilon \in \mathbb{F}_{p^n}$ and $\epsilon = \pm 1$, we have $(u+\epsilon)^{p^k} = (u+\epsilon)$ by the Frobenius property. Raising to the p^{n-k} power gives

$$\left(\alpha a(u+\epsilon)x^{p^k}\right)^{p^{n-k}} = \alpha^{p^{n-k}}a^{p^{n-k}}(u+\epsilon)^{p^{n-k}}x^{p^n} = (\alpha a(u+\epsilon))^{p^{n-k}}x,$$

where we used $x^{p^n} = x$ for all $x \in \mathbb{F}_{p^n}$.

Therefore, the linear terms combine as

$$\begin{aligned}\alpha a(u+\epsilon)x^{p^k} + \alpha a^{p^k}(u+\epsilon)x &= \alpha(u+\epsilon)\left(ax^{p^k} + a^{p^k}x\right)\\ &= \chi_1\left(\left((\alpha a(u+\epsilon))^{p^{n-k}} + \alpha a^{p^k}(u+\epsilon)\right)x\right).\end{aligned}$$

Setting $B = (\alpha a(u+\epsilon))^{p^{n-k}} + \alpha a^{p^k}(u+\epsilon)$, the inner sum becomes

$$\sum_{x\in\mathbb{F}_{p^n}}\chi_1\left(\alpha(u+\epsilon)x^{p^k+1} - \alpha(u+\epsilon\mu)x^{p^j+1} + Bx\right).$$

Since each of the four pairs $(\epsilon, \mu) \in \{(1,1),(1,-1),(-1,1),(-1,-1)\}$ corresponds to a different combination of $\eta(x+a)$ and $\eta(x)$, and these cases partition all possible $x \in \mathbb{F}_{p^n}$, the total count is obtained by summing the character sum contributions over all four cases. More precisely, for each $x \in \mathbb{F}_{p^n}$, exactly one pair (ϵ, μ) satisfies $\eta(x+a) = \epsilon$ and $\eta(x) = \epsilon\mu$, so we must sum over all four possibilities to capture all solutions.

This completes the proof. □

5.1 Simplifications for the case $j = k$

When $j = k$, the character sum simplifies significantly and we can obtain explicit bounds.

Corollary 5.2 *For $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^k+1}$ with $k < n$, the character sum reduces to*

$$\mathcal{N}_{a,b} = p^{-n} \sum_{\epsilon,\mu\in\{\pm 1\}} \sum_{\alpha,x\in\mathbb{F}_{p^n}} \chi_1\left(\alpha\epsilon(1-\mu)x^{p^k+1} + Bx + \alpha\left((u+\epsilon)a^{p^k+1} - b\right)\right),$$

where $B = (\alpha a(u+\epsilon))^{p^{n-k}} + \alpha a^{p^k}(u+\epsilon)$.

We now concentrate on the inner sum for fixed α. Let

$$S_\alpha := \sum_{x\in\mathbb{F}_{p^n}} \chi_1\left(A_1x^{p^k+1} + A_2x^{p^j+1} + Bx\right),$$

where $A_1 = \alpha(u+\epsilon)$ and $A_2 = -\alpha(u+\epsilon\mu)$.

Proposition 5.3 *The squared magnitude of S_α satisfies*

$$|S_\alpha|^2 = p^n \sum_{\substack{z\in\mathbb{F}_{p^n}\\ E(z)=0}} \chi_1\left(A_1z^{p^k+1} + A_2z^{p^j+1} + Bz\right),$$

where $E(z) = A_1(z^{p^k} + z^{p^{n-k}}) + A_2(z^{p^j} + z^{p^{n-j}})$.

Proof We compute

$$\begin{aligned}
|S_\alpha|^2 &= S_\alpha \cdot \bar{S}_\alpha \\
&= \sum_{x,y\in\mathbb{F}_{p^n}} \chi_1\left(A_1\left(x^{p^k+1} - y^{p^k+1}\right) + A_2\left(x^{p^j+1} - y^{p^j+1}\right) + B(x-y)\right) \\
&= \sum_{y,z\in\mathbb{F}_{p^n}} \chi_1\left(A_1\left(z^{p^k+1} + z^{p^k}y + zy^{p^k}\right) + A_2\left(z^{p^j+1} + z^{p^j}y + zy^{p^j}\right) + Bz\right) \\
&= \sum_{z\in\mathbb{F}_{p^n}} \chi_1\left(A_1z^{p^k+1} + A_2z^{p^j+1} + Bz\right) \sum_{y\in\mathbb{F}_{p^n}} \chi_1\left(E(z)\cdot y\right),
\end{aligned}$$

where we used the substitution $x = y + z$ and the fact that $\chi_1(cy) = 0$ unless $c = 0$.

The inner sum over y equals p^n if $E(z) = 0$ and equals 0 otherwise, completing the proof. □

Corollary 5.4 *When $k = j$ and $\mu = 1$ (or $\alpha = 0$), we have $E(z) \equiv 0$, hence $|S_\alpha|^2 = p^nS_\alpha$. This implies either $S_\alpha = 0$ or $S_\alpha = p^n$.*

Corollary 5.5 *When $k = j$, $\mu = -1$, $\alpha \neq 0$, and $\frac{n}{\gcd(n,2k)}$ is odd, there exist $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$ such that $\mathcal{N}_{a,b} \geq p^n$. Therefore, F cannot be APN under these conditions.*

Proof When $k = j$, $\mu = -1$, and $\alpha \neq 0$, the condition $E(z) = 0$ from Proposition 5.3 becomes $z^{p^{2k}} + z = 0$.

If $\frac{n}{\gcd(n,2k)}$ is odd, then $z^{p^{2k}} + z$ is a permutation polynomial with only $z = 0$ as its root. Therefore, $|S_\alpha|^2 = p^n S_\alpha$, which implies $S_\alpha \in \{0, p^n\}$.

