Analysis of (n, n)-functions obtained from the Maiorana-McFarland class

Nurdagül Anbar, Tekgül Kalaycı, and Wilfried Meidl

***Abstract*—Pott et al. (2018) showed that $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)$, $n = 2m$, $r \geq 1$, is a nontrivial example of a vectorial function with the maximal possible number $2^n - 2^m$ of bent components. Mesnager et al. (2019) generalized this result by showing conditions on $\Lambda(x) = x+\sum_{j=1}^{\sigma}\alpha_j x^{2^{t_j}}$, $\alpha_j \in \mathbb{F}_{2^m}$, under which $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$ has the maximal possible number of bent components. We simplify these conditions and further analyse this class of functions. For all related vectorial bent functions $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma\mathcal{F}(x))$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, which as we will point out belong to the Maiorana-McFarland class, we describe the collection of the solution spaces for the linear equations $\mathcal{D}_aF(x) = F(x) + F(x + a) + F(a) = 0$, which forms a spread of $\mathbb{F}_{2^n}$. Analysing these spreads, we can infer neat conditions for functions $H(x) = (F(x), G(x))$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ to exhibit small differential uniformity (for instance for $\Lambda(x) = x$ and $r = 0$ this fact is used in the construction of Carlet's, Pott-Zhou's, Taniguchi's APN-function). For some classes of $H(x)$ we determine differential uniformity and with a method based on Bezout's theorem nonlineariy.**

***Index Terms*—Almost perfect nonlinear (APN) function, differentially 4-uniform, differential uniformity, maximal bent components, nonlinearity, vectorial bent function.**

I. Introduction

The *Walsh transform* of a Boolean function f from an n-dimensional vector space $\mathbb{V}_n$ over $\mathbb{F}_2$ to $\mathbb{F}_2$ is the integer valued function

$$\widehat{f}(u) := \sum_{x\in\mathbb{V}_n}(-1)^{f(x)+\langle x,u\rangle},$$

where $\langle\, ,\,\rangle$ denotes any (nondegenerate) inner product in $\mathbb{V}_n$. The *Walsh spectrum* $\mathcal{W}_f := \{\widehat{f}(u) : u \in \mathbb{V}_n\}$ is independent from the inner product used in the Walsh transform. A Boolean function f is called *bent* (see [16]) if for all $u \in \mathbb{V}_n$ we have $|\widehat{f}(u)| = 2^{n/2}$. If $\mathcal{W}_f = \{0, \pm 2^{(n+1)/2}\}$ or $\mathcal{W}_f = \{0, \pm 2^{(n+2)/2}\}$, then f is called *semibent*, and more general, *s-plateaued* if $\mathcal{W}_f = \{0, \pm 2^{(n+s)/2}\}$ for some integer s, see [8], [21]. Apparently $n+s$ is always even. In particular, bent functions only exist if n is even.

The *nonlinearity* $NL(f)$ of a Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is the distance of f to the set of all affine functions, i.e.,

$$NL(f) := \min_{a\in\mathbb{V}_n, c\in\mathbb{F}_2} |\{x \in \mathbb{V}_n : f(x) \neq \langle a, x\rangle_n + c\}|.$$

The nonlinearity of f can be expressed via the Walsh transform as

$$NL(f) := 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{V}_n} |\widehat{f}(u)|.$$

As is well known, when n is even, bent functions are the functions with the largest nonlinearity.

For a vectorial function $F : \mathbb{V}_n \to \mathbb{V}_m$, also called an *$(n, m)$-function*, and a nonzero element $a \in \mathbb{V}_m$ the *component function* F_a is the Boolean function $F_a(x) = \langle a, F(x)\rangle$ ($\langle\, ,\,\rangle$ is a fixed inner product in $\mathbb{V}_m$). The nonlinearity is then the minimal nonlinearity among all component functions of F. Functions of which all components are bent, hence attaining the largest possible nonlinearity, are called *vectorial bent functions*. As is well known, for a vectorial bent function we always have $m \leq n/2$, see [13].

A function $F : \mathbb{V}_n \to \mathbb{V}_n$ is called *differentially k-uniform* if for all nonzero $a \in \mathbb{V}_n$ and $b \in \mathbb{V}_n$, the equation

$$D_aF(x) := F(x + a) + F(x) = b \qquad (1)$$

has at most k solutions. The smallest integer k for which F is differentially k-uniform is called the *differential uniformity* of F. Observing that with x_0 also $x_0 + a$ is a solution of Equation (1), the value for k is at least 2. Differentially 2-uniform functions are called *almost perfect nonlinear (APN)*.

Nonlinearity and differential uniformity are fundamental features for vectorial functions in cryptographic applications, we refer to [13], [14]. The analysis of aspects on nonlinearity and differential uniformity and on their interplay is of substantial relevance and attracts a lot of attention.

Most known examples and infinite classes of APN-functions and functions on $\mathbb{V}_n$ of small differential uniformity are quadratic, or involve quadratic functions, i.e., functions of which all component functions have algebraic degree (at most) 2, and hence all component functions are plateaued, see [4]. Differently from quadratic APN-functions in odd dimension, of which all component functions are always semibent, quadratic APN-functions in even dimension can have various Walsh spectra. For details we refer to [2], [11], [17]. However, all known infinite classes of quadratic APN-functions in even dimension n have the *classical spectrum*, i.e., solely bent components and semibent components. Only sporadic counterexamples are known. Similarly, several constructions and classes of differentially 4-uniform functions in even dimension are known, of which again all component functions are bent or semibent, see [1], [6] for examples. It appears that at least the simple constructions of functions with small differential uniformity yield functions that also have a large nonlinearity. However, there are only a few theoretical

Manuscript received March 20, 2020; revised April 19, 2021; accepted 25 April 2021. N. Anbar is supported by B.A.CF-19-01967; N. Anbar and T. Kalaycı are partially supported by TÜBİTAK Project under Grant 120F309; and W. Meidl is supported by the FWF Project P 30966.

N. Anbar and T. Kalaycı are with the Faculty of Engineering and Natural Sciences, Sabancı University, 34956 Istanbul, Turkey (e-mail: nurdagulanbar2@gmail.com; tekgulkalayci@sabanciuniv.edu).

W. Meidl is with the Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, 4040 Linz, Austria (e-mail: meidlwilfried@gmail.com).

results on connections between small differential uniformity and high nonlinearity, see [7, Section V.B.].

Having a large number of bent components, many quadratic APN-functions and differentially 4-uniform functions on $\mathbb{V}_{2m}$ contain an m-dimensional subspace of bent components, i.e., a vectorial bent function from $\mathbb{V}_{2m}$ to $\mathbb{V}_m$. For instance Carlet's function, the Zhou-Pott function and Taniguchi's function on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ are constructed as $H(x,y) = (F(x,y), G(x,y))$, taking for F the simplest vectorial Maiorana-McFarland bent function $F(x,y) = xy$, see [5], [18], [22]. Another function one often sees as a part of an APN-function is the Gold function $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^i+1})$, $n = 2m$, which is vectorial bent if $n \equiv 2 \bmod 4$, $\gcd(n,i) = 1$, and γ is a noncube in $\mathbb{F}_{2^n}$, see [5, p.99], ($\mathrm{Tr}^n_m(x) = x + x^{2^m}$ is the relative trace from $\mathbb{F}_{2^n}$ to the subfield $\mathbb{F}_{2^m}$).

In [15], it is shown that a function on $\mathbb{V}_n$, $n = 2m$, can have at most $2^n - 2^m$ bent components. (Nontrivial) examples are presented in the papers [12], [15], namely $\mathcal{F}_{r,\Lambda}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$, of which it is shown that $\mathrm{Tr}^n_1(a\mathcal{F}_{r,\Lambda}(x))$ is bent for every $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, where $\mathrm{Tr}^n_1(x) = \sum_{i=0}^{n-1} x^{2^i}$ is the absolute trace on $\mathbb{F}_{2^n}$, if Λ is a linearized polynomial which satisfies certain conditions, see Section II.

We then can associate to $\mathcal{F}_{r,\Lambda}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$ the vectorial bent function $F_{r,\Lambda,\gamma}(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$, $\gamma \notin \mathbb{F}_{2^m}$, from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, see [15, Proposition 3]. Note that if $r = 0$ and $\Lambda(x) = x$, then $F_{r,\Lambda,\gamma} = F_{0,x,\gamma}$ is equivalent to x^{2^m+1}, which, as pointed out in [6], can be seen as the Maiorana-McFarland bent function xy in univariate form. As we will see, bent functions of the form $F_{r,\Lambda,\gamma}(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$ share some interesting properties with the function xy. In particular we can associate to $F_{r,\Lambda,\gamma}(x)$ a spread of $\mathbb{F}_{2^n}$. Since xy, respectively its univariate version x^{2^m+1}, turned out to be a suitable component for the construction of APN-functions, the generalizations we consider in this article may also be good candidates to form components of quadratic functions with low differential uniformity. With these generalizations, we also get some known results on functions that are constructed with x^{2^m+1} as a component.

Though the properties of $\mathcal{F}_{r,\Lambda}$ apparently depend on the choice of r and Λ, to simplify notation, for fixed integer $r \geq 0$ and linearized polynomial $\Lambda \in \mathbb{F}_{2^m}[x]$, we will write $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$ for $\mathcal{F}_{r,\Lambda}(x)$. Similarly, for fixed r, Λ and $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ we will use the notation $F_{r,\Lambda,\gamma}(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))) = F(x)$.

This article is organized as follows: In Section II, we first give simplified conditions on Λ such that $x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$ achieves the upper bound on the number of bent component functions. For the associated vectorial bent functions $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$, we then analyse the collection of the solution spaces of

$$\mathcal{D}_a F(x) := F(x) + F(x+a) + F(a) = 0,$$

i.e., the collection of the kernels of $\mathcal{D}_a$, $a \in \mathbb{F}^*_{2^n}$. As we will see, the collection of these subspaces of $\mathbb{F}_{2^n}$ always forms a spread of $\mathbb{F}_{2^n}$. We also show that on the other hand, the set of the solution spaces of $\mathcal{D}_a K = 0$ has the quite opposite behaviour for the vectorial bent function $K(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^3)$, $n \equiv 2 \bmod 4$, γ noncube. In this case, all $2^n - 1$ solution spaces are different. We then investigate properties of the spreads of $\mathbb{F}_{2^n}$ obtained from bent functions of the form $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$. The interesting structural properties of the solution spaces for this class of functions allow us to derive neat conditions on $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $H(x) = (F(x), G(x))$ has a small differential uniformity. In Section III we analyse differential uniformity and nonlineariy of functions H that combine Maiorana-McFarland functions with the Gold function. For some classes we show that they have differential uniformity δ with $\delta \leq 4$. With a method based on Bezout's theorem, which we introduced in [1], we show that these functions have only bent and semibent components when m is odd (see Theorem 6), which does not always apply when m is even. We finish the paper with some computational results and some remarks in Section IV.

II. Properties of $\mathbf{x^{2^r}}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\mathbf{\Lambda(x)})$

In [15] Pott et al. showed that a function on $\mathbb{V}_n$, $n = 2m$, can have at most $2^n - 2^m$ bent components. A vectorial bent function from $\mathbb{V}_n$ to the subspace $\mathbb{V}_m$, seen as a function on $\mathbb{V}_n$, trivially attains this bound. With the objective to find nontrivial examples of functions on $\mathbb{F}_{2^n}$ with the maximal possible number $2^n - 2^m$ of bent components, in [15] it is shown that for the quadratic function $\mathcal{F}(x) = x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)$ on $\mathbb{F}_{2^n}$, the component function $F_\gamma(x) = \mathrm{Tr}^n_1(\gamma\mathcal{F}(x))$ is bent if and only if $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. We remark that for $r = 0$ we have $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)) = \tilde{\gamma}x^{2^m+1} + \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^2)$, $\tilde{\gamma} = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma)$, i.e., as a vectorial bent function, F differs from the norm function x^{2^m+1} only by a linear term (and the multiplication by a nonzero constant in $\mathbb{F}_{2^m}$). Since x^{2^m+1} is a vectorial bent function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, seen as a function on $\mathbb{F}_{2^n}$ it trivially has the maximal number of possible bent components.

