ON VECTORIAL FUNCTIONS WITH MAXIMAL NUMBER OF BENT COMPONENTS

XIANHONG XIE[1], YI OUYANG[2,3]

Abstract. We study vectorial functions with maximal number of bent components in this paper. We first give a construction of such functions from known ones, thus obtain two new classes from the Niho class and the Maiorana-McFarland class. Our construction gives a partial answer to an open problem proposed by Pott et al., and also solves an open problem proposed by Mesnager. We then show that the vectorial function $F: \mathbb{F}_{2^{2m}} \rightarrow \mathbb{F}_{2^{2m}}$, $x \mapsto x^{2^m+1} + x^{2^i+1}$ has maximal number of bent components if and only if $i = 0$.

Keywords Vectorial bent functions, Vectorial functions, Bent components, Niho quadratic function, Maiorana-McFarland class.

1. Introduction

Bent functions, as a special class of Boolean functions, were introduced by Rothaus [1] and have been extensively studied (see [2, 3, 4, 5, 6, 7, 8, 9]) due to their important applications in cryptography, coding theory and combinatorics.

The bentness of Boolean functions can be extended to a general vectorial function $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^k}$ by requesting all component functions $f_c(x) = \mathrm{Tr}_{2^k/2}(cF(x))$ ($c \in \mathbb{F}_{2^k}^*$) of F to be bent. Nyberg [10] showed that vectorial bent functions can only exist if n is even and $n \geq 2k$, and presented two different constructions of such functions from known classes of bent functions. The reader can refer to [11, 12, 13, 14, 15, 16, 17, 18] for more constructions of vectorial bent functions. However, relatively little work was done to construct bent functions from known vectorial bent functions. In this direction, Mesnager [19] proved the following result:

Theorem. *If $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^k}$ is a vectorial bent function, and $c_1, c_2, c_3 \in \mathbb{F}_{2^k}^*$ satisfying $c_1+c_2+c_3 \neq 0$ and $f_{c_1}^* + f_{c_2}^* + f_{c_3}^* = f_{c_1+c_2+c_3}^*$, then $f_{c_1}f_{c_2} + f_{c_1}f_{c_3} + f_{c_2}f_{c_3}$ is bent and its dual is $f_{c_1}^*f_{c_2}^* + f_{c_1}^*f_{c_3}^* + f_{c_2}^*f_{c_3}^*$.*

She raised an open problem to find vectorial bent functions satisfying the above condition.

Another interesting and important question in studying bentness of vectorial functions is that how large the number of bent components of a vectorial function could be. Suppose $F: \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^k}$ is a vectorial function. Nyberg's condition [10] is equivalent to that the possible maximum $2^k - 1$ can be attained only if n is even and $k \leq \frac{n}{2}$. For $k \geq \frac{n}{2}$, Zheng et al. [20] showed that this number is at

---

2020 *Mathematics Subject Classification.* 11T71, 94A60.

Corresponding author: Yi Ouyang (yiouyang@ustc.edu.cn).

Partially supported by Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302904) and Anhui Initiative in Quantum Information Technologies (Grant No. AHY150200).

most $2^k - 2^{k-\frac{n}{2}}$ and presented a class of vectorial functions with $2^k - 2^{k-\frac{n}{2}}$ bent components. The special case $k = n$ was proved by Pott et al. [21], where a class of binomial functions attaining the upper bound was presented. Further, Pott et al. [21] raised the following problem:

Problem 1. *Determine all linear mappings $\ell(x)$ over $\mathbb{F}_{2^n}$ such that the number of bent components of $x\ell(x)$ is $2^n - 2^{\frac{n}{2}}$.*

Let $n = k = 2m$. There are four known classes of vectorial functions from $\mathbb{F}_{2^n}$ to itself with $2^n - 2^m$ bent components:

(a) $F(x) = x^{2^m+1}$ ([22]);
(b) $F(x) = x^{2^i}(x + x^{2^m}) = x^{2^i}\mathrm{Tr}_{2^n/2^m}(x)$, $0 \le i \le n-1$ ([21]);
(c) $F(x) = x^{2^i}(\mathrm{Tr}_{2^n/2^m}(x) + \sum_{j=1}^{\rho} \gamma^{(j)}\mathrm{Tr}_{2^n/2^m}(x)^{2^{t_j}})$, where $\gamma^{(j)} \in \mathbb{F}_{2^m}, \rho \le m$ such that $\sum_{j=1}^{\rho}(\gamma^{(j)})^{2^{m-t_j}} z^{2^{k-t_j}-1} + 1 \neq 0$ and $\sum_{j=1}^{\rho}(\gamma^{(j)})^{2^{m-j}} z^{2^{t_j}-1} + 1 \neq 0$ for any $x \in \mathbb{F}_{2^m}$ ([18]);
(d) $F(x) = xh(\mathrm{Tr}_{2^n/2^m}(x))$, where $h : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ is a permutation ([20]).

We note that functions in (a) and (b) are of the form $x\ell(x)$.

We shall work on vectorial functions from $\mathbb{F}_{2^n}$ to itself with maximal number of bent components in this paper. Our main contributions are:

(A) We present two new classes of vectorial functions from $\mathbb{F}_{2^n}$ to itself with maximal number of bent components via the Niho quadratic function and the Maiorana–McFarland class. Moreover,
- From the Niho quadratic function, we obtain a new class of quadratic vectorial functions of the form
$$F(x) = x^{2^m+1} + u_1 x\mathrm{Tr}_{2^n/2}(u_2 x) = x\ell(x),$$
where $u_1, u_2 \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$ satisfying $u_1^{2^m} u_2 \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_{2^m/2}(u_1^{2^m} u_2) = 0$. This gives a partial answer to Problem 1.
- From the Maiorana–McFarland class, we obtain a family of vectorial bent functions and find three distinct bent components G_{c_1}, G_{c_2}, G_{c_3} such that $G_{c_1}^* + G_{c_2}^* + G_{c_3}^* = G_c^*$, where $c_1, c_2, c_3 \in \mathbb{F}_{2^m}^*$ and $c = c_1 + c_2 + c_3 \neq 0$, so that the conditions of Mesnager [19] are satisfied.

(B) We prove that the binomial vectorial function $F(x) = x^{2^m+1} + x^{2^i+1}$ ($0 \le i \le m-1$) has $2^n - 2^m$ bent components if and only if $i = 0$.

2. Preliminaries

2.1. **Basic Notations.** Let n and k be positive integers. For $k \mid n$, the trace function from $\mathbb{F}_{2^n}$ to its subfield $\mathbb{F}_{2^k}$ is $\mathrm{Tr}_{2^n/2^k}(x) = \sum_{i=0}^{\frac{n}{k}-1} x^{2^{ki}}$.

For a finite dimensional $\mathbb{F}_2$-vector space V, we always fix a non-degenerate inner product $\langle\ ,\ \rangle = \langle\ ,\ \rangle_V$ on V. In particular, if $V = \mathbb{F}_2^n$, we let
$$\langle (v_i), (w_i) \rangle = \sum_{i=1}^{n} v_i w_i;$$
If $V = \mathbb{F}_{2^n}$, let
$$\langle \omega, x \rangle = \mathrm{Tr}_{2^n/2}(\omega x).$$

For W a subspace of V, let $W^{\perp} = \{v \in V, \langle v, w\rangle = 0 \text{ for all } w \in W\}$ be the orthogonal complementary of W, then $\dim W^{\perp} = \dim V - \dim W$.

For a vectorial function $F : V \to W$, the component function of F at $w \in W$ is the function $F_w : v \to \mathbb{F}_2$, $v \mapsto \langle w, F(v)\rangle_W$.

2.2. **Bent and vectorial bent functions.** We call $F : V \to \mathbb{F}_2$ a Boolean function where V is a finite dimensional $\mathbb{F}_2$-vector space. In particular, if $V = \mathbb{F}_2^n$, then F is represented by a unique reduced polynomial $R(X_1, X_2, \cdots, X_n)$ over $\mathbb{F}_2$.

