On the behavior of some APN permutations under swapping points*

Lilya Budaghyan[1], Nikolay Kaleyski[1],
Constanza Riera[2], Pantelimon Stănică[3]

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

April 27, 2021

Abstract

We define the pAPN-spectrum (which is a measure of how close a function is to being APN) of an (n, n)-function F and investigate how its size changes when two of the outputs of a given function F are swapped. We completely characterize the behavior of the pAPN-spectrum under swapping outputs when F is the inverse function over $\mathbb{F}_{2^n}$. We further theoretically investigate this behavior for functions from the Gold and Welch monomial APN families, and experimentally determine the size of the pAPN-spectrum after swapping outputs for representatives from all infinite monomial APN families up to dimension $n = 10$; based on our computation results, we conjecture that the inverse function is the only monomial APN function for which swapping two its outputs can leave an empty pAPN-spectrum.

Keywords: Boolean functions, almost perfect nonlinear (APN), partial APN, binary finite fields, equations.
MSC 2020: 06E30, 11T06, 94A60, 94D10.

---

*This is a substantially revised and extended version of the article [5] that appeared in the proceedings of the Sequences and Their Applications – SETA 2020. In particular, the proofs for the Gold and Welch case, and the computational data given in the appendix, are new.

1 Introduction

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. We will denote the set of all such functions by $\mathcal{B}_n$. We shall denote by $\frac{1}{a}$ or $1/a$ the multiplicative inverse of a in $\mathbb{F}_{2^n}$, adopting the usual convention $\frac{1}{0} = 1/0 = 0$.

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, $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

A vectorial Boolean function, or (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 $\mathbb{F}_{2^n}$ (using the natural identification of the finite field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$, via some basis) of the form

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

The binary weight $w_2(i)$ of a positive integer i is the number of non-zero bits in its binary expansion, i.e. $w_2(i) = \sum_{j=0}^{K} b_j$, where $i = \sum_{j=0}^{K} b_j 2^j$ for some positive integer K and for $b_j \in \{0, 1\}$, where the sums involved are being computed over the integers. The algebraic degree of F is then the largest binary weight of an exponent i with $a_i \neq 0$. For an (n, n)-function F and for $a, b \in \mathbb{F}_{2^n}$, we define the Walsh transform $\mathcal{W}_F(a, b)$ of F to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^n(bF(x))$ at a, that is,

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

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 $\Delta_F = \delta$, then we say that F is differentially δ-uniform. Since $x + a$ is a solution to $F(x + a) + F(x) = b$ whenever x is, the differential uniformity is always even and is thus at least 2 for any F. If $\delta = 2$, then F is an *almost perfect nonlinear* (*APN*) function.

For an (n, n)-function F and an element $a \in \mathbb{F}_{2^n}$, the function $D_aF(x) = F(a + x) + F(x)$ is called the *(first-order) derivative* of F in direction a. In this way, the number $\Delta_F(a, b)$ can be interpreted as the number of solutions $x \in \mathbb{F}_{2^n}$ to the equation $D_aF(x) = b$. From this point of view, a function F is APN if and only if all of its derivatives D_aF for $a \neq 0$ are 2-to-1 functions.

APN functions are of significant interest in cryptography for the construction of block ciphers since they provide optimal resistance to differential cryptanalysis. Furthermore, some classes of APN functions correspond to optimal objects in other areas of mathematics and computer science, such as coding theory, projective geometry, and combinatorial design theory. Nonetheless, being cryptographically strong functions, APN functions are by design unpredictable and difficult to construct and analyze. For the purpose of making their analysis more tractable, a number of characterizations of APN-ness have been derived and can be found in the literature (see, for instance, [3, 7, 8, 19]). We give some of them below.

Lemma 1. *Let F be an (n,n)-function.*

(i) We always have
$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) \geq 2^{3n+1}(3\cdot 2^{n-1}-1),$$
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) (Janwa-Wilson-Rodier Condition[1]) F is APN if and only if all the points $x,y,z\in\mathbb{F}_{2^n}$ satisfying
$$F(x)+F(y)+F(z)+F(x+y+z)=0$$
belong to the surface $(x+y)(x+z)(y+z)=0$.

Along with S. Kwon, we introduced in [4] a notion of partial APN-ness in our attempt to resolve a conjecture on the upper bound on the algebraic degree of APN functions [3]. 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 x_0-APN, partially APN, or just 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 will also refer to (1) as the Janwa-Wilson-Rodier equation; the Janwa-Wilson-Rodier condition then essentially states that (1) has no solutions x outside of the curve $(x_0+x)(x_0+y)(x+y)=0$.

We will refer to the set of points $x_0\in\mathbb{F}_{2^n}$ for which a function is x_0-APN as the *pAPN-spectrum* of the function. Certainly, a function is APN if and only if it is x_0-APN for every point x_0; that is, its pAPN-spectrum is $\mathbb{F}_{2^n}$.

An alternate 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

[1] We have been calling this the "Rodier condition", but we realized that it did occur in the literature prior to Rodier's work, for power monomials in [11], so we will now call it by the three names.

x, namely $x = x_0$ and $x = x_0 + a$. An interesting approach is taken in [13], where it was observed that the partial APN concept is connected to the notion of a partial quadruple system (an instance of the much more general class of configurations called packings).

Another interpretation (observed by one of our reviewers) of partial APN-ness is the following: for an (n, n)-function F on $\mathbb{F}_{2^n}$, let D be the graph $\{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of the function F, and let $a, b \in \mathbb{F}_{2^n}$. Let $D + (a, b)$ denote the shift of D by (a, b). Then the *DDT (difference distribution table)* is the array whose (a, b) position is the intersection size of $D \cap (D + (a, b))$. The vectorial DDT does not just tabulate the sizes of the intersections, but the set of elements in $D \cap (D + (a, b))$. Then, $x_0 \in \mathbb{F}_{2^n}$ is an element in the pAPN-spectrum of F if and only if $(x_0, F(x_0)) \in D$ is not contained in any of these intersections provided the intersection has size at least 4. So the points in the pAPN-spectrum are exactly those which are never in the large intersections.

In this paper we show an intriguing property of the inverse, Gold and Welch functions: swapping two of their output values leads to a reduction in the size of their pAPN-spectra; in some cases, this reduction is quite significant. This shows that the effect of swapping two points in a given function can be quite unpredictable: as shown in [21], swapping two points of an APN function cannot increase the differential uniformity to more than 4; we note that differentially 4-uniform functions can be seen as a weakening of APN functions. In this sense, a function obtained from a two-point swap from an APN function is "close to APN" from the point of view of its differential uniformity. Since the notion of a partially APN function is itself a relaxation of that of an APN function, one would naturally expect that swapping two points in an APN function should give a function that is "close to APN" from the point of view partial APN-ness as well; instead, we see that the pAPN-spectrum can be reduced from full to empty by such an operation. Furthermore, Theorems 4, 6, and 8 show that characterizing which elements of the field belong to the pAPN-spectrum of such a function is, in general, very difficult.

The structure of the paper is as follows: in Section 2, we recall the conditions on the existence of solutions for quadratic and cubic equations over binary finite fields, we describe the Janwa-Wilson-Rodier equation for the swapping of two points, and prove that, for a function F satisfying $\Delta_F(a, b) \neq 2$ for any $a, b \in \mathbb{F}_{2^n}$, both F and any function obtained by swapping two of its outputs, have an empty pAPN-spectrum. In Section 3, we discuss the pAPN property for the inverse function swapped at two outputs, and we completely characterize the cases in which the resulting function has an empty pAPN-spectrum. In Sections 4 and 5, we discuss the pAPN property for the Gold and Welch function swapped at two outputs. Finally, in Appendix A, we give computational results for each of the infinite APN monomial families over $\mathbb{F}_{2^n}$ (except for the inverse, since it is characterized in Section 3) for $4 \leq n \leq 10$. As discussed there, and according to these experimental results, it appears that the inverse APN function is the only monomial APN function whose pAPN-spectrum can be reduced to the empty set by a two-point swap.

2 Considerations and useful remarks

Throughout the paper, we shall be using the following result from [1, 20], which describes the existence of solutions for quadratic and cubic equations over binary finite fields.

Theorem 2. *Let n be a natural number, and consider the finite field $\mathbb{F}_{2^n}$.*

(1) *The equation $x^2 + ax + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $a \neq 0$, has solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{b}{a^2}\right) = 0$. Otherwise, its two solutions are in $\mathbb{F}_{2^{2n}}$.*

(2) *The equation $x^3 + ax + b = 0$, with $a, b \in \mathbb{F}_{2^n}$, $b \neq 0$, has, denoting by t_1, t_2 for the roots of $t^2 + bt + a^3 = 0$ (note that these are in $\mathbb{F}_{2^n}$ or $\mathbb{F}_{2^{2n}}$, see above):*

   (i) *three solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) = \mathrm{Tr}_1^n(1)$ and t_1, t_2 are cubes in $\mathbb{F}_{2^n}$ for n even, and in $\mathbb{F}_{2^{2n}}$ for n odd;*

   (ii) *a unique solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) \neq \mathrm{Tr}_1^n(1)$;*

   (iii) *no solutions in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n(a^3/b^2) = \mathrm{Tr}_1^n(1)$ and t_1, t_2 are not cubes in $\mathbb{F}_{2^n}$ for n even, respectively, $\mathbb{F}_{2^{2n}}$ for n odd.*

A construction proposed in [21] designed to construct differentially 4-uniform permutations that involves swapping two outputs of a given (n, n)-function, has been the subject of many papers since then (see [6, 16, 17, 18, 22], to cite just a few works; a generalization allowing the modification of any two output values, of which swapping is a special case, is investigated in [12]). This naturally leads to the question of how swapping two outputs of a given function F would affect its pAPN-spectrum. We now describe the Janwa-Wilson-Rodier equation for an (n, n)-function F with two output points swapped. More precisely, given two points $x_0 \neq x_1$ in $\mathbb{F}_{2^n}$, we let $G_{x_0x_1}$ be the $\{x_0, x_1\}$-swapping of F defined by

$$G_{x_0x_1}(x) = F(x) + \left((x + x_0)^{2^n-1} + (x + x_1)^{2^n-1}\right)(y_0 + y_1), \tag{3}$$

where $y_0 = F(x_0), y_1 = F(x_1)$. We will sometimes denote $G_{x_0x_1}$ simply by G if there is no danger of confusion.

Note that $x^{2^n-1} = 1$ in $\mathbb{F}_{2^n}$ unless $x = 0$, and so for any $x, y \in \mathbb{F}_{2^n}$, the expression $(x + y)^{2^n-1}$ is equal to 1 if $x \neq y$ and is equal to 0 if $x = y$.

The Janwa-Wilson-Rodier equation of $G = G_{x_0x_1}$ at $\zeta \in \mathbb{F}_{2^n}$ becomes

$$\begin{aligned} 0 &= G(\zeta) + G(x) + G(y) + G(x + y + \zeta) = F(\zeta) + F(x) + F(y) + F(x + y + \zeta) \\ &+ \left((\zeta + x_0)^{2^n-1} + (\zeta + x_1)^{2^n-1} + (x + x_0)^{2^n-1} + (x + x_1)^{2^n-1} + (y + x_0)^{2^n-1}\right. \\ &\left.+(y + x_1)^{2^n-1} + (x + y + \zeta + x_0)^{2^n-1} + (x + y + \zeta + x_1)^{2^n-1}\right)(y_0 + y_1). \end{aligned} \tag{4}$$

We consider several cases depending on the value of ζ:

- If $\zeta = x_0$, then (4) becomes (for $x \neq \zeta \neq y \neq x$)

$$\begin{aligned} 0 &= F(x_0) + F(x) + F(y) + F(x + y + x_0) \\ &\quad + \left((x + x_1)^{2^n-1} + (y + x_1)^{2^n-1} + (x + y + x_0 + x_1)^{2^n-1}\right)(y_0 + y_1). \end{aligned} \tag{5}$$

- If $\zeta = x_1$, then (4) becomes (for $x \neq \zeta \neq y \neq x$)

$$\begin{aligned} 0 = &F(x_1) + F(x) + F(y) + F(x+y+x_1) \\ &+ \left((x+x_0)^{2^n-1} + (y+x_0)^{2^n-1} + (x+y+x_0+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{6}$$

- If $x_0 \neq \zeta \neq x_1$, then (4) becomes (for $x \neq \zeta \neq y \neq x$)

$$\begin{aligned} 0 = &F(\zeta) + F(x) + F(y) + F(x+y+\zeta) \\ &+ \left((x+x_0)^{2^n-1} + (x+x_1)^{2^n-1} + (y+x_0)^{2^n-1}\right. \\ &\left.+(y+x_1)^{2^n-1} + (x+y+\zeta+x_0)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\right)(y_0+y_1). \end{aligned} \tag{7}$$

We shall be referring to Equations (5)–(7) throughout the paper.

When studying how swapping outputs affects the pAPN-spectrum, we do not restrict ourselves to APN functions and often drop the conditions on the parameters in the definition of the infinite families; for example, in our experimental results for the Gold functions in Table 6, we consider all functions of the form x^{2^i+1} over $\mathbb{F}_{2^n}$ regardless of the value of $\gcd(i,n)$. In a number of cases, the functions in question are not APN, but are still differentially two-valued, i.e., there is a positive integer $s > 1$ such that all non-zero derivatives of these functions are 2^s-to-1. While such a function is clearly not ζ-APN for any $\zeta \in \mathbb{F}_{2^n}$, it is also easy to see that swapping two of its outputs will always result in an empty pAPN-spectrum. The following proposition therefore allows us to eliminate some trivial cases.