For case $D_{1,-1}$ (where $\eta(x + a) = 1$ and $\eta(x) = -1$, so $\epsilon = 1$), the character sum analysis yields:

$$S_\alpha = p^n \chi_1 \left(\alpha \left((u+1)a^{p^k+1} - b \right) \right).$$

The contribution from case $D_{1,-1}$ to the differential count is:

$$\mathcal{N}_{a,b}^{D_{1,-1}} = p^{-n} \sum_{\alpha \in \mathbb{F}_{p^n}} \chi_1 \left(\alpha \left((u+1)a^{p^k+1} - b \right) \right) S_\alpha.$$

When $b = (u + 1)a^{p^k+1}$, we have $\chi_1(\alpha((u + 1)a^{p^k+1} - b)) = \chi_1(0) = 1$ for all α, and thus:

$$\mathcal{N}_{a,b}^{D_{1,-1}} = p^{-n} \sum_{\alpha \in \mathbb{F}_{p^n}} S_\alpha = p^{-n}(0 + (p^n - 1) \cdot p^n) = p^n - 1.$$

Since $p^n - 1 > 2$ for any nontrivial finite field, this proves that F is not APN. □

This explicit construction complements our geometric approach and provides concrete parameter choices that witness the failure of the APN property.

6 The case $j = k$ j=k

When $j = k$ in the general class of the prior section, we can show a stronger result than the previous corollary.

Theorem 6.1 *We let $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^k+1}$ on $\mathbb{F}_{p^n}$, where $k < n$, $u \neq \pm 1$, $d = \gcd(n, k)$, $q = p^k$, $Q = p^n$. Then F(X) is not APN.*

Proof For given $a \in \mathbb{F}_p^*, b \in \mathbb{F}_p$ we need to look at the differential equation $F(x + a) - F(x) = b$, that is,

$$(x+a)^{\frac{p^n-1}{2}+p^k+1} + u(x+a)^{p^k+1} - x^{\frac{p^n-1}{2}+p^k+1} - ux^{p^k+1} = b.$$

Denoting $t_{x+a} = \eta(x + a), t_x = \eta(x)$, the equation above becomes

$$(x+a)^{p^k+1}(t_{x+a} + u) - x^{p^k+1}(t_x + u) = b. \tag{6.1}$$

We now distinguish four cases, which are displayed in the next table (we let $\epsilon = 1, 0$, if -1 is a $p^k - 1$ power in $\mathbb{F}_{p^n}$, respectively, not a power).

Case	t_{x+a}	t_x	Equation (6.1)	Number of roots
$D_{1,1}$	1	1	$x^{p^k} + a^{p^k-1}x + a^{p^k} - \frac{b}{u+1} = 0$	$\leq \epsilon \cdot (p^d - 1)$
$D_{-1,-1}$	-1	-1	$x^{p^k} + a^{p^k-1}x + a^{p^k} - \frac{b}{u-1} = 0$	$\leq \epsilon \cdot (p^d - 1)$
$D_{1,-1}$	1	-1	$x^{p^k+1} + \frac{a(1+u)}{2}x^{p^k} + \frac{a^{p^k}(1+u)}{2}x + \frac{a^{p^k+1}(1+u)-b}{2} = 0$	N_1
$D_{-1,1}$	-1	1	$x^{p^k+1} + \frac{a(1-u)}{2}x^{p^k} + \frac{a^{p^k}(1-u)}{2}x + \frac{a^{p^k+1}(1-u)+b}{2} = 0$	N_2

We shall look at the potential N_1, N_2 next, finding parameters a, b, for which either N_1, N_2 are greater than 2. With $r = \frac{a(1+u)}{2}$, $s = \frac{a^q(1+u)}{2}$, $t = \frac{a^{p^k+1}(1+u)-b}{2}$, for case $D_{1,-1}$, respectively, $r = \frac{a(1-u)}{2}$, $s = \frac{a^q(1-u)}{2}$, $t = \frac{a^{p^k+1}(1-u)+b}{2}$, for case $D_{-1,1}$, and using the substitution $x = (s - r^q)^{\frac{1}{q}}X - r$, both equations in cases $D_{1,-1}$ and $D_{-1,1}$ become

$$X^{q+1} + X + A = 0, \tag{6.2}$$

where

$$A = (u^q - u)^{-\frac{q+1}{q}}\left(-2b\,a^{-q-1} - u^2 + 1\right) = \frac{-2b\,a^{-q-1} - u^2 + 1}{\left(u - u^{\frac{1}{q}}\right)^{q+1}}, \text{ for case } D_{1,-1},$$

$$A = (u^q - u)^{-\frac{q+1}{q}}\left(2b\,a^{-q-1} - u^2 + 1\right) = \frac{2b\,a^{-q-1} - u^2 + 1}{\left(u - u^{\frac{1}{q}}\right)^{q+1}}, \text{ for case } D_{-1,1}.$$

Via [9, Theorem 8], we know that (6.2) has $p^d + 1$ roots if and only if there exists $U \in \mathbb{F}_Q \setminus \mathbb{F}_{p^{2d}}$ such that $A = \frac{(U-U^q)^{q^2+1}}{(U-U^{q^2})^{q+1}}$, in which case, those $p^d + 1$ roots are given by

$$x_0 = \frac{-1}{1 + (U - U^q)^{q-1}}, \; x_\alpha = \frac{-(U+\alpha)^{q^2-q}}{1 + (U - U^q)^{q-1}}, \; \alpha \in \mathbb{F}_{p^d}.$$

Regardless, of what the chosen $U \in \mathbb{F}_Q \setminus \mathbb{F}_{p^{2d}}$ is, since A is linear in b, then one is always able to find a value of b such that $A = \frac{(U-U^q)^{q^2+1}}{(U-U^{q^2})^{q+1}}$.

