On the Primary 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

Vectorial Boolean bent functions, which possess the maximal nonlinearity and the minimum differential uniformity, contribute to optimum resistance against linear cryptanalysis and differential cryptanalysis for the cryptographic algorithms that adopt them as nonlinear components. This paper is devoted to the new primary constructions of vectorial Boolean bent functions, including four types: vectorial monomial bent functions, vectorial Boolean bent functions with multiple trace terms, $\mathcal{H}$ vectorial functions and $\mathcal{H}$-like vectorial functions. For vectorial monomial bent functions, this paper answers one open problem proposed by E. Pasalic et al. and characterizes the vectorial monomial bent functions corresponding to the five known classes of bent exponents. For the vectorial Boolean bent functions with multiple trace terms, this paper answers one open problem proposed by A. Muratović-Ribić et al., presents six new infinite classes of explicit constructions and shows the nonexistence of the vectorial Boolean bent functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^k}$ of the form $\sum_{i=1}^{2^{k-2}} Tr_k^n(ax^{(2i-1)(2^k-1)})$ with $n = 2k$ and $a \in \mathbb{F}_{2^k}^*$. Moreover, $\mathcal{H}$ vectorial functions are further characterized. In addition, a new infinite class of vectorial Boolean bent function named as $\mathcal{H}$-like vectorial functions are derived, which includes $\mathcal{H}$ vectorial functions as a subclass.

1 Introduction

Vectorial Boolean functions, which are widely used in block ciphers, stream ciphers and Hash functions, paly an important role in cryptography. The security of the cryptographic algorithms, adopting vectorial Boolean functions as nonlinear components, usually depends on the cryptographic properties of the vectorial Boolean functions adopted. The nonlinearity and the differential uniformity of the adopted vectorial Boolean functions are two parameters that measure the resistence of the cryptographic algorithms against linear cryptanalysis [27, 39] and differential cryptanalysis [1, 2] respectively. The vectorial Boolean functions possessing the maximal nonlinearity, which is the optimal nonlinearity, are referred to as

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

vectorial Boolean bent functions. The concept bent of vectorial Boolean functions, which is an extension of Boolean bent functions [56], was first considered by Nyberg in [51], where it was shown that bent (n, m)-functions (i.e., the 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 named as *perfect nonlinear functions* [17, 51], for the reason possessing the minimum differential uniformity, which is the optimal differential uniformity. Thus, the constructions of vectorial Boolean bent functions have both theoretical significance and practical applications.

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.

Strict Maiorana-McFarland vectorial functions, extended Maiorana-McFarland vectorial functions and general Maiorana-McFarland vectorial functions are the three infinite classes of vectorial Boolean bent functions [11, 51, 52, 54, 57] stemming from the Maiorana-McFarland constructions of Boolean bent functions [22, 40]. In the light of the Partial Spread constructions of Boolean bent functions [22], two infinite classes of vectorial Boolean bent functions, $\mathcal{PS}_{ap}$ vectorial functions [11] and Partial Spread vectorial functions [15], were presented. In [5], two infinite classes of vectorial Boolean bent functions were introduced by investigating the bent component functions of non-bent vectorial Boolean functions. Two infinite classes of *vectorial hyper-bent functions*, which is a subclass of vectorial Boolean bent functions, were discussed in [38, 61]. A vectorial hyper-bent function is the vectorial Boolean function that every one of its component functions is a *hyper-bent function*, and the Boolean bent function $f(x)$ on $\mathbb{F}_{2^n}$ is a hyper-bent function if $f(x^j)$ is also bent for any $\gcd(j, 2^n - 1) = 1$ [61]. All the above infinite classes of vectorial Boolean bent functions are primary constructions, and a few primary constructions of vectorial Boolean bent functions which are not infinite classes can be found in [15]. Recently, the primary constructions of some other infinite classes of vectorial Boolean bent functions have attracted a lot of attentions.

The bent (n, m)-functions of the form $Tr_m^n(ax^d)$ are referred to as *vectorial monomial bent functions*, which are *monomial bent functions* if $m = 1$, i.e., the Boolean bent functions of the form $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$, and exist only if $\gcd(d, 2^n - 1) \neq 1$ [34], where d is integer and $a \in \mathbb{F}_{2^n}^*$. In [55], it was shown that $Tr_m^n(ax^d)$ is a vectorial monomial bent function if $Tr_1^n(ax^d)$ is a monomial bent function and x^d is a permutation on $\mathbb{F}_{2^m}$, i.e., $\gcd(d, 2^m - 1) = 1$, and some classes of vectorial monomial bent functions with the Kasami exponent, the Leander exponent and the Canteaut-Charpin-Kyureghyan exponent were investigated. However, whether the condition that $\gcd(d, 2^m - 1) = 1$ is necessary or not and how to relax the condition $\gcd(d, 2^m - 1) = 1$ for $Tr_m^n(ax^d)$ to be bent are unknown and left open in [55]. In [58], a counter example to show that $\gcd(d, 2^m - 1) = 1$ is not necessary for $Tr_m^n(ax^d)$ to be bent was found. In [26], it was shown that $Tr_k^n(ax^d)$, with $n = 2k$, is a vectorial monomial bent function if $\gcd(d, 2^n - 1) \mid (2^k + 1)$ and $Tr_1^n(ax^d)$ is a monomial bent function with the Gold exponent or the Kasimi exponent. However, in [26], whether the condition $\gcd(d, 2^n - 1) \mid (2^k + 1)$ is necessary or not for $Tr_k^n(ax^d)$ to be bent is unknown. In [48], it was proved that there does not exist a vectorial monomial bent function of the form $Tr_k^n(ax^d)$ with the Dillon exponent for $a \in \mathbb{F}_{2^k}^*$, $d = s(2^k - 1)$ and $\gcd(s, 2^k + 1) = 1$. Although many works have been done, the characterization of vectorial monomial bent functions is still not clear.

