APN functions in odd characteristic and the disproof of a conjecture

Daniele Bartoli
Department of Mathematics and Computer Science
University of Perugia
Perugia, Italy
daniele.bartoli@unipg.it

Pantelimon Stănică
Applied Mathematics Department
Naval Postgraduate School
Monterey, CA 93943, USA
pstanica@nps.edu

Keywords: Finite fields, varieties, irreducible components, APN functions

Abstract

In this paper, we disprove a conjecture by Pal and Budaghyan (DCC, 2024) regarding the existence of a family of APN permutations, by showing that, in reality, there are no APN functions of that form beyond those already listed in the known table. Moreover, we explore other related families of functions as potential APN candidates. However, we demonstrate that they are not suitable for APNness when the underlying field is large, despite being APN in smaller settings.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with $q = p^k$ elements, where k is a positive integer, and $\mathbb{F}_q^*$ be the multiplicative group of nonzero elements of $\mathbb{F}_q$ and denote by $\mathbb{F}_q[X]$ the polynomial ring in the indeterminate X over $\mathbb{F}_q$. 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 $a \in \mathbb{F}_q$. 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 $D_a f(x) = f(x+a) - f(x)$, 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 $\Delta_F(a, b) = \#\{x \in \mathbb{F}_{p^n} : F(x+a) - F(x) = b\}$ (cardinality). 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 (does not exist for $p = 2$), or *planar* function. If $m = n$ and $\delta = 2$, then F is called an *almost perfect nonlinear* (*APN*) function.

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

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 [5]. 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 1. [5, Cor. 3.7.4] Let $\mathbb{F}$ be an algebraic function field of constant field $\mathbb{L}$ (char. p) containing a primitive n-th root of unity ($n > 1$ and $\gcd(n, p) = 1$). Let $u \in \mathbb{F}$ be such that there is a place Q of $\mathbb{F}$ with $\gcd(v_Q(u), n) = 1$ (see [5, Definition 1.1.2] for the definition of the discrete valuation v_Q). Let $\mathbb{F}' = \mathbb{F}(y)$ with $y^n = u$. Then: $\Phi(T) = T^n - u$ 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; $e(P'|P) = \frac{n}{r_P}$, where $r_P := GCD(n, v_P(u)) > 0$; $\mathbb{L}$ is the constant field of $\mathbb{F}'$; If g' (g) is the genus of $\mathbb{F}'$ ($\mathbb{F}$), 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 1 is said to be a Kummer extension of $\mathbb{F}$. 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 $\mathcal{C}$ can be 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 [5, 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. We need the next two results.

Theorem 2. (Hasse-Weil bound, [5, 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 $|N_q - (q+1)| \leq 2g\sqrt{q}$.

Lemma 3. [1, 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 the class of functions of [2].

Theorem 4. 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 at most 4.

Proof. (Sketch) For $a \in \mathbb{F}_{p^n}^*, b \in \mathbb{F}_{p^n}$ we investigate 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 $t_a = \eta(x+a), t_x = \eta(x)$, and noting that $\frac{p^n+3}{2} = \frac{p^n-1}{2} + 2$, the equation above becomes $(x+a)^2(t_a+u) - x^2(t_x+u) = b$. We distinguish four cases, go through the possibilities and find that they collapse to only four possibilities (under our assumptions), which do occur for some $0 \neq a, b$. □

Combining some of the cases, depending upon the signs of the quadratic characters of $\eta(x), \eta(x+a)$ we want to show that the differential equation has at least three solutions and thus the function F is not APN. We fix $u \in \mathbb{F}_q \setminus \{0, \pm 1\}$. One can show the following.

Proposition 5. *There exist x_1, with $\eta(x_1) = \eta(x_1 + a) = 1$, and x_2, x_3 with $\eta(x_i) = -1, \eta(x_i + a) = 1, i = 2, 3$, if there exist $a, b, X, Y, Z, U, V, W, T \in \mathbb{F}_q$, $aZ \neq 0$, satisfying (we go through some equivalences to arrive at this system):*

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

and such that the three roots of the differential equation, namely

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

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

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

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

are also solutions of System (1).