In [12], it is shown that the property of having the maximal number of bent components is invariant under CCZ-equivalence, and that plateaued functions on $\mathbb{V}_n$ with $2^n - 2^m$ bent components cannot be APN. Furthermore, a more general nontrivial example of a function on $\mathbb{F}_{2^n}$ having $2^n - 2^m$ bent components is presented in [12, Theorem 6] as follows:
Let $n = 2m$, $\alpha_j \in \mathbb{F}_{2^m}$ and t_j be nonnegative integers for $1 \leq j \leq \sigma$. If both equations

$$\mathcal{A}_1(x) = \sum_{j=1}^{\sigma} \alpha_j^{2^{m-t_j}} x^{2^{m-t_j}-1} + 1 = 0,$$
$$\mathcal{A}_2(x) = \sum_{j=1}^{\sigma} \alpha_j^{2^{m-r}} x^{2^{t_j}-1} + 1 = 0, \tag{2}$$

do not have a solution in $\mathbb{F}_{2^m}$, then the function $F_\gamma : \mathbb{F}_{2^n} \to \mathbb{F}_2$ given as

$$F_\gamma(x) = \mathrm{Tr}^n_1\left(\gamma x^{2^r}\left(\mathrm{Tr}^n_m(x) + \sum_{j=1}^{\sigma} \alpha_j \mathrm{Tr}^n_m(x^{2^{t_j}})\right)\right)$$

is bent if and only if $\gamma \notin \mathbb{F}_{2^m}$. Hence $\mathcal{F} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $\mathcal{F}(x) = x^{2^r}(\mathrm{Tr}^n_m(x) + \sum_{j=1}^{\sigma} \alpha_j \mathrm{Tr}^n_m(x^{2^{t_j}}))$ has the maximal possible number of bent components. Note that the conditions in (2) are trivially satisfied for the function $x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)$ of [15].

A. Simplified Conditions on Λ

In this first subsection we show that the conditions in (2) completely describe the functions of the form $x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x))$, Λ is a linearized polynomial over $\mathbb{F}_{2^m}$, with the maximal possible number of bent components. We replace the conditions in (2) with a single simple necessary and sufficient condition. For a similar characterization we may also refer to the recent article [20].

We will require the concept of the *adjoint* $\mathcal{L}^*$ of a linear transformation $\mathcal{L}$ of $\mathbb{F}_{2^m}$ (with respect to the inner product $\langle x,y\rangle = \mathrm{Tr}_1^m(xy)$): Given a linear transformation $\mathcal{L}$ on $\mathbb{F}_{2^m}$, the adjoint of $\mathcal{L}$ is the uniquely determined linear map $\mathcal{L}^*$ on $\mathbb{F}_{2^m}$ that satisfies $\mathrm{Tr}_1^m(x,\mathcal{L}(y)) = \mathrm{Tr}_1^m(\mathcal{L}^*(x),y)$ for all $x,y\in\mathbb{F}_{2^m}$.

We first show the following lemma:

Lemma 1. *Let $\mathcal{A}_1(x)$ and $\mathcal{A}_2(x)$ be defined as in Equation* (2)*. Then the following conditions are equivalent.*

(i) $\mathcal{A}_1(x)=0$ *does not have a solution in* $\mathbb{F}_{2^m}$.
(ii) $\mathcal{A}_2(x)=0$ *does not have a solution in* $\mathbb{F}_{2^m}$.
(iii) $\Lambda(x) = x+\sum_{j=1}^{\sigma}\alpha_j x^{2^{t_j}}$ *is a permutation of* $\mathbb{F}_{2^m}$.

Proof: We start showing that (i) holds if and only if (iii) holds. Note that $\mathcal{A}_1(x)=0$ does not have a solution in $\mathbb{F}_{2^m}$ if and only if $\mathcal{L}_1(x)=x\mathcal{A}_1(x)$ is a linear permutation of $\mathbb{F}_{2^m}$. Observe that $\mathcal{L}_1$ then also permutes $\mathbb{F}_{2^n}$ (suppose that y is a solution in $\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$, then, using that $\alpha_j\in\mathbb{F}_{2^m}$, the element $\mathrm{Tr}_m^n(y)\in\mathbb{F}_{2^m}^*$ is a solution). Recall that the adjoint $\mathcal{L}_1^*$ of $\mathcal{L}_1$ and $\mathcal{L}_1$ have the same rank. Hence $\mathcal{L}_1$ permutes $\mathbb{F}_{2^m}$ if and only if $\mathcal{L}_1^*$ permutes $\mathbb{F}_{2^m}$. With standard calculations, using that $\mathrm{Tr}_1^m(xy^{2^{m-t}})=\mathrm{Tr}_1^m(x^{2^t}y)$, we infer that

$$\mathcal{L}_1^*(x) = x+\sum_{j=1}^{\sigma}\alpha_j x^{2^{t_j}} =: \Lambda(x).$$

This finishes the first part of the proof.

We conclude the proof by showing that (iii) holds if and only if (ii) holds. Observe that $\Lambda(x)=\mathcal{L}_1^*(x)$ permutes $\mathbb{F}_{2^m}$ if and only if

$$(\mathcal{L}_1^*(x))^{2^{m-r}} = x^{2^{m-r}} + \sum_{j=1}^{\sigma}\alpha_j^{2^{m-r}}x^{2^{m+t_j-r}}$$

is a permutation of $\mathbb{F}_{2^m}$. Substituting $x^{2^{m-r}}$ by x we see that this is equivalent to $x\mathcal{A}_2(x)$ being a (linear) permutation of $\mathbb{F}_{2^m}$, i.e., $\mathcal{A}_2(x)=0$ does not have a solution in $\mathbb{F}_{2^m}$. □

Theorem 1. *Let $r\geq 0$ be an integer, $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$, and let Λ be a linearized polynomial with coefficients in $\mathbb{F}_{2^m}$. The function $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$ given as*

$$F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x)))$$

is a vectorial bent function if and only if Λ is a permutation of $\mathbb{F}_{2^m}$. In particular, $\mathcal{F}:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$, $\mathcal{F}(x)=x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x))$ then has 2^n-2^m bent components (the set $\{\mathcal{F}_\gamma:\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}\}$ of component functions).

Proof: First note that with a linear transformation we can transform a linearized polynomial $\Lambda\in\mathbb{F}_{2^m}[x]$ to a polynomial of the form

$$\Lambda(x) = x+\sum_{j=1}^{\sigma}\alpha_j x^{2^{t_j}}\in\mathbb{F}_{2^m}[x]. \tag{3}$$

Such a coordinate transformation changes in F the term γx^{2^r} into a term $\bar\gamma x^{2^{\bar r}}$ for some integer $\bar r$ and an element $\bar\gamma\in\mathbb{F}_{2^n}$, which is again not in $\mathbb{F}_{2^m}$. Hence we may assume without loss of generality that Λ is of the form (3). With [12, Theorem 6] and Lemma 1 we then see the sufficiency of the condition in the theorem. It remains to show the necessity. Recall that F is a vectorial bent function if and only if all derivatives are balanced, i.e., for every $a\in\mathbb{F}_{2^n}^*$ the solution space of $\mathcal{D}_aF=0$ has dimension m. With straightforward standard calculations we get

$$\begin{aligned}\mathcal{D}_aF(x) &= \mathrm{Tr}_m^n(\gamma a^{2^r})\mathrm{Tr}_m^n(x+\sum_{j=1}^{\sigma}\alpha_j x^{2^{t_j}})\\ &\quad+\mathrm{Tr}_m^n(a+\sum_{j=1}^{\sigma}\alpha_j a^{2^{t_j}})\mathrm{Tr}_m^n(\gamma x^{2^r})\\ &= \mathrm{Tr}_m^n(\gamma a^{2^r})\mathrm{Tr}_m^n(\Lambda(x))+\mathrm{Tr}_m^n(\gamma x^{2^r})\mathrm{Tr}_m^n(\Lambda(a)).\end{aligned}$$

Let $a\in\mathbb{F}_{2^m}^*$, then $\mathcal{D}_aF(x)=0$ for all $x\in\mathbb{F}_{2^m}$. Hence $\mathbb{F}_{2^m}$ is in the solution space of $\mathcal{D}_aF=0$. Suppose that Λ is not a permutation, then for some $y\in\mathbb{F}_{2^m}^*$ we have $\Lambda(y)=0$. Let $z\in\mathbb{F}_{2^n}$ such that $\mathrm{Tr}_m^n(z)=y$ (thus $z\notin\mathbb{F}_{2^m}$). With $\mathrm{Tr}_m^n(\Lambda(z))=\Lambda(\mathrm{Tr}_m^n(z))=\Lambda(y)=0$, we see that $\mathcal{D}_aF(z)=0$, and hence the dimension of the solution space of $\mathcal{D}_aF=0$ is larger than m. □

B. $\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma\mathbf{x}^{\mathbf{2^r}}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\mathbf{\Lambda(x)}))$ *and Its Solution Spaces*

We start this subsection pointing out that all vectorial bent functions $F(x)=\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x)))$ belong to the completed (quadratic) Maiorana-McFarland class of vectorial bent functions. Recall that a vectorial bent function M from $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is called a vectorial Maiorana-McFarland function if $M(x,y)=x\pi(y)+R(y)$ for some permutation π of $\mathbb{F}_{2^m}$ and a function R on $\mathbb{F}_{2^m}$.

We say that two functions $F_1,F_2:\mathbb{V}_n\to\mathbb{V}_m$ are *extended affine equivalent (EA-equivalent)*, if there exist affine permutations L_1,L_2 on $\mathbb{V}_n$ and $\mathbb{V}_m$, respectively, and an affine function $a:\mathbb{V}_n\to\mathbb{V}_m$ such that $F_2(x)=L_2(F_1(L_1(x)))+a(x)$. A function F belongs to the completed Maiorana-McFarland class, if F is EA-equivalent to some function from the Maiorana-McFarland class. With a straightforward argument one can see that the standard criterion for a Boolean bent function to belong to the completed (Boolean) Maiorana-McFarland class, see [9], applies in the same way to vectorial bent functions: A vectorial bent function $F:\mathbb{V}_n\to\mathbb{V}_m$ is in the completed Maiorana-McFarland class if and only if there exists an m-dimensional subspace V of $\mathbb{V}_n$ such that F is affine on every coset of V.

Let now F be the vectorial bent function $F(x)=\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\Lambda(x))$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$, let $V=\mathbb{F}_{2^m}$, and

$d \in \mathbb{F}_{2^n}$. Evaluating F on the coset $V+d$, using that $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(z)=0$ for $z \in \mathbb{F}_{2^m}$, we obtain

$$\begin{aligned} F(z+d) &= \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma(z+d)^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(z+d))) \\ &= \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(z)+\Lambda(d))\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma z^{2^r}+\gamma d^{2^r}) \\ &= \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(d))\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma z^{2^r}) + \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(d))\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma d^{2^r}), \end{aligned}$$

which shows that F belongs to the completed Maiorana-McFarland class.

The objective in this subsection is to study the solution spaces for

$$\mathcal{D}_aF(x) = \mathrm{Tr}^{n}_{m}(\gamma a^{2^r})\mathrm{Tr}^{n}_{m}(\Lambda(x)) + \mathrm{Tr}^{n}_{m}(\gamma x^{2^r})\mathrm{Tr}^{n}_{m}(\Lambda(a)) = 0$$

for the quadratic vectorial bent functions $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$.

