On partially APN functions

Nurdagül Anbar[1 [0000−0003−4600−5088]], Tekgül Kalaycı[1 [0000−0002−8472−9792]], and Alev Topuzoğlu[1 [0000−0003−3427−3579]]

Sabancı University,
MDBF, Orhanlı, Tuzla, 34956 İstanbul, Turkey
nurdagulanbar2@gmail.com
tekgulkalayci@sabanciuniv.edu alev@sabanciuniv.edu

Abstract. We consider modifications of APN functions $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ or those of differential uniformity 4, and discuss their differential behaviour by using various concepts of partial APN-ness. We also present quantitative results on partial APN-ness of modified APN functions F over infinitely many extensions of $\mathbb{F}_{2^n}$.

Keywords: Partially APN functions, (p_a) property, partially APN spectrum, modified APN functions, difference squares, partially APN spectrum over infinitely many extensions

1 Introduction

Let $\mathbb{F}_q$ be the finite field with q elements, where $q = 2^n$, for some positive integer n. Various modifications of well known functions, in particular the inverse function x^{q-2} or rational fractional permutations have been studied extensively in relation to a large variety of problems, see for example the surveys [3,24], and the recent papers [9,10,14,15,17].

The affect of the change of values of APN functions at a small number of points or in larger sets, especially in subfields, has been of particular interest. Such modifications enabled constructions of new functions/permutations that have favourable differential properties, high algebraic degrees and high nonlinearity, see [5,9,13,14,17,19,20,21,22,23,25,26].

Another important gain in studying this affect is the insight it provides into the challenging problems concerning upper bounds for algebraic degrees of APN functions, the Hamming distance between them, and the construction of APN permutations for even n. We refer to [7,8,16] for some of the work in this direction.

In an attempt to better understand the planarity of a non-APN function (of low differential uniformity), it is natural to ask "how close it is to being APN". To address this vague question, one may like to identify/construct functions, with "many 2-to-1 derivatives". Here, we focus on such functions, which are referred to as *partially APN* functions.

In a recent work, Budaghyan et al. gave the following definition.

Definition 1. *([6]) Let $x_0 \in \mathbb{F}_{2^n}$ be fixed. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined*

to be an x_0-pAPN function (or x_0-partially APN) if all pairs of elements x, $y \in \mathbb{F}_{2^n}$, satisfying

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

lie on the curve $(x_0 + x)(x_0 + y)(x + y) = 0$.

This concept is motivated by one of the criteria for APN-ness, which is referred to as the *Janwa-Wilson-Rodier condition*. It states that a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is APN if and only if all triples of elements x, y, $z \in \mathbb{F}_{2^n}$ satisfying $F(x)+F(y)+F(z)+F(x+y+z) = 0$ belong to the surface $(x+y)(x+z)(y+z) = 0$.

It is clear therefore that F is APN if and only if it is x_0-pAPN for all $x_0 \in \mathbb{F}_{2^n}$. We refer to the set of points $x_0 \in \mathbb{F}_q$ where F is x_0-pAPN as the *p-spectrum of* F and put

$$p\text{-Spec}_{\text{q}}(F) = \{x_0 \in \mathbb{F}_q : F \text{ is } x_0\text{-pAPN}\}.$$

Clearly, F is APN if and only if the cardinality $|p\text{-Spec}_{\text{q}}(F)|$ is q. Hence one may consider a function F to be close to being APN, if $|p\text{-Spec}_{\text{q}}(F)|$ is large when compared to the field size.

Another notion of partial APN-ness can be found in [11] that we state below.

Definition 2. *([11]) Let $a \in \mathbb{F}_{2^n}^*$ be fixed. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is said to satisfy the property (p_a) if the equation $D_aF(x) = F(x) + F(x + a) = b$ has either 0 or 2 solutions for every $b \in \mathbb{F}_{2^n}$, i.e., the derivative $D_aF(x)$ of F in direction a is 2-to-1.*

Again, clearly, F is APN if and only if it satisfies the property (p_a) for all $a \in \mathbb{F}_{2^n}^*$. In fact, it is sufficient to check smaller sets to ensure APN-ness, see [11] and [12]. We also define the *$\wp$-spectrum of F* and put

$$\wp\text{-Spec}_{\text{q}}(F) = \{a \in \mathbb{F}_q^* : F \text{ satisfies the property } (p_a)\}.$$

We essentially focus on these two notions of partial APN-ness, while we briefly point to their relations to other recent work, [12] and [18], see Remarks 2, 3, 4.

We use the so-called *difference squares* to reformulate the conditions in the Definitions 1 and 2. By fixing an ordering of the elements of $\mathbb{F}_{2^n}$, therefore putting $\mathbb{F}_{2^n} = \{x_1 = 0, x_2, \ldots, x_{2^n}\}$, we define *the difference square corresponding to the function F* to be the $2^n - 1$ by 2^n array where the a-th row $\Delta_a(F)$, $a \in \{x_2, \ldots, x_{2^n}\}$, consists of the derivatives $D_aF(x_1)$, $\ldots$, $D_aF(x_{2^n})$.

With this terminology, it is obvious that the Definitions 1 and 2 can be expressed as follows.