In [48], the general construction of the bent (n,m)-functions of the form $Tr_m^n(a_1x^{d_1}+\sum_{i=2}^{j}a_ix^{d_1+v_i(2^m-1)})$ was studied, where $a_i\in\mathbb{F}_{2^n}^*$ for $i=1,2,\cdots,j$. An (n,m)-functions $Tr_m^n(a_1x^{d_1}+\sum_{i=2}^{j}a_ix^{d_1+v_i(2^m-1)})$ was shown in [48] to be bent if $\gcd(d_1,2^m-1)=1$ and the Boolean function $Tr_1^n(a_1x^{d_1}+\sum_{i=2}^{j}a_ix^{d_1+v_i(2^m-1)})$ on $\mathbb{F}_{2^n}$ is bent, where v_i is nonnegative integer for $i=2,3,\cdots,j$. In [48], whether the condition that $\gcd(d_1,2^m-1)=1$ is necessary or not was unknown, and an open problem (i.e., Open Problem 1 in [48]) left was to find a similar result to the above conclusion (i.e., Theorem 1 in [48]) with $\gcd(d_1,2^m-1)\neq 1$.

The explicit constructions of vectorial Boolean bent functions with multiple trace terms are rare, and only four classes of them can be found in the public literatures. The bent (n,m)-functions of the form $Tr_m^n(a_1x^{d_1}+a_2x^{d_2})$ are named as *vectorial binomial bent functions*, which are *binomial bent functions* if $m=1$, i.e., the Boolean bent functions of the form $Tr_1^n(a_1x^{d_1}+a_2x^{d_2})$ on $\mathbb{F}_{2^n}$, where $a_1,a_2\in\mathbb{F}_{2^n}^*$. Based on the three infinite classes of binomial bent functions given in [25], three infinite classes of the vectorial binomial bent functions with two Niho exponents and $m=k$ were presented in [48]. In [49], an infinite class of the hyper-bent (n,k)-functions of the form $Tr_k^n(\sum_{i=1}^{2^k}a_ix^{i(2^k-1)})$ was presented.

In [45], a new primary construction named as $\mathcal{H}$ *vectorial functions* was introduced, i.e., the infinite class of the vectorial Boolean bent functions of the form $yG(zy^{2^k-2})$, where $(y,z)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ and G is an o-polynomial on $\mathbb{F}_{2^k}$.

This paper is devoted to new primary constructions of vectorial Boolean bent functions. Four types of vectorial Boolean bent functions, i.e., vectorial monomial bent functions, vectorial Boolean bent functions with multiple trace terms, $\mathcal{H}$ vectorial functions and $\mathcal{H}$-like vectorial functions, are investigated.

Firstly, several general constructions of vectorial monomial bent functions are given, which imply answers to one open problem proposed by E. Pasalic et al. in [55], i.e., given a monomial bent function $Tr_1^n(ax^d)$, we present several conditions which are much closer to the sufficient and necessary conditions for $Tr_m^n(ax^d)$ to be bent than the condition that $\gcd(d,2^m-1)=1$. Subsequently, the vectorial monomial bent functions corresponding to the five known classes of bent exponents are characterized. For vectorial monomial bent functions, the main results are the existence and constructions of the vectorial monomial bent functions corresponding to the five known classes of bent exponents.

In the second place, several general constructions of the bent (n,m)-functions of the form $Tr_m^n(\sum_{i=1}^{j}a_ix^{d_i})$, where $a_i\in\mathbb{F}_{2^n}^*$ for $i=1,2,\cdots,j$, are derived, which are answers to one open problem proposed by A. Muratović-Ribić et al. in [48], i.e., we give similar results to Theorem 1 in [48] with $\gcd(d_1,2^m-1)\neq 1$. Then we focus on the explicit constructions of the vectorial Boolean bent functions with multiple trace terms. Six new infinite classes of the explicit constructions of such bent (n,m)-functions are obtained, i.e., one classes with 2^{r-1} Niho exponents, where $r<k$ and $\gcd(r,k)=1$, four classes with some Gold exponents and one class with 2^{k-2} Dillon exponents. For the vectorial Boolean bent functions with multiple trace terms, the main results are the six infinite classes of the explicit constructions. Furthermore, it is shown that there does not exist a bent (n,k)-function of the form $\sum_{i=1}^{2^{k-2}}Tr_k^n(ax^{(2i-1)(2^k-1)})$, where $a\in\mathbb{F}_{2^k}^*$.