Let $r \geq 0$ be an integer, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, and let Λ be a linear permutation of $\mathbb{F}_{2^m}$. For every $z \in \mathbb{F}_{2^m}$ we define the subspace $U_z(r,\gamma,\Lambda)$ of $\mathbb{F}_{2^n}$ as

$$U_z(r,\gamma,\Lambda) := \{x \in \mathbb{F}_{2^n} \,:\, \mathrm{Tr}^{n}_{m}(\gamma x^{2^r}) + z\mathrm{Tr}^{n}_{m}(\Lambda(x)) = 0\}. \tag{4}$$

To simplify the notation, for fixed r, γ and Λ, we will write U_z for $U_z(r,\gamma,\Lambda)$.

It is quite easily observed that $U_{z_1} \cap U_{z_2} = \{0\}$ if $z_1 \neq z_2$. More precisely we have the following lemma:

Lemma 2. *Let $r \geq 0$ be an integer, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and let Λ be a linearized permutation of $\mathbb{F}_{2^m}$. Then for every $z \in \mathbb{F}_{2^m}$, the subspace U_z in* (4) *is an m-dimensional subspace of $\mathbb{F}_{2^n}$. The subspaces U_z, $z \in \mathbb{F}_{2^m}$, together with $\mathbb{F}_{2^m}$ form a spread of $\mathbb{F}_{2^n}$.*

Proof: As already observed, for $F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$, the solution space for $\mathcal{D}_aF = 0$ is $\mathbb{F}_{2^m}$ if a is a nonzero element in $\mathbb{F}_{2^m}$. Note that for $a \notin \mathbb{F}_{2^m}$, the solution space of $\mathcal{D}_aF = 0$ is U_z with $z = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma a^{2^r})/\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(a))$. Hence every subspace U_z, which appears as the solution space of $\mathcal{D}_aF = 0$ for some $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ has dimension m. Since every a is a solution of $\mathcal{D}_aF(x) = 0$, the union of all solution spaces for $\mathcal{D}_aF = 0$, $a \in \mathbb{F}^*_{2^n}$ is $\mathbb{F}_{2^n}$. Moreover, the fact that for $a \in U_z$ the solution space of $\mathcal{D}_aF = 0$ is U_z implies that every U_z appears as a solution space. Therefore, besides from $\mathbb{F}_{2^m}$, all 2^m subspaces U_z, $z \in \mathbb{F}_{2^m}$, must appear as a solution space, and the intersection of each two of those spaces must be trivial. Hence the subspaces $\mathbb{F}_{2^m}$, U_z, $z \in \mathbb{F}_{2^m}$, form a spread of $\mathbb{F}_{2^n}$. □

Remark 1. *Note that whereas the subspaces $U_z = U_z(r,\gamma,\Lambda)$ depend on r, γ and Λ, the spread in Lemma 2, i.e., the collection of the subspaces U_z, $z \in \mathbb{F}_{2^m}$, solely depends on r and Λ.*

From Lemma 2, we immediately infer the following theorem:

Theorem 2. *For an integer $r \geq 0$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, and a linearized permutation $\Lambda \in \mathbb{F}_{2^m}[x]$, let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be the vectorial bent function*

$$F(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))).$$

For $a \in \mathbb{F}^*_{2^m}$ we then have $F(x) + F(x+a) + F(a) = 0$ if and only if $x \in \mathbb{F}_{2^m}$. The solution space of $\mathcal{D}_aF(x) = F(x) + F(x+a) + F(a) = 0$ is U_z if and only if $a \in U_z$, where U_z, $z \in \mathbb{F}_{2^m}$, are the subspaces defined in (4).

In the special case $r = 0$ and $\Lambda(x) = x$ it is easily observed that the spread in Lemma 2 reduces to the classical representation of the Desarguesian spread, i.e., the subspaces $U_z = U_z(0,\gamma,x)$ are the multiplicative cosets of $\mathbb{F}_{2^m}$ (the zero element added). In fact, this was shown in [6] for the function x^{2^m+1}, which differs from $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x))$ only by a linear term.

The set of the solution spaces of $\mathcal{D}_aF = 0$ forming a spread is a quite extremal property (and as we will see in Theorem 3 below not just the typical behaviour of a quadratic vectorial bent function). As every $a \in \mathbb{F}^*_{2^n}$ is a solution of $\mathcal{D}_aF(x) = 0$, hence every $a \in \mathbb{F}^*_{2^n}$ is in at least one of the solution spaces, the number of distinct solutions spaces takes on the minimal possible value $2^m + 1$.

In the following theorem we show that with this respect the vectorial bent function $K(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^3)$, $n = 2m$, m odd, and γ is a noncube in $\mathbb{F}_{2^n}$, is at the other end of the spectrum. For different $a, b \in \mathbb{F}_{2^n}$, the solution spaces S_a and S_b for $\mathcal{D}_aK = 0$ and $\mathcal{D}_bK = 0$ are different. Hence we have the maximal possible number $2^n - 1$ of distinct solution spaces. Employing Bezout's theorem on intersection points of two projective plane curves we more generally show that $|S_a \cap S_b| \leq 4$ if $a \neq b$.

Theorem 3. *Let $n = 2m$ for an odd integer m and $K(x) = \mathrm{Tr}^{n}_{m}(\gamma x^3)$ for a noncube $\gamma \in \mathbb{F}_{2^n}$. We denote by S_a the solution space of $\mathcal{D}_aK(x) = K(x+a) + K(x) + K(a) = 0$ for a nonzero $a \in \mathbb{F}_{2^n}$. If $a \neq b$, then $|S_a \cap S_b| \leq 4$.*

Proof: First of all note that without loss of generality, we can suppose that $a = 1$. Otherwise we perform the change of variable $x \to ax$ and exchange γ with γ/a^3. Note that with γ, also γ/a^3 is a noncube, hence not in $\mathbb{F}_{2^m}$.

Suppose that there exists $b \in \mathbb{F}_{2^n}$ with $b \neq 1$ such that $|S_1 \cap S_b| > 4$. We set $Y := x^{2^m}$ and $X := x$. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be the curves defined by

$$\begin{aligned} &\mathcal{X}_1 :\ \gamma^{2^m}Y^2 + \gamma^{2^m}Y + \gamma X^2 + \gamma X = 0, \quad \text{and} \\ &\mathcal{X}_2 :\ \gamma^{2^m}b^{2^m}Y^2 + \gamma^{2^m}b^{2^{m+1}}Y + \gamma b X^2 + \gamma b^2 X = 0, \end{aligned}$$

respectively. Since $b \neq 1$, the curves $\mathcal{X}_1$ and $\mathcal{X}_2$ are distinct conics. Note that x is a zero of $\mathrm{Tr}^{n}_{m}\big(\gamma(x^2+x)\big)$ (resp., $\mathrm{Tr}^{n}_{m}\big(\gamma(bx^2+b^2x)\big)$) if and only if (x, x^{2^m}) is a point on the curve $\mathcal{X}_1$ (resp., $\mathcal{X}_2$). Then the fact that $|S_1 \cap S_b| > 4$ implies that $\mathcal{X}_1$ and $\mathcal{X}_2$ intersect in more than 4 points. Therefore, they have a common component by Bezout's Theorem. The common component has to be a line as $\mathcal{X}_1$ and $\mathcal{X}_2$ are distinct conics. In particular, $\mathcal{X}_1$ is a union of two lines, say $\mathcal{X} = L_1 \cup L_2$. Since

$$\frac{\partial \mathcal{X}_1}{\partial X} = \gamma \quad \text{and} \quad \frac{\partial \mathcal{X}_1}{\partial Y} = \gamma^{2^m},$$

$\mathcal{X}_1$ has no singular affine points. In particular, L_1 and L_2 intersect at infinity, otherwise $\mathcal{X}_1$ would have an affine singular point. Therefore, by using the fact that $(0,0)\in\mathcal{X}_1$, we obtain the following equalities:

$$\begin{aligned}\gamma^{2^m}Y^2+\gamma^{2^m}Y+\gamma X^2+\gamma X &= (\alpha Y+\beta X+c)(\alpha Y+\beta X)\\ &= \alpha^2Y^2+c\alpha Y+\beta^2X^2\\ &\quad +c\beta X \qquad (5)\end{aligned}$$

for some nonzero α,β,c in the algebraic closure of $\mathbb{F}_{2^n}$. That is, by Equation (5), we have

$$\gamma^{2^m}=\alpha^2,\quad \gamma^{2^m}=c\alpha,\quad \gamma=\beta^2 \quad\text{and}\quad \gamma=c\beta.$$

Note that the facts that $\gamma^{2^m}=\alpha^2=c\alpha$ and $\gamma=\beta^2=c\beta$ imply that $c=\alpha=\beta$. Therefore, we have $\alpha^2=\beta^2$. This implies that $\gamma^{2^m}=\gamma$, i.e., $\gamma\in\mathbb{F}_{2^m}$, a contradiction. □

We finally remark that $S_a\cap S_b=\{0\}$ or $S_a=S_b$, where $S_a=\{x\in\mathbb{F}_{2^n} : F(x)+F(x+a)+F(a)=0\}$, is also not the typical behaviour of a nonquadratic vectorial Maiorana-McFarland bent function F. As we observed computationally, as a counterexample one may for instance take the function $F:\mathbb{F}_{2^4}\times\mathbb{F}_{2^4}\to\mathbb{F}_{2^4}$, $F(x,y)=xg_7(y)$, where g_7 is the first order Dickson polynomial $g_7(x)=x^7+x^5+x$, a permutation of $\mathbb{F}_{2^4}$.

C. Differential Uniformity Conditions

In [6], the properties of the Desarguesian spread of $\mathbb{F}_{2^n}$ in standard representation were employed to give conditions for the function $H(x)=(x^{2^m+1},G(x))$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to have small differential uniformity. The construction of Carlet's, the Zhou-Pott, and Taniguchi's APN-functions, all of the form $\tilde{H}(x,y)=(xy,G(x,y))$ are based on the analog observations in bivariate form, [5], [18], [22].

Clearly, the differential spectrum of our quadratic functions $H(x)=(F(x),G(x))$ is determined by the differential behaviour of G on the solution spaces of $\mathcal{D}_aF(x)=0$. With the analysis of these solution spaces for $F(x)=\mathrm{Tr}^n_m(\gamma x^{2^r}\mathrm{Tr}^n_m(\Lambda(x)))$ in Section II-B we immediately infer the following proposition:

Proposition 1. *Let $r\geq 0$ be an integer, $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ and let Λ be a linearized permutation of $\mathbb{F}_{2^m}$. For a quadratic function $G(x)$ from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ let $H:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ be given as*

$$H(x)=(\mathrm{Tr}^n_m(\gamma x^{2^r}\mathrm{Tr}^n_m(\Lambda(x))),G(x)).$$

Then H is differentially k-uniform if and only if

- *G is differentially k-uniform on $\mathbb{F}_{2^m}$;*
- *for all $z\in\mathbb{F}_{2^m}$ and every $a\in U_z$ the function $G(x)+G(x+a)$ from U_z to $\mathbb{F}_{2^m}$ has at most k elements in the preimage set of any element in $\mathbb{F}_{2^m}$.*

We now restrict ourselves to the case that $F(x)=\mathrm{Tr}^n_m(\gamma x^{2^r}\mathrm{Tr}^n_m(x))$, i.e., $\Lambda(x)=x$, and further analyse for this case the corresponding solution spaces

$$U_z=U_z(r,\gamma,\Lambda)=\{x\in\mathbb{F}_{2^n} : \mathrm{Tr}^n_m(\gamma x^{2^r})+z\mathrm{Tr}^n_m(x)=0\}. \qquad (6)$$

One objective is to obtain simpler conditions for a small differential uniformity of $H(x)=(F(x),G(x))$.