We can force x_0, x_1, and x_{-1} to be roots (asymptotically). Thus, we need

$$\begin{cases} \frac{-1}{1+(U-U^q)^{q-1}} = \xi X^2 \\ \frac{-1}{1+(U-U^q)^{q-1}} + a = Y^2 \\ \frac{-(U+1)^{q^2-q}}{1+(U-U^q)^{q-1}} = \xi Z^2 \\ \frac{-(U+1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a = V^2 \\ \frac{-(U-1)^{q^2-q}}{1+(U-U^q)^{q-1}} = \xi W^2 \\ \frac{-(U-1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a = T^2. \end{cases} \tag{6.3}$$

Combining the first and the third equation we get

$$\xi X^2(U+1)^{q^2-q} = \xi Z^2$$

and thus $Z = \pm X(U+1)^{(q^2-q)/2}$. With the same argument, $W = X(U-1)^{(q^2-q)/2}$. Thus it is enough to show the existence of solutions of the following system

$$\begin{cases} \frac{-1}{1+(U-U^q)^{q-1}} = \xi X^2 \\ \frac{-1}{1+(U-U^q)^{q-1}} + a = Y^2 \\ \frac{-(U+1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a = V^2 \\ \frac{-(U-1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a = T^2. \end{cases}$$

Clearly, all the roots of $1+(U-U^q)^{q-1}$ are distinct and so the poles of $\frac{-1}{1+(U-U^q)^{q-1}}$ are simple. This shows that

$$\frac{-1}{1+(U-U^q)^{q-1}} = \xi X^2$$

is absolutely irreducible and $\mathbb{K}(X,U) : \mathbb{K}(U)$, where $\mathbb{K}$ is the algebraic closure of $\mathbb{F}_q$, is a Kummer extension of the rational function field $\mathbb{K}(U)$ by Theorem 2.1. By Lemma 2.3 the field of constants of $\mathbb{K}(X,U)$ is $\mathbb{F}_q$. Consider the zeros of

$$\phi_1 := \frac{-1}{1+(U-U^q)^{q-1}} + a, \quad \phi_2 := \frac{-(U+1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a, \quad \phi_3 := \frac{-(U-1)^{q^2-q}}{1+(U-U^q)^{q-1}} + a.$$

They are roots of

$$\begin{aligned} \psi_1(U) &:= -1 + a(1+(U-U^q)^{q-1}), \\ \psi_2(U) &:= -(U+1)^{q^2-q} + a(1+(U-U^q)^{q-1}), \\ \psi_3(U) &:= -(U-1)^{q^2-q} + a(1+(U-U^q)^{q-1}), \end{aligned}$$

respectively.

Since we can suppose that $a \neq 0, 1$, all the roots of ψ_1, ψ_2, ψ_3 are distinct. In fact

$$\psi_i'(U) = -a(U-U^q)^{q-2}$$

and thus repeated roots can only belong to $\mathbb{F}_q$. On the other hand, $U \in \mathbb{F}_q$ being a root of ψ_i yields either $a = 0$ or $a = 1$.

Also, the zeros of ψ_i and ψ_j, $i \neq j$, are distinct. If ψ_1 and ψ_2 or ψ_1 and ψ_3 share a root, then such a root z satisfies $(z+1)^{q-1} = 1$ or $(z-1)^{q-1} = 1$, and thus $z \in \mathbb{F}_q$. We already showed that this is not possible. If ψ_2 and ψ_3 share a root z, then $z = (1+\lambda)(\lambda-1)$, for some λ in $\mathbb{F}_q \setminus \{0, \pm 1\}$ and thus $z \in \mathbb{F}_q$, again a contradiction to $a \neq 0, 1$. Consider the function field extensions

$$\mathbb{K}(Y,X,U):\mathbb{K}(X,U),\quad \mathbb{K}(V,Y,X,U):\mathbb{K}(Y,X,U),\quad \mathbb{K}(T,V,Y,X,U):\mathbb{K}(V,Y,X,U),$$

defined by $Y^2=\phi_1$, $V^2=\phi_2$, and $T^2=\phi_3$ respectively. From the argument above each ϕ_i is not a square in the corresponding function field and thus by Theorem 2.1 and Lemma 2.3 each of the above extensions is a Kummer extension with field of constants $\mathbb{F}_q$.

This shows that, if q is large enough, there are instances of U, X, Y, Z, V, W, T satisfying System (6.3) and thus (3.1) admits 3 solutions and $F(x)$ is not APN. □

Under some conditions, we can be more precise about the differential uniformity.

Theorem 6.2 *Let* $F(x)=x^{\frac{p^n-1}{2}+p^k+1}+ux^{p^k+1}$ *on* $\mathbb{F}_{p^n}$, *where* $k<n$, $u\neq\pm1$, $d=\gcd(n,k)$, $q=p^k$, $Q=p^n$. *Assume q is sufficiently large. Then:*

(1) *If* $\epsilon=0$ *(i.e.,* -1 *is not a* (p^k-1)*-power in* $\mathbb{F}_{p^n}$*), then* $\delta_F=p^d+1$.
(2) *If* $\epsilon=1$ *and* $\frac{n}{\gcd(n,2k)}$ *is odd, then* $\delta_F\geq p^n$ *and thus F cannot be APN.*
(3) *If* $\epsilon=1$ *and there exist* $(a,b,U)\in\mathbb{F}_Q^*\times\mathbb{F}_Q\times(\mathbb{F}_Q\setminus\mathbb{F}_{p^{2d}})$ *such that System (6.3) has solutions with exactly three distinct roots satisfying the character conditions, then* $\delta_F=3$.
(4) *If* $\delta_F\neq3$ *and* $\delta_F\neq p^n$*, and there exist parameters yielding exactly four distinct solutions from combining cases* $D_{1,1}$ *or* $D_{-1,-1}$ *with case* $D_{1,-1}$ *or* $D_{-1,1}$*, then* $\delta_F=4$.

Proof (1) When $\epsilon=0$, Cases $D_{1,1}$ and $D_{-1,-1}$ contribute no solutions since $u\pm1\neq0$ and the equations $x^{p^k}+a^{p^k-1}x+a^{p^k}-\frac{b}{u\pm1}=0$ would require -1 to be a (p^k-1)-power. The only contributions come from Cases $D_{1,-1}$ and $D_{-1,1}$, each potentially giving p^d+1 solutions when the conditions in (6.2) are satisfied with appropriate U. Since these cases are disjoint (different character conditions on x and $x+a$), we obtain $\delta_F=p^d+1$.

(2) This follows from Corollary 5.5 combined with the analysis in Section 5. When $\epsilon=1$, $\mu=-1$, $\alpha\neq0$, and $\frac{n}{\gcd(n,2k)}$ is odd, the character sum analysis shows $\mathcal{N}_{a,(u+\epsilon)a^{p^k+1}}=p^n$.

