

Further study on the maximum number of bent components of vectorial functions

Sihem Mesnager¹, Fengrong Zhang², Chunming Tang³, Yong Zhou²

1. LAGA, Department of Mathematics, University of Paris VIII
(and Paris XIII and CNRS), Saint-Denis cedex 02, France.

E-mail: smesnager@univ-paris8.fr

2. School of Computer Science and Technology, China University
of Mining and Technology, Xuzhou, Jiangsu 221116, China.

E-mail: {zhf1203,yzhou}@cumt.edu.cn

3. School of Mathematics and Information, China West Normal University, Nanchong, Sichuan
637002, China.

E-mail: tangchunmingmath@163.com

Abstract. In 2018, Pott, et al. have studied in [IEEE Transactions on Information Theory. Volume: 64, Issue: 1, 2018] the maximum number of bent components of vectorial function. They have presented several nice results and suggested several open problems in this context. This paper is in the continuation of their study in which we solve two open problems raised by Pott et al. and partially solve an open problem raised by the same authors. Firstly, we prove that for a vectorial function, the property of having the maximum number of bent components is invariant under the so-called CCZ equivalence. Secondly, we prove the non-existence of APN plateaued having the maximum number of bent components. In particular, quadratic APN functions cannot have the maximum number of bent components. Finally, we present some sufficient conditions that the vectorial function defined from $\mathbb{F}_{2^{2k}}$ to $\mathbb{F}_{2^{2k}}$ by its univariate representation:

$$\alpha x^{2^i} \left(x + x^{2^k} + \sum_{j=1}^{\rho} \gamma^{(j)} x^{2^{t_j}} + \sum_{j=1}^{\rho} \gamma^{(j)} x^{2^{t_j+k}} \right)$$

has the maximum number of components bent functions, where $\rho \leq k$. Further, we show that the differential spectrum of the function $x^{2^i} (x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})$ (where i, t_1, t_2 satisfy some conditions) is different from the binomial function $F^i(x) = x^{2^i} (x + x^{2^k})$ presented in the article of Pott et al.

Finally, we provide sufficient and necessary conditions so that the functions

$$Tr_1^{2k} \left(\alpha x^{2^i} \left(Tr_e^{2k}(x) + \sum_{j=1}^{\rho} \gamma^{(j)} (Tr_e^{2k}(x))^{2^j} \right) \right)$$

are bent.

Keywords: Vectorial functions, Boolean functions, Bent functions, Nonlinearity, APN functions, Plateaued functions, CCZ equivalence.

1 Introduction

Vectorial (multi-output) Boolean functions, that is, functions from the vector space \mathbb{F}_2^n (of all binary vectors of length n) to the vector space \mathbb{F}_2^m , for given positive integers n and m . These functions are called (n, m) -functions and include the (single-output) Boolean functions (which correspond to the case $m = 1$). In symmetric cryptography, multi-output functions are called *S-boxes*. They are fundamental parts of block ciphers. Being the only source of nonlinearity in these ciphers, S-boxes play a central role in their robustness, by providing confusion (a requirement already mentioned by C. Shannon), which is necessary to withstand known (and hopefully future) attacks. When they are used as S-boxes in block ciphers, their number m of output bits equals or approximately equals the number n of input bits. They can also be used in stream ciphers, with m significantly smaller than n , in the place of Boolean functions to speed up the ciphers.

We shall identify \mathbb{F}_2^n with the Galois field \mathbb{F}_{2^n} of order 2^n but we shall always use \mathbb{F}_2^n when the field structure will not really be used. The *component functions* of F are the Boolean functions $v \cdot F$, that is, $x \in \mathbb{F}_{2^n} \mapsto \text{Tr}_1^m(vF(x))$, where “ \cdot ” stands for an inner product in \mathbb{F}_{2^m} (for instance: $u \cdot v := \text{Tr}_1^m(uv)$, $\forall u \in \mathbb{F}_{2^m}, v \in \mathbb{F}_{2^m}$ where “ Tr_1^m ” denotes the absolute trace over \mathbb{F}_{2^m}). In order to classify vectorial Boolean functions that satisfy desirable nonlinearity conditions, or to determine whether, once found, they are essentially new (that is, inequivalent in some sense to any of the functions already found) we use some concepts of equivalence. For vectorial Boolean functions, there exist essentially two kinds concepts of equivalence: the extended affine EA-equivalence and the CCZ-equivalence (Carlet-Charpin-Zinoviev equivalence). Two (n, r) -functions F and F' are said to be EA-equivalent if there exist affine automorphisms L from \mathbb{F}_{2^n} to \mathbb{F}_{2^n} and L' from \mathbb{F}_{2^r} to \mathbb{F}_{2^r} and an affine function L'' from \mathbb{F}_{2^n} to \mathbb{F}_{2^r} such that $F' = L' \circ F \circ L + L''$. EA-equivalence is a particular case of CCZ-equivalence [4]. Two (n, r) -functions F and F' are said to be CCZ-equivalent if their graphs $G_F := \{(x, F(x)), x \in \mathbb{F}_{2^n}\}$ and $G_{F'} := \{(x, F'(x)), x \in \mathbb{F}_{2^n}\}$ are affine equivalent, that is, if there exists an affine permutation \mathcal{L} of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$ such that $\mathcal{L}(G_F) = G_{F'}$.

A standard notion of *nonlinearity* of an (n, m) -function F is defined as

$$\mathcal{N}(F) = \min_{v \in \mathbb{F}_{2^m}^*} nl(v \cdot F), \quad (1)$$

where $v \cdot F$ denotes the usual inner product on \mathbb{F}_{2^m} and $nl(\cdot)$ denotes the nonlinearity of Boolean functions (see definition in Section 2). From the covering radius bound, it is known that $\mathcal{N}(F) \leq 2^{n-1} - 2^{n/2-1}$. The functions achieving this bound are called (n, m) -*bent* functions. Equivalently, a vectorial Boolean function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^m}$ is said to be a vectorial bent function if all nonzero component functions of F are *bent* (Boolean) functions. Bent Boolean functions have maximum Hamming distance to the set of affine Boolean functions. The notion of bent function was introduced by Rothaus [9] and attracted a lot of research of more than four decades. Such functions are extremal combinatorial objects with several areas of application, such as coding

theory, maximum length sequences, cryptography. A survey on bent function can be found in [6] as well as the book [15].

In [16], it is shown that (n, m) -bent functions exist only if n is even and $m \leq n/2$. The notion of nonlinearity in (1) (denoted by \mathcal{N}), was first introduced by Nyberg in [16], which is closely related to Matsui's linear attack [13] on block ciphers. It has been further studied by Chabaud and Vaudenay [7]. The nonlinearity is invariant under CCZ equivalence (and hence under extended affine equivalence). Budaghyan and Carlet have proved in [1] that for bent vectorial Boolean functions, CCZ-equivalence coincides with EA-equivalence.

The problem of construction vectorial bent functions has been considered in the literature. Nyberg [16] investigated the constructions of vectorial bent functions; she presented two constructions based on Maiorana-McFarland bent functions and \mathcal{PS} bent functions, respectively. In [17], Satoh, Iwata, and Kurosawa have improved the first method of construction given in [16] so that the resulting functions achieve the largest degree. Further, several constructions of bent vectorial functions have been investigated in some papers [5,10,11,14,18]. A complete state of the art can be found in [15] (Chapter 12).

Very recently, Pott *et al.* [8] considered functions $\mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ of the form $F^i(x) = x^{2^i}(x + x^{2^k})$, where $n = 2k, i = 0, 1, \dots, n-1$. They showed that the upper bound of number of bent component functions of a vectorial function $F : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is $2^n - 2^{n/2}$ (n even). In addition, they showed that the binomials $F^i(x) = x^{2^i}(x + x^{2^k})$ have such a large number of bent components, and these binomials are inequivalent to the monomials $x^{2^{k+1}}$ if $0 < i < k$. Further, the properties (such as differential properties and complete Walsh spectrum) of the functions F^i were investigated.

