A new method for secondary constructions of vectorial bent functions

A. Bapić [*] E. Pasalic[†]

Abstract

In 2017, Tang et al. have introduced a generic construction for bent functions of the form $f(x) = g(x) + h(x)$, where g is a bent function satisfying some conditions and h is a Boolean function. Recently, Zheng et al. [22] generalized this result to construct large classes of bent vectorial Boolean function from known ones in the form $F(x) = G(x)+h(X)$, where G is a bent vectorial and h a Boolean function. In this paper we further generalize this construction to obtain vectorial bent functions of the form $F(x) = G(x)+\mathbf{H}(X)$, where $\mathbf{H}$ is also a vectorial Boolean function. This allows us to construct new infinite families of vectorial bent functions, EA-inequivalent to G, which was used in the construction. Most notably, specifying $\mathbf{H}(x) = \mathbf{h}(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx))$, the function $\mathbf{h} : \mathbb{F}_2^t \to \mathbb{F}_{2^t}$ can be chosen arbitrary which gives a relatively large class of different functions for a fixed function G. We also propose a method of constructing vectorial (n, n)-functions having maximal number of bent components.

Keywords: Bent functions, Vectorial bent functions, Algebraic degree, EA equivalence, CCZ equivalence, Maximal number of bent components

1 Introduction

Throughout the paper, with $\mathbb{F}_{2^n}$ we denote the finite field with 2^n elements, where $n = 2m$ is a positive integer. Any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is called an (n, m)-function. Specially, when $n = m$ we call F an S-box and when $m = 1$ we call F a Boolean function. An important class of Boolean functions was introduced by Rothaus [17] in 1976, which are defined in even number of variables with maximum Hamming distance to the set of all affine functions. These functions are called *bent* functions, and we will denote the set of all bent functions in dimension n with $\mathcal{B}_n$. Bent functions have been exhaustively studied in the past four decades because of their applications in cryptography, coding theory, graph theory, association schemes, etc. For more details on bent functions we refer to [9] and [19].

The bentness property has been extended to general (n, m)-functions F. We say that F is a *vectorial bent* (n, m)-function if the functions $Tr_1^m(\lambda F(x))$ are bent for all $\lambda \in \mathbb{F}_{2^m*} = \mathbb{F}_{2^m}\backslash\{0\}$. As shown by Nyberg [14], these functions exist only for $m \leq n/2$. The construction methods

[*] University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: amar.bapic@famnit.upr.si

[†] University of Primorska, FAMNIT & IAM, Koper Slovenia, e-mail: enes.pasalic6@gmail.com

of vectorial bent functions can be divided into two classes: *primary* (building functions from scratch) and *secondary* (building functions using known vectorial bent functions) *constructions*. For some known constructions (primary and secondary), see [4, 6, 8, 11, 12, 13, 15, 20].

Pott et al. [16] have proved that (n, n)-functions, $n = 2m$, can have at most $2^n - 2^m$ bent components, and those that posses the maximum number of bent components can give rise to new vectorial bent functions of maximal dimension. In the follow up work Mesnager et al. [10] generalized this approach and identified a larger family of functions having $2^n - 2^m$ bent components. In [21], the authors extend this to general (n, m)-functions, $m \geq n/2$, and prove that they can have at most $2^m - 2^{m-\frac{n}{2}}$ bent components which can be used to specify new vectorial bent functions.

In 2017, Tang et al. [18] proposed a secondary construction of bent functions of the form $f(x) = g(x) + h(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx))$, where $n = 2m$, g is any known bent function in $\mathcal{B}_n$ satisfying some conditions, $h(X_1, \ldots, X_t)$ is an arbitrary polynomial in $\mathbb{F}_2[X_1, \ldots, X_t]$, t is a positive integer such that $1 \leq t \leq m$, and $u_1, \ldots, u_t$ are t nonzero elements in $\mathbb{F}_{2^n}$ which satisfy some conditions. Using this construction, several new infinite families of bent functions from specific classes of bent functions (Kasami functions, Niho functions, Gold-like monomial functions, Maiorana-McFarland class) were obtained.

This result has been extended in a recent paper by Zheng et. al [22] to construct vectorial bent functions. Let $n = 2m$ and let k be its positive divisor such that $k \leq m$. The authors [22] proposed a method of constructing vectorial bent (n, k)-functions of the form $F(x) = G(x) + h(x)$, where G is a vectorial bent (n, k)-function satisfying certain properties and h is a Boolean function. Using this approach the authors in [22] constructed three new infinite families of vectorial bent (n, k)-functions, as well as new infinite families of vectorial plateaued $(n, k + t)$-functions (t nonegative integer) having maximal number of bent components.

In this paper we extend the result of Zheng *et al.* [22] for the purpose of constructing new vectorial bent (n, m)-functions, $n = 2m$ and $t|m$, of the form

$$F(x) = G(x) + \mathbf{H}(x), \tag{1}$$

where G is a suitable vectorial bent (n, m)-function and $\mathbf{H}$ is an (n, t)-function. More precisely, the assumption on G is that the duals of its components $G_\lambda(x) = Tr_1^m(\lambda F(x))$ satisfy certain forms of linearity so that $G_\lambda^*\left(x + \sum_{i=1}^t u_iw_i\right) = G_\lambda^*(x) + \sum_{i=1}^t w_ig_i(x)$ for all $x \in \mathbb{F}_{2^n}$ and $(w_1, \ldots, w_t) \in \mathbb{F}_2^t$, where G_λ^* denotes the dual bent function of G_λ. Most notably, specifying $\mathbf{H}(x) = \mathbf{h}(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx))$, the function $\mathbf{h} : \mathbb{F}_2^t \to \mathbb{F}_{2^t}$ can be chosen arbitrarily which gives a relatively large class of different functions for a fixed function G. It is also proved that the vectorial bentness of $F(x) = G(x) + \mathbf{H}(x)$ requires that $\mathbf{H}$ is not bent. We identify several suitable classes of vectorial bent functions G (satisfying the above mentioned property) which then give rise to infinite families of vectorial bent functions for any fixed G. We also consider the EA-equivalence between the newly constructed function F and G (since in the case of vectorial bent functions CCZ-equivalence coincides with EA-equivalence, see [1]). An immediate consequence of the result that $\mathbf{H}$ cannot be bent, is that G and $\mathbf{H}$ must be EA-inequivalent. Furthermore, one can easily conclude that assuming $\deg(\mathbf{H}) > \deg(G)$ implies that F and G are EA-inequivalent. Nevertheless, more general results related to the EA-equivalence between F and G are not easy to establish, see questions **Q1** and **Q2** in Section 3.