Definition 1*. *Let $x_0 \in \mathbb{F}_{2^n}$ be fixed. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is x_0-pAPN if for each $a \in \{x_2, \ldots, x_{2^n}\}$, the element $D_aF(x_0)$ appears exactly twice in the a-th row $\Delta_a(F)$.*

Definition 2*. *Let $a \in \mathbb{F}_{2^n}^*$ be fixed. A function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ satisfies the property (p_a) if any element in the a-th row $\Delta_a(F)$ appears exactly twice.*

The use of difference squares helps studying these two notions of partial APN-ness in a parallel manner (see the proofs of Theorems 1, 3), providing a tool to better comprehend the similarities/differences between them. The spectra

p-Spec$_{\mathrm{q}}(F)$ and $\wp$-Spec$_{\mathrm{q}}(F)$ can be compared for instance, when F is obtained by modifying the inverse function, see Theorems 1, 3 and Tables 1, 2 below. This approach provides a further insight into the affect of modifications on the differential behaviour of APN functions, and perhaps more importantly, it helps to analyse "fine" differences between non-APN functions, see Remarks 3, 5 and Example 1.

We also study modifications of a class $\mathcal{G}$ of functions over extensions of $\mathbb{F}_{2^n}$. The class $\mathcal{G}$ contains Gold and Kasami-Welch functions, which are known to be exceptional APN, i.e., they are APN over infinitely many extensions of $\mathbb{F}_q = \mathbb{F}_{2^n}$. It is also known that their one or two point modifications are not APN over extensions of sufficiently large degrees. Here we give the first quantitative results on the planarity of modifications of $G \in \mathcal{G}$ over $\mathbb{F}_{q^m}, m > 3$, namely we present upper bounds on the cardinalities of their p-spectra.

2 Modified APN/differentially 4-uniform functions

2.1 The inverse permutation

Modifications of the inverse function x^{q-2} turn out to provide some rare examples of functions with interesting differential properties. Following [8], we will first focus on such an interesting case, see part $(I.i)$ of Theorem 1. In what follows, we use the notation of [15, Theorem 2.5]. Let σ be a permutation of $\mathbb{F}_{2^n}$, induced by a permutation polynomial $F \in \mathbb{F}_{2^n}[x]$, i.e., $F(c) = \sigma(c)$ for all $c \in \mathbb{F}_{2^n}$.

If the values of F at pairwise distinct ℓ elements, say of $\alpha_1, \ldots, \alpha_\ell$, are interchanged so as to obtain the permutation σ',

$$\sigma' = (\sigma(\alpha_1) \ldots \ \sigma(\alpha_\ell)) \circ \sigma, \tag{2}$$

we denote the permutation polynomial that induces σ' by $F_{\alpha_1,\ldots,\alpha_\ell}$. Here we will only be concerned with the cases $\ell = 2$ and 3. Note that if $F(x) = x^{q-2}$, then $F_{0,\alpha}$ is the function with values $F_{0,\alpha}(0) = 1/\alpha$, $F_{0,\alpha}(\alpha) = 0$, and $F_{0,\alpha}(x) = 1/x$ for $x \neq 0, \alpha$.

We now sketch an alternative proof for Theorem 2 in [8], in order to explain our tool in this simple case. Our view point does not only simplify and shorten the proof in [8] considerably, but it also enables us to extend the result to the case $\ell = 3$ easily, i.e., to the case where 3 values $F(0), F(\alpha), F(\beta)$ are interchanged, see Theorem 2.

In what follows, we denote by $\mathrm{Tr}(z)$ the absolute trace of $z \in \mathbb{F}_{2^n}$. We also write p-Spec(F) or $\wp$-Spec(F) when the value of q is clear. We use the notation $\delta_F(a,b) = |\{x \in \mathbb{F}_q : D_aF(x) = b\}|$ as usual, and we put

$$\delta(F,a,x) = \delta_F(a, D_aF(x)), \quad \delta_F(a) = \max_{b \in \mathbb{F}_q} \delta_F(a,b).$$

Theorem 1. *Let $F(x) = x^{q-2}$ and the permutation polynomials $F_{0,\alpha}$ and $F_{\alpha,\beta}$ be as defined in (2) above. Then the following hold.*
I.i) If n is odd, then the permutation $F_{0,\alpha}$, $\alpha \in \mathbb{F}_{2^n}^*$, is not x_0-pAPN for any

$x_0 \in \mathbb{F}_{2^n}$. In other words, the p-Spec$(F_{0,\alpha})$ is empty for any $\alpha \in \mathbb{F}_{2^n}^*$.
I.ii) Suppose that n is even and ω satisfies $\omega^2+\omega+1=0$. Then $F_{0,\alpha}$ is x_0-pAPN if and only if $x_0 \notin \{0, \alpha, \alpha\omega, \alpha\omega^2\}$ and $\mathrm{Tr}(\frac{\alpha}{x_0+\alpha}) = 1$.
II.i) Consider the permutation $F_{\alpha,\beta}$. Suppose that n is odd and $x_0 \notin \{0, \alpha, \beta\}$. If $\mathrm{Tr}\left(\frac{(\alpha+\beta)x_0^2}{(\beta+x_0)^2(x_0+\alpha)}\right) = 0$ *or* $\mathrm{Tr}\left(\frac{(\alpha+\beta)x_0^2}{(\beta+x_0)^2(x_0+\alpha)}\right) = 0$, *then $F_{\alpha,\beta}$ is not x_0-pAPN. If, on the other hand,* $\mathrm{Tr}(\frac{\alpha}{\beta}) = 0$, *then $F_{\alpha,\beta}$ is x_0-pAPN for all $x_0 \in \mathbb{F}_{2^n} \setminus \{x \in \mathbb{F}_{2^n} : x^2 + \beta x + \alpha\beta = 0\}$.*
II.ii) Suppose that n is even, ω satisfies $\omega^2+\omega+1=0$ and $x_0 \notin \{0, \alpha, \beta\}$. Then $F_{\alpha,\beta}$ is x_0-pAPN if $x_0 \in \{\omega\alpha, \omega^2\alpha, \omega\beta, \omega^2\beta\}$ and either $\mathrm{Tr}\left(\frac{(\alpha+\beta)x_0^2}{(\beta+x_0)^2(x_0+\alpha)}\right) = 0$ *or* $\mathrm{Tr}\left(\frac{(\alpha+\beta)x_0^2}{(\alpha+x_0)^2(x_0+\beta)}\right) = 0$. *Otherwise it is not x_0-pAPN.*

