Partially APN Boolean functions and classes of functions that are not APN infinitely often

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. In the second part of the paper, we find conditions for some transformations not to be partially APN, and in the process, we find classes of functions that are never APN for infinitely many extensions of the prime field $\mathbb{F}_2$, extending some earlier results of Leander and Rodier.

Keywords: Boolean function, almost perfect nonlinear (APN), partial APN, Walsh-Hadamard coefficients.
2010 MSC: 94A60, 94C10, 06B30

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 [2, 6, 7, 10] 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. 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 $\Delta_F(a,b) = \#\{x \in \mathbb{F}_{2^n} : F(x+a) + F(x) = b\}$, where $\#S$ denotes the cardinality of a set S. 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 [3, 7, 8, 15]).

Lemma 1.1. *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.

Definition 1.2. 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 $(x_0+u)(x_0+v)(u+v)=0$.

Alternatively, we can say that a function F is x_0-APN if for any $a \neq 0$ the equation $F(x+a)+F(x) = F(x_0+a)+F(x_0)$ has only two solutions. 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 [5]). 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 [3], which claims that for $n \geq 3$ an APN function modified at a point cannot remain APN. While the start of this work has some initial study overlap with [3], our ultimate goal is to investigate the partial APN concept.

Our paper is organized as follows. In Section 2 we introduce the one point modification of an (n,n)-function and investigate its Walsh coefficients' third and fourth moments as compared to the original function. We further give a (local-global principle) characterization for the APNess of the modified version of an APN function, which was the original starting point of this investigation. A conjecture is proposed here, slightly strengthening the original conjecture of [3]. Section 3 contains a standalone characterization of the partial APN concept in terms of the third moments. In Section 4 we continue with some constructions and characterization of the pAPN property for monomial functions (in particular, we show that for power functions, the pAPN at a nonzero point will imply APNess, and, in general, the pAPNess at a nonzero point will imply APNess for quadratic functions). In Section 5, in the spirit of Rodier et al. we concentrate on the various linear transformations of some functions to show (non)pAPNess and in the process we show a much stronger version of a result by Leander and Rodier [12]. Section 6 contains the conclusion and further comments.

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, ϵ)-*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 2.1. *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, ϵ)-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 $(x_0, \epsilon = F(y) + F(z) + F(x_0 + y + z) - F(x_0))$-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, ϵ)-modification of a given function to be partially APN.

2.1 Preliminary lemmas

Lemma 2.2. *Let F be an (n,n)-function and F' be an (x_0, ϵ)-modification of F for $x_0, y_1 = y_0 + \epsilon \in \mathbb{F}_{2^n}$ and $y_1 \neq y_0 = F(x_0)$. Then,*

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

Proof. We have

$$\begin{aligned} \mathcal{W}_{F'}(a,b) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF'(x)+ax)} = \sum_{x \neq x_0} (-1)^{\mathrm{Tr}_1^n(bF(x)+ax)} + (-1)^{\mathrm{Tr}_1^n(by_1+ax_0)} \\ &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(bF(x)+ax)} + (-1)^{\mathrm{Tr}_1^n(ax_0+by_1)} - (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)}, \end{aligned}$$

which justifies our claim. □

For any given elements $a, b \in \mathbb{F}_{2^n}$, we let $E_F(a,b) = (-1)^{\mathrm{Tr}_1^n(ax_0+by_0)} D_F(b)$, where $D_F(b) = 1 - (-1)^{\mathrm{Tr}_1^n(b\,\epsilon)}$. Note that $E_F(a,b)$ depends on x_0, y_0, y_1. The following lemma can be easily shown by induction.

Lemma 2.3. *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) $E_F^{2m+1}(a,b) = 2^{2m} E_F(a,b)$.