Finally, we propose a method of constructing vectorial (n,n)-functions having maximal number of bent components using a similar design rationale as above, thus representing $F(x)=G(x)+\mathbf{H}'(x)$. This additionally enlarges the known families of such functions, already identified in [16, 10, 21]. Even in this case, representing $\mathbf{H}'(x)=\gamma\mathbf{h}(Tr_1^n(u_1x),\ldots,Tr_1^n(u_tx))$, $\gamma\in\mathbb{F}_{2^n}\backslash\mathbb{F}_{2^m}$, there are no conditions on $\mathbf{h}:\mathbb{F}_2^t\to\mathbb{F}_{2^t}$ which can be taken arbitrary.

The rest of this article is organised as follows. In Section 2 we give some basic definitions and notation used throughout the paper. Our main construction of vectorial bent functions, along with an analysis on EA-equivalence, is presented in Section 3. Some new infinite families of vectorial bent functions are derived in Section 4. In Section 5, we propose a new method of specifying infinite classes of vectorial (n,n) functions having maximum number of bent components. Some concluding remarks are given in section 6.

2 Preliminaries

With $\#S$ we denote the cardinality of a finite set S. The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $(x_1,\ldots,x_n)$, where $x_i\in\mathbb{F}_2$. With $\mathbb{F}_{2^n}$ we denote the finite field of order 2^n and with $\mathbb{F}_{2^n*}$ the multiplicative cyclic group consisting of 2^n-1 elements. For convenience, we will sometimes identify the vector space $\mathbb{F}_2^n$ with $\mathbb{F}_{2^n}$. A polynomial $F(x)\in\mathbb{F}_{2^n}[x]$ is called a *permutation polynomial* if the induced mapping $x\mapsto F(x)$ is a permutation over $\mathbb{F}_{2^n}$. Functions mapping from $\mathbb{F}_{2^n}\to\mathbb{F}_{2^m}$ are called (n,m)-functions. Specially, we will refer to (n,n)-functions as S-boxes and to $(n,1)$-functions as Boolean functions.

Moreover, any S-box $F:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ can be uniquely expressed by a *univariate polynomial* of (univariate) degree at most 2^n-1:

$$F(x)=\sum_{i=0}^{2^n-1}a_ix^i,\ \ a_i\in\mathbb{F}_{2^n}. \tag{2}$$

For the 2-adic expansion $i=i_0+i_12+i_22^2+\ldots i_{n-1}2^{n-1}$, the algebraic degree of F is defined as

$$\deg(F)=\max\{\mathrm{wt}(i):a_i\neq 0,\ 0\leq i<2^n\},$$

where $\mathrm{wt}(i)$ is the Hamming weight of $i=(i_0,i_1,\ldots,i_{n-1})$ (the number of nonzero coefficients i_j, $j=0,\ldots,n-1$).

For $x\in\mathbb{F}_{2^n}$ the *trace* $Tr_k^n(x):\mathbb{F}_{2^n}\to\mathbb{F}_{2^k}$ of x over $\mathbb{F}_{2^k}$, k is a divisor of n, is defined by

$$Tr_k^n(x)=x+x^{2^k}+\ldots+x^{2^{k(n/k-1)}}.$$

If $k=1$, then Tr_1^n is called the *absolute trace*. The *Walsh-Hadamard transform* (respectively *inverse Walsh-Hadamard transform*) of a Boolean function f on $\mathbb{F}_{2^n}$ at a point $u\in\mathbb{F}_{2^n}$ is defined by

$$W_f(u)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{f(x)+Tr_1^n(ux)}, \tag{3}$$

respectively,

$$(-1)^{f(u)} = \sum_{x\in\mathbb{F}_{2^n}} W_f(x)(-1)^{Tr_1^n(ux)}. \tag{4}$$

If $W_f(u) = \pm 2^{\frac{n}{2}}$ for all $u \in \mathbb{F}_{2^n}$, we say that f is a *bent function.* In case $W_f(u) \in \{0, \pm 2^{\frac{n+s}{2}}\}$ for all $u \in \mathbb{F}_{2^n}$, we say that f is *s-plateaued.* It is clear that bent Boolean functions exist only in even dimension. When a Boolean function f is bent, the Boolean function f^* such that $W_f(u) = 2^{\frac{n}{2}}(-1)^{f*(u)}$ for any $u \in \mathbb{F}_{2^n}$ is also bent and is called the *dual* of f.

If we identify $\mathbb{F}_{2^n}$ with $\mathbb{F}_2^n$, for the multivariate representation of f over $\mathbb{F}_2^n$, the Walsh-Hadamard transform of f at a point $w = (w_1, \ldots, w_n) \in \mathbb{F}_2^n$ is

$$W_f(w_1, \ldots, w_n) = \sum_{(x_1,\ldots,x_n)\in\mathbb{F}_2^n} (-1)^{f(x_1,\ldots,x_n)+\sum_{i=1}^n w_i x_i}. \tag{5}$$

For an (n, m)-function $F = (f_1, \ldots, f_m)$, where $f_1 \ldots, f_m : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are the *coordinate functions* of F, all the $2^m - 1$ nonzero linear combinations of the coordinates f_i are called *component functions* of F, i.e. the functions $F_\lambda(x) = Tr_1^m(\lambda F(x))$, $\lambda \in \mathbb{F}_{2^m*}$. The function $W_F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m*} \to \mathbb{R}$ defined by

$$W_F(\lambda, u) := W_{F_\lambda}(u) = \sum_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda F(x))+Tr_1^n(ux)},\ u \in \mathbb{F}_{2^n},\ \lambda \in \mathbb{F}_{2^n*},$$

is called the *Walsh-Hadamard transform* of the function F. The function F is said to be a *bent vectorial function* of dimension m if all the components of F are bent. These functions exist only for $m \le n/2$.

Two (n, m)-functions F and G are called *extended affine equivalent* (EA-equivalent) if there exist some affine permutation L_1 over $\mathbb{F}_{2^n}$, some affine permutation L_2 over $\mathbb{F}_{2^m}$ and some affine function $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $F = L_2 \circ G \circ L_1 + A$. They are called *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) (introduced in [3] and later named CCZ-equivalence in [2]) if there exists some affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^m}$, where $L_1 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^n}$ and $L_2 : \mathbb{F}_{2^n} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ are affine functions, such that $y = G(x)$ if and only if $L_2(x, y) = F \circ L_1(x, y)$. It is well known that EA-equivalence is a special case of CCZ-equivalence [2].