Proof. For proving parts (*I.i*) and (*I.ii*), we consider $D_aF_{0,\alpha}(x) = F_{0,\alpha}(x) + F_{0,\alpha}(a+x)$, where $a \in \mathbb{F}_q^*$. The values of $D_aF_{0,\alpha}(x)$ can obviously be determined as follows. Assuming $a \neq \alpha$ one has,
i) $D_aF_{0,\alpha}(x) = \frac{1}{\alpha} + \frac{1}{a} = \frac{a+\alpha}{a\alpha}$, when $x = 0$ or $x = a$.
ii) $D_aF_{0,\alpha}(x) = \frac{1}{a+\alpha}$, if $x = \alpha$ or $x = a + \alpha$.
In case $a = \alpha$ we have,
iii) $D_aF_{0,\alpha}(x) = \frac{1}{\alpha} = \frac{1}{a}$, when $x = 0$ or $x = a$. And finally,
iv) $D_aF_{0,\alpha}(x) = \frac{a}{ax+x^2}$, when $x \neq 0, \alpha, a, a + \alpha$.

In order to determine the p-Spec$(F_{0,\alpha})$, we need to check if there exists any $x \in \mathbb{F}_{2^n}$ such that $\delta(F_{0,\alpha}, a, x) \geq 4$ for some $a \in \mathbb{F}_{2^n}^*$. Obviously, such x cannot be in p-Spec$(F_{0,\alpha})$. We therefore need to understand how the derivatives that are changed after the modification are related to each other and to the remaining ones. For instance, the values of the derivatives in (i) and (ii) are the same, when $\frac{a+\alpha}{a\alpha} = \frac{1}{a+\alpha}$ holds for some a, i.e., exactly when
(3) $a^2 + \alpha a + \alpha^2 = 0$
has solutions in $\mathbb{F}_{2^n}^*$, i.e., if and only if $\mathrm{Tr}(\frac{\alpha^2}{\alpha^2}) = \mathrm{Tr}(1) = 0$. Similarly, $\frac{a+\alpha}{a\alpha} = \frac{a}{ax+x^2}$, or
(4) $(x + \alpha)a^2 + (\alpha x + x^2)a + \alpha x^2 = 0$
holds for some $a \in \mathbb{F}_{2^n}^*$ if and only if $\mathrm{Tr}\left(\frac{(x+\alpha)\alpha x^2}{x^2(x+\alpha)^2}\right) = \mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 0$.
The derivatives in (ii) and (iv) lead to the equation and the conditions
(5) $a^2 + (x + \alpha)a + x^2 = 0$,
$\mathrm{Tr}\left(\frac{x^2}{(x+\alpha)^2}\right) = \mathrm{Tr}(1) + \mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 0$. Finally, $\frac{1}{a} = \frac{a}{ax+x^2}$ leads to the equation
(6) $a^2 + xa + x^2 = 0$,
and the condition $\mathrm{Tr}(\frac{x^2}{x^2}) = \mathrm{Tr}(1) = 0$.
When n is odd, $\mathrm{Tr}(1) = 1$. If $\mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 0$, then Equation (4) has solutions, otherwise Equation (5) has solutions in $\mathbb{F}_{2^n}$.

Let $D_aF_{0,\alpha}(x) = b \in \Delta_aF_{0,\alpha}$, where $x \neq 0, \alpha, a, a+\alpha, a \neq \alpha$. If $\mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 0$, then $b = D_aF_{0,\alpha}(0)$ and hence $\delta_{F_{0,\alpha}}(a, b) \geq 4$. If $\mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 1$, then $b = D_aF_{0,\alpha}(\alpha)$ so that again, $b \in \Delta_aF_{0,\alpha}$ has 4 pre-images. Therefore, for all $x \in \mathbb{F}_{2^n}$,

there exists $a \in \mathbb{F}_{2^n}^*$ such that $\delta(F_{0,\alpha}, a, x) \geq 4$, i.e, $F_{0,\alpha}$ is not x_0-pAPN for any $x_0 \in \mathbb{F}_{2^n}$.

Suppose now that n is even. The differential behaviour of $F_{0,\alpha}$ is as follows. Since $\mathrm{Tr}(1) = 0$, the equations given in (3) and (6) have solutions in $\mathbb{F}_{2^n}$. Equation (3) implies that $D_a F_{0,\alpha}(0) = D_a F_{0,\alpha}(\alpha)$, where $a \neq \alpha$. So, $F_{0,\alpha}$ is not 0-pAPN and not α-pAPN. Similarly, Equation (6) implies that $F_{0,\alpha}$ is not x_0-pAPN for its solutions, i.e., for $x_0 = \alpha\omega$ and $x_0 = \alpha\omega^2$, where $\omega^2 + \omega + 1 = 0$. If $\mathrm{Tr}\left(\frac{\alpha}{x+\alpha}\right) = 1$, then Equations (4) and (5) have no solutions in $\mathbb{F}_{2^n}$, hence part (*I.ii*) follows. We omit the rest of the proof since similar arguments yield the result easily. □