Moreover, by the relation between the projectively equivalence of o-polynomials and the corresponding $\mathcal{H}$ functions, we further characterize $\mathcal{H}$ vectorial functions that the vectorial Boolean bent functions of the form $Tr_m^k(yG(zy^{2^k-2}))$, where $(y,z)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}$ and G is an o-polynomial on $\mathbb{F}_{2^k}$.

In addition, we present a new infinite class of the vectorial Boolean bent functions of the form $Tr_m^k(yV(zy^{2^k-2^{lc}})$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $l \mid k$, $c \in \mathbb{Z}_{\frac{k}{l}}$ and V is a φ-polynomial on $\mathbb{F}_{2^k}$ corresponding to $\Phi \equiv c$, and name it as $\mathcal{H}$-like vectorial functions, which includes $\mathcal{H}$ vectorial functions as a subclass.

The rest of this paper is organized as follows. Section 2 provides some preliminaries for the description of the paper and introduces the basic idea of the constructions of vectorial Boolean bent functions. Section 3 discusses vectorial monomial bent functions. Section 4 analyzes the vectorial Boolean bent functions with multiple trace terms. Section 5 characterizes $\mathcal{H}$ vectorial functions. Section 6 presents $\mathcal{H}$-like vectorial functions. And Section 7 concludes this paper.

2 Preliminaries

Throughout this paper, let k, m be two positive integers, $n = 2k$, $\mathbb{F}_{2^k}$ denote the Galois field $GF(2^k)$, $\mathbb{F}_{2^k}^* = \mathbb{F}_{2^k} \setminus \{0\}$, $\mathbb{F}_{2^n}$ be identified with $\mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and α be a primitive element of $\mathbb{F}_{2^n}$, and let $t = 2^{n-m} + 2^{n-2m} + \cdots + 2^m + 1$ if $m \mid n$.

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

$$Tr_m^k(z) = z + z^{2^m} + z^{2^{2m}} + \cdots + z^{2^{(\frac{n}{m}-1)m}}.$$

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

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

$$N_m^k(z) = z \cdot z^{2^m} \cdot z^{2^{2m}} \cdots z^{2^{(\frac{k}{m}-1)m}}.$$

A mapping $G : \mathbb{F}_{2^k} \to \mathbb{F}_{2^m}$ is referred to as a vectorial Boolean function, which is also known as a $(k,m)-$function, a multiple output Boolean function or an S-box, particularly, G is a Boolean function on $\mathbb{F}_{2^k}$ if $m = 1$. The $(k,m)-$function G can be represented as

$$G(z) = (g_1(z), g_2(z), \cdots, g_m(z)),$$

where $g_1(z)$, $g_2(z), \cdots, g_m(z)$ are m Boolean functions on $\mathbb{F}_{2^k}$ and called the *coordinate functions* of G. All nonzero linear combinations of the coordinate functions are called the *component functions* of G, and can be represented as $v \cdot G$ or $Tr_1^m(\lambda \cdot G)$, where $0 \neq v \in \mathbb{F}_2^m$ and $\lambda \in \mathbb{F}_{2^m}^*$.

G can be uniquely represented in the univariate polynomial representation as

$$G(z) = \sum_{i=0}^{2^k-1} a_i z^i, \ a_i \in \mathbb{F}_{2^k}.$$

The algebraic degree of G, denoted by $deg(G)$, is defined as

$$deg(G) = \max\{wt(i) : 0 \leq i \leq 2^k - 1, a_i \neq 0\},$$

where $wt(i)$ denotes the *Hamming weight* of i, i.e., the number of 1's of i in its 2-adic representation. G is called an *affine vectorial Boolean function* if $deg(G) \leq 1$. Particularly, the *linear vectorial Boolean functions* are the affine vectorial Boolean functions with the algebraic degree being 1 whose constant terms are null, and with the algebraic degree being 0 (i.e., constant functions).

For $m \mid k$, G can also be represented in a non-unique way as

$$G(z) = Tr_m^k(P(z)),\ P(z) \in \mathbb{F}_{2^k}[z].$$

An (n, m)-function F can be uniquely represented in the bivariate polynomial representation as

$$F(y, z) = \sum_{0 \le i_1, i_2 \le 2^k - 1} a_{i_1,i_2} y^{i_1} z^{i_2},\ (y, z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}, a_{i_1,i_2} \in \mathbb{F}_{2^k}.$$

The algebraic degree of F in the bivariate polynomial representation is

$$deg(F) = \max\{wt(i_1) + wt(i_2) : 0 \le i_1, i_2 \le 2^k - 1, a_{i_1,i_2} \ne 0\}.$$

For $m \mid k$, F can also be represented non-uniquely as

$$F(y, z) = Tr_m^k(P(y, z)),\ P(y, z) \in \mathbb{F}_{2^k}[y, z].$$

The *nonlinearity* of the Boolean function g on $\mathbb{F}_{2^k}$, denoted by $nl(g)$, is defined as

$$nl(g) = \min_{g' \in \mathbb{A}_n} d(g, g'),$$

where $\mathbb{A}_n$ is the set of all the affine Boolean functions on $\mathbb{F}_{2^k}$ and $d(g, g')$ is the *Hamming distance* between g and g', i.e., the cardinality of the set $\{x \in \mathbb{F}_{2^k} : g(x) \ne g'(x)\}$.