3 Generic construction of vectorial bent functions

Motivated by the results in [18] and [22], we give the following construction of vectorial Boolean functions.

Remark 1 *Throughout the paper, with G^*_λ we will denote the dual of the bent component G_λ, $\lambda \in \mathbb{F}_{2^m*}$, of a bent (n, m)-function G, $n = 2m$.*

Construction 1 *Let $u_1, \ldots, u_t$ be t linearly independent elements in $\mathbb{F}_{2^n*}$, where $n = 2m$ and $t|m$. Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be any vectorial bent function whose components $G_\lambda(x) =$*

$Tr_1^m(\lambda F(x))$, with $\lambda \in \mathbb{F}_{2^m*}$, satisfy

$$G_\lambda^*\left(x+\sum_{i=1}^{t} u_i w_i\right) = G_\lambda^*(x) + \sum_{i=1}^{t} w_i g_i(x) \tag{6}$$

for all $x \in \mathbb{F}_{2^n}$ and $(w_1, \dots, w_t) \in \mathbb{F}_2^t$, where $g_i(x)$ is a Boolean function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, $1 \le i \le t$. Let $\mathbf{h}(X_1, \dots, X_t)$ be any vectorial Boolean Function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Define $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, using G and $\mathbf{h}$, as

$$F(x) = G(x) + \mathbf{H}(x), \tag{7}$$

where $\mathbf{H} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^t}$ is defined by $\mathbf{H}(x) = \mathbf{h}(Tr_1^n(u_1x), \dots, Tr_1^n(u_tx))$. Equivalently, if $\mathbf{h}$ is defined using the finite field notation so that $\mathbf{h} : \mathbb{F}_{2^t} \to \mathbb{F}_{2^t}$, then define

$$F(x) = G(x) + \mathbf{H}(x) = G(x) + \mathbf{h}(Tr_1^n(u_1x) + \alpha Tr_1^n(u_2x) + \dots + \alpha^{t-1} Tr_1^n(u_tx)), \tag{8}$$

where α is a primitive element of $\mathbb{F}_{2^t}$.

Example 1 *Let us consider the Kasami function $G : \mathbb{F}_{2^8} \to \mathbb{F}_{2^4}$ defined with $G(x) = x^{2^4+1}$. It is well known that the components of G are bent whose duals G_λ^* satisfy (6) [7, 18]. We note that $(2^8-1)/(2^4-1) = 17$ and thus $\mathbb{F}_{2^4} = \langle \alpha^{17} \rangle$, where α is a root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_{2^8}[x]$.*

As suggested in [22], let us define $U = \{x \in \mathbb{F}_{2^8} : x \cdot x^{2^4} = 1\}$ and assume that $\{\tau_1, \dots, \tau_4\}$ is a basis of $\mathbb{F}_{2^4}$. The so-called defining set, introduced in [22] required in (6), is $S = \{\tau_1 v, \dots, \tau_4 v\}$, where $v \in U, v \neq 1$.

For example, we can take

$$S = \{u_1, \dots, u_4\} = \{\alpha^5 + \alpha^2 + \alpha, \alpha^7 + \alpha^4 + \alpha^3 + \alpha^2 + 1, \alpha^7 + \alpha^3 + \alpha^2, \alpha^6 + \alpha^5 + 1\}.$$

Let $\mathbf{h} : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined with $\mathbf{h}(x) = x^3$. Then

$$F(x) = G(x) + \mathbf{H}(x) = x^{17} + (Tr_1^8(u_1x) + \beta Tr_1^8(u_2x) + \dots + \beta^2 Tr_1^8(u_3x) + \beta^3 Tr_1^8(u_4x))^3,$$

where $\beta = \alpha^{17}$.

Using the mathematical software Sage *and* MAGMA*, we confirm that F is a bent $(8,4)$-function and it is CCZ-inequivalent to G and $\mathbf{H}$.*

In connection to Construction 1 and Example 1, we state the following theorem.

Theorem 1 *Let F be a function generated by Construction 1. Then, F is a vectorial bent (n,m)-function, and the dual of F is*

$$F^*(x) = G^*(x) + \tilde{\mathbf{H}}(x),$$

where $\tilde{\mathbf{H}}(x) = \mathbf{h}(g_1(x), \dots, g_t(x))$.

Proof. Let $\lambda \in \mathbb{F}_{2^m*}$ be arbitrary. Let us consider the component G_λ and let $\mathbf{h}_\lambda : \mathbb{F}_2^t \to \mathbb{F}_2$ be defined with $\mathbf{h}_\lambda = Tr_1^m(\lambda \mathbf{h})$. From the inverse Walsh-Hadamard transform we have that

$$(-1)^{\mathbf{h}_\lambda(X_1,\ldots,X_t)} = \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{\sum_{i=1}^t w_i X_i}. \tag{9}$$

For any $x \in \mathbb{F}_{2^n}$ and $1 \leq i \leq t \leq m$, taking $X_i = Tr_1^n(u_i x)$ we obtain

$$(-1)^{\mathbf{h}_\lambda(Tr_1^n(u_1x),\ldots,Tr_1^n(u_tx))} = \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{Tr_1^n\left((\sum_{i=1}^t w_i u_i)x\right)}. \tag{10}$$

Multiplying both sides of equation (10) by $(-1)^{G_\lambda(x)+Tr_1^n(\beta x)}$, we have

$$(-1)^{G_\lambda(x)+\mathbf{H}_\lambda(x)+Tr_1^n(\beta x)} = \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{G_\lambda(x)+Tr_1^n\left((\beta+\sum_{i=1}^t w_i u_i)x\right)}.$$

By summing the previous expression on both sides over all $x \in \mathbb{F}_{2^n}$ and from the fact that G is vectorial bent, we obtain that

$$\begin{aligned} W_{F_\lambda}(\beta) &= \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t) W_{G_\lambda}(\beta + \sum_{i=1}^t u_i w_i) \\ &= 2^m \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{G_\lambda^*(\beta+\sum_{i=1}^t u_i w_i)}. \end{aligned} \tag{11}$$

It follows from (6) and (11) that

$$W_{F_\lambda}(\beta) = 2^m(-1)^{G_\lambda^*(\beta)} \sum_{(w_1,\ldots,w_t)\in\mathbb{F}_2^t} W_{\mathbf{h}_\lambda}(w_1,\ldots,w_t)(-1)^{\sum_{i=1}^t w_i g_i(\beta)}.$$