The Walsh transform of $F : V \to \mathbb{F}_2$ is

$$W_F(w) = \sum_{v\in V}(-1)^{F(v)+\langle w,v\rangle},\ w \in V, \tag{1}$$

its inverse Walsh transform is

$$(-1)^{F(v)} = \frac{1}{2^{\dim V}}\sum_{w\in V} W_F(w)(-1)^{\langle w,v\rangle}. \tag{2}$$

In particular, if $V = \mathbb{F}_2^n$, the Walsh transform of F is

$$W_F(w_1, \cdots, w_n) = \sum_{(v_1,\cdots,v_n)\in\mathbb{F}_2^n}(-1)^{F(v_1,\cdots,v_n)+\sum\limits_{i=1}^{n} w_i v_i}, \tag{3}$$

its inverse Walsh transform is

$$(-1)^{F(v_1,\cdots,v_n)} = \frac{1}{2^n}\sum_{(w_1,\cdots,w_n)\in\mathbb{F}_2^n} W_F(w_1, \cdots, w_n)(-1)^{\sum\limits_{i=1}^{n} w_i v_i}; \tag{4}$$

if $V = \mathbb{F}_{2^n}$, the Walsh transform of F is

$$W_F(\omega) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{F(x)+\mathrm{Tr}_{2^n/2}(\omega x)}, \tag{5}$$

its inverse Walsh transform is

$$(-1)^{F(x)} = \frac{1}{2^n}\sum_{w\in\mathbb{F}_{2^n}} W_F(w)(-1)^{\mathrm{Tr}_{2^n/2}(wx)}. \tag{6}$$

Definition 1. *A Boolean function $F : V \to \mathbb{F}_2$ is called bent if $W_F(w) = \pm 2^{\frac{\dim V}{2}}$ for all $w \in V$.*

The dual of a bent function F, denoted as F^*, is defined via the equality

$$W_F(w) = 2^{\frac{\dim V}{2}}(-1)^{F^*(w)}.$$

Lemma 1. *A Boolean function $F : V \to \mathbb{F}_2$ is bent if and only if its first derivative*

$$D_aF(v) = F(v + a) + F(v)$$

in the direction of a is balanced for all $0 \neq a \in V$.

For a vectorial function $F : V \to W$, the Walsh transform $W_F(a,)$ of F is

$$W_F(a, \omega) = W_{F_a}(\omega) = \sum_{v\in V}(-1)^{F_a(v)+\langle\omega,v\rangle}, \quad a \in W - \{0\}, \omega \in V.$$

In particular, if $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^k}$, the Walsh transform $W_F(a, \omega)$ of F is

$$W_F(a, \omega) = W_{F_a}(\omega) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}_{2^k/2}(aF(x))+\mathrm{Tr}_{2^n/2}(\omega x)}, \quad a \in \mathbb{F}_{2^n}^*, \omega \in \mathbb{F}_{2^n},$$

Definition 2. *A vectorial Boolean function* $F: V \to W$ *is called bent if* $W_F(a,\omega) = W_{F_a}(\omega) = \pm 2^{\frac{\dim V}{2}}$ *for any* $a \in W - \{0\}$ *and* $\omega \in V$*, i.e., its component functions* F_a *for all* $a \neq 0$ *are bent.*

Lemma 2 ([10])**.** *If* $F: V \to W$ *is a vectorial bent function, then* $\dim V$ *is even and* $\dim W \leq \frac{\dim V}{2}$.

2.3. **Bent components.**

Proposition 1. *Let* $n = 2m = \dim V$ *and* $F: V \to V$ *be a vectorial function. Set*

$$S_F := \{v \in V: \ F_v \text{ is not bent}\}.$$

Then

(1) (*Pott et al.* [21]) $|S_F| \geq 2^m$*, and* $|S_F| = 2^m$ *if and only if* S_F *is an* m*-dimensional* $\mathbb{F}_2$*-subspace of* V.
(2) (*Hu et al.*[22]) *Moreover, if* $V = \mathbb{F}_{2^n}$ *and* $|S_F| = 2^m$*, then* $S_F = \mathbb{F}_{2^m}$.

3. Construction of Vectorial Functions With Maximum Number of Bent Components

Assume $n = 2m$. The main goal of this section is to construct vectorial functions from V of dimension n to itself with maximal number of bent components.

3.1. **A Generic construction.** This construction is inspired by recent work of Mesnager [19] and Tang et al. [3].

Definition 3. *Suppose* $f: V \to \mathbb{F}_2$ *and* $\{u_1, u_2, \ldots, u_k\} \subseteq V$ *for* $2 \leq k \leq n$*. We say that* $(f; u_1, \cdots, u_k)$ *satisfies Condition* **A** *if* $f(x)$ *is a bent function and*

$$D_{u_i} D_{u_j} f^*(x) = 0 \quad \text{for all pairs} \quad 1 \leq i < j \leq k. \tag{7}$$

Eq. (7) means that $f^*(x + u_i + u_j) = f^*(x + u_i) + f^*(x + u_j) + f^*(x)$. By induction, for any $(w_1, w_2, \cdots, w_k) \in \mathbb{F}_2^k$, one has

$$f^*(x + \sum_{i=1}^{k} w_i u_i) = f^*(x) + \sum_{i=1}^{k} w_i D_{u_i} f^*(x). \tag{8}$$

Theorem 1. *Suppose* $G: V \to V$, $0 \neq \beta \in V$, $2 \leq k \leq n$ *and* $\{u_1, u_2, \ldots, u_k\} \subseteq V$ *such that* $(G_\beta(x); u_1, \cdots, u_k)$ *satisfies Condition* **A**. *Then for any reduced polynomial* $H(X_1, \cdots, X_k)$ *over* $\mathbb{F}_2$*, the function*

$$F_\beta(x) := G_\beta(x) + H(\langle u_1, x\rangle, \cdots, \langle u_k, x\rangle) \tag{9}$$

is a bent function, whose dual is

$$F_\beta^*(x) = G_\beta^*(x) + H(D_{u_1} G_\beta^*(x), \cdots, D_{u_k} G_\beta^*(x)).$$

Our proof of this theorem is almost identical to that of [3, Theorem 8], which we include here for completeness.

Proof. Applying the inverse Walsh transform to the Boolean function $H: \mathbb{F}_2^k \to \mathbb{F}_2$ defined by $H(X_1, \cdots, X_k)$, we get

$$(-1)^{H(X_1, X_2, \cdots, X_k)} = \frac{1}{2^k} \sum_{(w_1, \cdots, w_k) \in \mathbb{F}_2^k} W_H(w_1, \cdots, w_k)(-1)^{\sum_{i=1}^{k} w_i X_i}. \tag{10}$$

Take $X_i = x_i = \langle u_i, x\rangle$ for $1 \le i \le k$ and then multiply both sides of the above identity by $(-1)^{G_\beta(x)+\langle\omega,x\rangle}$, note that $\sum_{i=1}^k w_i x_i = \langle \sum_{i=1}^k w_i u_i, x\rangle$, we get

$$\begin{aligned}&(-1)^{G_\beta(x)+H(x_1,\cdots,x_k)+\langle\omega,x\rangle}\\ &\qquad= \frac{1}{2^k}\sum_{(w_1,\cdots,w_k)\in\mathbb{F}_2^k} W_H(w_1,\cdots,w_k)(-1)^{G_\beta(x)+\langle\omega+\sum_{i=1}^k w_iu_i,x\rangle},\end{aligned}$$

which leads to

$$\begin{aligned}W_{F_\beta}(\omega) &= \sum_{x\in V}(-1)^{G_\beta(x)+H(x_1,\cdots,x_k)+\langle\omega,x\rangle}\\ &= \frac{1}{2^k}\sum_{x\in V}\sum_{(w_1,\cdots,w_k)\in\mathbb{F}_2^k} W_H(w_1,\cdots,w_k)(-1)^{G_\beta(x)+\langle\omega+\sum_{i=1}^k w_iu_i,x\rangle}\\ &= \frac{1}{2^k}\sum_{(w_1,\cdots,w_k)\in\mathbb{F}_2^k} W_H(w_1,\cdots,w_k)W_{G_\beta}(\omega+\sum_{i=1}^k w_iu_i).\end{aligned}$$

By definition of the dual of a bent function, then

$$\begin{aligned}W_{F_\beta}(\omega) &= \frac{2^m}{2^k}\sum_{(w_1,\cdots,w_k)\in\mathbb{F}_2^k} W_H(w_1,\cdots,w_k)(-1)^{G_\beta^*(\omega+\sum_{i=1}^k w_iu_i)}\\ &= \frac{2^m}{2^k}(-1)^{G_\beta^*(\omega)}\sum_{(w_1,\cdots,w_k)\in\mathbb{F}_2^k} W_H(w_1,\cdots,w_k)(-1)^{\sum_{i=1}^k w_iD_{u_i}G_\beta^*(\omega)}.\end{aligned}$$

This together with (10) yields

$$W_{F_\beta}(\omega) = 2^m(-1)^{G_\beta^*(\omega)+H(D_{u_1}G_\beta^*(\omega),D_{u_2}G_\beta^*(\omega),\cdots,D_{u_k}G_\beta^*(\omega))}.$$

Hence F_β is bent and

$$F_\beta^*(x) = G_\beta^*(x) + H(D_{u_1}G_\beta^*(x),\cdots,D_{u_k}G_\beta^*(x)). \qquad \square$$

3.2. **Construction via the Niho quadratic function.** Take $V = \mathbb{F}_{2^n}$ with the inner product given by the trace map. By Proposition 1 and Theorem 1, we have