The nonlinearity of g can be measured as

$$nl(g) = 2^{k-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^k}} W_g(\omega),$$

where $W_g(\omega)$ is the *Walsh transform* of g and defined as

$$W_g(\omega) = \sum_{z \in \mathbb{F}_{2^k}} (-1)^{g(z)+Tr_1^k(\omega z)},\ \forall\ \omega \in \mathbb{F}_{2^k}.$$

The *Walsh spectrum* of g is the set $\{W_g(\omega) : \omega \in \mathbb{F}_{2^k}\}$.

The well known Parseval's equation

$$\sum_{\omega \in \mathbb{F}_{2^k}} (W_g(\omega))^2 = 2^{2k},$$

implies that, for the Boolean function g on $\mathbb{F}_{2^k}$,

$$nl(g) \le 2^{k-1} - 2^{\frac{k}{2}-1}.$$

Definition 1. *Let f be a Boolean function on $\mathbb{F}_{2^n}$. Then f is referred to as a Boolean bent function if and only if $nl(f) = 2^{n-1} - 2^{\frac{n}{2}-1}$.*

The *nonlinearity* of the (k, m)-function G, denoted by $nl(G)$, is defined as

$$nl(G) = \min\{nl(Tr_1^m(\lambda G)) : \lambda \in \mathbb{F}_{2^m}^*\},$$

By the relation between the nonlinearity of Boolean functions and the Walsh transform, the nonlinearity of G can be measured as

$$nl(G) = 2^{k-1} - \frac{1}{2} \max_{\omega \in \mathbb{F}_{2^k}} \max_{\lambda \in \mathbb{F}_{2^m}^*} W_G(\omega, \lambda).$$

where $W_G(\omega, \lambda)$ is the *extended Walsh transform* of G and defined as

$$W_G(\omega, \lambda) = \sum_{z \in \mathbb{F}_{2^k}} (-1)^{Tr_1^m(\lambda F(z)) + Tr_1^k(\omega z)}, \ \forall\ \omega \in \mathbb{F}_{2^k}, \forall\ \lambda \in \mathbb{F}_{2^m}^*.$$

The *extended Walsh spectrum* of G is the set $\{W_G(\omega, \lambda) : \omega \in \mathbb{F}_{2^k}, \lambda \in \mathbb{F}_{2^m}^*\}$.

The Parseval's equation also implies that, for the (k, m)-function G,

$$nl(F) \leq 2^{k-1} - 2^{\frac{k}{2}-1}.$$

Among the many equivalent definitions of vectorial Boolean bent functions, we recall the following two definitions.

Definition 2. *Let F be an (n, m)-function. Then F is referred to as a vectorial Boolean bent function if and only if $nl(F) = 2^{n-1} - 2^{\frac{n}{2}-1}$.*

Definition 3. *A vectorial Boolean function is bent if and only if all of its component functions are Boolean bent functions.*

We recall the binary Kloosterman sums on $\mathbb{F}_{2^k}$, which is an classical exponential sums.

Definition 4. *The binary Kloosterman sums on $\mathbb{F}_{2^k}$ is defined as*

$$K(a) = \sum_{z \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k(z^{2^k-2} + az)}, \ \forall\ a \in \mathbb{F}_{2^k}.$$

2.1 The basic idea of constructing vectorial Boolean bent functions

Definition 3, which indicates that the bent property of vectorial Boolean functions can be characterized by their component functions, is the common underlying idea of all the constructions of vectorial Boolean bent functions.

The following theorem give the presentation of this idea over finite field.

Theorem 1 ([11, 51])**.** *An (n, m)-function F is bent if and only if $Tr_1^m(\lambda F)$ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$.*

To construct vectorial Boolean bent functions, it is the essential issue to ensure that $Tr_1^m(\lambda F)$ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$. In the following, we give two methods to deal with this issue.

2.1.1 The invariance of bentness under EA-equivalence

The equivalence relations of vectorial Boolean functions are important tools to study the existence, constructions and various properties of vectorial Boolean functions. The extended affine equivalence (EA-equivalence) and the Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence) are two greatly useful equivalence relations.

Definition 5 ([3, 8, 53]). *Let G, G' be two (k,m)-functions and*

$$G' = A_1 \circ G \circ A_2 + A_3.$$

The corresponding concepts of equivalence between G and G' are called:

- *Linear equivalence, if A_1 and A_2 are two linear permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_3 is null.*
- *Affine equivalence, if A_1 and A_2 are two affine permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_3 is null.*
- *Extended affine equivalence (EA-equivalence), if A_1 and A_2 are two affine permutations on $\mathbb{F}_{2^m}$ and $\mathbb{F}_{2^k}$ respectively, and A_3 is an affine (k,m)-function.*

Clearly, the relations among the three equivalence are: linear equivalence ⊂ affine equivalence ⊂ EA-equivalence.