The sum on the right corresponds to the inverse Walsh-Hadamard transform and thus we have

$$W_{F_\lambda}(\beta) = 2^m(-1)^{G_\lambda^*(\beta)+\mathbf{h}_\lambda(g_1(\beta),g_2(\beta),\ldots,g_t(\beta))} = 2^m(-1)^{(G^*(\beta)+\tilde{\mathbf{H}}(\beta))_\lambda}.$$

Since $\lambda \in \mathbb{F}_{2^m*}$ and $\beta \in \mathbb{F}_{2^n}$ are arbitrary, we have that F is vectorial bent and $F^*(x) = G^*(x) + \tilde{\mathbf{H}}(x)$. □

Remark 2 *If we have a function $f : X \to Y$, then the number of possible functions f equals to $\#Y^{\#X}$. Thus, since $\mathbf{h}$ is a (t,t)-function, there are 2^{t2^t} possible choices for $\mathbf{h}$. Hence, we can construct at most 2^{t2^t} bent (n,m)-functions F from a fixed bent function G and an arbitrary function $\mathbf{h}$. For example, in case $n = 8$ and $m = t = 4$, we have 2^{64} possibilities.*

The following lemma is a straightforward consequence of linearity of mapping $L : \mathbb{F}_{2^n} \to \mathbb{F}_2^t$, where $x \mapsto (Tr_1^n(u_1x),\ldots,Tr_1^n(u_tx))$ and $u_1,\ldots,u_t \in \mathbb{F}_{2^t}$ are linearly independent over $\mathbb{F}_2$.

Lemma 1 *Let $u_1, \ldots, u_t$ be t linearly independent elements in $\mathbb{F}_{2^t}{}^*$, $n = 2m, t|m$. Then the multiset*

$$V = \{(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx)) : x \in \mathbb{F}_{2^n}\} \tag{12}$$

contains exactly 2^{n-t} copies of every element of $\mathbb{F}_2^t$.

It is interesting to notice that $\mathbf{H}$ in Construction 1 cannot be bent as shown below.

Proposition 1 *Let $u_1, \ldots, u_m$ be m linearly independent elements in $\mathbb{F}_{2^n}{}^*$, where $n = 2m$. The function $\mathbf{H} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ defined by*

$$\mathbf{H}(x) = \mathbf{h}(Tr_1^n(u_1x), \ldots, Tr_1^n(u_mx)),$$

where $\mathbf{h} : \mathbb{F}_2^m \to \mathbb{F}_{2^m}$ is arbitrary, cannot be bent.

Proof. Let $\lambda \in \mathbb{F}_{2^m}{}^*$ be arbitrary. Let us consider the value of $W_{\mathbf{H}_\lambda}(0)$.

$$\begin{aligned} W_{\mathbf{H}_\lambda}(0) &= \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{H}_\lambda(x)} = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathbf{h}_\lambda\left(Tr_1^n(u_1x), \ldots, Tr_1^m(u_mx)\right)} \\ &\overset{(12)}{=} 2^{n-m} \sum_{X \in \mathbb{F}_2^m} (-1)^{\mathbf{h}_\lambda(X)} = 2^m \cdot W_{\mathbf{h}_\lambda}(0) \end{aligned}$$

Since $W_{\mathbf{h}_\lambda}(0) \neq \pm 1$, it follows that $W_{\mathbf{H}_\lambda}(0) \neq \pm 2^m$. Hence, $\mathbf{H}_\lambda$ cannot be bent. Thus, no components of $\mathbf{H}$ are bent Boolean functions. □

Remark 3 *From [18, Lemma 2.1] we know that if $u_1, \ldots, u_t \in \mathbb{F}_{2^n}{}^*$ are linearly independent and $f \in \mathbb{F}_2[X_1, \ldots, X_t]$ is a reduced polynmial of algebraic degree d, then $f(Tr_1^n(u_1x), \ldots, Tr_1^n(u_tx))$ is also of algebraic degree d. Hence, the algebraic degree of $\mathbf{H}$ is*

$$\deg(\mathbf{H}) = \max_{\lambda \in \mathbb{F}_{2^t}{}^*} \deg(\mathbf{H}_\lambda)$$

Remark 4 ***(CCZ-equivalence)*** *From [1, Theorem 1], CCZ-equivalence between bent (n, m)-functions coincides with EA-equivalence. Therefore, since $\mathbf{H}$ is not bent it follows that the functions G and $\mathbf{H}$ used in Construction 1 are always EA-inequivalent. Moreover, it is interesting to note that the bent function F is obtained by adding a nonlinear non-bent function $\mathbf{H}$ to a bent function G.*

Example 2 *Let us consider the bent $(8, 4)$-function $G(x) = \sum_{i=1}^{2^r-1} x^{(i2^{m-r}+1)(2^m-1)+1}$ with $m = 4, r = 3$. The function G satisfies property (6) with the defining set $U = \{u_1, \ldots, u_4\}$, where U forms a basis of $\mathbb{F}_{2^4}$ over $\mathbb{F}$. We note that $\deg(G) = 4$. Let us consider the functions $\mathbf{h}_2, \mathbf{h}_3, \mathbf{h}_4 : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ defined with*

$$\begin{aligned} \mathbf{h}_2(X) &= X^3; \\ \mathbf{h}_3(X) &= X^3 + X^{13}; \end{aligned}$$

$$\mathbf{h}_4(X) = X^3 + X^{13} + X^{15}.$$

We note that $\deg(\mathbf{h}_i) = i$*, for* $i = 2, 3, 4$*. Let* F_i *be the bent* $(8, 4)$*-function obtained from Construction 1 via* G *and* $\mathbf{h}_i$*. Using* Sage *and* MAGMA *we confirm that* $\deg(F_i) = 4$*. Furthermore, when considering the EA-equivalence between the functions we observe that* F_i *and* G *are EA-inequivalent, for* $i = 2, 3, 4$*. Moreover, the functions* F_2 *and* F_4*,* F_3 *and* F_4 *are EA-inequivalent, whereas* F_2 *and* F_3 *are EA-equivalent.*

The following result is a direct consequence of the fact that the algebraic degree is an EA-invariant.

Proposition 2 *With the same notation as in Construction 1, let* F *be a bent* (n, m)*-function constructed from* G *and* $\mathbf{H}$*. If* $\deg(\mathbf{H}) > \deg(G)$*, then* F *and* G *are EA-inequivalent.*

Proof. Follows directly from

$$\deg(F) = \max\{\deg(\mathbf{H}), \deg(G)\} = \deg(\mathbf{H}) > \deg(G)$$

and the fact that the algebraic degree is invariant under EA-equivalence.

