Partially APN functions with APN-like polynomial representations

Lilya Budaghyan[1], Nikolay Kaleyski[1],
Constanza Riera[3], Pantelimon Stănică[4]

[1] Department of Informatics, University of Bergen
Postboks 7803, N-5020, Bergen, Norway;
{Lilya.Budaghyan, Nikolay.Kaleyski}@uib.no
[3]Department of Computer science, Electrical engineering and Mathematical sciences,
Western Norway University of Applied Sciences
5020 Bergen, Norway; csr@hvl.no
[4] Department of Applied Mathematics, Naval Postgraduate School
Monterey, CA 93943-5212, U.S.A.; pstanica@nps.edu

February 7, 2020

Abstract

In this paper we investigate several families of monomial functions with APN-like exponents that are not APN, but are partially 0-APN for infinitely many extensions of the binary field $\mathbb{F}_2$. We also investigate the differential uniformity of some binomial partial APN functions. Furthermore, the partial APN-ness for some classes of multinomial functions is investigated. We show also that the size of the pAPN spectrum is preserved under CCZ-equivalence.

Keywords: Boolean function, almost perfect nonlinear (APN), partial APN (pAPN), CCZ-equivalence **2010 MSC:** 94A60, 94C10, 06B30

1 Introduction

The objects of this study are functions over the field with 2^n elements and some of their differential properties. For more on these objects the reader can consult [3, 7, 8, 11]. We will introduce here only some needed notions.

Let $\mathbb{F}_{2^n}$ be the finite field with 2^n elements for some positive integer n. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables and denote the set of all such functions by $\mathcal{B}_n$. For a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard* *transform* to be the integer valued function

$$\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)},$$

where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

Given a Boolean function f, the derivative of f in direction $a \in \mathbb{F}_{2^n}$ is the Boolean function D_aF defined by $D_af(x) = f(x+a) + f(x)$.

A vectorial Boolean function (often called an (n,m)-function) is a map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ for some positive integers m and n. When $m = n$, it can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (up to some linear equivalence using the identification of the finite field with the vector space), namely

$$F(x) = \sum_{i=0}^{2^n-1} a_i x^i, \ a_i \in \mathbb{F}_{2^n}.$$

Any positive integer $k \leq 2^n - 1$ can be represented as a sum $k = \sum_{i=0}^{n-1} k_i \cdot 2^i$, with $k_i \in \{0,1\}$. The *2-weight* of k is then $wt(k) = \sum_{i=0}^{n-1} k_i$, i.e. the number of powers of two that add up to k. The *algebraic degree* of the function is then the largest 2-weight of an exponent i with $a_i \neq 0$.

In general, for an (n,m)-function F, we define the Walsh transform $W_F(a,b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

$$W_F(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^m(bF(x))+\mathrm{Tr}_1^n(ax)}.$$

For an (n,n)-function F, and $a,b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a,b) = |\{x \in \mathbb{F}_{2^n} \mid F(x+a) + F(x) = b\}|$. We call the quantity $\Delta_F = \max\{\Delta_F(a,b) \ : \ a,b \in \mathbb{F}_{2^n}, a \neq 0\}$ the *differential uniformity* of F. If $\Delta_F \leq \delta$, then we say that F is *differentially δ-uniform.* If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function. There are several equivalent characterizations of APN-ness, and we state some below.

Lemma 1.1. *([8, 10, 16]) Let F be an (n,n)-function.*

(i) The following inequality is always true:

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) \geq 2^{3n+1}(3 \cdot 2^{n-1} - 1),$$

with equality if and only if F is APN.

(ii) If, in addition, F is APN and satisfies $F(0) = 0$, then

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1).$$

(*iii*) *(Rodier Condition) F is APN if and only if all the points x, y, z satisfying*

$$F(x) + F(y) + F(z) + F(x + y + z) = 0,$$

fulfill $(x + y)(x + z)(y + z) = 0$.

We introduced in [6] a notion of partial APN-ness in our attempt to resolve the open problem of the highest possible algebraic degree of an APN function [5].

Definition 1.2. *For a fixed $x_0 \in \mathbb{F}_{2^n}$, we call an (n, n)-function a (*partial*) x_0-*APN function *(which we typically refer to as simply x_0-APN, partially APN or pAPN for short) if all points, x, y, satisfying*

$$F(x_0) + F(x) + F(y) + F(x_0 + x + y) = 0 \tag{1}$$

belong to the curve

$$(x_0 + x)(x_0 + y)(x + y) = 0. \tag{2}$$

We refer to the set of points x_0 for which F is x_0-APN as the pAPN spectrum *of F.*

Certainly, a function is APN if and only if it is x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$. We refer to equation (1) as the *Rodier equation*.

An alternative way to express the fact that a given function F is x_0-APN is to say that, for any $a \neq 0$, the equation $F(x + a) + F(x) = F(x_0 + a) + F(x_0)$ has only two solutions x, namely x_0 and $x_0 + a$.

The remainder of the paper is organized as follows. In the next section, we show that the size of the pAPN spectrum is preserved under CCZ-equivalence. Next, in Section 3, we theoretically and experimentally investigate the partial APN-ness of monomial functions. We consider monomial functions which are known to be APN under certain conditions, and find conditions under which they are partially APN. In Section 4, we show that the binomial $F(x) = x^{2^n-1} + x^{2^n-2}$ over $\mathbb{F}_{2^n}$ is 1-APN but not 0-APN for $n \geq 3$. In Section 5 we derive some conditions under which a polynomial of the form $F(x) = x(Ax^2+Bx^q+Cx^{2q})+x^2(Dx^q+Ex^{2q})+Gx^{3q}$ for $q = 2^k, 2^k+1$ with $1 \leq k \leq n-1$ is (not) partially APN (this class of polynomials was suggested by Dillon as containing potential APN or differentially 4-uniform functions). Since every APN function is 0-APN as well, some of the results from Sections 3, 4 and 5 imply non-existence results for APN functions.

2 The size of the pAPN spectrum is preserved under CCZ-equivalence

We first recall that two functions $F, G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ are *CCZ-equivalent* [9] if there exists an affine permutation $\mathcal{A}$ on $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ such that $\{(x, G(x)), x \in \mathbb{F}_{2^n}\} = \mathcal{A}(\{(x, F(x)), x \in \mathbb{F}_{2^n}\})$. As in [9], we use the identification of the elements in $\mathbb{F}_{2^n}$ with the elements in $\mathbb{F}_2^n$, and denote by x both an element in $\mathbb{F}_{2^n}$ and the corresponding element in $\mathbb{F}_2^n$.

Theorem 2.1. *The size of the pAPN spectrum is preserved under CCZ-equivalence. More precisely, if F and G are two CCZ-equivalent (n,n)-functions and $\mathcal{A}$ is the corresponding CCZ-isomorphism, and denoting the respective pAPN spectra of F, G by S_F, S_G, if $x_0 \in S_F$, and $(\tilde{x}_0, G(\tilde{x}_0)) = \mathcal{A}(x_0, F(x_0))$, we have that $\tilde{x}_0 \in S_G$.*

Proof. We first decompose the affine permutation as an affine block-matrix, $\mathcal{A}\mathbf{u} = \begin{pmatrix} \mathcal{A}_{11} & \mathcal{A}_{12} \\ \mathcal{A}_{21} & \mathcal{A}_{22} \end{pmatrix} \mathbf{u} + \begin{pmatrix} c \\ d \end{pmatrix}$, for an input vector $\mathbf{u}$, where $\mathcal{A}_{11}, \mathcal{A}_{21}, \mathcal{A}_{12}, \mathcal{A}_{22}$ are $n \times n$ matrices with entries in $\mathbb{F}_2$, and $\begin{pmatrix} c \\ d \end{pmatrix}$ is a column vector in $\mathbb{F}_{2^{2n}}$.