Lemma 3. *Let $r\geq 0$ be an integer, and $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$. For $z\in\mathbb{F}_{2^m}$ let $U_z=U_z(r,\gamma,\Lambda)$ with $\Lambda(x)=x$ be given as in (6). Then $U_0=\beta\mathbb{F}_{2^m}$, where β is the unique element satisfying $\gamma\beta^{2^r}=1$. If $\alpha\in U_z$, $z\neq 0$, then for every $c\in\mathbb{F}^*_{2^m}$ the element $c\alpha$ lies in $U_{c^{2^r-1}z}$.*

Proof: Obviously, for $x=\beta y$ with $\gamma\beta^{2^r}=1$ and $y\in\mathbb{F}_{2^m}$, we have $\mathrm{Tr}^n_m(\gamma x^{2^r})=\mathrm{Tr}^n_m(y^{2^r})=0$. Hence $x\in U_0$, and by the dimension of U_0 we have $U_0=\beta\mathbb{F}_{2^m}$. Let α be in U_z, i.e., $\gamma\alpha^{2^r}+z\alpha=d\in\mathbb{F}_{2^m}$. Hence for $c\alpha$, $c\in\mathbb{F}^*_{2^m}$, we have $\gamma(c\alpha)^{2^r}+(c^{2^r-1}z)(c\alpha)=c^{2^r}d\in\mathbb{F}_{2^m}$. Therefore, $c\alpha\in U_{c^{2^r-1}z}$. □

As a consequence of Lemma 3 we obtain the following lemma:

Lemma 4. *Let $r\geq 0$ be an integer, and $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$. Let η be a primitive element of $\mathbb{F}_{2^m}$, let $\gcd(2^m-1,2^r-1)=2^d-1$ and $R_d=\{1,\eta,\eta^2,\ldots,\eta^{2^d-2}\}$. Then every subspace $U_z=U_z(r,\gamma,\Lambda)$ with $\Lambda(x)=x$ given as in (6) and $z\neq 0$, is of the form $U_z=cU_s$ for some $c\in\mathbb{F}^*_{2^m}$ and a unique $s\in R_d$. In particular, if $\gcd(2^m-1,2^r-1)=1$, i.e., $R_d=\{1\}$, then for every U_z, $z\neq 0$, we have $U_z=cU_1$ for some $c\in\mathbb{F}^*_{2^m}$. In the special case $r=0$, i.e., $\gcd(2^m-1,2^r-1)=2^m-1$ and $R_d=\mathbb{F}^*_{2^m}$, the relation between the subspaces U_z described as above dissolves, and the spread $\mathbb{F}_{2^m}\cup\{U_z : z\in\mathbb{F}_{2^m}\}$ reduces to the standard representation of the Desarguesian spread of $\mathbb{F}_{2^n}$, i.e., $\{\beta^i\mathbb{F}_{2^m} : i=0,\ldots,2^m\}$ where β is a primitive (2^m+1)th root of unity.*

Proof: Observe that every nonzero element z in $\mathbb{F}_{2^m}$ has a unique representation as $z=c\eta^t$ for some $t\in\{0,1,\ldots,2^d-2\}$ and (2^d-1)th power $c\in\mathbb{F}_{2^m}$. Since $\gcd(2^m-1,2^r-1)=2^d-1$, any (2^d-1)th power is (2^r-1)th power, i.e., $c=c_1^{2^r-1}$ for some $c_1\in\mathbb{F}^*_{2^m}$. The general statement of the lemma follows then from the fact that $U_z=U_{c_1^{2^r-1}\eta^t}=c_1U_{\eta^t}$ as shown in Lemma 3.
In particular, if $\gcd(2^m-1,2^r-1)=1$, i.e., $d=1$, then $R_d=R_1=\{1\}$ and for every nonzero z we have $U_z=cU_1$ for some $c\in\mathbb{F}^*_{2^m}$.
If $r=0$ then $d=m$, $R_m=\mathbb{F}^*_{2^m}$ and the observed relation between the subspaces U_z reduces to the trivial statement that $U_z=U_s$ for a unique $s\in\mathbb{F}^*_{2^m}$. As already remarked, in this case we obtain the standard representation of the spread. In fact it is easily seen from (6) that for $r=0$, every subspace U_z is a multiplicative coset of $\mathbb{F}_{2^m}$ (plus the 0). Hence, we only need to show that $\{\beta^i\mathbb{F}_{2^m} : i=0,\ldots,2^m\}$ forms the set of multiplicative cosets of $\mathbb{F}_{2^m}$. Note that $\beta^i\mathbb{F}_{2^m}=\beta^j\mathbb{F}_{2^m}$ for some $i,j\in\{0,\ldots,2^m\}$ if and only if $\beta^{i-j}\in\mathbb{F}_{2^m}$. This holds if and only if $i-j\equiv 0 \mod (2^m+1)$, which is possible only in the case that $i=j$ as β is a primitive (2^m+1)th root of unity. □

We first can recover results in [6] as the special case when $r=0$, cf. [6, Theorem 2.1, Proposition 2.3]. We give the proof for completeness, and remark that differently than stated in [6, Proposition 2.3], the condition in (ii) is required only for $\beta\in\mathbb{F}_{2^n}$ for which $\beta^{2^m+1}=1$.

Corollary 1. *Let $H:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ be given as $H(x)=(\mathrm{Tr}^n_m(\gamma x\mathrm{Tr}^n_m(x)),G(x))$ for some $\gamma\in\mathbb{F}_{2^n}\setminus\mathbb{F}_{2^m}$ and a quadratic function $G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$.*

(i) *H is APN (resp.,differentially k-uniform) if and only if $G(ax)+G(ax+a)=b$ has at most 2 (resp., k) solutions for all b and nonzero a in $\mathbb{F}_{2^n}$ as a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$.*

(ii) *If $G(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma x^{2^i+1} + \tau x^{2^{i+m}+1})$, $\sigma, \tau \in \mathbb{F}_{2^n}$, $\gcd(m,i)=1$, then H is APN if and only if $\sigma\beta^{1+2^i} + \tau\beta^{1-2^i} \notin \mathbb{F}_{2^m}$ for all $\beta \in \mathbb{F}_{2^n}$ with $\beta^{2^m+1}=1$. If H is not APN, then H has differential uniformity 2^m.*

Proof: (i) Note that for $a \in \mathbb{F}_{2^n}^*$ and $F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(x))$, the solution space of $F(x)+F(x+a)+F(a)=0$ is exactly $a\mathbb{F}_{2^m}$. Without loss of generality we may assume that $G(0)=0$. Then H is APN (differentially k-uniform) if and only if $G(ax)+G(ax+a)+G(a)=0$ has two solutions, 0 and 1, (at most k solutions) in $\mathbb{F}_{2^m}$, which gives the desired conclusion.

(ii) By Lemma 4, case $r=0$, the function H is APN if and only if for every element $\beta\mathbb{F}_{2^m}$ of the Desarguesian spread in standard representation, the function G restricted to $\beta\mathbb{F}_{2^m}$ is APN. Equivalently, for every (2^m+1)th root of unity $\beta \in \mathbb{F}_{2^n}$, the function $G(\beta x)$ is APN as a function on $\mathbb{F}_{2^m}$. For $x \in \mathbb{F}_{2^m}$ we have

$$\begin{aligned} G(\beta x) &= \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma\beta^{2^i+1}x^{2^i+1} + \tau\beta^{2^{i+m}+1}x^{2^i+1}) \\ &= \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma\beta^{2^i+1} + \tau\beta^{2^{i+m}+1})x^{2^i+1}, \end{aligned}$$

which assuming that $\gcd(m,i)=1$ is APN if and only if $\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma\beta^{2^i+1} + \tau\beta^{2^{i+m}+1}) \neq 0$, i.e., $\sigma\beta^{2^i+1} + \tau\beta^{2^{i+m}+1} \notin \mathbb{F}_{2^m}$. With $\beta^{2^m+1}=1$ this is equivalent to $\sigma\beta^{1+2^i}+\tau\beta^{1-2^i} \notin \mathbb{F}_{2^m}$. Otherwise, $G(\beta x)$ is the 0-function for some β, hence H has differential uniformity 2^m. □

Remark 2. *Let W be the set of (2^m+1)th roots of unity. If $\tau=0$, hence $G(x)=\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma x^{2^i+1})$, then the condition in Corollary 1 (ii) reduces to $\sigma\beta^{2^i+1} \notin \mathbb{F}_{2^m}$ for all $\beta \in W$. This is satisfied if σ does not lie in any of the spread elements $\beta^{-(2^i+1)}\mathbb{F}_{2^m}$ for $\beta \in W$. Clearly such σ exist if and only if $\{\beta^{-(2^i+1)} : \beta \in W\} \neq W$, which holds if and only if $\gcd(2^m+1, 2^i+1) > 1$. This applies if and only if m and i are both odd. If m is even and $\tau=0$, then H in Corollary 1 (ii) always has the worst possible differential uniformity 2^m.*

For $\gcd(m,r) < m$, with quadratic functions G with some additional property, we can take advantage of the relations between the solution spaces U_z which we showed in Lemma 4.

Corollary 2. *Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be a quadratic function such that $G(0)=0$ and for every nonzero $c \in \mathbb{F}_{2^m}$ we have $G(c\alpha)=K(c)G(\alpha)$ for some nonzero constant $K(c) \in \mathbb{F}_{2^m}$ (depending on c) and every $\alpha \in \mathbb{F}_{2^n}$. For an integer $r \geq 0$ and $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, let $F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(x))$, and let $U_z = U_z(r,\gamma,\Lambda)$ be defined as in (4). If $\gcd(2^m-1, 2^r-1) = 2^d-1$, then $H(x)=(F(x),G(x))$ is differentially k-uniform if and only if*

(i) *G is differentially k-uniform on $\mathbb{F}_{2^m}$;*

(ii) *G is differentially k-uniform as a function from U_0 to $\mathbb{F}_{2^m}$;*

(iii) *for every $0 \leq t \leq 2^d-2$, the function G is differentially k-uniform as a function from U_{η^t} to $\mathbb{F}_{2^m}$, where η is a fixed primitive element of $\mathbb{F}_{2^m}$.*

If $\gcd(2^m-1, 2^r-1)=1$, then Condition (iii) reduces to the condition that G is differentially k-uniform as a function from U_1 to $\mathbb{F}_{2^m}$.

Proof: For $a \in \mathbb{F}_{2^m}^*$ we require that $G(x)+G(x+a)+G(a)=0$ has at most k solutions in $\mathbb{F}_{2^m}$, i.e., G is differentially k-uniform as a function on $\mathbb{F}_{2^m}$. For an element $a \in U_z = U_c(r,\gamma,x)$ for some $z \in \mathbb{F}_{2^m}$, the solution space of $F(x)+F(x+a)+F(a)=0$ is precisely U_z. Hence we require that the equation $G(x)+G(x+a)+G(a)=0$ has at most k solutions in U_z. For $z=0$ this is Condition (ii) in the corollary.