In this paper, we will consider three open problems raised by Pott *et al.* [8]. In the first part, we prove that CCZ equivalence is preserved for vectorial functions having the maximum number of bent components. Next, we consider APN plateaued functions and investigate if they can have the maximum number of bent components. We shall give a negative answer to this question. Finally, we consider the bentness property of functions $\mathbb{F}_{2^{2k}} \rightarrow \mathbb{F}_{2^{2k}}$ of the form

$$G(x) = \alpha x^{2^i} \left(x + x^{2^k} + \sum_{j=1}^{\rho} \gamma^{(j)} x^{2^{t_j}} + \sum_{j=1}^{\rho} \gamma^{(j)} x^{2^{t_j+k}} \right), \quad (2)$$

where $m \leq k, \gamma^{(j)} \in \mathbb{F}_{2^k}$ and $0 \leq t_j \leq k$ be a nonnegative integer. In particular, we show the functions $x^{2^{t_2}}(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})$ are inequivalent to $x^{2^{t_2}}(x + x^{2^k})$, where $t_1 = 1$ and $\gcd(t_2, k) \neq 1$. Here we use the concept of CCZ-equivalence when we speak about the equivalence of functions. The rest of the paper is organized as follows. Some preliminaries are given in Section 2. In Section 3, we prove our result on the stability under CCZ equivalence of a function having the maximum number of bent components which solve Problem 4 in [8]. Next, in Section 4, we prove that APN plateaued functions cannot have the maximum number of bent components, which partially solves Problem 8 in [8]. Finally, in Section 5 we

investigate Problem 2 in [8]. To this end, we provide several functions defined as $G(x) = xL(x)$ on $\mathbb{F}_{2^{2k}}$ (where $L(x)$ is a linear function on $\mathbb{F}_{2^{2k}}$) such that the number of bent components $Tr_1^{2k}(\alpha F(x))$ is maximal.

2 Preliminaries and notation

Throughout this article, $\|E\|$ denotes the cardinality of a finite set E , the binary field is denoted by \mathbb{F}_2 and the finite field of order 2^n is denoted by \mathbb{F}_{2^n} . The multiplicative group $\mathbb{F}_{2^n}^*$ is a cyclic group consisting of $2^n - 1$ elements. The set of all Boolean functions mapping from \mathbb{F}_{2^n} (or \mathbb{F}_2^n) to \mathbb{F}_2 is denoted by B_n .

Recall that for any positive integers k , and r dividing k , the trace function from \mathbb{F}_{2^k} to \mathbb{F}_{2^r} , denoted by Tr_r^k , is the mapping defined as:

$$Tr_r^k(x) := \sum_{i=0}^{\frac{k}{r}-1} x^{2^{ir}} = x + x^{2^r} + x^{2^{2r}} + \cdots + x^{2^{k-r}}.$$

In particular, the *absolute trace* over \mathbb{F}_2 of an element $x \in \mathbb{F}_{2^n}$ equals $Tr_1^n(x) = \sum_{i=0}^{n-1} x^{2^i}$.

There exist several kinds of possible *univariate representations* (also called trace, or polynomial, representations) of Boolean functions which are not all unique and use the identification between the vector-space \mathbb{F}_2^n and the field \mathbb{F}_{2^n} . Any Boolean function over \mathbb{F}_2^n can be represented in a unique way as a polynomial in one variable $x \in \mathbb{F}_{2^n}$ of the form $f(x) = \sum_{j=0}^{2^n-1} a_j x^j$, where $a_0, a_{2^n-1} \in \mathbb{F}_2$, a_j 's are elements of \mathbb{F}_{2^n} for $1 \leq j < 2^n - 1$ such that $a_j^2 = a_{2^i \bmod (2^n-1)}$. The binary expansion of j is $j = j_0 + j_1 2 + \cdots + j_{n-1} 2^{n-1}$ and we denote $\vec{j} = (j_0, j_1, \dots, j_{n-1})$. The algebraic degree of f equals $\max\{wt(\vec{i}) \mid a_j \neq 0, 0 \leq j < 2^n\}$ where $wt(\vec{i}) = j_0 + j_1 + \cdots + j_{n-1}$. Affine functions (whose set is denoted by A_n) are those of algebraic degree at most 1. The Walsh transform of $f \in B_n$ at $\lambda \in \mathbb{F}_{2^n}$ is defined as

$$W_f(\lambda) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x) + Tr_1^n(\lambda x)}.$$

The *nonlinearity* of $f \in B_n$ is defined as the minimum Hamming distance to the set of all n -variable affine functions, i.e.,

$$nl(f) = \min_{g \in A_n} d(f, g).$$

where $d(f, g)$ is the Hamming distance between f and g . Following is the relationship between nonlinearity and Walsh spectrum of $f \in B_n$

$$nl(f) = 2^{n-1} - \frac{1}{2} \max_{\lambda \in \mathbb{F}_{2^n}} |W_f(\lambda)|.$$

By Parseval's identity $\sum_{\lambda \in \mathbb{F}_{2^n}} W_f(\lambda)^2 = 2^{2n}$, it can be shown that $\max\{|W_f(\lambda)| : \lambda \in \mathbb{F}_{2^n}\} \geq 2^{\frac{n}{2}}$ which implies that $nl(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$. If n is an even integer a

function $f \in \mathcal{B}_n$ is said to be *bent* if $W_f(\lambda) \in \{2^{\frac{n}{2}}, -2^{\frac{n}{2}}\}$, for all $\lambda \in \mathbb{F}_{2^n}$. Moreover, a function $f \in \mathcal{B}_n$ is said to be *t-plateaued* if $W_f(\lambda) \in \{0, \pm 2^{\frac{n+t}{2}}\}$, for all $\lambda \in \mathbb{F}_{2^n}$. The integer t ($0 \leq t \leq n$) is called the *amplitude* of f . Note that a bent function is a 0-plateaued function. In the following, “ \langle, \rangle ” denotes the standard inner (dot) product of two vectors, that is, $\langle \lambda, x \rangle = \lambda_1 x_1 + \dots + \lambda_n x_n$, where $\lambda, x \in \mathbb{F}_2^n$. If we identify the vector space \mathbb{F}_2^n with the finite field \mathbb{F}_{2^n} , we use the trace bilinear form $Tr_1^n(\lambda x)$ instead of the dot product, that is, $\langle \lambda, x \rangle = Tr_1^n(\lambda x)$, where $\lambda, x \in \mathbb{F}_{2^n}$.

For vectorial functions $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$, the extended Walsh-Hadamard transform defined as,

$$W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle v, F(x) \rangle + \langle u, x \rangle},$$

where $F(x) = (f_1(x), f_2(x), \dots, f_m(x))$, $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$.

Let F be a vectorial function from \mathbb{F}_{2^n} into \mathbb{F}_{2^m} . The linear combination of the coordinates of F are the Boolean functions $f_\lambda : x \mapsto Tr_1^m(\lambda F(x))$, $\lambda \in \mathbb{F}_{2^m}$, where f_0 is the null function. The functions f_λ ($\lambda \neq 0$) are called the *components* of F . A vectorial function is said to be *bent* (resp. *t-plateaued*) if all its components are bent (resp. *t-plateaued*). A vectorial function F is called *vectorial plateaued* if all its components are plateaued with possibly different amplitudes.

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be an (n, n) -function. For any $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2^n$, we denote

$$\begin{aligned} \Delta_F(a, b) &= \{x | x \in \mathbb{F}_2^n, F(x \oplus a) \oplus F(x) = b\}, \\ \delta_F(a, b) &= \|\Delta_F(a, b)\|, \end{aligned}$$

Then, we have $\delta(F) := \max_{a \neq 0, b \in \mathbb{F}_2^n} \delta_F(a, b) \geq 2$ and the functions for which equality holds are said to be *almost perfect nonlinear* (APN).

A nice survey on Boolean and vectorial Boolean functions for cryptography can be found in [2] and [3], respectively.

3 The stability of a function having the maximum number of bent components under CCZ equivalence

In [8], Pott et al. have shown that the maximum number of bent components of a vectorial (n, n) -function F is $2^n - 2^k$ where $k := \frac{n}{2}$ (n even). They left open the problem whether the property of a function having the maximum number of bent components is invariant under CCZ equivalence or not. In this section we solve this problem by giving a positive answer in the following theorem.