Remark 1. We note that the difference between differential behaviours of the functions $F_{0,\alpha}$ and $F_{\alpha,\beta}$ is expected although only two values are interchanged in both cases. In fact these two permutation polynomials are of different Carlitz rank. With the terminology and notation of [15] for instance, 0 is a pole of $F(x) = x^{q-2}$, hence Theorem 2.5 in [15] implies that the $\mathrm{Crk}(F_{0,\alpha})$=2, while $\mathrm{Crk}(F_{\alpha,\beta})$=4. Indeed, these polynomials can be expressed as

$$F_{0,\alpha}(x) = ((\delta^2 x + \delta)^{q-2} + \delta^{-1})^{q-2} + \delta, \quad \delta = 1/\alpha,$$

$$F_{\alpha,\beta}(x) = \left(\left(\left(\left(\frac{(\alpha+\beta)^2 x}{\alpha^2\beta^2}\right)^{q-2} + \frac{\alpha\beta^2}{\alpha^2+\beta^2}\right)^{q-2} + \frac{\alpha+\beta}{\alpha\beta}\right)^{q-2} + \frac{\alpha\beta}{\alpha+\beta}\right)^{q-2} + \frac{1}{\beta}$$

respectively, see [1]. This observation motivates the investigation of permutation polynomials of Carlitz rank 3. Hence we consider permutations $F_{0,\alpha,\beta}$, which are obtained from $F(x) = x^{q-2}$ by interchanging its values at three elements $0, \alpha, \beta$, as in (2) above. The following result easily follows by the arguments that we used in the proof of Theorem 1. A full classification can also be given, though it is too technical to state here.

Theorem 2. *Let $F(x) = x^{q-2}$ and the permutation polynomial $F_{0,\alpha,\beta}$ be as defined in (2) above. Then the following hold.*

i) If $\mathrm{Tr}(\frac{\alpha}{\beta}) = 0$, then $F_{0,\alpha,\beta}$ is not 0-pAPN, and it is not β-pAPN.
ii) If $\mathrm{Tr}(\frac{\beta}{\alpha+\beta}) = 0$, then $F_{0,\alpha,\beta}$ is not 0-pAPN, and it is not α-pAPN.
iii) If $\mathrm{Tr}(\frac{x_0}{\beta+x_0}) = 0$, then $F_{0,\alpha,\beta}$ is not x_0-pAPN.

We now focus on the notion of partial APN-ness, which is given in Definition 2. In this abstract we state and sketch the proof of our result for the function $F_{0,\alpha}$ only.

Theorem 3. *Let $F(x) = x^{q-2}$ and the permutation polynomial $F_{0,\alpha}$ be as defined above. Then the following hold.*
i) Suppose that n is odd. Then the property (p_a) holds for $a \in \mathbb{F}_q^*$ if and only if $\alpha = a$, or $\mathrm{Tr}(\frac{\alpha}{a+\alpha}) = 1$ and $\mathrm{Tr}(\frac{\alpha}{a}) = 0$.
ii) Suppose that n is even and ω satisfies $\omega^2 + \omega + 1 = 0$. Then the property (p_a) holds for $a \in \mathbb{F}_q^*$ if and only if $a \notin \{\alpha, \alpha\omega, \alpha\omega^2\}$ and $\mathrm{Tr}(\frac{\alpha}{a+\alpha}) = \mathrm{Tr}(\frac{\alpha}{a}) = 1$.

Sketch of Proof. In order to characterize $a \in \mathbb{F}_q^*$ such that the property (p_a) holds, one simply considers the same equations as in the proof of the first part of Theorem 1, arising from the derivatives given in (i)-(iv), and solve them for x. For instance, Equation (3) implies that the property (p_a) does not hold when $\mathrm{Tr}(1) = 0$, and $a = \alpha\omega$ or $a = \alpha^2\omega$, where $\omega^2 + \omega + 1 = 0$. Similarly, the property (p_a) does not hold when $\mathrm{Tr}(\frac{\alpha}{a+\alpha}) = 0$ because of Equation (4), and when $\mathrm{Tr}(\frac{\alpha}{a}) + \mathrm{Tr}(1) = 0$ because of Equation (5). Hence when n is even, the property (p_a) holds if and only if $a \notin \{\alpha, \alpha\omega, \alpha\omega^2\}$ and $\mathrm{Tr}(\frac{\alpha}{a+\alpha}) = \mathrm{Tr}(\frac{\alpha}{a}) = 1$. □

Table 1 below shows how p-Spec$(F_{\alpha,\beta})$ and $\wp$-Spec$(F_{\alpha,\beta})$ are related for the same values of $\alpha, \beta \in \mathbb{F}_{2^n}$. The entry $(c, d)^\mu$ refers to the fact that there are μ pairs (α, β), $\alpha \neq \beta$, such that $c = |p\text{-Spec}(F_{\alpha,\beta})|$ and $d = |\wp\text{-Spec}(F_{\alpha,\beta})|$. For instance, one can see that while p-Spec$_{2^5}(F_{0,\alpha})$ is empty for all $\alpha \in \mathbb{F}_{2^5}^*$ (Theorem 1, *I.i*), $|\wp\text{-Spec}_{2^5}(F_{0,\alpha})| = 6$.

