On the Existence and Constructions of Vectorial Boolean Bent Functions*

Yuwei Xu[1,2] and ChuanKun Wu[1]

[1]State Key Laboratory of Information Security
Institute of Information Engineering
Chinese Academy of Sciences, Beijing 100093, China
[2]University of Chinese Academy of Sciences
Beijing 100049, China
Email: {xuyuwei, ckwu}@iie.ac.cn

Abstract

Recently, one of the hot topics on vectorial Boolean bent functions is to construct vectorial Boolean bent functions in the form $Tr_m^n(P(x))$ from Boolean bent functions in the form $Tr_1^n(P(x))$, where $P(x) \in \mathbb{F}_{2^n}[x]$. This paper first presents three constructions of vectorial Boolean bent functions in the form $Tr_m^n(P(x))$, where two of them give answers to two open problems proposed by Pasalic et al. and Muratović-Ribić et al. respectively. The main results in this paper are the existence and constructions of several kinds of vectorial Boolean bent functions in the form $Tr_m^n(P(x))$.

1 Introduction

Bent functions were initially introduced by Rothaus in [42], where it was shown that n-variable Boolean bent functions exist if and only if n is even. Because of the wide applications of bent functions in combinatorial design theory, coding theory, spread spectrum and cryptography, much research has been done about bent functions (see for example [5, 8, 10, 15, 30, 32, 34–36]). The concept of *bent* for vectorial Boolean functions, which is an extension of Boolean bent functions, was first considered by Nyberg in [38], where it was shown that bent (n, m)-functions (i.e., vectorial Boolean functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$) exist if and only if n is even and $n \geq 2m$. Vectorial Boolean bent functions are also called perfect nonlinear functions [11], and there are several equivalent descriptions of vectorial Boolean bent functions, such as maximally nonlinear vectorial Boolean functions, vectorial Boolean functions having flat Walsh spectra, vectorial Boolean functions whose non-zero components are Boolean bent functions, vectorial Boolean functions having the minimum differential uniformity, etc. Because of possessing the maximal nonlinearity and the minimum differential uniformity, vectorial Boolean bent functions have the optimum resistance against linear cryptanalysis [23, 28] and differential cryptanalysis [1, 2]. Thus, the constructions of vectorial Boolean bent functions have both theoretical significance as well as practical applications.

*This work was supported by NSFC under no. 61173134.

The construction methods of vectorial Boolean bent functions can be divided into two categories: primary constructions and secondary constructions. Primary constructions are also called direct constructions, and secondary constructions lead to vectorial Boolean bent functions based on some known vectorial Boolean bent functions, which are also called indirect constructions. Among the constructions of vectorial Boolean bent functions, primary constructions hold a key status. Most of primary constructions of vectorial Boolean bent functions stem from the Maiorana-McFarland method [18, 29] or the Partial Spread method [18]. The strict Maiorana-McFarland constructions, the extended Maiorana-McFarland constructions and the general Maiorana-McFarland constructions are three important constructions [11, 39, 40, 43] of vectorial Boolean bent functions in the light of Maiorana-McFarland constructions. By the Partial Spread method, the $\mathcal{PS}_{ap}$ constructions [11] and a Partial Spread construction [13] of vectorial Boolean bent functions have been presented. Particularly, by studying new connections between vectorial Boolean bent functions and the hyperovals of the projective plane, S. Mesnager [33] introduced a new primary construction of bent $(n, \frac{n}{2})$-functions from o-polynomials, named class $\mathcal{H}$ of vectorial functions, which is closely related to class $\mathcal{H}$ of Boolean functions [14, 18]. Except the well known Direct Sum Construction, only two secondary constructions of vectorial Boolean bent functions (Proposition 9.5 and Proposition 9.6 in [11]) can be found in public literatures, which are the generalizations of two secondary constructions of Boolean bent functions in [7] and [9] respectively. In addition, Proposition 9.6 in [11] includes Direct Sum Construction as a special case. For more information about constructions of vectorial Boolean bent functions, please refer to [3, 13, 33].

Recently, a new primary construction of vectorial Boolean bent functions in the form $Tr_m^n(P(x))$ from Boolean bent functions in the form $Tr_1^n(P(x))$ has attracted a lot of attentions, where $P(x) \in \mathbb{F}_{2^n}[x]$.

The Boolean bent functions in the form $Tr_1^n(ax^d)$ are known as monomial bent functions, where d (in the sense of modulo $2^n - 1$) is named as a bent exponent when there exists an integer a such that $Tr_1^n(ax^d)$ is bent. So far, only five kinds of monomial bent functions [31], have been found and they are named by respective kinds of bent exponent, as listed in Table 1. In [41], when $Tr_1^n(ax^d)$ is bent, it was shown that the vectorial monomial Boolean function $Tr_m^n(ax^d)$ is bent if x^d is a permutation over $\mathbb{F}_{2^m}$. Following this conclusion, three kinds of monomial bent functions, Kasami case, Leander case and Canteaut-Charpin-Kyureghyan case, have been analyzed, and some kinds of vectorial monomial bent functions have been constructed [41]. However, it remains to be an open problem to judge whether the sufficient condition that x^d is a permutation over $\mathbb{F}_{2^m}$ is also a necessary condition, which will indicate whether the constructions of vectorial monomial bent functions in [41] are optimal. In [22], two kinds of vectorial monomial bent functions in the form $Tr_{\frac{n}{2}}^n(ax^d)$ are constructed based on monomial bent functions in Gold case and Kasimi case. For a monomial bent function $Tr_1^n(ax^d)$ that belongs to Gold case or Kasimi case, it was shown in [22] that $Tr_{\frac{n}{2}}^n(ax^d)$ is bent if $\gcd(d, 2^n - 1) \mid (2^{\frac{n}{2}} + 1)$ and $a \notin \{x^{\gcd(d,2^n-1)} : x \in \mathbb{F}_{2^n}\}$. However, whether the condition $\gcd(d, 2^n - 1) \mid (2^{\frac{n}{2}} + 1)$ is necessary remains unclear. In [37], it was also proved that there does not exist vectorial monomial bent functions in the form $Tr_{\frac{n}{2}}^n(ax^d)$ as in Dillon case, where $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, $d = l(2^{\frac{n}{2}} - 1)$ and $\gcd(l, 2^{\frac{n}{2}} + 1) = 1$.

The bent properties of binomial Boolean functions in the form $Tr_1^n(a_1x^{d_1} + a_2x^{d_2})$ were studied in [20, 21], where d_i, $i = 1, 2$, are Niho exponents, i.e., the restriction of x^{d_i} on $\mathbb{F}_{2^{\frac{n}{2}}}$ is linear. Soon afterwards, a construction of Boolean bent functions with 2^r Niho exponents

Table 1: Monomial Bent Functions in the Form $Tr_1^n(ax^d)$

Case	Exponent d	Condition 1	[1]Conditions 2	References
Gold	2^s+1	$s \in \mathbb{N}$	$a \notin \{x^d : x \in \mathbb{F}_{2^n}\}$	[26]
Dillon	$l(2^{\frac{n}{2}}-1)$	$\gcd(l, 2^{\frac{n}{2}}+1)=1$ (or $l=1$)	[2]$K(a)=-1, \mathbb{F}^*_{2^{\frac{n}{2}}}$ (or $K(N^n_{\frac{n}{2}}(a))=-1, \mathbb{F}^*_{2^n}$)	[16, 26] [24]
Kasami	$2^{2s}-2^s+1$	$\gcd(3,n)=1$, $\gcd(s,n)=1$	$a \notin \{x^3 : x \in \mathbb{F}_{2^n}\}$	[19, 26]
Leander	$(2^s+1)^2$	$n=4s$, s odd	$a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}^*_{2^n}\}$	[17, 26], Theorem 12
Canteaut-Charpin-Kyureghyan	$2^{2s}+2^s+1$	$n=6s$, $s>1$ integer	$a \in \{x^d : x \in \mathbb{F}^*_{2^n}\}$ $\cdot\{\rho : Tr_s^{3s}(\rho)=0, \rho \in \mathbb{F}^*_{2^{3s}}\}$	[6, 17], Theorem 14

[1] Necessary and sufficient conditions for $Tr_1^n(ax^d)$ to be bent.