Theorem 1. *Let $n = 2k$ and $F, F'' : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be CCZ-equivalent functions. Then F has $2^n - 2^k$ bent components if and only if F'' has $2^n - 2^k$ bent components.*

Proof. Let F be a function with $2^n - 2^k$ bent components. Define

$$S = \{v \in \mathbb{F}_2^n : x \rightarrow \langle v, F(x) \rangle \text{ is not bent}\}.$$

By Theorem 3 of [8], S is a linear subspace of dimension k . Then, let U be any k -dimensional subspace of \mathbb{F}_2^n such that $U \cap S = \{0\}$. Let v_1, \dots, v_k be a basis of S and u_1, \dots, u_k be a basis of U . Define a new function $F' : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ as

$$F'(x) = (H(x), I(x))$$

where $H(x) = (\langle v_1, F(x) \rangle, \dots, \langle v_k, F(x) \rangle)$ and $I(x) = (\langle u_1, F(x) \rangle, \dots, \langle u_k, F(x) \rangle)$. Then, F' is EA-equivalent to F . Recall that the property of a function having the maximum number of bent components is invariant under EA equivalence. Thus, F' has $2^n - 2^k$ bent components. Since F and F'' are CCZ-equivalent functions, F'' is CCZ-equivalent to F' , which has $2^n - 2^k$ bent components. Let $\mathcal{L}(x, y, z) = (L_1(x, y, z), L_2(x, y, z), L_3(x, y, z))$, (with $L_1 : \mathbb{F}_2^n \times F_2^k \times F_2^k \rightarrow \mathbb{F}_2^n$, $L_2 : \mathbb{F}_2^n \times F_2^k \times F_2^k \rightarrow \mathbb{F}_2^k$ and $L_3 : \mathbb{F}_2^n \times F_2^k \times F_2^k \rightarrow \mathbb{F}_2^k$) be an affine permutation of $\mathbb{F}_2^n \times F_2^k \times F_2^k$ which maps the graph of F' to the graph of F'' . Then, the graph $\mathcal{G}_{F''} = \{\mathcal{L}(x, H(x), I(x)) : x \in \mathbb{F}_2^n\}$. Thus $L_1(x, H(x), I(x))$ is a permutation and for some affine function $L'_1 : \mathbb{F}_2^n \times F_2^k \rightarrow \mathbb{F}_2^n$ and linear function $L''_1 : \mathbb{F}_2^k \rightarrow \mathbb{F}_2^n$ we can write $L_1(x, y, z) = L'_1(x, y) + L''_1(z)$. For any element v of \mathbb{F}_2^n we have

$$\begin{aligned} \langle v, L_1(x, H(x), I(x)) \rangle &= \langle v, L'_1(x, H(x)) \rangle + \langle v, L''_1(I(x)) \rangle \\ &= \langle v, L'_1(x, H(x)) \rangle + \langle L''_1^*(v), I(x) \rangle \\ &= \langle L''_1^*(v), I(x) \rangle + \langle v', H(x) \rangle + \langle v'', x \rangle + a, \end{aligned} \quad (3)$$

where $a \in \mathbb{F}_2$, $v' \in \mathbb{F}_2^k$, $v'' \in \mathbb{F}_2^n$ and L''_1^* is the adjoint operator of L''_1 , in fact, L''_1^* is the linear permutation whose matrix is transposed of that of L''_1 . Since $L_1(x, H(x), I(x))$ is a permutation, then any function $\langle v, L_1(x, H(x), I(x)) \rangle$ is balanced (recall that this property is a necessary and sufficient condition) and, hence, cannot be bent. From the construction of F' , $\langle L''_1^*(v), I(x) \rangle + \langle v', H(x) \rangle + \langle v'', x \rangle + a$ is not bent if and only if $L''_1^*(v) = 0$. Therefore, $L''_1^*(v) = 0$ for any $v \in \mathbb{F}_2^n$. This means that L''_1 is null, that is, $L_1(x, H(x), I(x)) = L'_1(x, H(x))$. We can also write $L_i(x, y, z) = L'_i(x, y) + L''_i(z)$ for $i \in \{2, 3\}$ where $L'_i : \mathbb{F}_2^n \times F_2^k \rightarrow \mathbb{F}_2^k$ are affine functions and $L''_i : F_2^k \rightarrow \mathbb{F}_2^k$ are linear functions. Set $F''_1(x) = L_1(x, H(x), I(x)) = L'_1(x, H(x))$ and $F''_2(x) = (L'_2(x, H(x)) + L''_2(I(x)), L'_3(x, H(x)) + L''_3(I(x)))$. Then, $F''(x) = F''_2 \circ F''_1^{-1}(x)$. For any $v \in \mathbb{F}_2^n$ and $u = (u', u'') \in \mathbb{F}_2^k \times \mathbb{F}_2^k$,

$$\begin{aligned} W_{F''}(v, u) &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, F''(x) \rangle + \langle v, x \rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, F'' \circ F''_1(x) \rangle + \langle v, F''_1(x) \rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, F''_2(x) \rangle + \langle v, F''_1(x) \rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle u, (L''_2(I(x)), L''_3(I(x))) \rangle + \langle u, (L'_2(x, H(x)), L'_3(x, H(x))) \rangle + \langle v, L'_1(x, H(x)) \rangle} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{\langle L''_2^*(u') + L''_3^*(u''), I(x) \rangle + \langle v', H(x) \rangle + \langle v'', x \rangle + a}. \end{aligned}$$

By the construction of $I(x)$, if $L_2''^*(u') + L_3''^*(u'') \neq 0$, $\langle L_2''^*(u') + L_3''^*(u''), I(x) \rangle + \langle v', H(x) \rangle$ is bent. Thus, $\langle u, F''(x) \rangle$ is bent when $L_2''^*(u') + L_3''^*(u'') \neq 0$, where $u = (u', u'') \in \mathbb{F}_2^k \times \mathbb{F}_2^k$. For $i = 2, 3$, let A_i be the matrices of size $k \times k$ defined as

$$L_i''(z) = zA_i,$$

where $z = (z_1, \dots, z_k) \in \mathbb{F}_2^k$. Then,

$$\begin{aligned} L_2''^*(u') + L_3''^*(u'') &= u'A_2^T + u''A_3^T \\ &= (u', u'') \begin{bmatrix} A_2^T \\ A_3^T \end{bmatrix}. \end{aligned} \quad (4)$$

Recall that \mathcal{L} is a affine permutation. Hence, the rank of the linear function $(L_1''(z), L_2''(z), L_3''(z)) = (0, L_2''(z), L_3''(z))$ from \mathbb{F}_2^k to $\mathbb{F}_2^n \times F_2^k \times F_2^k$ is k . By $(L_1''(z), L_2''(z), L_3''(z)) = z[0|A_2|A_3]$, the rank of the matrix $[A_2|A_3]$ is k . Thus, the rank of the matrix $\begin{bmatrix} A_2^T \\ A_3^T \end{bmatrix} = [A_2|A_3]^T$ is also k . Set

$$\begin{aligned} S' &= \{(u', u'') \in \mathbb{F}_2^k \times \mathbb{F}_2^k : L_2''^*(u') + L_3''^*(u'') = 0\} \\ &= \{(u', u'') \in \mathbb{F}_2^k \times \mathbb{F}_2^k : (u', u'') \begin{bmatrix} A_2^T \\ A_3^T \end{bmatrix} = 0\}. \end{aligned}$$

Then, S' is a linear subspace of dimension k . By the previous discussion, if $u = (u', u'') \in \mathbb{F}_2^n \setminus S'$, the component function $\langle u, F''(x) \rangle$ is bent. Thus, $F''(x)$ has at least $2^n - 2^k$ bent components. From Theorem 3 in [8], $F''(x)$ has exactly $2^n - 2^k$ bent components, which completes the proof. \square

4 The non-existence of APN plateaued functions having the maximum number of bent components

In [8], the authors asked if APN functions could have the maximum number of bent components or not. In this section we investigate the case of all APN plateaued functions. The result is given the following theorem.