Another interesting question can be formulated as follows. Suppose that F and G were EA-inequivalent, then there would exist affine permutations L_1, L_2 on $\mathbb{F}_{2^n}, \mathbb{F}_{2^m}$, respectively, and an affine mapping $A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ such that $G(x) = L_2(F(L_1(x)) + A(x)$. Since $F = G + \mathbf{H}$, we can rewrite the previous equation as

$$G(x) + L_2(G(L_1(x)) = E_2(\mathbf{H}(L_1(x)) + A(x), \tag{13}$$

where E_2 is the linear part of the affine permutation L_2. The right-hand expression is obviously in the EA-class of $\mathbf{H}$ and since by Proposition 1 the function $\mathbf{H}$ cannot be bent, we deduce that the function on the left-hand side is not bent either. We notice that $G(x) + L_2(G(L_1(x))$ is the sum of two vectorial bent functions lying in the same EA-class. Generally, it is not known if a set $\mathcal{S}$ of bent functions is closed under addition, and thus we cannot say anything about the bentness of $G(x) + L_2(G(L_1(x))$, where $\mathcal{S}$ represents the EA-equivalence class of G. If the sum is bent, then obviously F and G cannot be EA-equivalent, because of (13) and the fact that $\mathbf{H}$ is not bent. On the other hand, if the sum is not bent we cannot say anything certain on the EA-equivalence. Thus we leave this question as an open problem.
Q1: What can we say about EA-equivalence between F and G, if F and G have the same algebraic degree?

Q2: Let F_i be bent (n, m)-functions obtained from Construction 1 via G_i and $\mathbf{H}_i$, for $i = 1, 2$. Assuming that $\deg(F_1) = \deg(F_2)$, what can we say about the EA-equivalence between F_1 and F_2?

From Example 2, we have observed that among the functions F_2, F_3 and F_4, the functions F_2 and F_3 were EA-equivalent, whilst the other pairings were EA-inequivalent. Thus, it is natural to ask, what choice of G or $\mathbf{H}$ affects this EA-equivalence.

4 New infinite families of vectorial bent functions

In [22] the authors constructed several infinite families of vectorial bent functions using certain vectorial bent functions G which satisfy property (6). The very same functions can be used to construct new families of vectorial bent functions via Construction 1. In addition, we consider vectorial bent functions from the Maiorana-McFarland class which were not considered in [22], but were considered by Tang *et al.* [18] in the construction of bent Boolean functions.

We summarise some useful results from [22] in the following theorem.

Theorem 2 *Let G be one of the following bent vectorial Boolean functions:*

(i) $G(x) = x^{2^m+1},\ n = 2m$

(ii) $G(x) = \sum_{i=1}^{2^r-1} x^{(i2^{m-r}+1)(2^m-1)+1},\ n = 2m,\ \gcd(r, m) = 1$

(iii) $G(x) = Tr_k^n(\omega x^{2^m+1}),\ n = 4m,\ m \geq 2$ *and* ω *is a generator of the cyclic group* $U = \{x \in \mathbb{F}_{2^{2m}} : x^{2^m+1} = 1\}$.

Then G is a bent (n, m)-function which satisfies (6) with the defining set

(i) $\{u_1, \ldots, u_m\} \subset \mathbb{F}_{2^{n*}}$ *such that* $u_i u_j^{2^m} \in \mathbb{F}_{2^{m*}}$ *for all* $1 \leq i < j \leq m$*;*

(ii) $\{u_1, \ldots, u_m\}$ *is a basis of* $\mathbb{F}_{2^m}$ *over* $\mathbb{F}_2$*;*

(iii) $\{u_1, \ldots, u_m\} \subset \mathbb{F}_{2^{n*}}$ *such that* $u_i u_j^{2^m} \in \mathbb{F}_{2^{m*}}$ *for all* $1 \leq i < j \leq m$*,*

respectively.

Theorem 3 *Let $G(x)$ be one of the three bent (n, m)-functions in Theorem 2, $\{u_1, \ldots, u_t\}$ its corresponding defining set for property (6) and let t be a positive divisor of m. Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function $F(x) = G(x) + \mathbf{H}(x)$, generated by Construction 1, is a bent vectorial (n, m)-function.*

Proof. The result is an immediate consequence of Construction 1, Theorem 1 and Theorem 2. $\square$

Let us define $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ with $F(x, y) = x\pi(y) + g(y)$, where $\pi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation and $g : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is an arbitrary function. A function defined in such a way belongs to the class of vectorial bent Maiorana-McFarland functions. Let $\lambda \in \mathbb{F}_{2^{m*}}$ be arbitrary, we then have the component $F_\lambda(x, y) = Tr_1^m(\lambda x\pi(y) + \lambda g(y))$. Its corresponding dual is defined with (see [5]):

$$F_\lambda^*(x, y) = Tr_1^m \left(y\pi^{-1}(x/\lambda) + \lambda g(\pi^{-1}(x/\lambda)) \right),$$

where π^{-1} is the inverse permutation of π. Motivated by [18, Section E], we will consider two subclasses of the vectorial Maiorana-McFarland class which satisfy property (6).

Following the methodology in [18], we note that (6) can be written in bivariate form as follows:

$$G_\lambda^*\left(x+\sum_{i=1}^{t}\alpha_i w_i, y+\sum_{i=1}^{t}\beta_i w_i\right)=G_\lambda^*(x,y)+\sum_{i=1}^{t} w_i g_i(\alpha_i,\beta_i) \tag{14}$$

for all $(x,y)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ and $(w_1,\ldots,w_t)\in\mathbb{F}_2^t$, where $u_i=(\alpha_i,\beta_i)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ and g_i is a Boolean function from $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to $\mathbb{F}_2$, $1\le i\le t$.

