Partially APN Boolean functions

Lilya Budaghyan[1], Nikolay S. Kaleyski[1], Soonhak Kwon[2], Constanza Riera[3], and Pantelimon Stănică[4]

[1]Department of Informatics, University of Bergen,
5020 Bergen, Norway; {Lilya.Budaghyan, Nikolay.Kaleyski}@uib.no
[2]Department of Mathematics, Sungkyunkwan University,
Suwon 16419, Republic of Korea; shkwon@skku.edu
[3]Department of Computing, Mathematics, and Physics,
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

Abstract

In this paper we define a notion of partial APNness and find various characterizations and constructions of classes of functions satisfying this condition. We connect this notion to the known conjecture that APN functions modified at a point cannot remain APN.

Keywords: Boolean function, almost perfect nonlinear (APN), partial APN, Walsh-Hadamard coefficients.

1 Introduction

The objects of this study are Boolean functions and some of their differential properties. We will introduce here only some needed notions, and the reader can consult [1, 3, 4, 7, 8, 11] for more on Boolean functions.

Let n be a positive integer and $\mathbb{F}_{2^n}$ denote the finite field with 2^n elements, and $\mathbb{F}_{2^n}^* = \mathbb{F}_{2^n} \setminus \{0\}$. Further, let $\mathbb{F}_2^m$ denote the m-dimensional vector space over $\mathbb{F}_2$. We call a function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$ a *Boolean function* on n variables. The cardinality of a set S is denoted by $\#S$. For $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ we define the *Walsh-Hadamard transform* to be the integer-valued function $\mathcal{W}_f(u) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\mathrm{Tr}_1^n(ux)}$, $u \in \mathbb{F}_{2^n}$, where $\mathrm{Tr}_1^n : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is the absolute trace function, given by $\mathrm{Tr}_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$. This transform satisfies Parseval's relation $\sum_{a \in \mathbb{F}_{2^n}} \mathcal{W}_f(a)^2 = 2^{2n}$.

Given a Boolean function f, the derivative of f with respect to $a \in \mathbb{F}_{2^n}$ is the Boolean function $D_a f(x) = f(x+a) + f(x)$, for all $x \in \mathbb{F}_{2^n}$.

For positive integers n and m, any map $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a vectorial Boolean function, or (n,m)-function. When $m = n$, F can be uniquely represented as a univariate polynomial over $\mathbb{F}_{2^n}$ (using the natural identification of the finite field with the vector space) of the form $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$, $a_i \in \mathbb{F}_{2^n}$. The algebraic degree of F is then the largest Hamming weight of the exponents i, with $a_i \neq 0$. For an (n,m)-function F, we define the Walsh transform $\mathcal{W}_F(a,b)$ to be the Walsh-Hadamard transform of its component function $\mathrm{Tr}_1^m(bF(x))$ at a, that is,

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

For an (n,n)-function F, and $a, b \in \mathbb{F}_{2^n}$, we let $\Delta_F(a,b) = \#\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}$. 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 called an *almost perfect nonlinear* (*APN*) function. There are many useful characterizations and properties of APN functions, some of which are stated below (see [2, 4, 5, 10]).

Lemma 1. *Let F be an (n,n)-function. The following hold:*

(i) we 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 $F(0) = 0$ and F is APN, 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 $F(x) + F(y) + F(z) + F(x+y+z) = 0$, belong to the curve $(x+y)(x+z)(y+z) = 0$.

We next introduce the notion of a partial APN function. Let $x_0 \in \mathbb{F}_{2^n}$. We call an (n,n)-function F a (*partial*) *x_0-APN function*, or simply x_0-APN function, if all the points u, v satisfying $F(x_0) + F(u) + F(v) + F(x_0+u+v) = 0$, belong to the curve $(x_0+u)(x_0+v)(u+v) = 0$. Certainly, an APN function is an x_0-APN for any point x_0.