[2] Kloosterman sums $K(a)=\sum_{x \in \mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+ax)}$.

was introduced [25], and further study on it can be found say in [4, 12]. In [27], an equivalent form of the construction as in [25] was presented. In [37], it was shown that the vectorial Boolean function $Tr^n_{\frac{n}{2}}(a_1x^{d_1}+a_2x^{d_2})$ is bent for some special sets of a_1, a_2, d_1, d_2 as specified in [21]. Based on Boolean bent functions in the form $Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$, the construction of vectorial Boolean bent functions in the form $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ was studied in [37]. For a Boolean bent function $Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$, where $d_i = d_1 + v_i(2^m-1)$, $i=2,3,\cdots,r$, and v_i are nonnegative integers, it was shown in [37] that, the vectorial Boolean function $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is bent if x^{d_1} is a permutation over $\mathbb{F}_{2^m}$. And one of the open problems left in [37] was to find a similar result to the above conclusion in the case when x^{d_1} is not a permutation over $\mathbb{F}_{2^m}$.

This paper is devoted to the existence and constructions of vectorial Boolean bent functions in the form $Tr_m^n(P(x))$ based on Boolean bent functions in the form $Tr_1^n(P(x))$, where $P(x) \in \mathbb{F}_{2^n}[x]$. We firstly present three constructions of vectorial Boolean bent functions, where two of them provide answers to the two open problems proposed by E.Pasalic et al. in [41] and by A.Muratović-Ribić et al. in [37] respectively. Moreover, by the techniques presented in section 3, we analyze the bent properties of several kinds of vectorial Boolean functions in the form $Tr_m^n(P(x))$. It is mainly obtained that the existence and the constructions of vectorial monomial bent functions in the form $Tr_m^n(ax^d)$ using the known five kinds of monomial bent functions. In addition, a construction of vectorial Boolean bent functions in the form $Tr_m^n(\sum_{i=1}^{2^s-1} ax^{(i\cdot 2^{\frac{n}{2}-s}+1)(2^{\frac{n}{2}}-1)+1})$ is presented, where $(i\cdot 2^{\frac{n}{2}-s}+1)(2^{\frac{n}{2}}-1)+1$, $i=1,2,\cdots,2^s-1$, are Niho exponents and $\gcd(s,\frac{n}{2})=1$.

The rest of this paper is organized as follows. Section 2 provides some preliminaries for the description of the paper. Section 3 presents three constructions of vectorial Boolean bent functions, and gives answers to two open problems proposed by E.Pasalic et al. and A.Muratović-Ribić et al. respectively. Section 4 analyzes the bent properties of several kinds of vectorial Boolean functions, and Section 5 concludes this paper.

2 Preliminaries

Throughout this paper, let $\mathbb{F}_{2^n}$ denote the Galois field $GF(2^n)$, m and n be two positive integers, α be a primitive element of $\mathbb{F}_{2^n}$, and let the Kloosterman sums be $K(a) = \sum_{x\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+ax)}$.

For $m \mid n$, the trace function $Tr_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, is defined as

$$Tr_m^n(x) = x + x^{2^m} + x^{2^{2m}} + \cdots + x^{2^{(n/m-1)m}},\ x \in \mathbb{F}_{2^n}.$$

In particular, Tr_1^n is called the absolute trace function over $\mathbb{F}_{2^n}$. Note that the trace function has the well known properties that $Tr_1^n(x) = Tr_1^m \circ Tr_m^n(x)$ and $Tr_m^n(x) = Tr_m^n(x^2)$.

For $m \mid n$, the norm function $N_m^n : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, is defined as

$$N_m^n(x) = x \cdot x^{2^m} \cdot x^{2^{2m}} \cdots x^{2^{(n/m-1)m}},\ x \in \mathbb{F}_{2^n}.$$

A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ can be uniquely represented in the univariate polynomial representation as

$$f(x) = \sum_{i=0}^{2^n-1} \sigma_i x^i, \sigma_i \in \mathbb{F}_{2^n},$$

where $\sigma_0, \sigma_{2^n-1} \in \mathbb{F}_2$, and $\sigma_{2i \bmod (2^n-1)} = \sigma_i^2$ for $1 \le i \le 2^n - 2$. Note that $\sigma_0, \sigma_{2^n-1} \in \mathbb{F}_2$ and $\sigma_{2i \bmod (2^n-1)} = \sigma_i^2$ for $1 \le i \le 2^n - 2$ if and only if $f^2(x) \equiv f(x) (\mathrm{mod}\ x^{2^n} - x)$. The Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ can also be represented in a non-unique way [34] as

$$f = Tr_1^n(P(x)),\ P(x) \in \mathbb{F}_{2^n}[x].$$

The linear Boolean functions $\varphi : \mathbb{F}_{2^n} \to \mathbb{F}_2$ are the functions

$$\varphi(x) = Tr_1^n(ax), a \in \mathbb{F}_{2^n}.$$

The affine Boolean functions on $\mathbb{F}_{2^n}$ are the functions $\varphi(x) + \delta$, where $\delta \in \mathbb{F}_2$.

A mapping $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ is referred to as a vectorial Boolean function, which is also known as an $(n, m)-$function, a multiple output Boolean function or an S-box, and can be uniquely represented as

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

which is called the univariate polynomial representation of the vectorial Boolean function. If $m \mid n$, the vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ can also be represented in a non-unique way [11] as

$$F = Tr_m^n(P(x)),\ P(x) \in \mathbb{F}_{2^n}[x].$$

If $m \mid n$, the linear vectorial Boolean functions $\phi : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ are the functions

$$\phi(x) = Tr_m^n(ax), a \in \mathbb{F}_{2^n}.$$

If $m \mid n$, the affine vectorial Boolean functions on $\mathbb{F}_{2^n}$ are the functions $\phi(x) + \eta$, where $\eta \in \mathbb{F}_{2^m}$.

The Walsh transform of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$, denoted by $W_f(\omega)$, is defined as

$$W_f(\omega) = \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+Tr_1^n(\omega x)}, \forall\ \omega \in \mathbb{F}_{2^n}.$$

The extended Walsh transform of a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$, denoted by $W_F(\omega, \lambda)$, is defined as

$$W_F(\omega, \lambda) = \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda F(x))+Tr_1^n(\omega x)}, \forall\ \omega \in \mathbb{F}_{2^n}, \forall\ \lambda \in \mathbb{F}_{2^m}^*.$$

Among the equivalent definitions of the bent property of Boolean functions and vectorial Boolean functions, we recall the following definitions.

Definition 1. *For even n, a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called bent if and only if $W_f(\omega) = \pm 2^{\frac{n}{2}}$ holds for all $\omega \in \mathbb{F}_{2^n}$.*

Definition 2. *For even n, a vectorial Boolean function $F : \mathbb{F}_{2^n} \to \mathbb{F}_m$ is called bent if and only if $W_F(\omega, \lambda) = \pm 2^{\frac{n}{2}}$ holds for all $\omega \in \mathbb{F}_{2^n}$ and for all $\lambda \in \mathbb{F}_{2^m}^*$.*

3 Constructions of vectorial Boolean bent functions from Boolean bent functions in trace form

In this section, using Boolean bent functions in trace form, three constructions of vectorial Boolean bent functions are given. The first two constructions, Theorem 1 and Theorem 3, provide answers to the two open problems proposed by E.Pasalic et al. [41] and A.Muratović-Ribić et al. [37] respectively.

Before the discussion, two useful lemmas are presented. These two lemmas seem to be known in basic Algebra, however, it is difficult to find an explicit reference, hence we include their proofs here.

Lemma 1. *Let $G = \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Then $G = \langle \alpha^d \rangle = \langle \alpha^{\gcd(d,2^n-1)} \rangle$.*

Proof. Note the fact that $G = \{x^d : x \in \mathbb{F}_{2^n}^*\}$ is a cyclic subgroup of $\mathbb{F}_{2^n}^*$. For any $x \in \mathbb{F}_{2^n}^*$, there is an integer u such that $x = \alpha^u$, where $1 \leq u \leq 2^n - 1$. Then $G \subseteq \langle \alpha^{ud} \rangle \subseteq \langle \alpha^d \rangle$. For $\forall\ \alpha^{vd} \in \langle \alpha^d \rangle$, where $1 \leq v \leq 2^n - 1$ is an integer, since $\alpha^v \in \mathbb{F}_{2^n}^*$, then $\alpha^{vd} \in G$, and we have $\langle \alpha^d \rangle \subseteq G$. Therefore, $G = \langle \alpha^d \rangle$.