Since each linear function from $\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$ to $\mathbb{F}_2$ can be written as $Tr_1^m(ux+vy)$, where $(u,v)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$, the vectorial Boolean function in (7) by Construction 1 can be rewritten as:

$$F(x,y)=G(x,y)+\mathbf{h}\left(Tr_1^m(\alpha_i x+\beta_i y),\ldots,Tr_1^m(\alpha_t x+\beta_t y)\right). \tag{15}$$

Lemma 2 *Let $u_1,\ldots,u_t$ be any t linearly independent elements in $\mathbb{F}_{2^n*}$, where $1\le t\le m$. Write $u_i=(\alpha_i,\beta_i)\in\mathbb{F}_{2^m}\times\mathbb{F}_{2^m}$. Let $G(x,y)=y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$. If $Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)=0$ for each $1\le i<j\le t$ and $\lambda\in\mathbb{F}_{2^m*}$, then the dual component G_λ^* satisfies* (6) *with*

$$g_i(x,y)=Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)+\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right). \tag{16}$$

Proof. It follows from (6) and the fact that π is linear that

$$\begin{aligned}
G_\lambda^*\left(x+\sum_{i=1}^{t}w_i\alpha_i, y+\sum_{i=1}^{t}w_i\beta_i\right) &= Tr_1^m\left(\left(y+\sum_{i=1}^{t}w_i\beta_i\right)\pi^{-1}\left(\frac{x}{\lambda}+\sum_{i=1}^{t}w_i\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^{t}w_i Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)\right)+\\
&+\sum_{i=1}^{t}Tr_1^m\left(w_i^2\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right)+\sum_{1\le i<j\le t}w_iw_jTr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^{t}w_i Tr_1^m\left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)+\beta_i\pi^{-1}\left(\frac{x}{\lambda}\right)+\beta_i\pi\left(\frac{\alpha_i}{\lambda}\right)\right)+\\
&+\sum_{1\le i<j\le t}w_iw_jTr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)\\
&= G_\lambda^*(x,y)+\sum_{i=1}^{t}w_i g_i(x,y)+\sum_{1\le i<j\le t}w_iw_jTr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right),
\end{aligned}$$

where g_i is defined by (16). The conclusion follows from the assumption that

$$Tr_1^m\left(\beta_i\pi^{-1}\left(\frac{\alpha_j}{\lambda}\right)+\beta_j\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right)=0,$$

for each $1\le i<j\le t$ and $\lambda\in\mathbb{F}_{2^m*}$. ∎

The following result is an immediate consequence of Lemma 2.

Corollary 1 *Let $\alpha_1, \ldots, \alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^{m*}}$, $1 \leq t \leq m$. Write $u_i = (\alpha_i, 0)$. Let $G(x, y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$. Then the dual component G^*_λ satisfies (6) with*

$$g_i(x, y) = Tr_1^m \left(y\pi^{-1}\left(\frac{\alpha_i}{\lambda}\right)\right), \tag{17}$$

for any $\lambda \in \mathbb{F}_{2^{m*}}$.

The use of of non-quadratic vectorial bent functions in the Maiorana-McFarland class in Construction 1 is given below.

Proposition 3 *Let s be a positive divisor of m such that m/s is odd. Let $u_i = (\alpha_i, \beta_i) \in \mathbb{F}_{2^s} \times \mathbb{F}_{2^s}$ be any t linearly independent elements, where $1 \leq t \leq m$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that $d(2^s + 1) \equiv 1 \pmod{2^m - 1}$ and $a \in \mathbb{F}_{2^{m*}}$. If $\alpha_i\beta_j + \alpha_j\beta_i = 0$ and $Tr_1^m(\beta_i\alpha_j^2 + \beta_j\alpha_i^2) = 0$ for any $1 \leq i < j \leq t$ and $\lambda \in \mathbb{F}_{2^{m*}}$, then the dual component G^*_λ satisfies (6) with*

$$g_i(x, y) = Tr_1^m \left(\frac{y}{(a\lambda)^{2^s+1}} \left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right) + \frac{1}{(a\lambda)^{2^s+1}} \left(\beta_i\alpha_i x + \beta_i\alpha_i x^{2^s} + \beta_i\alpha_i^2\right)\right) \tag{18}$$

Proof. Since $\pi^{-1}(x) = x^{2^s+1}$, we have that $G^*_\lambda(x, y) = Tr_1^m \left(y \left(\frac{x}{\lambda}\right)^{2^s+1}\right)$. It follows from (6) and the fact that $\alpha_i^{2^s} = \alpha_i, \beta_i^{2^s} = \beta_i$, that

$$\begin{aligned}
G^*_\lambda\left(x + \sum_{i=1}^t w_i\alpha_i, y + \sum_{i=1}^t w_i\beta_i\right) &= Tr_1^m \left(\left(y + \sum_{i=1}^t w_i\beta_i\right)\left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i \frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right) \\
&= Tr_1^m \left(\left(y + \sum_{i=1}^t w_i\beta_i\right)\left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i \frac{\alpha_i}{a\lambda}\right)^{2^s} \left(\frac{x}{a\lambda} + \sum_{i=1}^t w_i \frac{\alpha_i}{a\lambda}\right)\right) \\
&= Tr_1^m \left(y\left(\frac{x}{a\lambda}\right)^{2^s+1} + y\frac{x}{a\lambda}\sum_{i=1}^t w_i \left(\frac{\alpha_i}{a\lambda}\right)^{2^s} + y\left(\frac{x}{a\lambda}\right)^{2^s} \sum_{i=1}^t w_i\frac{\alpha_i}{a\lambda} + y\sum_{i=1}^t w_i\left(\frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right. \\
&+ \sum_{i=1}^t w_i\beta_i\left(\frac{x}{a\lambda}\right)^{2^s+1} + \sum_{i=1}^t w_i\beta_i \frac{x}{a\lambda}\sum_{j=1}^t w_j\left(\frac{\alpha_j}{a\lambda}\right)^{2^s} + \sum_{i=1}^t w_i\beta_i\left(\frac{x}{a\lambda}\right)^{2^s}\sum_{j=1}^t w_j\frac{\alpha_j}{a\lambda} \\
&\left.+ \sum_{i=1}^t w_i\beta_i\left(\frac{\alpha_i}{a\lambda}\right)^{2^s+1}\right) = G^*_\lambda(x, y) + \sum_{i=1}^t w_i Tr_1^m \left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right) + \\
&+ \sum_{i=1}^t\sum_{j=1}^t w_i w_j Tr_1^m \left(\frac{1}{(a\lambda)^{2^s+1}}\left(\beta_i\alpha_j x + \beta_i\alpha_j x^{2^s} + \beta_i\alpha_j^2\right)\right) \\
&= G^*_\lambda(x, y) + \sum_{i=1}^t w_i Tr_1^m \left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right) + \\
&+ \sum_{i=1}^t w_i Tr_1^m \left(\frac{1}{(a\lambda)^{2^s+1}}\left(\beta_i\alpha_i x + \beta_i\alpha_i x^{2^s} + \beta_i\alpha_i^2\right)\right) \\
&+ \sum_{1\leq i<j\leq t} Tr_1^m \left((x^{2^s} + x)(\beta_i\alpha_j + \beta_j\alpha_i) + \beta_i\alpha_j^2 + \beta_j\alpha_i^2\right) \\
&= G^*_\lambda(x, y) + \sum_{i=1}^t w_i g_i(x, y) + \sum_{1\leq i<j\leq t} Tr_1^m \left((x^{2^s} + x)(\beta_i\alpha_j + \beta_j\alpha_i) + \beta_i\alpha_j^2 + \beta_j\alpha_i^2\right),
\end{aligned}$$

where g_i is defined by (18). The conclusion follows immediately from the assumption that $\alpha_i\beta_j + \alpha_j\beta_i = 0$ and $Tr_1^m(\beta_i\alpha_j^2 + \beta_j\alpha_i^2) = 0$. □