2.2 The third and fourth moments and an APN characterization of a one point modification of an APN function

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

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

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

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 2.2 and applying Lemma 2.3, 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

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

Furthermore, with $\epsilon = y_1 - y_0$, we compute

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

$$= 2^{2n} \left(\delta_0(F(0)) - \delta_0(y_1 - y_0 + F(0)) \right),$$

and

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

Using these identities in (2), we obtain

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

and the theorem is shown. □

Corollary 2.5. *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, ϵ)-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 2.4 (ii). □

Corollary 2.6. *Let F be an APN (n,n)-function satisfying $F(0) = 0$. Let $x_0 = 0 = y_0$, and let F' be the $(0, \epsilon)$-modification of F. Then, F' is APN if and only if*

$$\sum_{a,b \in \mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) (-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0.$$

Proof. By Lemma 1.1, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^4(a,b) = 2^{3n+1}(3\cdot 2^{n-1}-1)$, and $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1}-1)$. Also, by the same lemma, F' is APN if and only if $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_{F'}^4(a,b) = 2^{3n+1}(3\cdot 2^{n-1}-1)$. This, together with Theorem 2.4 (i), implies that F' is APN if and only if

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

On the other hand, since $x_0 = 0 = y_0$, $E_F(a,b) = D_F(a,b) = 1-(-1)^{\mathrm{Tr}_1^n(b\epsilon)}$, and

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)E_F(a,b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)}\\ &= 2^{2n+1}(3\cdot 2^{n-1}-1) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)}.\end{aligned}$$

This, together with the previous corollary, gives the sufficient and necessary condition $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$. □

2.3 A local-global principle of APNess

In this subsection we will show that a single point modification of an APN function is APN if and only if is partially APN.

Theorem 2.7. *Let F be an (n,n)-function and F' be its (x_0,ϵ)-modification, $y_1 = y_0+\epsilon$. For any $x,y\in\mathbb{F}_{2^n}$, let*

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

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. To show (i), 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, unless $F(u)+F(v)+F(u+v+x_0)+F(x_0)=0$ 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. To show (ii) we write

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

$$\cdot \sum_{a\in\mathbb{F}_{2^n}} (-1)^{\mathrm{Tr}_1^n(a(u+v+x_0))}$$

$$= 2^n \sum_{u\in\mathbb{F}_{2^n}} \sum_{b\in\mathbb{F}_{2^n}} \left((-1)^{\mathrm{Tr}_1^n(b(F(u)+F(u+x_0)+y_0))} - (-1)^{\mathrm{Tr}_1^n(b(F(u)+F(u+x_0)+y_1))}\right)$$
$$= 2^{2n}\left(|S_{x_0,y_0}| - |S_{x_0,y_1}|\right),$$

and the theorem 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 2.7 gives

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

By Theorem 2.4, 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 1.1 we have:

Theorem 2.8. *If F is APN and its (x_0,ϵ)-modification F' with $\epsilon \neq 0$ 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 the fact that F' is x_0-APN.

In light of Theorem 2.8, it follows that the conjecture from [3] can be strengthened as follows:

Conjecture 2.9. *An (x_0,ϵ)-modification of an APN function with $\epsilon \neq 0$ 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,ϵ)-modification of F with $y_1 = y_0+\epsilon \neq y_0 = F(x_0)$ 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 2.10. *Let F be an (n,n)-function and let F' be its (x_0,ϵ)-modification for $x_0, y_0 \in \mathbb{F}_{2^n}$ with $\epsilon \neq 0$. Then,*

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

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. The main claim, item (a) and the first equation in (b) follow easily from Theorem 2.4 (ii) and Theorem 2.7 (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 1.1, we get $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^3(a,b) = 2^{2n+1}(3\cdot 2^{n-1} - 1)$. From this and the main claim of this corollary, we have

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

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 1.1 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. □

Note that Corollary 2.6 can also be deduced from Theorem 2.7. Furthermore, we can deduce the following corollary:

Corollary 2.11. *Let F be an (n,n)-function. Let $x_0 = 0 = y_0$, and F' be the $(0,\epsilon)$-modification of F for some $\epsilon \in \mathbb{F}_{2^n}^*$. Then, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} = 0$.*

Proof. Using the notation of Theorem 2.7, $S_{0,0} = \mathbb{F}_2^n$, while $S_{0,\epsilon} = \emptyset$. Then, by Theorem 2.7, $\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(a,b) = 2^{3n}$. On the other hand,

$$\begin{aligned}\sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)E_F(b) &= \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b) - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)} \\ &= 2^{3n} - \sum_{a,b\in\mathbb{F}_{2^n}} \mathcal{W}_F^2(a,b)(-1)^{\mathrm{Tr}_1^n(b\epsilon)},\end{aligned}$$

which shows the corollary. □

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 1.1.