We assume that F is x_0-APN, and we want to show that G is $\tilde{x}_0$-APN, where $\tilde{x}_0 = \mathcal{A}_{11}x_0 + \mathcal{A}_{12}F(x_0) + c$. For that, we consider the Rodier equation of G at $\tilde{x}_0$, namely

$$G(\tilde{x}_0) + G(\tilde{x}) + G(\tilde{y}) + G(\tilde{x}_0 + \tilde{x} + \tilde{y}) = 0. \tag{3}$$

To simplify notation, we let $\tilde{z} = \tilde{x}_0 + \tilde{x} + \tilde{y}$. We know that there exist x_0, x, y, z such that

$$\begin{aligned}
&\tilde{x}_0 = \mathcal{A}_{11}x_0 + \mathcal{A}_{12}F(x_0) + c, \quad \tilde{x} = \mathcal{A}_{11}x + \mathcal{A}_{12}F(x) + c, \\
&\tilde{y} = \mathcal{A}_{11}y + \mathcal{A}_{12}F(y) + c, \quad \tilde{z} = \mathcal{A}_{11}z + \mathcal{A}_{12}F(z) + c, \\
&G(\tilde{x}_0) = \mathcal{A}_{21}x_0 + \mathcal{A}_{22}F(x_0) + d, \quad G(\tilde{x}) = \mathcal{A}_{21}x + \mathcal{A}_{22}F(x) + d, \\
&G(\tilde{y}) = \mathcal{A}_{21}y + \mathcal{A}_{22}F(y) + d, \quad G(\tilde{z}) = \mathcal{A}_{21}z + \mathcal{A}_{22}F(z) + d.
\end{aligned} \tag{4}$$

Observe that if $\tilde{x}_0 + \tilde{x} + \tilde{y} + \tilde{z} = 0$, then

$$\mathcal{A}_{12}\left(F(x_0) + F(x) + F(y) + F(z)\right) = \mathcal{A}_{11}\left(x_0 + x + y + z\right).$$

Similarly, the Rodier equation (3) for G at $\tilde{x}_0$ becomes

$$\mathcal{A}_{22}\left(F(x_0) + F(x) + F(y) + F(z)\right) = \mathcal{A}_{21}\left(x_0 + x + y + z\right).$$

We can write the previous identities in matrix form, namely

$$\mathcal{A}\left(\begin{pmatrix} x_0 \\ F(x_0) \end{pmatrix} + \begin{pmatrix} x \\ F(x) \end{pmatrix} + \begin{pmatrix} y \\ F(y) \end{pmatrix} + \begin{pmatrix} z \\ F(z) \end{pmatrix}\right) = 0,$$

to which we can apply $\mathcal{A}^{-1}$, obtaining

$$x_0 + x + y + z = 0 \text{ and } F(x_0) + F(x) + F(y) + F(z) = 0. \tag{5}$$

Now, since $z = x_0 + x + y$ and F is x_0-APN, then equation (5) has only the trivial solutions on $(x_0 + x)(x_0 + y)(x + y) = 0$. Therefore, $(\tilde{x}_0 + \tilde{x})(\tilde{x}_0 + \tilde{y})(\tilde{x} + \tilde{y}) = 0$, and the result is shown. $\square$

3 Partial x_0-APN monomials

In [6], a list of exponents i for which x^i is 0-APN but not APN over $\mathbb{F}_{2^n}$ was computed. This list is given as Table 1 in this paper (exponents are taken up to cyclotomic cosets). We observe that the function x^{21} appears for various dimensions, which raises the natural question of whether this is merely a coincidence or is the consequence of a more general rule. As our first result, we show that the latter is true.

n	Exponents i	Δ_F
1-5	-	-
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7,21,35,61,63,83,91,111,117,119,175	6
	41,187	8
	45,125	4
10	15, 27, 45, 75, 111, 117, 147, 189, 207, 255	6
	21, 69, 87, 237, 375	4
	51	8
	93	92
	105, 351	10
	231, 363, 495	42
	447	12
11	79, 109, 183, 251, 367, 463, 695, 703	4
	7, 11, 15, 21, 29, 31, 37, 47, 49, 51, 53, 55, 67, 71, 73, 75, 81, 83, 85, 99, 101, 103, 111 113, 121, 125, 127, 137, 139, 149, 153, 155, 157, 159, 167, 171, 173, 179, 181, 185, 187, 189, 191, 201, 203, 205, 213, 215, 217, 219, 221, 223, 229, 247, 255, 293, 295, 301, 307, 309, 311, 317, 319, 331, 333, 335, 339, 341, 343, 347, 351, 359, 371, 373, 375, 379, 381, 383, 423, 427, 443, 469, 471, 475, 477, 479, 491, 493, 495, 507, 511, 687, 727, 731, 735, 751, 763, 767, 879, 887, 959, 991	6
	19, 25, 27, 39, 41, 45, 61, 77, 87, 91, 105, 119, 123, 141, 147, 163, 165, 175, 199, 211, 233, 235, 237, 239, 349, 363, 415, 429, 431, 439, 501, 503, 699, 895	8
	59, 93, 169, 243, 303, 509	10
	245, 447	16
	23, 69, 115, 207, 253, 299, 437, 759	22
	89, 445	88

Table 1: Power functions $F(x) = x^i$ over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 10$ that are 0-APN but not APN

Proposition 3.1. *The function $F(x) = x^{21}$ is 0-APN if and only if n is not a multiple of 6.*

Proof. Let $F(x) = x^{21}$, and $x_0 = 0$. Then the conditions expressed by (1) and (2) state that the equality

$$x^{21} + y^{21} + (x + y)^{21} = 0 \tag{6}$$

implies

$$xy(x+y)=0.$$

Assuming $y \neq 0$ (since otherwise the condition $(x_0+x)(x_0+y)(x+y)=0$ is already satisfied) and dividing both sides of (6) by y^{21}, we get

$$a^{21}+(a+1)^{21}+1=0$$

where $a = x/y$. Assume further that $x \neq 0$, hence $a \neq 0$; this is then equivalent to

$$a^{19}+a^{16}+a^{15}+a^4+a^3+1=0,$$

which can be written as

$$(a+1)(a^6+a^3+1)(a^6+a^4+a^3+a+1)(a^6+a^5+a^3+a^2+1)=0. \tag{7}$$

Note that $F(x)=x^{21}$ is 0-APN if and only if $a=1$ is the only root of the polynomial on the left-hand side of (7).

It can be easily verified that each of the three polynomials of degree six is irreducible over $\mathbb{F}_2$. We now use [15, Theorem 3.46], which states that if a degree ℓ polynomial f is irreducible over $\mathbb{F}_q$ and $n \in \mathbb{N}$, then f factors into d irreducible polynomials in $\mathbb{F}_{q^n}[x]$ of the same degree ℓ/d, where $d = gcd(\ell, n)$. Therefore, the polynomial from (7) has roots other than 1 if and only if the dimension n of $\mathbb{F}_{2^n}$ is a multiple of six. $\square$

The experimentally computed differential properties of x^{21} for dimensions $n \leq 15$ are given in Table 2. The differential spectrum is the multiset $\{\Delta_F(a,b) : a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}\}$, with the multiplicity of a given value in this multiset given as a superscript after the value; e.g. the differential spectrum of x^{21} for $n=2$ contains the value 0 six times and the value 2 six times.

Dimension	Differential uniformity	Differential spectrum
1	2	$0^{1}, 2^{1}$
2	2	$0^{6}, 2^{6}$
3	6	$0^{42}, 2^{7}, 6^{7}$
4	2	$0^{120}, 2^{120}$
5	2	$0^{496} 2^{496}$
6	20	$0^{3780}, 12^{126}, 20^{126}$
7	6	$0^{9906}, 2^{5461}, 6^{889}$
8	4	$0^{38760}, 2^{20400}, 4^{6120}$
9	6	$0^{159432}, 2^{78694}, 4^{18396}, 6^{5110}$
10	4	$0^{585156}, 2^{401016}, 4^{61380}$
11	6	$0^{2523951}, 2^{1285516}, 4^{337755}, 6^{45034}$
12	20	$0^{9541350}, 2^{6183450}, 4^{1031940}, 14^{8190}, 20^{8190}$
13	6	$0^{41323595}, 2^{19175131}, 4^{5430633}, 6^{1171313}$
14	8	$0^{163338510}, 2^{80538828}, 4^{20642580}, 6^{3211068}, 8^{688086}$
15	8	$0^{649474707}, 2^{327866602}, 4^{82081335}, 6^{12320392}, 8^{1966020}$

Table 2: Differential uniformity and differential spectrum of x^{21} over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 15$

The approach described above can easily be generalized to any power function $F(x) = x^\ell$: the polynomial $x^\ell + 1 + (x+1)^\ell$ can be expressed as the product $p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ of powers of $\mathbb{F}_2$-irreducible polynomials $p_1, p_2, \dots, p_k$. If at least one of these polynomials has degree at least 2, then F is 0-APN over infinitely many fields $\mathbb{F}_{2^n}$, and is not 0-APN over infinitely many fields. More precisely, F is not 0-APN over $\mathbb{F}_{2^n}$ if n is a multiple of the degree of some p_i with $\deg(p_i) \geq 2$ (since this polynomial will split into a product of linear terms by [15, Theorem 3.46]), and is 0-APN if n is not divisible by the least common multiple of all of those degrees.