Definition 6 ([3, 8, 13]). *Let G, G' be two (k,m)-functions and*

$$A(GR_G) = GR_{G'},$$

where $GR_G = (z, G(z))$ and $GR_{G'} = (z, G'(z))$ are graphs of $G(z)$ and $G'(z)$ respectively. The corresponding concept of equivalence between G and G' is called Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence) if A is an affine permutation on $\mathbb{F}_{2^k} \times \mathbb{F}_{2^m}$.

CCZ-equivalence is a more general concept than EA-equivalence [4, 8]. Under EA-equivalence, the algebraic degree, the nonlinearity and the differential uniformity [8] are invariable. Under CCZ-equivalence, the nonlinearity and the differential uniformity [8] are also invariable, however, the algebraic degree is not always the same. For example, any permutation and its inverse are CCZ-equivalent [13], but the algebraic degree of a permutation is often different from its inverse. For $k > 5$, $m > 1$ and $m \mid k$, the concept of CCZ-equivalence of (k,m)-functions is strictly more general than EA-equivalence [4]. Although CCZ-equivalence is more general than EA-equivalence, the two concepts of equivalent relations are equivalent in some special cases [3], such as for Boolean functions [4] and vectorial Boolean bent functions [5].

Since the nonlinearity of vectorial Boolean functions is an invariant under EA-equivalence, the bent property of vectorial Boolean functions is invariable under EA-equivalence [11]. Thus, for an (n,m)-function F and $\forall\ \lambda \in \mathbb{F}_{2^m}^*$, $Tr_1^m(\lambda F)$ is bent if it is EA-equivalent to some Boolean bent functions. By Theorem 1, the following conclusion can be obtained.

Theorem 2. *Let F be an (n,m)-function, and F have a bent component function f. Then F is bent if $Tr_1^m(\lambda F)$ is EA-equivalent to f for all $\lambda \in \mathbb{F}_{2^m}^*$.*

To construct some bent (n,m)-function F that has a bent component function f, we may consider how to ensure $Tr_1^m(\lambda F)$ to be EA-equivalent to f for all $\lambda \in \mathbb{F}_{2^m}^*$.

2.1.2 The class of a bent component function

Boolean bent functions have been studied extensively in public literatures, and the characterizations of many classes of Boolean bent functions are clear. For an (n,m)-function F, if it can be determined that $Tr_1^m(\lambda F)$ belongs to some classes of Boolean bent function for every $\lambda \in \mathbb{F}_{2^m}$, then the bent property of F is sure. By Theorem 1, the following conclusion can be obtained.

Theorem 3. *Let F be an (n,m)-function, and F have a bent component function f. Then F is bent if $Tr_1^m(\lambda F)$ and f belong to the same class of Boolean bent functions for all $\lambda \in \mathbb{F}_{2^m}^*$.*

To construct some bent (n,m)-function F that has a bent component function f, we may focus on the class of Boolean bent functions that f belongs to.

Remark 1. *Usually, if two Boolean functions are EA-equivalent, they belong to the same class of Boolean functions. Thus, Theorem 3 almost always includes Theorem 2 as a special case.*

Hereafter, we will study the existence and constructions of vectorial Boolean bent functions by Theorem 1, Theorem 2 or Theorem 3 according to the situation.

3 Vectorial monomial bent functions

An integer d (in the sense of modulo 2^n-1) is named as a *bent exponent* if there exists an element $a \in \mathbb{F}_{2^n}^*$ such that the Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent. So far, five classes of bent exponents [43] have been found (see Table 1), and the corresponding five classes of monomial bent functions have been well studied in public literatures. However, the characterization of the vectorial monomial bent functions with the five known classes of bent exponents is still not clear. In this section, we study the existence and constructions of vectorial monomial bent functions.

3.1 General constructions of vectorial monomial bent functions

This subsection discusses the general constructions of vectorial monomial bent functions and answers one open problem proposed by E. Pasalic et al. [55].

In order to obtain the general constructions of vectorial monomial bent functions, we give the following theorem, which can be obtained by Theorem 2 directly.

Theorem 4. *Let $Tr_1^n(ax^d)$ be a monomial bent function. Then $Tr_m^n(ax^d)$ is a vectorial monomial bent function if $Tr_1^n(a\lambda x^d)$ is linear equivalent to $Tr_1^n(ax^d)$ for all $\lambda \in \mathbb{F}_{2^m}^*$.*

To make use of Theorem 4, it is foremost to ensure the linear equivalence between $Tr_1^n(a\lambda x^d)$ and $Tr_1^n(ax^d)$ for all $\lambda \in \mathbb{F}_{2^m}^*$. We give three equivalent conditions which will be used to meet the condition that $Tr_1^n(a\lambda x^d)$ is linear equivalent to $Tr_1^n(ax^d)$ for all $\lambda \in \mathbb{F}_{2^m}^*$.

Before that, a useful lemma is presented as follows, which can be proved easily.

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

Theorem 5. *Let $m \mid n$ and d be integer. Then the following three conditions are equivalent:*

(1) $\mathbb{F}_{2^m}^* \subseteq \{x^d : x \in \mathbb{F}_{2^n}^*\}$.