(3) From the proof of Theorem 6.1, when System (6.3) has solutions, Case $D_{1,-1}$ or $D_{-1,1}$ contributes p^d+1 solutions. However, we need to verify that only three of these satisfy the full character and distinctness conditions.

For exactly three solutions, we require:

- The roots x_0, x_1, x_{-1} from [9, Theorem 8] all satisfy $\eta(x_i)=-1$ and $\eta(x_i+a)=1$ (or vice versa for the other case).
- The remaining p^d-2 roots fail the character conditions.
- Cases $D_{1,1}$ and $D_{-1,-1}$ contribute no additional solutions.

This occurs when:

$$\eta\left(\frac{-1}{1+(U-U^q)^{q-1}}\right)=-\eta(\xi),\quad \eta\left(\frac{-(U\pm1)^{q^2-q}}{1+(U-U^q)^{q-1}}\right)=-\eta(\xi),$$

and

$$\eta\left(\frac{-1}{1+(U-U^q)^{q-1}}+a\right)=1,\quad \eta\left(\frac{-(U\pm 1)^{q^2-q}}{1+(U-U^q)^{q-1}}+a\right)=1,$$

while the other p^d-2 roots either violate the character conditions or coincide.

Since the function field $\mathbb{K}(T,V,Y,X,U)$ has genus bounded by a polynomial in p^d, and the number of $\mathbb{F}_Q$-rational places grows like Q by Hasse-Weil, for Q sufficiently large we can find such (a, b, U).

(4) This follows by examining when Cases $D_{1,1}$ or $D_{-1,-1}$ contribute exactly one solution (which requires $\epsilon=1$ and specific (a, b) making the linearized polynomial equation have a unique solution), while one of Cases $D_{1,-1}$ or $D_{-1,1}$ contributes exactly three solutions as in (3). The conditions are:

- For Case $D_{1,1}$: $b=(u+1)a^{p^k}$ yields the solution $x=0$, and $\eta(a)=1$.
- Combined with three solutions from Case $D_{1,-1}$ as in (3).
- The four solutions $x=0,x_0,x_1,x_{-1}$ are all distinct.

Alternatively, similar analysis applies with Case $D_{-1,-1}$ and $D_{-1,1}$. □

Remark 6.3 (1) For small q, computational verification shows that $\delta_F\in\{3,4\}$ frequently occurs when $\epsilon=1$. The distinction depends on subtle interactions between the character conditions and the choice of (a, b, U).

(2) When $\epsilon=1$ and $p^d>2$, it may be possible to have $\delta_F=p^d+1$ if all p^d+1 roots from (6.2) simultaneously satisfy the character conditions. However, this requires special alignments and appears rare in practice.

(3) The condition "q sufficiently large" in part (3) can be made explicit using the Hasse-Weil bound: we need $Q-2g\sqrt{Q}-1>(\text{number of forbidden places})$, where g is the genus of $\mathbb{K}(T,V,Y,X,U)$ computed via Theorem 2.1.

7 Value distribution and permutation properties

Having established that the functions under consideration often fail to be APN, we now investigate their permutation properties. The functions discussed can be analyzed under a single unifying framework based on their shared algebraic structure.

7.1 A general criterion for non-permutation $d\geq 2$

Each of the functions can be expressed in the general form $F(x)=(\eta(x)+u)x^d$, where $\eta(x)=x^{\frac{p^n-1}{2}}$ is the quadratic character. This common structure allows for a straightforward proof regarding their permutation properties.

Proposition 7.1 *Let $F(x)=(\eta(x)+u)x^d$ be a function on $\mathbb{F}_{p^n}$, where $u\in\mathbb{F}_{p^n}\setminus\{0,\pm 1\}$. The function F(x) is **not a permutation polynomial** if there exists an element $g\in\mathbb{F}_{p^n}^*\setminus\{1\}$ that satisfies two conditions simultaneously:*

(1) $g^d=1$ *(g is a d-th root of unity).*
(2) $\eta(g)=1$ *(g is a quadratic residue).*

Proof Assume such a g exists. For any $x \in \mathbb{F}_{p^n}^*$, we evaluate $F(gx)$:

$$\begin{aligned} F(gx) &= (\eta(gx) + u)(gx)^d \\ &= (\eta(g)\eta(x) + u)(g^d x^d) \\ &= (1 \cdot \eta(x) + u)(1 \cdot x^d) \quad \text{by conditions (1) and (2)} \\ &= (\eta(x) + u)x^d \\ &= F(x). \end{aligned}$$

Since there exists a $g \neq 1$ such that $F(gx) = F(x)$ for all $x \in \mathbb{F}_{p^n}^*$, the function is not injective and thus is not a permutation. □

Proposition 7.2 *Let $F(x) = (\eta(x) + u)x^2$ be a function on $\mathbb{F}_{p^n}$, where $u \in \mathbb{F}_{p^n} \setminus \{0, \pm 1\}$ and $p^n \equiv 3 \pmod 4$. Then F(x) is 2-to-1 if $(-1 + u)/(1 + u)$ is a square in $\mathbb{F}_{p^n}$, and it is a permutation otherwise.*

Proof First, note that the unique preimage of 0 is 0. Also, given $x \in \mathbb{F}_{p^n}^*$, there is no $y \in \mathbb{F}_{p^n}^*$ distinct from x with $\eta(x) = \eta(y)$ such that $F(x) = F(y)$. Indeed, from $F(x) = F(y)$ one gets $x^2 = y^2$, yielding $x = y$ or $x = -y$. The latter case is impossible since -1 is not a square in $\mathbb{F}_{p^n}$.