We can also try to characterize those power functions $F(x) = x^\ell$ which are 0-APN over any finite field, regardless of its dimension. By the above discussion, the polynomial $x^\ell + 1 + (x+1)^\ell$ in this case can only have two irreducible factors, viz. x and $(x+1)$. Suppose we have the decomposition

$$x^\ell + 1 + (x+1)^\ell = x^\alpha (x+1)^\beta.$$

Let $k = \deg(x^l + (x+1)^l + 1)$, i.e. k is the second largest exponent in $(x+1)^l$ after l. Thus,

$$x^k + \dots + x^{\ell - k} = x^{\alpha+\beta} + \dots + x^\alpha$$

so that we get $k = \alpha + \beta$ and $\ell - k = \alpha$, which implies $\ell = 2\alpha + \beta$.

Theorem 3.2. *Suppose $x^\ell + 1 + (x+1)^\ell$ can be written as*

$$x^\ell + 1 + (x+1)^\ell = x^\alpha (x+1)^\beta,$$

for some $\alpha, \beta \in \mathbb{N}$. Then $\alpha = \beta = \ell/3$, and $\ell = 3 \cdot 2^k$ for some $k > 0$. Furthermore, $F(x) = x^\ell$ with $\ell = 3 \cdot 2^k$ are the only power functions which are 0-APN over any finite binary field. All other power functions are 0-APN and not 0-APN over infinitely many finite binary fields.

Proof. Let $f(x)$ be the polynomial $x^\ell + 1 + (x+1)^\ell$. Then

$$x^\alpha (x+1)^\beta + x^\beta (x+1)^\alpha = f(x) + f(x+1) = 0$$

for any $x \in \mathbb{F}_{2^n}$. Suppose $\alpha \geq \beta$ and $x \notin \{0, 1\}$. Dividing both sides of the above equation by $x^\beta (x+1)^\beta$, we obtain

$$\frac{x^\alpha (x+1)^\beta + x^\beta (x+1)^\alpha}{x^\beta (x+1)^\beta} = x^{\alpha - \beta} + (x+1)^{\alpha - \beta} = 0$$

for all $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$. Therefore, if $\alpha - \beta \neq 0$, the polynomial $x^{\alpha-\beta} + (x+1)^{\alpha-\beta}$ has more roots than its degree, which is impossible. So $\alpha = \beta$, and hence $x^{\alpha-\beta} + (x+1)^{\alpha-\beta}$ is the null polynomial. Thus we have

$$x^\ell + 1 + (x+1)^\ell = (x(x+1))^\alpha.$$

We now prove that $x^\ell + 1 + (x+1)^\ell$ can be written in the form $(x(x+1))^\alpha$ if and only if $\ell = 3 \cdot 2^k$ for some $k \in \mathbb{N}$. First, observe that we can restrict ourselves to the case of ℓ odd, since if we have $\ell = 2\ell'$, then

$$(x(x+1))^\alpha = x^\ell + 1 + (x+1)^\ell = (x^{l'} + 1 + (x+1)^{l'})^2$$

implies $x^{\ell'} + 1 + (x+1)^{\ell'} = (x(x+1))^{\alpha/2}$. Thus, let $\ell = 2m+1$ for $m \in \mathbb{N}$. Note that the binomial coefficients $\binom{2m+1}{1} = \binom{2m+1}{2m} = 2m+1$ are always odd, so that x^{2m} is the term with largest exponent and x is the term with smallest exponent in $x^\ell + 1 + (x+1)^\ell$. Suppose $\alpha > 1$. Then the term with smallest exponent in $(x(x+1))^\alpha$ is x^α which contradicts x being the term with smallest exponent. Thus $\alpha = 1$, and $x^\ell + 1 + (x+1)^\ell = x(x+1)$. It is now easy to see that this implies $\ell = 3$. Hence, the exponents ℓ for which $x^\ell + 1 + (x+1)^\ell$ is of the form $(x(x+1))^\alpha$ are precisely those of the form $\ell = 3 \cdot 2^k$, and $\alpha = 2^k$. Finally, from the above discussion, we have that the exponents $\ell = 3 \cdot 2^k$ are precisely those for which x^ℓ is 0-APN over all finite fields $\mathbb{F}_{2^n}$, regardless of the dimension n. □

Remark 3.3. *The same approach can be used for a polynomial function F as well, however it is not possible to restrict the choice of (x, y) to pairs of the type $(x, 1)$ in general so that we would have to factorize $F(x) + F(y) + F(x+y)$ for all possible values of y in order to obtain a necessary and sufficient condition for F to be 0-APN. Selecting some concrete y, e.g. $y = 1$, would however allow us to obtain a necessary condition for the 0-APN-ness of F.*

It is also interesting whether a characterization of 1-APN-ness as the one discussed in this section can be obtained for e.g. $F(x) = x^{21}$. In this case, we consider the equation $x^{21} + y^{21} + (x+y+1)^{21} + 1 = 0$ which can be written as

$$\left(\frac{x}{y+1}\right)^{20} + \left(\frac{x}{y+1}\right)^{17} + \left(\frac{x}{y+1}\right)^{16} + \left(\frac{x}{y+1}\right)^{5} + \left(\frac{x}{y+1}\right)^{4}$$
$$+ \left(\frac{x}{y+1}\right) + \frac{y}{(y+1)^{17}} + \frac{y^4}{(y+1)^5} + \frac{y^{16}}{(y+1)^{20}} = 0.$$

This seems more difficult to handle than the 0-APN-ness by this method, however.

We showed in [6] that the Gold function $f_1(x) = x^{2^t+1}$ is 0-APN if and only if $\gcd(n,t) = 1$, which is known to be also equivalent to f_1 being APN. One would wonder (as we suggested in [6] for monomial functions) if perhaps under $\gcd(n,t) \neq 1$, the Gold function is 1-APN. We shall see below that in reality, the Gold function is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$, under $\gcd(n,t) = d \neq 1$. Note that the derivatives of the Gold functions are known to be 2^d-to-1 maps, so that such a function is either APN if $d = 1$, or not x_0-APN for any x_0 if $d > 1$. We now state and prove our main theorem in this section.

Theorem 3.4. *The following are true:*

(*i*) *Let $f_1(x) = x^{2^t+1}$ be the Gold function on $\mathbb{F}_{2^n}$ (known to be APN for $\gcd(t,n) = 1$). If $\gcd(n,t) = d > 1$, then f_1 is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$.*

(*ii*) *Let* $f_2(x) = x^{2^r-2^t+1}$, $r > s$, *be the generalization of the Kasami function* $x \mapsto x^{2^{2t}-2^t+1}$ *on* $\mathbb{F}_{2^n}$ *(known to be APN for* $\gcd(t,n) = 1$*). Then,* f_2 *is* 0*-APN if and only if* $\gcd(t,n) = \gcd(r-t,n) = d = 1$*. Moreover, if* $\gcd(t, r-t, n) > 1$*, then* f_2 *is not* x_0*-APN for any* $x_0 \neq 0$*.*

(*iii*) *Let* $f_3(x) = x^{2^r+2^t-1}$, $r > t$, *be the generalization of the Niho function* $x \mapsto x^{2^{2t}+2^t-1}$ *on* $\mathbb{F}_{2^n}$ *(known to be APN for* $n = 2r+1$, $2t = r$*; or,* $n = 2t+1$ *and* $2r = 3t+1$*). Then,* f_3 *is* 0*-APN if and only if* $\gcd(r,n) = \gcd(t,n) = 1$*. Note that, for* $t = 2$*, this includes* $f(x) = x^{2^r+3}$*, the Welch function (known to be APN for* $n = 2r+1$*). In this case,* f *is* 0*-APN if and only if* n *is odd and* $\gcd(r,n) = 1$*. If* $t = 1$*, this case includes the Gold function* f_1 *with* $x_0 = 0$*.*

(*iv*) *Let* $f_4(x) = x^{2^{2t}+2^t+1}$ *be the Bracken-Leander function on* $\mathbb{F}_{2^n}$ *(we do not necessarily impose the condition* $n = 4t$*). If* t *is odd, then* f_4 *is not* 0*-APN on any* $\mathbb{F}_{2^n}$ *when* n *is even. If* $n = 4t$ *and* t *even, then* f *is* 0*-APN.*

(*v*) *Let* $f_5(x) = x^{2^n-2^s}$ *(which coincides with the inverse function* x^{-1} *extended by* $0^{-1} = 0$ *for* $s = 1$*). Then,* f_5 *is* 0*-APN if and only if* $\gcd(n, s+1) = 1$*.*

Proof. We proved in [6] that f_1 is 0-APN if and only if $\gcd(n,t) = 1$. In the same paper we also proved that a quadratic function is x_0-APN (for some x_0) if and only if it is APN. Therefore, f_1 is not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$, under $\gcd(n,t) > 1$.