Proposition 3. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be such that $\Delta_F(a,b) \geq 4$ whenever $\Delta_F(a,b) \neq 0$. Then F has an empty pAPN-spectrum. Furthermore, for any $x_0, x_1 \in \mathbb{F}_{2^n}$, the pAPN-spectrum of the $\{x_0,x_1\}$-swapping $G_{x_0x_1}$, as defined in (3), is also empty.*

Proof. We use the fact that a function F is ζ-APN if and only if the equation $D_aF(\zeta) = D_aF(x)$ only has the trivial solutions $x = \zeta$ and $x = a+\zeta$ for any $a \in \mathbb{F}_{2^n}^*$. Since $\Delta_F(a, D_aF(\zeta)) \geq 4$ for any $a \in \mathbb{F}_{2^n}^*$ and any $\zeta \in \mathbb{F}_{2^n}$ by the hypothesis, it is clear that F cannot be ζ-APN for any ζ.

Suppose now that $x_0, x_1 \in \mathbb{F}_{2^n}$, and $G = G_{x_0x_1}$ is obtained by swapping the outputs of F at x_0 and x_1. Consider some $\zeta \in \mathbb{F}_{2^n}$. Let $a, b \in \mathbb{F}_{2^n}$ be such that $x_0 = \zeta + a$ and $x_1 = \zeta + b$. First, suppose that $ab = 0$, say $a = 0$. Then

$$D_bG(\zeta) = G(\zeta) + G(\zeta+b) = F(\zeta+b) + F(\zeta) = D_bF(\zeta).$$

Since $\Delta_F(b, D_bF(\zeta)) \geq 4$, there must be some $w \in \mathbb{F}_{2^n}$ such that $D_bF(w) = D_bF(\zeta)$ and $w \neq \zeta, \zeta+b$. Thus $\{x_0,x_1\} \cap \{w, b+w\} = \emptyset$ and hence

$$D_bG(w) = D_bF(w) = D_bF(\zeta) = D_bG(\zeta),$$

showing that G is not ζ-APN.

Suppose now that $ab \neq 0$, and let $c = a+b$. We then have

$$D_cG(\zeta) = G(\zeta) + G(\zeta+a+b) = F(\zeta) + F(\zeta+a+b) = D_cF(\zeta)$$

due to $\{x_0, x_1\} \cap \{\zeta, \zeta + a + b\} = \emptyset$. Since $\Delta_F(c, D_cF(\zeta)) \geq 4$, we can find $w \in \mathbb{F}_{2^n}$ with $D_cF(w) = D_cF(\zeta)$ and $w \neq \zeta, \zeta + a + b$. Suppose now that $x_0 = \zeta + a = w$. Then $x_1 = \zeta + b = w + a + b = w + c$. Thus, $\{x_0, x_1\}$ and $\{w, w + c\}$ are either identical or disjoint. In both cases, we have

$$D_cG(w) = D_cF(w) = D_cF(\zeta) = D_cG(\zeta),$$

witnessing that G is not ζ-APN. $\square$

3 The pAPN property for the inverse function swapped at two outputs

In this section, we discuss the pAPN property for the inverse function swapped at two outputs, and we completely characterize the cases in which the resulting function has an empty pAPN-spectrum. We recall that the inverse function is APN over $\mathbb{F}_{2^n}$ for odd values of n, and is differentially 4-uniform for even values of n [15]; by Proposition 3, it then has an empty pAPN-spectrum in the even case.

Theorem 4. *Let $F(x) = x^{2^n-2}$ be the inverse function on $\mathbb{F}_{2^n}$ and let $G_{x_0x_1}$ be the $\{x_0, x_1\}$-swapping of F for some $x_0, x_1 \in \mathbb{F}_{2^n}$ with $x_0 \neq x_1$. If n is odd, then:*

- *(i) If $x_0x_1 = 0$, then $G_{x_0x_1}$ is not ζ-APN for any $\zeta \in \mathbb{F}_{2^n}$.*
- *(ii) If $x_0x_1 \neq 0$, then $G_{x_0x_1}$ is not ζ-APN for $\zeta \in \{x_0, x_1\}$, and is 0-APN if and only if $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 1$. Furthermore, if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$, $G_{x_0x_1}$ is not ζ-APN for the solutions of $\zeta^2 + x_0\zeta + x_0x_1 = 0$, and, if $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 0$, $G_{x_0x_1}$ is not ζ-APN for the solutions of the equation $\zeta^2 + x_1\zeta + x_0x_1 = 0$ (note that, if the trace is 1, there are no solutions). Furthermore, $G_{x_0x_1}$ is not ζ-APN if $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_1+\zeta)(x_0+\zeta)^2}\right) = 0$, or $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_0+\zeta)(x_1+\zeta)^2}\right) = 0$. Otherwise, $G_{x_0x_1}$ is ζ-APN.*

If n is even (we let ω is a primitive element of $\mathbb{F}_4$), then:

- *(i) If $x_0 = 0$, then G_{0x_1} is not x_1-APN, and, for $\zeta \neq x_1$, G_{0x_1} is ζ-APN if and only if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)\left(= \mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right)\right) = 1$ and $\zeta \neq x_1\omega, x_1\omega^2$.*
- *(ii) If $x_0x_1 \neq 0$, then, $G_{x_0x_1}$ is not ζ-APN for $\zeta \notin \{\omega x_0, \omega x_1, \omega^2 x_0, \omega^2 x_1\}$. Furthermore, for those values of ζ, $G_{x_0x_1}$ is not ζ-APN if $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_1+\zeta)(x_0+\zeta)^2}\right) = 0$, or $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_0+\zeta)(x_1+\zeta)^2}\right) = 0$. Otherwise, $G_{x_0x_1}$ is ζ-APN.*

Proof. In the following, we will write G as shorthand for G_{x_0,x_1}.

We first examine the case when $x_0 = 0$. Let ζ be an arbitrary element of $\mathbb{F}_{2^n}$, and consider the Janwa-Wilson-Rodier equation for G at ζ. We distinguish three subcases, namely $\zeta = 0$, $\zeta = x_1$, and $\zeta \neq 0, x_1$, which we treat next.

Suppose first that $\zeta = 0$. We then work under the assumption $xy(x+y) \neq 0$, and obtain from (5)

$$\begin{aligned} 0 =& F(x) + F(y) + F(x+y) + \left((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_1)^{2^n-1}\right) y_1 \\ =& x^{2^n-2} + y^{2^n-2} + (x+y)^{2^n-2} \\ &\qquad + \left((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_1)^{2^n-1}\right) y_1. \end{aligned}$$

Taking x such that $x \neq 0, x_1$ and letting $y = x + x_1$, we get $x^{2^n-2} + (x+x_1)^{2^n-2} + x_1^{2^n-2} = 0$. Multiplying both sides by $x_1 x(x+x_1)$ renders $x^2 + x x_1 + x_1^2 = 0$, which, by Theorem 2, has two solutions if and only if $\mathrm{Tr}_1^n(x_1^2/x_1^2) = \mathrm{Tr}_1^n(1) = 0$, and that is true if and only if n is even. These solutions are $x = \omega x_1, \omega^2 x_1$ (where ω be a primitive element of $\mathbb{F}_4$), which are always nontrivial. Therefore, G cannot be 0-APN when n is even.

If n is odd, then we take $x, y \in \mathbb{F}_{2^n}$ such that $x \neq 0, y, x_1, x_1 + y$ and $y \neq x_1$, and Equation (5) becomes

$$F(x_1) + F(x) + F(y) + F(x+y) = 0,$$

that is,

$$x^2 y + x y^2 + x_1 y^2 + x_1 x^2 + x y x_1 = 0,$$

and taking an arbitrary $a \neq 0, 1$, we see that the pair $x = x_1\left(1 + \frac{1}{a^2+a}\right)$, $y = x_1\left(a + \frac{1}{a+1}\right)$ is a solution to the above equation. We now argue that $xy \neq 0$ and $x \neq y$. Both of these conditions are equivalent to the equation $a^2 + a + 1 = 0$ having no solutions in $\mathbb{F}_{2^n}$, which is true since n is odd and $a^2 + a = 1$ would imply $\mathrm{Tr}_1^n(a^2 + a) = \mathrm{Tr}_1^n(1)$. Next, we verify that $y \neq x + x_1$. Assuming that $y = x + x_1$ leads to $a^3 + a^2 + a + 1 = (a+1)^3 = 0$, which is impossible by the choice of a. Thus, G is not 0-APN when n is odd.

We now consider the case of $x_0 = 0, \zeta = x_1$ (for any n, odd or even). Equation (6) transforms into

$$0 = F(x_1) + F(x) + F(y) + F(x+y+x_1) + \left(x^{2^n-1} + y^{2^n-1} + (x+y+x_1)^{2^n-1}\right) y_1. \quad (8)$$

Let $x, y, a \in \mathbb{F}_{2^n}$ be such that $x \neq y = ax \neq 0$ (thus, $a \neq 0, 1$) and $x \neq x_1(a+1)^{-1}$ (so that $y \neq x + x_1$). Then (8) becomes

$$\begin{aligned} 0 &= x_1^{2^n-2} + x^{2^n-2} + y^{2^n-2} + (x+y+x_1)^{2^n-2} + y_1 \\ &= x^{2^n-2} + y^{2^n-2} + (x+y+x_1)^{2^n-2}, \end{aligned}$$

which is equivalent to $0 = x^2 + y^2 + xy + x_1(x+y) = x^2(a^2+a+1) + x_1 x(a+1)$, rendering the solution $x = x_1(a+1)(a^2+a+1)^{-1}$ (taking $a \neq \omega, \omega^2$ for n even, with no restrictions for n odd as we have $a^2 + a + 1 \neq 0$) . It is easy to see that neither x nor ax can be equal to x_1, and so G is not x_1-APN.
Finally, given $x_0 = 0$, we consider the case of $\zeta \neq 0, x_1$. Then, equation (7) becomes

$$\begin{aligned} 0 &= F(\zeta) + F(x) + F(y) + F(x+y+\zeta) \\ &\quad + \left(x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1} + (y+x_1)^{2^n-1}\right. \end{aligned} \quad (9)$$

$$+(x+y+\zeta)^{2^n-1}+(x+y+\zeta+x_1)^{2^n-1}\big)\,y_1.$$

We now assume that G is ζ-APN, and so (9) has only trivial solutions. Take $y=0$ and $x_1+\zeta\neq x\neq x_1$ in (9). We get $\zeta^{-1}+x^{-1}+(x+\zeta)^{-1}+y_1=0$, which is equivalent to $x^2(1+y_1\zeta)+x\zeta(1+y_1\zeta)+\zeta^2=0$, and moreover (with $y_1=1/x_1$), $x^2+x\zeta+\frac{\zeta^2 x_1}{x_1+\zeta}=0$. By Theorem 2 this equation has no solutions if and only if

$$\mathrm{Tr}_1^n\left(\frac{\frac{\zeta^2 x_1}{x_1+\zeta}}{\zeta^2}\right)=\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=1. \tag{10}$$

Now, take $0\neq y=x_1\neq x\neq 0$ in (9), as well as $x\neq x_1+\zeta$, $x\neq\zeta$. We get $\zeta^{-1}+x^{-1}+(x+x_1+\zeta)^{-1}=0$, which is equivalent to $x^2+x(x_1+\zeta)+x_1\zeta+\zeta^2=0$, which has no solutions if and only if

$$\mathrm{Tr}_1^n\left(\frac{\zeta(x_1+\zeta)}{(x_1+\zeta)^2}\right)=\mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right)=1. \tag{11}$$

Now, put together the conditions from equations (10) and (11). We obtain

$$0=\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)+\mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right)=\mathrm{Tr}_1^n(1).$$

When n is odd, we have $\mathrm{Tr}_1^n(1)=1$. We obtain a contradiction, and therefore, G cannot be ζ-APN for n odd.

For n even, the conditions from equations (10) and (11) are equivalent, since $\mathrm{Tr}_1^n(1)=0$, and $\frac{x_1}{x_1+\zeta}+\frac{\zeta}{x_1+\zeta}=1$. Therefore, when n is even and $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=0$, the function G is not ζ-APN. Assume now $\zeta\neq 0,x_1$, and $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=\mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right)=1$. Let first $y=0$. Then, Equation (9) becomes

$$0=\zeta^{-1}+x^{-1}+(x+\zeta)^{-1}+\left((x+x_1)^{2^n-1}+1+(x+\zeta+x_1)^{2^n-1}\right)y_1.$$

Taking $x=x_1$ or $x=\zeta+x_1$, we obtain the equation

$$0=\zeta^{-1}+x_1^{-1}+(x_1+\zeta)^{-1},\ \text{that is, } 0=\zeta^2+x_1\zeta+x_1^2,$$

and so we can see that G is not ζ-APN for the two solutions of $\zeta^2+x_1\zeta+x_1^2=0$, namely $\zeta_0=x_1\omega$ and $\zeta_1=x_1\omega^2$, where ω is a primitive element of $\mathbb{F}_4$. In these two cases, if $n\equiv 0 \pmod 4$, then $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=0$, leading to a contradiction. If $n\equiv 2 \pmod 4$, then $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)=1$, and thus these are valid solutions of Equation (9). Combining these facts, we see that G is not ζ-APN in this case if $\zeta=x_1\omega$ or $\zeta=x_1\omega^2$.

Taking $x\neq x_1,\zeta+x_1$, we obtain the equation

$$0=\zeta^{-1}+x^{-1}+(x+\zeta)^{-1}+x_1^{-1},\ \text{that is, } 0=x^2+\zeta x+\frac{\zeta^2 x_1}{x_1+\zeta},$$

which does not have solutions since $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) = 1$.