Theorem 2. *Let F be a plateaued APN function defined on \mathbb{F}_2^n (where $n \geq 4$ is an even positive integer). Then F cannot have the maximum number of bent components.*

Proof. Let F be a plateaued APN function on \mathbb{F}_2^n . Denote

$$N_t = \{v \in \mathbb{F}_2^n : W_F(u, v) = \pm 2^{\frac{n+t}{2}}\},$$

where $W_F(u, v) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot F(x) + u \cdot x}$ and t is a positive integer ($0 \leq t \leq n$). We have

$$\begin{aligned}
\sum_{u, v \in \mathbb{F}_2^n} W_F^4(u, v) &= \sum_{v \in \mathbb{F}_2^n} (2^{\frac{n+t_v}{2}})^2 \sum_{u \in \mathbb{F}_2^n} W_F^2(u, v) \\
&= 2^n \sum_{v \in \mathbb{F}_2^n} 2^{t_v} \sum_{u \in \mathbb{F}_2^n} W_F^2(u, v) \\
&= 2^{3n} \sum_{v \in \mathbb{F}_2^n} 2^{t_v} \\
&= 2^{3n} (N_0 + N_2 2^2 + \cdots + N_n 2^n).
\end{aligned} \tag{5}$$

Since F is APN, we have

$$\sum_{u, v \in \mathbb{F}_2^n} W_F^4(u, v) = 2^{3n} (3 \cdot 2^n - 2). \tag{6}$$

From Equations (5) and (6), we have

$$N_0 + N_2 2^2 + \cdots + N_n 2^n = 3 \cdot 2^n - 2.$$

Therefore, we have $N_0 \equiv 2 \pmod{4}$. Since $n \geq 4$, $2^n - 2^{\frac{n}{2}} \equiv 0 \pmod{4}$. Hence,

$$N_0 \neq 2^n - 2^{\frac{n}{2}}.$$

Thus, F does not have the maximum number of bent components. In particular, quadratic APN functions cannot have the maximum number of bent components. \square

5 New constructions of bent component functions of vectorial functions

In this section we provide several functions defined as $G(x) = xL(x)$ on $\mathbb{F}_{2^{2k}}$ such that the number of bent components $Tr_1^{2k}(\alpha F(x))$ equals $2^{2k} - 2^k$, where $L(x)$ is a linear function on $\mathbb{F}_{2^{2k}}$. We first recall two lemmas which will be useful in our context.

Lemma 1. [8] *Let $V = \mathbb{F}_{2^{2k}}$ and let \langle, \rangle be a nondegenerate symmetric bilinear form on V . If $\mathcal{L} : V \rightarrow V$ is linear, we denote the adjoint operator by \mathcal{L}^* , i.e., $\langle x, \mathcal{L}(y) \rangle = \langle \mathcal{L}^*(x), y \rangle$ for all $x, y \in V$. The function $f : V \rightarrow \mathbb{F}_2$, defined by $x \mapsto \langle x, \mathcal{L}(x) \rangle$, is bent if and only if $\mathcal{L} + \mathcal{L}^*$ is invertible.*

Lemma 2. [8] *Let $V = \mathbb{F}_{2^{2k}}$ and $\langle x, y \rangle = Tr_1^n(xy)$ be the trace bilinear form. If $\mathcal{L} : V \rightarrow V$ is defined by $\mathcal{L}(x) = \alpha x^{2^i}$, $\alpha \in V$ and for any $i = 0, 1, \dots, n-1$, then $\mathcal{L}^*(x) = \alpha^{2^{n-i}} x^{2^{n-i}}$.*

In [8], the authors presented a construction of bent functions through adjoint operators. We start by providing a simplified proof of [8, Theorem 4] (which is the main result of their article).

Theorem 3. [8, Theorem 4] *Let $V = \mathbb{F}_{2^{2k}}$ and i be a nonnegative integer. Then, the mapping F_α^i defined by*

$$F_\alpha^i(x) = Tr_1^{2k}(\alpha x^{2^i}(x + x^{2^k}))$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$.

Proof. From the proof of [8, Theorem 4], we know

$$\mathcal{L}(x) + \mathcal{L}^*(x) = Tr_k^{2k}(\alpha x^{2^i}) + \alpha^{2^{2k-i}} \left(Tr_k^{2k}(x) \right)^{2^{k-i}}.$$

From Lemma 1, we need to show that $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if $x = 0$.

Let $\nabla_a = \{x | Tr_k^{2k}(x) = a, a \in \mathbb{F}_{2^k}\}$. We all know $Tr_k^{2k}(x)$ is a surjection from $\mathbb{F}_{2^{2k}}$ to \mathbb{F}_{2^k} and $|\nabla_a| = 2^{2k-k}$ for any $a \in \mathbb{F}_{2^k}$. We also know $\nabla_0 = \mathbb{F}_{2^k}$.

If $\alpha \notin \mathbb{F}_{2^k}$, then $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if

$$\begin{cases} Tr_k^{2k}(\alpha x^{2^i}) = 0, \\ Tr_k^{2k}(x) = 0, \end{cases} \quad (7)$$

i.e., $x = 0$. If for any $x \neq 0$, we always have $\mathcal{L}(x) + \mathcal{L}^*(x) \neq 0$, then $\alpha \notin \mathbb{F}_{2^k}$. In fact, if $\alpha \in \mathbb{F}_{2^k}$, then

$$\mathcal{L}(x) + \mathcal{L}^*(x) = \alpha Tr_k^{2k}(x^{2^i}) + \left(\alpha Tr_k^{2k}(x) \right)^{2^{k-i}} = \alpha Tr_k^{2k}(x) + \left(\alpha Tr_k^{2k}(x) \right)^{2^{k-i}}.$$

Further, $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ for any $x \in \mathbb{F}_{2^k}$. Thus, we have $F_\alpha^i(x)$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. \square

Now, we are going to present a first new family of bent functions through adjoint operators.

Theorem 4. *Let $V = \mathbb{F}_{2^{2k}}$ and i be a nonnegative integer. Let t_1, t_2 be two positive integers such that $0 \leq t_1, t_2 \leq k$ and both $z^{2^{k-t_1}-1} + z^{2^{k-t_2}-1} + 1 = 0$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1 = 0$ have no solutions on \mathbb{F}_{2^k} . Then, the function F_α^i defined on V by*

$$F_\alpha^i(x) = Tr_1^{2k}(\alpha x^{2^i}(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})) \quad (8)$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$.

Proof. We have

$$\begin{aligned} F_\alpha^i(x) &= Tr_1^{2k}(\alpha x^{2^i}(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})) \\ &= Tr_1^{2k}(x\alpha x^{2^i}) + Tr_1^{2k}(x\alpha^{2^k} x^{2^{i+k}}) + Tr_1^{2k}(x\alpha^{2^{2k-t_1}} x^{2^{i+2k-t_1}}) \\ &\quad + Tr_1^{2k}(x\alpha^{2^{k-t_1}} x^{2^{i+k-t_1}}) + Tr_1^{2k}(x\alpha^{2^{2k-t_2}} x^{2^{i+2k-t_2}}) + Tr_1^{2k}(x\alpha^{2^{k-t_2}} x^{2^{i+k-t_2}}) \\ &= Tr_1^{2k}(x\mathcal{L}(x)), \end{aligned} \quad (9)$$

where

$$\begin{aligned}
\mathcal{L}(x) &= \alpha x^{2^i} + \alpha^{2^k} x^{2^{i+k}} + \alpha^{2^{2k-t_1}} x^{2^{i+2k-t_1}} + \alpha^{2^{k-t_1}} x^{2^{i+k-t_1}} \\
&\quad + \alpha^{2^{2k-t_2}} x^{2^{i+2k-t_2}} + \alpha^{2^{k-t_2}} x^{2^{i+k-t_2}} \\
&= \alpha x^{2^i} + (\alpha x^{2^i})^{2^k} + \alpha^{2^{k-t_1}} x^{2^{i+k-t_1}} + (\alpha^{2^{k-t_1}} x^{2^{i+k-t_1}})^{2^k} \\
&\quad + \alpha^{2^{k-t_2}} x^{2^{i+k-t_2}} + (\alpha^{2^{k-t_2}} x^{2^{i+k-t_2}})^{2^k} \\
&= \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right) + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_1}} + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_2}}
\end{aligned}$$