Now, let $f_2(x) = x^{2^r-2^t+1}$ be the generalization of the Kasami function. Multiplying the Rodier equation for f_2 at 0 by $(x+y)^{2^t}$, we get

$$\begin{aligned} 0 &= (x+y)^{2^t}\left(x^{2^r-2^t+1} + y^{2^r-2^t+1} + (x+y)^{2^r-2^t+1}\right) \\ &= \left(x^{2^t} + y^{2^t}\right)\left(x^{2^r-2^t+1} + y^{2^r-2^t+1}\right) + (x+y)^{2^r}(x+y) \\ &= x^{2^r-2^t+1}y^{2^t} + y^{2^r-2^t+1}x^{2^t} + x^{2^r}y + xy^{2^r}. \end{aligned}$$

Label $y = ax$. Then, assuming $xy \neq 0$, $a \neq 0, 1$, the equation above becomes

$$\begin{aligned} 0 &= a^{2^r} + a^{2^t} + a^{2^r-2^t+1} + a \\ &= a^{2^t}(a^{2^r-2^t} + 1) + a(a^{2^r-2^t} + 1) \\ &= (a^{2^t} + a)(a^{2^t(2^{r-t}-1)} + 1) \\ &= a(a^{2^t-1} + 1)(a^{2^{r-t}-1} + 1)^{2^t}. \end{aligned}$$

Having some $a \neq 1$ satisfy $a^{2^t-1}+1 = 0$ is equivalent to $\gcd(2^t-1, 2^n-1) = 2^{\gcd(t,n)}-1 > 1$, that is, $\gcd(t,n) > 1$. Similarly, having $a^{2^{r-t}-1} + 1 = 0$ for $a \neq 1$ is equivalent to $\gcd(2^{r-t}-1, 2^n-1) = 2^{\gcd(r-t,n)} - 1 > 1$, that is, $\gcd(r-t,n) > 1$.

We conclude that the above equation has no solutions outside of $a = 0, 1$ if and only if $\gcd(t,n) = \gcd(r-t,n) = 1$.

Next, let $\gcd(t, r-t, n) = d > 1$, and let $x_0 \in \mathbb{F}_{2^n}$. Let ζ be a (2^n-1)-primitive root of unity, and write $x_0 = \zeta^k$, for some $0 \le k \le 2^n - 2$. Multiplying the Rodier equation of f_2 at ζ^k by $(x+y+\zeta^k)^{2^t}$, we get

$$\begin{aligned} & (x+y+\zeta^k)^{2^t}\left(x^{2^r-2^t+1}+y^{2^r-2^t+1}+\zeta^{k(2^r-2^t+1)}\right)+(x+y+\zeta^k)^{2^r}(x+y+\zeta^k) \\ = \; & x^{2^t}y^{2^r-2^t+1}+y^{2^t}x^{2^r-2^t+1}+y^{2^t}\zeta^{k(2^r-2^t+1)}+x^{2^t}\zeta^{k(2^r-2^t+1)} \\ & +\zeta^{k2^t}(x^{2^r-2^t+1}+y^{2^r-2^t+1})+yx^{2^r}+xy^{2^r}+\zeta^k(x^{2^r}+y^{2^r})+\zeta^{k2^r}(x+y), \end{aligned}$$

and using $\zeta^{k(2^t-1)}=\zeta^{k(2^r-1)}=1$ (both identities can be shown by observing that $k=m\cdot\frac{2^n-1}{2^d-1}$ for some integer m and so, both $k(2^t-1)$ and $k(2^r-1)$ are multiples of 2^n-1), along with the substitution $y=ax$, we get

$$\begin{aligned} & x^{2^r+1}(a^{2^r}+a^{2^r-2^t+1}+a^{2^t}+a)+x^{2^r}\zeta^k(a^{2^r}+1) \\ & +x^{2^t}\zeta^k(a^{2^t}+1)+x^{2^r-2^t+1}\zeta^k(a^{2^r-2^t+1}+1)+x(1+a)\zeta^k=0. \end{aligned}$$

Taking $a\in\mathbb{F}_{2^d}\setminus\mathbb{F}_2$, and so, $a^{2^d-1}=1$, which implies $a^{2^t-1}=1$, and observing that the first term above is zero, we get

$$x^{2^r}\zeta^k(a+1)+x^{2^t}\zeta^k(a+1)+x^{2^r-2^t+1}\zeta^k(a+1)+x\zeta^k(a+1)=0,$$

that is,

$$x^{2^r}+x^{2^t}+x^{2^r-2^t+1}+x=x(x^{2^t-1}+1)(x^{2^{r-t}-1}+1)^{2^t}=0,$$

which has nontrivial solutions if $\gcd(t,n)>1$. By Proposition 4.1 of [6], if a power function is x_0-APN for some $x_0\neq 0$ then it is not x_0-APN for all $x_0\neq 0$.

For $f_3(x)=x^{2^r+2^t-1}$, the Rodier equation at 0 is

$$0 \;=\; x^{2^r+2^t-1}+y^{2^r+2^t-1}+(x+y)^{2^r+2^t-1},$$

which multiplied by $x+y$ gives

$$\begin{aligned} 0 &= x^{2^r+2^t}+y^{2^r+2^t}+yx^{2^r+2^t-1}+xy^{2^r+2^t-1}+(x^{2^r}+y^{2^r})(x^{2^t}+y^{2^t}) \\ &= xy^{2^r+2^t-1}+yx^{2^r+2^t-1}+x^{2^r}y^{2^t}+y^{2^r}x^{2^t}. \end{aligned}$$

Writing $y=xa$, the above equation becomes (assuming $x\neq 0$)

$$\begin{aligned} 0 &= a^{2^r+2^t-1}+a^{2^r}+a^{2^t}+a \\ &= a(a^{2^r-1}+1)(a^{2^t-1}+1). \end{aligned}$$

Thus, f is 0-APN if and only if $\gcd(r,n)=\gcd(t,n)=1$.

The Rodier equation (1) for $f_4(x)=x^{2^{2t}+2^t+1}$ at 0 becomes

$$\begin{aligned} 0 &= x^{2^{2t}+2^t+1}+y^{2^{2t}+2^t+1}+(x+y)^{2^{2t}+2^t+1} \\ &= x^{2^{2t}+2^t+1}+y^{2^{2t}+2^t+1}+(x+y)^{2^{2t}}(x+y)^{2^t}(x+y) \\ &= x^{2^{2t}+1}y^{2^t}+x^{2^{2t}}y^{2^t+1}+x^{2^t+1}y^{2^{2t}}+x^{2^t}y^{2^{2t}+1}+x^{2^{2t}+2^t}y+xy^{2^{2t}+2^t}. \end{aligned}$$

Taking $y = ax$, $a \neq 0, 1$, and dividing by $x^{2^{2t}+2^t+1} \neq 0$, we obtain

$$0 = a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a, \tag{8}$$

or, equivalently,

$$0 = (a^{2^t+1} + a^{2^t} + a)^{2^t} + a(a^{2^t} + a + 1)^{2^t}. \tag{9}$$

If t is odd and n is even, then $3 \mid \gcd(2^{t-1} - 1, 2^n - 1) = 2^{\gcd(t-1,n)} - 1$ and so, we can choose $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$. Then $a \neq 0, 1$ and $a^2 + a + 1 = 0$. Further, $a^{2^t} + a + 1 = 0$ (since $a^{2^{t-1}} = a$) and the equation above becomes

$$(a(a + 1) + (a + 1) + a)^{2^t} = (a^2 + a + 1)^{2^t} = 0,$$

which certainly holds, and so, f_4 is not 0-APN.