Theorem 2. *Suppose $G : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ has $2^n - 2^m$ bent components. Suppose $2 \le k \le n$ and $\{u_1,\cdots,u_k\} \subseteq \mathbb{F}_{2^n}$ such that $(G_\beta(x); u_2,\cdots,u_k)$ satisfies Condition* **A** *and $D_{\beta u_1}D_{u_j}G_\beta^*(x) = 0$ for $1 < j \le k$ for all $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$. Then for any reduced polynomial $R(X_2,\cdots,X_k)$ over $\mathbb{F}_2$, the vectorial function*

$$F(x) := G(x) + u_1xR(\mathrm{Tr}_{2^n/2}(u_2x),\mathrm{Tr}_{2^n/2}(u_3x),\cdots,\mathrm{Tr}_{2^n/2}(u_kx)) \qquad (11)$$

has $2^n - 2^m$ bent components. Furthermore, the component $F_\beta(x) = \mathrm{Tr}_{2^n/2}(\beta F(x))$ is bent and its dual

$$F_\beta^*(x) = G_\beta^*(x) + D_{\beta u_1}G_\beta^*(x)R(D_{u_2}G_\beta^*(x),\cdots,D_{u_k}G_\beta^*(x)).$$

Remark 1. (1) Comparing with the constructions in [21, 20], the vectorial function constructed by Theorem 2 is new and its dual is explicitly given.

(2) Comparing with the constructions presented in [3] and [27], the vectorial functions with maximal number of bent components by our construction can have high algebraic degrees if we choose the reduced polynomial R with high algebraic degree

and $u_1, u_2, \ldots, u_k$ linearly independent over $\mathbb{F}_2$, in this case the algebraic degree of $R(\mathrm{Tr}_{2^n/2}(u_1x), \ldots, \mathrm{Tr}_{2^n/2}(u_kx))$ is equal to the algebraic degree of $R(X_1, \ldots, X_k)$ (see [3]).

From now on in this subsection, let $G(x) = x^{2^m+1}$. For $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, let

$$\gamma = \beta + \beta^{2^m} \in \mathbb{F}_{2^m}^*.$$

The component function of G at β is the monomial Niho quadratic function

$$G_\beta : x \in \mathbb{F}_{2^n} \mapsto \mathrm{Tr}_{2^n/2}(\beta x^{2^m+1}). \tag{12}$$

It is a bent function (see [19]) and its dual G_β^* is given by

$$G_\beta^*(x) = \mathrm{Tr}_{2^m/2}(\gamma^{-1}x^{2^m+1}) + 1. \tag{13}$$

To apply Theorem 2, we first show that the function $G_\beta(x)$ satisfies Condition **A** when $u_1, u_2, \cdots, u_k$ are appropriately chosen.

Lemma 3. *Suppose $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, $k \le m$ and $\{u_1, u_2, \cdots, u_k\} \subseteq \mathbb{F}_{2^n}$ such that $\mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}u_i) = 0$ for all $1 \le i < j \le k$. Then $(G_\beta(x); u_1, \cdots, u_k)$ satisfies Condition* **A** *and for $1 \le j \le k$,*

$$D_{u_j}G_\beta^*(x) = \mathrm{Tr}_{2^n/2}(\gamma^{-1}xu_j^{2^m}) + \mathrm{Tr}_{2^m/2}(\gamma^{-1}u_j^{2^m+1}).$$

Proof. By Eq. (13), the derivative of $G_\beta^*(x)$ in the direction of $u_j \in \mathbb{F}_{2^n}$ is

$$\begin{aligned} D_{u_j}G_\beta^*(x) &= \mathrm{Tr}_{2^m/2}(\gamma^{-1}x^{2^m+1}) + 1 + \mathrm{Tr}_{2^m/2}(\gamma^{-1}(x+u_j)^{2^m+1}) + 1 \\ &= \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}x) + \mathrm{Tr}_{2^m/2}(\gamma^{-1}u_j^{2^m+1}). \end{aligned}$$

Then the second order derivative in the direction of (u_i, u_j) is

$$\begin{aligned} D_{u_i}D_{u_j}G_\beta^*(x) &= D_{u_j}G_\beta^*(x+u_i) + D_{u_j}G_\beta^*(x) \\ &= \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}x) + \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}(x+u_i)) \\ &= \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}u_i) = 0, \end{aligned}$$

with the last equality followed by our assumption. □

By Lemma 3 and Theorem 1, then we have

Theorem 3. *Let $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$ and $G_\beta(x) = \mathrm{Tr}_{2^n/2}(\beta x^{2^m+1})$. If $k \le m$ and $\{u_1, u_2, \cdots, u_k\} \subseteq \mathbb{F}_{2^n}$ satisfying $\mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j^{2^m}u_i) = 0$ for any $1 \le i < j \le k$, then the function*

$$F_\beta(x) := G_\beta(x) + \mathrm{Tr}_{2^n/2}(u_1x)R(\mathrm{Tr}_{2^n/2}(u_2x), \cdots, \mathrm{Tr}_{2^n/2}(u_kx)) \tag{14}$$

where $R(X_2, \cdots, X_n)$ is any reduced polynomial over $\mathbb{F}_2$, is bent and its dual is

$$F_\beta^*(x) = G_\beta^*(x) + D_{u_1}G_\beta^*(x)R(D_{u_2}G_\beta^*(x), \cdots, D_{u_k}G_\beta^*(x)).$$

Our first construction of vectorial functions with maximal number of bent components is the following result:

Theorem 4. *Let $3 \le k \le m$ and $\{u_1, u_2, \cdots, u_k\} \subseteq \mathbb{F}_{2^m}$ satisfy $\mathrm{Tr}_{2^m/2}(u_1u_j) = 0$ for $j \ge 2$. Then for any reduced polynomial $R(X_2, \cdots, X_k)$ over $\mathbb{F}_2$,*

$$F(x) = x^{2^m+1} + u_1xR(\mathrm{Tr}_{2^n/2}(u_2x), \mathrm{Tr}_{2^n/2}(u_3x), \cdots, \mathrm{Tr}_{2^n/2}(u_kx)),$$

has $2^n - 2^m$ bent components. More precisely, for $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, F_β is bent and

$$F_\beta^*(x) = G_\beta^*(x) + D_{\beta u_1}G_\beta^*(x)R(D_{u_2}G_\beta^*(x), \cdots, D_{u_k}G_\beta^*(x)).$$

Proof. Since $u_i \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_{2^m/2}(u_1u_j) = 0$, we have $\gamma^{-1}u_ju_i \in \mathbb{F}_{2^m}$,

$$D_{u_i}D_{u_j}G^*_\beta(x) = \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_ju_i) = 0,\ 2 \le i < j \le k \le m,$$

and

$$D_{\beta u_1}D_{u_j}G^*_\beta(x) = \mathrm{Tr}_{2^n/2}(\gamma^{-1}u_j\beta u_1) = \mathrm{Tr}_{2^m/2}(u_ju_1) = 0,\ 2 \le j \le k.$$

Therefore, $(g_\beta(x); \beta u_1, u_2, \ldots, u_k)$ satisfies $\mathbf{A}$ for any $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$. □

Remark 2. In Theorem 4, if we take $\{u_i : 1 \le i \le m\}$ to be an orthogonal basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ under the inner product $\langle x, y\rangle = \mathrm{Tr}_{2^m/2}(xy)$, and take the polynomial $R(X_2, \ldots, X_m) = X_2 \cdots X_m$, then the function

$$F(x) = x^{2^m+1} + u_1x\prod_{i=2}^{m}\mathrm{Tr}_{2^n/2}(u_ix)$$

has maximal algebraic degree m and maximal number of bent compnents $2^n - 2^m$.

For $k = 2$, we have the following result.