Corollary 2 *Let s be a positive divisor of m such that m/s is odd. Let $\alpha_1, \ldots, \alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^{s*}}$, $1 \leq t \leq m$. Write $u_i = (\alpha_i, 0)$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that $d(2^s + 1) \equiv 1 \ (mod\ 2^m - 1)$ and $a \in \mathbb{F}_{2^{m*}}$. Then the dual component G^*_λ satisfies (6) with*

$$g_i(x, y) = Tr_1^m\left(\frac{y}{(a\lambda)^{2^s+1}}\left(\alpha_i^2 + \alpha_i x + \alpha_i x^{2^s}\right)\right) \tag{19}$$

Theorem 4 *Let $\alpha_1, \ldots, \alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^{m*}}$, $t|m$. Let $G(x, y) = y\pi(x)$, where π is a linear permutation over $\mathbb{F}_{2^m}$, and let $\mathbf{h}$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function*

$$F(x, y) = y\pi(x) + \mathbf{h}(Tr_1^m(\alpha_1 x), \ldots, Tr_1^m(\alpha_t x)),$$

generated by Construction 1, is a bent vectorial Boolean function.

Proof. The result follows immediately from Theorem 1 and Corollary 1. □

Example 3 *Let $G : \mathbb{F}_{2^4} \times \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined with $G(x, y) = xy$. Let $U = \{1, \beta, \beta^2, \beta^3\}$, where $\beta = \alpha^{17}$, α is a root of the primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{F}_{2^8}[x]$. Let $\mathbf{h} : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ be defined with $\mathbf{h}(X) = X^3$. From Theorem 4, the function*

$$F(x, y) = xy + \left(Tr_1^m(x) + \beta Tr_1^m(\beta x) + \beta^2 Tr_1^m(\beta^2 x) + \beta^3 Tr_1^m(\beta^3 x)\right)^3$$

is a quadratic bent $(8, 4)$-function EA-inequivalent to G.

Theorem 5 *Let s be a positive divisor of m such that m/s is odd. Let $\alpha_1, \ldots, \alpha_t$ be any t linearly independent elements in $\mathbb{F}_{2^{s*}}$, $t|m$. Let $G(x, y) = x\pi(y)$, where $\pi(y) = ay^d$ for a positive integer d such that $d(2^s+1) \equiv 1 \ (mod\ 2^m-1)$ and $a \in \mathbb{F}_{2^{m*}}$, and let $\mathbf{h}$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function*

$$F(x, y) = axy^d + \mathbf{h}(Tr_1^m(\alpha_1 x), \ldots, Tr_1^m(\alpha_t x)),$$

generated by Construction 1, is a bent vectorial Boolean function.

Proof. The result follows immediately from Theorem 1 and Corollary 2. □

5 New families of (n, n)-functions with maximal number of bent components

In 2018 Pott *et al.* [16] proved that an (n, n)-function, $n = 2m$, can have at most $2^n - 2^m$ bent components.

A new infinite class of bent (n, m)-functions of the form

$$F^i_\alpha(x) = Tr^n_m(\alpha x^{2^i}(x + x^{2^k})),$$

where $\alpha \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^n}$. Later, Mesnager et al. [10] presented a class of (n, n)-functions with maximal number of bent components CCZ-inequivalent to F^i_α and this topic was also treated by Zheng et al. [22].

A generic method of generating new vectorial plateaued $(n, m + t)$-functions with maximal number of bent components, where $n = 2m$ and $t > 1$, was given in [22]. More precisely, given a bent (n, m)-function G, under certain conditions, the $(n, m + t)$-function $T_1(x) = (G(x), f_1(x), \ldots, f_t(x))$ is vectorial plateaued if and only if the (n, t)-function $(f_1(x), \ldots, f_t(x))$ is vectorial plateaued. For certain choices of the bent functions G, it was shown that T_1 has the maximal number of bent components. In the same article, they also show that the (n, n)-functions $T_2 = (G(x), Tr^n_1(u_1x), Tr^n_1(u_1x)Tr^n_1(u_2x), \ldots, \prod_{i=1}^m Tr^n_1(u_ix))$, under additional conditions and certain choices of the bent (n, m)-function G, also have the maximal number of bent components.

In the rest of this section, we present a new method to construct (n, n)-functions with maximal number of bent components. We note that the functions T_1 and T_2 above are constructed by extending a bent (n, m)-function G through addition of suitably chosen coordinates, whereas in our method we are summing a bent (n, m)-function G and some (n, n)-function $\mathbf{H}'$.

Construction 2 *Let $u_1, \ldots, u_t$ be t linearly independent elements in $\mathbb{F}_{2^{n*}}$, where $n = 2m$ and $t|m$. Let $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ be any vectorial bent function whose components G_λ, $\lambda \in \mathbb{F}_{2^{m*}}$, satisfy property* (6)*. Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean Function from $\mathbb{F}^t_2$ to $\mathbb{F}_{2^t}$. Generate a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ from G and $\mathbf{h}$ as follows*

$$F(x) = G(x) + \mathbf{H}'(x), \tag{20}$$

where $\mathbf{H}' : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined as $\mathbf{H}'(x) = \gamma\mathbf{h}(Tr^n_1(u_1x), \ldots, Tr^n_1(u_tx))$, where $\gamma \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$. Equivalently, if $\mathbf{h}$ is defined using finite field notation,

$$F(x) = G(x) + \mathbf{H}'(x) = G(x) + \gamma\mathbf{h}(Tr^n_1(u_1x) + \alpha Tr^n_1(u_2x) + \cdots + \alpha^{t-1}Tr^n_1(u_tx)), \tag{21}$$

where α is a primitive element of $\mathbb{F}_{2^t}$.