Assume now that $n = 4t$ for t even (hence $\gcd(t - 1, n) = 1$ and $\gcd(2t - 1, n) = 1$). As in [2], we apply the relative trace $\mathrm{Tr}_t^{4t}(x) = x + x^{2^t} + x^{2^{2t}} + x^{2^{3t}}$ to equation (8) and obtain

$$\begin{aligned}
0 &= \mathrm{Tr}_t^{4t}\left(a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a\right)\\
&= a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a\\
&\quad + a^{2^{3t}+2^{2t}} + a^{2^{3t}+2^t} + a^{2^{3t}} + a^{2^{2t}+2^t} + a^{2^{2t}} + a^{2^t}\\
&\quad + a^{2^{4t}+2^{3t}} + a^{2^{4t}+2^{2t}} + a^{2^{4t}} + a^{2^{3t}+2^{2t}} + a^{2^{3t}} + a^{2^{2t}}\\
&\quad + a^{2^{5t}+2^{4t}} + a^{2^{5t}+2^{3t}} + a^{2^{5t}} + a^{2^{4t}+2^{3t}} + a^{2^{4t}} + a^{2^{3t}}\\
&= a^{2^{2t}+2^t} + a^{2^{2t}+1} + a^{2^{2t}} + a^{2^t+1} + a^{2^t} + a\\
&\quad + a^{2^{3t}+2^{2t}} + a^{2^{3t}+2^t} + a^{2^{3t}} + a^{2^{2t}+2^t} + a^{2^{2t}} + a^{2^t}\\
&\quad + a^{2^{3t}+1} + a^{2^{2t}+1} + a + a^{2^{3t}+2^{2t}} + a^{2^{3t}} + a^{2^{2t}}\\
&\quad + a^{2^t+1} + a^{2^{3t}+2^t} + a^{2^t} + a^{2^{3t}+1} + a + a^{2^{3t}}\\
&= a + a^{2^t} + a^{2^{2t}} + a^{2^{3t}},
\end{aligned} \tag{10}$$

since $a^{2^{4t}} = a$. Adding the first and second powers of (10) to (8) renders

$$a^2 + a^{2^{3t}+1} + a^{2^{2t}+2^t} + a^{2^{3t}} = 0. \tag{11}$$

Taking the 2^{2t} powers of both sides of this last equation, we get

$$a^{2^{2t+1}} + a^{2^{5t}+2^{2t}} + a^{2^{4t}+2^{3t}} + a^{2^{5t}} = a^{2^{2t+1}} + a^{2^{2t}+2^t} + a^{2^{3t}+1} + a^{2^t} = 0,$$

which added to (11) gives

$$a^{2^{3t}} + a^{2^{2t+1}} + a^{2^t} + a^2 = 0.$$

Using (10), we obtain

$$a^{2^{2t+1}} + a^{2^{2t}} + a^2 + a = 0,$$

implying
$$(a+a^{2^{2t}})^2+a+a^{2^{2t}}=(a^{2^{2t}}+a)(a^{2^{2t}}+a+1)=0,$$
which has solutions if and only if $a+a^{2^{2t}}=0$, or $1+a+a^{2^{2t}}=0$. Substituting $a^{2^{2t}}=a$ into (8) renders
$$a^{2^t+1}+a^2+a+a^{2^t+1}+a^{2^t}+a=0,$$
that is,
$$0=a^{2^t}+a^2=a^2(a^{2^t-2}+1)=a^2(a^{2^{t-1}-1}+1)^2,$$
and so $a^{2^{t-1}-1}=1$, which is impossible under $\gcd(t-1,n)=1$. If $a^{2^{2t}}=a+1$, then (8) becomes $a^2+a+1=0$, which implies that $a^{2^{2t}}=a^2$. This is equivalent to $a^{2^{2t-1}-1}=1$, which is impossible if $\gcd(2t-1,n)=1$.

Lastly, the Rodier equation for $f_5(x)=x^{2^n-2^s}$ at 0 is
$$x^{2^n-2^s}+y^{2^n-2^s}+(x+y)^{2^n-2^s}=0.$$
Suppose that $x,y\neq 0,1$, and that $x\neq y$. Let $y=xa$, with $a\neq 0,1$. Then, we can rewrite the equation as
$$x^{2^n-2^s}\left(1+a^{2^n-2^s}+(1+a)^{2^n-2^s}\right)=0.$$
Since $x\neq 0$, this implies that $1+a^{2^n-2^s}+(1+a)^{2^n-2^s}=0$. Multiplying by $(1+a)^{2^s}$, renders $a^{2^n-2^s}+a^{2^s}=a^{2^s}(a^{2^{n-s-1}-1}+1)^{2^{s+1}}=0$. This equation has solutions if and only if $\gcd(n,s+1)>1$. □

Remark 3.5. *Note that the case (iv) includes the function $F(x)=x^{21}$. In that particular case, however, we were able to prove a stronger result than the one contained in (iv) above.*

Remark 3.6. *We could have referred to (reversed) Dickson polynomials* [13] *in some of the arguments above, but we felt that in this case it would not bring further light to the proofs.*

As in Remark 3.5, it is not difficult to find specific values of exponents that are 0-APN for infinitely many extensions of $\mathbb{F}_{2^n}$, but, in this paper, we prefer to give more general results. On the other hand, there are polynomials for which we can find general conditions not to be partial APN (and, consequently, not APN), and we provide such instances below.

Proposition 3.7. *Let s and n be positive integers, then the following functions over $\mathbb{F}_{2^n}$ are not 0-APN:*
1) $f_6(x)=x^{2^{2s+1}+2^{s+1}+2^s-1}$ when $n\geq 4$ is even;
2) $f_7(x)=x^{2^{4s}+2^{3s}+2^{2s}+2^s-1}$ (a Dobbertin-like function known to be APN for $n=5s$) when s is odd and n is even;
3) $f_8(x)=x^{2^{2s+1}+5}$ when n is even.

Proof. The Rodier equation for f_6 at $x_0 = 0$ is

$$x^{2^{2s+1}+2^{s+1}+2^s-1} + y^{2^{2s+1}+2^{s+1}+2^s-1} + (x+y)^{2^{2s+1}+2^{s+1}+2^s-1} = 0,$$

rendering, in the same way as before, for $y = ax$ (under $0 \neq x \neq y \neq 0$)

$$a^{2^s+2^{s+1}+2^{2s+1}-1} + a^{2^{s+1}+2^{2s+1}} + a^{2^s+2^{2s+1}} + a^{2^s+2^{s+1}} + a^{2^{2s+1}} + a^{2^{s+1}} + a^{2^s} + a = 0.$$

Since n is even, then we can take $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, and so $a^3 = 1$, implying $a^2 + a + 1 = 0$. For such an a, observe that $a^{2^{s+1}} = a^{2^s} + 1, a^{2^{2s+1}} = a^{2^{2s}} + 1$, and the previous expression becomes

$$\begin{aligned}
&a^{2^s-1}(a^{2^s}+1)(a^{2^{2s}}+1) + (a^{2^s}+1)(a^{2^{2s}}+1) + a^{2^s}(a^{2^{2s}}+1) \\
&\qquad + a^{2^s}(a^{2^s}+1) + a^{2^{2s}} + 1 + a^{2^s} + 1 + a^{2^s} + a \\
=&a^{2^{2s}+2^{s+1}-1} + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a^{2^{2s}+2^s} + a^{2^{2s}} \\
&\quad + a^{2^s} + 1 + a^{2^{2s}+2^s} + a^{2^s} + a^{2^{s+1}} + a^{2^s} + a^{2^{2s}} + a \\
=&a^{2^{2s}-1}(a^{2^s}+1) + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a^{2^s} + a^{2^s} + 1 + 1 + a \\
=&a^{2^{2s}+2^s-1} + a^{2^{2s}-1} + a^{2^{2s}+2^s-1} + a^{2^{s+1}-1} + a^{2^s-1} + a \\
=&a^{2^{2s}-1} + a^{2^{s+1}-1} + a^{2^s-1} + a = a^{-1}\left(a^{2^{2s}} + a^{2^{s+1}} + a^{2^s} + a^2\right) \\
=&a^{-1}\left(a^{2^{2s}} + a^{2^s} + 1 + a^{2^s} + a^2\right) = a^{-1}\left(a^{2^{2s}} + a^2 + 1\right) = 0,
\end{aligned}$$

since $a^{2^{2s}} = a^{2^{2s-1}} + 1 = a^{2^{2s-2}} = \cdots = a^{2^{2s-2s}} = a$, and so $a^{2^{2s}} + a^2 + 1 = a + a^2 + 1 = 0$.

Similarly, the Rodier equation for the 0-APN-ness of f_7 implies

$$\begin{aligned}
&a^{2^s+2^{2s}+2^{3s}+2^{4s}} + a^{1+2^{2s}+2^{3s}+2^{4s}} + a^{1+2^s+2^{3s}+2^{4s}} + a^{1+2^s+2^{2s}+2^{4s}} \\
&+ a^{1+2^s+2^{2s}+2^{3s}} + a^{1+2^{3s}+2^{4s}} + a^{1+2^{2s}+2^{4s}} + a^{1+2^s+2^{4s}} + a^{1+2^{2s}+2^{3s}} \\
&+ a^{1+2^s+2^{3s}} + a^{1+2^{2s}+2^s} + a^{1+2^{4s}} + a^{1+2^{3s}} + a^{1+2^{2s}} + a^{1+2^s} + a^2 = 0.
\end{aligned}$$

Using a similar method as in the first part of our proposition, with n even, and taking $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$ and s odd, one can show that the above expression is zero, and so, f_7 is not 0-APN.