If $z \neq 0$, then by Lemma 4, $U_z = cU_{\eta^t}$ for a unique $0 \leq t \leq 2^d-2$ and $c \in \mathbb{F}_{2^m}^*$. The condition that $G(x)+G(x+a)+G(a)=0$ has at most k' solutions as a function from U_z to $\mathbb{F}_{2^m}$ for all nonzero $a \in U_z$ can then be rewritten that $G(cx)+G(c(x+a))+G(ca)=0$ has at most k' solutions as a function from U_{η^t} to $\mathbb{F}_{2^m}$ for all nonzero $a \in U_{\eta^t}$ (k' may depend on a and $k' \leq k$). By our assumption, we have $G(cx)+G(c(x+a)) = K(c)(G(x)+G(x+a))$ for a nonzero constant $K(c) \in \mathbb{F}_{2^m}$. Hence $G(cx)+G(c(x+a))$ is k'-to-1 from U_{η^t} to $\mathbb{F}_{2^m}$ if and only if $G(x)+G(x+a)$ is. The last statement in the corollary follows immediately. □

Remark 3. *The condition in Corollary 2 is satisfied by every monomial G (in the sense that G is a relative trace of a monomial). But also the binomial G in Corollary 1 (ii), which has been used in [6] for the case that $F(x)=x^{2^m+1}$, i.e., $r=0$, satisfies the condition for all $c \in \mathbb{F}_{2^m}$. Also note that the condition $G(c\alpha)=K(c)G(\alpha)$ for all $c \in \mathbb{F}_{2^m}$ in the above corollary is stronger than needed, and may be replaced by $G(c\alpha)=K(c)G(\alpha)$ for all $c \in \{1, \eta, \ldots, \eta^{\frac{2^m-1}{2^d-1}-1}\}$, where η is a primitive element of $\mathbb{F}_{2^m}$.*

III. Differential uniformity and nonlinearity results

In this section we analyse functions $H(x)=(F(x),G(x))$ where F is a Maiorana-McFarland bent function $F(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\gamma x^{2^r}\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(x))$, and G is a Gold function $G(x) = \mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma x^{2^i+1})$. We also add some results on the case that $G(x)=\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma x^{2^i+1} + \tau x^{2^{i+m}+1})$. We start with the differential uniformity of H, in the second part of this section we will also investigate the nonlinearity.

The case $r=0$ is covered by Corollary 1(ii). The form of the binomial $G(x)$, which, restricted to the elements of the corresponding spread, is the Gold APN-function, indicates that the APN-functions H are a version of Carlet's function in [5], which is given in bivariate form. They all have the classical spectrum, we refer to [1].

Besides from the case when $r=0$, in the light of Corollary 2, the case that $\gcd(2^m-1, 2^r-1)=1$ seems most promising to construct functions with small differential uniformity. In this case, the differential uniformity of H depends on the behaviour of G on only three elements of the spread, $\mathbb{F}_{2^m}$, $U_0 = \beta\mathbb{F}_{2^m}$, where $\gamma\beta^{2^r}=1$, and U_1. For a given G, the conditions (i), (ii) in Corollary 2 for the spread elements $\mathbb{F}_{2^m}$ and U_0 look simpler than the condition for U_1. With the argument used in the proof of Corollary 1 for $G(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma x^{2^i+1} + \tau x^{2^{i+m}+1}))$ we infer that $H(x)$ is differentially k-uniform (for some $k < 2^m$) if and only if

(I) $\sigma + \tau \notin \mathbb{F}_{2^m}$ and $\sigma\beta^{2^i+1} + \tau\beta^{2^{i+m}+1} \notin \mathbb{F}_{2^m}$, where β is the unique element such that $\gamma\beta^{2^r} = 1$;

(II) $G(x) + G(x+a) + G(a) = 0$ has at most k solutions in U_1 for every nonzero $a \in U_1$.

To investigate the differential uniformity of H, we transform (II) into a condition for a function from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$. As $\{1, \gamma\}$ is a basis for $\mathbb{F}_{2^n}$ over $\mathbb{F}_{2^m}$, we can write

$$\gamma^{2^r+1} = a_1\gamma + a_0 \quad \text{for some } a_1, a_0 \in \mathbb{F}_{2^m}.$$

Let $c \in \mathbb{F}_{2^m}$ such that $c^{2^r} = a_1$. Define ψ on $\mathbb{F}_{2^n}$ by

$$\psi(T) := T + (\gamma + c)T^{2^r}. \tag{7}$$

Note that since $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, we have $\gamma + c \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$.

Proposition 2. *ψ is an isomorphism from $\mathbb{F}_{2^m}$ to U_1.*

Proof: We recall that $|U_1| = 2^m$. Therefore, it is enough to show that ψ is one-to-one on $\mathbb{F}_{2^m}$ and $\psi(\mathbb{F}_{2^m}) \subseteq U_1$.

Note that $\psi(x) = 0$ if and only if $x = 0$ or $(c+\gamma)x^{2^r-1} + 1 = 0$, i.e., $x^{2^r-1} = (c+\gamma)^{-1}$. Since $(c+\gamma)^{-1} \notin \mathbb{F}_{2^m}$, for $x \in \mathbb{F}_{2^m}$, we have $\psi(x) = 0$ if and only if $x = 0$, which proves that ψ is one-to-one on $\mathbb{F}_{2^m}$.

$\psi(x) \in U_1$ if and only if $\psi(x) + \gamma\psi(x)^{2^r} \in \mathbb{F}_{2^m}$. By definition of ψ, we have the following equalities:

$$\begin{aligned}\psi(x) + \gamma\psi(x)^{2^r} &= x + (c+\gamma)x^{2^r} + \gamma\left(x + (c+\gamma)\,x^{2^r}\right)^{2^r}\\ &= x + cx^{2^r} + \gamma c^{2^r}x^{2^{2r}} + \gamma^{2^r+1}x^{2^{2r}}\\ &= x + cx^{2^r} + (\gamma a_1 + \gamma^{2^r+1})x^{2^{2r}}\\ &= x + cx^{2^r} + a_0x^{2^{2r}}.\end{aligned}$$

Note that we have used the fact that $c^{2^r} = a_1$ in the third equality and that $\gamma^{2^r+1} = \gamma a_1 + a_0$ in the fourth equality. Since $x, c, a_0 \in \mathbb{F}_{2^m}$, we conclude that $\psi(x) + \gamma\psi(x)^{2^r} \in \mathbb{F}_{2^m}$. □

With Proposition 2 we obtain the following corollary.

Corollary 3. *For $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and an integer r with $\gcd(r,m) = 1$ let $H(x) = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)), G(x))$ with $G(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma x^{2^i+1})$. Let $\gamma^{2^r+1} = a_1\gamma + a_0$, $a_0, a_1 \in \mathbb{F}_{2^m}$, and $c \in \mathbb{F}_{2^m}$ such that $c^{2^r} = a_1$, and let $\psi(x) = x + (\gamma + c)x^{2^r}$ be the isomorphism in Proposition 2. Then H is differentially k-uniform (for some $k < 2^m$) if and only if*

(a) *$\sigma \notin \mathbb{F}_{2^m}$ and $\sigma\gamma^{(-2^i-1)2^{-r}} \notin \mathbb{F}_{2^m}$;*

(b) *for every nonzero $b \in U_1$ and for the function*

$$\begin{aligned}&\mathrm{Tr}^n_m(\sigma b(c+\gamma)^{2^i})x^{2^{r+i}} + \mathrm{Tr}^n_m(\sigma b)x^{2^i}\\ &+ \mathrm{Tr}^n_m(\sigma b^{2^i}(c+\gamma))x^{2^r} + \mathrm{Tr}^n_m(\sigma b^{2^i})x\end{aligned} \tag{8}$$

on $\mathbb{F}_{2^m}$, the preimage of an element in $\mathbb{F}_{2^m}$ has size at most k.

Proof: For $\tau = 0$ the Condition (I) above reduces to the condition that $\sigma \notin \mathbb{F}_{2^m}$ and $\sigma\beta^{2^i+1} \notin \mathbb{F}_{2^m}$, where β is the unique element such that $\gamma\beta^{2^r} = 1$. Expressing β in terms of γ, Condition (a) follows.

With Proposition 2, Condition (II) above can be rewritten as $G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a)) = 0$ has at most k solutions in $\mathbb{F}_{2^m}$ for every nonzero $a \in \mathbb{F}_{2^m}$, i.e., the function $G(\psi(x))$ from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^m}$ is differentially k-uniform. With $\psi(a) = b \in U_1$ we have

$$\begin{aligned}&G(\psi(x) + \psi(a)) + G(\psi(x)) + G(\psi(a))\\ &= \mathrm{Tr}^n_m\left(\sigma\left(b\psi(x)^{2^i} + b^{2^i}\psi(x)\right)\right)\\ &= \mathrm{Tr}^n_m\left(\sigma\left(b\left(x + (c+\gamma)x^{2^r}\right)^{2^i} + b^{2^i}\left(x + (c+\gamma)x^{2^r}\right)\right)\right)\\ &= \mathrm{Tr}^n_m(\sigma b(c+\gamma)^{2^i})x^{2^{r+i}} + \mathrm{Tr}^n_m(\sigma b)x^{2^i} + \mathrm{Tr}^n_m(\sigma b^{2^i}(c+\gamma))x^{2^r}\\ &\quad + \mathrm{Tr}^n_m(\sigma b^{2^i})x,\end{aligned}$$

which completes the proof. □

Lemma 5. *Let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ and let r and i be integers relatively prime to m.*

(i) *If $i \neq r$, then the polynomial in (8) does not vanish.*

(ii) *If $i = r$ and $\gamma^{-1} \notin U_1^{2^r-1}$, then the polynomial in (8) does not vanish.*

Proof: We may assume that $\sigma \notin \mathbb{F}_{2^m}$ so that Condition (a) in Corollary 3 can be satisfied, and first consider the Case (i) that $i \neq r$. Then it suffices to show that $\mathrm{Tr}^n_m(\sigma b)$ and $\mathrm{Tr}^n_m(\sigma b^{2^i})$ can not be both zero as this shows that the polynomial in (8) does not vanish. Suppose that $\mathrm{Tr}^n_m(\sigma b) = \mathrm{Tr}^n_m(\sigma b^{2^i}) = 0$, i.e., $\sigma b, \sigma b^{2^i} \in \mathbb{F}_{2^m}$. This holds if and only if $\sigma^{2^i}b^{2^i}, \sigma b^{2^i} \in \mathbb{F}_{2^m}$, which implies that $\sigma^{2^i-1} \in \mathbb{F}_{2^m}$. Since $\gcd(i,m) = 1$, this holds if and only if $\sigma \in \mathbb{F}_{2^m}$, which contradicts our assumption.

Case (ii): The polynomial in (8) is then of the form

$$\mathrm{Tr}^n_m(\sigma b(c+\gamma)^{2^r})x^{2^{2r}} + (\mathrm{Tr}^n_m(\sigma b + \sigma b^{2^r}(c+\gamma)))x^{2^r} + \mathrm{Tr}^n_m(\sigma b^{2^r})x. \tag{9}$$

We recall that $\gamma^{2^r+1} = a_1\gamma + a_0$ and $c^{2^r} = a_1$. Then we have the following equalities:

$$\begin{aligned}\sigma b(c+\gamma)^{2^r} &= \sigma bc^{2^r} + \sigma b\gamma^{2^r} = \sigma ba_1 + \frac{\sigma b\gamma^{2^r+1}}{\gamma}\\ &= \sigma ba_1 + \frac{\sigma b}{\gamma}(a_1\gamma + a_0) = \frac{\sigma ba_0}{\gamma}.\end{aligned} \tag{10}$$

By definition of U_1, we also have

$$\sigma b^{2^r} = \frac{\sigma b}{\gamma} + \frac{\sigma e}{\gamma}, \tag{11}$$

where $e \in \mathbb{F}_{2^m}$ such that $b + \gamma b^{2^r} = e$. Moreover by our assumption, e is not 0, otherwise $\gamma^{-1} = b^{2^r-1} \in U_1^{2^r-1}$. Therefore, by Equation (10), we conclude that the coefficient of $x^{2^{2r}}$ in Equation (9) is zero if and only if $\sigma b/\gamma \in \mathbb{F}_{2^m}$. In this case, we have $\sigma/\gamma \notin \mathbb{F}_{2^m}$ since $U_1 \cap \mathbb{F}_{2^m} = \{0\}$, i.e., by Equation (11) the coefficient of x can not be zero. □

We remark that if r is odd, hence $\gcd(2^r-1, 2^n-1) = 1$, we can exchange the condition in Lemma 5(ii) with $\gamma^{-v} \notin U_1$ where $v(2^r-1) \equiv 1 \bmod (2^n-1)$.