Theorem 5. *Suppose $u_1, u_2 \in \mathbb{F}_{2^n}$ such that $u_1u_2^{2^m} \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_{2^m/2}(u_1u_2^{2^m}) = 0$. Then*

$$F(x) = x^{2^m+1} + u_1x\mathrm{Tr}_{2^n/2}(u_2x)$$

has $2^n - 2^m$ bent components: for $\beta \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, F_β is bent and

$$\begin{aligned}F^*_\beta(x) =&\mathrm{Tr}_{2^m/2}(\lambda^{-1}x^{2^m+1}) + 1 + \big(\mathrm{Tr}_{2^n/2}(\lambda^{-1}(\beta u_1)^{2^m}x) + \mathrm{Tr}_{2^m/2}(\lambda^{-1}(\beta u_1)^{2^m+1})\big)\\ &\times\big(\mathrm{Tr}_{2^n/2}(\lambda^{-1}u_2^{2^m}x) + \mathrm{Tr}_{2^m/2}(\lambda^{-1}u_2^{2^m+1})\big).\end{aligned}$$

Note that the function $F(x)$ given by Theorem 5 is of the form $x\ell(x)$, thus is a solution of Problem 1. We now show it is not equivalent to the functions in cases (a) and (b) in the introduction. Recall for a vectorial function F and $a, b \in V$, $\delta_F(a, b) := |\{x \in \mathbb{F}_{2^n} :\ F(x + a) + F(x) = b\}|$. The differential spectrum of F is

$$\{\delta_F(a, b) :\ a \in \mathbb{F}^*_{2^n},\ b \in \mathbb{F}_{2^n}\}.$$

It was shown in [23] and [21] respectively that

$$\delta_{x^{2^m+1}}(a, b) \in \{0, 2^m\} \text{ and } \delta_{x^{2^i}(1+x^{2^m})}(a, b) \in \{0, 2^{\gcd(i,m)}, 2^m\}\ (0 < i < m).$$

Then the inequivalence of our function in Theorem 5 to theirs follows from

Theorem 6. *Suppose $u_1, u_2 \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, $u_1u_2^{2^m} \in \mathbb{F}_{2^m}$ and $\mathrm{Tr}_{2^m/2}(u_1u_2^{2^m}) = 0$. Then the differential spectrum of $F(x) = x^{2^m+1} + u_1x\mathrm{Tr}_{2^n/2}(u_2x)$ is given by*

$$\delta_F(a, b) \in \begin{cases}\{0, 2\}, & \text{if } \ \mathrm{Tr}_{2^n/2}(u_2a) = 1,\\ \{0, 2^{m-1}, 2^m\}, & \text{if } \ \mathrm{Tr}_{2^n/2}(u_2a) = 0.\end{cases}$$

Proof. We have

$$\begin{aligned}&F(x + a) + F(x)\\ &\qquad = x^{2^m}a + xa^{2^m} + a^{2^m+1} + u_1x\mathrm{Tr}_{2^n/2}(u_2a) + u_1a\mathrm{Tr}_{2^n/2}(u_2(x + a)).\end{aligned}$$

Notice that if x is a solution of $F(x + a) + F(x) = b$, so is $x + a$.

(A) Assume $\mathrm{Tr}_{2^n/2}(u_2a) = 1$. The equation $F(x + a) + F(x) = b$ is reduced to

$$x^{2^m}a + xa^{2^m} + a^{2^m+1} + u_1x + u_1a\mathrm{Tr}_{2^n/2}(u_2x) + u_1a = b, \tag{15}$$

and then to one of the following two systems of equations:

$$\begin{cases} x^{2^m}a + xa^{2^m} + u_1x = b + a^{2^m+1} + u_1a, \\ \mathrm{Tr}_{2^n/2}(u_2x) = 0; \end{cases} \qquad \begin{cases} x^{2^m}a + xa^{2^m} + u_1x = b + a^{2^m+1}, \\ \mathrm{Tr}_{2^n/2}(u_2x) = 1. \end{cases}$$

We claim that $x^{2^m}a + xa^{2^m} + u_1x$ is a permutation over $\mathbb{F}_{2^n}$. Then $\delta_F(a,b) \in \{0,2\}$ follows from the claim immediately.

For $x, y \in \mathbb{F}_{2^n}$, let

$$x^{2^m}a + xa^{2^m} + u_1x = y^{2^m}a + ya^{2^m} + u_1y.$$

Set $z = \mathrm{Tr}_{2^n/2^m}(xa^{2^m}) - \mathrm{Tr}_{2^n/2^m}(ya^{2^m}) \in \mathbb{F}_{2^m}$, then $y = x + u_1^{-1}z$ and

$$\begin{aligned} &z = \mathrm{Tr}_{2^n/2^m}(xa^{2^m} - ya^{2^m}) = -\mathrm{Tr}_{2^n/2^m}(a^{2^m}u_1^{-1}z) = -z\mathrm{Tr}_{2^n/2^m}(a^{2^m}u_1^{-1}) \\ &\quad \Rightarrow z(1 + \mathrm{Tr}_{2^n/2^m}(a^{2^m}u_1^{-1})) = 0. \end{aligned}$$

Suppose $\mathrm{Tr}_{2^n/2^m}(a^{2^m}u_1^{-1}) = 1$. Notice that $u_1^{2^m}u_2 \in \mathbb{F}_{2^m}^*$ and $au_1^{-2^m} = \frac{au_2}{u_1^{2^m}u_2}$, thus

$$\begin{aligned} \mathrm{Tr}_{2^n/2^m}(a^{2^m}u_1^{-1}) = \mathrm{Tr}_{2^n/2^m}(au_1^{-2^m}) = \mathrm{Tr}_{2^n/2^m}\left(\frac{au_2}{u_1^{2^m}u_2}\right) = \frac{\mathrm{Tr}_{2^n/2^m}(au_2)}{u_1^{2^m}u_2} = 1 \\ \Rightarrow \mathrm{Tr}_{2^n/2^m}(au_2) = u_1^{2^m}u_2. \end{aligned}$$

Since $\mathrm{Tr}_{2^n/2}(u_2a) = 1$, we have $\mathrm{Tr}_{2^n/2}(u_2a) = \mathrm{Tr}_{2^m/2}(u_1^{2^m}u_2) = 1$, which is a contradiction to the assumption $\mathrm{Tr}_{2^m/2}(u_1^{2^m}u_2) = 0$. Thus $z = 0$ and $x^{2^m}a + xa^{2^m} + u_1x$ is a linear permutation over $\mathbb{F}_{2^n}$.

(B) Assume $\mathrm{Tr}_{2^n/2}(u_2a) = 0$. The equation $F(x+a) + F(x) = b$ is reduced to

$$x^{2^m}a + xa^{2^m} + a^{2^m+1} + u_1a\mathrm{Tr}_{2^n/2}(u_2x) = b. \tag{16}$$

Assume that x, y are two solutions of (16). Then

$$x^{2^m}a + xa^{2^m} + a^{2^m+1} + u_1a\mathrm{Tr}_{2^n/2}(u_2x) = b, \tag{17}$$

$$y^{2^m}a + ya^{2^m} + a^{2^m+1} + u_1a\mathrm{Tr}_{2^n/2}(u_2y) = b, \tag{18}$$

which means that $z = x + y$ is a solution of

$$z^{2^m}a + za^{2^m} + u_1a\mathrm{Tr}_{2^n/2}(u_2z) = 0. \tag{19}$$

or equivalently,

$$\begin{cases} z^{2^m}a + za^{2^m} = 0, \\ \mathrm{Tr}_{2^n/2}(u_2z) = 0; \end{cases} \quad \text{or} \quad \begin{cases} z^{2^m}a + za^{2^m} = u_1a, \\ \mathrm{Tr}_{2^n/2}(u_2z) = 1. \end{cases}$$

Thus $\delta_F(a,b) = 0$ or the number of solutions of these two systems of equations.

Let $X_u = \{x \in \mathbb{F}_{2^n} : \mathrm{Tr}_{2^n/2}(ux) = 0\}$. The zero set of the first system of equations is the $\mathbb{F}_2$-vector space $a^{-2^m}\mathbb{F}_{2^m} \cap X_{u_2}$. Note that $\dim_{\mathbb{F}_2} a^{-2^m}\mathbb{F}_{2^m} = m$ and $\dim_{\mathbb{F}_2} X_{u_2} = n-1$, $a^{-2^m}\mathbb{F}_{2^m} \cap X_{u_2}$ must be of dimension either $m-1$ or m.

For the second system, note that $z^{2^m}a + za^{2^m} \in \mathbb{F}_{2^m}$, we must have $u_1a \in \mathbb{F}_{2^m}$. Hence $u_2a^{-2^m} = \frac{u_1^{2^m}u_2}{(u_1a)^{2^m}} \in \mathbb{F}_{2^m}$. The solution of $z^{2^m}a + za^{2^m} = u_1a$ is $z = \frac{u_1a}{a^{2^m}(1+\xi)}$

with $\xi^{2^m+1} = 1$. Then

$$\begin{aligned}\mathrm{Tr}_{2^n/2}(u_2 z) &= \mathrm{Tr}_{2^n/2}\Big(\frac{u_2 u_1 a}{a^{2^m}(1+\xi)}\Big) = \mathrm{Tr}_{2^n/2}\Big(\frac{u_2 a^{-2^m} u_1 a}{1+\xi}\Big)\\ &= \mathrm{Tr}_{2^m/2}(u_2 a^{-2^m} u_1 a) = \mathrm{Tr}_{2^m/2}(u_2 u_1^{2^m}) = 0.\end{aligned}$$

Hence the second system has no zeroes at all. □

3.3. **Construction via the Maiorana-MacFarland class.** In this case, we let $V = \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ and the corresponding inner product be

$$\langle (y_1, z_1), (y_2, z_2)\rangle = \mathrm{Tr}_{2^m/2}(y_1 y_2) + \mathrm{Tr}_{2^m/2}(z_1 z_2).$$

Let ϕ be a permutation of $\mathbb{F}_{2^m}$, and G be the associated map defined by

$$\begin{aligned} G : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} &\longrightarrow \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}\\ (y, z) &\longmapsto (y\phi(z), z).\end{aligned}$$

Then G has maximal number of bent components: for $(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$, the component function

$$G_{a,b}(y, z) = \mathrm{Tr}_{2^m/2}(ay\phi(z) + bz), \tag{20}$$

at (a, b) is a bent function in the Maiorana- MacFarland class, whose dual

$$G^*_{a,b}(y, z) = \mathrm{Tr}_{2^m/2}((z + b)\phi^{-1}(a^{-1}y)). \tag{21}$$

We assume ϕ is an automorphism of $\mathbb{F}_{2^m}$ from now on in this subsection.