A function F is called *weakly APN* if for any $a \neq 0$ the function $F(x+a) + F(x)$ takes at least $2^{n-2} + 1$ different values (see [1]). Note that the notion of partial APN function differs from the notion of weakly APN function. For example, it can be checked that $F(x) = x^{2^n-2}$ over $\mathbb{F}_{2^n}$ with n even is weakly APN but not x_0-APN, for $x_0 \in \mathbb{F}_{2^n}$. On the other hand, $F(x) = x^7$ over $\mathbb{F}_{2^{11}}$ is 0-APN but not weakly APN.

Our proposal for the partial APN concept comes from a study of the conjecture in [2], which claims that for $n \geq 3$ an APN function modified at a point cannot remain APN. While this work has some overlap with [2], our ultimate goal is to investigate the partial APN concept.

2 Boolean functions modified at a point

Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and consider an arbitrary point $x_0 \in \mathbb{F}_{2^n}$ and some nonzero $\epsilon \in \mathbb{F}_{2^n}^*$. Denote $y_0 = F(x_0)$ and $y_1 = y_0 + \epsilon$. Then the function F' over $\mathbb{F}_{2^n}$ defined by

$$F'(x) = \begin{cases} F(x) & \text{if } x \neq x_0 \\ y_1 & \text{if } x = x_0. \end{cases} \tag{1}$$

is called a *(single point)* (x_0, y_1)*-modification of* F.

It is rather easy to show that there are single point modifications of an APN function F that are not APN.

Proposition 2. *If an* (n, n)*-function* F *is APN for* $n > 1$*, then for any* $x_0 \in \mathbb{F}_{2^n}$ *there exists* $\epsilon \in \mathbb{F}_{2^n}^*$ *such that the* $(x_0, F(x_0) + \epsilon)$*-modification of* F *is not APN.*

Proof. Suppose F is APN and $x_0 \in \mathbb{F}_{2^n}$ is given. Take $y, z \in \mathbb{F}_{2^n}$ such that x_0, y and z are distinct and let F' be the $(x_0, F(y) + F(z) + F(x_0 + y + z))$ modification of F. Then we have $F'(x_0) \neq F(x_0)$ since F is APN and $F'(x_0) + F'(y) + F'(z) + F'(x_0 + y + z) = 0$ so that F' cannot be APN. □

Next, we find some necessary and sufficient conditions for an (x_0, y_1)-modification of a given function to be partially APN.

Lemma 3. *Let* F *be an* (n, n)*-function and* F' *be an* (x_0, y_1)*-modification of* F *for* $x_0, y_1 \in \mathbb{F}_{2^n}$ *and* $y_1 \neq y_0 = F(x_0)$*. Then, with* $\epsilon = y_0 + y_1$*,*

$$\mathcal{W}_{F'}(a, b) = \mathcal{W}_F(a, b) - (-1)^{\mathrm{Tr}_1^n(ax_0 + by_0)}(1 - (-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}).$$

For any given elements $a, b \in \mathbb{F}_{2^n}$ let us denote $E_F(a, b) = (-1)^{\mathrm{Tr}_1^n(ax_0 + by_0)} D_F(b)$ where $D_F(b) = 1 - (-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}$. Note that $E_F(a, b)$ depends on x_0, y_0 and y_1.

Lemma 4. *Let* F *be an* (n, n)*-function and let* $x_0, y_1 \in \mathbb{F}_{2^n}$ *with* $y_1 \neq y_0 = F(x_0)$ *and* $\epsilon = y_0 + y_1$*. Then for any integer* $m \geq 1$ *and any elements* $a, b \in \mathbb{F}_{2^n}$*, we have*

(*i*) $E_F^{2m}(a, b) = 2^{2m-1} D_F(b)$*, and*

(*ii*) $E_F^{2m+1}(a, b) = 2^{2m} E_F(a, b)$.