The Rodier equation for f_8 is

$$x^{2^{2s+1}+5} + y^{2^{2s+1}+5} + (x+y)^{2^{2s+1}+5} = 0,$$

which, when $y = ax$, $a \neq 0, 1$, $x \neq 0$, becomes

$$\begin{aligned}
0 &= 1 + a^{2^{2s+1}+5} + (1 + a^{2^{2s+1}})(1+a)^5 \\
&= 1 + a^{2^{2s+1}+5} + \left(1 + a^{2^{2s+1}}\right)\left(1 + a + a^4 + a^5\right) \\
&= a + a^4 + a^5 + a^{2^{2s+1}} + a^{2^{2s+1}+1} + a^{2^{2s+1}+4}.
\end{aligned}$$

Since n is even, we can take $a \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, and so $a^3 = 1$, implying $a^2 + a + 1 = 0$. For such an a, observe that $a^4 = a, a^5 = a^2, a^{2^{2s+1}} = a^2, a^{2^{2s+1}+4} = a^{2^{2s+1}+1}$, and the previous expression becomes $a + a + a^2 + a^2 + a^{2^s+1} + a^{2^s+1} = 0$, implying that f_8 is not 0-APN. $\square$

4 Binomial partial APN functions

It was observed in [6] that if a monomial is 0-APN and x_0-APN for some $0 \neq x_0 \in \mathbb{F}_{2^n}$, then it is APN. We also know that for any quadratic (n,n)-function F and for any $x_0 \in \mathbb{F}_{2^n}$, F is x_0-APN if and only if it is APN. Similarly, it was suggested and consequently shown in [6] that any partially 1-APN monomial function is APN. It is natural to wonder if such a statement is true for other types of functions. We give below an instance when such a claim fails.

Theorem 4.1. *Let $F(x) = x^{2^n-1} + x^{2^n-2}$ be defined on $\mathbb{F}_{2^n}$. Then F is 1-APN, but not 0-APN, for all $n \geq 3$. Furthermore, F is differentially 4-uniform.*

Proof. Let $F(x) = x^{2^n-1} + x^{2^n-2}$, and $x_0 = 1$. Then, the Rodier condition (1) becomes

$$x^{2^n-1} + x^{2^n-2} + y^{2^n-1} + y^{2^n-2} + (x+y+1)^{2^n-1} + (x+y+1)^{2^n-2} = 0,$$

which is equivalent to (since $x^{2^n-1} = 1$, for $x \in \mathbb{F}_{2^n}^*$),

$$1 + x^{-1} + 1 + y^{-1} + 1 + (x+y+1)^{-1} = 0, \text{ assuming } xy(x+y+1) \neq 0.$$

Multiplying the previous equation by $xy(x+y+1)$, we obtain

$$y(x+y+1) + x(x+y+1) + xy(x+y+1) + xy = 0 \iff (x+y)(1+x)(1+y) = 0,$$

which proves the first claim.

To show that F is not 0-APN, let us consider the Rodier equation for $x_0 = 0$,

$$\begin{aligned}
&x^{2^n-1} + x^{2^n-2} + y^{2^n-1} + y^{2^n-2} + (x+y)^{2^n-1} + (x+y)^{2^n-2} = 0\\
\iff &1 + x^{-1} + 1 + y^{-1} + 1 + (x+y)^{-1} = 0\\
\iff &y(x+y) + x(x+y) + xy(x+y) + xy = 0\\
\iff &(x+y)^2 + xy(x+y) + xy = 0\\
\iff &1 + \frac{xy}{x+y} + \frac{xy}{(x+y)^2} = 0. \qquad (12)
\end{aligned}$$

We will find $0 \neq x \neq y \neq 0$ to satisfy the previous equation. Let $t = x + y$. Then, the previous equation is equivalent to

$$\begin{aligned}
&t^2 + x(x+t)(t+1) = 0, \text{ (observe that } t \neq 1)\\
\iff &x^2 + tx + \frac{t^2}{t+1} = 0\\
\iff &\left(\frac{x}{t}\right)^2 + \frac{x}{t} + \frac{1}{t+1} = 0.
\end{aligned}$$

Labeling $z = \frac{x}{t}$, we obtain the equation

$$z^2 + z + \frac{1}{t+1} = 0.$$

We now use the fact that for $0 \neq v \in \mathbb{F}_{2^n}$ the equation $X^2 + X = v$ has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(v) = 0$ (see Berlekamp et al. [1]). Taking any of the $2^{n-1} - 1$ nontrivial values of $v \in \mathbb{F}_{2^n}^*$ for which $\mathrm{Tr}_1^n(v) = 0$, $t = 1 + v^{-1} \neq 0$ and z a solution of $X^2 + X = v$, we have that $x = tz, y = t(z+1)$ will satisfy equation (12) and $0 \neq x \neq y \neq 0$, hence F is not 0-APN.

We next show that F is differentially 4-uniform. We first write the equation $D_aF(x) = b$, under $a \neq 0, b \in \mathbb{F}_{2^n}$, namely,

$$x^{2^n-1} + x^{2^n-2} + (x+a)^{2^n-1} + (x+a)^{2^n-2} = b, \tag{13}$$

with $x \in \mathbb{F}_{2^n}$. *Case* 1. Let $b = 1 + a^{-1}$. We can see that $x = 0$, $x = a$ are solutions of (13). Further, if $x \neq 0, x \neq a$, then (13) becomes $x^{2^n-2} + (x+a)^{2^n-2} = b$, which is equivalent to $x^{-1} + (x+a)^{-1} = b = 1 + a^{-1}$, that is,

$$(a+1)x^2 + (a^2+a)x + a^2 = 0. \tag{14}$$

We can see that $a \neq 1$ and so, $a^2 + a \neq 0$, and therefore, by taking $y = xa^{-1}$, we obtain that (14) is equivalent to $y^2 + y = (a+1)^{-1}$, which, by [1] has solutions y (and thus x) if and only if $\mathrm{Tr}_1^n((a+1)^{-1}) = 0$. There certainly exist $a \in \mathbb{F}_{2^n}$ satisfying this condition, in which case equation (14) has two more solutions, in addition to $0, a$.
Case 2. Let $b \neq 1 + a^{-1}$. Then x is not equal to 0 or to a in (13) and so, the first and third terms are equal to 1, and (13) becomes

$$x^{-1} + (x+a)^{-1} = b, \tag{15}$$

that is, $bx^2 + abx + a = 0$, which has at most two solutions x (in general, the equation above may have four solutions if $b = a^{-1}$, namely $\{0, a, a\alpha, a\alpha^2\}$, where $\alpha \in \mathbb{F}_{2^2} \setminus \mathbb{F}_2$, but we removed $0, a$ from the possibilities because of (13)). In fact, we know exactly when equation (15) has no solutions, namely, when $\mathrm{Tr}_1^n\left(\frac{1}{ab}\right) = 1$.

In conclusion, equation (13) has at most 4 solutions (with that bound attained), and therefore F is differentially 4-uniform. $\square$

Remark 4.2. *The non-*0*-APN-ness of the above function can also be derived from* [6, Thm. 5.5]*, but we preferred to give a self-contained argument above.*

5 Partial APN functions based on Dillon's polynomial

Dillon [12] suggested investigating functions of the form

$$F(x) = x(Ax^2 + Bx^{2^k} + Cx^{2^{k+1}}) + x^2(Dx^{2^k} + Ex^{2^{k+1}}) + Gx^{3\cdot 2^k} \tag{16}$$

over $\mathbb{F}_{2^n}$, with $n = 2k$, as candidates for APN or differentially 4-uniform functions. An infinite family of APN functions of this type was constructed in [4]. In this section, we investigate several such functions for being partial APN functions, and consequently, APN functions (recall that we showed in [6] that for quadratic functions, pAPN property is equivalent to the APN property). The motivation for this section is to point out that any of the functions coming from F can be investigated quite easily for APN-ness using the not so restrictive concept of pAPN-ness.

First, we write the Rodier condition at $x_0 = 0$ for the function F above, which we generalize by taking arbitrary $1 \le k \le n-1$. Now, letting $y = ax$, $a \ne 0, 1, x \ne 0$, we obtain

$$\begin{aligned}0 =&Ax^3(a+a^2) + Bx^{2^k+1}\left(a+a^{2^k}\right) + Cx^{2^{k+1}+1}\left(a+a^{2^{k+1}}\right)\\&+ Dx^{2^k+2}\left(a^2+a^{2^k}\right) + Ex^{2^{k+1}+2}\left(a^2+a^{2^{k+1}}\right) + Gx^{2^{k+1}+2^k}\left(a^{2^k}+a^{2^{k+1}}\right).\end{aligned} \tag{17}$$

We will not provide the proof of the next theorem (whose proof is not that complicated, containing cases that are known via APN-ness), but we will provide the proof of the last theorem of this section, since it is more involved.