Let now $xy \neq 0$. Assume that $\zeta \notin \{0, x_1, x_1\omega, x_1\omega^2\}$, and $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) = \mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right) = 1$, since in the other cases we have shown that G is not ζ-APN. Equation (9) becomes

$$\begin{aligned}0 = \zeta^{-1} + x^{-1} + y^{-1} + F(x+y+\zeta) + \big((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} \\ +(x+y+\zeta)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\big)\, y_1.\end{aligned}$$

If $y = x+\zeta$, and excluding the trivial solutions $x, y = \zeta$, we see that, in the cases $x = x_1, x_1+\zeta$, we obtain the equation

$$0 = \zeta^{-1} + x_1^{-1} + (x_1+\zeta)^{-1},$$

which has only the solutions $\zeta_0 = x_1\omega$ and $\zeta_1 = x_1\omega^2$, which we have excluded.

If $x \neq x_1, \zeta + x_1$, we obtain the equation

$$0 = \zeta^{-1} + x^{-1} + (x+\zeta)^{-1} + x_1^{-1},$$

which has as we have seen no solutions since $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right) = 1$.

If $y \neq x+\zeta$, we consider the following cases: if $x = x_1$ or $x = y+\zeta+x_1$, the equation above becomes

$$0 = \zeta^{-1} + y^{-1} + (x_1+y+\zeta)^{-1},$$

which is equivalent to

$$0 = y^2 + y(x_1+\zeta) + \zeta(\zeta+x_1),$$

which has no solutions since $\mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right) = 1$. If $x \neq x_1, y+\zeta+x_1$ ($y \neq x_1, x+\zeta+x_1$), the equation above becomes

$$0 = \zeta^{-1} + x^{-1} + y^{-1} + (x+y+\zeta)^{-1},$$

which, taking $y = x+a,\ a \neq 0, \zeta+x_1$, is equivalent to

$$0 = x^2 + ax + \zeta(a+\zeta),$$

which only has the trivial solutions $x = \zeta, x = \zeta+a$.

Therefore, G is ζ-APN if and only if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_1+\zeta}\right)\left(= \mathrm{Tr}_1^n\left(\frac{\zeta}{x_1+\zeta}\right)\right) = 1$.

We now turn to the case when $x_0x_1 \neq 0$. We first assume that $\zeta = 0$. Then, suppose $x = x_0$. Equation (7) becomes

$$0 = x_0^{-1} + y^{-1} + (y+x_0)^{-1} + \left(1 + (y+x_1)^{2^n-1} + (y+x_0+x_1)^{2^n-1}\right)\left(x_0^{-1} + x_1^{-1}\right).$$

If $y = x_1$, this equation becomes $x_0^{-1} + x_1^{-1} + (x_1+x_0)^{-1} = 0$, which is equivalent to $x_1^2 + x_0x_1 + x_0^2 = 0$, and this has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{x_0^2}{x_0^2}\right) = \mathrm{Tr}_1^n(1) = 0$, which holds if n is even. Note that these solutions are $x_1 = \omega x_1, \omega^2 x_0$, so, in these two cases, G is not 0-APN.

If $x = x_0$, $y \neq x_1$, we have the options $y = x_0 + x_1$, which gives the same equation as $y = x_1$, or $y \neq x_0 + x_1$, which renders

$$0 = y^{-1} + (y + x_0)^{-1} + x_1^{-1}.$$

This equation is equivalent to $y^2 + x_0 y + x_0 x_1 = 0$, which has solutions y if and only if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$.

The case $x = x_1$ is symmetrical. Now, suppose $x, y \neq x_0, x_1$. Take $y \neq x + x_0, x + x_1$. Then, (5) becomes

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

which is equivalent (taking $y = \alpha x$, $\alpha \neq 0, 1$) to

$$x(1 + \alpha + \alpha^2) = 0$$

which has a solution if and only if n is even (note that the existence of solutions is independent of the values of x_0 and x_1, and that we can choose x so that the conditions $x, y \neq x_0, x_1$ and $y \neq x + x_0, x + x_1$ are satisfied). Hence, G is never 0-APN if n is even.

It only remains to investigate the cases $y \neq x + x_0$ or $y = x + x_1$ (with $x, y \neq x_0, x_1$) for n odd. However, these cases yield the same conditions $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 1$.

Hence, G is 0-APN in the odd case if and only if $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 1$, and is never 0-APN in the even case.

Let now $\zeta \neq 0$. We examine two subcases, depending on whether ζ is one of x_0, x_1 or not.

We first assume that $\zeta = x_0$ (the case when $\zeta = x_1$ is treated in a similar manner). Then equation (5) becomes

$$\begin{aligned} 0 &= x_0^{2^n-2} + x^{2^n-2} + y^{2^n-2} + (x + y + x_0)^{2^n-2} \\ &\quad + \left((x + x_1)^{2^n-1} + (y + x_1)^{2^n-1} + (x + y + x_0 + x_1)^{2^n-1}\right)\left(x_0^{2^n-2} + x_1^{2^n-2}\right). \end{aligned} \tag{12}$$

Note that, if one of the terms in the parenthesized expression equals 1, then (discarding the cases corresponding to trivial solutions) the latter vanishes. We consider the following cases:

- $y = x_1$ and $x = x_0$ immediately implies the trivial solution $x = \zeta$.
- $y = x_1$ and $x \neq x_0$. Equation (12), taking $x \neq 0, x_0 + x_1$, reduces to $0 = x_0^{2^n-2} + x^{2^n-2} + x_1^{2^n-2} + (x + x_1 + x_0)^{2^n-2}$, which is equivalent to $x^2 + (x_0 + x_1)x + x_0 x_1 = 0$, leading to the trivial solutions $x = x_0, x_1$. If we take $x = 0$ or $x = x_0 + x_1$, the equation $x_0^{-1} + x_1^{-1} + (x_0 + x_1)^{-1} = 0$, which is equivalent to $x_0^2 + x_0 x_1 + x_1^2 = 0$, which has solutions $x_1 = \omega x_0, \omega^2 x_1$ if n is even, and no solutions if n is odd. So, if n is even, and $x_1 = \omega x_0, \omega^2 x_1$, G is not x_0-APN.
- $y = x_0$ and $x \neq x_1$. Equivalent to the previous case.

- $y = x_0$ and $x = x_1$ immediately implies the trivial solution $y = \zeta$.
- $x, y \neq x_0, x_1$ but $y = x + x_0 + x_1$. Equation (12), taking $x \neq 0, x_0 + x_1$, reduces to

$$0 = x_0^{2^n-2} + x^{2^n-2} + (x + x_0 + x_1)^{2^n-2} + x_1^{2^n-2},$$

  which is equivalent to $x_0^2 + (x_0 + x_1)x + x_0x_1 = 0$, which only has trivial solutions. Taking $x = 0$ or $x = x_0 + x_1$, we obtain as before that, if n is even, and $x_1 = \omega x_0, \omega^2 x_1$, G is not x_0-APN.

- $x, y \neq x_0, x_1$, $y \neq x + x_0 + x_1$. The equation above is then

$$\begin{aligned} 0 &= x_0^{2^n-2} + x^{2^n-2} + y^{2^n-2} + (x + y + x_0)^{2^n-2} + x_0^{2^n-2} + x_1^{2^n-2} \\ &= x^{2^n-2} + y^{2^n-2} + (x + y + x_0)^{2^n-2} + x_1^{2^n-2}. \end{aligned} \tag{13}$$

  Taking $x = 0$, equation (13) reduces to

$$0 = y^{2^n-2} + (y + x_0)^{2^n-2} + x_1^{2^n-2},$$

  which is equivalent to $y^2 + yx_0 + x_0x_1 = 0$, which has solutions in y if and only if $\mathrm{Tr}_1^n\left(\frac{x_0x_1}{x_0^2}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$. In this case, notice that $y = x_0$ is not a solution, so that we can conclude that, if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$, the function is not x_0-APN.

  If $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) \neq 0$, we consider the case $x \neq 0$ (similarly, $y \neq 0$). Taking $y = x + x_0$, then Equation (13) reduces to

$$0 = x^{-1} + (x + x_0)^{-1} + x_1^{-1},$$

  and further to $0 = x^2 + x_0x + x_0x_1$, which does not have solutions since we have assumed $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) \neq 0$.

  Taking $y \neq x + x_0$, we can write $y = x + a$, $a \neq 0, x_0, x_0 + x_1$. Then, Equation (13) reduces to

$$0 = x^{-1} + (x + a)^{-1} + (a + x_0)^{-1} + x_1^{-1},$$

  which is equivalent to $0 = x^2 + ax + \frac{a(a+x_0)x_1}{a+x_0+x_1}$ (recall that $y \neq x + x_0 + x_1$, that is, $a + x_0 + x_1 \neq 0$). Thus, the previous equation has solutions a if and only if $\mathrm{Tr}_1^n\left(\frac{(a+x_0)x_1}{a(a+x_0+x_1)}\right) = 0$. If n is odd, we can take $a = x_1$, since in that case, the trace becomes $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0} + 1\right) = 0$, which holds by our assumption (note that, by inspection, the solutions are nontrivial). We now assume that n is even. With $\alpha = x_0/x_1$ (recall that $\mathrm{Tr}_1^n(1/\alpha) = 1$), we write the expression inside the trace as

$$\frac{(a + x_0)x_1}{a(a + x_0 + x_1)} = \frac{z}{(z + 1)(\alpha z + 1)},$$

where $z = x_1/(a+x_0)$. If $\mathrm{Tr}_1^n\left(\frac{1}{1+\alpha}\right) = 0$, taking $z = \alpha^{-1/2}$, we get that the trace satisfies $\mathrm{Tr}_1^n\left(\frac{z}{(z+1)(\alpha z+1)}\right) = \mathrm{Tr}_1^n\left(\frac{1}{\alpha+1}\right) = 0$. If $\mathrm{Tr}_1^n\left(\frac{1}{1+\alpha}\right) = 1$, then we write

$$\frac{(a+x_0)x_1}{a(a+x_0+x_1)} = \frac{x_1}{a} + \frac{x_1^2}{a(a+x_0+x_1)}.$$

Thus, $\mathrm{Tr}_1^n\left(\frac{(a+x_0)x_1}{a(a+x_0+x_1)}\right) = \mathrm{Tr}_1^n\left(\frac{x_1}{a} + \frac{x_1^2}{a(a+x_0+x_1)}\right) = \mathrm{Tr}_1^n\left(\frac{x_1^2}{a^2} + \frac{x_1^2}{a(a+x_0+x_1)}\right)$. Under $\mathrm{Tr}_1^n\left(\frac{1}{1+\alpha}\right) = 1$, we look for a value of a such that $\left(\frac{x_1^2}{a^2}\right)^2 = \frac{x_1^2}{a(a+x_0+x_1)}$ (thus, the above trace is 0). That will happen if and only if $\left(\frac{a}{x_1}\right)^3 + \left(\frac{a}{x_1}\right) + \frac{x_0}{x_1} + 1 = 0$. With $z = \frac{a}{x_1}$, by Theorem 2, the equation $z^3 + z + \alpha + 1 = 0$ has three solutions or no solution in $\mathbb{F}_{2^n}$ if and only if $\mathrm{Tr}_1^n\left(\frac{1}{(1+\alpha)^2}\right) = \mathrm{Tr}_1^n\left(\frac{1}{1+\alpha}\right) = \mathrm{Tr}_1^n(1) = 0$, since n is even, along with some conditions on the roots of an associated quadratic, or a unique solution if $\mathrm{Tr}_1^n\left(\frac{1}{1+\alpha}\right) \neq \mathrm{Tr}_1^n(1) = 0$, which always happens by our assumption. Thus, there exists a such that $\mathrm{Tr}_1^n\left(\frac{(a+x_0)x_1}{a(a+x_0+x_1)}\right) = 0$. Note that the solutions of the Janwa-Wilson-Rodier equation are nontrivial.

Therefore, for any n, G is not x_0-APN, regardless of $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right)$. By symmetry, G is not x_1-APN.

Consider now the case of $\zeta \neq x_0, x_1, 0$. Assume first that $xy \neq 0$. Then, we can write $x = \beta\zeta$, and $y = \alpha\zeta$, with $\alpha, \beta \neq 0, 1$ and $\alpha \neq \beta$. Equation (7) then becomes

$$0 = \zeta^{2^n-2}(1 + \alpha^{2^n-2} + \beta^{2^n-2} + (1+\alpha+\beta)^{2^n-2}) + P(x_0^{2^n-2} + x_1^{2n-2}),$$

where $P = (x+x_0)^{2^n-1} + (x+x_1)^{2^n-1} + (y+x_0)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+\zeta+x_0)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}$. Assume that $P = 0$ (which can be achieved, for instance, if all the parenthesized expressions in P are different from zero). The equation becomes

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

which, since $\zeta \neq 0$, is equivalent to

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

which, assuming $1+\alpha+\beta \neq 0$, and multiplying both sides by $\alpha\beta(1+\alpha+\beta)$, becomes

$$\begin{aligned} 0 &= \alpha\beta(1+\alpha+\beta) + \beta(1+\alpha+\beta) + \alpha(1+\alpha+\beta) + \alpha\beta \\ &= \alpha\beta + \alpha^2\beta + \alpha\beta^2 + \beta + \alpha\beta + \beta^2 + \alpha + \alpha^2 + \alpha\beta + \alpha\beta \\ &= \alpha + \alpha^2 + \beta + \beta^2 + \alpha^2\beta + \alpha\beta^2. \end{aligned}$$

Writing $\beta = \gamma\alpha$, with $\gamma \neq 0, 1, \frac{1}{\alpha}$, the equation above becomes

$$0 = \alpha + \alpha^2 + \gamma\alpha + \gamma^2\alpha^2 + \gamma\alpha^3 + \gamma^2\alpha^3 = \alpha(1+\gamma)(\gamma\alpha^2 + (1+\gamma)\alpha + 1).$$

Since $\alpha \neq 0, \gamma \neq 1$, we obtain the equivalent equation

$$\alpha^2 + \frac{1+\gamma}{\gamma}\alpha + \frac{1}{\gamma} = 0,$$

which has as only solutions $\alpha = 1, \frac{1}{\gamma}$, which are not valid.