Table 1: Comparison of p-Spec$(F_{\alpha,\beta})$ and $\wp$-Spec$(F_{\alpha,\beta})$ for $F(x) = x^{q-2}$

n	Spectra
4	$(0,0)^{15}, (0,4)^{30}, (2,1)^{60}, (8,4)^{15}$
5	$(0,6)^{31}, (6,9)^{155}, (8,10)^{155}, (9,9)^{155}$
6	$(0,0)^{63}, (0,1)^{378}, (0,2)^{378}, (0,3)^{378}$ $(2,0)^{189}, (2,1)^{378}, (4,0)^{189}, (30,12)^{63}$
7	$(0,36)^{127}, (26,34)^{889}, (28,34)^{889}, (29,33)^{889}, (30,34)^{889}$ $(32,33)^{889}, (32,34)^{1778}, (35,33)^{889}, (36,33)^{889}$

Table 2 illustrates the case of 3 point modification. The result on $\wp$-Spec$(F_{0,\alpha,\beta})$ is not at all difficult to prove, however it is too technical to state here because of the many boundary conditions one needs to consider. Hence we will be content with giving the computational results only.

Table 2: Comparison of p-Spec$(F_{0,\alpha,\beta})$ and $\wp$-Spec$(F_{0,\alpha,\beta})$ for $F(x) = x^{q-2}$

n	Spectra
4	$(0,0)^{30}, (1,3)^{120}, (8,4)^{60}$
5	$(2,1)^{155}, (2,2)^{155}, (2,4)^{155}, (4,3)^{155}, (6,5)^{155}, (6,8)^{155}$
6	$(6,6)^{126}, (6,11)^{378}, (7,3)^{378}, (7,7)^{378}, (7,9)^{378}$
7	$(8,8)^{756}, (8,12)^{378}, (12,6)^{189}, (12,10)^{189}, (13,9)^{378}, (13,11)^{378}$ $(12,9)^{889}, (12,12)^{889}, (12,16)^{889}, (12,17)^{889}, (14,13)^{889},$ $(14,16)^{889}(14,20)^{889}, (16,12)^{889}, (16,14)^{889}, (16,17)^{889}$ $(16,20)^{889}, (18,14)^{889}, (18,16)^{889}, (18,17)^{889}, (18,19)^{1778},$ $(22,24)^{889}, (24,25)^{889}$

Remark 2. We note that the cardinality of the $\wp$-Spec(F) carries information concerning the planarity criterion developed in [18]. With the terminology and notation of [18], the $\wp$-Spec(F) is the set $\mathbb{F}_{2^n}^* \setminus D_F$, where D_F is the set of *critical directions*, defined as $D_F = \{a \in \mathbb{F}_{2^n}^* : \delta_F(a) \geq 4\}$. Hence, the number of the so-called *vanishing flats* (see [18], page 7102) is at least $\frac{1}{3}(2^n - 1 - |\wp\text{-Spec}(F)|)$. One can obtain therefore a lower bound for the number of vanishing flats for the functions $F_{\alpha,\beta}$ and $F_{0,\alpha,\beta}$ for $4 \leq n \leq 7$ from the values given in Tables 1 and 2, when α, β vary over $\mathbb{F}_{2^n}$.

Remark 3. Recall that when n is even, $F(x) = x^{q-2}$ is differentially 4-uniform. It is easy to see that for each $x \in \mathbb{F}_{2^n}^*$, there exist (exactly 3) values of $a \in \mathbb{F}_{2^n}^*$, such that $D_aF(x) = \frac{1}{a}$ repeats 4 times in Δ_aF, and that this holds for any $a \in \mathbb{F}_{2^n}^*$, implying that $|p\text{-Spec}_q(F)| = |\wp\text{-Spec}_\text{q}(F)| = 0$. Hence, F is "not close to being APN" with respect to both concepts, although all other elements in the a-th row Δ_aF, for each $a \in \mathbb{F}_{2^n}^*$ repeat only twice. One may therefore argue that this property entitles F to be partially APN! The differential behaviour of $F_{0,\alpha}(x)$ however is quite different, as shown in the proof of Theorem 1 above. Indeed, there are rows $\Delta_aF_{0,\alpha}$ with more elements repeating 4 times, but also those with all of its elements repeating only twice, see Example 1 below.

Example 1. Let $n = 6$, and consider $F_{0,\alpha}(x)$, where $\alpha^6 + \alpha^4 + \alpha^3 + \alpha + 1 = 0$. There are 12 rows $\Delta_aF_{0,\alpha}$ with 2 elements repeating 4 times, and 12 values of a such that each element in $\Delta_aF_{0,\alpha}$ repeats twice, i.e., $\delta_{F_{0,\alpha}}(a) = 2$. Hence $|\wp\text{-Spec}_\text{q}(F_{0,\alpha})| = 12$, and Table 1 shows that $|p\text{-Spec}_q(F_{0,\alpha})| = 30$, i.e., $F_{0,\alpha}(x)$ is partially APN with respect to both concepts.

Remark 4. The property of $F(x) = x^{q-2}$ that we mentioned in Remark 3 singles it out among the non-APN monomials, see [12] and [18]. Indeed, the number of vanishing flats of F attains the lower bound $\frac{2^n-1}{3}$ for such monomials (see [18], Proposition III.1). It is also the only known differentially 4-uniform monomial so far, where the associated code C_F has no codewords of weight 4, see Problem 1 in [12].

Remark 5. A comparison of the large values of the spectra in Tables 1 and 2 reveals that the function $F_{\alpha,\beta}$ is closer to being APN then $F_{0,\alpha,\beta}$, although the latter is obtained by changing values at 3 elements. This observation is in accordance with the result in [14] that if n is even, APN permutations cannot be of small Carlitz rank when compared with the field size.