In the following we make use of the Kronecker function $\delta_0(z) = \begin{cases} 1 & \text{if } z = 0 \\ 0 & \text{if } z \neq 0. \end{cases}$

Theorem 5. *Let* F *be an* (n, n)*-function and* F' *be its* (x_0, y_1)*-modification for some* $x_0, y_1 \in \mathbb{F}_{2^n}$ *with* $y_1 \neq y_0 = F(x_0)$*. Then the following hold:*

(*i*) $\dfrac{1}{4} \displaystyle\sum_{a,b \in \mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a, b) - \mathcal{W}_{F'}^4(a, b)\right) = \sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a, b) E_F(a, b) - (3 \cdot 2^{3n} - 2^{2n+1})$;

$$(ii)\ \sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 3\cdot 2^{2n+1} \cdot \left(\delta_0(F(0)) - \delta_0(y_1 - y_0 + F(0))\right) + 2^{2n+2}\delta_0(x_0)\left(\delta_0(y_0) - \delta_0(y_1)\right).$$

Proof. We show (i) first. Taking fourth powers in the identity $\mathcal{W}_{F'}(a,b) = \mathcal{W}_F(a,b) - E_F(a,b)$ of Lemma 3 and applying Lemma 4, we get

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right)\\
&= \sum_{a,b\in\mathbb{F}_{2^n}} \left(4\mathcal{W}_F^3(a,b)E_F(a,b) - 6\mathcal{W}_F^2(a,b)E_F^2(a,b) + 4\mathcal{W}_F(a,b)E_F^3(a,b) - E_F^4(a,b)\right)\\
&= \sum_{a,b\in\mathbb{F}_{2^n}} \left(4\mathcal{W}_F^3(a,b)E_F(a,b) - 12\mathcal{W}_F^2(a,b)D_F(b) + 16\mathcal{W}_F(a,b)E_F(a,b) - 8D_F(b)\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
&\frac{1}{4}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right)\\
&= \sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b)E_F(a,b) - 3\mathcal{W}_F^2(a,b)D_F(b) + 4\mathcal{W}_F(a,b)E_F(a,b) - 2D_F(b)\right).
\end{aligned}$$

We now observe that $\sum_{a,b\in\mathbb{F}_{2^n}} D_F(b) = 2^n \sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^n \sum_{b\in\mathbb{F}_{2^n}} (1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}) = 2^{2n}$, since $\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$ when $\epsilon \neq 0$. Further, by Parseval's identity we get $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)D_F(b) = \sum_{b\in\mathbb{F}_{2^n}} D_F(b) \sum_{a\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b) = 2^{2n}\sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^{3n}$. Finally, we use the inverse Walsh-Hadamard transform to obtain

$$\begin{aligned}
\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)E_F(a,b) &= \sum_{a,b,u\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+y_0)+a(u+x_0))} D_F(b)\\
&= \sum_{b,u\in\mathbb{F}_{2^n}} \left(D_F(b)(-1)^{\mathrm{Tr}_1^n(b(F(u)+y_0))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+x_0))} \right)\\
&= 2^n \sum_{b\in\mathbb{F}_{2^n}} \left(D_F(b)(-1)^{\mathrm{Tr}_1^n(b(F(x_0)+y_0))} \right) = 2^n \sum_{b\in\mathbb{F}_{2^n}} D_F(b) = 2^{2n}.
\end{aligned}$$

Combining the above results, we obtain

$$\frac{1}{4}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) = \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) - (3\cdot 2^{3n} - 2^{2n+1}),$$

and our first claim is shown.

By a similar argument as in part (i), we obtain

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right)$$

$$= \sum_{a,b\in\mathbb{F}_{2^n}} \left(3\mathcal{W}_F^2(a,b)E_F(a,b) - 3\mathcal{W}_F(a,b)E_F^2(a,b) + E_F^3(a,b)\right) \tag{2}$$
$$= 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 6\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)D_F(b) + 4\sum_{a,b\in\mathbb{F}_{2^n}} E_F(a,b).$$

Furthermore, we compute

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F(a,b)D_F(b)\\
&= \sum_{b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right) \sum_{u\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(u))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(au)}\\
&= 2^n \sum_{b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\right) (-1)^{\mathrm{Tr}_1^n(bF(0))}\\
&= 2^n \left(\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(0))} - \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(y_1-y_0+F(0))}\right)\\
&= 2^{2n}\left(\delta_0(F(0)) - \delta_0(y_1-y_0+F(0))\right),
\end{aligned}$$

and

$$\begin{aligned}
\sum_{a,b\in\mathbb{F}_{2^n}} E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} \left(1-(-1)^{\mathrm{Tr}_1^n(b(y_1-y_0))}\right)\\
&= 2^{2n}\delta_0(x_0)\left(\delta_0(y_0)-\delta_0(y_1)\right).
\end{aligned}$$