Theorem 3.1. *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 4.1. *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). To show the first claim, it will be enough to show the necessity part only. Now, we assume that F is x_0-APN, that is $G(x_0, y, z) \neq 0$ for all y, z with $(y+x_0)(z+x_0)(y+z) \neq 0$, and we want to show that F is x_1-APN for any other $x_1 \in \mathbb{F}_{2^n}^*$. By absurd, we assume that there is some $x_1 \neq 0$, for which F is not x_1-APN. Then, there exist $x_1 \neq y_1 \neq z_1 \neq x_1$ such that $G(x_1, y_1, z_1) = 0$. Using the homogeneous property of G, namely $0 = k^m G(x_1, y_1, z_1) = G(kx_1, ky_1, kz_1)$ for any $k \neq 0$, and taking $k = x_0/x_1 \neq 0$, then the condition can be written as $G(x0, y, z) = 0$ for $y = ky_1, z = kz_1$ and y, z with $(y + x_0)(z + x_0)(y + z) \neq 0$, and that is a contradiction. □

A partial APN concept on (n, n)-functions is also considered in [9]: F is said to satisfy 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 in general 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 4.2. *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 $\mathbb{F}_{2^n}$, then F is 0-APN if and only if $\gcd(d - 1, n) = 1$;

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

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

$$y^m \left(1 + \alpha^m + (1 + \alpha)^m\right) = 0,$$

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

$$\frac{1 + x^{im} + (1 + x^i)^m}{x} = \sum_{k=1}^{m-1} \binom{m}{k}_2 x^{i(m-k)-1}$$

vanishes at g, that is, $1 + g^{i\,m} + \left(1 + g^i\right)^m = 0$. Then it will vanish at g^{2^ℓ}, for all ℓ, since $1 + g^{i\,m\,2^\ell} + \left(1 + g^{i\,2^\ell}\right)^m = \left(1 + g^{i\,m} + \left(1 + g^i\right)\right)^{2^\ell} = 0$. 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

$$\begin{aligned} 0 &= F(y) + F(z) + F(y + z) \\ &= y^{2^d-1} + z^{2^d-1} + (y + z)^{2^d-1} \\ &= \frac{zy^{2^d-1} + yz^{2^d-1}}{y + z} = \frac{(\alpha^{2^d-1} + \alpha)z^{2^d}}{z(\alpha + 1)}, \end{aligned}$$

where $y = z\alpha, \alpha \neq 0, 1$. Therefore, when (and only 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

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

where $y = z\alpha, \alpha \neq 0, 1$. Therefore, when (and only 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
1-5	-	-
6	27	12
7	7,21,31,55	6
	19,47	4
8	15,45	14
	21,111	4
	51	50
	63	6
9	7,21,35,61,63,83,91,111,117,119,175	6
	41,187	8
	45,125	4
10	15,27,45,75,111,117,147,189,207,255	6
	21,69,87,237,375	4
	51	8
	93	92
	105,351	10
	231,363,495	42
	447	12

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

Example 4.3. Table 1 lists the exponents i for which x^i is 0-APN but not APN over $\mathbb{F}_{2^n}$ for $1 \leq n \leq 10$. Only one representative from every cyclotomic coset is given. There are no functions of this type for $n \leq 5$.

While there are power functions that are partial 0-APN but not APN, this is not true for partial 1-APN power functions. The proof is, in fact, rather immediate (we thank Dr. Namhun Koo for providing the included short proof here).