Due to $|\langle \alpha^{\gcd(d,2^n-1)} \rangle| = \frac{2^n-1}{\gcd(d,2^n-1)} = |\langle \alpha^d \rangle|$ and the fact that there is a unique cyclic subgroup of order $\frac{2^n-1}{\gcd(d,2^n-1)}$ in $\mathbb{F}_{2^n}^*$, we have $\langle \alpha^{\gcd(d,2^n-1)} \rangle = \langle \alpha^d \rangle$. □

Lemma 2. *Let $m \mid n$ and $G = \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Then $\mathbb{F}_{2^m}^* \subseteq G$ if and only if $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$.*

Proof. By Lemma 1, it is known that $G = \langle \alpha^{\gcd(d,2^n-1)} \rangle$ is a cyclic subgroup of $\mathbb{F}_{2^n}^*$, hence the order of G is $\frac{2^n-1}{\gcd(d,2^n-1)}$.

Since $m \mid n$, we have $(2^m - 1) \mid (2^n - 1)$, thus $\mathbb{F}_{2^m}^*$ is a cyclic subgroup of order $2^m - 1$ in $\mathbb{F}_{2^n}^*$. If $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$, then there is a cyclic subgroup of order $2^m - 1$ in G. Since $G \subseteq \mathbb{F}_{2^n}^*$ and the fact that there is a unique cyclic subgroup of order $2^m - 1$ in $\mathbb{F}_{2^n}^*$, we get that G and $\mathbb{F}_{2^n}^*$ have the same cyclic subgroup $\mathbb{F}_{2^m}^*$. Thus, $\mathbb{F}_{2^m}^* \subseteq G$.

The necessity is obvious. Hence the conclusion of Lemma 2 holds. □

The following theorem gives a sufficient condition for the vectorial Boolean functions in the form $Tr_m^n(ax^d)$ to be bent, which includes Theorem 1 in [41] as a special case. The theorem hence answers one open problem raised in [41] (named Open Problem 1 in this paper).

Theorem 1. *Let $n \geq 4$ be even and $m \mid n$, and let $f(x) = Tr_1^n(ax^d)$ be a Boolean bent function. If $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$, then the vectorial Boolean function $F(x) = Tr_m^n(ax^d)$ is bent.*

Proof. Let $G = \{x^d : x \in \mathbb{F}_{2^n}^*\}$. If $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$, according to Lemma 2, then $\mathbb{F}_{2^m}^* \subseteq G$. Thus, for all $\lambda \in \mathbb{F}_{2^m}^*$, there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^d$. Therefore, for all $\omega \in \mathbb{F}_{2^n}$ and for all $\lambda \in \mathbb{F}_{2^m}^*$, we have

$$\begin{aligned}
W_F(\omega, \lambda) &= \Sigma_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^m(\lambda F(x))+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^m(\lambda Tr_m^n(ax^d))+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(a\lambda x^d)+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(a\beta^d x^d)+Tr_1^n(\omega x)} \\
&= \Sigma_{y\in\mathbb{F}_{2^n}}(-1)^{Tr_1^n(ay^d)+Tr_1^n(\omega\beta^{-1} y)} \\
&= W_f(\omega\beta^{-1}) \\
&= \pm 2^{\frac{n}{2}}
\end{aligned}$$

By definition 2, $F(x)$ is bent and hence the conclusion holds. □

In [41], it was proved that, if the Boolean function $Tr_1^n(ax^d)$ is bent, then x^d is a permutation over $\mathbb{F}_{2^m}$ is a sufficient condition for the vectorial Boolean function $Tr_m^n(ax^d)$ to be bent, and an open problem was left as below.

Open Problem 1 ([41])**.** *Assume that the Boolean function $Tr_1^n(ax^d)$ is bent, prove or disprove that the condition x^d is a permutation over $\mathbb{F}_{2^m}$ is necessary for the vectorial Boolean function $Tr_m^n(ax^d)$ to be bent.*

In order to answer Open problem 1, we first give the following Theorem.

Theorem 2. *Let $m \mid n$. If x^d is a permutation over $\mathbb{F}_{2^m}$, then $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$.*

Proof. Since $m \mid n$, we have $(2^m - 1) \mid (2^n - 1)$. If x^d is a permutation over $\mathbb{F}_{2^m}$, then $\gcd(d, 2^m - 1) = 1$ must hold, thus $\gcd(\gcd(d, 2^n - 1), 2^m - 1) = 1$. Therefore, $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$. □

Remark 1. Note that the inverse of Theorem 2 does not hold. For example, let $m = 2, n = 6, d = 3$, then $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$ holds. However, $\gcd(d, 2^m - 1) = 3 \neq 1$, which means that x^d is not a permutation over $\mathbb{F}_{2^m}$.

Following from Theorem 1, Theorem 2 and Remark 1, the answer to Open Problem 1 can be made, i.e., the condition that x^d is a permutation over $\mathbb{F}_{2^m}$ is not necessary.

Remark 2. By Remark 1, it is known that the sufficient condition of Theorem 1 is weaker than that in E.Pasalic et al's Theorem 1 of [41], i.e. our condition is closer to the necessary condition. By Corollary 1 and Corollary 3, it is easy to verify that the condition $(2^m - 1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$ is necessary in Gold case for $m = \frac{n}{2}$ and in Leander case for any $m \mid n$.

The following theorem provides a sufficient condition for the vectorial Boolean functions in the form $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ to be bent, which gives an answer to A.Muratović-Ribić et al.'s Open Problem 1 in [37] (named Open Problem 2 in this paper).

Theorem 3. *Let $n \geq 4$ be even, $m \mid n$, and $d_i = d_1 + v_i \frac{2^n-1}{\gcd(d_1,2^n-1)}$, where $i = 2, 3, \cdots, r$ and v_i are nonzero integers, and let $f(x) = Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$ be a Boolean bent function. If $(2^m-1) \mid \frac{2^n-1}{\gcd(d_1^2,2^n-1)}$, then the vectorial Boolean function $F(x) = Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is bent.*

Proof. Let $G_1 = \{x^{d_1} : x \in \mathbb{F}_{2^n}^*\}$ and $G_2 = \{x^{d_1^2} : x \in \mathbb{F}_{2^n}^*\}$. If $(2^m-1) \mid \frac{2^n-1}{\gcd(d_1^2,2^n-1)}$, by Lemma 2, we have $\mathbb{F}_{2^m}^* \subseteq G_2$. Thus, for all $\lambda \in \mathbb{F}_{2^m}^*$, there exist some $\gamma \in \mathbb{F}_{2^n}^*$ such that $\lambda = \gamma^{d_1^2}$ and $\gamma^{d_1} \in G_1$. For nonnegative integers v_i, $i = 2, 3, \cdots, r$, because the order of G_1 is $\frac{2^n-1}{\gcd(d_1,2^n-1)}$, if $d_i = d_1 + v_i \frac{2^n-1}{\gcd(d_1,2^n-1)}$, then $\gamma^{d_1 d_i} = \gamma^{d_1^2}$. Therefore, for all $\omega \in \mathbb{F}_{2^n}$ and for all $\lambda \in \mathbb{F}_{2^m}^*$, we have

$$\begin{aligned}
W_F(\omega,\lambda) &= \Sigma_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda F(x))+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda Tr_m^n(\sum_{i=1}^r a_i x^{d_i}))+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\lambda \sum_{i=1}^r a_i x^{d_i})+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\gamma^{d_1^2} \sum_{i=1}^r a_i x^{d_i})+Tr_1^n(\omega x)} \\
&= \Sigma_{x\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\sum_{i=1}^r a_i \gamma^{d_1 d_i} x^{d_i})+Tr_1^n(\omega x)} \\
&= \Sigma_{y\in\mathbb{F}_{2^n}} (-1)^{Tr_1^n(\sum_{i=1}^r a_i y^{d_i})+Tr_1^n(\omega \gamma^{-d_1} y)} \\
&= W_f(\omega\gamma^{-d_1}) \\
&= \pm 2^{\frac{n}{2}}
\end{aligned}$$

By definition 2 it is known that $F(x)$ is bent. □

In [37], under the condition that x^{d_1} is a permutation over $\mathbb{F}_{2^m}$, A.Muratović-Ribić et al. presented the following conclusion: If the Boolean function $Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$ is bent, then the vectorial Boolean function $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is also bent, where $d_i = d_1 + v_i(2^m-1)$ and v_i are nonnegative integers, $i = 2, \cdots, r$. In the mean time, an open problem was left as follows.