(2) $\gcd(d, 2^n - 1) \mid t$.

(3) $\gcd(\frac{d}{\gcd(d,t)}, 2^m - 1) = 1$.

Proof. By Lemma 1, it is known that $\{x^d : x \in \mathbb{F}_{2^n}^*\} = \langle \alpha^{\gcd(d,2^n-1)} \rangle$. Since $\mathbb{F}_{2^m}^* = \langle \alpha^t \rangle$, the equivalence between item (1) and item (2) can be obtained. In the following, we prove the equivalence between item (1) and item (3).

Let $\mathrm{lcm}[t, d]$ denote the lowest common multiple of t and d. By Lemma 1, $\{x^d : x \in \mathbb{F}_{2^n}^*\} = \langle \alpha^d \rangle$. Then we have

$$\begin{aligned} & \mathbb{F}_{2^m}^* \subseteq \{x^d : x \in \mathbb{F}_{2^n}^*\} \\ \Leftrightarrow\ & \langle \alpha^t \rangle \subseteq \langle \alpha^d \rangle \\ \Leftrightarrow\ & \langle \alpha^t \rangle \cap \langle \alpha^d \rangle = \langle \alpha^t \rangle \\ \Leftrightarrow\ & \langle \alpha^{\mathrm{lcm}[t,d]} \rangle = \langle \alpha^t \rangle \\ \Leftrightarrow\ & \gcd(\mathrm{lcm}[t, d], 2^n - 1) = t \\ \Leftrightarrow\ & \gcd(\frac{td}{\gcd(d, t)}, 2^n - 1) = t \\ \Leftrightarrow\ & \gcd(\frac{d}{\gcd(d, t)}, 2^m - 1) = 1. \end{aligned}$$

Given the above, the conclusion of the theorem holds. □

Note that $\mathbb{F}_{2^m}^* \subseteq \{x^d : x \in \mathbb{F}_{2^n}^*\}$ if and only if there exists some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^d$ for all $\lambda \in \mathbb{F}_{2^m}^*$. If one of the three conditions in Theorem 5 holds, by Definition 5, then $Tr_1^n(a\lambda x^d) = Tr_1^n(a(\beta x)^d)$ is linear equivalent to $Tr_1^n(ax^d)$ for all $\lambda \in \mathbb{F}_{2^m}^*$. Thus, according to Theorem 4 and Theorem 5, the general constructions of the vectorial monomial bent functions corresponding to the three conditions in Theorem 5 can be obtained as the following theorem.

Theorem 6. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. If one of the three conditions in Theorem 5 holds, then $Tr_m^n(ax^d)$ is a vectorial monomial bent function.*

In [55], given a monomial bent function $Tr_1^n(ax^d)$, E. Pasalic et al. proved that x^d is a permutation on $\mathbb{F}_{2^m}$, i.e., $\gcd(d, 2^m - 1) = 1$, is sufficient for $Tr_m^n(ax^d)$ to be bent, and left an open problem as follows.

Open Problem 1 ([55]). *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. Let x^d be a permutation of $\mathbb{F}_{2^m}$. Then $Tr_m^n(ax^d)$ is a vectorial monomial bent function.*

The condition that the mapping x^d is a permutation over $\mathbb{F}_{2^m}$ seems to be a necessary condition as well, but this still remains open.

It is certainly of interest to relax the condition regarding the permutation property of x^d over $\mathbb{F}_2^m$. Anyway, a generalization of the above result for nonpermutating over $\mathbb{F}_{2^m}$ seems not to be straightforward.

In [58], by giving a counter example, it was shown that the condition $\gcd(d, 2^m-1) = 1$ is not necessary. However, the relaxation of the condition regarding the permutation property of x^d on $\mathbb{F}_2^m$ is still unknown. Here, we answer Open Problem 1 adequately. Before that, we investigate the relation between $\gcd(d, 2^m - 1) = 1$ and the three conditions in Theorem 5.

According to item (3) of Theorem 5, the following theorem can be obtained directly.

Theorem 7. *Let $m \mid n$ and d be integer. If $\gcd(d, 2^m - 1) = 1$, then every one of the three conditions in Theorem 5 holds. But it is not vice versa.*

By Theorem 6 and Theorem 7, we have that, given a monomial bent function $Tr_1^n(ax^d)$, every one of the three conditions in Theorem 5 is closer to the sufficient and necessary conditions for $Tr_m^n(ax^d)$ to be bent than $\gcd(d, 2^m - 1) = 1$.

While how much difference between $\gcd(d, 2^m - 1) = 1$ and the three conditions in Theorem 5? In fact, given a monomial bent function $Tr_1^n(ax^d)$, there exist many conditions that are much closer to the sufficient and necessary conditions for $Tr_m^n(ax^d)$ to be bent than $\gcd(d, 2^m - 1) = 1$, and further than every one of the three conditions in Theorem 5.