According to Lemma 2, the adjoint operator $\mathcal{L}^*(x)$ is

$$\begin{aligned}
\mathcal{L}^*(x) &= \alpha^{2^{2k-i}} x^{2^{2k-i}} + \alpha^{2^{2k-i}} x^{2^{k-i}} + \alpha^{2^{2k-i}} x^{2^{t_1-i}} \\
&\quad + \alpha^{2^{2k-i}} x^{2^{k+t_1-i}} + \alpha^{2^{2k-i}} x^{2^{t_2-i}} + \alpha^{2^{2k-i}} x^{2^{k+t_2-i}} \\
&= \alpha^{2^{2k-i}} \left(x^{2^{2k-i}} + x^{2^{k-i}} + x^{2^{t_1-i}} + x^{2^{k+t_1-i}} + x^{2^{t_2-i}} + x^{2^{k+t_2-i}} \right) \\
&= \alpha^{2^{2k-i}} \left(x^{2^{k-i}} + (x^{2^{k-i}})^{2^k} + x^{2^{t_1-i}} + (x^{2^{t_1-i}})^{2^k} + x^{2^{t_2-i}} + (x^{2^{t_2-i}})^{2^k} \right) \quad (10) \\
&= \alpha^{2^{2k-i}} \left((x + x^{2^k})^{2^{k-i}} + (x + x^{2^k})^{2^{t_1-i}} + (x + x^{2^k})^{2^{t_2-i}} \right) \\
&= \alpha^{2^{2k-i}} \left((x + x^{2^k})^{2^{k-i}} + (x + x^{2^k})^{2^{t_1+k-i}} + (x + x^{2^k})^{2^{t_2+k-i}} \right)
\end{aligned}$$

Thus, we have

$$\begin{aligned}
\mathcal{L}(x) + \mathcal{L}^*(x) &= \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right) + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_1}} + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_2}} \\
&\quad + \alpha^{2^{2k-i}} \left((x + x^{2^k})^{2^{k-i}} + (x + x^{2^k})^{2^{t_1+k-i}} + (x + x^{2^k})^{2^{t_2+k-i}} \right).
\end{aligned}$$

Note that we have $\mathcal{L}(x) \in \mathbb{F}_{2^k}$ and $(x + x^{2^k})^{2^{k-i}} + (x + x^{2^k})^{2^{t_1+k-i}} + (x + x^{2^k})^{2^{t_2+k-i}} \in \mathbb{F}_{2^k}$ for any $x \in \mathbb{F}_{2^k}$. From Lemma 1, it is sufficient to show that $\mathcal{L}(x) + \mathcal{L}^*(x)$ is invertible. That is, we need to show that $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if $x = 0$.

Since both $z^{2^{k-t_1}-1} + z^{2^{k-t_2}-1} + 1 = 0$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} , we have both $\left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right) + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_1}} + \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_2}} = 0$ and $(x + x^{2^k})^{2^{k-i}} + (x + x^{2^k})^{2^{t_1+k-i}} + (x + x^{2^k})^{2^{t_2+k-i}} = 0$ if and only if

$$\begin{cases} \alpha x^{2^i} + (\alpha x^{2^i})^{2^k} = 0, \\ x + x^{2^k} = 0. \end{cases} \quad (11)$$

From the proof of Theorem 3, when both $z^{2^{k-t_1}-1} + z^{2^{k-t_2}-1} + 1 = 0$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} , we have $F_\alpha^i(x)$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. \square

We immediately have the following statement by setting $t_2 = k - t_1$ in the previous theorem.

Corollary 1. Let $V = \mathbb{F}_{2^{2k}}$ and i be a nonnegative integer. Let t_1, t_2 be two positive integers such that $t_1 + t_2 = k$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1 = 0$ has no solution in \mathbb{F}_{2^k} . Then, the mapping F_α^i defined on V by

$$F_\alpha^i(x) = Tr_1^{2k}(\alpha G(x))$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$, where $G(x) = x^{2^i} \left(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}} \right)$.

The previous construction given by Theorem 4 can be generalized as follows.

Theorem 5. Let $V = \mathbb{F}_{2^{2k}}$ and i be a nonnegative integer. Let t_1, t_2 be two positive integers such that $0 \leq t_1, t_2 \leq k$ and both $(\gamma^{(1)})^{2^{k-t_1}} z^{2^{k-t_1}-1} + (\gamma^{(2)})^{2^{k-t_2}} z^{2^{k-t_2}-1} + 1 = 0$ and $(\gamma^{(1)})^{2^{k-i}} z^{2^{t_1}-1} + (\gamma^{(2)})^{2^{k-i}} z^{2^{t_2}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} , where $\gamma^{(1)}, \gamma^{(2)} \in \mathbb{F}_{2^k}$. Then, the mapping F_α^i defined by

$$F_\alpha^i(x) = Tr_1^{2k} \left(\alpha x^{2^i} \left(x + x^{2^k} + \gamma^{(1)}(x^{2^{t_1}} + x^{2^{t_1+k}}) + \gamma^{(2)}(x^{2^{t_2}} + x^{2^{t_2+k}}) \right) \right) \quad (12)$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$.

Proof. We have

$$F_\alpha^i(x) = Tr_1^{2k}(x\mathcal{L}(x)), \quad (13)$$

where

$$\begin{aligned} \mathcal{L}(x) &= \alpha x^{2^i} + \alpha^{2^k} x^{2^{i+k}} + (\gamma^{(1)})^{2^{k-t_1}} \left(\alpha^{2^{2k-t_1}} x^{2^{i+2k-t_1}} + \alpha^{2^{k-t_1}} x^{2^{i+k-t_1}} \right) \\ &\quad + (\gamma^{(2)})^{2^{k-t_2}} \left(\alpha^{2^{2k-t_2}} x^{2^{i+2k-t_2}} + \alpha^{2^{k-t_2}} x^{2^{i+k-t_2}} \right) \\ &= \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right) + (\gamma^{(1)})^{2^{k-t_1}} \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_1}} \\ &\quad + (\gamma^{(2)})^{2^{k-t_2}} \left(\alpha x^{2^i} + (\alpha x^{2^i})^{2^k} \right)^{2^{k-t_2}} \end{aligned}$$

The adjoint operator $\mathcal{L}^*(x)$ is

$$\begin{aligned} \mathcal{L}^*(x) &= \alpha^{2^{2k-i}} x^{2^{2k-i}} + \alpha^{2^{2k-i}} x^{2^{k-i}} + (\gamma^{(1)})^{2^{k-i}} \left(\alpha^{2^{2k-i}} x^{2^{t_1-i}} \right. \\ &\quad \left. + \alpha^{2^{2k-i}} x^{2^{k+t_1-i}} \right) + (\gamma^{(2)})^{2^{k-i}} \left(\alpha^{2^{2k-i}} x^{2^{t_2-i}} + \alpha^{2^{2k-i}} x^{2^{k+t_2-i}} \right) \\ &= \alpha^{2^{2k-i}} \left((x + x^{2^k})^{2^{k-i}} + (\gamma^{(1)})^{2^{k-i}} (x + x^{2^k})^{2^{t_1-i}} + (\gamma^{(2)})^{2^{k-i}} (x + x^{2^k})^{2^{t_2-i}} \right) \\ &= \alpha^{2^{2k-i}} \left((x + x^{2^k})^{2^{k-i}} + (\gamma^{(1)})^{2^{k-i}} (x + x^{2^k})^{2^{t_1+k-i}} + (\gamma^{(2)})^{2^{k-i}} (x + x^{2^k})^{2^{t_2+k-i}} \right) \end{aligned} \quad (14)$$

Note that we have $\mathcal{L}(x) \in \mathbb{F}_{2^k}$ and $(x + x^{2^k})^{2^{k-i}} + (\gamma^{(1)})^{2^{k-i}} (x + x^{2^k})^{2^{t_1+k-i}} + (\gamma^{(2)})^{2^{k-i}} (x + x^{2^k})^{2^{t_2+k-i}} \in \mathbb{F}_{2^k}$ for any $x \in \mathbb{F}_{2^{2k}}$. In order to show that $\mathcal{L}(x) + \mathcal{L}^*(x)$ is invertible, we need to show that $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if $x = 0$.