2.2 The Gold function

Let $G(x) = x^{2^k+1}$ be the Gold function on $\mathbb{F}_{2^n}$, where n is odd and $\gcd(k, n) = 1$. Our arguments used in Theorems 1, 2 and 3 can be employed for analysing the modified Gold function $G_{0,\alpha}(x)$ also, which we do not include here. Note that $D_aG_{0,\alpha}(x) = x^{2^k+1} + (x + a)^{2^k+1} = a^{2^k+1} + ax^{2^k} + xa^{2^k}$, when $x \neq 0, \alpha$. On the other hand, $D_aG_{0,\alpha}(0) = \alpha^{2^k+1} + a^{2^k+1}$, and $D_aG_{0,\alpha}(\alpha) = \alpha^{2^k+1} + a^{2^k+1} + a\alpha^{2^k} + \alpha a^{2^k}$. Equations obtained through these derivatives can be solved by tools used in the proof of Theorem 4 in [8] and results on p-Spec$(G_{0,\alpha})$ and $\wp$-Spec$(G_{0,\alpha})$ can be deduced.

3 Modified APN functions over extension fields

In this section we focus on the p-spectra of modifications of Gold and Kasami-Welch functions over extension fields. As mentioned in Section 1, they are both exceptional APN, while their modifications are not APN over extension fields of sufficiently large degrees. It is interesting therefore to obtain bounds for their p-spectra.

3.1 One point modification

Given a function $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$. Consider the function $G_{\alpha|\beta}$, obtained from G by modifying it at a single point $\alpha \in \mathbb{F}_{2^n}$, i.e., by putting $G_{\alpha|\beta}(\alpha) = \beta$, while $G_{\alpha|\beta}(x) = G(x)$, for any $x \neq \alpha$.

Here we study a class $\mathcal{G}_{\alpha|\beta}$ of functions G satisfying the following conditions.
i) $\deg(G) \leq q-2$, where $q = 2^n$,
ii) $G(\alpha) \neq \beta$,
iii) Denoting by d_t the coefficient of $X^t + Y^t$ in $G_{\alpha|\beta}(X+\alpha+a) + G_{\alpha|\beta}(X+\alpha) + G_{\alpha|\beta}(Y+\alpha+a) + G_{\alpha|\beta}(Y+\alpha)$, d_1, d_2 satisfy $d_1 = 0$ and $d_2 \neq 0$.

Obviously, $G_{\alpha|\beta}$ can be expressed as $G_{\alpha|\beta}(x) = ((x+\alpha)^{q-1}+1)(G(\alpha)+\beta)+G(x)$. It was observed in [4] that any $G_{\alpha|\beta}$ is not APN over extensions $\mathbb{F}_{q^m}$, for all sufficiently large m, see Theorem 2.3 in [4]. Therefore one would like to seek information about $p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha|\beta})$. The following theorem provides an upper bound for $|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha|\beta})|$.

Theorem 4. *Let $G \in \mathcal{G}_{\alpha|\beta}$. Then,*

$$|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha|\beta})| \leq q^m - \frac{q^m - (q-5)(q-6)q^{m/2} - \left(\frac{5q}{2} - 11\right)}{q-4}$$

for any $m \geq 4$.

Proof. Since we look for the solutions (x, y) of $G_{\alpha|\beta}(X+a) + G_{\alpha|\beta}(x)(X) + G_{\alpha|\beta}(Y+a) + G_{\alpha|\beta}(Y) = 0$ such that $x \neq y$ and $x \neq y + a$, we consider

$$H(X,Y) = \frac{G_{\alpha|\beta}(X+a) + G_{\alpha|\beta}(X) + G_{\alpha|\beta}(Y+a) + G_{\alpha|\beta}(Y)}{(X+Y)(X+Y+a)}. \tag{3}$$

Let $\mathcal{H}$ be the curve defined by $H(X,Y)$. Consider the change of coordinates that sends X and Y to $X+\alpha$ and $Y+\alpha$, respectively. Then by Equation (3), we have $(X+Y)(X+Y+a)\tilde{H}(X,Y) = \sum_{t=1}^{q-2} d_t(X^t + Y^t)$, where $\tilde{H}(X,Y) = H(X+\alpha, Y+\alpha)$. Note that $(0,0)$ belongs to the curve $\tilde{\mathcal{H}}$ defined by $\tilde{H}$. Moreover, by our assumption on d_1 and d_2, the multiplicity of $(0,0)$ is 1, i.e., $(0,0)$ is a simple $\mathbb{F}_q$-rational point of $\tilde{\mathcal{H}}$. Hence, by [2, Lemma 2.1], we conclude that the absolutely irreducible component $\tilde{\mathcal{X}}$ of $\tilde{\mathcal{H}}$ passing through $(0,0)$ is defined over $\mathbb{F}_q$ and is of degree $\leq q-4$. Also, we observe that $\tilde{\mathcal{X}}$ is not the curve defined by $X+Y$ or $X+Y+a$ since the multiplicity of $(1:1:0)$ at infinity is 2. This shows that the absolutely irreducible component $\mathcal{X}$ of $\mathcal{H}$ passing through (α, α) is defined over $\mathbb{F}_q$, is of degree $\leq q-4$, and is different from the ones defined by $X+Y$ and $X+Y+a$. Then, by the Hasse-Weil bound, the number $N(\mathcal{X})$ of $\mathbb{F}_{q^m}$-rational points of $\mathcal{X}$ satisfies

$$N(\mathcal{X}) \geq q^m + 1 - (q-5)(q-6)q^{m/2}. \tag{4}$$

Denote by N the number of affine $\mathbb{F}_{q^m}$-rational points (x, y) of $\mathcal{X}$ such that $x \neq y$ and $x \neq y + a$. Note that $\mathcal{X}$ has at most $(q/2-2)$ $\mathbb{F}_{q^m}$-rational points