Theorem 7. *Let $2 \le k \le m$, $(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$, ϕ and G be given as above. If the set $\{u_i = (u_{i,1}, u_{i,2}) \in V : 1 \le i \le k\}$ satisfies*

$$\mathrm{Tr}_{2^m/2}\big(u_{j,2}\phi^{-1}(a^{-1}u_{i,1}) + u_{i,2}\phi^{-1}(a^{-1}u_{j,1})\big) = 0 \textit{ for all } \ 1 \le i < j \le k,$$

then $(G_{a,b}(y, z); u_1, \cdots, u_k)$ satisfies Condition **A** *and for $1 \le i \le k$,*

$$D_{u_i} G^*_{a,b}(y, z) = \mathrm{Tr}_{2^m/2}\big((z + b)\phi^{-1}(a^{-1}u_{i,1}) + u_{i,2}\phi^{-1}(a^{-1}(y + u_{i,1}))\big).$$

As a consequence, for any reduced polynomial $H(X_1, \cdots X_k)$ over F_2, the function

$$F_{a,b}(y, z) = G_{a,b}(y, z) + H(\mathrm{Tr}_{2^m/2}(u_{1,1}y + u_{1,2}z), \ldots, \mathrm{Tr}_{2^m/2}(u_{k,1}y + u_{k,2}z))$$

is bent and its dual is

$$F^*_{a,b}(y, z) = G^*_{a,b}(y, z) + H(D_{u_1}G^*_{a,b}(y, z), \ldots, D_{u_k}G^*_{a,b}(y, z)).$$

Proof. It suffices to check that $(G_{a,b}(y, z); u_1, \cdots, u_k)$ satisfies Condition **A**. By Eq. (21), the derivative of $G^*_{a,b}(y, z)$ in the direction of u_i is

$$\begin{aligned} D_{u_i} G^*_{a,b}(y, z) &= G^*_{a,b}(y + u_{i,1}, z + u_{i,2}) + G^*_{a,b}(y, z)\\ &= \mathrm{Tr}_{2^m/2}\big((z + b)\phi^{-1}(a^{-1}u_{i,1}) + u_{i,2}\phi^{-1}(a^{-1}(y + u_{i,1}))\big).\end{aligned}$$

Then the second order derivative in the direction (u_i, u_j) is

$$\begin{aligned} &D_{u_j} D_{u_i} G^*_{a,b}(y, z)\\ &\quad= D_{u_j} G^*_{a,b}(y + u_{i,1}, z + u_{i,2}) + D_{u_j} G^*_{a,b}(y, z)\\ &\quad= \mathrm{Tr}_{2^m/2}\big(\phi^{-1}(a^{-1})(u_{j,2}\phi^{-1}(u_{i,1}) + u_{i,2}\phi^{-1}(u_{j,1}))\big) = 0.\end{aligned}$$ □

Our second construction of vectorial functions with maximal number of bent components is the following result:

Theorem 8. *Let $2 \le k \le m$, ϕ and G be given as above. Suppose $u = (u_{1,1}, 0)$ and choose $u_i = (u_{i,1}, u_{i,2})$ for $2 \le i \le k$ such that*

$$\mathrm{Tr}_{2^m/2}(\phi^{-1}(u_{1,1})u_{i,2}) = 0 \quad \text{and} \quad u_{i,1} = \phi(u_{i,2}).$$

Then for any reduced polynomial $R(X_2, \cdots X_k)$ over F_2, the vectorial function

$$F(y,z) = (y\phi(z), z) + (u_{1,1}y, 0)R(\mathrm{Tr}_{2^m/2}(u_{2,1}y + u_{2,2}z), \ldots, \mathrm{Tr}_{2^m/2}(u_{k,1}y + u_{k,2}z))$$

has $2^n - 2^m$ bent components: for any $(a,b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$,

$$\begin{aligned} F_{a,b}(y,z) = \langle (a,b), F(y,z)\rangle &= \mathrm{Tr}_{2^m/2}(ay\phi(z) + bz) \\ &+ \mathrm{Tr}_{2^m/2}(au_{1,1}y)R(\mathrm{Tr}_{2^m/2}(u_{2,1}y + u_{2,2}z), \ldots, \mathrm{Tr}_{2^m/2}(u_{k,1}y + u_{k,2}z)) \end{aligned}$$

is bent and

$$F_{a,b}^*(y,z) = G_{a,b}^*(y,z) + D_{u_{1,1}a,0}G_{a,b}^*(y,z)R(D_{u_2}G_{a,b}^*(y,z), \ldots, D_{u_k}G_{a,b}^*(y,z)).$$

Proof. Since $\mathrm{Tr}_{2^m/2}(\phi^{-1}(u_{1,1})u_{i,2}) = 0$ and $u_{i,1} = \phi(u_{i,2})$, we have

$$\begin{aligned} D_{u_i}D_{(au_{1,1},0)}G_{a,b}^*(y,z) &= \mathrm{Tr}_{2^m/2}(\phi^{-1}(a^{-1})u_{i,2}\phi^{-1}(au_{1,1})) \\ &= \mathrm{Tr}_{2^m/2}(u_{i,2}\phi^{-1}(u_{1,1})) = 0. \end{aligned}$$

for $2 \le i \le k$, and

$$D_{(u_j}D_{u_i}G_{a,b}^*(y,z) = \mathrm{Tr}_{2^m/2}\big(\phi^{-1}(a^{-1})(u_{j,2}\phi^{-1}(u_{i,1}) + u_{i,2}\phi^{-1}(u_{j,1}))\big) = 0$$

for $2 \le i < j \le k$. Therefore, $(G_{a,b}; (au_{1,1}, 0), u_2, \ldots, u_k)$ satisfies Condition **A** for $(a,b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$. □

Suppose m' is a divisor of m, then (20) can be written as

$$G_{a,b}(y,z) = \mathrm{Tr}_{2^m/2}(ay\phi(z) + bz) = \mathrm{Tr}_{2^{m'}/2}(G'_{a,b}(y,z)),$$

where $G'_{a,b}(y,z) = \mathrm{Tr}_{2^m/2^{m'}}(ay\phi(z) + bz)$.

Theorem 9. *Suppose m' is a divisor of m, $G'_{a,b}(y,z) = \mathrm{Tr}_{2^m/2^{m'}}(ay\phi(z) + bz)$. Then $G'_{a,b}(y,z)$ is a vectorial bent function for $(a,b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$. Furthermore, for $c \in \mathbb{F}_{2^{m'}}^*$, $G_{ca,cb}(y,z) = \mathrm{Tr}_{2^{m'}/2}(cG'_{a,b}(y,z))$ is a bent function and its dual is*

$$G_{ca,cb}^*(y,z) = \mathrm{Tr}_{2^m/2}\big(z\phi^{-1}((ac)^{-1}y) + bc\phi^{-1}((ac)^{-1}y)\big).$$

Proof. Note that for any $c \in \mathbb{F}_{2^{m'}}^*$, one has $(ca, cb) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$, thus $G_{ca,cb}(y,z)$ is bent function in the Maiorana-MacFarland class and the dual can be obtained directly from (21). □

Remark 3. Take $a = b = 1$. Let c_1, c_2, c_3 be three pairwise distinct elements in $\mathbb{F}_{2^{m'}}^*$ such that $c := c_1 + c_2 + c_3 \neq 0$. For $s \in \{c, c_1, c_2, c_3\}$, let

$$G_s(y,z) := G_{s,s}(y,z) = \mathrm{Tr}_{2^m/2}(sy\phi(z) + sz).$$

Then G_c and G_{c_i} are all bent functions and

$$G_{c_1}(y,z) + G_{c_2}(y,z) + G_{c_3}(y,z) = G_c(y,z). \tag{22}$$

To have the equality

$$G_{c_1}^*(y,z) + G_{c_2}^*(y,z) + G_{c_3}^*(y,z) = G_c^*(y,z). \tag{23}$$

it suffices to find an automorphism ϕ of $\mathbb{F}_{2^m}$ such that

(C1) $\phi^{-1}(c^{-1}y) = \phi^{-1}(c_1^{-1}y) + \phi^{-1}(c_2^{-1}y) + \phi^{-1}(c_3^{-1}y)$;
(C2) $c\phi^{-1}(c^{-1}y) = c_1\phi^{-1}(c_1^{-1}y) + c_2\phi^{-1}(c_2^{-1}y) + c_3\phi^{-1}(c_3^{-1}y)$.