Open Problem 2 (named Open problem 1 in [37])**.** *Let $n \geq 4$ be an even, and let $m \leq \frac{n}{2}$ and $m \mid n$. Let x^{d_1} be a permutation of $\mathbb{F}_{2^m}$, and let $f(x) = Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$ be a Boolean bent function, where $m \mid \frac{n}{2}$ and $d_i = d_1 + v_i(2^m-1)$ for $i = 2, \cdots, r$ and some integers $v_i \geq 0$. Then, the function $F(x) = Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is a vectorial bent function.*

Is there a similar result to the above for the functions in the form $f(x) = Tr_1^n(\sum_{i=1}^r x^{d_i})$, if x^{d_1} is not a permutation over $\mathbb{F}_{2^m}$?

Before giving our answer to Open problem 2, we present the following Theorem.

Theorem 4. *Let $m \mid n$. If x^d is a permutation over $\mathbb{F}_{2^m}$, then $(2^m-1) \mid \frac{2^n-1}{\gcd(d^2,2^n-1)}$ must hold.*

Proof. Since $m \mid n$, we have $(2^m-1) \mid (2^n-1)$. If x^d is a permutation over $\mathbb{F}_{2^m}$, then $\gcd(d, 2^m-1) = 1$, and thus $\gcd(\gcd(d^2, 2^n-1), 2^m-1) = 1$. Therefore, $(2^m-1) \mid \frac{2^n-1}{\gcd(d^2,2^n-1)}$. □

Remark 3. Note that the inverse of Theorem 4 does not hold. For example, let $m = 2, n = 18, d = 3$, then $(2^m - 1) \mid \frac{2^n-1}{\gcd(d^2,2^n-1)}$ holds. However, $\gcd(d, 2^m - 1) = 3 \neq 1$, which means that x^d is not a permutation over $\mathbb{F}_{2^m}$.

By Theorem 3, Theorem 4 and Remark 3, we get the following theorem which is an answer to Open Problem 2.

Theorem 5. *Let $n \geq 4$ be even, $m \mid n$, $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$, $v_i = \frac{t \cdot u_i}{\gcd(d_1,2^n-1)}$, $d_i = d_1 + v_i(2^m - 1)$, where $i = 2, \cdots, r$ and u_i are nonzero integers, and let $f(x) = Tr_1^n(\sum_{i=1}^r a_i x^{d_i})$ be a Boolean bent function. If $(2^m - 1) \mid \frac{2^n-1}{\gcd(d_1^2,2^n-1)}$, then the vectorial Boolean function $F(x) = Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is bent.*

In the above, we have given two sufficient conditions for the vectorial Boolean function $F(x)$ to be bent. However, none of the sufficient conditions has been proved to be necessary, although they seem to be very close and $(2^m-1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$ in Theorem 1 is indeed sufficient and necessary conditions in some special cases, which we will be shown in the next section.

Note that in the above discussions, we focused our attention on exponents, input and output dimensions, however the coefficients of $P(x)$ have not been considered. When considering a class of Boolean bent functions as a whole, and focusing on the coefficient set of $P(x)$ such that $Tr_1^n(P(x))$ is bent, a new construction of vectorial Boolean bent functions can be described as followings.

Theorem 6. *Let $n \geq 4$ be even, $m \mid n$ and denote*

$$C = \{(c_1, c_2, \cdots, c_r) \in \mathbb{F}_{2^n}^r : \ Tr_1^n(\sum_{i=1}^r c_i x^{d_i}) \text{ is bent}\}.$$

Then the vectorial Boolean function $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is bent if and only if

$$(a_1, a_2, \cdots, a_r) \cdot \mathbb{F}_{2^m}^* \subseteq C.$$

Proof. For all $\omega \in \mathbb{F}_{2^n}$ and for all $\lambda \in \mathbb{F}_{2^m}^*$,

$$\begin{aligned} W_{Tr_m^n(\sum_{i=1}^r a_i x^{d_i})}(\omega, \lambda) &= \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^m(\lambda Tr_m^n(\sum_{i=1}^r a_i x^{d_i})) + Tr_1^n(\omega x)} \\ &= \Sigma_{x \in \mathbb{F}_{2^n}} (-1)^{Tr_1^n(\sum_{i=1}^r a_i \lambda x^{d_i}) + Tr_1^n(\omega x)} \\ &= W_{Tr_1^n(\sum_{i=1}^r a_i \lambda x^{d_i})}(\omega). \end{aligned}$$

Thus, $Tr_m^n(\sum_{i=1}^r a_i x^{d_i})$ is bent if and only if $Tr_1^n(\sum_{i=1}^r a_i \lambda x^{d_i})$ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$. For all $\lambda \in \mathbb{F}_{2^m}^*$, $Tr_1^n(\sum_{i=1}^r a_i \lambda x^{d_i})$ is bent if and only if $(a_1, a_2, \cdots, a_r)\lambda \in C$. For all $\lambda \in \mathbb{F}_{2^m}^*$, the condition $(a_1, a_2, \cdots, a_r)\lambda \in C$ is equivalent to

$$(a_1, a_2, \cdots, a_r) \cdot \mathbb{F}_{2^m}^* \subseteq C.$$

Consequently, the conclusion of the theorem holds. □

4 On the existence and constructions of vectorial Boolean bent functions

By the results and techniques presented in section 3, we analyze the bentness of several kinds of vectorial Boolean functions in the form $Tr_m^n(P(x))$, mainly about the existence and constructions of vectorial monomial bent functions in the form $Tr_m^n(ax^d)$.

In order to construct new vectorial monomial bent functions, we analyze the five known kinds of monomial bent functions in Table 1 by considering the coefficients and by considering the exponent, integer s, input and output dimensions.

Theorem 7 (Gold Case)**.** *Let $n \geq 4$ be even, $m \mid n$, $a \in \mathbb{F}_{2^n}$, $s \in \mathbb{N}$, and $d = 2^s + 1$. And denote $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$. Then the vectorial Boolean function $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^{\gcd(d,t)} \rangle, 0\}$. Moreover, there are $2^n - \frac{2^n-1}{\gcd(d,t)} - 1$ such vectorial monomial bent functions.*

Proof. By Theorem 2 in [26], the set of the coefficients such that $Tr_1^n(ax^d)$ is bent is

$$C = \{c : c \neq x^d, c, x \in \mathbb{F}_{2^n}\}.$$

Then, by Theorem 6, we get that $Tr_m^n(ax^d)$ is bent if and only if

$$\begin{aligned}
& a \cdot \mathbb{F}_{2^m}^* \subseteq \{c : c \neq x^d, c, x \in \mathbb{F}_{2^n}\} \\
\Leftrightarrow \quad & a \cdot \mathbb{F}_{2^m}^* \bigcap \{x^d : x \in \mathbb{F}_{2^n}\} = \varnothing \\
\Leftrightarrow \quad & a \notin \{x^d : x \in \mathbb{F}_{2^n}\} \cdot \mathbb{F}_{2^m}^* \\
& \text{(by Lemma 1)} \\
\Leftrightarrow \quad & a \notin \{\langle \alpha^{\gcd(t, \gcd(d, 2^n-1))} \rangle, 0\} \\
& \text{(Since } t \mid (2^n - 1)) \\
\Leftrightarrow \quad & a \notin \{\langle \alpha^{\gcd(d,t)} \rangle, 0\}
\end{aligned}$$

So we have that $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^{\gcd(d,t)} \rangle, 0\}$.