Lemma 5 in particular implies that H will never possess the worst case differential uniformity 2^m, as long as Condition (a) is satisfied. As seen in Corollary 1, the worst case differential uniformity 2^m occurs frequently for $r = 0$ and $G(x) =$

$\mathrm{Tr}_{\mathrm{m}}^{\mathrm{n}}(\sigma x^{2^i+1})$, by Remark 2 in any case whenever m is even. Applying the following lemma on the number of solutions of certain linearized polynomials, for many combinations of $r > 0$ and i we can infer upper bounds for the smallest k for which H is differentially k-uniform.

Lemma 6. *Let r be an integer with $\gcd(r,m) = 1$ and l be a linearized polynomial of the form*

$$l(x) = C_0x + C_1x^{2^r} + C_2x^{2^{2r}} + \cdots + C_dx^{2^{dr}} \in \mathbb{F}_{2^m}[x] \quad (12)$$

of degree 2^{dr}. Then l has at most 2^d solutions in $\mathbb{F}_{2^m}$.

For the proof we refer to [19].

Theorem 4. *Let r be an integer with $\gcd(r,m) = 1$, $i = dr$, $\gcd(d,m) = 1$, let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, and in the case of $i = r$, let $\gamma^{-1} \notin U_1^{2^r-1}$. Then*

$$H(x) = \left(\mathrm{Tr}_m^n\left(\gamma x^{2^r}(x + x^{2^m})\right), \mathrm{Tr}_m^n\left(\sigma x^{2^i+1}\right)\right)$$

is differentially 2^{d+1}-uniform if and only if $\sigma, \sigma\gamma^{-(2^i+1)2^{-r}} \notin \mathbb{F}_{2^m}$. In particular if $i = r$, then H is differentially 4-uniform.

Proof: By assumption, Condition (a) in Corollary 3 is satisfied. By Lemma 5, the linearized polynomial in (8) in Condition (b) does not vanish. Observe that with $i = dr$, the linearized polynomial in (8) is of the form (12) and of degree $2^{(d+1)r}$. The claim follows then from Lemma 6. □

Remark 4. *The condition $\gcd(d,m) = 1$, i.e., $\gcd(i,m) = 1$, is required to guarantee that the polynomial in (8) does not vanish (see Lemma 5). However, $\gcd(i,m) = 1$ is not necessary for the polynomial in (8) not to vanish. Theorem 4 is hence also applicable more general for arbitrary i under the assumption that the polynomial in (8) does not vanish.*

As we can see, for $i = r$, the function H is differentially 4-uniform for most choices of $\gamma, \sigma \in \mathbb{F}_{2^n}$. With such a choice one can in fact obtain differentially 4-uniform functions of the same shape for infinitely many extensions of $\mathbb{F}_{2^n}$.

Corollary 4. *Let $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ such that $\gamma^{-1} \notin U_1^{2^r-1}$. For some r with $\gcd(r,m) = 1$, let*

$$H(x) = \left(\mathrm{Tr}_m^n\left(\gamma x^{2^r}(x + x^{2^m})\right), \mathrm{Tr}_m^n\left(\sigma x^{2^r+1}\right)\right)$$

be differentially 4-uniform. Then for any positive odd integer s with $\gcd(s,r) = 1$,

$$H_s(x) = \left(\mathrm{Tr}_{ms}^{ns}\left(\gamma x^{2^r}(x + x^{2^{ms}})\right), \mathrm{Tr}_{ms}^{ns}\left(\sigma x^{2^r+1}\right)\right)$$

is also differentially 4-uniform. If H is differentially 4-uniform but not APN, so is H_s.

Proof: By Theorem 4, we first have to show that $\gamma, \sigma, \sigma\gamma^{-(2^r+1)2^{-r}} \notin \mathbb{F}_{2^{ms}}$. If $\gamma \in \mathbb{F}_{2^{ms}}$, then $\gamma \in \mathbb{F}_{2^n} \cap \mathbb{F}_{2^{ms}} = \mathbb{F}_{2^m}$, which gives a contradiction. Similarly, σ and $\sigma\gamma^{-(2^r+1)2^{-r}}$ can not lie in $\mathbb{F}_{2^{ms}}$. Hence H_s is differentially 4-uniform. Note that

$$U_1 \subseteq \{\, x \in \mathbb{F}_{2^{ns}} \,|\, x + \gamma x^{2^r} \in \mathbb{F}_{2^{ms}} \} =: U_1^{(s)},$$

and the map ψ given in Equation (7) is an isomorphism from $\mathbb{F}_{2^{ms}}$ to $U_1^{(s)}$. If H is not APN, then there exists $a \in \mathbb{F}_{2^m} \subseteq \mathbb{F}_{2^{ms}}$ such that the polynomial in (8) has exactly 4 zeros in $\mathbb{F}_{2^m}$. Since $\mathrm{Tr}_{ms}^{ns}(\alpha) = \mathrm{Tr}_m^n(\alpha)$ for each $\alpha \in \mathbb{F}_{2^n}$, we conclude that $H_s(x+\psi(a)) + H_s(x) + H_s(\psi(a)) = 0$ has also exactly 4 solutions. □

We finish this section with results on the nonlinearity. Recall that an APN-function that has only bent and semibent components is commonly called an APN-function with classical spectrum. Several of the known (quadratic) differentially 4-uniform functions have the same property, i.e., all component functions are bent or semibent.

Remark 5. *By Proposition 22 in [3], for every differentially 4-uniform function F in even dimension n, which only has bent and semibent component functions, the number of bent components is determined by the number of 4's in the differential spectrum. In particular, if F is APN, then F has $2(2^n-1)/3$ bent and $(2^n-1)/3$ semibent components. If on the other hand F has only 0 and 4 in the differential spectrum, then all component functions are semibent.*

In the light of Remark 5, we use the term "functions with classical spectrum" more general also for differentially 4-uniform functions with only bent and semibent components.

We will use that a quadratic Boolean function $f : \mathbb{V}_n \to \mathbb{F}_2$ is always s-plateaued for some integer s with $n+s$ even. The integer s is the dimension of the *linear space* of f defined as $\Lambda_f = \{a \in \mathbb{V}_n \,:\, f(x) + f(x+a) \text{ is constant}\}$. For the proof of Theorem 5 we will use Proposition 2.4 in [1], which is a generalization of Lemma 6 above:

Lemma 7. *Let r be an integer with $\gcd(r,m) = 1$ and let $f_1(X,Y)$, $f_2(X,Y)$ be linearized polynomials of the form*

$$C_0X + D_0Y + C_1X^{2^r} + D_1Y^{2^r} + \cdots + C_dX^{2^{dr}} + D_dY^{2^{dr}}$$

$\in \mathbb{F}_{2^m}[X,Y]$, of degree 2^{d_1r} and 2^{d_2r}, respectively. If f_1 and f_2 do not have a common factor, then

$$|\{(x,y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \,:\, f_1(x,y) = f_2(x,y) = 0\}| \le 2^{d_1+d_2}.$$

In the following theorem, besides from $i = r$, which guarantees that H is differentially 4-uniform, we suppose that m is odd, and γ and σ are in different multiplicative cosets of $\mathbb{F}_{2^m}$. We will use in the proof that there exists an element $\rho \in \mathbb{F}_{2^n}$ such that $\sigma\rho \in \mathbb{F}_{2^m}$ and $\gamma\rho \notin \mathbb{F}_{2^m}$ if and only if $\sigma\gamma^{-1} \notin \mathbb{F}_{2^m}$.

Theorem 5. *Let $\gamma, \sigma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, where $n = 2m$, m odd, and suppose that $\sigma\gamma^{-1} \notin \mathbb{F}_{2^m}$ and $\gamma^{2^r}\sigma^{-(2^r-1)} \notin \mathbb{F}_{2^m}$. Then for an integer r relatively prime to m,*

$$H(x) = \left(\mathrm{Tr}_m^n\left(\gamma x^{2^r}(x + x^{2^m})\right), \mathrm{Tr}_m^n\left(\sigma x^{2^r+1}\right)\right)$$

has the classical spectrum.

Proof: For $(\eta,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, let

$$H_{\eta,\mu}(x) = \mathrm{Tr}_1^m\left(\eta\mathrm{Tr}_m^n\left(\gamma x^{2^r}(x + x^{2^m})\right) + \mu\mathrm{Tr}_m^n\left(\sigma x^{2^r+1}\right)\right)$$

be the component function of H corresponding to (η,μ).

If $\mu = 0$, then $H_{\eta,\mu}(x) = \mathrm{Tr}_1^n(\eta\gamma x^{2^r}(x + x^{2^m}))$, which is bent since $\eta\gamma \notin \mathbb{F}_{2^m}$.

If $\eta = 0$, then $H_{\eta,\mu}$ reduces to the Gold function $H_{\eta,\mu}(x) =$

$\mathrm{Tr}_1^n(\mu\sigma x^{2^r+1})$. With the standard calculations for the Gold function, with $\gcd(m,r)=1$, we see that $H_{\eta,\mu}$ is bent if $\mu\sigma$ is not a (2^r+1)th power in $\mathbb{F}_{2^n}$, and otherwise $H_{\eta,\mu}$ is semibent. Hence we can assume that $\eta\mu \neq 0$.

Let $\zeta \in \mathbb{F}_{2^n}$ such that $\sigma\zeta^{2^r} \in \mathbb{F}_{2^m}$ and $\gamma\zeta^{2^r} \notin \mathbb{F}_{2^m}$. As $\sigma\zeta^{2^r} \in \mathbb{F}_{2^m}$ implies that $\zeta \notin \mathbb{F}_{2^m}$, we have $\mathbb{F}_{2^n} = \mathbb{F}_{2^m}(\zeta)$, say $\zeta + \zeta^{2^m} = \alpha$ for some nonzero $\alpha \in \mathbb{F}_{2^m}$. We can uniquely write $x = X + \zeta Y$ for some $X, Y \in \mathbb{F}_{2^m}$. Then we have

$$x + x^{2^m} = X + \zeta Y + (X+\zeta Y)^{2^m} = (\zeta + \zeta^{2^m})Y = \alpha Y.$$

Define

$$\begin{aligned} F(X,Y) := F(X+\zeta Y) &= \mathrm{Tr}_m^n\left(\gamma\alpha(X^{2^r} + \zeta^{2^r}Y^{2^r})Y\right) \\ G(X,Y) := G(X+\zeta Y) &= \mathrm{Tr}_m^n\left(\sigma(X+\zeta Y)^{2^r+1}\right) \\ &= \mathrm{Tr}_m^n\Big(\sigma(X^{2^r+1} + \zeta Y X^{2^r} \\ &\qquad + \zeta^{2^r}Y^{2^r}X + \zeta^{2^r+1}Y^{2^r+1})\Big). \end{aligned}$$