Theorem 6. 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

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

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

Proof. (Sketch) We apply Theorem 1 and Lemma 3 to derive the result. □

We now show that the conjecture of [2] is false, and not only is there no infinite family of APN functions, but in fact there are no APN functions besides those listed in [2, Table 5].

Theorem 7. 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. (Sketch) The case $u = 3$, required separate algebraic number theory treatment. For $u \neq 0, \pm 1, 3$, we use function field theory to show this result for $q \geq 2719$, and Magma to cover $125 < q < 2719$ (that is, outside [2, Table 5], which lists $q = 5^3$ as the highest cardinality when the function is APN, for some values of u). □

Remark 8. Via Magma, we checked that, in addition to [2, Table 5], there are other interesting examples of best differential uniformity functions, for small dimensions. For example, if $p = 3$, $n = 1$, $u = -1$, or, if $p = 3$, $n = 2$, $u = g, g^3, g^5, g^7$, the function is PN.

There are other related classes of functions in the same vein that one can consider. However, they do not exhibit favorable behavior.

For example, if $F(x) = x^{\frac{p^n-1}{2}+3} + ux^3$ on $\mathbb{F}_{p^n}$ with $p > 3$, computationally, we observed that, for some u, 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.

However we can show the next result.

Theorem 9. Let $q \equiv 1 \pmod 3$. Choose a nonsquare $\xi \in \mathbb{F}_q$ and 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. The proof is involved and uses Cardano's formulas. Their expressions is slightly easier to analyze if $q \equiv 1 \pmod 3$. □

One can also generalize the class of [2] to allow "any" quadratic exponent not only 2, that is, $F(x) = x^{\frac{p^n-1}{2}+p^k+1} + ux^{p^j+1}$ $0 \leq j \leq k < n$, on $\mathbb{F}_{p^n}$. Unfortunately, once again, we do not obtain an infinite class. However, for small dimensions, we do observe good differential uniformity. For computational purposes, we express the entries of the DDT in terms of Weil sums.

Theorem 10. 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 Difference Distribution Table entries at $(a, b) \in \mathbb{F}_{p^n}^* \times \mathbb{F}_{p^n}$ are given by

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

Corollary 11. For the function in our previous theorem under the condition $k = j$, if $\mu = -1$, $\alpha \neq 0$, and $\frac{n}{\gcd(n,2k)}$ is odd, then $\mathcal{N}_{a,\alpha(u+\epsilon)a^{p^k+1}} = p^n$, and therefore, the function cannot be APN.

When $j = k$ in the general class of the prior theorem, we can show a stronger result.

Theorem 12. 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, $(x+a)^{\frac{p^n-1}{2}+p^k+1} + u(x+a)^{p^k+1} - x^{\frac{p^n-1}{2}+p^k+1} - ux^{p^k+1} = b$.

Using similar techniques as in the previous theorems, we apply Theorem 1 and Lemma 3 to derive the result. □

References

[1] D. Bartoli, M. Giulietti, G. Zini, Complete $(k, 3)$-arcs from quartic curves, Des. Codes Cryptogr. **79** (2016), 487–505.

[2] L. Budaghyan, M. Pal, Arithmetization-oriented APN permutations. Des. Codes Cryptogr. (2024), https://doi.org/10.1007/s10623-024-01487-7.

[3] J.W.P. Hirschfeld, Projective Geometry over finite fields (2nd Ed.), Oxford Mathematical Monographs, 1998.

[4] K.H. Kim, J. Choe, S. Mesnager, *Solving* $X^{q+1} + X + a = 0$ *over finite fields*, Finite Fields Appl. 70, 101797 (2021).

[5] H. Stichtenoth, H Algebraic function fields and codes, Volume 254 of Graduate Texts in Mathematics, 2nd edn. Springer, Berlin (2009).