We need then to assume that $P = 0$ and $1 + \alpha + \beta = 0$, or that $P = 1$. If $P = 0$ and $1 + \alpha + \beta = 0$, the equation becomes

$$0 = \zeta^{2^n-2}(1 + \alpha^{-1} + (1+\alpha)^{-1}),$$

which is equivalent to $\alpha^2 + \alpha + 1 = 0$, which has solutions $\alpha = \omega, \omega^2$ (where $\omega, \omega^2 \in \mathbb{F}_4$ are the solutions of $x^2 + x + 1 = 0$) if and only if n is even. In the case n odd, then, there are no solutions, and in the case n even, these solutions are nontrivial as long as $P = 0$, i.e., as long as either $\zeta \neq \omega x_0, \omega^2 x_0, \omega x_1, \omega^2 x_1$, or, if $\zeta = \omega x_0$, then $x_1 = \omega^2 x_0$, or, if $\zeta = \omega x_1$, then $x_0 = \omega^2 x_1$, or, if $\zeta = \omega^2 x_0$, then $x_1 = \omega x_0$, or, if $\zeta = \omega^2 x_1$, then $x_0 = \omega x_1$. In those cases, G is not ζ-APN.

If $P = 1$, an odd number of terms in the parenthesis must be zero. Taking $x = x_0$ and $y = 0$, $P = 1$ if and only if $\zeta = x_0 + x_1$. Then, the equation becomes $0 = (x_0 + x_1)^{-1}$, rendering trivial solutions.

Now, let $P = 1$, and consider $x = x_0$ and $y \neq 0$. If $\zeta = x_0 + x_1$, then, $P = 1$ if and only if $y = x_1$, rendering only trivial solutions.

Let $\zeta \notin \{x_0 + x_1, x_0, x_1\}$. Taking $x = x_0$ and $y \neq 0$, we see that $P = 1$ if and only if (to produce valid solutions) $y = x_1$ or $y = \zeta + x_0 + x_1$, or $y \neq x_1, \zeta + x_0 + x_1$. The first two cases yield only trivial solutions. Let $y = x_0 + \zeta$. Then, the equation becomes $0 = \zeta^{-1} + (x_0 + \zeta)^{-1} + x_1^{-1}$, which is equivalent to $\zeta^2 + x_0\zeta + x_0x_1 = 0$, which has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$. In that case, G is not ζ-APN for the solutions ζ_0, ζ_1 of this equation. By symmetry, if $\mathrm{Tr}_1^n\left(\frac{x_0}{x_1}\right) = 0$, G is not ζ-APN for the solutions ζ_0, ζ_1 of the equation $\zeta^2 + x_1\zeta + x_0x_1 = 0$.

Let now $x = x_0$ and $y \notin \{0, x_0, x_1, \zeta, \zeta + x_0 + x_1\}$. The equation is then

$$0 = \zeta^{-1} + y^{-1} + (y + x_0 + \zeta)^{-1} + x_1^{-1},$$

which, taking $y = \zeta + a$, where $a \notin \{0, x_0, \zeta + x_0, \zeta + x_1, x_0 + x_1\}$ (note that we were assuming $\zeta \neq x_1$), is equivalent to

$$a^2 + a(x_0 + \zeta) + \frac{\zeta^2(x_0 + x_1)}{x_1 + \zeta} = 0,$$

which has solutions a if either $\zeta = x_0$ and so, $a = \zeta$, which is not permissible, or $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_1+\zeta)(x_0+\zeta)^2}\right) = 0$. Hence G is not ζ-APN, under this last trace condition. By symmetry, if $\mathrm{Tr}_1^n\left(\frac{(x_0+x_1)\zeta^2}{(x_0+\zeta)(x_1+\zeta)^2}\right) = 0$, G is also not ζ-APN.

Take now again $P = 1$ but $x \neq x_0$, and, by symmetry, $x \neq x_1$ and $y \neq x_0x_1$. Then, $P = 1$ if and only if $y = x + \zeta + x_0$ or $y = x + \zeta + x_1$. Taking $y = x + \zeta + x_0$, and writing $x = \zeta + a$, where $a \neq 0, x_0 + x_1, \zeta + x_0, \zeta + x_1$, the equation is

$$0 = \zeta^{-1} + (\zeta + a)^{-1} + (a + x_0)^{-1} + x_1^{-1},$$

which we have already handled.

Finally, let $\zeta \neq x_0, x_1, 0$ and take $x = 0$. We can write $y = \alpha\zeta$, with $\alpha \neq 0, 1$. Then Equation (7) becomes

$$0 = \zeta^{2^n-2}(1 + \alpha^{2^n-2} + (1 + \alpha)^{2^n-2}) + P(x_0^{2^n-2} + x_1^{2n-2}),$$

where $P = (\alpha\zeta + x_0)^{2^n-1} + (\alpha\zeta + x_1)^{2^n-1} + (\zeta(1 + \alpha) + x_0)^{2^n-1} + (\zeta(1 + \alpha) + x_1)^{2^n-1}$.

If $P = 0$, this equation is equivalent to $\zeta(1+\alpha+\alpha^2) = 0$, which has no solutions if n is odd, and has the solutions $\alpha = \omega, \omega^2$ if n is even. These solutions are valid if and only if $P = 0$, i.e. if $\zeta \notin \{\omega x_0, \omega^2 x_0, \omega x_1, \omega^2 x_1\}$, or, if $\zeta = \omega\{x_0, x_1\}$, then $x_1 = \omega^2\{x_0, x_1\}$, or, if $\zeta = \omega^2\{x_0, x_1\}$, then $x_1 = \omega\{x_0, x_1\}$. In these cases, as seen before, G is not ζ-APN.

If $P = 1$, then we must have that $x_0 = \alpha\zeta$, and $x_1 \neq (1 + \alpha)\zeta$, or that $x_1 = \alpha\zeta$, and $x_0 \neq (1 + \alpha)\zeta$. Assume that $x_0 = \alpha\zeta$, and $x_1 \neq (1 + \alpha)\zeta$. Then Equation (7) becomes $0 = \zeta^{-1} + \zeta^{-1}(1+\alpha)^{-1} + x_1^{-1}$ which is equivalent to $\zeta(\zeta(1+\alpha)+\alpha x_1)) = 0$, which, since $\zeta \neq 0, \alpha \neq 1$, is equivalent to $\alpha = \frac{\zeta}{\zeta+x_1}$. Together with $x_0 = \alpha\zeta$ and $x_1 \neq (1 + \alpha)\zeta$, this implies $\zeta^2 + x_0\zeta + x_0x_1 = 0$ and $\zeta \neq x_1 + 1$. A solution exists if and only if $\mathrm{Tr}_1^n\left(\frac{x_1}{x_0}\right) = 0$, and, for those ζ, only if $\zeta \neq x_1+1$. However, in that case, G is not ζ-APN. By symmetry, G is not ζ-APN if $\zeta^2+x_1\zeta+x_0x_1 = 0$ and $\zeta \neq x_0+1$. However, we have already obtained a less restrictive condition, and so this case does not yield anything new.

We can simplify the results for n even and $x_0x_1 \neq 0$; there are two possibilities for the Janwa-Wilson-Rodier equation (7) at ζ. The parenthesized expression is either equal to 0 or to 1.

Consider $\zeta \neq 0$ (the case $\zeta = 0$ was already treated). If the parenthesized expression in (7) is 0, $\zeta \neq x_0, x_1$, and x, $y, x + y + \zeta \neq 0$, then equation (7) transforms into

$$\zeta^{-1} + x^{-1} + y^{-1} + (x + y + \zeta)^{-1} = 0,$$

which is equivalent to $0 = x^2y + xy^2 + x^2\zeta + y^2\zeta + x\zeta^2 + y\zeta^2 = (x + y)(x + \zeta)(y + \zeta)$, rendering trivial solutions.

If the parenthesized expression in (7) is 0, $\zeta \neq x_0, x_1$ and $x = 0$, but $y, y + \zeta \neq 0$, then Equation (7) transforms into

$$\zeta^{-1} + y^{-1} + (y + \zeta)^{-1} = 0,$$

which is equivalent to $0 = y^2 + \zeta y + \zeta^2$, which has solutions if and only if $\mathrm{Tr}_1^n\left(\frac{\zeta^2}{\zeta^2}\right) = \mathrm{Tr}_1^n(1) = 0$, which is always true for n even. These solutions are always nontrivial, since $y = x = 0$ and $y = \zeta$ are never solutions, under $\zeta \neq 0$. These solutions are, of course, only valid if the parenthesised expression evaluates to 0. For $\zeta = x_1 + x_0$, however, this expression is always zero, and so the function cannot be ζ-APN.

Take now $x_1 \neq x_0+\zeta$. We know that $y^2+\zeta y+\zeta^2 = 0$ has exactly two different roots, $y_0 = \zeta\omega$ and $y_1 = \zeta\omega^2$, where ω is a primitive element of $\mathbb{F}_4$. When $y_j = x_k$ for $j, k = 0, 1$ or $y_j = x_k + \zeta$, these solutions are not valid, since then the parenthesized expression is 1. Suppose that $y_0 = x_0$. The equation $x_0^2 + \zeta x_0 + \zeta^2 = 0$ always has solutions in

ζ since n is even and $\mathrm{Tr}_1^n\left(\frac{x_0^2}{x_0^2}\right) = \mathrm{Tr}_1^n(1) = 0$, namely $\zeta_0 = x_0\omega$ and $\zeta_1 = x_0\omega^2$. The other forbidden roots give the values $\zeta_0 = x_1\omega$ and $\zeta_1 = x_1\omega^2$. For these four values, the function G can thus be ζ-APN. For all other values, G is not ζ-APN.

If $\zeta = x_0\omega$, then we consider the following subcases:

- If $x_1 = \omega x_0 = \zeta$, then, taking $y = x + \omega x_0$, Equation 6 becomes

$$0 = (\omega x_0)^{-1} + x^{-1} + (x + \omega x_0)^{-1} + P(x_0^{-1} + (\omega x_0)^{-1}),$$

  where $P = (x+x_0)^{-1} + (y+x_0)^{2^n-1} + 1$, which has the nontrivial solutions $x = x_0$, $y = \omega^2 x_0$ and $y = x_0$, $x = \omega^2 x_0$, implying that G is not ζ-APN in that case.

- A similar analysis can be done for $x_1 = \omega^2 x_0$, or $x_1 \neq \omega x_0 = \zeta$, rendering that G is not ζ-APN under these conditions on ζ.

By symmetry, we obtain a similar result in the case of $y = 0$. If the expression in the parentheses in (7) is 0 and $y = x + \zeta$, but $x \neq 0, \zeta$, then (7) transforms into $\zeta^{-1} + x^{-1} + (x + \zeta)^{-1} = 0$, which is equivalent to $x^2 + \zeta x + \zeta^2 = 0$. We have already handled this equation in the case $x = 0$ above, and we do not get any new information from this.

If the parenthesized expression in (7) is 1, we cannot possibly have $x_0 = x_1 + \zeta$. We must then have that $x = x_0$, or $x = x_1$, or $y = x_0$, or $y = x_1$, or $x + y = \zeta + x_0$, or $x + y = \zeta + x_1$. We take first the case $\zeta \neq x_0, x_1, x_0 + x_1$. If $x = x_0$, then the equation becomes $\zeta^{-1} + x_0^{-1} + y^{-1} + (x_0 + y + \zeta)^{-1} + x_0^{-1} + x_1^{-1} = 0$, which is equivalent to

$$y^2(x_1 + \zeta) + y(\zeta + x_0)(\zeta + x_1) + \zeta x_1(\zeta + x_1) = 0,$$

and that, since $x_1 \neq \zeta$, is equivalent to $y^2 + y(\zeta + x_0) + \zeta x_0 = 0$, that is, $(y+\zeta)(y+x_0) = 0$.

Note that both solutions implied by this equation are invalid, since $y = \zeta$ is one of the trivial solutions, and $y = x_0$ leads to the expression in the parentheses in (7) to evaluate to 0, and hence implies $x = y$, another trivial solution. The other cases also yield trivial solutions.

We now consider $\zeta \in \{x_0, x_1, x_0 + x_1\}$. Suppose that $\zeta = x_0$, and the parenthesized expression in (5) is 1. Then, we have that $x = x_1$, or $y = x_1$, or $x + y = x_0 + x_1$. On inspection, they either yield trivial solutions, or a contradiction. We have then that the function is ζ-APN.