Theorem 4.4. *Any partial* 1*-APN power function* $F(z) = z^k$ *is APN.*

Proof. By proposition 4.1, it will be sufficient to show that f is 0-APN. Suppose, on the contrary, that $F(z) = z^k$ is not 0-APN. Then there exist $x, y \in \mathbb{F}_{2^n}$ with $xy(x+y) \neq 0$ satisfying $F(0)+F(x)+F(y)+F(x+y) = 0$. Since $x \neq 0$,

$$\begin{aligned} 0 &= F(x) + F(y) + F(x+y) = x^k + y^k + (x+y)^k \\ &= 1 + (y/x)^k + (1+y/x)^k = F(1) + F(y/x) + F(1+y/x) \\ &= F(1) + F(a) + F(b) + F(1+a+b), \end{aligned}$$

where $a = \frac{y}{x}$, $b = 1 + \frac{y}{x}$, $1 + a + b = 0$. Since F is 1-APN, one must have $(a+1)(b+1)(a+b) = 0$. However,

$$0 = (a+1)(b+1)(a+b) = \left(\frac{y}{x} + 1\right) \cdot \frac{y}{x} \cdot 1.$$

Thus we get $x = y$ or $y = 0$, contradicting the fact $xy(x+y) \neq 0$. □

This is not true in general, for non-monomials: 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, $x^{12} + x^7$.

Nonetheless, it seems likely that if some (n,n)-function F is x-APN for all $x \in \mathbb{F}_{2^n} \setminus \{x_0\}$, then it is x_0-APN (and hence APN) as well. This can be easily observed to be true for quadratic functions. Recall that F is x_0-APN if for any $a \neq 0$ the equation $F(x_0)+F(x)+F(x+a)+F(x_0+a) = D_aF(x)+D_aF(x_0) = 0$ has precisely two solutions, namely, $x = x_0$ and $x = x_0 + a$. Since D_aF is an affine function, this is equivalent to $D_aF(x+x_0) = D_aF(0)$ having only $x = x_0$ and $x = a + x_0$ as solutions.

Proposition 4.5. *Let* F *be a quadratic* (n,n)*-function and* $x_0 \in \mathbb{F}_{2^n}$*. Then* F *is* x_0*-APN if and only if* F *is APN.*

5 Classes of never 0-APN (hence never APN) for infinitely many extensions of $\mathbb{F}_2$

Building up on some of their earlier work on the function $x^3+\mathrm{Tr}_1^n(x^9)$, which is APN on $\mathbb{F}_{2^n}$, for all dimensions n, Budaghyan et al. [4] generalized this class to $L_1(x^3)+L_2(x^9)$, where L_1, L_2 are linear functions on $\mathbb{F}_{2^n}$, and found conditions under which this function is APN.

In a series of papers, Rodier and his collaborators [1, 11, 12, 14, 15] concentrated on finding classes of functions that are never APN for infinitely many extensions of the prime field $\mathbb{F}_2$. Here we present classes of functions that are never 0-APN (and hence never APN) for infinitely many extensions of $\mathbb{F}_2$, and in the process even extend some of the existing results.

Theorem 5.1. *Let L be a linear polynomial on $\mathbb{F}_{2^n}$, g be a primitive element of $\mathbb{F}_{2^n}$ and $d \geq 1$ be a positive integer. Furthermore, let F and G be defined over $\mathbb{F}_{2^n}$ by $F(x) = L\left(x^{2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$ and $G(x) = L\left(x^{2^{d+1}+2^d+1}\right) + \mathrm{Tr}_1^n(x^3)$. If $\gcd(d,n) > 1$, then neither F nor G is 0-APN.*

In general, $L\left(x^m\right) + \mathrm{Tr}_1^n(x^3)$ is not 0-APN if there exists some $1 \leq i \leq 2^n-1$, such that $P_{g^i}(x) = \prod_{j\in C_i}(x-g^j)$ divides $\sum_{k=1}^{m-1} \binom{m}{k}_2 x^{i(m-k)-1}$, 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.