Since $|\{\langle \alpha^{\gcd(d,t)} \rangle, 0\}| = \frac{2^n-1}{\gcd(d,t)} + 1$, it is known that there are $2^n - \frac{2^n-1}{\gcd(d,t)} - 1$ such vectorial monomial bent functions. □

Example 1. Let $s = 2$, $n = 4$ and $m = 2$. Then $d = 2^s + 1 = 5$. Thus, $\langle \alpha^{\gcd(d,t)} \rangle = \langle \alpha^{\gcd(5,5)} \rangle = \langle \alpha^5 \rangle \neq \mathbb{F}_{2^4}^*$. For $\forall\ a \in \mathbb{F}_{2^4} \backslash \{\langle \alpha^5 \rangle, 0\} = \{\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{11}, \alpha^{12}, \alpha^{13}, \alpha^{14}\}$, $Tr_2^4(ax^5)$ is a vectorial monomial bent function.

Before giving another necessary and sufficient condition for vectorial Boolean functions in the form $Tr_{\frac{n}{2}}^n(ax^d)$ in Gold case to be bent, we give the following lemma.

Lemma 3. *Let the monomial Boolean function $f(x) = Tr_1^n(ax^d)$ be bent. Then* $\gcd(d, 2^{\frac{n}{2}} - 1) = 1$ *if and only if* $\gcd(d, 2^{\frac{n}{2}} + 1) \neq 1$.

Proof. **Necessity:** If $\gcd(d, 2^{\frac{n}{2}} - 1) = 1$, according to conclusion (1) of Lemma 1 in [26], then $W_f(0) = -2^{\frac{n}{2}}$. By conclusion (2) of Lemma 1 in [26], we have $\gcd(d, 2^{\frac{n}{2}} + 1) \neq 1$.

Sufficiency: Since $f(x) = Tr_1^n(ax^d)$ is bent, then $W_f(0) = \pm 2^{\frac{n}{2}}$. If $\gcd(d, 2^{\frac{n}{2}} + 1) \neq 1$, by the conclusion (2) of Lemma 1 in [26], then $W_f(0) \neq 2^{\frac{n}{2}}$. Therefore, $W_f(0) = -2^{\frac{n}{2}}$. Thus, by conclusion (1) of Lemma 1 in [26], we have $\gcd(d, 2^{\frac{n}{2}} - 1) = 1$. □

The following corollary shows that the condition $(2^m-1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$ in Theorem 1 is necessary for $m=\frac{n}{2}$ in Gold case.

Corollary 1 (Gold Case)**.** *Let $n \geq 4$ be even, $s \in \mathbb{N}$, $a \in \mathbb{F}_{2^n}$, $d=2^s+1$, and let the monomial Boolean function $Tr_1^n(ax^d)$ be bent. Then the vectorial Boolean function $Tr_{\frac{n}{2}}^n(ax^d)$ is bent if and only if $\gcd(d,2^n-1) \mid (2^{\frac{n}{2}}+1)$.*

Proof. **Necessity:** If $Tr_{\frac{n}{2}}^n(ax^d)$ is bent, by Theorem 7, we have $a \notin \{\langle \alpha^{\gcd(d,2^{\frac{n}{2}}+1)} \rangle, 0\}$, and then $\{\langle \alpha^{\gcd(d,2^{\frac{n}{2}}+1)} \rangle, 0\} \neq \mathbb{F}_{2^n}$, thus $\gcd(d,2^{\frac{n}{2}}+1) \neq 1$. By Lemma 3, we have $\gcd(d,2^{\frac{n}{2}}-1)=1$. Therefore, $\gcd(d,2^n-1)=\gcd(d,2^{\frac{n}{2}}+1)$. Hence, $\gcd(d,2^n-1) \mid (2^{\frac{n}{2}}+1)$.

Sufficiency: This follows directly from Theorem 1. □

For the Dillon exponent $d=2^{\frac{n}{2}}-1$, it was shown in [18] that $Tr_1^n(ax^d)$ is bent if and only if $K(a)=-1$, where $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, and it was shown in [24] that $Tr_1^n(ax^d)$ is bent if and only if $K(N_{\frac{n}{2}}^n(a))=-1$, where $a \in \mathbb{F}^*_{2^n}$. In [16], it was shown that $Tr_1^n(ax^{l(2^{\frac{n}{2}}-1)})$ is bent if and only if $K(a)=-1$, where $\gcd(l,2^{\frac{n}{2}}+1)=1$ and $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$. We recall Theorem 5 in [16] and Theorem 3 in [24] as the following theorem. Note that the Kloosterman sums $K(a)=\sum_{x \in \mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+ax)}$ defined in this paper is the same as in [24] and is different from that in [16].

Theorem 8 ([16, 24])**.** *Let n be even, l be an integer and $d=l(2^{\frac{n}{2}}-1)$.*

If $\gcd(l,2^{\frac{n}{2}}+1)=1$ and $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, then the monomial Boolean function $Tr_1^n(ax^d)$ is bent if and only if

$$a \in \{\beta : K(\beta)=-1, \beta \in \mathbb{F}^*_{2^{\frac{n}{2}}}\}.$$

If $l=1$ and $a \in \mathbb{F}^*_{2^n}$, then the monomial Boolean function $Tr_1^n(ax^d)$ is bent if and only if

$$a \in \{\beta : K(N_{\frac{n}{2}}^n(\beta))=-1, \beta \in \mathbb{F}^*_{2^n}\}.$$

Theorem 9 (Dillon Case)**.** *Let n be even, l be an integer, $\gcd(l,2^{\frac{n}{2}}+1)=1$ (or $l=1$), and $d=l(2^{\frac{n}{2}}-1)$, and let $a \in \{\beta : K(\beta)=-1, \beta \in \mathbb{F}^*_{2^{\frac{n}{2}}}\}$ (or $a \in \{\beta : K(N_{\frac{n}{2}}^n(\beta))=-1, \beta \in \mathbb{F}^*_{2^n}\}$ accordingly). If $(2^m-1) \mid (2^{\frac{n}{2}}+1)$, then the vectorial Boolean function $Tr_m^n(ax^d)$ is bent.*

Proof. Note that $\gcd(l,2^{\frac{n}{2}}+1)=1$, then $2^{\frac{n}{2}}+1=\frac{2^n-1}{\gcd(d,2^n-1)}$, and then $(2^m-1) \mid \frac{2^n-1}{\gcd(d,2^n-1)}$. By Theorem 1 and Theorem 8, the conclusion of the theorem holds. □

In [37], it was proved that the nonexistence of vectorial monomial bent function in the form $Tr_{\frac{n}{2}}^n(ax^d)$ for $\gcd(l,2^{\frac{n}{2}}+1)=1$ and $a \in \mathbb{F}^*_{2^{\frac{n}{2}}}$ in Dillon case. Here, for $l=1$ and $a \in \mathbb{F}^*_{2^n}$, we prove that the vectorial monomial bent functions in the form $Tr_{\frac{n}{2}}^n(ax^d)$ do not exist either. Before the proof of this conclusion, ie., theorem 10, we first give a lemma as below.