at infinity. Also, by Bezout's theorem there are at most $2(q-4)$ $\mathbb{F}_{q^m}$-rational points (x,y) of $\mathcal{X}$ satisfying $x=y$ or $x=y+a$. Therefore, by Equation (4), $N \geq q^m-(q-5)(q-6)q^{m/2}-(5q/2-11)$. For $c \in \mathbb{F}_{q^m}$, set $t_c=\delta_{G_{\alpha|\beta}}(a,c)$. Note that if $t_{D_aG_{\alpha|\beta}(x_0)}>2$ then $G_{\alpha|\beta}$ is not x_0-pAPN. In this case, $S_{D_aG_{\alpha|\beta}(x_0)}$ contributes $t_{D_aG_{\alpha|\beta}(x_0)}(t_{D_aG_{\alpha|\beta}(x_0)}-2)$ affine $\mathbb{F}_{q^m}$-rational points (x,y) of $\mathcal{H}$ with $x\neq y$ and $x\neq y+a$. Therefore,

$$\sum_{t_{D_aG_{\alpha|\beta}(x)}>2} t_{D_aG_{\alpha|\beta}(x)}(t_{D_aG_{\alpha|\beta}(x)}-2) \geq q^m-(q-5)(q-6)q^{m/2}-\left(\frac{5q}{2}-11\right). \tag{5}$$

Note that $t_{D_aG_{\alpha|\beta}(x)} \leq q-2$ as the degree of $G_{\alpha|\beta}(x)$ is $q-1$, i.e.,

$$(q-4)\sum_{t_{D_aG_{\alpha|\beta}(x)}>2} t_{D_aG_{\alpha|\beta}(x)} \geq \sum_{t_{D_aG_{\alpha|\beta}(x)}>2} t_{D_aG_{\alpha|\beta}(x)}(t_{D_aG_{\alpha|\beta}(x)}-2). \tag{6}$$

Since the number of the elements x_0 for which $G_{\alpha|\beta}$ is not x_0-pAPN is greater than or equal to $\sum_{t_{D_aG_{\alpha|\beta}(x)}>2} t_{D_aG_{\alpha|\beta}(x)}$, by Equations (5) and (6), the number is greater than or equal to $(q^m-(q-5)(q-6)q^{m/2}-(5q/2-11))/(q-4)$, which gives the desired result. □

Remark 6. We can observe from Theorem II.3 in [18] that the number of vanishing flats corresponding to $G_{\alpha|\beta}$ given in Theorem 4 is at least $\frac{1}{8}\left(q^m-(q-5)(q-6)q^{m/2}-\left(\frac{5q}{2}-11\right)\right)$.

Theorem 4 yields the following result for Gold and Kasami-Welch functions.

Corollary 1. Let $G(x)=x^{2^k+1}$ or $G(x)=x^{2^{2k}-2^k+1}$ over $\mathbb{F}_{2^n}$. Suppose that $n>2$, $k>1$, $G(\alpha)\neq\beta$ and $G(\alpha)+\beta=G(a)$ for some a in $\mathbb{F}_{2^n}^*$. Then for any $m\geq 4$,

$$|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha|\beta})| \leq q^m-\frac{q^m-(q-5)(q-6)q^{m/2}-\left(\frac{5q}{2}-11\right)}{q-4}.$$

3.2 Interchanging values at two points

For a function $G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, we now consider $G_{\alpha,\beta}$, obtained from G by modifying it at $\alpha\neq\beta$ i.e., by putting $G_{\alpha,\beta}(\alpha)=G(\beta)$, $G_{\alpha,\beta}(\beta)=G(\alpha)$, and $G_{\alpha,\beta}(x)=G(x)$, for any $x\neq\alpha,\beta$. Hence, $G_{\alpha,\beta}(x)=((x+\alpha)^{q-1}+(x+\beta)^{q-1})(G(\alpha)+G(\beta))+G(x)$. Again, we study a class $\mathcal{G}_{\alpha,\beta}$ of functions G satisfying the following conditions.
i) $\deg(G)\leq q-5$, $q=2^n$,
ii) $G(\alpha)\neq G(\beta)$,
iii) Denoting by d_t the coefficient of X^t+Y^t in $G_{\alpha,\beta}(X+\alpha+a)+G_{\alpha,\beta}(X+\alpha)+G_{\alpha,\beta}(Y+\alpha+a)+G_{\alpha,\beta}(Y+\alpha)$ for a non-zero $a\neq\alpha+\beta$, d_1 and d_2 satisfy $d_1=0$ and $d_2\neq 0$.

$G_{\alpha|\beta}(x)=((x+\alpha)^{q-1}+1)(G(\alpha)+\beta)+G(x)$. Theorem 2.4 in [4] shows that $G_{\alpha,\beta}$ is not APN over extensions $\mathbb{F}_{q^m}$, for all sufficiently large m. Therefore

again, it is interesting to find an upper bound for $|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha,\beta})|$. The proof of Theorem 5 below uses some tools, different from those used in the proof of Theorem 4. However it is rather long so we need to exclude it.