Since both $(\gamma^{(1)})^{2^{k-t_1}} z^{2^{k-t_1}-1} + (\gamma^{(2)})^{2^{k-t_2}} z^{2^{k-t_2}-1} + 1 = 0$ and $(\gamma^{(1)})^{2^{k-i}} z^{2^{t_1}-1} + (\gamma^{(2)})^{2^{k-i}} z^{2^{t_2}-1} + 1 = 0$ have no solutions on \mathbb{F}_{2^k} , we have both $\mathcal{L}(x) = 0$ and

$(x + x^{2^k})^{2^{k-i}} + (\gamma^{(1)})^{2^{k-i}}(x + x^{2^k})^{2^{t_1+k-i}} + (\gamma^{(2)})^{2^{k-i}}(x + x^{2^k})^{2^{t_2+k-i}} = 0$ if and only if

$$\begin{cases} \alpha x^{2^i} + (\alpha x^{2^i})^{2^k} = 0, \\ x + x^{2^k} = 0. \end{cases} \quad (15)$$

By using the proof of Theorem 3, we have $F_\alpha^i(x)$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. \square

By the same process used to prove Theorem 5, one can get the following result.

Theorem 6. *Let $V = \mathbb{F}_{2^{2k}}$ and i, ρ be two nonnegative integers such that $\rho \leq k$. Let $\gamma^{(j)} \in \mathbb{F}_{2^k}$ and $0 \leq t_j \leq k$ be a nonnegative integer, where $j = 1, 2, \dots, \rho$. Assume that both equations $\sum_{j=1}^{\rho} (\gamma^{(j)})^{2^{k-t_j}} z^{2^{k-t_j}-1} + 1 = 0$ and $\sum_{j=1}^{\rho} (\gamma^{(j)})^{2^{k-i}} z^{2^{t_j}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} . Then, the mapping F_α^i defined on V by*

$$F_\alpha^i(x) = Tr_1^{2k}(\alpha G(x)) \quad (16)$$

is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$, where $G(x) = x^{2^i} \left(Tr_k^{2k}(x) + \sum_{j=1}^{\rho} \gamma^{(j)} (Tr_k^{2k}(x))^{2^{t_j}} \right)$.

Lemma 3. *[8] Let $F_\alpha(x) = Tr_1^{2k}(\alpha G(x))$, be a Boolean bent function for any $\alpha \in \mathbb{F}_2^{2k} \setminus \mathbb{F}_2^k$, where $G : \mathbb{F}_2^{2k} \rightarrow \mathbb{F}_2^{2k}$. Then, $F : \mathbb{F}_2^{2k} \rightarrow \mathbb{F}_2^k$, defined as $F(x) = Tr_k^{2k}(\alpha G(x))$ is a vectorial bent function for any $\alpha \in \mathbb{F}_2^{2k} \setminus \mathbb{F}_2^k$.*

According to Theorem 6 and Lemma 3, we immediately get the following theorem.

Theorem 7. *Let $G(x)$ be defined as in Theorem 6. Then, the mapping F_α defined by*

$$F_\alpha(x) = Tr_k^{2k}(\alpha G(x)) \quad (17)$$

is a vectorial bent function for any $\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$.

In [8], the authors presented the differential spectrum of the functions $G : \mathbb{F}_{2^{2k}} \rightarrow \mathbb{F}_{2^{2k}}$ defined by $G(x) = x^{2^i}(x + x^{2^k})$. Their result is given below.

Lemma 4. *[8] Let i be a nonnegative integer such that $i < k$. The differential spectrum of the functions $G(x) = x^{2^i}(x + x^{2^k})$, $G : \mathbb{F}_{2^{2k}} \rightarrow \mathbb{F}_{2^{2k}}$, is given by,*

$$\delta_G(a, b) \in \begin{cases} \{0, 2^k\} & \text{if } a \in \mathbb{F}_{2^k}^*, \\ \{0, 2^{\gcd(i, k)}\} & \text{if } a \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}. \end{cases} \quad (18)$$

In particular, $\delta_G(a, b) = 2^k$ only for $a \in \mathbb{F}_{2^k}^$ and $b \in \mathbb{F}_{2^k}$.*

Now we are going to show that the differential spectrum of the functions $x^{2^i}(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})$ is different from the one of the functions $x \mapsto x^{2^i}(x + x^{2^k})$.

Theorem 8. Let $F_\alpha^i(x) = Tr_1^{2k}(\alpha G(x))$ be defined as Theorem 4, where $G(x) = x^{2^i}(x + x^{2^k} + x^{2^{t_1}} + x^{2^{t_1+k}} + x^{2^{t_2}} + x^{2^{t_2+k}})$. If there exists $t_1 = 1$ and $\gcd(t_2, k) \neq 1$ such that both $z^{2^{k-t_1}-1} + z^{2^{k-t_2}-1} + 1 = 0$ and $z^{2^{t_1}-1} + z^{2^{t_2}-1} + 1 = 0$ have no solutions on \mathbb{F}_{2^k} , then for $i = t_2$, there exist elements $a \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ such that the number $\delta_G(a, b)$ is equal to 2 for any $b \in \mathbb{F}_{2^{2k}}$, which is neither $2^{\gcd(i, k)}$ nor 2^k .

Proof. Let $a \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ such that $\tau^{2^{t_1}} = \tau$, where $\tau = a + a^{2^k} \neq 0$ (since $t_1 | k$). We have

$$G(x) + G(x + a) = a^{2^i} \left(x + x^{2^k} + (x + x^{2^k})^{2^{t_1}} + (x + x^{2^k})^{2^{t_2}} \right) + (x + a)^{2^i} \left(a + a^{2^k} + (a + a^{2^k})^{2^{t_1}} + (a + a^{2^k})^{2^{t_2}} \right). \quad (19)$$

Thus, for any $x' \in \mathbb{F}_{2^{2k}}$, there must be one element $b \in \mathbb{F}_{2^{2k}}$ such that $G(x') + G(x' + a) = b$.

Let x', x'' are the solutions of $G(x) + G(x + a) = b$. Hence

$$\begin{aligned} & G(x') + G(x' + a) + G(x'') + G(x'' + a) \\ &= a^{2^i} \left(x' + x'^{2^k} + (x' + x'^{2^k})^{2^{t_1}} + (x' + x'^{2^k})^{2^{t_2}} + x'' + x''^{2^k} \right. \\ & \quad \left. + (x'' + x''^{2^k})^{2^{t_1}} + (x'' + x''^{2^k})^{2^{t_2}} \right) \\ & \quad + (x' + x'')^{2^i} \left(a + a^{2^k} + (a + a^{2^k})^{2^{t_1}} + (a + a^{2^k})^{2^{t_2}} \right) = 0. \end{aligned} \quad (20)$$

Since $x + x^{2^k} \in \mathbb{F}_{2^k}$ for any $x \in \mathbb{F}_{2^{2k}}$, (20) implies that $(x' + x'')^{2^i} \left(a + a^{2^k} + (a + a^{2^k})^{2^{t_1}} + (a + a^{2^k})^{2^{t_2}} \right)$ belongs to the multiplicative coset $a^{2^i} \mathbb{F}_{2^k}^*$. Thus, we necessarily have $x' + x'' = a\nu$, where $\nu \in \mathbb{F}_{2^k}^*$. Further, $x' + x'' + (x' + x'')^{2^k} = a\nu + a^{2^k} \nu$. Since $t_1 | t_2$, from (20), we have

$$\begin{aligned} & \left(\tau + \tau^{2^{t_1}} + \tau^{2^{t_2}} \right) \nu^{2^i} + \tau \nu + \tau^{2^{t_1}} \nu^{2^{t_1}} + \tau^{2^{t_2}} \nu^{2^{t_2}} \\ &= \tau \left(\nu^{2^i} + \nu + \nu^{2^{t_1}} + \nu^{2^{t_2}} \right) = 0. \end{aligned} \quad (21)$$

If we set $i = t_2$, then from (21) we have $\delta_G(a, b) = 2 \neq 2^{\gcd(i, k)}$ since $\gcd(i, k) = \gcd(t_2, k) \neq 1$.