Theorem 6 *Let F be an (n, n)-function generated by Construction 2. Then F has $2^n - 2^m$ bent components.*

Proof. Let $G(x) = (f_1(x), \ldots, f_m(x))$, where $f_1, \ldots, f_m : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are the coordinates of G. Without loss of generality, we can extend G to an (n, n)-function with $G(x) = (f_1, \ldots, f_m, 0, \ldots, 0)$.

For $\lambda \in \mathbb{F}_{2^n}{}^*$ we have that G_λ is not bent if and only if $Tr_1^n(\lambda G(x)) = 0$. This holds, if $\lambda \notin \mathbb{F}_{2^m}{}^*$. Hence, the number of bent components is $2^n - 1 - (2^m - 1) = 2^n - 2^m$. Let $\lambda \in \mathbb{F}_{2^n}$ such that G_λ is bent. We have that

$$F_\lambda(x) = G_\lambda(x) + Tr_1^n(\lambda \mathbf{H}'(x))$$

is also bent, by the result of Tang et al. and the fact that $Tr_1^n(\lambda \mathbf{H}')$ is a Boolean function. The number of bent components of F equals to the number of bent components of G, which is $2^n - 2^m$. Hence F is an (n, n)-function with maximal number of bent components. □

Theorem 7 *Let $G(x)$ be one of the bent (n, m)-functions in Theorem 1, 4 or 5 and let $\{u_1, \ldots, u_t\}$ (with $t|m$) be its corresponding defining set for the property* (6). *Let $\mathbf{h}(X_1, \ldots, X_t)$ be any vectorial Boolean function from $\mathbb{F}_2^t$ to $\mathbb{F}_{2^t}$. Then the function $F(x) = G(x) + \mathbf{H}'(x)$, generated by Construction 2, is an (n, n)-function with maximal number of bent components.*

Proof. The result follows immediately from Theorem 6 and Construction 2. □

6 Concluding remarks

In this paper we have proposed a generic method to construct vectorial bent (n, m)-functions and several infinite families of vectorial bent functions from the Kasami, Niho, Gold-like monomials and bent vectorial Maiorana-McFarland functions were obtained. By modifying the method, we were also able to give a generic construction for (n, n)-functions with maximal number of bent components. An important question, which has not been answered in this article, is whether these vectorial bent functions are embedded in the known primary classes or alternatively suitable choices of G and $\mathbf{H}$ may provide us with functions that are not included in the known primary classes.

Acknowledgment: Amar Bapić is supported in part by the Slovenian Research Agency (research program P1-0404 and Young Researchers Grant). Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694, N1-1059), and the European Commission for funding the InnoRenew CoE project (Grant Agreement no. 739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Union of the European regional Development Fund).

References

[1] L. Budaghyan and C. Carlet. CCZ-equivalence of bent vectorial functions and related constructions. *Designs, Codes and Cryptography*, 59(1):69–87, 2011.

[2] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. on Inform. Theory*, 52(3): 1141–1152, 2006.

[3] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2): 125–156, 1998.

[4] C. Carlet and S. Mesnager. On Dillon's class h of bent functions, Niho bent functions and o-polynomials. *Journal of Combinatorial Theory, Series A*, 118(8): 2392 – 2410, 2011.

[5] A. Çeşmelioğlu, W. Meidl, and A. Pott. Vectorial bent functions and their duals. *Linear Algebra and its Applications*, 548(1): 305 – 320, 2018.

[6] D. Dong, X. Zhang, L. Qu, and S. Fu. A note on vectorial bent functions. *Information Processing Letters*, 113(22): 866 – 870, 2013.

[7] S. Mesnager. Several New Infinite Families of Bent Functions and Their Duals. *Information Processing Letters*, 60(7): 4397–4407, 2014.

[8] S. Mesnager. Bent vectorial functions and linear codes from o-polynomials. *Designs, Codes and Cryptography*, 77(1): 99–116, 2015.

[9] S. Mesnager. Bent Functions - Fundamentals and Results. *Springer*, 2016.

[10] S. Mesnager, F. Zhang, C. Tang and Y.Zhou. Further study on the maximum number of bent components of vectorial functions. *Designs, Codes and Cryptography*, 87(1): 2597–2610, 2019.

[11] A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial bent functions from multiple terms trace functions. *IEEE Trans. on Inform. Theory*, 60(1): 1337–1347, 2014.

[12] A. Muratović-Ribić, E. Pasalic, and S. Bajrić. Vectorial hyperbent trace functions from the $\mathcal{PS}_{\mathrm{ap}}$ class—their exact number and specification. *IEEE Trans. on Inform. Theory*, 60(1):4408–4413, 2014.

[13] K. Nyberg. Perfect nonlinear s-boxes. In *EUROCRYPT*, 1991.

[14] K. Nyberg. S-boxes and round functions with controllable linearity and differential uniformity. In *Fast Software Encryption: Second International Workshop. Leuven, Belgium, 14-16 December 1994, Proceedings*, pages 111–130, 1994.

[15] E. Pasalic and W. Zhang. On multiple output bent functions. *Information Processing Letters*, 112(1): 811–815, 2012.

[16] A. Pott, E. Pasalic, A. Muratović-Ribić, and S. Bajrić. On the maximum number of bent components of vectorial functions. *IEEE Trans. on Inform. Theory*, 64(1): 403–411, 2018.

[17] O. Rothaus. On "bent" functions. *Journal of Combinatorial Theory, Series A*, 20(3): 300 – 305, 1976.

[18] C. Tang, Z. Zhou, Y. Qi, X. Zhang, C. Fan, and T. Helleseth. Generic construction of bent functions and bent idempotents with any possible algebraic degrees. *IEEE Trans. on Inform. Theory*, 63(10): 6149–6157, 2017.

[19] N. Tokareva. Bent functions: Results and applications to cryptography. *Academic Press*, 2015.

[20] Y. Xu, C. Carlet, S. Mesnager, and C. Wu. Classification of bent monomials, constructions of bent multinomials and upper bounds on the nonlinearity of vectorial functions. *IEEE Trans. on Inform. Theory*, 64(1): 367–383, 2018.

[21] L. Zheng, J. Peng, H. Kan, L. Jun, and J. Luo. On constructions and properties of (n, m)-functions with maximal number of bent components. *Designs, Codes and Cryptography*, 88(1): 2171-–2186, 2020.

[22] L. Zheng, J. Peng, H. Kan, and Y. Li. Constructing vectorial bent functions via second-order derivatives. *CoRR*, abs/1905.10508, 2019.