Using these identities in (2), we obtain

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right)\\
&= 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 3\cdot 2^{2n+1}\left(\delta_0(F(0)) - \delta_0(y_1-y_0+F(0))\right)\\
&\qquad + 2^{2n+2}\delta_0(x_0)\left(\delta_0(y_0)-\delta_0(y_1)\right),
\end{aligned}$$

and the theorem is shown. □

Corollary 6. *Let F be an (n,n)-function satisfying $F(0)=0$, and $x_0\in\mathbb{F}_{2^n}$, $\epsilon\in\mathbb{F}_{2^n}^*$. Let further F' be its $(x_0, F(x_0)+\epsilon)$-modification. Then we have, with $y_1 = F(x_0)+\epsilon$:*

(a) if $x_0 = y_0 = 0$ then $y_1\neq 0$ and

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) - 2^{2n+1};$$

(b) if $x_0\neq 0$ then

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

Proof. Follows easily from Theorem 5 (ii). □

Theorem 7. *Let F be an (n,n)-function and F' be its (x_0,y_1) modification. For any $x,y\in\mathbb{F}_{2^n}$, let*

$$\begin{aligned} T_{x,y} &= \{(u,v)\in\mathbb{F}_{2^n}^2 : (u+x)(v+x)(u+v)\neq 0, F(u)+F(v)+F(u+v+x)+y=0\},\\ S_{x,y} &= \{u\in\mathbb{F}_{2^n} : F(u)+F(u+x)+y=0\}. \end{aligned}$$

Then:

$$(i)\ \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0} - \#T_{x_0,y_1}\right);$$

$$(ii)\ \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) = 2^{2n}\left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right).$$

Proof. We only show (i), since (ii) is similar. We write

$$\begin{aligned} \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}\right)\\ &\qquad\cdot \sum_{u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+y_0))}(-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))}\\ &= \sum_{b,u,v,w\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}\right)(-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+y_0))}\\ &\qquad\cdot \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))}\\ &= 2^n \sum_{b,u,v\in\mathbb{F}_{2^n}} \left(1-(-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}\right)(-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_0))}\\ &= 2^n \sum_{u,v\in\mathbb{F}_{2^n}} \left(\sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_0))} \right. \qquad (3)\\ &\qquad \left. - \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(u+v+x_0)+y_1))} \right). \qquad (4) \end{aligned}$$

Now, the inner sums in (3) and (4) will be zero unless one of the exponents is zero, that is, if $F(u)+F(v)+F(u+v+x_0)+F(x_0)=0$ or $F(u)+F(v)+F(u+v+x_0)+y_1=0$.

Since there are $3\cdot 2^n-2$ pairs (u,v) satisfying $(u+x_0)(v+x_0)(u+v)=0$, the above equation becomes

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) = 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0} - \#T_{x_0,y_1}\right),$$

and the first claim is proven. □

Note that in the above theorem we in fact showed that $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} = 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right)$, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} = 2^{2n}\left(\#T_{x_0,y_1}\right)$. That is, for an (n,n)-function F and its one point modification F' at x_0, Theorem 7 gives

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} \\ - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} &= 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right) - 2^{2n}\left(\#T_{x_0,y_1}\right). \qquad (5)\end{aligned}$$

By Theorem 5, we get

$$\begin{aligned}\frac{1}{4}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) - 2^{2n}(3\cdot 2^n - 2) \\ &= 2^{2n}(\#T_{x_0,y_0} - \#T_{x_0,y_1}),\end{aligned}$$

where the last equality comes from the equation (5).