For one element $b \in \mathbb{F}_{2^{2k}}$, if for any $x' \in \mathbb{F}_{2^{2k}}$, we always have $G(x') + G(x' + a) \neq b$, then $\delta_G(a, b) = 0$.

□

Theorem 9. Let i, ρ be two nonnegative integers such that $\rho \leq k$. Let $0 \leq t_j \leq k$ be a nonnegative integer, where $j = 1, 2, \dots, \rho$. Assume that both $\sum_{j=1}^{\rho} z^{2^{k-t_j}-1} + 1 = 0$ and $\sum_{j=1}^{\rho} z^{2^{t_j}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} . Then, the mapping F_α^i defined by

$$F_\alpha^i(x) = Tr_1^{2k}(\alpha G(x)) \quad (22)$$

where $G(x) = x^{2^i} \left(\text{Tr}_k^{2k}(x) + \sum_{j=1}^{\rho} (\text{Tr}_k^{2k}(x))^{2^{tj}} \right)$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. Further, if the number of the solutions of $\sum_{j=1}^{\rho} z^{2^{tj}} + z + z^{2^i} = 0$ on \mathbb{F}_{2^k} is not equal to $2^{\gcd(i,k)}$, then there exist elements $a \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ such that the number $\delta_G(a, b)$ does not equal $2^{\gcd(i,k)}$ for any $b \in \mathbb{F}_{2^{2k}}$.

Proof. From Theorem 6, we know $F_{\alpha}^i(x)$ is bent if and only if $\alpha \notin \mathbb{F}_{2^k}$. We have

$$\begin{aligned} G(x) + G(x+a) &= a^{2^i} \left(\text{Tr}_k^{2k}(x) + \sum_{j=1}^{\rho} (\text{Tr}_k^{2k}(x))^{2^{tj}} \right) \\ &\quad + (x+a)^{2^i} \left(\text{Tr}_k^{2k}(a) + \sum_{j=1}^{\rho} (\text{Tr}_k^{2k}(a))^{2^{tj}} \right) = b. \end{aligned} \quad (23)$$

Let $a \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ such that $a + a^{2^k} = 1$. We need to show the number of solutions of $G(x) + G(x+a) = b$ is not equal to $2^{\gcd(i,k)}$ for any $b \in \mathbb{F}_{2^{2k}}$. Let $\rho = \gcd(i, k)$. We suppose $\delta_G(a, b) = 2^{\rho}$ and let x', x'' are the solutions of (23) for some b . Hence

$$\begin{aligned} &G(x') + G(x' + a) + G(x'') + G(x'' + a) \\ &= a^{2^i} \left(\text{Tr}_k^{2k}(x' + x'') + \sum_{j=1}^{\rho} (\text{Tr}_k^{2k}(x' + x''))^{2^{tj}} \right) + (x' + x'')^{2^i} = 0 \end{aligned} \quad (24)$$

since $\sum_{j=1}^{\rho} z^{2^{tj}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} , that is, $\left(\text{Tr}_k^{2k}(a) + \sum_{j=1}^{\rho} (\text{Tr}_k^{2k}(a))^{2^{tj}} \right) =$

1. For any $x \in \mathbb{F}_{2^{2k}}$, (24) implies that $(x' + x'')^{2^i}$ belongs to the multiplicative coset $a^{2^i} \mathbb{F}_{2^k}^*$. Thus, we necessarily have $x' + x'' = a\nu$, where $\nu \in \mathbb{F}_{2^k}^*$. Further, $\text{Tr}_k^{2k}(x' + x'') = x' + x'' + (x' + x'')^{2^k} = a\nu + a^{2^k} \nu$. From (24), we have

$$\nu^{2^i} + \nu + \sum_{j=1}^{\rho} \nu^{2^{tj}} = 0. \quad (25)$$

We also know that the number of the solutions of $\sum_{j=1}^{\rho} z^{2^{tj}} + z + z^{2^i} = 0$ on \mathbb{F}_{2^k} is not equal to $2^{\gcd(i,k)}$, thus, if $a \in \{x | \text{Tr}_k^{2k}(x) = 1, x \in \mathbb{F}_{2^{2k}}\}$, the number $\delta_G(a, b)$ is not equals $2^{\gcd(i,k)}$ for any $b \in \mathbb{F}_{2^{2k}}$ \square

Theorem 10. Let $n = 2k, e$ be two positive integers. Let $V = \mathbb{F}_{2^{2k}}$ and i be a non-negative integer. Let $E = \{x | x \in \mathbb{F}_{2^{2k}}, \text{Tr}_k^{2k}(x) \in \mathbb{F}_{2^e}\}$ and $O = \{x \in \mathbb{F}_{2^{2k}}, \text{Tr}_k^{2k}(x) \in M\}$, where $M = \{y + \text{Tr}_e^k(y) | y \in \mathbb{F}_{2^k}\}$. Let F_{α}^i be the function defined on V by

$$F_{\alpha}^i(x) = \text{Tr}_1^{2k} \left(\alpha x^{2^i} \text{Tr}_e^{2k}(x) \right). \quad (26)$$

If $\frac{k}{e}$ is even, then F_{α}^i is bent if and only if $\alpha \notin E$. If $\frac{k}{e}$ is odd, then F_{α}^i is bent if and only if $\alpha \notin O$. Further, if k is odd and $e = 2$, then F_{α}^i is bent if and only if $\alpha \notin O$.

Proof. We have

$$\begin{aligned}
F_\alpha^i(x) &= Tr_1^{2k} \left(\alpha x^{2^i} (x + x^{2^e} + x^{2^{2e}} + \cdots + x^{2^{2k-e}}) \right) \\
&= Tr_1^{2k} (x \alpha x^{2^i}) + Tr_1^{2k} (x \alpha^{2^{2k-e}} x^{2^i+2k-e}) + Tr_1^{2k} (x \alpha^{2^{2k-2e}} x^{2^i+2k-2e}) \\
&\quad + \cdots + Tr_1^{2k} (x \alpha^{2^e} x^{2^i+e}) \\
&= Tr_1^{2k} (x \mathcal{L}(x)),
\end{aligned} \tag{27}$$

where

$$\begin{aligned}
\mathcal{L}(x) &= \alpha x^{2^i} + \alpha^{2^{2k-e}} x^{2^i+2k-e} + \alpha^{2^{2k-2e}} x^{2^i+2k-2e} + \cdots + \alpha^{2^e} x^{2^i+e} \\
&= \alpha x^{2^i} + (\alpha x^{2^i})^{2^{2k-e}} + (\alpha x^{2^i})^{2^{2k-2e}} + \cdots + (\alpha x^{2^i})^{2^e} \\
&= Tr_e^{2k} (\alpha x^{2^i}).
\end{aligned}$$

According to Lemma 2, the adjoint operator $\mathcal{L}^*(x)$ is

$$\begin{aligned}
\mathcal{L}^*(x) &= \alpha^{2^{2k-i}} x^{2^{2k-i}} + \alpha^{2^{2k-i}} x^{2^{2e-i}} + \alpha^{2^{2k-i}} x^{2^{2e-2i}} + \cdots + \alpha^{2^{2k-i}} x^{2^{2k-e-i}} \\
&= \alpha^{2^{2k-i}} \left(x^{2^{2k-i}} + x^{2^{2e-i}} + x^{2^{2e-2i}} + \cdots + x^{2^{2k-e-i}} \right) \\
&= \alpha^{2^{2k-i}} \left(x + x^{2^e} + x^{2^{2e}} + \cdots + x^{2^{2k-e}} \right)^{2^{2k-i}} \\
&= \alpha^{2^{2k-i}} (Tr_e^{2k}(x))^{2^{2k-i}}.
\end{aligned} \tag{28}$$

Thus, we have

$$\mathcal{L}(x) + \mathcal{L}^*(x) = Tr_e^{2k}(\alpha x^{2^i}) + \alpha^{2^{2k-i}} (Tr_e^{2k}(x))^{2^{2k-i}}.$$

From Lemma 1, it is sufficient to show that $\mathcal{L}(x) + \mathcal{L}^*(x)$ is invertible. That is, we need to show that $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ if and only if $x = 0$.