Note that, for n even, for any of the possible values ζ such that G is ζ-APN, namely $\zeta \in \{\omega x_0, \omega^2 x_0, \omega x_1, \omega^2 x_1\}$, there are no nontrivial solutions to the equations $\zeta^2 + x_0\zeta + x_0x_1 = 0$ and $\zeta^2 + x_1\zeta + x_0x_1 = 0$. Therefore the conditions for n even are further simplified. $\square$

To supplement the above discussion, we perform an exhaustive search by going over all pairs $(x_0, x_1) \in \mathbb{F}_{2^n}^2$ and compute the size of the pAPN-spectrum of the (x_0, x_1)-swapping of the inverse function x^{2^n-2} over $\mathbb{F}_{2^n}$ for $4 \leq n \leq 10$. The results are presented in Table 1 below. The sizes of the pAPN-spectra of all (x_0, x_1)-swaps are given in the last column, with multiplicities given in superscript, e.g., the entry 0^{45} for $n = 4$ indicates that the pAPN-spectrum of the (x_0, x_1)-swapping is empty for 45 pairs $\{x_0, x_1\}$. The remaining columns give the exponent d, the differential uniformity of x^{2^n-2} (which is known to be 2, respectively 4 for odd, respectively, even n [15]), and the size of the pAPN-spectrum of x^{2^n-2}. We recall that the pAPN-spectrum of the inverse function over $\mathbb{F}_{2^n}$ is full for odd values of n, and is empty for even values of n by Proposition 3.

For odd dimensions, an empty pAPN-spectrum is obtained precisely in the case of swapping a pair $(x_0, x_1) = (0, x)$ with $0 \neq x \in \mathbb{F}_{2^n}$. In even dimensions, the points (x_0, x_1) whose swap gives an empty spectrum are much more varied, and do not exhibit any clear pattern. However, any swap of the form $(x_0, x_1) = (0, x)$ with $0 \neq x \in \mathbb{F}_{2^n}$ gives a function with a large pAPN-spectrum, e.g. containing 8 elements for $n = 4$, or 30 elements for $n = 6$.

n	d	δ_F	Spectrum	Swapped spectrum
4	7	4	0	$0^{45}, 2^{60}, 8^{15}$
5	15	2	32	0^{31}, 6^{155}, 8^{155}, 9^{155}
6	31	4	0	0^{1197}, 2^{567}, 4^{189}, 30^{63}
7	63	2	128	0^{127}, 26^{889}, 28^{889}, 29^{889}, 30^{889}, 32^{2667}, 35^{889}, 36^{889}
8	127	4	0	0^{19125}, 2^{10200}, 4^{3060}, 128^{255}
9	255	2	512	0^{511}, 116^{4599}, 118^{4599}, 119^{4599}, 120^{6132}, 122^{9198}, 124^{22995}, 125^{4599}, 126^{4599}, 127^{4599}, 128^{9198}, 129^{4599}, 130^{13797}, 131^{4599}, 133^{4599}, 134^{13797}, 135^{4599}, 136^{4599}, 138^{4599}
10	511	4	0	0^{277233}, 2^{230175}, 4^{15345}, 510^{1023}

Table 1: pAPN-spectra of two-point swaps of the inverse function

4 The Gold APN case

A natural question arising from the above investigations is, how does swapping output values affect the other infinite families of APN monomials. In this section, we present our results on the Gold functions.

We will need the following theorem from [14], which shows that a trinomial $z^{p^k} - az - b$ in the finite field $\mathbb{F}_{p^n}$ has either zero, one, or p^g roots, where $g = \gcd(n, k)$. This result was made more explicit by [9].

Theorem 5. *Let p be a prime. Let $f(z) = z^{p^k} - az - b$ in $\mathbb{F}_{p^n}$, $g = \gcd(n, k)$, $m = n/\gcd(n, k)$ and Tr_g be the trace function from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^g}$. For $0 \leq i \leq m - 1$, we define $t_i = \sum_{j=i}^{m-2} p^{n(j+1)}$, $\alpha_0 = a, \beta_0 = b$. If $m > 1$, then, for $1 \leq r \leq m - 1$, we set*

$$\alpha_r = a^{1+p^k+\cdots+p^{kr}} \text{ and } \beta_r = \sum_{i=0}^{r} a^{s_i} b^{p^{ki}},$$

where $s_i = \sum_{j=i}^{r-1} p^{k(j+1)}$, for $0 \leq i \leq r - 1$ and $s_r = 0$. Then:

- *if* $\alpha_{m-1} = 1$ *and* $\beta_{m-1} \neq 0$, *then* f *has no roots in* $\mathbb{F}_{p^n}$*;*
- *if* $\alpha_{m-1} \neq 1$, *then* f *has precisely one root in* $\mathbb{F}_{p^n}$, *namely* $x = \beta_{m-1}/(1-\alpha_{m-1})$*;*
- *if* $\alpha_{m-1} = 1$ *and* $\beta_{m-1} = 0$, *then* f *has precisely* p^g *roots in* $\mathbb{F}_{p^n}$ *given by* $x + \delta\tau$, *where* $\delta \in \mathbb{F}_{p^g}$, τ *is fixed in* $\mathbb{F}_{p^n}$ *with* $\tau^{p^k-1} = a$, *and, for any* $e \in \mathbb{F}_{p^n}^*$ *with* $\mathrm{Tr}_g(e) \neq 0$, *where* $x = \dfrac{1}{\mathrm{Tr}_g(e)} \displaystyle\sum_{i=0}^{m-1} \left(\sum_{j=0}^{i} e^{p^{kj}} \right) a^{t_i} b^{p^{ki}}$.

Theorem 6. *Let* $F(x) = x^{2^k+1}$ *be the Gold function on* $\mathbb{F}_{2^n}$, *where* n *is odd and* $\gcd(k,n) = 1$. *Let* G_{0x_1} *be the* $\{0, x_1\}$*-swapping of* F *for some* $x_1 \in \mathbb{F}_{2^n}^*$. *Then*:

(i) G_{0,x_1} *is not* 0*-APN;*

(ii) G_{0,x_1} *is not* x_1*-APN for* $0 \neq x_1 \in \mathbb{F}_{2^n}$ *if and only if there exists* $0 \neq t \in \mathbb{F}_{2^n}$ *such that* $\displaystyle\sum_{i=0}^{n-1} t^{2^{ki}} = 0$*;*

(iii) if $0 \neq \zeta \neq x_1$, *then* G_{0x_1} *is* ζ*-APN if and only if there are no solutions to either of* $u^{2^k} + u + (x_1/\zeta)^{2^k+1} = 0$, *and* $y^{2^k} + y(x_1+\zeta)^{2^k-1} + x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta} = 0$, *that is, if and only if* $\displaystyle\sum_{i=0}^{n-1} \left(\frac{x_1}{\zeta}\right)^{2^{ki}} \neq 0$ *and* $\displaystyle\sum_{i=0}^{n-1} \left((x_1+\zeta)^{-2^k} \left(x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta} \right) \right)^{2^{ki}} \neq 0.$

Proof. Let $G_{x_0x_1}$ be the $\{x_0, x_1\}$-swapping of F. The Janwa-Wilson-Rodier equation (4) of $G_{x_0x_1}$ at ζ becomes

$$\begin{aligned}
&x^{2^k}y + x^{2^k}\zeta + y^{2^k}x + y^{2^k}\zeta + \zeta^{2^k}x + \zeta^{2^k}y \\
&+ \big((\zeta+x_0)^{2^n-1} + (\zeta+x_1)^{2^n-1} + (x+x_0)^{2^n-1} + (x+x_1)^{2^n-1} + (y+x_0)^{2^n-1} \\
&+(y+x_1)^{2^n-1} + (x+y+\zeta+x_0)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\big)(y_0+y_1) = 0.
\end{aligned} \tag{14}$$

We will use below the fact that under $\gcd(k,n) = 1$, the equation $z^{2^k-1} = a$ has a unique solution in $\mathbb{F}_{2^n}$. Let $x_0 = 0$ (hence $y_0 = 0$). We consider three cases depending on the value of ζ.

In the first case, suppose that $\zeta = 0$. If $0 \neq x \neq y \neq 0$, then equation (14) becomes

$$x^{2^k}y + y^{2^k}x + \big((x+x_1)^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_1)^{2^n-1}\big)\, y_1 = 0.$$

If $x = x_1$ (similarly, for $y = x_1$ and $x + y = x_1$), then we get (certainly, $0 \neq y \neq x_1$, respectively, $0 \neq x \neq x_1$), $x_1^{2^k}y + y^{2^k}x_1 = 0$, rendering $(y/x_1)^{2^k-1} = 1$, and since $\gcd(k,n) = 1$, this last equation has only the trivial solution $y = x_1$.

We now assume $x \neq x_1 \neq y$ and $x + y \neq x_1$. Thus, recalling that $y_1 = x_1^{2^k+1}$, equation (14) becomes $x^{2^k}y + y^{2^k}x + x_1^{2^k+1} = 0$. Taking $u = x/x_1, v = y/x_1$, and dividing by $x_1^{2^k+1}$ above, we get $u^{2^k}v + v^{2^k}u + 1 = 0$. Let us take α with $\alpha^{2^k} + \alpha \neq 0, 1$. Such an α certainly exists; we can, for instance, take α to be a primitive element of $\mathbb{F}_{2^n}$. Writing $v = \alpha u$, the above equation becomes

$$u^{2^k+1} = \left(\alpha^{2^k} + \alpha\right)^{-1}.$$

Since n is odd, $\gcd(2^k + 1, 2^n - 1) = 1$, and so, the equation above has a unique solution $u \neq 1$ in $\mathbb{F}_{2^n}$ for every $\alpha \in \mathbb{F}_{2^n}$ satisfying $\alpha^{2^k} + \alpha \neq 0, 1$. Thus, G_{0x_1} cannot be 0-APN.

In the second case, let $\zeta = x_1 \neq 0$. If $x_1 \neq x \neq y \neq x_1$, then equation (14) becomes

$$\begin{aligned} &x^{2^k}y + x^{2^k}x_1 + y^{2^k}x + y^{2^k}x_1 + x_1^{2^k}x + x_1^{2^k}y \\ &\quad + \left(x^{2^n-1} + y^{2^n-1} + (x + y + x_1)^{2^n-1}\right) y_1 = 0. \end{aligned} \tag{15}$$

If $x = 0$, then $y \neq 0, x_1$ and the above equation becomes $y^{2^k}x_1 + x_1^{2^k}y = 0$, which only has the trivial solutions $y = 0$ and $y = x_1$. The cases when $y = 0$ and $y = x + x_1$ are handled similarly.

We next assume that $xy \neq 0, x + y \neq x_1$. Thus, equation (14) becomes

$$x^{2^k}y + x^{2^k}x_1 + y^{2^k}x + y^{2^k}x_1 + x_1^{2^k}x + x_1^{2^k}y + x_1^{2^k+1} = 0. \tag{16}$$

Dividing by $x_1^{2^k+1}$ and labelling $u = x/x_1, v = y/x_1$, we obtain

$$u^{2^k}v + u^{2^k} + v^{2^k}u + v^{2^k} + u + v + 1 = 0. \tag{17}$$

We now let $w = u + v$ and rewrite (17) as $w^{2^k}(u + 1) + w(u + 1)^{2^k} + 1 = 0$, that is, $w^{2^k} + w(u + 1)^{2^k-1} + (u + 1)^{-1} = 0$.

We now apply Theorem 5. Here, $p = 2$, $a = (u + 1)^{2^k-1}$, $b = (u + 1)^{-1}$, and $m = \frac{n}{\gcd(k,n)} = n$. Then,

$$\alpha_{n-1} = \left((u + 1)^{2^k-1}\right)^{1+2^k+\cdots+2^{k(n-1)}} = \left((u + 1)^{2^k-1}\right)^{\frac{2^{kn}-1}{2^k-1}} = (u + 1)^{2^{kn}-1} = 1.$$

Furthermore,

$$\begin{aligned} \beta_{n-1} &= \sum_{i=0}^{n-1} \left((u + 1)^{2^k-1}\right)^{\sum_{j=i}^{n-2} 2^{k(j+1)}} \left((u + 1)^{-1}\right)^{2^{ki}} \\ &= \sum_{i=0}^{n-1} (u + 1)^{2^{k(i+1)}\left(2^{k(n-i-1)}-1\right)-2^{ki}} \\ &= (u + 1)^{2^{kn}} \sum_{i=0}^{n-1} (u + 1)^{-2^{ki}(2^k+1)}. \end{aligned}$$

Thus, $\beta_{n-1} = 0$ if and only if there exists u such that $\sum_{i=0}^{n-1} (u+1)^{-2^{ki}(2^k+1)} = 0$. We conclude that G_{0x_1} is not x_1-APN if and only if there exists $t \neq 0$ such that $\sum_{i=0}^{n-1} t^{2^{ki}} = 0$.

In the final case, we assume that $0 \neq \zeta \neq x_1 \neq 0$. Equation (14) becomes

$$\begin{aligned} 0 &= x^{2^k} y + y^{2^k} x + x^{2^k} \zeta + \zeta^{2^k} x + y^{2^k} \zeta + \zeta^{2^k} y \\ &+ \big(x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1} \\ &+ (y+x_1)^{2^n-1} + (x+y+\zeta)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\big)\, y_1. \end{aligned} \tag{18}$$

We will show that equation (18) has no nontrivial solutions x, y. All of the resulting subcases are similar, so we will explicitly describe only some of them.