Take $\phi = \phi^{-1} : z \mapsto z^{-1}$, then (C1) and (C2) are satisfied, so is Eq.(23). This gives a solution of the open problem proposed by Mesnager ([19, Open Problem 2]).

4. Binomial vectorial functions with maximal number of bent components

We still suppose $n = 2m$. The main result of this section is

Theorem 10. *The binomial vectorial function $F(x) = x^{2^m+1} + x^{2^i+1}$ for $0 \leq i \leq m-1$ on $\mathbb{F}_{2^n}$ has $2^n - 2^m$ bent components if and only if $i = 0$, i.e., $F(x)$ is affine equivalent to x^{2^m+1}.*

Remark 4. The special case of odd m was proved by Zheng et al. [20].

From now on, fix i such that $0 \leq i < m$, and let

$$d = \gcd(m+i, 2m) = \gcd(m+i, 2i).$$

Let $F(x) = x^{2^m+1} + x^{2^i+1}$. For $a \in \mathbb{F}_{2^n}$, the component function $F_a(x) = \mathrm{Tr}_{2^n/2}(ax^{2^m+1} + ax^{2^i+1})$. Let

$$L_a(y) := a^{2^i} y^{2^{2i}} + (a + a^{2^m})^{2^i} y^{2^{m+i}} + ay. \tag{24}$$

If $a \in \mathbb{F}_{2^m}$, then $F_a(x) = \mathrm{Tr}_{2^n/2}(ax^{2^i+1})$ and (24) is reduced to

$$L_a(y) := a^{2^i} y^{2^{2i}} + ay. \tag{25}$$

For any $y \in \mathbb{F}_{2^n}^*$, the derivative of $F_a(x)$ at direction y is

$$\begin{aligned} D_y F_a(x) &= \mathrm{Tr}_{2^n/2}(a((x+y)^{2^m+1} + (x+y)^{2^i+1})) + \mathrm{Tr}_{2^n/2}(a(x^{2^m+1} + x^{2^i+1})) \\ &= \mathrm{Tr}_{2^n/2}(x(ay^{2^i} + (a + a^{2^m})y^{2^m} + a^{2^{n-i}} y^{2^{n-i}})) = \mathrm{Tr}_{2^n/2}(xL_a(y)^{-2^i}). \end{aligned}$$

The root set of $L_a(y)$ in $\mathbb{F}_{2^n}$ forms an $\mathbb{F}_{2^d}$-vector space, hence the number of the roots of $L_a(y)$ in $\mathbb{F}_{2^n}$ is either 1 or a power of 2^d.

Lemma 4. *Assume $v_2(i) = v_2(m)$. For $\xi \in \mathbb{F}_{2^d}$ such that $\xi^{2^{d/2}+1} = 1$, let $a = \frac{1}{1+\xi}$. Then $a \notin \mathbb{F}_{2^m}$ and $L_a(y) = 0$ for any $y \in \mathbb{F}_{2^d}$.*

Proof. By $v_2(i) = v_2(m)$, d is even, $m = \frac{d}{2} \cdot m'$ and $i = \frac{d}{2} \cdot i'$ with m' and i' both odd. Then

$$\xi^{2^m} = \xi^{2^i} = \xi^{-1} \implies a^{2^m} = a^{2^i} = \xi a.$$

This means that $a \notin \mathbb{F}_{2^m}$ and

$$L_a(y) = a^{2^i} y^{2^{2i}} + (a + a^{2^m})^{2^i} y^{2^{m+i}} + ay = a(\xi y^{2^{2i}} + (1+\xi) y^{2^{m+i}} + y).$$

Note that for any $y_0 \in \mathbb{F}_{2^d} = \mathbb{F}_{2^{2i}} \cap \mathbb{F}_{2^{m+i}}$, $y_0^{2^{2i}} = y_0^{2^{m+i}}$, hence $L_a(y_0) = 0$. □

We need the following two general results.

Lemma 5. [28, Theorem 5.30] *Let χ' be a multiplicative character of $\mathbb{F}_{2^m}^*$ of order $2^d - 1$. Then for any $(a, b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}$,*

$$\sum_{x \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(ax^{2^d-1}+b)} = (-1)^{\mathrm{Tr}_{2^m/2}(b)} \sum_{j=1}^{2^d-2} \overline{\chi'^j}(a) G(\chi'^j),$$

where $\overline{\chi}$ and $G(\chi)$ are the conjugate and the Gauss sum of χ.

Lemma 6. *Suppose $d < m$ is a factor of m. Let $\gcd(2^d-1, \frac{m}{d}) = t$. Then the set $N = \{y \in \mathbb{F}_{2^m}^* : \ \mathrm{Tr}_{2^m/2^d}(y^{2^d-1}) = 0\}$ has order*

$$|N| = \begin{cases} \dfrac{2^m-2^d}{2^d} + \dfrac{(2^d-1)(-1)^{\frac{m}{d}-1}}{2^d} \displaystyle\sum_{\chi \in (\widehat{\mathbb{F}}_{2^d}^*)^{\frac{2^d-1}{t}} \setminus \{\chi_0\}} G(\chi)^{\frac{m}{d}}, & \text{if } t \neq 1; \\ 2^{m-d}-1, & \text{if } t = 1. \end{cases}$$

where $\widehat{\mathbb{F}}_{2^d}^*$ is the set of the multiplicative characters of $\mathbb{F}_{2^d}^*$ and χ_0 is the trivial character. In particular, N is non-empty.

Proof. We have

$$\begin{aligned} |N| &= \frac{1}{2^d} \sum_{v \in \mathbb{F}_{2^d}} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^d/2}(v \mathrm{Tr}_{2^m/2^d}(y^{2^d-1}))} \\ &= \frac{2^m-1}{2^d} + \frac{1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \sum_{y \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(vy^{2^d-1})} \end{aligned} \tag{26}$$

Suppose $\mathbb{F}_{2^m}^* = \langle \beta \rangle$, then $\mathbb{F}_{2^m}^* = \bigcup_{i=0}^{\frac{2^m-1}{2^d-1}-1} \beta^i \mathbb{F}_{2^d}^*$. Note that $\gcd(\frac{2^m-1}{2^d-1}, 2^d-1) = \gcd(\frac{m}{d}, 2^d-1) = t$. If $t = 1$, one has

$$\begin{aligned} |N| &= \frac{2^m-1}{2^d} + \frac{2^d-1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \sum_{i=0}^{\frac{2^m-1}{2^d-1}-1} (-1)^{\mathrm{Tr}_{2^m/2}(v\beta^{i(2^d-1)})} \\ &= \frac{2^m-1}{2^d} + \frac{2^d-1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \sum_{i=0}^{\frac{2^m-1}{2^d-1}-1} (-1)^{\mathrm{Tr}_{2^m/2}(v\beta^{i})} \\ &= \frac{2^m-1}{2^d} + \frac{2^d-1}{2^d} \sum_{v \in \mathbb{F}_{2^m}^*} (-1)^{\mathrm{Tr}_{2^m/2}(v)} = \frac{2^m-2^d}{2^d} \geq 1. \end{aligned}$$

If $t \neq 1$, suppose χ' is a multiplicative character of $\mathbb{F}_{2^m}^*$ of order 2^d-1, then by Lemma 5 and Eq. (26),

$$\begin{aligned} |N| &= \frac{2^m-1}{2^d} + \frac{1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \Big(\sum_{y \in \mathbb{F}_{2^m}} (-1)^{\mathrm{Tr}_{2^m/2}(vy^{2^d-1})} - 1 \Big) \\ &= \frac{2^m-1}{2^d} + \frac{1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \Big(\sum_{j=1}^{2^d-2} \overline{\chi'^j}(v) G(\chi'^j) - 1 \Big) \\ &= \frac{2^m-1}{2^d} + \frac{1}{2^d} \sum_{v \in \mathbb{F}_{2^d}^*} \sum_{j=0}^{2^d-2} \overline{\chi'^j}(v) G(\chi'^j). \end{aligned} \tag{27}$$