Let us investigate the existence of $y \in \mathbb{F}_{p^n}^*$ with $\eta(x) = -\eta(y)$ such that $F(x) = F(y)$. Without loss of generality, assume that $\eta(x) = 1$. In this case, $F(x) = F(y)$ yields $x^2 = \frac{-1+u}{1+u} y^2$. If $\frac{-1+u}{1+u}$ is not a square, no solutions arise from this case and $F(x)$ is a permutation. If $\frac{-1+u}{1+u}$ is a square, let $g \in \mathbb{F}_{p^n}$ be such that $g^2 = \frac{-1+u}{1+u}$. Thus $x = \pm gy$. Since -1 is a non-square, only one of these two solutions is admissible. Thus, in this case, $F(x)$ is 2-to-1. □

7.2 The *k*-to-1 mapping property

The preceding proof reveals more than a simple lack of injectivity; it characterizes the function's collision structure. The set of all elements satisfying the two conditions in the theorem forms a subgroup of $\mathbb{F}_{p^n}^*$, namely

$$G = \left\{ g \in \mathbb{F}_{p^n}^* \mid g^d = 1 \text{ and } \eta(g) = 1 \right\}.$$

The function $F(x)$ is constant on the cosets of this subgroup. The size of this subgroup, $k = |G|$, can be calculated as

$$k = \gcd\left(d, \frac{p^n - 1}{2}\right).$$

If $k > 1$, then $F(x)$ is a ***k*-to-1 mapping** from $\mathbb{F}_{p^n}^*$ onto its image (Table 1).

Table 1 Summary of non-permutation conditions and minimum nonzero fiber sizes for $F(x) = (\eta(x) + u)x^d$. Here $k = \gcd(d, \frac{p^n-1}{2})$ gives a lower bound on the number of preimages for each nonzero value in the image. The actual fiber sizes may be strictly larger for some values due to additional collisions

Function Family	Exponent d	Condition for Non-Permutation	Min. Fiber Size
$(\eta(x) + u)x^2$	2	$p^n \equiv 1 \pmod 4$	≥ 2
$(\eta(x) + u)x^3$	3	$p^n \equiv 1 \pmod 6$	≥ 3
$(\eta(x) + u)x^{p^k+1}$	$p^k + 1$	$\gcd(p^k + 1, \frac{p^n-1}{2}) > 1$	$\geq \gcd(p^k + 1, \frac{p^n-1}{2})$

- **For** $d = 2$: The condition for non-permutation requires $\gcd(2, (p^n - 1)/2) > 1$, which holds if and only if $p^n \equiv 1 \pmod 4$. In this case, every nonzero value in the image has at least 2 preimages.
- **For** $d = 3$: The condition for non-permutation requires $\gcd(3, (p^n - 1)/2) > 1$, which holds if and only if $p^n \equiv 1 \pmod 6$. In this case, every nonzero value in the image has at least 3 preimages.
- **For** $d = p^k + 1$: The function is not a permutation whenever $\gcd(p^k + 1, (p^n - 1)/2) > 1$. This condition holds in many cases, for instance when n is even. Every nonzero value in the image has at least $\gcd(p^k + 1, (p^n - 1)/2)$ preimages.

Remark 7.3 The argument presented establishes that $F(x) = (\eta(x) + u)x^d$ has the property that every nonzero value in its image has at least $k = \gcd(d, (p^n - 1)/2)$ preimages whenever $k > 1$. However, this is only a lower bound—some values may have strictly more than k preimages due to additional collisions beyond those forced by the group structure.

In the complementary case where $k = 1$, the group G is trivial, so this collision structure does not arise. For such parameters, the function could potentially be a permutation, though the argument does not determine this. A full characterization of the permutation property for cases where $\gcd(d, (p^n - 1)/2) = 1$ would require analyzing whether other types of collisions occur and remains an interesting open problem.

The computational data in the appendix suggests that for small fields, the minimum fiber size k is often achieved, but a complete theoretical characterization is lacking.

7.3 Further analysis of the value distribution

While the preceding analysis reveals the structural k-to-1 nature of these functions on $\mathbb{F}_{p^n}^*$, it does not determine the full value distribution or the maximum possible number of collisions. To investigate these quantitative properties, particularly for the family with $d = 2$, we turn to character sums.

The character sum technique we developed in Section 5 provides a computational approach to determining the number of preimages $N_F(c)$ exactly. Recall that for any function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$,

$$N_F(c) = \frac{1}{p^n} \sum_{x \in \mathbb{F}_{p^n}} \sum_{\alpha \in \mathbb{F}_{p^n}} \chi_1(\alpha(F(x) - c)) = 1 + \frac{1}{p^n} \sum_{\alpha \in \mathbb{F}_{p^n}^*} \sum_{x \in \mathbb{F}_{p^n}} \chi_1(\alpha(F(x) - c)).$$

The number of preimages $N_F(c)$ for the general function $F(x) = (\eta(x) + u)x^d$ can be expressed exactly using the character sum formula:

$$N_F(c) = 1 + \frac{1}{p^n} \sum_{\alpha \in \mathbb{F}_{p^n}^*} \chi_1(-\alpha c) \sum_{x \in \mathbb{F}_{p^n}} \chi_1\left(\alpha(\eta(x) + u)x^d\right).$$

The inner sum can be decomposed according to whether $\eta(x) = 1$ or $\eta(x) = -1$. This formulation makes the explicit computation of the value distribution tractable for moderate field sizes and connects the problem to well-known exponential sums.

Our computational experiments (see Appendix) for the specific case where $d = 2$, combined with its established 2-to-1 structure for $p^n \equiv 1 \pmod 4$ and further computations for $u \neq 0, \pm 1, \pm 3$, motivate the following conjecture regarding its maximum number of collisions.

Conjecture 7.4 *For $F(x) = x^{\frac{p^n+3}{2}} + ux^2$ (the case $d = 2$) with $u \in \mathbb{F}_{p^n} \setminus \{0, \pm 1, \pm 3\}$, $p^n \equiv 1 \pmod 4$, and p^n sufficiently large, we have*

$$\max_{c \in \mathbb{F}_{p^n}} N_F(c) \in \{3, 4\}.$$

Moreover, the precise value depends on subtle arithmetic properties of u relative to the quadratic character structure of $\mathbb{F}_{p^n}$.

This conjecture, if true, would provide a complete characterization of the worst-case value collision behavior for this specific family, complementing our results on differential uniformity. The transition from APN-ness (where $\max N_F(c) \leq 2$) to a state where the maximum multiplicity is 3 or 4 represents a controlled degradation of the function's injectivity properties as the field size grows.

8 Open problems and future work

Our work, using methods from algebraic geometry, disproves the conjecture by Budaghyan and Pal on the APN-ness of the family $F(x) = x^{(q+3)/2} + ux^2$ for large fields. Mesnager and Wu [11] independently disproved the same conjecture using a distinct methodology based on direct algebraic analysis and character sum estimates. The combined results from both papers solidify the conclusion that this construction is not a viable source for new infinite APN families, while also highlighting several key challenges that remain.