Therefore, we obtain the following equivalence:

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^4(a,b) - \mathcal{W}_{F'}^4(a,b)\right) = 0 \Longleftrightarrow \#T_{x_0,y_0} = \#T_{x_0,y_1}. \qquad (6)$$

The definition of x_0-APN implies that F' is x_0-APN if and only if $(u+x_0)(v+x_0)(u+v) \neq 0 \Longrightarrow F'(u)+F'(v)+y_1+F'(u+v+x_0) \neq 0$. However, when $(u+x_0)(v+x_0)(u+v) \neq 0$, one has $F'(u)+F'(v)+y_1+F'(u+v+x_0) = F(u)+F(v)+y_1+F(u+v+x_0)$. Therefore, F' is x_0-APN if and only if $(u+x_0)(v+x_0)(u+v) \neq 0 \Longrightarrow F(u)+F(v)+y_1+F(u+v+x_0) \neq 0$. In other words, F' is x_0-APN if and only if T_{x_0,y_1} is the empty set.

Now, the set T_{x_0,y_0} with $y_0 = F(x_0)$ is empty if and only if F is x_0-APN. By (6) and Lemma 1 we have:

Theorem 8. *If F is APN and its (x_0,y_1)-modification F' with $y_1 \neq F(x_0)$ is x_0-APN, then F' is APN.*

Note that this can also be directly derived from the definition of one point modification. Indeed, suppose to the contrary, that F' is x_0-APN but it is not APN. Then for some $a \neq 0$ and some b the equation $F'(x+a)+F'(x) = b$ has more than 2 solutions. Let x_1, x_2, x_3 be three distinct solutions to this equation. We consider two cases. If $\{x_1,x_2,x_3\} \cap \{x_0, x_0+a\} = \emptyset$ then $F'(x_i+a)+F'(x_i) = F(x_i+a)+F(x_i)$ for $i \in \{1,2,3\}$ and this contradicts F being APN. If $\{x_1,x_2,x_3\} \cap \{x_0, x_0+a\} \neq \emptyset$, then it contradicts F' being x_0-APN.

In light of Theorem 8, it follows that the conjecture from [2] can be strengthened as follows:

Conjecture 9. *An (x_0,y_1)-modification of an APN function with $y_1 \neq F(x_0)$ is not x_0-APN.*

One way of showing that this is true would be to show $\{F(x_0)+F(u)+F(v)+F(x_0+u+v) : u,v \in \mathbb{F}_{2^n}\} = \mathbb{F}_{2^n}$. Indeed, suppose that F' is an (x_0,y_1)-modification

of F with $y_1 \neq y_0 = F(x_0)$ and that F' is not APN. This is true if and only if the equation $F'(x_0) + F'(u) + F'(v) + F'(x_0 + u + v) = 0$ is satisfied by a pair of elements $u, v \in \mathbb{F}_{2^n}$ with $(u + x_0)(v + x_0)(u + v) \neq 0$. Writing $\epsilon = y_0 + y_1$, this is equivalent to $F(x_0) + F(u) + F(v) + F(x_0 + u + v) = \epsilon$ or, in other words, $\epsilon \in \{F(x_0) + F(u) + F(v) + F(x_0 + u + v) : u, v \in \mathbb{F}_{2^n}\}$. Thus, the difference ϵ between $F(x_0)$ and $F'(x_0)$ must not be expressible as $D_aF(x_0) + D_aF(y)$ in order for F' to be x_0-APN.

Corollary 10. *Let F be an (n, n)-function and let F' be its (x_0, y_1)-modification for $x_0, y_0 \in \mathbb{F}_{2^n}$ with $y_1 \neq y_0 = F(x_0)$. Then,*

$$\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3 \cdot 2^{2n} \left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 3 \cdot 2^{2n+1} \left(\delta_0(F(0)) - \delta_0(y_1 - y_0 + F(0))\right) + 2^{2n+2}\delta_0(x_0) \left(\delta_0(y_0) - \delta_0(y_1)\right).$$

Furthermore,

(a) *If $F(0) = 0 \neq x_0$, then,* $\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3 \cdot 2^{2n} \left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 3 \cdot 2^{2n+1}$;

(b) *If $F(0) = 0 = x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 3 \cdot 2^{2n} \left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 2^{2n+1} = 2^{2n+1}(3 \cdot 2^{n-1} - 1)$;

(c) *If F is APN and $F(0) = 0 \neq x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1) + 3 \cdot 2^{2n} \#S_{x_0,y_1}$;

(d) *If F is APN and $F(0) = 0 = x_0$, then* $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 0$.