Suppose N is the norm mapping from $\mathbb{F}_{2^m}$ to $\mathbb{F}_{2^d}$. For $\chi \in \widehat{\mathbb{F}}_{2^d}^*$, it can be lifted from $\mathbb{F}_{2^d}$ to $\mathbb{F}_{2^m}$ by $\chi' = \chi \circ \mathrm{N}$ (see [28, Theorem 5.28]). Furthermore, χ is of order

2^d-1 if and only if χ' is of order 2^d-1. Then

$$\sum_{j=0}^{2^d-2}\overline{\chi'^j}(v)G(\chi'^j)=\sum_{\chi\in\widehat{\mathbb{F}}^*_{2^d}}\overline{\chi}(\mathrm{N}(v))G(\chi\circ\mathrm{N})=(-1)^{\frac{m}{d}-1}\sum_{\chi\in\widehat{\mathbb{F}}^*_{2^d}}\overline{\chi}(v^{\frac{2^m-1}{2^d-1}})G(\chi)^{\frac{m}{d}}.$$

Suppose $\delta=\beta^{\frac{2^m-1}{2^d-1}}\in\mathbb{F}^*_{2^d}$, then $\mathbb{F}^*_{2^d}=\bigcup_{j=0}^{\frac{2^d-1}{t}-1}\delta^j\langle\delta^{\frac{2^d-1}{t}}\rangle$. By Eq. (27), we get

$$\begin{aligned}|N|&=\frac{2^m-1}{2^d}+\frac{(-1)^{\frac{m}{d}-1}}{2^d}\sum_{v\in\mathbb{F}^*_{2^d}}\sum_{\chi\in\widehat{\mathbb{F}}^*_{2^d}}\overline{\chi}(v^{\frac{2^m-1}{2^d-1}})G(\chi)^{\frac{m}{d}}\\&=\frac{2^m-1}{2^d}+\frac{(-1)^{\frac{m}{d}-1}}{2^d}\sum_{\chi\in\widehat{\mathbb{F}}^*_{2^d}}G(\chi)^{\frac{m}{d}}\sum_{j=0}^{\frac{2^d-1}{t}-1}\sum_{v\in\delta^j\langle\delta^{\frac{2^d-1}{t}}\rangle}\overline{\chi}(v^{\frac{2^m-1}{2^d-1}})\\&=\frac{2^m-1}{2^d}+\frac{(-1)^{\frac{m}{d}-1}t}{2^d}\sum_{\chi\in\widehat{\mathbb{F}}^*_{2^d}}G(\chi)^{\frac{m}{d}}\sum_{j=0}^{\frac{2^d-1}{t}-1}\overline{\chi}(\delta^{j\frac{2^m-1}{2^d-1}})\end{aligned}$$

Note that $\gcd(\frac{2^m-1}{t(2^d-1)},\frac{2^d-1}{t})=1$, then

$$\sum_{i=0}^{\frac{2^d-1}{t}-1}\overline{\chi}(\delta^{i\frac{2^m-1}{2^d-1}})=\sum_{i=0}^{\frac{2^d-1}{t}-1}\overline{\chi}(\delta^{it})=\sum_{x\in\langle\delta^t\rangle}\overline{\chi}(x)=\begin{cases}0, & \text{if } \chi\neq\chi_0;\\ \frac{2^d-1}{t}, & \text{if } \chi=\chi_0.\end{cases}$$

Hence we have

$$|N|=\frac{2^m-2^d}{2^d}+\frac{(2^d-1)(-1)^{\frac{m}{d}-1}}{2^d}\sum_{\chi\in(\widehat{\mathbb{F}}^*_{2^d})^{\frac{2^d-1}{t}}\setminus\{\chi_0\}}G(\chi)^{\frac{m}{d}}.$$

By properties of Gauss sum, we have

$$|N|\geq\frac{2^m-2^d-(2^d-1)(t-1)2^{\frac{m}{2}}}{2^d}.$$

Note that $t\neq1$ and

$$2^m-2^d-(2^d-1)(t-1)2^{\frac{m}{2}}=2^m-t2^{\frac{m}{2}+d}+(t-1)2^{\frac{m}{2}}-2^d>2^m-t2^{\frac{m}{2}+d}.$$

Since $t=\gcd(\frac{m}{d},2^d-1)\leq2^d-1$, then $2^m-t2^{\frac{m}{2}+d}>2^m-2^{\frac{m}{2}+2d}\geq0$ if $\frac{m}{d}\geq4$. If $m=3d$, then $t=\gcd(3,2^d-1)=3$ and d is even. one has

$$|N|=2^{3d}-2^d-(2^d-1)2^{\frac{3d}{2}+1}>2^{3d}-2^{\frac{5d}{2}+1}\geq0.$$

If $m=2d$, then $t=\gcd(2,2^d-1)=1$, which contradicts to $t\neq1$. Thus we complete the proof. □

Back to our situation, we have the following result.

Lemma 7. *Suppose $v_2(m)<v_2(i)$, then there exists $a\in\mathbb{F}_{2^n}-\mathbb{F}_{2^m}$, such that $L_a(y)$ has roots in $\mathbb{F}^*_{2^n}$.*

Proof. For $v_2(m) < v_2(i)$, note that $d = \gcd(m, i) = \gcd(m + i, n)$. It suffices to show that there exists $a \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$ such that $L_a(y)$ has a root $y_0 \in \mathbb{F}_{2^m}^*$. Note that for $y \in \mathbb{F}_{2^m}^*$,

$$L_a(y) = a^{2^i} y^{2^{2i}} + (a + a^{2^m})^{2^i} y^{2^{m+i}} + ay = a^{2^i} y^{2^{2i}} + (a + a^{2^m})^{2^i} y^{2^i} + ay. \quad (28)$$

Then we just need to find $(a, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^*$ such that

$$\begin{cases} a + a^{2^m} = y^{-2^i-1} v, \\ (ay^{2^i+1})^{2^i} + ay^{2^i+1} = y^{2^i-2^{2i}} v \end{cases} \quad (29)$$

for some $v \in \mathbb{F}_{2^d}^*$ (here $a \notin \mathbb{F}_{2^m}$ is automatic). Let $z = av^{-1}y^{2^i+1}$, then we just need to find $(z, y) \in \mathbb{F}_{2^n} \times \mathbb{F}_{2^m}^*$ such that

$$\begin{cases} z + z^{2^m} = 1, & (30) \\ z^{2^i} + z = y^{2^i-2^{2i}}. & (31) \end{cases}$$

We consider Eq. (31). Note that the $\mathbb{F}_{2^d}$-linear maps $\varphi_i : z \mapsto z^{2^i} + z$ and $\varphi_d : z \mapsto z^{2^d} + z$ from $\mathbb{F}_{2^m}$ to itself have the same kernel $\mathbb{F}_{2^d}$ and $\varphi_i(z) = \varphi_d(z + z^{2^d} + \cdots + z^{2^{(\frac{i}{d}-1)d}})$, then $\mathrm{Im}(\varphi_i) \subseteq \mathrm{Im}(\varphi_d)$ and hence $\mathrm{Im}(\varphi_d) = \mathrm{Im}(\varphi_i)$. Note also that the group homomorphisms $y \mapsto y^{2^i(1-2^i)}$ and $y \mapsto y^{2^d-1}$ from $\mathbb{F}_{2^m}^*$ to itself have the same kernel and image. Then there is a one-to-one correspondents of solutions $(z, y) \in \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}^*$ of Eq. (31) and of

$$z^{2^d} + z = y^{2^d-1}. \quad (32)$$

Eq. (32) is soluble if and only if there exists $y \in \mathbb{F}_{2^m}^*$ such that $\mathrm{Tr}_{2^m/2^d}(y^{2^d-1}) = 0$, which is guaranteed by Lemma 6 as $d < m$ in this case. Thus there exists $(z_0, y_0) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}^*$ such that $z_0^{2^i} + z_0 = y_0^{2^i-2^{2i}}$.

Let $w \in \mathbb{F}_{2^{2d}} \setminus \mathbb{F}_{2^d}$ satisfy $w^{2^d} + w = v_0$, then $w^{2^{m-d}} = w^{2^i} = w$ and $z = z_0 + w \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^m}$ is a solution of Eqs. (30) and (31). Thus, $y_0 \in \mathbb{F}_{2^m}^*$ and $a = (z_0 + w)y_0^{-2^i-1} v$ satisfy the equation $L_a(y) = 0$. □

Lemma 8. *For $0 \le i \le m - 1$, if $F(x) = x^{2^m+1} + x^{2^i+1}$ has $2^n - 2^m$ bent components, then $v_2(m) \le v_2(i)$.*

Proof. Assume $v_2(m) > v_2(i)$. In this case $d = \gcd(m, i) = \gcd(n, i)$, and $2d = \gcd(2i, m)$. This means $2^d - 1 = \gcd(2^m - 1, 2^i - 1)$ and $2^{2d} - 1 = \gcd(2^m - 1, 2^{2i} - 1)$, which then implies that $2^d + 1$ is a factor of $2^m - 1$ and thus prime to $2^m + 1$.