Lemma 4. *Let $n \geq 4$ be even. For $\forall\ \lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, let $n_\lambda = N_{\frac{n}{2}}^n(a\lambda)$, where $a \in \mathbb{F}^*_{2^n}$. Then $\{n_\lambda : \lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}}\} = \mathbb{F}^*_{2^{\frac{n}{2}}}$.*

Proof. Note the fact that, for $\forall\ \lambda_1, \lambda_2 \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, if $\lambda_1 \neq \lambda_2$, then $\lambda_1^{2^{\frac{n}{2}}+1} \neq \lambda_2^{2^{\frac{n}{2}}+1}$. Therefore, $\{\lambda^{2^{\frac{n}{2}}+1} : \lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}}\} = \mathbb{F}^*_{2^{\frac{n}{2}}}$. Thanks to $n_\lambda = N^n_{\frac{n}{2}}(a\lambda) = a^{2^{\frac{n}{2}}+1}\lambda^{2^{\frac{n}{2}}+1}$ and $a^{2^{\frac{n}{2}}+1} \in \mathbb{F}^*_{2^{\frac{n}{2}}}$, we have $\{n_\lambda : \lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}}\} = \mathbb{F}^*_{2^{\frac{n}{2}}}$. □

Theorem 10. *Let $n \geq 4$ be even, $a \in \mathbb{F}^*_{2^n}$ and $d = 2^{\frac{n}{2}} - 1$. Then there does not exist a vectorial monomial bent function in the form $Tr^n_{\frac{n}{2}}(ax^d)$.*

Proof. Assume the contrary that such a vectorial monomial bent function $Tr^n_{\frac{n}{2}}(ax^d)$ exists. Let $n_\lambda = N^n_{\frac{n}{2}}(a\lambda)$. By Theorem 3 in [24] and Theorem 6, we get that $Tr^n_{\frac{n}{2}}(ax^d)$ is bent if and only if $K(n_\lambda) = \sum_{x\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+n_\lambda x)} = -1$ holds for all $\lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}}$. Thus, by Lemma 4 we have

$$
\begin{aligned}
& \sum_{x\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+n_\lambda x)} = -1, \text{ for all } \lambda \in \mathbb{F}^*_{2^{\frac{n}{2}}} \\
\Leftrightarrow\ & \sum_{x,y\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1}+y)} = -1 \\
\Leftrightarrow\ & \sum_{x\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x^{-1})} \sum_{y\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(y)} = -1 \\
\Leftrightarrow\ & \Big(\sum_{x\in\mathbb{F}^*_{2^{\frac{n}{2}}}} (-1)^{Tr_1^{\frac{n}{2}}(x)}\Big)^2 = -1
\end{aligned}
$$

This is obviously impossible, which means that the assumption of the existence of vectorial monomial bent function $Tr^n_{\frac{n}{2}}(ax^d)$ is wrong, and hence the conclusion of the theorem holds. □

Theorem 11 (Kasami Case)**.** *Let $n \geq 4$ be even, $m \mid n$, $a \in \mathbb{F}_{2^n}$, $\gcd(3, n) = 1$, $\gcd(s, n) = 1$, and $d = 2^{2s} - 2^s + 1$. And denote $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$. Then the vectorial Boolean function $Tr^n_m(ax^d)$ is bent if and only if $a \notin \{\langle\alpha^{\gcd(3,t)}\rangle, 0\}$. Moreover, there are $2^n - \frac{2^n-1}{\gcd(3,t)} - 1$ such vectorial monomial bent functions.*

Proof. By Theorem 6 in [26] and Theorem 6, the proof is similar to that of Theorem 7. □

Example 2. Let $s = 3$, $n = 10$ and $m = 5$. Then $\gcd(s, n) = \gcd(3, n) = 1, d = 2^{2s} - 2^s + 1 = 57$ and $\langle\alpha^{\gcd(3,2^{\frac{n}{2}}+1)}\rangle = \langle\alpha^3\rangle \neq \mathbb{F}^*_{2^{10}}$. For $\forall\ a \in \mathbb{F}_{2^{10}}\backslash\{\langle\alpha^3\rangle, 0\}$, $Tr^{10}_5(ax^{57})$ is a vectorial monomial bent function.

Corollary 2 (Kasami Case)**.** *Let $n \geq 4$ be even, $m \mid n$, $a \in \mathbb{F}_{2^n}$, $\gcd(3, n) = 1$, $\gcd(s, n) = 1$, and $d = 2^{2s} - 2^s + 1$.*

(1) *If m is even and $3m \mid n$, or m is odd, then the vectorial Boolean function $Tr^n_m(ax^d)$ is bent if and only if $a \notin \{\langle\alpha^3\rangle, 0\}$. Moreover, there are $\frac{2(2^n-1)}{3}$ such vectorial monomial bent functions.*

(2) *If m is even and $3m \nmid n$, then there does not exist a vectorial monomial bent function in the form $Tr_m^n(ax^d)$.*

Proof. Denote $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$.

By [19], 3 is a factor of $2^n - 1$. If m is odd, then $\gcd(3, 2^m - 1) = 1$. Since $2^n - 1 = (2^m - 1)t$, then $\gcd(3, t) = 3$.

If m is even, then $\gcd(3, t) = \gcd(3, 2^{n \bmod 3m} + 2^m + 3 \cdot \lfloor \frac{n}{3m} \rfloor + 1) = \gcd(3, 2^{n \bmod 3m} + 2^m + 1)$. Because $m \mid n$, so $n \bmod 3m$ has three possible values: $0, m, 2m$. Thus, for even m, we get that

$$\gcd(3,t) = \begin{cases} \gcd(3, 2^m + 2) = 3, & 0 \equiv n (\mathrm{mod}\ 3m) \\ \gcd(3, 2^{m+1} + 1) = 1, & m \equiv n (\mathrm{mod}\ 3m) \\ \gcd(3, 2^{2m} + 2^m + 1) = 1, & 2m \equiv n (\mathrm{mod}\ 3m). \end{cases}$$

If $\gcd(3, t) = 3$, then $\{\langle \alpha^{\gcd(3,t)} \rangle, 0\} = \{\langle \alpha^3 \rangle, 0\}$. If $\gcd(3, t) = 1$, then $\{\langle \alpha^{\gcd(3,t)} \rangle, 0\} = \mathbb{F}_{2^n}$. By Theorem 11, for $\gcd(3, t) = 3$, we know that $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^3 \rangle, 0\}$, and the number of such functions in the form $Tr_m^n(ax^d)$ is $\frac{2(2^n-1)}{3}$. On the other hand, there does not exist a vectorial monomial bent function in the form $Tr_m^n(ax^d)$ for $\gcd(3, t) = 1$. □

In [26], it was proved that there exist monomial bent functions in the form $Tr_1^n(ax^d)$ with $d = (2^s + 1)^2$, and the result was extended in [17]. It was shown in [17] that the monomial Boolean function $Tr_1^{4s}(ax^{(2^s+1)^2})$ is bent if and only if there exist $\rho \in \varepsilon \mathbb{F}_{2^s}^*$ and $\beta \in \mathbb{F}_{2^n}^*$ such that $a = \rho\beta^d$ holds, where s is a positive odd integer, $n = 4s$ and $\varepsilon \in \mathbb{F}_4 \backslash \mathbb{F}_2$. Note the fact that, the condition that there exist $\rho \in \varepsilon \mathbb{F}_{2^s}^*$ and $\beta \in \mathbb{F}_{2^n}^*$ such that $a = \rho\beta^d$ is equivalent to $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \mathbb{F}_{2^s}^* \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. By Lemma 1, $\{x^d : x \in \mathbb{F}_{2^n}^*\} = \langle \alpha^{\gcd(d, 2^n-1)} \rangle = \langle \alpha^{2^s+1} \rangle$ holds. Since $\mathbb{F}_{2^s}^* = \langle \alpha^{(2^s+1)(2^{2s}+1)} \rangle$, we have $\mathbb{F}_{2^s}^* \subset \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Therefore, $\mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \mathbb{F}_{2^s}^* \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\} = \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Thus, Theorem 4.8 in [17] can be described equivalently and more succinctly as the following theorem.