Proof. The function F is 0-APN if and only if there are no solutions $x, y \in \mathbb{F}_{2^n}^*$, $x \neq y$ of the equation

$$\begin{aligned} 0 &= F(x) + F(y) + F(x+y) \\ &= L\left(x^{2^d+1} + y^{2^d+1} + (x+y)^{2^d+1}\right) + \mathrm{Tr}_1^n\left(x^3 + y^3 + (x+y)^3\right) \\ &= L\left(x^{2^d} y + x\, y^{2^d}\right) + \mathrm{Tr}_1^n(x^2y + xy^2). \end{aligned}$$

Writing $y = \alpha x$, this is equivalent to the equation

$$L\left(x^{2^d+1}(\alpha + \alpha^{2^d})\right) = \mathrm{Tr}_1^n\left(x^3(\alpha+\alpha^2)\right)$$

having no solution for $\alpha \neq 0, 1$. Now, if $m = \gcd(d,n) > 1$, we take $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^d} \cap \mathbb{F}_{2^n}$. Then $\alpha^{2^d} + \alpha = 0$, and for $x = 1$ we have $\mathrm{Tr}_1^n(x^3(\alpha+\alpha^2)) = 0$, since it is known that $\mathrm{Tr}_1^n(u) = 0$ if and only if $u = b^2 + b$ (in characteristic 2), which renders nontrivial solutions to the above equation. The first claim is shown.

We now concentrate on $G(x)$. Once again we want to show that the Rodier equation

$$G(x)+G(y)+G(x+y)=0$$

has no solutions $x,y\in\mathbb{F}_{2^n}^*$ with $x\neq y$. Similarly to the case for F above and writing $y=\alpha x$, we can easily see that this is equivalent to the equation

$$L\left(x^{2^{d+1}+2^d+1}(\alpha+\alpha^{2^d})(1+\alpha^{2^d}+\alpha^{2^{d+1}})\right)=\mathrm{Tr}_1^n\left(x^3(\alpha+\alpha^2)\right) \qquad (7)$$

having no solutions with $\alpha\neq 0,1$. So, denoting $m=\gcd(d,n)>1$, we can take $\alpha\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2\subseteq\mathbb{F}_{2^d}\cap\mathbb{F}_{2^n}$. Then we have $\alpha+\alpha^{2^d}=0$ so that this α along with $x=1$ constitute a solution to (7) implying that G is not 0-APN.

The last claim can be argued as in the proof of Theorem 4.2(i). □

Remark 5.2. The condition on d in the above theorem is important. Indeed, we have computationally checked that if $n=5$, then $x^9+\mathrm{Tr}_1^n(x^3)$ is 0-APN, and potentially there may be some other cases.

These classes of functions can be further generalized so as to encompass even more functions that are not 0-APN.

Theorem 5.3. *Let L_1 and L_2 be linear functions over $\mathbb{F}_{2^n}$. If $\gcd(d,r,n)>1$, then $L_1(x^{2^d+1})+L_2(x^{2^r+1})$ is not 0-APN.*

Furthermore, if L_1 is the identity and L_2 is the absolute trace, then $x^{2^d+1}+\mathrm{Tr}_1^n(x^{2^r+1})$ is not 0-APN if $\gcd(d,n)>1$ and $\gcd(2^r+1,2^n-1)=1$, or $\gcd(d,r,n)>1$.

Finally, if $\gcd(d,s,n)>1$, then $L_1\left(x^{2^{d+1}+2^d+1}\right)+L_2\left(x^{2^{s+1}+2^s+1}\right)$ is not 0-APN.

Proof. We consider first the function $L_1(x^{2^d+1})+L_2(x^{2^r+1})$. As before, we investigate the solvability of the equation

$$L_1\left(x^{2^d+1}(\alpha+\alpha^{2^d})\right)=L_2\left(x^{2^r+1}(\alpha+\alpha^{2^r})\right), \qquad (8)$$

where $y=\alpha x$ for $x\neq 0$ and $\alpha\neq 0,1$. Denoting $m=\gcd(d,r,n)>1$, we can take $\alpha\in\mathbb{F}_{2^m}\setminus\mathbb{F}_2\subseteq\mathbb{F}_{2^d}\cap\mathbb{F}_{2^r}$. Then $\alpha^{2^d}+\alpha=\alpha^{2^r}+\alpha=0$, so that (8) has nontrivial solutions and thus the considered function is not 0-APN.