If the expression in the parentheses in (18) is equal to 0, then we need to investigate the equation

$$x^{2^k} y + y^{2^k} x + x^{2^k} \zeta + \zeta^{2^k} x + y^{2^k} \zeta + \zeta^{2^k} y = 0.$$

Writing $y = \alpha x$, we get

$$x^{2^k+1}\alpha + x^{2^k+1}\alpha^{2^k} + x^{2^k}\zeta + x\zeta^{2^k} + \alpha^{2^k} x^{2^k}\zeta + \alpha x \zeta^{2^k} = 0,$$

which becomes

$$x^{2^k+1}(\alpha + \alpha^{2^k}) + x^{2^k}\zeta(1+\alpha^{2^k}) + x\zeta^{2^k}(\alpha+1) = 0.$$

Dividing by x^{2^k+1}, and labelling $z = \frac{\zeta}{x}$, we get

$$z^{2^k}(\alpha+1) + z(\alpha+1)^{2^k} + \alpha + \alpha^{2^k} = 0.$$

Dividing by $1+\alpha$ and observing that $\frac{\alpha^{2^k}+\alpha}{\alpha+1} = \frac{\alpha^{2^k}+1+\alpha+1}{\alpha+1} = \frac{(\alpha+1)^{2^k}+\alpha+1}{\alpha+1} = (\alpha+1)^{2^k-1}+1$, we obtain

$$z^{2^k} + z(\alpha+1)^{2^k-1} + (\alpha+1)^{2^k-1} + 1 = 0,$$

which can be factored as

$$(z+1)^{2^k} + (z+1)(\alpha+1)^{2^k-1} = 0,$$

that is,

$$(z+1)((z+1)^{2^k-1} + (\alpha+1)^{2^k-1}) = 0,$$

with roots $z = 1$ and $z = \alpha$. Both of these, however, are trivial, since then $x = \zeta$, respectively, $y = \zeta$.

Assume now that the parenthesized expression in (18) does not evaluate to 0 (which can only happen if an odd number of terms vanish). Equation (18) becomes

$$x^{2^k} y + y^{2^k} x + x^{2^k} \zeta + \zeta^{2^k} x + y^{2^k} \zeta + \zeta^{2^k} y + x_1^{2^k+1} = 0.$$

If $x = 0$, then (18) becomes $y^{2^k}\zeta + \zeta^{2^k}y + x_1^{2^k+1} = 0$. Dividing by ζ^{2^k+1} and labelling $u = y/\zeta$, we get $u^{2^k} + u + (x_1/\zeta)^{2^k+1} = 0$. By the same argument as in the previous case, solutions to this equation exist if and only if $\sum_{i=0}^{n-1}(x_1/\zeta)^{(2^k+1)2^{ki}} = 0$. Thus, if there exist solutions to this equation other than $u = \frac{x_1}{\zeta}$ or $u = 1 + \frac{x_1}{\zeta}$ (which would give $y = x_1$ or $y = \zeta + x_1$, making the parenthesized expression in (18) vanish), then G_{0x_1} is not ζ-APN (note that $y = 0, y = \zeta$ cannot be solutions).

We have to ensure that the potential solutions of $u^{2^k}+u+(x_1/\zeta)^{2^k+1} = 0$ are different from $u = \frac{x_1}{\zeta}$ (which would give $y = x_1$) and $u = 1 + \frac{x_1}{\zeta}$ (which would give $y = \zeta + x_1$), since in both cases the expression inside the parentheses in (18) would vanish. If $y = x_1$ or $y = \zeta + x_1$, since $x = 0$, then (18) becomes $x_1^{2^k}\zeta + \zeta^{2^k}x_1 + x_1^{2^k+1} = 0$. Dividing by $x_1^{2^k+1}$ and relabelling $z = \frac{\zeta}{x_1}$, we obtain the equation $z^{2^k} + z + 1 = 0$, which has no solutions by Theorem 5.

If $x = x_1$, then (18) transforms into

$$x_1^{2^k}y + y^{2^k}x_1 + x_1^{2^k}\zeta + \zeta^{2^k}x_1 + y^{2^k}\zeta + \zeta^{2^k}y + x_1^{2^k+1} = 0,$$

which can be rewritten as $y^{2^k} + y(x_1+\zeta)^{2^k-1} + x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta} = 0$. If a solution y exists to this previous equation (observe that y cannot be equal to x_1), then G_{0x_1} is not ζ-APN. By a similar argument as the one in the second case, by Theorem 5 we get $\alpha_{n-1} = 1$, and

$$\beta_{n-1} = (x_1+\zeta)^{2^{kn}}\sum_{i=0}^{n-1}\left((x_1+\zeta)^{-2^k}\left(x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta}\right)\right)^{2^{ki}}.$$

Therefore, G_{0x_1} is not ζ-APN if and only if $\displaystyle\sum_{i=0}^{n-1}\left((x_1+\zeta)^{-2^k}\left(x_1^{2^k} + \frac{x_1\zeta^{2^k}}{x_1+\zeta}\right)\right)^{2^{ki}} = 0.$

The remaining cases give the same equations (up to relabelling). □

Remark 7. *Our computations for $4 \le n \le 10$ suggest that swapping any two outputs in a Gold APN function produce a function with a non-empty pAPN-spectrum, but we do not yet have a theoretical argument explaining this. See Table 6 in the appendix for detailed computational results.*

5 The Welch APN case

Recall that the Welch APN function is defined over $\mathbb{F}_{2^n}$ as $F(x) = x^{2^k+3}$ for $n = 2k+1$. In this section, we generalize this function by allowing k in x^{2^k+3} to be any positive integer.

To simplify notation, we denote

$$\begin{aligned}E(\zeta, x_1, x, y) &= \zeta^{2^n-1} + (\zeta+x_1)^{2^n-1} + x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1}\\ &\quad + (y+x_1)^{2^n-1} + (x+y+\zeta)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1},\\ C(\zeta, x, y) &= \zeta^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x+y+\zeta)^{2^k+3}\end{aligned}$$

in $\mathbb{F}_{2^n}$. Certainly, $E(\zeta, x_1, x, y) \in \{0,1\}$.

Theorem 8. *Let $F(x) = x^{2^k+3}$ be the Welch function on $\mathbb{F}_{2^n}$, where n is odd and let G_{0x_1} be the $\{0, x_1\}$-swapping of F for some $0 \neq x_1 \in \mathbb{F}_{2^n}$. Then:*

- *G_{0x_1} is not 0-APN if $\gcd(2^k+3, 2^n-1) = 1$ (which always happens if $n = 2k+1$), nor x_1-APN in general;*
- *if $\zeta \neq 0, x_1$, then G_{0x_1} is not ζ-APN if and only if there is a solution (x, y) of the system $C(\zeta, x, y) = 0$ and $E(\zeta, x_1, x, y) = 0$, or $C(\zeta, x, y) = x_1^{2^k+3}$ and $E(\zeta, x_1, x, y) = 1$, where $x_1, \zeta \neq x \neq y \neq x_1, \zeta$.*

Proof. Let G_{0x_1} be the $\{0, x_1\}$-swapping of F. The Janwa-Wilson-Rodier equation (4) of G_{0x_1} at ζ becomes

$$\begin{aligned}&\zeta^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x+y+\zeta)^{2^k+3}\\&+\big(\zeta^{2^n-1} + (\zeta+x_1)^{2^n-1} + x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1}\\&+(y+x_1)^{2^n-1} + (x+y+\zeta)^{2^n-1} + (x+y+\zeta+x_1)^{2^n-1}\big)\, x_1^{2^k+3} = 0.\end{aligned} \tag{19}$$

First, assume that $\zeta = 0$. Then (19) becomes

$$\begin{aligned}&x^{2^k}y^3 + x^{2^k+2}y + x^{2^k+1}y^2 + y^{2^k}x^3 + y^{2^k+1}x^2 + y^{2^k+2}x\\&+\big(x_1^{2^n-1} + x^{2^n-1} + (x+x_1)^{2^n-1} + y^{2^n-1}\\&+(y+x_1)^{2^n-1} + (x+y)^{2^n-1} + (x+y+x_1)^{2^n-1}\big)\, x_1^{2^k+3} = 0.\end{aligned} \tag{20}$$

If the expression inside the parentheses vanishes (with $y = \alpha x \neq 0, x$), the equation becomes

$$\alpha(\alpha^{2^k-1}+1)(\alpha^2+\alpha+1) = 0,$$

which does not have solutions other than $\alpha = 0, 1$ (which contradict $y \neq 0, x$), since $\gcd(k, n) = 1$ and n is odd. Thus, we need to assume that the parenthesized expression in (20) does not vanish, that is, $E(0, x_1, x, y) = 1$. The equation thus becomes

$$x^{2^k}y^3 + x^{2^k+2}y + x^{2^k+1}y^2 + y^{2^k}x^3 + y^{2^k+1}x^2 + y^{2^k+2}x + x_1^{2^k+3} = 0.$$

Taking $y = \alpha x \neq 0, x$ (so, $\alpha \neq 0, 1$) we obtain,

$$x^{2^k+3}\alpha(\alpha^{2^k-1}+1)(\alpha^2+\alpha+1) = x_1^{2^k+3},$$

and since $\alpha(\alpha^{2^k-1}+1)(\alpha^2+\alpha+1) \neq 0$, if $\gcd(2^k+3, 2^n-1) = 1$, then there exists a unique solution

$$x^{2^k+3} = \frac{x_1^{2^k+3}}{\alpha(\alpha^{2^k-1}+1)(\alpha^2+\alpha+1)},$$

and so G_{0x_1} is not 0-APN.

We argue now that when $n = 2k+1$ we have $\gcd(2^k+3, 2^n-1) = 1$. Let us denote $d = \gcd(2^k+3, 2^n-1)$. We then have

$$\begin{aligned} 2^k &\equiv -3 \pmod{d} \\ 2^{2k+1} &\equiv 1 \pmod{d}, \end{aligned}$$

and so

$$\begin{aligned} 2^{2k+1} &\equiv 2 \cdot 3^2 \pmod{d} \\ 2^{2k+1} &\equiv 1 \pmod{d}, \end{aligned}$$

which, by subtraction, renders $17 \equiv 0 \pmod{d}$, and so, $d = 1$ or $d = 17$. However, by [10, Lemma 9] we know that $\gcd(2^s+1, 2^n-1) = \frac{2^{\gcd(n,2s)}-1}{2^{\gcd(n,s)}-1}$, which, if $s = 2$ and n is odd becomes $\gcd(2^n-1, 2^4+1) = 1$. Therefore, $\gcd(2^k+3, 2^n-1) = 1$, when $n = 2k+1$. Now, suppose that $\zeta = x_1$. Then (19) becomes

$$\begin{aligned} & x_1^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x+y+x_1)^{2^k+3} + \left(x_1^{2^n-1} + x^{2^n-1} + (x+x_1)^{2^n-1}\right. \\ & \left. + y^{2^n-1} + (y+x_1)^{2^n-1} + (x+y+x_1)^{2^n-1} + (x+y)^{2^n-1}\right) x_1^{2^k+3} = 0. \end{aligned} \tag{21}$$

If the parenthesized expression above does not vanish, that is, $E(\zeta, x_1, x, y) = 1$, the equation becomes

$$x^{2^k+3} + y^{2^k+3} + (x+y+x_1)^{2^k+3} = 0,$$

which, dividing by $x_1^{2^k+3}$, and taking $u = x/x_1, v = y/x_1$, becomes

$$u^{2^k+3} + v^{2^k+3} + (u+v+1)^{2^k+3} = 0.$$

Noting that $u = 0$ can not be a solution, we take $v = \alpha u$ with $\alpha \neq 0, 1$ and divide both sides by u^{2^k+3}. Since $\gcd(2^k+3, 2^n-1) = 1$, then a unique (2^k+3)-root exists and this last equation becomes

$$\beta = \frac{1 + u(1+\alpha)}{u} = (1 + \alpha^{2^k+3})^{1/(2^k+3)},$$

which (taking α such that $\beta + \alpha + 1 \neq 0$) renders the solution $u = (\beta + \alpha + 1)^{-1}$. Surely, one can find many values of α such that $1 \neq u \neq v \neq 1$, and consequently, $x_1 \neq x \neq y \neq x_1$. Therefore, G_{0x_1} is not x_1-APN, either.

Finally, assume that $0 \neq \zeta \neq x_1$. If the expression in the parentheses in (19) is zero, that is, $E(\zeta, x_1, x, y) = 0$, the equation becomes

$$\zeta^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x+y+\zeta)^{2^k+3} = 0.$$

If the expression in the parentheses in (19) is not zero, that is, $E(\zeta, x_1, x, y) = 1$, the equation is then

$$x_1^{2^k+3} + \zeta^{2^k+3} + x^{2^k+3} + y^{2^k+3} + (x+y+\zeta)^{2^k+3} = 0,$$

which concludes the proof of the theorem. □

Remark 9. *As with the Gold function, our computational results in Table* 5 *suggest that swapping any two points of the Welch APN function leads to a function with a non-empty spectrum. At the moment, we cannot theoretically justify why this happens.*

Acknowledgements

The authors would like to thank the referees for the thorough reading and detailed comments, which improved our manuscript. The paper was started while the fourth named author visited the Selmer Center at the University of Bergen and the 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 is supported by the "Optimal Boolean Functions" grant of the 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] K. A. Browning, J. F. Dillon, M. T. McQuistan, A. J. Wolfe, *An APN permutation in dimension six*, Finite Fields: Theory and Applications, pp. 33-42, Contemp. Math. 518, Amer. Math. Soc., Providence, RI, 2010.

[3] 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.

[4] 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 & Communications - CCDS 12 (2020), 527–545; preliminary version in Proc. Sequences and Their Applications – SETA 2018, Hong Kong, 2018.

[5] L. Budaghyan, N. Kaleyski, C. Riera, P. Stănică, *On the sensitivity of some APN permutations to swapping points*, Proc. Sequences and Their Applications – SETA 2020, Paper # 9.

[6] M. Calderini, I.Villa, *On the Boomerang Uniformity of some Permutation Polynomials*, Cryptogr. Commun. 12 (2020), 1161–1178.

[7] 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.

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

[9] R. S. Coulter, M. Henderson, *A note on the roots of trinomials over a finite field*, Bull. Austral. Math. Soc. 69 (2004), 429–432.