For $\frac{k}{e}$ being even, we have $Tr_e^{2k}(x) = 0$ if and only if $x \in E$. If $\alpha \notin E$, then $\mathcal{L}(x) + \mathcal{L}^*(x) = 0$ is only if

$$\begin{cases} Tr_e^{2k}(\alpha x^{2^i}) = Tr_e^k \left(Tr_k^{2k}(\alpha x^{2^i}) \right) = 0, \\ Tr_e^{2k}(x) = 0, \end{cases} \tag{29}$$

i.e., $x = 0$. If for any $x \neq 0$, we have $\mathcal{L}(x) + \mathcal{L}^*(x) \neq 0$, then $\alpha \notin E$. In fact, if suppose $\alpha \in E$, then

$$\begin{aligned}
\mathcal{L}(x) + \mathcal{L}^*(x) &= Tr_e^{2k}(\alpha x^{2^i}) + \alpha^{2^{2k-i}} (Tr_e^{2k}(x))^{2^{2k-i}} \\
&= Tr_k^{2k}(\alpha) Tr_e^k \left(Tr_k^{2k}(x^{2^i}) \right) + \alpha^{2^{2k-i}} (Tr_e^{2k}(x))^{2^{2k-i}} \\
&= 0
\end{aligned}$$

for any $x \in E$. Hence, $F_\alpha^i(x)$ is bent if and only if $\alpha \notin E$.

Similarly, for $\frac{k}{e}$ odd, we have $Tr_e^{2k}(x) = 0$ if and only if $x \in O$. We can prove $F_\alpha^i(x)$ is bent if and only if $\alpha \notin O$.

Similarly, for k odd and $e = 2$, we have $Tr_2^{2k}(x) = 0$ if and only if $x \in O$. We can prove $F_\alpha^i(x)$ is bent if and only if $\alpha \notin O$. \square

Remark 1. Note that Theorem 3 is special case of Theorem 10. It corresponds to the case where $e = k$.

Similary to Theorem 6, we have the following statement.

Theorem 11. *Let i, ρ be two nonnegative integers such that $\rho \leq k$. Let $\gamma^{(j)} \in \mathbb{F}_{2^k}$ and $0 \leq t_j \leq k$ be a nonnegative integer, where $j = 1, 2, \dots, \rho$. Let both $\sum_{j=1}^{\rho} (\gamma^{(j)})^{2^{k-t_j}} z^{2^{k-t_j}-1} + 1 = 0$ and $\sum_{j=1}^{\rho} (\gamma^{(j)})^{2^{k-i}} z^{2^{t_j}-1} + 1 = 0$ have no solution in \mathbb{F}_{2^k} . Let E and O be defined as Theorem 10. Let the function F_{α}^i be defined by*

$$F_{\alpha}^i(x) = Tr_1^{2k} \left(\alpha x^{2^i} \left(Tr_e^{2k}(x) + \sum_{j=1}^{\rho} \gamma^{(j)} (Tr_e^{2k}(x))^{2^{t_j}} \right) \right). \quad (30)$$

If $\frac{k}{e}$ is even, then F_{α}^i is bent if and only if $\alpha \notin E$. If $\frac{k}{e}$ is odd, then F_{α}^i is bent if and only if $\alpha \notin O$. Further, if k is odd and $e = 2$, then F_{α}^i is bent if and only if $\alpha \notin O$.

6 Conclusions

This paper is in the line of a very recent paper published in the IEEE-transactions Information Theory by Pott et al [8] in which several open problems have been raised. In the present paper, we have established that the property of a function having the maximal number of bent components is invariant under CCZ-equivalence which gives an answer to an open problem in [8]. Next, we have proved the non-existence of APN plateaued functions having the maximal number of bent components which gives a partial answer to an open problem in [8]. Furthermore, we have exhibited several bent functions F_{α}^i for any $\alpha \in \mathbb{F}_{2^{2k}} \setminus \mathbb{F}_{2^k}$ provided that some conditions hold. In other words, the set of those α for which F_{α}^i is bent is of maximal cardinality $2^{2k} - 2^k$. This provide an answer to another open problem in [8]. In addition, we have studied the differential spectrum of certain functions and showed that it is not equal to those studied in [8].

References

1. L. Budaghyan and C. Carlet.: On CCZ-equivalence and its use in secondary constructions of bent functions, Proceedings of the International Workshop on Coding and Cryptography WCC 2009.
2. C. Carlet.: ‘Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 257–397, 2010.
3. C. Carlet.: Vectorial Boolean Functions for Cryptography, Chapter of the monography *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. Hammer eds, Cambridge University Press, pp. 398–469, 2010.
4. C. Carlet, P. Charpin and V. Zinoviev.: “Codes, bent functions and permutations suitable for DES-like cryptosystems”, *Designs, Codes and Cryptography*, 15(2), pp. 125–156, 1998.

5. C. Carlet and S. Mesnager.: On the construction of bent vectorial functions. *Journal of Information and Coding Theory: Algebraic and Combinatorial Coding Theory* Vol. 1, No. 2, pp. 133-148 (2010).
6. C. Carlet, S. Mesnager.: Four decades of research on bent functions”, *Designs, Codes and Cryptography*, vol. 78, no. 1, pp. 5–50, 2016.
7. F. Chabaud and S. Vaudenay.: Links between differential and linear cryptanalysis. Proceedings of *EUROCRYPT’94*, *Lecture Notes in Computer Science* 950, pp. 356-365 (1995).
8. A. Pott, E. Pasalic, A. Muratović-Ribić and S. Bajrić.: On the maximum number of bent components of vectorial functions, *IEEE Transactions on Information Theory*. Volume: 64, Issue: 1, pp. 403-411, 2018.
9. O. S. Rothaus.: On bent functions, *J. Combin. Theory, Ser. A*, vol. 20, pp. 300–305, May 1976.
10. Pasalic, E. and Zhang, W. G.: On Multiple Output Bent Functions, *Inf. Process. Lett.* vol. 112, no. 21, pp. 811–815, nov, 2012.
11. K. Feng and J. Yang.: Vectorial boolean functions with good cryptographic properties. *Int. J. Found. Comput. Sci.*, vol. 22(6):1271-1282, 2011
12. C. Tang, Y. Qi, M. Xu.: New Quadratic Bent Functions in Polynomial Forms with Coefficients in Extension Fields, <https://eprint.iacr.org/2013/405.pdf>
13. M. Matsui.: Linear cryptanalysis method for DES cipher, In: *Advances in Cryptology—EUROCRYPT’93*, *Lecture Notes in Computer Science*, vol.765, Berlin: Springer-Verlag, pp.386–397, 1993.
14. S. Mesnager.: Bent vectorial functions and linear codes from o-polynomials. *Journal Designs, Codes and Cryptography*. 77(1), pages 99-116 (2015).
15. S. Mesnager.: Bent functions: fundamentals and results, pp. 1–544, Springer, Switzerland 2016.
16. K. Nyberg, “Perfect non-linear S-boxes”, *Proceedings of EUROCRYPT’ 91*, *Lecture Notes in Computer Science*, vol. 547, pp. 378–386, 1992.
17. T. Satoh, T. Iwata and K. Kurosawa.: On cryptographically secure vectorial Boolean functions. *Proceeding of Asiacrypt’99* *Lecture Notes in Computer Science*, Springer-Verlag, Berlin, pp.20-28 (1999).
18. J. Wu, Y. Wei, and X. Wang.: An optimized method for multiple output bent functions. *Acta Electronica Sinica*, vol. 33(3):521-523, 2005.