For $(\eta,\mu) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$, we denote by $H_{\eta,\mu}$ the component function of H corresponding to (η,μ). That is,

$$H_{\eta,\mu}(X,Y) = \mathrm{Tr}_1^m\left(\eta F(X,Y) + \mu G(X,Y)\right).$$

To determine the nonlinearity, we have to determine the linear space $\Lambda_{\eta,\mu}$ of $H_{\eta,\mu}$. Recall that $\Lambda_{\eta,\mu}$ consists of the elements $(u,v) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ such that

$$H_{\eta,\mu}(X+u, Y+v) + H_{\eta,\mu}(X,Y) + H_{\eta,\mu}(u,v) = 0 \quad (13)$$

for all $(X,Y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$. Equation (13) holds for all (X,Y) if and only if

$$\begin{aligned} &\mathrm{Tr}_1^n\Big(\eta\gamma\alpha(vX^{2^r} + u^{2^r}Y + \zeta^{2^r}vY^{2^r} + \zeta^{2^r}v^{2^r}Y) \\ &+ \mu\sigma(uX^{2^r} + u^{2^r}X + \zeta vX^{2^r} + \zeta u^{2^r}Y + \zeta^{2^r}v^{2^r}X + \zeta^{2^r}uY^{2^r} \\ &+ \zeta^{2^r+1}vY^{2^r} + \zeta^{2^r+1}v^{2^r}Y)\Big) = 0 \qquad (14) \end{aligned}$$

for all (X,Y). Note that we used the facts that $\eta,\mu \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_1^n(x) = \mathrm{Tr}_1^m(\mathrm{Tr}_m^n(x))$ to obtain Equation (14). By setting $\tilde{\eta} := \eta\gamma\alpha$ and $\tilde{\mu} := \mu\sigma$, we observe that Equation (14) is equivalent to

$$\begin{aligned} &\mathrm{Tr}_1^n\Big((\tilde{\eta}v + \tilde{\mu}u + \tilde{\mu}\zeta v)X^{2^r} + (\tilde{\mu}u^{2^r} + \tilde{\mu}\zeta^{2^r}v^{2^r})X\Big) \\ &+ \mathrm{Tr}_1^n\Big((\tilde{\eta}\zeta^{2^r}v + \tilde{\mu}\zeta^{2^r}u + \tilde{\mu}\zeta^{2^r+1}v)Y^{2^r} \\ &+ (\tilde{\eta}u^{2^r} + \tilde{\eta}\zeta^{2^r}v^{2^r} + \tilde{\mu}\zeta u^{2^r} + \tilde{\mu}\zeta^{2^r+1}v^{2^r})Y\Big) = 0 \end{aligned}$$

for all (X,Y), which applies if and only if

$$\mathrm{Tr}_1^m\Big(\mathrm{Tr}_m^n(\tilde{\eta}v + \tilde{\mu}u + \tilde{\mu}\zeta v + (\tilde{\mu}u^{2^r} + \tilde{\mu}\zeta^{2^r}v^{2^r})^{2^r})X^{2^r}\Big) = 0,$$

and

$$\begin{aligned} &\mathrm{Tr}_1^m\Big(\mathrm{Tr}_m^n(\tilde{\eta}\zeta^{2^r}v + \tilde{\mu}\zeta^{2^r}u + \tilde{\mu}\zeta^{2^r+1}v + (\tilde{\eta}u^{2^r} + \tilde{\eta}\zeta^{2^r}v^{2^r} \\ &+ \tilde{\mu}\zeta u^{2^r} + \tilde{\mu}\zeta^{2^r+1}v^{2^r})^{2^r})Y^{2^r}\Big) = 0 \end{aligned}$$

for all (X,Y). This holds if and only if

$$\begin{aligned} &\mathrm{Tr}_m^n\left(\tilde{\eta}v + \tilde{\mu}u + \tilde{\mu}\zeta v + (\tilde{\mu}u^{2^r} + \tilde{\mu}\zeta^{2^r}v^{2^r})^{2^r}\right) = 0, \quad \text{and} \\ &\mathrm{Tr}_m^n\Big(\tilde{\eta}\zeta^{2^r}v + \tilde{\mu}\zeta^{2^r}u + \tilde{\mu}\zeta^{2^r+1}v + (\tilde{\eta}u^{2^r} + \tilde{\eta}\zeta^{2^r}v^{2^r} \\ &+ \tilde{\mu}\zeta u^{2^r} + \tilde{\mu}\zeta^{2^r+1}v^{2^r})^{2^r}\Big) = 0. \end{aligned}$$

Therefore, $(u,v) \in \Lambda_{\eta,\mu}$ if and only if (u,v) is a zero of the polynomials

$$\begin{aligned} &\mathrm{Tr}_m^n(\tilde{\eta} + \tilde{\mu}\zeta)V + \mathrm{Tr}_m^n(\tilde{\mu})U + \mathrm{Tr}_m^n(\tilde{\mu}^{2^r})U^{2^{2r}} \\ &+ \mathrm{Tr}_m^n(\tilde{\mu}^{2^r}\zeta^{2^{2r}})V^{2^{2r}}, \text{and} \\ &\mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})V + \mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r})U + \mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)^{2^r})U^{2^{2r}} \\ &+ \mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)^{2^r}\zeta^{2^{2r}})V^{2^{2r}}. \end{aligned}$$

Recall that $\tilde{\eta} \in \gamma\mathbb{F}_{2^m}$ and $\tilde{\mu} \in \sigma\mathbb{F}_{2^m}$. Since $\sigma\zeta^{2^r} \in \mathbb{F}_{2^m}$ and $\gamma\zeta^{2^r} \notin \mathbb{F}_{2^m}$, we have $\mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r}) = 0$ and $\mathrm{Tr}_m^n(\tilde{\eta}\zeta^{2^r}) \neq 0$. Note that since $\mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r}) = 0$ we can not have $\mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r+1}) = 0$ or $\mathrm{Tr}_m^n(\tilde{\mu}^{2^r}\zeta^{2^{2r}+2^r}) = 0$, otherwise we would have $\zeta \in \mathbb{F}_{2^m}$ since $\gcd(r,m) = 1$. Note that $\mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r}) = \mathrm{Tr}_m^n(\tilde{\mu}^{2^r}\zeta^{2^r}) = 0$ holds if and only if $\tilde{\mu}\zeta^{2^r}, \tilde{\mu}^{2^r}\zeta^{2^r} \in \mathbb{F}_{2^m}$. Equivalently, this holds if and only if $\tilde{\mu}^{2^r}\zeta^{2^{2r}}, \tilde{\mu}^{2^r}\zeta^{2^r} \in \mathbb{F}_{2^m}$. This implies that $\zeta^{2^r(2^r-1)} \in \mathbb{F}_{2^m}$. Then this is equivalent to $\zeta \in \mathbb{F}_{2^m}$ as $\gcd(r,m) = 1$, which is a contradiction. Hence, we conclude that $\mathrm{Tr}_m^n(\tilde{\mu}^{2^r}\zeta^{2^r}) \neq 0$ if $\mathrm{Tr}_m^n(\tilde{\mu}\zeta^{2^r}) = 0$.

With $\eta, \mu \neq 0$ we have $\tilde{\eta}, \tilde{\mu} \neq 0$. Moreover, note that then $\tilde{\eta}, \tilde{\mu} \notin \mathbb{F}_{2^m}$, and hence, $\mathrm{Tr}_m^n(\tilde{\eta})\mathrm{Tr}_m^n(\tilde{\mu}) \neq 0$. Consequently,

$$\begin{aligned} L_1(U,V) &= \mathrm{Tr}_m^n(\tilde{\eta} + \tilde{\mu}\zeta)V + \mathrm{Tr}_m^n(\tilde{\mu})U + \mathrm{Tr}_m^n(\tilde{\mu})^{2^r}U^{2^{2r}} \\ &= 0, \quad \text{and} \\ L_2(U,V) &= \mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})V + \mathrm{Tr}_m^n(\tilde{\eta} + \tilde{\mu}\zeta)^{2^r}U^{2^{2r}} \\ &\qquad + \mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})^{2^r}V^{2^{2r}} = 0. \end{aligned}$$

(a) Suppose that $\tilde{\eta} + \tilde{\mu}\zeta \in \mathbb{F}_{2^m}$. Now we show that $\tilde{\eta} + \tilde{\mu}\zeta \neq 0$. Suppose $\tilde{\eta} + \tilde{\mu}\zeta = 0$. This implies that $\gamma(\sigma\zeta)^{-1} \in \mathbb{F}_{2^m}$, i.e., $\gamma^{2^r}(\sigma\zeta)^{-2^r} = \gamma^{2^r}\sigma^{-(2^r-1)}(\sigma\zeta^{2^r})^{-1} \in \mathbb{F}_{2^m}$. Since $\sigma\zeta^{2^r} \in \mathbb{F}_{2^m}$, this implies that $\gamma^{2^r}\sigma^{-(2^r-1)} \in \mathbb{F}_{2^m}$, which is a contradiction. Then we have $(\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r} \notin \mathbb{F}_{2^m}$ and

$$\begin{aligned} &\mathrm{Tr}_m^n(\tilde{\mu})U + \mathrm{Tr}_m^n(\tilde{\mu})^{2^r}U^{2^{2r}} = 0, \quad \text{and} \\ &\mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})V + \mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})^{2^r}V^{2^{2r}} = 0. \end{aligned}$$

Note that there are at most 2 solutions for U and for V since $\gcd(2r,m) = 1$ by Lemma 6. This shows that the number of solutions is at most 4. Therefore, the corresponding component function is either bent or semibent.

(b) Suppose that $\tilde{\eta} + \tilde{\mu}\zeta \notin \mathbb{F}_{2^m}$, i.e., $\mathrm{Tr}_m^n(\tilde{\eta} + \tilde{\mu}\zeta) \neq 0$. If $(\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r} \in \mathbb{F}_{2^m}$, then $L_1(U,V) = L_2(U,V) = 0$ if and only if $(U,V) = (0,0)$. That is, the corresponding component function is bent. Therefore, we can suppose that $\tilde{\eta} + \tilde{\mu}\zeta, (\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r} \notin \mathbb{F}_{2^m}$. Let $\mathcal{X}_1$ and $\mathcal{X}_2$ be two curves defined by L_1 and L_2, respectively. Then $\mathcal{X}_1$ and $\mathcal{X}_2$ have unique points at infinity, namely $(0:1:0)$ and $(1:\alpha:0)$, respectively, where $\alpha^{2^r} = \mathrm{Tr}_m^n(\tilde{\eta} + \tilde{\mu}\zeta)/\mathrm{Tr}_m^n((\tilde{\eta} + \tilde{\mu}\zeta)\zeta^{2^r})$. That is, they have distinct points at infinity; and hence, they do not have any common component. Therefore, L_1 and L_2 do not have a common factor. Then by Lemma 7, we conclude that the system has at most 4 solutions as $\gcd(2r,m) = 1$. That is, the corresponding component function is either bent or semibent. □

For the case $i = r$ and m odd, we can now summarize the nonlinearity and differential uniformity results as follows:

Theorem 6. *Let* $\gamma, \sigma \in \mathbb{F}_{2^n}$, *where* $n = 2m$ *for an odd integer* m, *and* r *be a positive integer relatively prime to* m. *If* $\gamma, \sigma, \sigma\gamma^{-(2^r+1)2^r}, \sigma\gamma^{-1}, \gamma^{2^r}\sigma^{-(2^r-1)} \notin \mathbb{F}_{2^m}$ *and* $\gamma^{-1} \notin U_1^{2^r-1}$, *then*

$$H(x) = \left(\mathrm{Tr}_m^n\left(\gamma x^{2^r}(x + x^{2^m})\right), \mathrm{Tr}_m^n\left(\sigma x^{2^r+1}\right)\right)$$

is differentially 4*-uniform and has the classical spectrum.*

We finally remark that using Lemma 7 which depends on Bezout's theorem is also capable to deduce similar results for functions H using the binomial $G(x) = \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma x^{2^i+1} + \tau x^{2^{m+i}+1})$, $\tau \neq 0$, instead of the monomial. For instance with the same method one can show the following theorem, which we state without giving the details of the proof.

Theorem 7. *Let* $\gcd(r, m) = 1$, $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$, $\tau \in \mathbb{F}_{2^m}^*$ *such that* $\tau^{-1} \neq \mathrm{Tr}_m^n(\gamma^{-1})$, *and* $\sigma = \gamma + \tau$. *Then* $H(x) = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)), \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma x^{2^r+1} + \tau x^{2^{m+r}+1}))$ *is differentially* $2^{2\gcd(m,2)}$*-uniform, and any component function of* H *is at most* $2\gcd(2, m)$*-plateaued. In particular, if* m *is odd, then* $H(x)$ *is differentially* 4*-uniform and has the classical spectrum.*

IV. Computational results and perspectives

In this section we first add some computational results obtained by MAGMA. We then conclude the paper with some questions and remarks.