[10] P. Ellingsen, P. Felke, C. Riera, P. Stănică, A. Tkachenko, *C-differentials, multiplicative uniformity and (almost) perfect c-nonlinearity*, IEEE Trans. Inf. Theory 66:9 (2020), 5781–5789.

[11] H. Janwa, M. Wilson, *Hyperplane sections of Fermat varieties in* P^3 *in char.* 2 *and some applications to cyclic codes*, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, Proceedings AAECC10 (G. Cohen, T. Mora and O. Moreno, Eds.), LNCS 673, Springer-Verlag, New York/Berlin, pp. 180–194, 1993.

[12] N.S. Kaleyski, *Changing APN functions at two points*, Cryptography and Communications 11.6 (2019): 1165-1184.

[13] S. Li, W. Meidl, A. Polujan, A. Pott, C. Riera, P. Stănică, *Vanishing Flats: A Combinatorial Viewpoint on the Planarity of Functions and Their Application*, IEEE Trans. Inf. Theory 66:11 (2020), 7101–7112.

[14] J. Liang, *On the solutions of trinomial equations over finite fields*, Bull. Cal. Math. Soc. 70 (1978), 379–382.

[15] K. Nyberg, *Differentially uniform mappings for cryptography*, Workshop on the Theory and Application of of Cryptographic Techniques 1993 May 23 (pp. 55-64). Springer, Berlin, Heidelberg.

[16] D. Tang, C. Carlet, X. Tang, *Differentially* 4*-uniform bijections by permuting the inverse function*, Des. Codes. Cryptogr. 77 (2014), 117–141.

[17] L. Qu, Y. Tan, C. H. Tan, C. Li, *Constructing differentially* 4*-uniform permutations over* $\mathbb{F}_{2^{2k}}$ *via the switching method*, IEEE Trans. Inf. Theory 59:4 (2013), 4675–4686.

[18] L. Qu, Y. Tan, C. Li, G. Gong, *More constructions of differentially* 4*-uniform permutations on* $\mathbb{F}_{2^{2k}}$, Des., Codes Cryptogr. 78 (2016), 391–408.

[19] 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.

[20] K. S. Williams, *Note on cubics over* $GF(2^n)$ *and* $GF(3^n)$, J. Number Theory 7 (1975), 361–365.

[21] Y. Yu, M. Wang, Y. Li, *Constructing differentially* 4*-uniform permutations from known ones*, Chinese Journal of Electronics 22.3 (2013): 495–499.

[22] Z. Zha, L. Hu, S. Sun, *Constructing new differentially* 4*-uniform permutations from the inverse function*, Finite Fields Appl. 25 (2014), 64–78.

A Experimental data on the infinite APN families

For functions from each of the infinite APN monomial families over $\mathbb{F}_{2^n}$ with $n \leq 10$ (except for the inverse family which is characterized by Theorem 4), we have computed the size of the pAPN-spectrum of $G_{x_0x_1}$ for all possible pairs $(x_0, x_1) \in \mathbb{F}_{2^n}^2$. The results are given in Tables 2, 3, 4, 5, 6 below.

In all cases, the results are computed for generalizations of the respective infinite families, with all restrictions on the parameters dropped. This means that we consider the following functions over $\mathbb{F}_{2^n}$, with the parameter i being any positive integer in the range $1 \leq i \leq n-1$:

- $x^{2^{4i}+2^{3i}+2^{2i}+2^i-1}$ for Dobbertin,
- $x^{2^{2i}-2^i+1}$ for Kasami,
- $x^{2^i+2^{i/2}-1}$ or $x^{2^i+2^{(3i+1)/2}-1}$ for even and odd values of i, respectively, for Niho,
- x^{2^i+3} for Welch, and
- x^{2^i+1} for Gold.

The first two columns of each table specify the degree n of the extension field $\mathbb{F}_{2^n}$ and the value of the parameter i. The third column gives the smallest element from the cyclotomic coset of the resulting exponent d. The fourth and fifth columns give the differential uniformity and size of the pAPN-spectrum of x^d over $\mathbb{F}_{2^n}$, respectively. Finally, the last column describes how the pAPN-spectrum changes after swapping two output values of the function. More precisely, for every pair $\{x_0, x_1\} \subseteq \mathbb{F}_{2^n}$ with $x_0 \neq x_1$, we compute the size of the pAPN-spectrum of $G_{x_0x_1}$; the last column then lists the sizes of all possible spectra obtained in this way. The frequencies with which these sizes occur over all possible pairs $\{x_0, x_1\}$ are given as superscripts. For example, the first row of Table 2 contains $0^{45}, 2^{60}, 8^{15}$ in the last column. This means that, out of the 120 pairs $\{x_0, x_1\} \subseteq \mathbb{F}_{2^4}$, 45 pairs produce a function with an empty pAPN-spectrum, 60 pairs produce a function which is ζ-APN for two values of ζ, and the remaining 15 pairs lead to functions that are ζ-APN for 8 values of ζ.

By Proposition 3, all exponents d such that x^d has 2^s-to-1 derivatives for some fixed $s > 1$ are omitted. All such functions and all two-point swaps of these functions have an empty pAPN-spectrum by the proposition, and are therefore of very limited interest. These include all Gold functions with $\gcd(i, n) > 1$ and all Kasami functions with $\gcd(i, n) > 1$ and $n/\gcd(i, n)$ odd. They also include the exponents $i = 3, 4$ for $n = 6$ and $i = 5$ for $n = 10$ in the Dobbertin case; $i = 3$ for $n = 6$ in the Kasami case; $i = 1$ for even n, $i = 4$ for $n = 6$ and $i = 8$ for $n = 10$ in the Welch case; $i = 1, 2$ for n even, $i = 3$ for $n = 5$, $i = 4$ for $n = 6$, $i = 5$ for $n = 8$ and $i = 6$ for $n = 9$ in the Niho case.

We note that in some cases, swap operations lead to a full-sized pAPN-spectrum, indicating that the corresponding function is APN. This occurs exclusively in even dimensions for APN functions, and is caused by pairs $\{x_0, x_1\}$ with $x_0 \neq x_1$ but $F(x_0) = F(x_1)$, where F is the function in question. Consider, for example, $F(x) = x^3$ for $n = 6$ and $i = 2$ in Table 2; there are 63 pairs leading to a pAPN-spectrum of size 64. We know that APN power functions over even-degree extensions of $\mathbb{F}_2$ are 3-to-1; in this case, x^3 has 21 non-zero images y, for each of which there are three pre-images x_1, x_2, x_3 such that $F(x_1) = F(x_2) = F(x_3) = y$. Since a pair of elements from among $\{x_1, x_2, x_3\}$ can be selected in three different ways, each of the 21 images contributes three pairs, leading to these 63 pairs which trivially preserve the APN-ness of the initial function.

The only exceptions to this occur for $n = 4$; for example, for $F(x) = x^3$ in Table 2, there are 30 pairs giving a full pAPN-spectrum, while the trivial pairs as described above account for only 15 of these. To the best of our knowledge, $n = 4$ is the highest extension degree for which APN functions at Hamming distance 2 from each other exist; this is reflected in e.g. [12] and agrees with the results presented in the tables.

Conversely, we can observe that the inverse function is the only APN function among the ones considered whose pAPN-spectrum can become empty after a two-point swap. We ran a separate experiment in which we computed the sizes of the pAPN-spectra of all two-points swaps for representatives from all known CCZ-equivalence classes of APN functions, and observed the same phenomenon: the inverse function is the only one for which an empty pAPN-spectrum could be obtained by swapping two points. Based on this, we formulate the following conjecture.

Conjecture 10. *Let F be any APN power function over $\mathbb{F}_{2^n}$, CCZ-inequivalent to the inverse power function x^{2^n-2}, and let $G_{x_0x_1}$ be the (x_0, x_1)-swapping of F for some $(x_0, x_1) \in \mathbb{F}_{2^n}^2$. Then the pAPN-spectrum of $G_{x_0x_1}$ is not empty.*

According to some limited computational experiments, the same might be true for quadratic APN functions; however, we do not state this a conjecture in general since we do not have enough data, nor heuristics on why that would happen.

We note that the multiset of the sizes of the pAPN-spectra of all functions obtained by swapping two points in a given function is not CCZ-invariant. Counterexamples can be found easily, for instance by considering the Kim function and its CCZ-equivalent permutation [2] over $\mathbb{F}_{2^6}$: the pAPN-spectra of all functions obtained by swapping two outputs of the former are of even size, while pAPN-spectra of odd size can be obtained from the latter. Hence, our conjecture relates only to power APN functions and does not include the ones CCZ-equivalent to them.

Some of the functions listed in the table have a singleton pAPN-spectrum, e.g. $F(x) = x^{47}$ for $i = 3$ and $n = 7$ in Table 2. All such functions are 0-APN.

The function $F(x) = x^{15}$ over $\mathbb{F}_{2^8}$, as given in Table 4, is remarkable due to the fact that all possible pairs $\{x_0, x_1\}$ lead to a function with a singleton pAPN-spectrum. When $x_0 = 0$, the resulting function is x_1-APN, and when $x_0 \neq 0$, the resulting function is 0-APN.

Table 2: pAPN-spectra of two-point swaps of the Dobbertin function

n	i	d	δ_F	Spectrum	Swapped spectrum
4	1,3	7	4	0	0^{45}, 2^{60}, 8^{15}
	2	3	2	16	16^{30}, 4^{90}
5	1,2,3,4	15	2	32	0^{31}, 6^{155}, 8^{155}, 9^{155}
6	1	23	10	0	0^{2016}
	2	3	2	64	10^{189}, 12^{378}, 16^{189}, 22^{378}, 24^{378}, 26^{378}, 64^{63}, 8^{63}
	5	31	4	0	0^{1197}, 2^{567}, 30^{63}, 4^{189}
7	1,5	29	2	128	25^{889}, 28^{889}, 29^{889}, 30^{1778}, 31^{2667}, 32^{889}, 42^{127}
	2,4	43	2	128	22^{889}, 26^{889}, 28^{127}, 30^{889}, 32^{2667}, 36^{1778}, 38^{889}
	3	47	4	1	0^{4572}, 1^{3556}
	6	63	2	128	0^{127}, 26^{889}, 28^{889}, 29^{889}, 30^{889}, 32^{2667}, 35^{889}, 36^{889}
8	1	29	10	0	0^{32640}
	2,6	21	4	1	0^{14025}, 1^{18615}
	3	43	30	0	0^{32640}
	4	9	2	256	256^{255}, 48^{2040}, 52^{2040}, 54^{2040}, 56^{2040}, 58^{6120}, 60^{3060}, 62^{5100}, 70^{510}, 74^{255}, 80^{2040}, 86^{4080}, 88^{3060}
	5	59	12	0	0^{32640}
	7	127	4	0	0^{19125}, 128^{255}, 2^{10200}, 4^{3060}
9	1	29	8	0	0^{130816}
	2	117	6	1	0^{80227}, 1^{50589}
	3	5	2	512	112^{13797}, 114^{1533}, 118^{4599}, 120^{13797}, 122^{13797}, 124^{9198}, 126^{14308}, 128^{18396}, 130^{9198}, 132^{9198}, 134^{9198}, 136^{4599}, 142^{4599}, 144^{4599}
	4	95	8	0	0^{130816}
	5	83	6	1	0^{80227}, 1^{50589}
	6	17	2	512	106^{4599}, 114^{4599}, 118^{9198}, 120^{22995}, 122^{13797}, 124^{18396}, 126^{11242}, 128^{4599}, 132^{9198}, 136^{18396}, 138^{4599}, 142^{9198}
	7	85	8	0	0^{130816}
	8	255	2	512	0^{511}, 116^{4599}, 118^{4599}, 119^{4599}, 120^{6132}, 122^{9198}, 124^{22995}, 125^{4599}, 126^{4599}, 127^{4599}, 128^{9198}, 129^{4599}, 130^{13797}, 131^{4599}, 133^{4599}, 134^{13797}, 135^{4599}, 136^{4599}, 138^{4599}
10	1	29	4	0	0^{523776}
	2,4,6,8	213	2	1024	1024^{1023}, 224^{10230}, 228^{10230}, 230^{15345}, 232^{25575}, 241^{10230}, 243^{10230}, 244^{25575}, 245^{10230}, 246^{20460}, 247^{10230}, 250^{30690}, 251^{20460}, 252^{20460}, 254^{30690}, 255^{10230}, 258^{10230}, 260^{20460}, 261^{5115}, 262^{1023}, 263^{10230}, 264^{25575}, 265^{10230}, 266^{10230}, 267^{10230}, 268^{10230}, 269^{10230}, 270^{10230}, 271^{20460}, 272^{20460}, 274^{5115}, 275^{20460}, 278^{20460}, 279^{20460}, 283^{10230}, 291^{10230}
	3	151	6	0	0^{523776}
	7	89	6	0	0^{523776}
	9	511	4	0	0^{277233}, 2^{230175}, 4^{15345}, 510^{1023}