8.1 Problem A: Complete differential spectrum determination

The work of Mesnager and Wu [11] has advanced beyond APN-ness by determining the exact asymptotic differential uniformity of $F_{2,u}(x) = x^{(q+3)/2} + ux^2$. They show that for sufficiently large q, $\delta_{F_{2,u}} \in \{3, 4, 5\}$ depending on the parameters of u. For the special cases $u = \pm 1$, they achieved complete spectrum determination.

Question 8.1 *Can we determine the complete differential spectrum* $\{\Delta_F(a,b) : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$ *for arbitrary* $u \in \mathbb{F}_q$*?*

This requires understanding not just the maximum differential uniformity, but the precise distribution of values. Our case analysis in Section 3 ((3.2)) provides a framework, but determining which combinations of cases contribute for generic (a, b, u) remains open.

Question 8.2 *Can the geometric approach in Section 4 be refined to yield exact uniformity values, thereby providing a geometric explanation for the specific integers* $\{3, 4, 5\}$ *that appear as differential uniformities?*

The function field methods give asymptotic existence results via Hasse-Weil bounds, but extracting precise counts would require computing genera and rational place distributions more explicitly.

8.2 Problem B: Value distribution and k-to-1 characterization

Conjecture 7.4 suggests that $\max_c N_F(c) \in \{3, 4\}$ for the family $F(x) = x^{(q+3)/2} + ux^2$ when $q \equiv 1 \pmod 4$ is large and $u \notin \{0, \pm 1, \pm 3\}$.

Question 8.3 *Prove or disprove Conjecture 7.4. More generally, characterize the full value distribution* $\{N_F(c) : c \in \mathbb{F}_q\}$.

Understanding when exactly $N_F(c) = 3$ versus $N_F(c) = 4$ occurs would illuminate the subtle interplay between the quadratic character structure and the polynomial structure. The character sum framework in Section 6 provides computational tools, but a theoretical characterization is lacking.

Question 8.4 *For which parameters (q, u) is* $F(x) = x^{(q+3)/2} + ux^2$ *a k-to-1 mapping for some fixed k? Are there parameter families where F is exactly 3-to-1 or 4-to-1?*

8.3 Problem C: Closing the gap for small fields

Our geometric proof of the nonvalidity of Budaghyan-Pal conjecture guarantees non-APN-ness for $q \geq 2719$, while computational results show this holds for all $q > 125$. Similarly, results in [11] prove theorems for very large q (e.g., $q \geq 27535^2$).

Question 8.5 *Close the gap between the asymptotic threshold from Hasse-Weil bounds and the computationally verified threshold. Can refined genus calculations or improved bounds (e.g., Aubry-Perret) reduce the required field size? That may be useful for other problems where such a gap cannot be closed, computationally.*

For Theorem 3.2 in Section 4, the genus of $\mathbb{K}_5$ grows with the system complexity. Explicit genus computation using Theorem 2.1 part (4) could yield better constants.

8.4 Problem D: Beyond the patched monomial construction

The comprehensive analysis in our work (for exponents $d = 2, 3, p^k + 1$) and the independent results of Mesnager and Wu for $d = 2$ provide strong evidence that the "patched monomial" construction $F(x) = (\eta(x) + u)x^d$ is unlikely to yield infinite APN families.

Question 8.6 *Prove a general impossibility theorem: for which classes of exponents d can one show that $F(x) = (\eta(x) + u)x^d$ fails to be APN for sufficiently large q?*

Our methods apply when the differential equation can be analyzed via case splitting on $\eta(x)$ and $\eta(x + a)$. Identifying the structural properties of d that make this approach work would unify the results.

Question 8.7 *Can alternative constructions succeed? Specifically:*

(1) *Does $F(x) = (\eta(x) + u)L(x)$ for a suitable linearized polynomial L(x) yield infinite APN families?*
(2) *What about $F(x) = (\eta(x) + u_1)x^{d_1} + (\eta(x) + u_2)x^{d_2}$ with multiple terms?*
(3) *Can Dembowski-Ostrom polynomials of the form $F(x) = \sum_{i,j} c_{ij}x^{p^i+p^j}$ combined with character-dependent coefficients work?*

The function field approach in Section 4 could potentially extend to these generalizations, provided the resulting systems remain tractable.

8.5 Problem E: Differential uniformity in the $j = k$ case

From the proof of Theorem 6.1, when $\epsilon = 0$ (i.e., -1 is not a $(p^k - 1)$-power in $\mathbb{F}_{p^n}$), the analysis in Section 6 shows that Cases $D_{1,1}$ and $D_{-1,-1}$ contribute no solutions, while Cases $D_{1,-1}$ and $D_{-1,1}$ each contribute at most $p^d + 1$ solutions for $F(x) = x^{(p^n-1)/2+p^k+1} + ux^{p^k+1}$.

Question 8.8 *Under the condition $\epsilon = 0$, is it true that $\delta_F = p^d + 1$? Or can the differential uniformity be strictly smaller due to constraints from multiple (a, b) pairs?*

The bound comes from Case $D_{1,-1}$ or $D_{-1,1}$ contributing $p^d + 1$ solutions via [9, Theorem 8], but whether this maximum is always attained requires careful analysis of when the parameter $U \in \mathbb{F}_Q \setminus \mathbb{F}_{p^{2d}}$ can be chosen to satisfy all necessary conditions simultaneously.

The character sum formulas in Section 6 provide one approach, but for large fields, more sophisticated techniques (e.g., fast Fourier transforms over finite fields, or specialized algorithms for Weil sum evaluation) may be necessary.

Appendix

We now display computational data showing the differential spectrum and value distribution for various dimensions and parameters u. The notation a^b means that the uniformity a has frequency b. For each case, we also provide $\max_c N_F(c)$ (the maximum number of preimages of any value) and δ_F (the differential uniformity).

Function $F(x) = x^{\frac{p^n+3}{2}} + ux^2$

Remark 8.9 Via Magma [3] and SageMath, we found that, in addition to [4, Table 5], there are other interesting examples of best differential uniformity functions. For example, if $p = 3$, $n = 1$, $u = -1$, the function is PN with $\max_c N_F(c) = 2$; if $p = 3$, $n = 2$, $u = g, g^3, g^5, g^7$, the function is PN with $\max_c N_F(c) = 2$.