Proof. Item (a) and the first equation in (b) follow easily from Theorem 5 (ii) and Theorem 7 (ii). For the second equation of (b), we suppose $F(0) = 0 = x_0$. Then, $S_{x_0,y_0} = \{u \in \mathbb{F}_{2^n} | F(u) + F(u) + F(0) = 0\} = \mathbb{F}_{2^n}$, so $\#S_{x_0,y_0} = 2^n$. Also, $S_{x_0,y_1} = \{u \in \mathbb{F}_{2^n} | F(u) + F(u) + F'(0) = 0\} = \emptyset$, so $\#S_{x_0,y_1} = 0$.

To show (c), we assume that F is APN with $F(0) = 0 \neq x_0$. Then, $S_{x_0,y_0} = \{u \in \mathbb{F}_{2^n} | F(u) + F(u + x_0) + F(x_0) = 0\} = \{0, x_0\}$. By Lemma 1, we get $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1)$. By Theorem 5 (ii) and the main claim of this corollary, we have

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) &= 2^{2n+1}(3 \cdot 2^{n-1} - 1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) \\ &= 3 \cdot 2^{2n} \left(\#S_{x_0,y_0} - \#S_{x_0,y_1}\right) - 3 \cdot 2^{2n+1},\end{aligned}$$

which is equivalent to $2^{2n+1}(3 \cdot 2^{n-1} - 1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 3 \cdot 2^{2n} \left(2 - \#S_{x_0,y_1}\right) - 3 \cdot 2^{2n+1}$, and so, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 2^{2n+1}(3 \cdot 2^{n-1} - 1) + 3 \cdot 2^{2n} \#S_{x_0,y_1}$.

To show (d), we now suppose that F is APN and $F(0) = 0 = x_0$. Then, by Lemma 1 and point (b) of this corollary, $\sum_{a,b\in\mathbb{F}_{2^n}} \left(\mathcal{W}_F^3(a,b) - \mathcal{W}_{F'}^3(a,b)\right) = 2^{2n+1}(3\cdot 2^{n-1} - 1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1} - 1)$, which implies that $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^3(a,b) = 0$, and the claim is shown. □

3 A characterization of partial APN functions

We now provide a necessary and sufficient condition for a function to be x_0-APN. As a consequence of our theorem we can obtain the APN conditions of Lemma 1.

Theorem 11. *Let F be an (n,n)-function and $x_0 \in \mathbb{F}_{2^n}$. Then F is x_0-APN if and only if*

$$\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))} = 2^{2n+1}(3\cdot 2^{n-1} - 1).$$

Proof. We have

$$\begin{aligned}
&\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))} \\
&= \sum_{a,b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(ax_0+bF(x_0))} \sum_{u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w))+a(u+v+w))} \\
&= \sum_{b,u,v,w\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(w)+F(x_0)))} \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+w+x_0))} \\
&= 2^n \sum_{b,u,v\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(x_0)+F(u+v+x_0)))} \\
&= 2^n \sum_{u,v\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(v)+F(x_0)+F(u+v+x_0)))} \\
&= 2^{2n} \#\{(u,v)\in\mathbb{F}_{2^n}^2 : F(u)+F(v)+F(x_0)+F(u+v+x_0) = 0\} \\
&= 2^{2n}\left(3\cdot 2^n - 2 + \#T_{x_0,y_0}\right).
\end{aligned}$$

Since T_{x_0,y_0} is empty if and only if F is x_0-APN, the claim follows. □

4 Monomial partial APN functions

For a monomial $F(x) = x^m$, the polynomial $G(x,y,z) = F(x)+F(y)+F(z)+F(x+y+z)$ is a symmetric homogeneous polynomial of degree m, and so, $G(kx,ky,kz) = k^m G(x,y,z)$ for all $k \in \mathbb{F}_{2^n}$. Using this property, we show that a monomial F is APN if and only if F is partial APN on a subspace of dimension 1 (that is, it is partial APN at 0 and some $x_0 \neq 0$).