Theorem 12. *Let s be positive odd, $n = 4s$ and $d = (2^s + 1)^2$. The monomial Boolean function $Tr_1^n(ax^d)$ is bent if and only if $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$.*

Lemma 5. *Let s be positive odd, $n = 4s$ and $d = (2^s+1)^2$. Then $\{x^d : x \in \mathbb{F}_{2^n}^*\} \cap \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\} = \varnothing$.*

Proof. Because s is odd, so we have $\gcd(3, (2^s-1)(2^{2s}+1)) = 1$. For all $\varepsilon \in \mathbb{F}_4 \backslash \mathbb{F}_2$, the order of ε is 3, thus $\varepsilon^{(2^s-1)(2^{2s}+1)} \neq 1$. By Lemma 1, the order of $\{x^d : x \in \mathbb{F}_{2^n}^*\}$ is $(2^s-1)(2^{2s}+1)$. Then we have $\{x^d : x \in \mathbb{F}_{2^n}^*\} \cap \mathbb{F}_4 \backslash \mathbb{F}_2 = \varnothing$. Thus, $\{x^d : x \in \mathbb{F}_{2^n}^*\} \cap \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\} = \varnothing$. □

Theorem 13 (Leander Case)**.** *Let s be a positive odd integer, $n = 4s$, $m \mid n$ and $d = (2^s + 1)^2$. Then we have*

(1) *Let $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Then the vectorial Boolean function $Tr_m^n(ax^d)$ is bent if and only if $m \mid s$.*

(2) *Let m be odd. Then the vectorial Boolean function $Tr_m^n(ax^d)$ is bent if and only if $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$.*

Proof. (1) **Necessity:** If $Tr_m^n(ax^d)$ is bent, according to Theorem 6, we obtain

$$a \cdot \mathbb{F}_{2^m}^* \subseteq C = \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}.$$

If m is even, then $\mathbb{F}_4 \backslash \mathbb{F}_2 \subseteq \mathbb{F}_{2^m}^*$. Let $a = \varepsilon \cdot \tau$, where $\varepsilon \in \mathbb{F}_4 \backslash \mathbb{F}_2$ and $\tau \in \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Then $\varepsilon^2 \in \mathbb{F}_4 \backslash \mathbb{F}_2 \subseteq \mathbb{F}_{2^m}^*$. Let $\lambda = \varepsilon^2$. Then $a\lambda = \varepsilon^3 \tau = \tau \in \{x^d : x \in \mathbb{F}_{2^n}^*\}$. By Lemma 5, we have $a\lambda \notin \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Thus, m cannot be even, i.e., m is odd. Since $m \mid 4s$, we have $m \mid s$.

Sufficiency: If $m \mid s$, then $(2^m - 1) \mid (2^s - 1)(2^{2s} + 1)$. By Theorem 1 and Theorem 12, $Tr_m^n(ax^d)$ is bent.

(2) **Necessity:** According to Theorem 12, the proof is trivial.

Sufficiency: According to the assumption that m is odd and $m \mid 4s$, we have $m \mid s$. The remainder of the proof is the same as the proof of the sufficiency of conclusion (1). □

Example 3. Let $s = 3, m = 3$. Then $n = 4s = 12$ and $d = (2^s + 1)^2 = 81$. For all $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{\beta^{81} : \beta \in \mathbb{F}_{2^{12}}^*\}$, $Tr_3^{12}(ax^{81})$ is a vectorial monomial bent function.

By conclusion (1) of Theorem 13, the following corollary can be obtained, which implies that, in Leander case, the sufficient condition in Theorem 1 is also a necessary condition, and there does not exist a vectorial Boolean function in the form $Tr_{\frac{n}{2}}^n(ax^d)$ having maximal output dimension $\frac{n}{2}$.

Corollary 3 (Leander Case)**.** *Let s be positive odd, $n = 4s$, $m \mid n$, and $d = (2^s + 1)^2$, and let $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. Then we have*

(1) *The vectorial Boolean function $Tr_m^n(ax^d)$ is bent if and only if $(2^m - 1) \mid (2^s - 1)(2^{2s} + 1)$.*

(2) *There does not exist a vectorial Boolean function in the form $Tr_m^n(ax^d)$ for even m.*

Proof. Because s is odd, so we get that $m \mid s$ if and only if $(2^m - 1) \mid (2^s - 1)(2^{2s} + 1)$. By Theorem 13, the conclusions hold. □

In [6], without considering the equivalence induced by replacing a with $a\beta^d$ for $\beta \in \mathbb{F}_{2^n}^*$, it was shown that $Tr_1^n(ax^d)$ is bent if and only if $Tr_s^{3s}(a) = 0$, where the integer $s > 1$, $n = 6s$, $d = 2^{2s} + 2^s + 1$ and $a \in \mathbb{F}_{2^{3s}}^*$. Considering the equivalence induced by replacing a with $a\beta^d$ for $\beta \in \mathbb{F}_{2^n}^*$, the following theorem follows from Theorem 3 in [6].

Theorem 14. *Let $s > 1$ be an integer, $n = 6s$ and $d = 2^{2s} + 2^s + 1$. The monomial Boolean function $Tr_1^n(ax^d)$ is bent if and only if $a \in \{\rho : Tr_s^{3s}(\rho) = 0, \rho \in \mathbb{F}_{2^{3s}}^*\} \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$.*

Theorem 15 (Canteaut-Charpin-Kyureghyan Case)**.** *Let $s > 1$ be an integer, $n = 6s$ and $d = 2^{2s} + 2^s + 1$, and let $a \in \{\rho : Tr_s^{3s}(\rho) = 0, \rho \in \mathbb{F}_{2^{3s}}^*\} \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$. If $m \mid 2s$, then the vectorial Boolean function $Tr_m^n(ax^d)$ is bent.*

Proof. Due to the equality $2^n - 1 = d(2^{2s} - 1)(2^{2s} - 2^s + 1)$, we have $\frac{2^n - 1}{\gcd(d, 2^n - 1)} = (2^{2s} - 1)(2^{2s} - 2^s + 1)$. If $m \mid 2s$, then $(2^m - 1) \mid (2^{2s} - 1)(2^{2s} - 2^s + 1)$. By Theorem 1 and Theorem 14, $Tr_m^n(ax^d)$ must be bent. □

Now we give a construction of vectorial Boolean bent functions in the form $Tr_{\frac{n}{2}}^n(\sum_{i=1}^{2^s - 1} x^{d_i})$, where d_i's are Niho exponents.

Theorem 16 (Niho Case)**.** *Let n be even, s be a positive integer, $s < \frac{n}{2}$ and $\gcd(s, \frac{n}{2}) = 1$, and $a + a^{2^{\frac{n}{2}}} \neq 0$. If $m \mid \frac{n}{2}$, then $Tr_m^n(\sum_{i=1}^{2^s-1} ax^{(i\cdot 2^{\frac{n}{2}-s}+1)(2^{\frac{n}{2}}-1)+1})$ is bent.*

Proof. If $m \mid \frac{n}{2}$, then $(2^m - 1) \mid (2^{\frac{n}{2}} - 1)$, thus $2^{\frac{n}{2}} \equiv 1 (\mathrm{mod}\ 2^m - 1)$. For all $\lambda \in \mathbb{F}_{2^m}^*$, we have that $\lambda + (a\lambda)^{2^{\frac{n}{2}}} = (a + a^{\frac{n}{2}})\lambda \neq 0$.

And by Theorem 2 in [27], we have

$$(a, a, \cdots, a) \cdot \mathbb{F}_{2^m}^* \subseteq C = \{(c_1, c_2, \cdots, c_{2^s-1}) : Tr_1^n(\sum_{i=1}^{2^s-1} c_i x^{(i\cdot 2^{\frac{n}{2}-s}+1)(2^{\frac{n}{2}}-1)+1}) \text{ is bent}\}$$

By Theorem 6, $Tr_m^n(\sum_{i=1}^{2^s-1} ax^{(i\cdot 2^{\frac{n}{2}-s}+1)(2^{\frac{n}{2}}-1)+1})$ must be bent. □

5 Conclusions

This paper presents three constructions of vectorial Boolean bent functions and provides answers to two open problems raised in [41] and in [37] respectively. Moreover, the bent properties of several kinds of vectorial Boolean functions are analyzed. In brief, for $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$, we get the following results.

- In Gold case, $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^{\gcd(d,t)} \rangle, 0\}$, and $Tr_{\frac{n}{2}}^n(ax^d)$ is bent if and only if $\gcd(d, 2^n - 1) \mid (2^{\frac{n}{2}} + 1)$.
- In Dillon case, $Tr_m^n(ax^d)$ is bent if $(2^m - 1) \mid (2^{\frac{n}{2}} + 1)$, and there does not exist a vectorial monomial bent function in the form $Tr_{\frac{n}{2}}^n(ax^{2^{\frac{n}{2}}+1})$ for $a \in \mathbb{F}_{2^n}^*$.
- In Kasami case, $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^{\gcd(3,t)} \rangle, 0\}$. Moreover, $Tr_m^n(ax^d)$ is bent if and only if $a \notin \{\langle \alpha^3 \rangle, 0\}$, when m is even and $3m \mid n$ or m is odd, and there does not exist a vectorial monomial bent function in the form $Tr_m^n(ax^d)$, when m is even and $3m \nmid n$.
- In Leander case, $Tr_m^n(ax^d)$ is bent if and only if $m \mid s$, when $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$, and $Tr_m^n(ax^d)$ is bent if and only if $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$, when m is odd. Moreover, when $a \in \mathbb{F}_4 \backslash \mathbb{F}_2 \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$, $Tr_m^n(ax^d)$ is bent if and only if $(2^m - 1) \mid (2^s - 1)(2^{2s} + 1)$, and there is no vectorial Boolean function in the form $Tr_m^n(ax^d)$ for even m.
- In Canteaut-Charpin-Kyureghyan Case, $Tr_m^n(ax^d)$ is bent if $m \mid 2s$ holds.