Let α be a primitive element of $\mathbb{F}_{2^n}$. Let $a = \alpha^{k(2^m+1)} \in \mathbb{F}_{2^m}^*$ such that $a^{2^i-1} = \alpha^{(2^m+1)(2^d-1)}$. By Proposition 1, for this a, $F_a(x) = \mathrm{Tr}_{2^n/2}(ax^{2^i+1})$ is not bent. By Lemma 1, $D_y F_a(x) = \mathrm{Tr}_{2^n/2}(x(ay^{2^i} + (ay)^{2^{n-i}}))$ is not balanced for some $y \in \mathbb{F}_{2^n}$, i.e. $a^{2^i-1} y^{2^{2i}-1} + 1 = 0$ is soluble. Let $a^{2^i-1} = \alpha^{(2^m+1)(2^d-1)} = y_0^{1-2^{2i}}$ and let $y_1 \in \mathbb{F}_{2^n}^*$ such that $y_0^{1-2^{2i}} = y_1^{2^{2d}-1}$. Then the congruent equation

$$(2^{2d} - 1)x \equiv (2^d - 1)(2^m + 1) \bmod (2^n - 1)$$

is soluble, equivalently, the equation

$$(2^d + 1)x \equiv 2^m + 1 \bmod (2^d + 1) \cdot \frac{2^n - 1}{2^{2d} - 1}$$

is soluble. This is not possible since $2^d + 1$ is prime to $2^m + 1$. □

Proof of Theorem 10. If $i = 0$, the result is trivial. We now assume $i \neq 0$ and $v_2(m) \leq v_2(i)$.

If $F(x)$ has maximal number of bent components, by Lemma 1, $F_a(x)$ is bent function for all $a \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$ and hence $D_y f_a(x)$ is balanced for any $y \in \mathbb{F}_{2^n}^*$. This implies $L_a(y) \neq 0$ for all $y \in \mathbb{F}_{2^n}^*$. Hence to show $F(x)$ does not have maximal number of bent components, it suffices to show there exists $a \in \mathbb{F}_{2^n} - \mathbb{F}_{2^m}$, such that $L_a(y)$ has a root in $\mathbb{F}_{2^n}^*$:

(i) If $v_2(m) = v_2(i)$, this is implied by Lemma 4.
(ii) If $v_2(m) < v_2(i)$, this is implied by Lemma 7.

Thus for $i \neq 0$, $F(x)$ cannot have $2^n - 2^m$ bent components. □

Remark 5. For a general binomial vectorial function $F(x) = x^{d_1} + x^{d_2}$, our experimental result indicates that $F(x)$ is affine equivalent to x^{2^m+1} or $x^{2^i}(x + x^{2^m})$ if $F(x)$ has maximal number of bent components, but so far we do not have a proof. We leave this as an open problem for future study.

5. Conclusion

We firstly give a generic construction of vectorial functions with maximal number of bent components, and obtain two new classes of such vectorial functions based on the Niho quadratic function and the Maiorana-MacFarland class. Moreover, we solve the open problem proposed by Mesnager, and partially answer the open problem proposed by Pott et al. We then show that the binomial function $F(x) = x^{2^m+1} + x^{2^i+1} : \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ has maximal number of bent components if and only if $i = 0$

References

[1] O. Rothaus, "On 'bent' functions." *J. Combinat. Theory, Ser. A*, **20**(3), 300-305 (1976).
[2] C. Carlet, S. Mesnager, " Four decades of research on bent functions." Des. Codes Cryptogr., **78**(1), 5-50 (2016).
[3] 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. Inf. Theory*, **63**(10), 6149-6157 (2017).
[4] S. Mesnager, "Bent Functions: Fundamentals and Results." Springer, Cham 2016.
[5] G. Leander, "Monomial bent functions." *IEEE Trans. Inf. Theory*, **52**(2), 738-743 (2006).
[6] G. Leander, A. Kholosha, "Bent functions with 2^r Niho exponents." *IEEE Trans. Inf. Theory*, **52**(12), 5529-5532 (2006).
[7] N. Li, T. Helleseth, X. Tang and A. Kholosha, "Several new classes of bent functions from Dillon exponents." *IEEE Trans. Inf. Theory*, **59**(3), 1818-1831 (2013).
[8] J. Peng, C. Tan, H. Kan, "On existence of vectorial bent functions from the $\mathcal{PS}_{ab}$ class." *Scientia Sinica Math.*, **47**(9), 995-1010 (2017).
[9] C. Carlet, "On bent and highly nonlinear balanced/resilient functions and their algebraic immunities," in *AAECC* (Lecture Notes in Computer Science), **3857**, M. P. C. Fossorier, H. Imai, S. Lin, A. Poli, Eds, New York, NY, USA: Springer-Verlag, 1-28 (2006).
[10] K. Nyberg, "Perfect nonlinear S-boxs," in Advance in Cryptology-EUROCRYPT. Berlin, Germany: Springer-Verlag, **547**, 378-385 (1991).
[11] A. Çeşmelioğlu, W. Meidl, A. Pott, "Vectorial bent functions and their duals," *Linear Algebra Appl.*, **548**, 305-320, 2018.
[12] K. Feng, J. Yang, "Vectorial Boolean functions with good cryptographic properties," *Int. J. Found. Comput. Sci.*, **22**(6), 1271-1282, 2011.
[13] S. Mesnager, "Bent functions from spreads," J. Amer. Math. Soc., to be published.
[14] E. Pasalic, W. Zhang, "On multiple output bent functions." *Inform. Process. Lett.*, **112**(21), 811-815 (2012).

[15] S. Mesnager, "Bent vectorial functions and linear codes from o-polynomials." *Des. Codes Cryptogr.*, **77**(1), 99-116 (2015).

[16] A. Muratović-Ribić, E. Pasalic and S. Bajrić, "Vectorial bent functions from multiple terms trace functions." *IEEE Trans. Inf. Theory*, **60**(2), 1337-1347 (2014).

[17] 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. Inf. Theory*, **64**(1), 367-383 (2018).

[18] S. Mesnager, F. Zhang, C. Tang and Y. Zhou, "Further study on the maximum number of bent components of vectorial functions." *Des., Codes and Cryptogr.*, **87**, 2597-2610 (2019).

[19] S. Mesnager, "Several new infinite families of bent functions and their duals." *IEEE Trans. Inf. Theory*, **60**(7), 4397-4407 (2014).

[20] L. Zheng, J. Peng, H. Kan, Y. Li and J. Luo, "On constructions and properties of (n, m)-functions with maximal number of bent components." *Des. Codes Cryptogr.*, **88**(9), 2171-2186 (2020).

[21] A. Pott, E. Pasalic, A. Muratovic, S. Bajric, "On the maximum number of bent components of vectorial functions." *IEEE Trans. Inf. Theory*, **64**(1), 403-411, 2018.

[22] H. Hu, B. Wang, X. Xie and Y. Luo, "Two problems about monomial bent functions," *arXiv:2102.12304v1.*

[23] K. Nyberg, "Differentially uniform mappings for cryptography," in Advance in Cryptology-EUROCRYPT. Berlin, Germany: Springer-Verlag, **765**, 55-64 (1993).

[24] A. W. Bluher, "On $x^{q+1} + ax + b$." *Finite Fields Appl.*, **10**(3), 285-305 (2004).

[25] T. Helleseth, A. Kholosha, "On the equation $x^{2^l+1} + x + a = 0$ over $\mathbb{F}_{2^k}$." *Finite Fields Appl.*, **14**(1), 159-176 (2008).

[26] T. Helleseth, L. Hu, A. Kholosha, X. Zeng, N. Li and W. Jiang, "Period-different m-sequences with at most four-valued cross correlation." *IEEE Trans. Inf. Theory*, **55**(7), 3305-3311 (2009).

[27] L. Zheng, J. Peng, H. Kan and Y. Li, "Several new infinite families of bent functions via second order derivatives." *Cryptogr. Commun.*, **12**(1), 1143-1160 (2020).

[28] R. Lidl, H. Niederreiter, *Finite Fields.* Cambridge, U.K.: Cambridge Univ. Press, 1984.

[1]University of Science and Technology of China, Key Laboratory of Electromagnetic Space Information, CAS, Hefei, Anhui 230027, China

Email address: xianhxie@mail.ustc.edu.cn

[2]School of Mathematical Sciences, CAS Wu Wen-Tsun Key Laboratory of Mathematics, University of Science and Technology of China, Hefei 230026, China

[3]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, China

Email address: yiouyang@ustc.edu.cn