Theorem 5.1. *Let $1 \le k \le n-1$ and consider the function F from* (16). *The following functions are not x_0-APN for any $x_0 \in \mathbb{F}_{2^n}$:*

(i) $F_1(x) = Ax^3 + Bx^{2^k+1}$ *if* $AB \ne 0$, $\gcd(k-1, n) = 1$, $k \ge 1$, *and* $F_2(x) = Ax^3 + Cx^{2^{k+1}+1}$ *if* $AC \ne 0$ *and* $\gcd(k, n) = 1$.

(ii) $F_3(x) = Ax^3 + Dx^{2^k+2}$ *if* $AD \ne 0$ *and* $\gcd(k, n) = 1$, $k > 1$.

(iii) $F_4(x) = Ax^3 + Ex^{2^{k+1}+2}$ *if* $AE \ne 0$ *and* $\gcd(k+1, n) = 1$.

(iv) $F_5(x) = Ax^3 + Gx^{3\cdot 2^k}$ *if* $AG \ne 0$, $\frac{A}{G} \in \mathbb{F}_{2^n}^{2^k-1}$ *and there exists z such that* $\mathrm{Tr}_1^n((A/G)^{1/(2^k-1)}/z^3) = 0$.

(v) $F_6(x) = Bx^{2^k+1} + Cx^{2^{k+1}+1}$ *if* $BC \ne 0$ *and* $k \ge 1$.

(vi) $F_7(x) = Bx^{2^k+1} + Dx^{2^k+2}$ *if* $BD \ne 0$.

(vii) $F_8(x) = Bx^{2^k+1} + Ex^{2^{k+1}+2}$ *if* $BE \ne 0$, *and* $\gcd(k, n) > 1$, *or n is odd and* $\gcd(k, n) = 1$.

(viii) $F_9(x) = Bx^{2^k+1} + Gx^{2^{k+1}+2^k}$ *if* $BG \ne 0$ *and* $\gcd(k+1, n) = 1$.

(ix) $F_{10}(x) = Cx^{2^{k+1}+1} + Dx^{2^k+2}$ *if* $CD \ne 0$ *and* $\gcd(k, n) = 1$.

(x) $F_{11}(x) = Cx^{2^{k+1}+1} + Ex^{2^{k+1}+2}$ *if* $CE \ne 0$.

(xi) $F_{12}(x) = Cx^{2^{k+1}+1} + Gx^{2^{k+1}+2^k}$ *if* $CG \ne 0$.

(xii) $F_{13}(x) = Dx^{2^k+2} + Ex^{2^{k+1}+2}$ *if* $DE \ne 0$.

(xiii) $F_{14}(x) = Dx^{2^k+2} + Gx^{2^{k+1}+2^k}$ *if* $DG \ne 0$ *and* $\gcd(k, n) = 1$.

(xiv) $F_{15}(x) = Ex^{2^{k+1}+2} + Gx^{2^{k+1}+2^k}$ *if* $EG \ne 0$ *and* $\gcd(k-1, n) = 1$.

We can certainly go beyond binomials and we do so in the next theorem without attempting to be exhaustive.

Theorem 5.2. *Let Let $1 \le k \le n-1$, $G \neq 0$, $\gcd(k,n) > 1$, n odd, and $A/G \in \mathbb{F}_{2^n}^{2^k-1}$. Then $F_{16}(x) = Ax^3 + Bx^{2^k+1} + Ex^{2^{k+1}+2} + Gx^{2^{k+1}+2^k}$ is not x_0-APN for any x_0.*

Proof. The Rodier equation (17) for F_{16} at $x_0 = 0$ is equivalent to

$$x^3(a+a^2)\left(A + Gx^{3\cdot(2^k-1)}(a+a^2)^{2^k-1}\right) \\ + x^{2^k+1}a\left(1+a^{2^k-1}\right)\left(B + Ex^{2^k+1}\left(a+a^{2^k}\right)\right) = 0.$$

If $\gcd(k,n) > 1$, then taking $a \neq 0, 1$ such that $a^{2^k-1} = 1$, the second term is zero. Furthermore $(a+a^2)^{2^k-1} = a^{2^k-1}(a+1)^{2^k-1} = \frac{(a+1)^{2^k}}{a+1} = \frac{a^{2^k}+1}{a+1} = \frac{a+1}{a+1} = 1$, and so the first term becomes $x^3(a+a^2)\left(A + Gx^{3\cdot(2^k-1)}\right)$, which is zero for the unique solution x of $x^3 = \left(\frac{A}{G}\right)^{1/(2^k-1)}$, which exists since n is odd (that is, $\gcd(3, 2^n-1) = 1$).
A quadratic function is pAPN for some x_0 if and only if it is APN [6]. Hence the claim of the theorem follows. □

We now replace 2^k by 2^k+1 in Dillon's polynomial (16).

Theorem 5.3. *Let $1 \le k \le n-1$. The following statements hold:*

(i) *If $AC \neq 0$, then the functions $H_1(x) = Ax^3 + Cx^{2^{k+1}+3}$ (respectively, $H_2(x) = Ax^3 + Cx^{2^k+3}$) is not 0-APN.*

(ii) *If $AG \neq 0$, then the functions $H_3(x) = Ax^3 + Gx^{2^{k+1}+2^k+3}$ is not 0-APN if n is odd; if n is even, then H_3 is 0-APN if and only if $\left(\frac{A}{G}\right)^{2^{-k}} \notin \{u^3 : x \in \mathbb{F}_{2^n}\}$.*

(iii) *If $BC \neq 0$, and $\gcd(2^k+1, 2^n-1) = 1$, which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is even, then $H_4(x) = Bx^{2^k+2} + Cx^{2^{k+1}+3}$ is not 0-APN.*

(iv) *If $BD \neq 0$, $H_5(x) = Bx^{2^k+2} + Dx^{2^k+3}$ is never 0-APN.*

(v) *If $BG \neq 0$, and $\gcd(2^{k+1}+1, 2^n-1) = 1$ (which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is odd), then $H_6(x) = Bx^{2^k+2} + Gx^{2^{k+1}+2^k+3}$ is not 0-APN.*

(vi) *If $CDEG \neq 0$, then $H_7(x) = Cx^{2^{k+1}+3} + Dx^{2^k+3}$, $H_8(x) = Cx^{2^{k+1}+3} + Ex^{2^{k+1}+4}$, and $H_9(x) = Cx^{2^{k+1}+3} + Gx^{2^{k+1}+2^k+3}$ are never 0-APN.*

(vii) *If $DE \neq 0$, and $\gcd(2^k+1, 2^n-1) = 1$, which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is even, then $H_{10}(x) = Dx^{2^k+3} + Ex^{2^{k+1}+4}$ is not 0-APN.*

(viii) *If $DG \neq 0$, then $H_{11}(x) = Dx^{2^k+3} + Gx^{2^{k+1}+2^k+3+1}$ is never 0-APN.*

(*ix*) *If* $EG \neq 0$ *and* $gcd(k,n) = 1$, *then* $H_{12}(x) = Ex^{2^{k+1}+4} + Gx^{2^{k+1}+2^k+3}$ *is not* 0-*APN.*

Proof. Let us replace 2^k by 2^k+1 in Dillon's polynomial (16); as before, letting $y = ax$, $x \neq 0$, $a \neq 0, 1$, in the Rodier equation for Dillon's polynomial we obtain

$$\begin{aligned} 0 &= Ax^3(a+a^2) + Bx^{2^k+2}\left(a^2+a^{2^k}\right) \\ &+ Cx^{2^{k+1}+3}\left(a+a^2+a^3+a^{2^{k+1}}+a^{2^{k+1}+1}+a^{2^{k+1}+2}\right) \\ &+ Dx^{2^k+3}\left(a+a^2+a^3+a^{2^k}+a^{2^k+1}+a^{2^k+2}\right) \\ &+ Ex^{2^{k+1}+2^2}\left(a^4+a^{2^{k+1}}\right) + Gx^{2^{k+1}+2^k+3}\left(a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1\right) \\ &= Ax^3(a+a^2) + Bx^{2^k+2}\left(a^2+a^{2^k}\right) + Cx^{2^{k+1}+3}\left(1+a+a^2\right)\left(a+a^{2^{k+1}}\right) \\ &+ Dx^{2^k+3}\left(1+a+a^2\right)\left(a+a^{2^k}\right) + Ex^{2^{k+1}+2^2}\left(a^4+a^{2^{k+1}}\right) \\ &+ Gx^{2^{k+1}+2^k+3}\left(a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1\right). \end{aligned} \tag{18}$$

We only consider combinations rendering non-quadratic functions. Let $AC \neq 0$, $H_1(x) = Ax^3 + Cx^{2^{k+1}+3}$ (similarly, for $AD \neq 0$, $H_2(x) = Ax^3 + Dx^{2^k+3}$). The Rodier equation (18) for H_1 at 0 is therefore

$$Ax^3(a+a^2) = Cx^{2^{k+1}+3}\left(1+a+a^2\right)\left(a+a^{2^{k+1}}\right),$$

that is $x^{2^{k+1}} = \frac{A(1+a)}{C(1+a+a^2)\left(1+a^{2^{k+1}-1}\right)}$ (recall that $a \neq 0, 1$ and if a is a primitive third root of unity then the displayed equation above cannot hold for nontrivial solutions x). Since this last equation always has nontrivial solutions, the function H_1 cannot be 0-APN.