Theorem 8. *Let $m \mid n$, d be integer, $l_1, l_2 \in \mathbb{N}^*$, $l_1 \geq 2$, $l_1 > l_2$, Condition-A denote every one of the three conditions in Theorem 5 and Condition-B denote every one of the three conditions in Theorem 5 with $d = d^{l_1}$. Then*

$$Condition - A \overset{\nRightarrow}{\Leftarrow} Condition - B \overset{\nRightarrow}{\Leftarrow} \gcd(\frac{d^{l_1}}{\gcd(d^{l_2}, t)}, 2^m - 1) = 1 \overset{\nRightarrow}{\Leftarrow} \gcd(d, 2^m - 1) = 1$$

Proof. Condition-A $\overset{\nRightarrow}{\Leftarrow}$ Condition-B is obvious.

Since $l_1 > l_2$, $\gcd(\frac{d^{l_1}}{\gcd(d^{l_1},t)}, 2^m - 1) = 1 \overset{\nRightarrow}{\Leftarrow} \gcd(\frac{d^{l_1}}{\gcd(d^{l_2},t)}, 2^m - 1) = 1$ is also obvious. By Theorem 5, Condition-B $\overset{\nRightarrow}{\Leftarrow} \gcd(\frac{d^{l_1}}{\gcd(d^{l_2},t)}, 2^m - 1) = 1$ holds.

Since $\gcd(\frac{d^{l_1}}{\gcd(d^{l_2},t)}, 2^m - 1) = 1 \overset{\nRightarrow}{\Leftarrow} \gcd(d^{l_1}, 2^m - 1) = 1$, and $\gcd(d^{l_1}, 2^m - 1) = 1 \Leftrightarrow \gcd(d, 2^m - 1) = 1$, we have that $\gcd(\frac{d^{l_1}}{\gcd(d^{l_2},t)}, 2^m - 1) = 1 \overset{\nRightarrow}{\Leftarrow} \gcd(d, 2^m - 1) = 1$.

Given the above, the conclusion of the theorem holds. □

According to Theorem 6 and Theorem 8, the following theorem can be obtained.

Theorem 9. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. Then $Tr_m^n(ax^d)$ is a vectorial monomial bent function if one of the following four conditions holds, where $l, l' \in \mathbb{N}^*$, $l \geq l'$:*

(1) $\mathbb{F}_{2^m}^* \subseteq \{x^{d^l} : x \in \mathbb{F}_{2^n}^*\}$.

(2) $\gcd(d^l, 2^n - 1) \mid t$.

(3) $\gcd(\frac{d^l}{\gcd(d^{l'},t)}, 2^m - 1) = 1$.

(4) $\gcd(d, 2^m - 1) = 1$.

Remark 2. **(1)** *Note that, in this paper, without statement, there is no restriction that $Tr_1^n(ax^d)$ is bent when referring to the four conditions in Theorem 9.*

(2) *The construction corresponding to item (4) of Theorem 9 is Theorem 1 in [55]. For the convenience of discussion, we let Theorem 9 include the condition $\gcd(d, 2^m - 1)$.*

In [51], it was shown that bent (n, m)-functions exist if and only if n is even and $n \geq 2m$. Thus, by Theorem 9, we have the following corollary.

Corollary 1. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. Then one of the four conditions in Theorem 9 holds only if $m \leq k$.*

Anwsers to Open Problem 1. *Following from Theorem 8 and Theorem 9, given a monomial bent function $Tr_1^n(ax^d)$, we have that every one of the three conditions corresponding to item (1)-item (3) of Theorem 9 is closer to the sufficient and necessary conditions for $Tr_m^n(ax^d)$ to be a vectorial monomial bent function than* $\gcd(d, 2^m - 1) = 1$.

Although the non-necessity of $\gcd(d, 2^m - 1) = 1$ and every one of the three conditions corresponding to item (1)-item (3) of Theorem 9 with $l \geq 2$ for $Tr_m^n(ax^d)$ to be bent can be obtained by Theorem 8 and Theorem 9 directly, given a monomial bent function $Tr_1^n(ax^d)$, whether every one of the three conditions in Theorem 5 is necessary or not for $Tr_m^n(ax^d)$ to be bent is also interesting. According to Theorem 8, item (1) of Remark 4, item (1) of Remark 5, item (1) of Remark 7 and item (1) of Remark 8 (see below), we have the following conclusion.

Theorem 10. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. For $Tr_m^n(ax^d)$ to be a vectorial monomial bent function, every one of the four conditions in Theorem 9 is*

(1) *sufficient but not necessary in general case;*

(2) *sufficient and necessary if d is a Kasami exponent or a Leander exponent.*

In addition, if d is a Gold exponent, then every one of the four conditions in Theorem 9 with $m = k$ is also sufficient and necessary for $Tr_k^n(ax^d)$ to be bent.

On the other hand, in some cases, the four conditions in Theorem 9 may be equivalent.