Proposition 12. *Let $F(x) = x^m$ over $\mathbb{F}_{2^n}$. Then:*

(*i*) *If $x_0 \neq 0$, then F is x_0-APN if and only if F is x_1-APN for all $x_1 \in \mathbb{F}_{2^n}^*$;*

(*ii*) *F is APN if and only if F is 0-APN and x_1-APN for some $x_1 \in \mathbb{F}_{2^n}^*$.*

Proof. Certainly, (*ii*) is a consequence of (*i*). For a proof of the first claim, note that F is x_0-APN if and only if $G(x_0, y, z) \neq 0$ for all y, z with $(y + x_0)(z + x_0)(y + z) \neq 0$. Using the homogeneous property of G, $0 \neq G(x_0, y, z) = G(kx_0, ky, kz)$ for any $k \neq 0$, so the condition can be written as $G(x_1, y, z) \neq 0$ for all $x_1 \neq 0$ and y, z with $(y+x_1)(z+x_1)(y+z) \neq 0$. □

Charpin and Kyureghyan [6] also considered a partial APN concept on (n, n)-functions: we say that F satisfies the property (p_a), $a \in \mathbb{F}_{2^n}^*$, if the equation $F(x)+F(x+a) = b$ has either 0 or 2 solutions for every $b \in \mathbb{F}_{2^n}$. They showed that a mapping F is APN if and only if F satisfies (p_a) for all nonzero a belonging to a hyperplane. It is not clear if such a result is true for our notion of partial APNness. From the result above, we see that a similar result is true for monomials, i.e. F is APN if and only if it is partial APN for a subspace of dimension 1. Moreover, when F is a monomial, the property (p_1) implies the property (p_a) for any $a \neq 0$. Therefore our result on 0-APN has some analogy with the property (p_1), but 0-APN is a more general condition than the property (p_1), as the following examples will show.

We let $\binom{a}{b}_2$ denote the residue modulo 2 of the binomial coefficient $\binom{a}{b}$. We next investigate and explicitly construct many classes of Boolean functions that are 0-APN (but not necessarily APN).

Theorem 13. *Let $\mathbb{F}_{2^n}$ be the extension field of $\mathbb{F}_2$ corresponding to the primitive polynomial f of degree n and let g be one of the (primitive) roots of f. Then:*

(*i*) *if $F(x) = x^m$ over $\mathbb{F}_{2^n}$, then F is 0-APN if and only if for $1 \leq i \leq 2^n-1$, the minimal polynomial $P_{g^i}(X) = \prod_{j \in C_i}(X - g^j)$ of g^i, where $C_i = \{(i \cdot 2^j) \pmod{2^n - 1} : j = 0, 1, \ldots\}$ is the unique cyclotomic coset of i modulo $2^n - 1$, does not divide $\sum_{k=1}^{mi-1} \binom{mi}{k}_2 x^{mi-k-1}$;*

(*ii*) *if $F(x) = x^{2^d-1}$ over $\mathbb{F}_{2^n}$, where $\gcd(d - 1, n) = 1$, then F is 0-APN;*

(*iii*) *if $F(x) = x^{2^d+1}$ over $\mathbb{F}_{2^n}$, where $\gcd(d, n) = 1$, then F is 0-APN.*

Proof. If $F(x) = x^m$, then F is 0-APN if and only if the Rodier equation $F(y) + F(z) + F(y + z) = y^m + z^m + (y + z)^m = 0$, has no solution $y, z \in \mathbb{F}_{2^n}^*$ with $y \neq z$. Given two distinct elements $y, z \in \mathbb{F}_{2^n}^*$, let $z = y\alpha$, where $\alpha \neq 0, 1$. Then, the equation above becomes $y^m (1 + \alpha^m + (1 + \alpha)^m) = 0$, implying $1 + \alpha^m + (1 + \alpha)^m = 0$. Then, if there exists $\alpha \neq 0, 1$ satisfying the previous equation, then there exists $1 \leq i \leq 2^n - 1$ such that $\dfrac{1 + X^{im} + (1 + X^i)^m}{X} = \displaystyle\sum_{k=1}^{mi-1} \binom{mi}{k}_2 x^{mi-k-1}$ vanishes at g, that is, $1+g^{i\,m}+(1 + g^i)^m = 0$. Then it will vanish at g^{2^ℓ}, for all ℓ, since $1+g^{i\,m\,2^\ell}+\left(1 + g^{i\,2^\ell}\right)^m =$

$(1+g^{i\,m}+(1+g^i))^{2^\ell}=0$. Thus, the minimal polynomial $P_{g^i}(X)=\prod_{j\in C_i}(X-g^j)$ of g^i divides $\sum_{k=1}^{mi-1}\binom{mi}{k}_2 x^{mi-k-1}$. The converse is certainly true, and the first claim is shown.