In the particular case when L_1 is the identity and L_2 is the trace function, it is sufficient to show that the function $x^{2^d+1}+\mathrm{Tr}_1^n(x^{2^r+1})$ is not 0-APN if $\gcd(d,n)>1$ and $\gcd(2^r+1,2^n-1)=1$ since the other case follows from the previously proven statement. The relevant Rodier equation is

$$x^{2^d+1}(\alpha+\alpha^{2^d})=\mathrm{Tr}_1^n\left(x^{2^r+1}(\alpha+\alpha^{2^r})\right).$$

Denoting $m = \gcd(d, n) > 1$, we can find $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$ for which the left hand side vanishes. Now we argue that regardless of the value of α, there exists an element x such that $x^{2^r+1}(\alpha + \alpha^{2^r}) = \beta^2 + \beta$ for some β. If $\alpha + \alpha^{2^r} = 0$, we are done since x can take any value. If $\alpha + \alpha^{2^r} \neq 0$, taking $\beta = \alpha + \alpha^{2^r}$, if $\beta + 1 \neq 0$, or any other nonzero element β of the finite field such that $\beta + 1 \neq 0$, the above claim is implied by the existence of solutions x such that $x^{2^r+1} = \frac{\beta^2+\beta}{\alpha+\alpha^{2^r}}$. This in turn follows from the fact that $\gcd(2^r+1, 2^n-1) = 1$ and thus every element of $\mathbb{F}_{2^n}$ has a $2^r + 1$-st root (see e.g. [13]).
To show the last claim, we again examine the relevant Rodier equation which in this case (by applying the same approach as above) takes the form

$$L_1\left(\left(\alpha + \alpha^{2^d}\right)\left(1 + \alpha^{2^d} + \alpha^{2^{d+1}}\right)\right) = L_2\left(\left(\alpha + \alpha^{2^s}\right)\left(1 + \alpha^{2^s} + \alpha^{2^{s+1}}\right)\right).$$

Denoting $m = \gcd(d, s, n) > 1$, we can find $\alpha \in \mathbb{F}_{2^m} \setminus \mathbb{F}_2$, so that , $\alpha + \alpha^{2^d} = \alpha + \alpha^{2^s} = 0$. The Rodier equation thus has nontrivial solutions and the function in question is not 0-APN. □

Recall the following result (obtained using a combination of theoretical and computational arguments) of Leander and Rodier [12].

Theorem 5.4 (Leander-Rodier, 2011)**.** *If $n \geq 2$ and d is a nonzero integer which is not a power of 2, then the function*

$$F(x) = x^{2^n-2} + \beta\, x^d$$

over $\mathbb{F}_{2^n}$ is not APN for $d \leq 29$ and any $\beta \in \mathbb{F}_{2^n}^*$.

Below we find more classes of functions that are not 0-APN for infinitely many extensions $\mathbb{F}_{2^n}$. In the process, we extend the previous result of Leander and Rodier.

Theorem 5.5. *Let $a > b$ be positive integers. Assuming that one of x^a and x^b are 0-APN on $\mathbb{F}_{2^n}$ and $\gcd(a - b, 2^n - 1) = 1$, the polynomial $x^a + \beta\, x^b$ is not 0-APN for any $\beta \in \mathbb{F}_{2^n}^*$. Let $c > d$ be positive integers. In particular,*

(i) if $\gcd(c-1, n) = \gcd(c-d, n) = 1$, or $\gcd(d-1, n) = \gcd(c-d, n) = 1$, then the polynomial $x^{2^c-1} + \beta\, x^{2^d-1}$ is not 0-APN;