For $p = 5, n = 2$, with g a primitive root in $\mathbb{F}_{5^2}$, the possible differential uniformity values are 2, 3, 5, 7. The function is APN for u equal to g^3, g^9, g^{15}, g^{21}. Notably, $\max_c N_F(c) = 13$ for $u = g^{12}$, which is significantly larger than other cases. The complete data:

For higher dimensions: when $p = 5, n = 3$, possible DU values are 3, 4, 6, 7, 8; when $p = 5, n = 4$, possible DU values are 3, 4, 5, 6; when $p = 7, n = 2$, possible DU values are 2, 3, 4, 5, and the function is APN for u equal to $g^2, g^{12}, g^{14}, g^{26}, g^{36}, g^{38}$; when $p = 7, n = 3$, possible DU values are 3, 4, 5; when $p = 11, 13$ and $n = 2$, possible DU values are 3, 4, 5, 6.

Table 2 Properties of $F(x) = x^{\frac{p^n+3}{2}} + ux^2$ for $n = 1$

p	u : Differential Spectrum	$\max_c N_F(c)$	δ_F
5	$2 : \{0^4, 1^{12}, 2^4\}$	2	2
	$3 : \{0^4, 1^{12}, 2^4\}$	2	2
7	$2 : \{0^{12}, 1^{24}, 3^6\}$	1	3
	$3 : \{0^{12}, 1^{18}, 2^{12}\}$	2	2
	$4 : \{0^{12}, 1^{18}, 2^{12}\}$	2	2
	$5 : \{0^{12}, 1^{24}, 3^6\}$	1	3
11	$2 : \{0^{40}, 1^{30}, 2^{40}\}$	2	2
	$3 : \{0^{50}, 1^{20}, 2^{30}, 3^{10}\}$	1	3
	$4 : \{0^{30}, 1^{60}, 2^{10}, 3^{10}\}$	2	3
	$5 : \{0^{40}, 1^{50}, 3^{20}\}$	1	3
	$6 : \{0^{40}, 1^{50}, 3^{20}\}$	1	3
	$7 : \{0^{30}, 1^{60}, 2^{10}, 3^{10}\}$	2	3
	$8 : \{0^{50}, 1^{20}, 2^{30}, 3^{10}\}$	1	3
	$9 : \{0^{40}, 1^{30}, 2^{40}\}$	2	2
13	$2 : \{0^{48}, 1^{84}, 3^{24}\}$	2	3
	$3 : \{0^{60}, 1^{48}, 2^{36}, 3^{12}\}$	2	3
	$4 : \{0^{48}, 1^{72}, 2^{24}, 3^{12}\}$	2	3
	$5 : \{0^{24}, 1^{108}, 2^{24}\}$	2	2
	$6 : \{0^{60}, 1^{66}, 2^{12}, 3^{12}, 5^6\}$	4	5
	$7 : \{0^{60}, 1^{66}, 2^{12}, 3^{12}, 5^6\}$	4	5
	$8 : \{0^{24}, 1^{108}, 2^{24}\}$	2	2
	$9 : \{0^{48}, 1^{72}, 2^{24}, 3^{12}\}$	2	3
	$10 : \{0^{60}, 1^{48}, 2^{36}, 3^{12}\}$	2	3
	$11 : \{0^{48}, 1^{84}, 3^{24}\}$	2	3

Table 3 Properties of $F(x) = x^{\frac{p^n+3}{2}} + ux^2$ for $n = 1$ (continued)

p	u : Differential Spectrum	$\max_c N_F(c)$	δ_F
17	$2 : \{0^{64}, 1^{144}, 2^{64}\}$	2	2
	$3 : \{0^{96}, 1^{136}, 2^{16}, 4^{16}, 5^8\}$	4	5
	$4 : \{0^{96}, 1^{112}, 2^{32}, 3^{32}\}$	2	3
	$5 : \{0^{80}, 1^{144}, 2^{16}, 3^{32}\}$	2	3
	$6 : \{0^{112}, 1^{80}, 2^{48}, 3^{32}\}$	4	3
	$7 : \{0^{64}, 1^{144}, 2^{64}\}$	2	2
	$8 : \{0^{80}, 1^{112}, 2^{80}\}$	2	2
	$9 : \{0^{80}, 1^{112}, 2^{80}\}$	2	2
	$10 : \{0^{64}, 1^{144}, 2^{64}\}$	2	2
	$11 : \{0^{112}, 1^{80}, 2^{48}, 3^{32}\}$	4	3
	$12 : \{0^{80}, 1^{144}, 2^{16}, 3^{32}\}$	2	3
	$13 : \{0^{96}, 1^{112}, 2^{32}, 3^{32}\}$	2	3
	$14 : \{0^{96}, 1^{136}, 2^{16}, 4^{16}, 5^8\}$	4	5
	$15 : \{0^{64}, 1^{144}, 2^{64}\}$	2	2
19	$2 : \{0^{108}, 1^{180}, 2^{18}, 3^{18}, 4^{18}\}$	1	4
	$3 : \{0^{108}, 1^{144}, 2^{72}, 3^{18}\}$	1	3
	$4 : \{0^{108}, 1^{126}, 2^{108}\}$	1	2
	$5 : \{0^{108}, 1^{180}, 2^{18}, 3^{18}, 4^{18}\}$	2	4
	$6 : \{0^{90}, 1^{198}, 2^{18}, 3^{36}\}$	2	3
	$7 : \{0^{126}, 1^{126}, 2^{72}, 4^{18}\}$	1	4
	$8 : \{0^{126}, 1^{126}, 2^{72}, 4^{18}\}$	2	4
	$9 : \{0^{72}, 1^{198}, 2^{72}\}$	2	2
	$10 : \{0^{72}, 1^{198}, 2^{72}\}$	2	2
	$11 : \{0^{126}, 1^{126}, 2^{72}, 4^{18}\}$	2	4
	$12 : \{0^{126}, 1^{126}, 2^{72}, 4^{18}\}$	1	4
	$13 : \{0^{90}, 1^{198}, 2^{18}, 3^{36}\}$	2	3
	$14 : \{0^{108}, 1^{180}, 2^{18}, 3^{18}, 4^{18}\}$	2	4
	$15 : \{0^{108}, 1^{126}, 2^{108}\}$	1	2
	$16 : \{0^{108}, 1^{144}, 2^{72}, 3^{18}\}$	1	3
	$17 : \{0^{108}, 1^{180}, 2^{18}, 3^{18}, 4^{18}\}$	1	4