APN-functions of the form $\mathbf{H(x)} = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma\mathbf{x}^{\mathbf{2^r}}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\mathbf{x})), \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma\mathbf{x}^{\mathbf{2^i+1}} + \tau\mathbf{x}^{\mathbf{2^{m+i}+1}}))$**:**

For $n = 6$, for both, $r = 0$ and $r = 1$, there are 2352 combinations of σ and τ that give APN-functions H (for γ w.l.o.g. we chose a primitive element of $\mathbb{F}_{2^6}$). As also the form of G indicates, for $r = 0$, all APN-functions belong to the class introduced in Carlet [5], the bivariate form of the construction in [6]. The Γ-rank of all these APN-functions is 1146, which confirms this observation. All APN-functions for $r = 1$ have Γ-rank 1166 and Δ-rank 96, the same as the function in Taniguchi [18], hence they belong to the same class. (For the definitions of the Γ-rank and of the Δ-rank, and for the Γ-rank and the Δ-rank for all classes of quadratic APN-functions in dimension 6 we refer to [10].)

For $r = 0$, as one expects, many combinations of σ, τ yield APN-functions also for larger n, belonging to the infinite class of APN-functions in [5]. The number seems smaller for $r \neq 0$. However until $n = 30$ we confirmed the existence of APN-functions H for some $r > 0$ (our calculations use $r = 1, 2$).

Differential uniformity for $\mathbf{H(x)} = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma\mathbf{x}^{\mathbf{2^r}}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\mathbf{x})), \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma\mathbf{x}^{\mathbf{2^i+1}}))$**:**

Though, at least in small dimension, many of these functions with $i \neq r$ are also differentially 4-uniform, we confirmed that for $i = dr$, $d \neq 1$, there are functions H that are only differentially 2^{d+1}-uniform, hence by Theorem 4 they take on the largest possible value. For instance, for $m = 4$, $r = 1$, $i = 2$ (Remark 4 then applies), there are combinations of γ, σ (satisfying the conditions in Theorem 4), for which H is differentially 8-uniform.

Nonlinearity for $\mathbf{H(x)} = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma\mathbf{x}^{\mathbf{2^r}}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\mathbf{x})), \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma\mathbf{x}^{\mathbf{2^r}}))$**:**

By Theorem 5, H has only bent and semibent components when m is odd (and $\sigma\gamma^{-1} \notin \mathbb{F}_{2^m}$ and $\gamma^{2^r}\sigma^{-(2^r-1)} \notin \mathbb{F}_{2^m}$). For even m we observe that many of the functions which by Theorem 4 are differentially 4-uniform, have bent semibent and 4-plateaued components.

Our analysis of the properties of $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$ in connection with being a component of an (n, n)-functions for arbitrary linearized permutations Λ, may help to find further interesting results on classes of (n, n)-functions. Recall also that the function G to be combined with $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$ is chosen in order to satisfy the condition $G(c\alpha) = K(c)G(\alpha)$ for all $c \in \mathbb{F}_{2^m}^*$ and $\alpha \in \mathbb{F}_{2^n}$ in Corollary 2. One may attempt to investigate combinations with other choices for G, perhaps satisfying a similar condition.

It would certainly be interesting to find further infinite classes of APN-functions. As mentioned above, computationally we found APN-functions of the form $H(x) = (\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(x)), \mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\sigma x^{2^i+1} + \tau x^{2^{m+i}+1}))$ and $r > 0$ for all $n \leq 30$. In this connection we remark that a plateaued APN-function in even dimension n with a nonclassical spectrum must have even more than $2(2^n - 1)/3$ bent component functions. Starting with vectorial bent functions which allow nontrivial extensions to (n, n)-functions with a large number of bent components, may be a promising strategy to obtain such APN-functions.

The function $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$ is the most obvious vectorial bent function contained in the function $x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x))$ on $\mathbb{F}_{2^n}$ with $2^n - 2^m$ bent component functions. But there are other ones, some of which may not even be Maiorana-McFarland bent functions, see also Question 1 in [15]. A similar analysis for those functions would certainly be more difficult, but being obtained from that special class of (n, n)-functions with the maximal number of bent components, some of them may share interesting properties. A general question in this direction is to characterize the quadratic bent functions F for which the collection of the solutions spaces for $\mathcal{D}_aF(x) = 0$, $a \in \mathbb{F}_{2^n}^*$ forms a spread of $\mathbb{F}_{2^n}$.

As we saw, the spread for $\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\gamma x^{2^r}\mathrm{Tr}^{\mathrm{n}}_{\mathrm{m}}(\Lambda(x)))$ reduces to the Desarguesian spread in standard representation if $r = 0$ and $\Lambda(x) = x$. To describe properties of the spreads in general, and the relation between the spreads when r or Λ varies, seems an interesting problem. Whether all our considered spreads are Desarguesian spreads seems not to have an obvious answer.

Acknowledgement

We thank our editor and the reviewers for the efforts and the professional work. We are grateful to our reviewers for their very comprehensive and constructive detailed reviews. The extensive suggestions, pointing out deficiencies and pointing to further interesting closely related questions, some of which we added in the last section on perspectives, greatly helped to improve the article.

REFERENCES

[1] N. Anbar, T. Kalaycı, and W. Meidl, "Determining the Walsh spectra of Taniguchi's and related APN-functions," *Finite Fields Appl.,* vol. 60, 101577, 20 pp., Nov. 2019.

[2] C. Beierle and G. Leander, "New instances of quadratic APN functions," 2020, *arXiv:2009.07204*. [Online]. Available: https://arxiv.org/abs/2009.07204

[3] A. Canteaut, S. Duval, and L. Perrin, "A generalisation of Dillon's APN permutation with the best known differential and nonlinear properties for all fields of size 2^{4k+2}," *IEEE Trans. Inf. Theory,* vol. 63, no. 11, pp. 7575–7591, Nov. 2017.

[4] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Models and Methods in Mathematics, Computer Science, and Engineering,* Y. Crama and P. L. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 257–397.

[5] C. Carlet, "Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions," *Des., Codes Cryptogr.,* vol. 59, nos. 1-3, pp. 89-109, Apr. 2011.

[6] C. Carlet, "More constructions of APN and differentially 4-uniform functions by concatenation," *Sci. China Math.,* vol. 56, no. 7, pp. 1373-1384, July 2013.

[7] C. Carlet, "Characterizations of the differential uniformity of vectorial functions by the Walsh transform," *IEEE Trans. Inf. Theory,* vol. 64, no. 9, pp. 6443-6453, Sept. 2018.

[8] S. Chee, S. Lee, and K. Kim, "Semi-bent functions," in *Advances in Cryptology—ASIACRYPT,* Lecture Notes in Computer Science, vol. 917, J. Pieprzyk and R. Safavi-Naini, Eds. Berlin, Germany: Springer-Verlag, 1994, pp. 107-118.

[9] J. F. Dillon, "Elementary Hadamard difference sets," Ph.D. dissertation, Univ. Maryland, College Park, MD, USA, 1974.

[10] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," *Adv. Math. Commun.,* vol. 3, no. 1, pp. 59-81, Feb. 2009.

[11] Y. Edel, "Quadratic APN functions as subspaces of alternating bilinear forms," in *Proc. of the Contact Forum Coding Theory and Cryptogr. III*, Belgium, 2011, pp. 11-24.

[12] S. Mesnager, F. Zhang, C. Tang, and Y. Zhou, "Further study on the maximum number of bent components of vectorial functions," *Des., Codes Cryptogr.,* vol. 87, no. 11, pp. 2597-2610, Nov. 2019.

[13] K. Nyberg, "Perfect nonlinear S-boxes," in *Advances in Cryptology—EUROCRYPT,* Lecture Notes in Computer Science, vol. 547, D. W. Davies, Ed. Berlin, Germany: Springer, 1991. pp. 378–386.

[14] K. Nyberg, "Differentially uniform mappings for cryptography," in *Advances in Cryptology—EUROCRYPT*, Lecture Notes in Computer Science, vol. 765, T. Helleseth, Ed. Berlin, Germany: Springer, 1993, pp. 55–64.

[15] A. Pott, E. Pasalic, A. Muratović-Ribić, and S. Bajrić, "On the maximum number of bent components of vectorial functions," *IEEE Trans. Inf. Theory,* vol. 64, no. 1, pp. 403-411, Jan. 2018.

[16] O. Rothaus, "On "bent" functions," *J. Combinatorial Theory Ser. A,* vol. 20, no. 3, pp. 300-305, May 1976.

[17] K.-U. Schmidt. (Sep. 2017). Codes in classical association schemes. Presented at Finite Geometries 5th Irsee Conference. [Online]. Available: http://cage.ugent.be/~ml/irsee5/slides/Schmidt.pdf

[18] H. Taniguchi, "On some quadratic APN functions," *Des., Codes Cryptogr.,* vol. 87, no. 9, pp. 1973-1983, Sep. 2019.

[19] H. M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences," Ph.D. dissertation, Univ. Southern California, Los Angeles, CA, USA, 1970.

[20] L. Zheng, J. Peng, H. Kan, Y. Li, and J. Luo, "On constructions and properties of (n,m)-functions with maximal number of bent components," *Des., Codes Cryptogr.,* vol. 88, no. 10, pp. 2171–2186, Oct. 2020.

[21] Y. Zheng and X. Zhang, "On plateaued functions," *IEEE Trans. Inf. Theory,* vol. 47, no. 3, pp. 1215-1223, Mar. 2001.

[22] Y. Zhou and A. Pott, "A new family of semifields with 2 parameters," *Adv. Math,* vol. 234, pp. 43-60, Feb. 2013.

Nurdagül Anbar earned her B.S degree in Mathematics at Middle East Technical University (METU), Ankara, Turkey in 2007. Then she earned her Master's degree on the subject "Ramification in extensions of rational function fields" and Ph.D. degree on the subject "Algebraic curves in prime characteristic" with Prof. Henning Stichtenoth at Sabancı University. During her Ph.D. (March 2011-February 2012), she visited the University of Perugia in Italy. After obtaining her Ph.D., she worked as a post-doctoral researcher at Sabancı University (July 2012-February 2014), Max Planck Institute for Mathematics (March 2014-May 2014) in Bonn, Germany, the Technical University of Denmark (November 2014-September 2016) in Lyngby, Denmark, Otto-von-Guericke-Universitat (October 2016-March 2017) in Magdeburg, Germany, RICAM (May 2017-January 2018) and Johannes Kepler University (February 2018-Au-gust 2018) in Linz, Austria. Since September 2018, she works as a faculty member in the Faculty of Engineering and Natural Sciences at Sabancı University.

Tekgül Kalaycı received her B.S. degree in Mathematics from Dokuz Eylül University, İzmir, in 2011. She finished her M.S. in Mathematics at İzmir Instıtute of Technology, İzmir, in 2014. She pursued her Ph.D. studies at Sabancı University, İstanbul, under the supervision of Prof. Alev Topuzoğlu and received her degree in 2019. Currently, she has a postdoctoral postition at Sabancı University. Her research interests include permutation polynomials, factorization of polynomials, Boolean functions, bent functions, coding theory, finite fields and their applications.

Wilfried Meidl received the Ph.D. degree from Klagenfurt University, Austria, in 1998. From 2000 to 2002 he was with the Institute of Discrete Mathematics, OEAW, Vienna, Austria. From 2002–2004 he was with Temasek Labs, National University of Singapore, and from 2005–2014 he was with Sabancı University, Istanbul, Turkey. He is now with RICAM, OEAW, Linz, Austria. His research interests include sequences, permutation polynomials, finite fields and their applications, Boolean functions, bent functions.