(ii) if $\gcd(c, n) = \gcd(c - d, n) = 1$, or $\gcd(d, n) = \gcd(c - d, n) = 1$, then the polynomial $x^{2^c+1} + \beta\, x^{2^d+1}$ is not 0-APN;

(iii) if $\gcd(c, n) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1) = 1$, or $\gcd(d - 1, n) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1) = 1$, then the polynomial $x^{2^c+1} + \beta\, x^{2^d-1}$ is not 0-APN;

(iv) if $\gcd(c-1,n) = \gcd(2^{c-1}-2^{d-1}-1, 2^n-1) = 1$, *or* $\gcd(d,n) = \gcd(2^{c-1}-2^{d-1}-1, 2^n-1) = 1$, *then the polynomial* $x^{2^c-1}+\beta\, x^{2^d+1}$ *is not* 0*-APN.*

Proof. Let $F(x) = x^a + \beta\, x^b$ $(a > b)$. Then F is 0-APN if and only if $0 = F(y) + F(z) + F(y+z)$ has no solutions y, z with $yz(y+z) \neq 0$. The relevant Rodier equation takes the form

$$0 = F(y) + F(z) + F(y+z) = y^a + \beta\, y^b + z^a + \beta z^b + (y+z)^a + \beta(y+z)^b,$$

which, with $y = z\alpha$ with $\alpha \neq 0, 1$, becomes

$$0 = z^a\left(\alpha^a + 1 + (\alpha+1)^a\right) + \beta z^b\left(\alpha^b + 1 + (\alpha+1)^b\right).$$

Note that the polynomial x^m is 0-APN if and only $x^m + 1 + (x+1)^m$ has no root $x \neq 0, 1$, and such m can be classified by Theorem 4.2 (i). Assume that at least one of x^a and x^b are 0-APN. Then one can always find $\alpha \in \mathbb{F}_{2^n}$ such that

$$\alpha^a + 1 + (\alpha+1)^a \neq 0 \neq \alpha^b + 1 + (\alpha+1)^b.$$

For example, when x^a is 0-APN, one can choose any $\alpha \neq 0, 1$ outside the roots of $x^b + 1 + (x+1)^b = 0$. Therefore one has

$$z^{a-b} = \beta \frac{\alpha^b + 1 + (\alpha+1)^b}{\alpha^a + 1 + (\alpha+1)^a}.$$

When $\gcd(a-b, 2^n-1) = 1$, the above equation always has a unique solution z for any $\alpha \neq 0, 1$, and one has $y = z\alpha \neq z$, since $\alpha \neq 1$.

We now show the other claims. When $a = 2^c - 1$ and $b = 2^d - 1$, with $\gcd(c-1, n) = 1$ or $\gcd(d-1, n)$, then by Theorem 4.2, one of x^a or x^b is 0-APN. One has $a - b = 2^d(2^{c-d} - 1)$ and $\gcd(a-b, 2^n-1) = \gcd(2^{c-d} - 1, 2^n - 1) = 2^{\gcd(c-d,n)} - 1$, which becomes one if and only if $\gcd(c-d, n) = 1$. Therefore, when $\gcd(c-d, n) = 1$ the polynomial $x^{2^c-1} + \beta\, x^{2^d-1}$ is not 0-APN by the first part of the proof.

When $a = 2^c + 1$ and $b = 2^d + 1$ with $\gcd(c, n) = 1$ or $\gcd(d, n) = 1$, then by Theorem 4.2, one of x^a or x^b is 0-APN. One has $a - b = 2^d(2^{c-d} - 1)$ and $\gcd(a-b, 2^n-1) = \gcd(2^{c-d} - 1, 2^n - 1) = 2^{\gcd(c-d,n)} - 1$ which becomes one if and only if $\gcd(c-d, n) = 1$. Therefore, when $\gcd(c-d, n) = 1$, the polynomial $x^{2^c+1} + \beta\, x^{2^d+1}$ is not 0-APN.