Table 3: pAPN-spectra of two-point swaps of the Kasami function

n	i	d	δ_F	Spectrum	Swapped spectrum
4	1,3	3	2	16	16^{30}, 4^{90}
	2	7	4	0	0^{45}, 2^{60}, 8^{15}
5	1,4	3	2	32	10^{31}, 6^{155}, 8^{310}
	2,3	11	2	32	10^{31}, 6^{155}, 8^{310}
6	1,5	3	2	64	10^{189}, 12^{378}, 16^{189}, 22^{378}, 24^{378}, 26^{378}, 64^{63}, 8^{63}
7	1,6	3	2	128	22^{889}, 26^{889}, 28^{127}, 30^{889}, 32^{2667}, 36^{1778}, 38^{889}
	2,5	13	2	128	21^{127}, 27^{889}, 28^{889}, 29^{2667}, 30^{889}, 32^{1778}, 38^{889}
	3,4	23	2	128	25^{889}, 28^{889}, 29^{889}, 30^{1778}, 31^{2667}, 32^{889}, 42^{127}
8	1,7	3	2	256	256^{255}, 48^{2040}, 52^{4080}, 54^{4080}, 56^{2040}, 58^{4080}, 62^{3060}, 66^{2040}, 70^{510}, 74^{255}, 76^{1020}, 80^{2040}, 82^{2040}, 88^{3060}, 90^{2040}
	2,6	13	12	0	0^{32640}
	3,5	39	2	256	256^{255}, 53^{2040}, 55^{2040}, 57^{2040}, 60^{4080}, 61^{4080}, 62^{6630}, 65^{2040}, 81^{2040}, 83^{2040}, 85^{4080}, 88^{1020}, 98^{255}
	4	31	16	0	0^{32640}
9	1,8	3	2	512	112^{9198}, 114^{4599}, 116^{13797}, 118^{4599}, 120^{9198}, 122^{4599}, 124^{9198}, 126^{20440}, 128^{4599}, 130^{13797}, 132^{13797}, 136^{4599}, 138^{4599}, 140^{9198}, 142^{4599}
	2,7	13	2	512	108^{1533}, 118^{4599}, 119^{9198}, 120^{4599}, 121^{9198}, 122^{4599}, 123^{13797}, 124^{4599}, 125^{4599}, 126^{4599}, 127^{4599}, 128^{22995}, 129^{13797}, 130^{4599}, 132^{4599}, 133^{13797}, 135^{4599}, 144^{511}
	4,5	47	2	512	116^{4599}, 117^{9198}, 121^{4599}, 123^{4599}, 124^{4599}, 125^{9198}, 126^{9198}, 127^{9198}, 128^{13797}, 129^{4599}, 131^{27594}, 132^{10731}, 133^{4599}, 135^{9198}, 136^{4599}, 99^{511}
10	1,9	3	2	1024	1024^{1023}, 212^{1023}, 216^{10230}, 218^{20460}, 220^{20460}, 222^{10230}, 224^{10230}, 226^{20460}, 230^{30690}, 232^{20460}, 238^{15345}, 240^{10230}, 242^{5115}, 246^{5115}, 252^{10230}, 256^{10230}, 258^{30690}, 262^{30690}, 264^{10230}, 266^{20460}, 268^{35805}, 270^{20460}, 272^{10230}, 276^{20460}, 278^{20460}, 280^{30690}, 284^{30690}, 286^{10230}, 288^{20460}, 290^{10230}, 292^{10230}, 294^{10230}
	3,7	57	2	1024	1024^{1023}, 219^{20460}, 220^{10230}, 227^{10230}, 228^{10230}, 229^{10230}, 231^{10230}, 232^{36828}, 233^{10230}, 234^{10230}, 235^{10230}, 240^{10230}, 242^{20460}, 244^{10230}, 248^{5115}, 255^{10230}, 259^{10230}, 260^{20460}, 263^{10230}, 266^{40920}, 269^{10230}, 270^{10230}, 271^{10230}, 272^{10230}, 273^{20460}, 274^{10230}, 275^{10230}, 276^{10230}, 277^{20460}, 278^{20460}, 279^{20460}, 280^{10230}, 281^{20460}, 282^{10230}, 283^{10230}, 284^{30690}, 290^{10230}
	5	63	32	0	0^{523776}

Table 4: pAPN-spectra of two-point swaps of the Niho function

n	i	d	δ_F	Spectrum	Swapped spectrum
4	3	3	2	16	$16^{30}, 4^{90}$
5	1,2	5	2	32	$10^{31}, 6^{155}, 8^{310}$
	4	7	2	32	$10^{31}, 6^{155}, 8^{310}$
6	3	15	8	0	0^{2016}
	5	7	6	0	0^{2016}
7	1,2,5	5	2	128	$20^{889}, 28^{127}, 30^{1778}, 32^{2667}, 34^{889}, 36^{889}, 38^{889}$
	3	29	2	128	$25^{889}, 28^{889}, 29^{889}, 30^{1778}, 31^{2667}, 32^{889}, 42^{127}$
	4	19	4	1	$0^{4572}, 1^{3556}$
	6	15	2	128	$22^{889}, 26^{889}, 28^{1016}, 32^{889}, 34^{1778}, 36^{2667}$
8	3	39	2	256	$256^{255}, 53^{2040}, 55^{2040}, 57^{2040}, 60^{4080}, 61^{4080}, 62^{6630}, 65^{2040}, 81^{2040}, 83^{2040}, 85^{4080}, 88^{1020}, 98^{255}$
	4	19	16	0	0^{32640}
	6	29	10	0	0^{32640}
	7	15	14	1	1^{32640}
9	1,2	5	2	512	$112^{13797}, 114^{1533}, 118^{4599}, 120^{13797}, 122^{13797}, 124^{9198}, 126^{14308}, 128^{18396}, 130^{9198}, 132^{9198}, 134^{9198}, 136^{4599}, 142^{4599}, 144^{4599}$
	3	39	8	0	0^{130816}
	4	19	2	512	$116^{4599}, 117^{511}, 119^{4599}, 121^{4599}, 122^{4599}, 123^{4599}, 124^{9198}, 125^{27594}, 126^{9198}, 127^{13797}, 128^{9198}, 129^{9198}, 130^{4599}, 131^{4599}, 132^{9198}, 133^{4599}, 135^{6132}$
	5	63	6	1	$0^{129283}, 1^{1533}$
	7	13	2	512	$108^{1533}, 118^{4599}, 119^{9198}, 120^{4599}, 121^{9198}, 122^{4599}, 123^{13797}, 124^{4599}, 125^{4599}, 126^{4599}, 127^{4599}, 128^{22995}, 129^{13797}, 130^{4599}, 132^{4599}, 133^{13797}, 135^{4599}, 144^{511}$
	8	31	2	512	$106^{4599}, 114^{4599}, 118^{9198}, 120^{22995}, 122^{13797}, 124^{18396}, 126^{11242}, 128^{4599}, 132^{9198}, 136^{18396}, 138^{4599}, 142^{9198}$
10	3	39	32	0	0^{523776}
	4	19	6	0	0^{523776}
	5	125	34	0	0^{523776}
	6	71	6	0	0^{523776}
	7	9	2	1024	$1024^{1023}, 206^{20460}, 208^{10230}, 210^{10230}, 212^{11253}, 220^{20460}, 222^{10230}, 230^{10230}, 232^{5115}, 234^{10230}, 236^{15345}, 238^{10230}, 242^{25575}, 248^{15345}, 254^{5115}, 256^{20460}, 258^{10230}, 260^{20460}, 262^{5115}, 264^{30690}, 266^{20460}, 268^{30690}, 270^{40920}, 272^{30690}, 274^{30690}, 278^{20460}, 280^{10230}, 286^{20460}, 288^{10230}, 292^{10230}, 294^{10230}, 300^{10230}, 308^{10230}$
	8	61	6	0	0^{523776}
	9	31	30	0	0^{523776}

Table 5: pAPN-spectra of two-point swaps of the Welch function

n	i	d	δ_F	Spectrum	Swapped spectrum
4	2,3	7	4	0	$0^{45}, 2^{60}, 8^{15}$
5	1	5	2	32	10^{31}, 6^{155}, 8^{310}
	2,4	7	2	32	10^{31}, 6^{155}, 8^{310}
	3	11	2	32	10^{31}, 6^{155}, 8^{310}
6	2,5	7	6	0	0^{2016}
	3	11	10	0	0^{2016}
7	1	5	2	128	20^{889}, 28^{127}, 30^{1778}, 32^{2667}, 34^{889}, 36^{889}, 38^{889}
	2,6	7	6	1	0^{5461}, 1^{2667}
	3	11	2	128	21^{127}, 27^{889}, 28^{889}, 29^{2667}, 30^{889}, 32^{1778}, 38^{889}
	4	19	4	1	0^{4572}, 1^{3556}
	5	13	2	128	21^{127}, 27^{889}, 28^{889}, 29^{2667}, 30^{889}, 32^{1778}, 38^{889}
8	2,7	7	6	0	0^{32640}
	3	11	10	0	0^{32640}
	4	19	16	0	0^{32640}
	5	25	6	0	0^{32640}
	6	13	12	0	0^{32640}
9	1	5	2	512	112^{13797}, 114^{1533}, 118^{4599}, 120^{13797}, 122^{13797}, 124^{9198}, 126^{14308}, 128^{18396}, 130^{9198}, 132^{9198}, 134^{9198}, 136^{4599}, 142^{4599}, 144^{4599}
	2,8	7	6	1	0^{129283}, 1^{1533}
	3	11	8	0	0^{130816}
	4	19	2	512	116^{4599}, 117^{511}, 119^{4599}, 121^{4599}, 122^{4599}, 123^{4599}, 124^{9198}, 125^{27594}, 126^{9198}, 127^{13797}, 128^{9198}, 129^{9198}, 130^{4599}, 131^{4599}, 132^{9198}, 133^{4599}, 135^{6132}
	5	35	6	1	0^{129283}, 1^{1533}
	6	25	8	0	0^{130816}
	7	13	2	512	108^{1533}, 118^{4599}, 119^{9198}, 120^{4599}, 121^{9198}, 122^{4599}, 123^{13797}, 124^{4599}, 125^{4599}, 126^{4599}, 127^{4599}, 128^{22995}, 129^{13797}, 130^{4599}, 132^{4599}, 133^{13797}, 135^{4599}, 144^{511}
10	2,9	7	6	0	0^{523776}
	3	11	10	0	0^{523776}
	4	19	6	0	0^{523776}
	5	35	34	0	0^{523776}
	6	49	8	0	0^{523776}
	7	25	8	0	0^{523776}

Table 6: pAPN-spectra of two-point swaps of the Gold function

n	i	d	δ_F	Spectrum	Swapped spectrum
4	1,3	3	2	16	16^{30}, 4^{90}
5	1,4	3	2	32	10^{31}, 6^{155}, 8^{310}
	2,3	5	2	32	10^{31}, 6^{155}, 8^{310}
6	1,5	3	2	64	10^{189}, 12^{378}, 16^{189}, 22^{378}, 24^{378}, 26^{378}, 64^{63}, 8^{63}
7	1,6	3	2	128	22^{889}, 26^{889}, 28^{127}, 30^{889}, 32^{2667}, 36^{1778}, 38^{889}
	2,5	5	2	128	20^{889}, 28^{127}, 30^{1778}, 32^{2667}, 34^{889}, 36^{889}, 38^{889}
	3,4	9	2	128	22^{889}, 26^{889}, 28^{1016}, 32^{889}, 34^{1778}, 36^{2667}
8	1,7	3	2	256	256^{255}, 48^{2040}, 52^{4080}, 54^{4080}, 56^{2040}, 58^{4080}, 62^{3060}, 66^{2040}, 70^{510}, 74^{255}, 76^{1020}, 80^{2040}, 82^{2040}, 88^{3060}, 90^{2040}
	3,5	9	2	256	256^{255}, 48^{2040}, 52^{2040}, 54^{2040}, 56^{2040}, 58^{6120}, 60^{3060}, 62^{5100}, 70^{510}, 74^{255}, 80^{2040}, 86^{4080}, 88^{3060}
9	1,8	3	2	512	112^{9198}, 114^{4599}, 116^{13797}, 118^{4599}, 120^{9198}, 122^{4599}, 124^{9198}, 126^{20440}, 128^{4599}, 130^{13797}, 132^{13797}, 136^{4599}, 138^{4599}, 140^{9198}, 142^{4599}
	2,7	5	2	512	112^{13797}, 114^{1533}, 118^{4599}, 120^{13797}, 122^{13797}, 124^{9198}, 126^{14308}, 128^{18396}, 130^{9198}, 132^{9198}, 134^{9198}, 136^{4599}, 142^{4599}, 144^{4599}
	4,5	17	2	512	106^{4599}, 114^{4599}, 118^{9198}, 120^{22995}, 122^{13797}, 124^{18396}, 126^{11242}, 128^{4599}, 132^{9198}, 136^{18396}, 138^{4599}, 142^{9198}
10	1,9	3	2	1024	1024^{1023}, 212^{1023}, 216^{10230}, 218^{20460}, 220^{20460}, 222^{10230}, 224^{10230}, 226^{20460}, 230^{30690}, 232^{20460}, 238^{15345}, 240^{10230}, 242^{5115}, 246^{5115}, 252^{10230}, 256^{10230}, 258^{30690}, 262^{30690}, 264^{10230}, 266^{20460}, 268^{35805}, 270^{20460}, 272^{10230}, 276^{20460}, 278^{20460}, 280^{30690}, 284^{30690}, 286^{10230}, 288^{20460}, 290^{10230}, 292^{10230}, 294^{10230}
	3,7	9	2	1024	1024^{1023}, 206^{20460}, 208^{10230}, 210^{10230}, 212^{11253}, 220^{20460}, 222^{10230}, 230^{10230}, 232^{5115}, 234^{10230}, 236^{15345}, 238^{10230}, 242^{25575}, 248^{15345}, 254^{5115}, 256^{20460}, 258^{10230}, 260^{20460}, 262^{5115}, 264^{30690}, 266^{20460}, 268^{30690}, 270^{40920}, 272^{30690}, 274^{30690}, 278^{20460}, 280^{10230}, 286^{20460}, 288^{10230}, 292^{10230}, 294^{10230}, 300^{10230}, 308^{10230}