To test whether $F=x^{2^d-1}$ is 0-APN, one needs to check the (in)solvability of the Rodier equation $0=F(y)+F(z)+F(y+z)=y^{2^d-1}+z^{2^d-1}+(y+z)^{2^d-1}=\dfrac{zy^{2^d-1}+yz^{2^d-1}}{y+z}=\dfrac{(\alpha^{2^d-1}+\alpha)z^{2^d}}{z(\alpha+1)}$, where $y=z\alpha, \alpha\neq 0,1$. Therefore, when $\gcd(2^d-2,2^n-1)=1$, there is no $\alpha\neq 0,1$ satisfying the above equation, that is, x^{2^d-1} is 0-APN. The condition $\gcd(d-1,n)=1$ follows form the known identity $\gcd(2^a-1,2^b-1)=2^{\gcd(a,b)}-1$, since $1=\gcd(2^d-2,2^n-1)=\gcd(2^{d-1}-1,2^n-1)=2^{\gcd(d-1,n)}-1$.

In the same way, we consider $F(x)=x^{2^d+1}$ over $\mathbb{F}_{2^n}$. To test whether F is 0-APN, one needs to check the solvability of the Rodier equation

$$0=F(y)+F(z)+F(y+z)=y^{2^d+1}+z^{2^d+1}+(y+z)^{2^d+1}=zy^{2^d}+yz^{2^d}=(\alpha^{2^d}+\alpha)z^{2^d+1},$$

where $y=z\alpha, \alpha\neq 0,1$. Therefore, when $1=\gcd(2^d-1,2^n-1)=2^{\gcd(d,n)}-1$, that is, for $\gcd(d,n)=1$, there is no $\alpha\neq 0,1$ satisfying the above equation, so x^{2^d+1} is 0-APN. □

n	Exponents i	Δ_F
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7,21,35,61,83,91,111,117,119,175	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	12

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

Example 14. Table 1 lists the exponents i for which x^i is 0-APN but not APN over $\mathbb{F}_{2^n}$. Only one representative from every cyclotomic coset is given. There are no functions of this type for $n\leq 5$. We also verified that there are no power functions $F(x)=x^i$ over $\mathbb{F}_{2^n}$,

$n \leq 15$, which are 1-APN but not 0-APN, suggesting that perhaps 1-APN-ness implies 0-APN-ness for power functions. This is not true in general: we found over six million polynomials over $\mathbb{F}_{2^3}$ that are 1-APN but not APN, for example, $x^7 + x^6$. Out of these, 64 have coefficients in $\mathbb{F}_2$: 48 of them have the differential spectrum $\{0^{31}, 2^{22}, 4^3\}$, while the remaining 16 have the spectrum $\{0^{42}, 2^7, 6^7\}$. We also found 6944 polynomials of this type over $\mathbb{F}_{2^4}$ with coefficients in $\mathbb{F}_2$, for example, $x^{12} + x^7$.

References

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

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

[3] 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.

[4] 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.

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

[6] P. Charpin, G. M. Kyureghyan, *On sets determining the differential spectrum of mappings*, Internat. J. Inf. Coding Theory 4(2-3) (2017), 170–184.

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

[8] S. Mesnager, Bent functions: fundamentals and results, Springer Verlag, 2016.

[9] F. Rodier, *Functions of degree* $4e$ *that are not APN infinitely often*, Cryptogr. Commun. 3:4 (2011), 227–240.

[10] 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.

[11] N. Tokareva, Bent Functions, Results and Applications to Cryptography, Academic Press, San Diego, CA, 2015.