When $a = 2^c + 1$ and $b = 2^d - 1$ with $\gcd(c, n) = 1$ or $\gcd(d-1, n) = 1$, then by Theorem 4.2, one of x^a or x^b is 0-APN. One has $a - b = 2^c - 2^d + 2$ and $\gcd(a-b, 2^n-1) = \gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1)$. Therefore, when

$\gcd(2^{c-1} - 2^{d-1} + 1, 2^n - 1) = 1$, the polynomial $x^{2^c+1} + \beta\, x^{2^d-1}$ is not 0-APN.

Lastly, when $a = 2^c - 1$ and $b = 2^d + 1$ with $\gcd(c - 1, n) = 1$ or $\gcd(d, n) = 1$, then by Theorem 4.2, one of x^a or x^b is 0-APN. One has $a-b = 2^c - 2^d - 2$ and $\gcd(a - b, 2^n - 1) = \gcd(2^{c-1} - 2^{d-1} - 1, 2^n - 1)$. Therefore, when $\gcd(2^{c-1} - 2^{d-1} - 1, 2^n - 1) = 1$ the polynomial $x^{2^c-1} + \beta\, x^{2^d+1}$ is not 0-APN. □

From the above examples, one can find many binomials which are not 0-APN for infinitely many extensions of the prime field $\mathbb{F}_2$. For example, both $x^7 + x^3$ and $x^5 + x^3$ are not 0-APN for all finite fields $\mathbb{F}_{2^n}$ when $n > 2$. We can easily generalize (for any odd n) Leander and Rodier's result of Theorem 5.4 [12] in our next corollary.

Corollary 5.6. *Assume that n is odd and d is a positive integer with* $\gcd(d+1, 2^n - 1) = 1$. *Then $x^{2^n-2} + \beta\, x^d$ is not 0-APN for any $\beta \in \mathbb{F}_{2^n}^*$.*

Proof. Observe that x^{2^n-2} is APN for n odd. By the previous theorem $x^{2^n-2} + \beta\, x^d$ is not APN if $1 = \gcd(2^n - 2 - d, 2^n - 1) = \gcd(2^n - 1, d + 1)$ and the proof is done. □

6 Conclusion and further comments

In this paper we introduce a partial APN (pAPN) concept, which may help in understanding the APN property and its properties. We certainly just scratched the surface in the investigation of the pAPN notion and there are certainly many more questions one could ask. For example, we propose further constructions of large classes of such pAPN functions, as well as perhaps look into the construction of permutation pAPN, which may shed light into the well known and quite difficult problem of the permutation APN problem.

Acknowledgements. The authors would like to thank the referees for their thorough reading and useful comments, and the editors for handling our manuscript very efficiently. The paper was started while the fourth named author visited Selmer center at UiB in the Summer of 2018. This author thanks the institution for the excellent working conditions. S.K. was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. 2016R1D1A1B03931912 and No. 2016R1A5A1008055). The research of the first two authors was supported by Trond Mohn foundation.

References

[1] Y. Aubry, G. McGuire, F. Rodier, *A few more functions that are not APN infinitely often*, Finite fields: theory and applications, 23–31, Contemp. Math., 518, Amer. Math. Soc., Providence, RI, 2010.

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

[3] 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.

[4] L. Budaghyan, C. Carlet, G. Leander, *On a construction of quadratic APN functions*, Proc. IEEE Inf. Theory Workshop ITW'09, Oct. 2009, pp. 374–378.

[5] A. Caranti, F. Dalla Volta, M. Sala, *On some block ciphers and imprimitive groups*, Applicable algebra in engineering, communication and computing 20(5-6) (2009), 339–350.

[6] 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.

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

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

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

[11] E. Férard, R. Oyono, F. Rodier, *Some more functions that are not APN infinitely often. The case of Gold and Kasami exponents*, Arithmetic, geometry, cryptography and coding theory, 27–36, Contemp. Math., 574, Amer. Math. Soc., Providence, RI, 2012.

[12] G. Leander, F. Rodier, *Bounds on the degree of APN polynomials: the case of* $x^{-1} + g(x)$, Des. Codes Cryptogr. 59(1-3) (2011), 207–222.

[13] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1994.

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

[15] 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.