Next, $H_3(x) = Ax^3 + Gx^{2^{k+1}+2^k+3}$ whose Rodier equation at 0 is

$$Ax^3(a+a^2) = Gx^{2^{k+1}+2^k+3}\left(a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1\right),$$

which is equivalent to (the expression in the parentheses on the right-hand side cannot be zero, otherwise there are no non-trivial solutions)

$$x^{3\cdot 2^k} = \frac{A(a+a^2)}{G\left(a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1\right)}. \tag{19}$$

If n is odd, then equation (19) will always have nontrivial solutions. If n is even, taking 2^k-th roots on both sides, we obtain

$$u^3 = \left(\frac{A}{G}\right)^{2^{-k}},$$

where

$$u = x\left(\frac{a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1}{a+a^2}\right)^{2^{-k}}$$

is any of the 2^k roots. The claim is inferred.

Next, take $BC \neq 0$, and $H_4(x) = Bx^{2^k+2} + Cx^{2^{k+1}+3}$. The Rodier equation at 0 is now

$$x^{2^k+1} = \frac{B\left(a^2+a^{2^k}\right)}{C\left(1+a+a^2\right)\left(a+a^{2^{k+1}}\right)}.$$

If $\gcd(2^k+1, 2^n-1) = 1$ (which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is even), then the equation above has nontrivial solutions (certainly, for example, for a such that $a \notin \mathbb{F}_4^*$).

If $BD \neq 0$, then it is straightforward to check that the cubic $H_5(x) = Bx^{2^k+2} + Dx^{2^k+3}$ is never 0-APN, since its Rodier equation at 0 is equivalent to

$$x = \frac{B\left(a^2+a^{2^k}\right)}{D\left(1+a+a^2\right)\left(a+a^{2^k}\right)},$$

which obviously has nontrivial solutions (certainly, for a such that the denominator above is not zero).

If $BG \neq 0$, then the Rodier equation at 0 for $H_6(x) = Bx^{2^k+2} + Gx^{2^{k+1}+2^k+3}$ is

$$x^{2^{k+1}+1} = \frac{B\left(a^2+a^{2^k}\right)}{G\left(a^{2^{k+1}+2^k+3}+(a+1)^{2^{k+1}+2^k+3}+1\right)}.$$

If $\gcd(2^{k+1}+1, 2^n-1) = 1$ (which happens if n is odd, or $n \equiv 2 \pmod 4$ and k is odd), then the equation above has nontrivial solutions (certainly, for a such that the denominator above is not zero, which can easily be achieved).

If $CD \neq 0$, the Rodier equation at 0 for the cubic $H_7(x) = Cx^{2^{k+1}+3} + Dx^{2^k+3}$ is

$$x^{2^k} = \frac{D\left(a+a^{2^k}\right)}{C\left(a+a^{2^{k+1}}\right)}.$$

Since $\gcd(2^k, 2^n-1) = 1$, the above equation always has nontrivial solutions (for an a that is not a $(2^{k+1}-1)$ root of 1). A similar straightforward analysis can be done, under $CEG \neq 0$, for the cubics $H_8(x) = Cx^{2^{k+1}+3} + Ex^{2^{k+1}+4}$ and $H_9(x) = Cx^{2^{k+1}+3} + Gx^{2^{k+1}+2^k+3}$.

If $DE \neq 0$, the Rodier equation at 0 for $H_{10}(x) = Dx^{2^k+3} + Ex^{2^{k+1}+4}$ renders

$$x^{2^k+1} = \frac{D(1+a+a^2)\left(a+a^{2^k}\right)}{E\left(a^4+a^{2^{k+1}}\right)},$$

a similar equation as for H_4. If $DG \neq 0$, the Rodier equation at 0 for $H_{11}(x) = Dx^{2^k+3} + Gx^{2^{k+1}+2^k+3}$ is similar to the one of H_7.

If $EG \neq 0$, the Rodier equation for the quartic $H_{12}(x) = Ex^{2^{k+1}+4} + Gx^{2^{k+1}+2^k+3}$ is equivalent to

$$x^{2^k-1} = \frac{E\left(a^4 + a^{2^{k+1}}\right)}{G\left(a^{2^{k+1}+2^k+3} + (a+1)^{2^{k+1}+2^k+3} + 1\right)},$$

which has a nontrivial solution x if $\gcd(k, n) = 1$ (for any value of a for which the denominator does not vanish).

Thus, the theorem is shown. $\square$

Certainly, there are other values of q, for which one can investigate the pAPN property of various combinations of terms in Dillon's polynomial. Furthermore, a fruitful direction for future work is to check and find conditions for pAPN-ness of other classes of multinomials, like the generalization proposed by Budaghyan and Carlet in [4], or perhaps, as a separate and quite interesting venue, to find classes of pAPN permutations.

Acknowledgements. The authors express their deep appreciation to the editor, as well as to the three anonymous referees, whose thorough reading and constructive comments have greatly improved the paper. The paper was started while the fourth named author visited Selmer center at University of Bergen and Western Norway University of Applied Sciences in the Spring of 2019. This author thanks these institutions for the excellent working conditions. The research of the first two named authors was supported by Trond Mohn foundation.

References

[1] E. R. Berlekamp, H. Rumsey, G. Solomon, *On the solutions of algebraic equations over finite fields*, Information and Control 10 (1967), 553–564.

[2] C. Bracken, G. Leander, *A highly nonlinear differentially* 4 *uniform power mapping that permutes fields of even degree*, Finite Fields Appl. 16 (4) (2010), 231–242.

[3] L. Budaghyan, Construction and Analysis of Cryptographic Functions, Springer-Verlag, 2014.

[4] L. Budaghyan, C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures*, IEEE Trans. Inform. Theory 54:5 (2008), 2354–2357.

[5] L. Budaghyan, C. Carlet, T. Helleseth, N. Li, B. Sun, *On upper bounds for algebraic degrees of APN functions*, IEEE Trans. Inform. Theory 64:6 (2018), 4399–4411.

[6] L. Budaghyan, N. Kaleyski, S. Kwon, C. Riera, P. Stănică, *Partially APN Boolean functions and classes of functions that are not APN infinitely often*, Cryptography

and Communication, 2019; preliminary version as *Partially APN Boolean functions*, Proc. Sequences and Their Applications – SETA 2018, Hong Kong, 2018.

[7] C. Carlet, *Boolean functions for cryptography and error correcting codes*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 257–397, 2010.

[8] C. Carlet, *Vectorial Boolean Functions for Cryptography*, In: Y. Crama, P. Hammer (eds.), Boolean Methods and Models, Cambridge Univ. Press, Cambridge, pp. 398–472, 2010.

[9] C. Carlet, P. Charpin, V. Zinoviev, *Codes, Bent Functions and Permutations Suitable For DES-like Cryptosystems*, Des. Codes Cryptogr. 15 (1998), 125–156.

[10] F. Chabaud and S. Vaudenay, *Links between differential and linear cryptanalysis*, Advances in Cryptology–EUROCRYPT'94, LNCS 950, pp. 356–365, 1995.

[11] T. W. Cusick, P. Stănică, Cryptographic Boolean Functions and Applications (Ed. 2), Academic Press, San Diego, CA, 2017.

[12] J. F. Dillon, *APN Polynomials and Related Codes*, Polynomials over Finite Fields and Applications, Banff International Research Station, Nov. 2006.

[13] X. Hou, G. L. Mullen, J. A. Sellers and J. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. 15 (2009), 748–773.

[14] D. R. Hughes, *Collineation groups and non-Desarguesian planes*, American J. Math 81 (1959), 921–938; *ibid.* 82, 113–119.

[15] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, 1997.

[16] F. Rodier, *Borne sur le degré des polynômes presque parfaitement non-linéaires*, Arithmetic, Geometry, Cryptography and Coding Theory, G. Lachaud, C. Ritzenthaler and M.Tsfasman eds., Contemporary Math. no 487, AMS, Providence (RI), USA, pp. 169–181, 2009.