Table 4 $F(x) = x^{\frac{p^n+3}{2}} + ux^2$ for $p = 5, n = 2$

u	$\max_c N_F(c)$	δ_F	u	$\max_c N_F(c)$	δ_F
g^1	2	3	g^{13}	2	3
g^2	4	3	g^{14}	4	3
g^3	2	2	g^{15}	2	2
g^4	2	3	g^{16}	2	3
g^5	2	3	g^{17}	2	3
g^6	4	5	g^{18}	4	5
g^7	2	3	g^{19}	2	3
g^8	2	3	g^{20}	2	3
g^9	2	2	g^{21}	2	2
g^{10}	4	3	g^{22}	4	3
g^{11}	2	3	g^{23}	2	3
g^{12}	13	7			

Function $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$

For this function with $u \neq 0, \pm 1$, we observe the following behavior:

For $p = 7, n = 2$, the DU values are 4, 6; for $p = 7, n = 3$, the DU values are 3, 4, 5; for $p = 11, n = 2$, the DU values are 4, 5, 6, 8.

Table 5 Properties of $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$

p	n	u : Differential Spectrum	$\max_c N_F(c)$	Status
5	1	$2 : \{0^8, 1^4, 2^8\}$	2	APN
		$3 : \{0^8, 1^4, 2^8\}$	2	APN
		$4 : \{0^8, 1^4, 2^8\}$	3	APN
5	2	g^4, g^8, g^{16}, g^{20}	6	DU=9
		other u values	2	APN
5	3	2, 3	2	DU=8
7	1	2	3	DU=3
		3	3	APN
		4	3	APN
		5	3	DU=3
		6	4	DU=3
11	1	3, 8	2	APN
		other values	3	DU=3
13	1	2, 11	–	APN

Table 6 Properties of $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^j+1}$ for selected parameters

p	n	j	k	$\max_c N_F(c)$	δ_F
5	2	0	1	2–4	3
5	2	1	1	12	13
5	3	0	1	6	7
5	3	0	2	6	7
5	3	1	2	4	7
5	3	2	2	2	2
7	2	0	1	4	5

General case $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^j+1}$

For the general family with $0 \le j \le k < n$, we tested various parameter combinations:

Remark 8.10 The data supports Conjecture 7.4: for $F(x) = x^{\frac{p^n+3}{2}} + ux^2$ with $u \notin \{0, \pm 1, \pm 3\}$ and $p^n > 125$, we consistently observe $\max_c N_F(c) \in \{1, 2, 3, 4\}$, with values 3 and 4 appearing for larger primes when $\delta_F \ge 3$. The exceptional case $\max_c N_F(c) = 13$ at $p = 5, n = 2, u = g^{12}$ occurs in a small field and corresponds to high differential uniformity $\delta_F = 7$.

Acknowledgements The second-named author (PS) would like to thank the first-named author (DB) for the invitation at the Dipartimento di Matematica e Informatica at Università degli Studi di Perugia, Italy, and the great working conditions while this paper was being written. The first-named author (DB) thanks the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA–INdAM) which supported the research.

Author Contributions All authors contributed equally in the writing of the paper.

Funding Funding of DB was partially provided by Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA—INdAM).

Data Availability No datasets were generated or analysed during the current study.

Declarations

Ethics approval and consent to participate Not applicable.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

References

1. Aubry, Y., Perret, M.: A Weil theorem for singular curves. In: Arithmetic, geometry and coding theory, De Gruyter Proceedings in Mathematics 1–7 (1996)
2. Bartoli, D., Giulietti, M., Zini, G.: Complete $(k, 3)$-arcs from quartic curves. Des. Codes Cryptogr. **79**, 487–505 (2016)
3. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3–4), 235–265 (1997)

4. Budaghyan, L., Pal, M.: Arithmetization-oriented APN permutations. Des. Codes Cryptogr. (2024). https://doi.org/10.1007/s10623-024-01487-7
5. Fulton, W.: Algebraic curves. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, Advanced Book Classics (1989)
6. Hartshorne, R.: Algebraic geometry, Graduate Texts in Mathematics, no. 52, Springer-Verlag, New York-Heidelberg, (1977)
7. Hirschfeld, J.W.P.: Projective geometry over finite fields (2nd Ed.), Oxford Mathematical Monographs, (1998)
8. Hirschfeld, J.W.P., Korchmáros, G., Torres, F.: Algebraic curves over a finite field, Princeton University Press, (2013)
9. Kim, K.H., Choe, J., Mesnager, S.: Solving $X^{q+1} + X + a = 0$ over finite fields. Finite Fields Appl. **70**, 101797 (2021)
10. Lidl, R., Niederreiter, H.: Finite fields (Ed. 2), Encycl. Math. Appl., vol 20, Cambridge Univ. Press, Cambridge, (1997)
11. Mesnager, S., Wu, H.: The differential and boomerang properties of a class of binomials. IEEE Trans. Inf. Th. **71**(6), 4854–4871 (2025)
12. Mills, D.: On the evaluation of weil sums of Dembowski-Ostrom polynomials. J. Number Theory **92**(1), 87–98 (2002)
13. Mollin, R.A., Small, C.: On permutation polynomials over finite fields. Int. J. Math. Math. Sci. **10**(3), 535–543 (1987)
14. Stănică, P.: Using double Weil sums in finding the c-Boomerang Connectivity Table for monomial functions on finite fields. Appl. Algebra Eng. Commun. Comput. **34**, 581–602 (2023)
15. Stichtenoth, H.: H Algebraic function fields and codes, Volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009)
16. Zheng, Y., Wang, Q., Wei, W.: On inverses of permutation polynomials of small degree over finite fields. IEEE Trans. Inf. Theory **66**(2), 914–922 (2020)