  In addition, we proved that $Tr_m^n(\sum_{i=1}^{2^s-1} ax^{d_i})$ is bent if $m \mid \frac{n}{2}$ holds, where d_is are some specific Niho exponents and $a + a^{2^{\frac{n}{2}}} \neq 0$.

References

[1] Eli Biham, Orr Dunkelman, and Nathan Keller. Related-key boomerang and rectangle attacks. In *Advances in Cryptology–EUROCRYPT 2005*, pages 507–525. Springer, 2005.

[2] Eli Biham and Adi Shamir. Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, 4(1):3–72, 1991.

[3] Lilya Budaghyan and Claude Carlet. CCZ-equivalence of bent vectorial functions and related constructions. *Designs, Codes and Cryptography*, 59(1-3):69–87, 2011.

[4] Lilya Budaghyan, Claude Carlet, Tor Helleseth, Alexander Kholosha, and Sihem Mesnager. Further results on Niho bent functions. *Information Theory, IEEE Transactions on*, 58(11):6979–6985, 2012.

[5] Lilya Budaghyan, Alexander Kholosha, Claude Carlet, and Tor Helleseth. Univariate Niho bent functions from o-polynomials. *arXiv preprint arXiv:1411.2394*, 2014.

[6] Anne Canteaut, Pascale Charpin, and Gohar M Kyureghyan. A new class of monomial bent functions. *Finite Fields and Their Applications*, 14(1):221–241, 2008.

[7] Claude Carlet. A construction of bent function. In *Proceedings of the third international conference on Finite fields and applications*, pages 47–58. Cambridge University Press, 1996.

[8] Claude Carlet. A larger class of cryptographic Boolean functions via a study of the Maiorana-Mcfarland construction. In *Advances in CryptologyCRYPTO 2002*, pages 549–564. Springer, 2002.

[9] Claude Carlet. On the confusion and diffusion properties of Maiorana–Mcfarland's and extended Maiorana–Mcfarland's functions. *Journal of Complexity*, 20(2):182–204, 2004.

[10] Claude Carlet. Boolean functions for cryptography and error correcting codes. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 2:257, 2010.

[11] Claude Carlet. Vectorial Boolean functions for cryptography. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, 134:398–469, 2010.

[12] Claude Carlet, Tor Helleseth, Alexander Kholosha, and Sihem Mesnager. On the dual of bent functions with 2^r Niho exponents. 2011 IEEE International Symposium on Information Theory Proceedings (ISIT), 2011.

[13] Claude Carlet and Sihem Mesnager. On the construction of bent vectorial functions. *International Journal of Information and Coding Theory*, 1(2):133–148, 2010.

[14] Claude Carlet and Sihem Mesnager. On Dillon's class $\mathcal{H}$ of bent functions, Niho bent functions and o-polynomials. *Journal of Combinatorial Theory, Series A*, 118(8):2392–2410, 2011.

[15] Ayça Çeşmelioğlu and Wilfried Meidl. A construction of bent functions from plateaued functions. *Designs, codes and cryptography*, 66(1-3):231–242, 2013.

[16] Pascale Charpin and Guang Gong. Hyperbent functions, Kloosterman sums, and Dickson polynomials. *IEEE transactions on information theory*, 54(9):4230–4238, 2008.

[17] Pascale Charpin and Gohar M Kyureghyan. Cubic monomial bent functions: A subclass of $\mathcal{M}^*$. *SIAM Journal on Discrete Mathematics*, 22(2):650–665, 2008.

[18] John Francis Dillon. *Elementary Hadamard difference sets.* PhD thesis, University of Maryland, College Park., 1974.

[19] John Francis Dillon and Hans Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

[20] Hans Dobbertin and Gregor Leander. A survey of some recent results on bent functions. In *Sequences and Their Applications-SETA 2004*, pages 1–29. Springer, 2005.

[21] Hans Dobbertin, Gregor Leander, Anne Canteaut, Claude Carlet, Patrick Felke, and Philippe Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, 113(5):779–798, 2006.

[22] Deshuai Dong, Xue Zhang, Longjiang Qu, and Shaojing Fu. A note on vectorial bent functions. *Information Processing Letters*, 113(22):866–870, 2013.

[23] Miia Hermelin, Joo Yeon Cho, and Kaisa Nyberg. Statistical tests for key recovery using multidimensional extension of Matsuis algorithm 1. In *EUROCRYPT*, 2009.

[24] Philippe Langevin and Gregor Leander. Monomial bent functions and Stickelberger's theorem. *Finite Fields and Their Applications*, 14(3):727–742, 2008.

[25] Gregor Leander and Alexander Kholosha. Bent functions with 2^r Niho exponents. *IEEE transactions on information theory*, 52(12):5529–5532, 2006.

[26] Nils Gregor Leander. Monomial bent functions. *IEEE transactions on information theory*, 52(2):738–743, 2006.

[27] Nian Li, Tor Helleseth, Alexander Kholosha, and Xiaohu Tang. On the Walsh transform of a class of functions from Niho exponents. *IEEE transactions on information theory*, 59(7):4662–4667, 2013.

[28] Mitsuru Matsui. Linear cryptanalysis method for DES cipher. In *Advances in CryptologyEUROCRYPT93*, pages 386–397. Springer, 1994.

[29] Robert L McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory, Series A*, 15(1):1–10, 1973.

[30] Sihem Mesnager. A new class of bent functions in polynomial forms. In *Proceedings of international Workshop on Coding and Cryptography, WCC 2009*, pages 5–18. 2009.

[31] Sihem Mesnager. Bent and hyper-bent functions in polynomial form and their link with some exponential sums and Dickson polynomials. *IEEE transactions on information theory*, 57(9):5996–6009, 2011.

[32] Sihem Mesnager. A new class of bent and hyper-bent Boolean functions in polynomial forms. *Designs, Codes and Cryptography*, 59(1-3):265–279, 2011.

[33] Sihem Mesnager. Bent vectorial functions and linear codes from o-polynomials. *Designs, Codes and Cryptography*, pages 1–18, 2013.

[34] Sihem Mesnager. Several new infinite families of bent functions and their duals. *IEEE Transactions on Information Theory*, 60(7):4397–4407, 2014.

[35] Sihem Mesnager. Bent functions from spreads. *Topics in Finite Fields*, 632:295, 2015.

[36] Sihem Mesnager and J-P Flori. Hyperbent functions via Dillon-like exponents. *Information Theory, IEEE Transactions on*, 59(5):3215–3232, 2013.

[37] Amela Muratović-Ribić, Enes Pasalic, and Samed Bajric. Vectorial bent functions from multiple terms trace functions. *IEEE transactions on information theory*, 60(2):1337–1347, 2014.

[38] Kaisa Nyberg. Perfect nonlinear S-boxes. In *Advances in Cryptology-EUROCRYPT'91*, pages 378–386. Springer, 1991.

[39] Kaisa Nyberg. On the construction of highly nonlinear permutations. In *Advances in CryptologyEUROCRYPT92*, pages 92–98. Springer, 1993.

[40] Kaisa Nyberg. New bent mappings suitable for fast implementation. In *Fast software encryption*, pages 179–184. Springer, 1994.

[41] Enes Pasalic and Wei-Guo Zhang. On multiple output bent functions. *Information Processing Letters*, 112(21):811–815, 2012.

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

[43] Takashi Satoh, Tetsu Iwata, and Kaoru Kurosawa. On cryptographically secure vectorial Boolean functions. In *Advances in Cryptology-ASIACRYPT99*, pages 20–28. Springer, 1999.