Theorem 5. *Let $G \in \mathcal{G}_{\alpha,\beta}$. Then for any $m \geq 4$,*

$$|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha,\beta})| \leq q^m - \frac{q^m - (q-7)(q-8)q^{m/2} - \left(\frac{9q}{4} - 14\right)}{q-5}.$$

Corollary 1. *Let $G(x) = x^{2^k+1}$ or $G(x) = x^{2^{2k}-2^k+1}$ over $\mathbb{F}_q$, where $q = 2^n$. Suppose that $n > 2$, $k > 1$, $\alpha \neq \beta$ and $G(\alpha) \neq G(\beta)$. Set $\gamma = \alpha + \beta$. If $\frac{a^2+a\gamma+\gamma^2}{\gamma(a+\gamma)}(G(\alpha) + G(\alpha+\gamma)) = G(a)$ for some nonzero $a \in \mathbb{F}_q$, then $|p\text{-Spec}_{\mathrm{q^m}}(G_{\alpha,\beta})|$ satisfies the bound given in Theorem 5.*

Acknowledgement

N. Anbar and T. Kalaycı are supported by TÜBİTAK Project under Grant 120F309.

References

1. Aksoy, E., Çeşmelioğlu, A., Meidl, W., Topuzoğlu, A.: On the Carlitz rank of permutation polynomials. Finite Fields Appl. **15**, 428–440 (2009).
2. Anbar, N., Odžak, A., Patel, V., Quoos, L., Somoza, A., Topuzoğlu, A.: On the difference between permutation polynomials. Finite Fields Appl. **49**, 132–142 (2018).
3. Anbar, N., Odžak, A., Patel, V., Quoos, L., Somoza, A., Topuzoğlu, A.: On the Carlitz rank of permutation polynomials: Recent developments. In: Bouw, I., Ozman, E., Johnson-Leung, J., Newton, R. (eds.) Women in Numbers Europe II. Association for Women in Mathematics Series **11**, 39–55. Springer, Cham (2018).
4. Aubry, Y., McGuire, G., Rodier, F.: 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).
5. Bracken, C., Tan, C. H., Tan, Y.: Binomial differentially 4-uniform permutations with high nonlinearity. Finite Fields Appl. **18**, no. 3, 537-546 (2012).
6. Budaghyan, L., Kaleyski, N., Kwon, S., Riera, C., Stănică P.: Partially APN Boolean functions and classes of functions that are not APN infinitely often. Cryptogr. Commun. **12**, no. 3, 527-545 (2020).
7. Budaghyan, L., Carlet, C., Helleseth, T., Kaleyski, N.S.: On the distance between APN functions. IEEE Trans. Inform. Theory **66**, no. 9, 5742–5753 (2020).
8. Budaghyan, L., Kaleyski, N., Riera, C., Stănică, P.: On the behavior of some APN permutations under swapping points. Cryptogr. Commun. (2021).
9. Calderini, M., Villa, I.: On the boomerang uniformity of some permutation polynomials. Cryptogr. Commun. **12**, no. 6, 1161-1178 (2020).
10. Calderini, M.: Differentially low uniform permutations from known 4-uniform functions. Des. Codes Cryptogr. **89**, no. 1, 33–52 (2021).
11. Charpin, P., Kyureghyan, G.M.: On sets determining the differential spectrum of mappings. Internat. J. Inf. Coding Theory **4**(2-3), 170–184 (2017).

12. Charpin, P., Peng, J.: Differential uniformity and the associated codes of cryptographic functions. Adv. Math. Commun. **13**, no. 4, 579-600 (2019).
13. Jeong, J., Koo, N., Kwon, S.: Constructing differentially 4-uniform involutions over $\mathbb{F}_{2^{2k}}$ by using Carlitz form. Finite Fields Appl. **78**, 101957, 34 pp. (2022).
14. Jeong, J., Koo, N., Kwon, S.: On the boomerang uniformity of permutations of low Carlitz rank. (2020). arXiv:2009.08612.
15. Kalaycı, T., Stichtenoth, H., Topuzoğlu, A.: Permutation polynomials and factorization. Cryptogr. Commun. **12**, no. 5, 913-934 (2020).
16. Kaleyski, N. S.: Towards a deeper understanding of APN functions and related longstanding problems, PhD thesis, University of Norway, August 2021.
17. Li, K., Qu, L., Sun, B., Li, C.: New results about the boomerang uniformity of permutation polynomials. IEEE Trans. Inform. Theory **65**, no. 11, 7542-7553 (2019).
18. Li, S., Meidl, W., Polujan, A., Pott, A., Riera, C., Stănică, P.: Vanishing flats: A combinatorial viewpoint on the planarity of functions and their application. IEEE Trans. Inform. Theory **66**, no. 11, 7101–7112 (2020).
19. Li, Y., Wang, M., Yu, Y.: Constructing differentially 4-uniform permutations over GF(2^{2k}) from the inverse function revisited, eprint.iacr.org/2013/731.
20. Peng, J., Tan, C., Wang, Q.: A new family of differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ for odd k. Sci. China Math. **59**, no.6, 1221-1234 (2016).
21. Qu, L., Tan, Y., Tan, C.H., Li, C.: Constructing differentially 4-uniform permutations over $\mathbb{F}_{2^{2k}}$ via the switching method. IEEE Trans. Inform. Theory, **59**, no. 7, 4675-4686 (2013).
22. Qu, L., Tan, Y., Li, C., Gong, G.: More constructions of differentially 4-uniform permutations on $\mathbb{F}_{2^{2k}}$. Des. Codes Cryptogr. **78**, no. 2, 391-408 (2016).
23. Tang, D., Carlet, C., Tang, X.: Differentially 4-uniform bijections by permuting the inverse function. Des. Codes. Cryptogr. **77**, no. 1, 117-141 (2015).
24. Topuzoğlu, A.: Carlitz rank of permutations of finite fields: A survey. J. Symbolic Comput. **64**, 53-66 (2014).
25. Yu, Y., Wang, M., Li, Y.: Constructing differentially 4 uniform permutations from known ones. Chin. J. Electron., 495-499 (2013).
26. Zha, Z., Hu, L., Sun, S.: Constructing new differentially 4-uniform permutations from the inverse function. Finite Fields Appl. **25**, 64-78 (2014).