Theorem 11. *Let $m \mid n$ and d be integer. If* $\gcd(2^m - 1, t) = 1$*, then the four conditions in Theorem 9 are equivalent.*

Proof. According to Theorem 5 and Theorem 8, it only needs to prove that $\gcd(\frac{d}{\gcd(d,t)}, 2^m - 1) = 1$ is necessary for $\gcd(d, 2^m - 1) = 1$ to hold. Since $\gcd(2^m - 1, t) = 1$, we have that $\gcd(d, 2^m - 1) = 1$ if and only if $\gcd(\frac{d}{\gcd(d,t)}, 2^m - 1) = 1$ holds. □

Remark 3. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. Then* $\gcd(2^m - 1, t) = 1$ *is not necessary for the four conditions in Theorem 9 to be equivalent. The reason is as follows.*

Let $m = 3$ and $n = 84$. By Theorem 15, Theorem 16, Theorem 22 and Theorem 23 (see below), we have that the four conditions in Theorem 9 are equivalent if d is a Kasami exponent or a Leander exponent. However, $\gcd(2^m - 1, t) = \gcd(2^m - 1, \frac{n}{m}) = 7$.

Assuming that $\gcd(2^m - 1, t) = 1$, given a monomial bent function $Tr_1^n(ax^d)$, whether every one of the four conditions in Theorem 9 are necessary or not for $Tr_m^n(ax^d)$ to be bent is interesting. However, we cannot determine the necessity, and this is left as an open problem.

Open Problem 2. *Let $m \mid n$ and $Tr_1^n(ax^d)$ be a monomial bent function. If* $\gcd(2^m-1, t) = 1$*, it is not yet known whether every one of the four conditions in Theorem 9 is necessary or not for $Tr_m^n(ax^d)$ to be a vectorial monomial bent function.*

Trivially, by Theorem 1, the (n, m)-function $Tr_m^n(ax^d)$ is bent if and only if $Tr_1^n(a\lambda x^d)$ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$, where $a \in \mathbb{F}_{2^n}^*$. The same idea was also considered in [58]. For the convenience of discussion, we list this fact as the following theorem.

Theorem 12 ([58])**.** *Let $m \mid n$, $a \in \mathbb{F}_{2^n}^*$ and denote*

$$C = \{\beta \in \mathbb{F}_{2^n} : Tr_1^n(\beta x^d) \ is \ a \ monomial \ bent \ function\}.$$

Then $Tr_m^n(ax^d)$ a vectorial monomial bent function if and only if

$$a \cdot \mathbb{F}_{2^m}^* \subseteq C.$$

3.2 The characterizations of vectorial monomial bent functions

In this subsection, we focus on the characterizations of the vectorial monomial bent functions with the known bent exponents.

3.2.1 The known monomial bent functions

It is known that there are five classes of monomial bent functions, accordingly, five classes of bent exponents have been found so far. The known monomial bent functions are introduced below and listed in Table 1, which will be used to characterize the vectorial monomial bent functions corresponding to the five known classes of bent exponents.

The monomial bent functions with the Gold exponent $d = 2^s + 1$ are well known, where $s \in \mathbb{N}$. By Lemma 1, this can be described as the following theorem.

Theorem 13 (Gold Case [34])**.** *Let $s \in \mathbb{N}$, $d = 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. The Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent if and only if*

$$a \notin \langle \alpha^{\gcd(d, 2^n-1)} \rangle.$$

It was shown in [22] that the Boolean function $Tr_1^n(ax^{2^k-1})$ on $\mathbb{F}_{2^n}$ is bent if and only if $K(a) = 0$ with $a \in \mathbb{F}_{2^k}^*$, and in [32] that $Tr_1^n(ax^{2^k-1})$ on $\mathbb{F}_{2^n}$ is bent if and only if $K(N_k^n(a)) = 0$ with $a \in \mathbb{F}_{2^n}^*$. In [18], it was shown that $Tr_1^n(ax^{s(2^k-1)})$ on $\mathbb{F}_{2^n}$ is bent if and only if $K(a) = 0$, where $\gcd(s, 2^k + 1) = 1$ and $a \in \mathbb{F}_{2^k}^*$. For the Dillon exponent $d = s(2^k - 1)$ with s integer, we recall Theorem 5 in [18] and Theorem 3 in [32] as the following theorem. Note that the Kloosterman sums defined in this paper is the same as that in [18] and is different from that in [32].

Theorem 14 (Dillon Case [18, 32])**.** *Let s be an integer and $d = s(2^k - 1)$. For the Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$, the following conclusions hold:*

(1) *Let* $\gcd(s, 2^k + 1) = 1$ *and $a \in \mathbb{F}_{2^k}^*$. Then $Tr_1^n(ax^d)$ is bent if and only if*

$$a \in \{\mu : K(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\}.$$

(2) *Let $s=1$ and $a \in \mathbb{F}_{2^n}^*$. Then $Tr_1^n(ax^d)$ is bent if and only if*

$$a \in \{\beta : K(N_k^n(\beta)) = 0, \beta \in \mathbb{F}_{2^n}^*\}.$$

The conclusion for the monomial bent functions on $\mathbb{F}_{2^n}$ with the Kasami exponent $d = 2^{2s} - 2^s + 1$, where $s \in \mathbb{N}$ and $\gcd(s,n) = 1$, was conjectured in [28] and proved in [23]. Since $3 \mid (2^n - 1)$, by Lemma 1, the conclusion for the monomial bent functions with the Kasami exponent can be described as follows.

Theorem 15 (Kasami Case [23, 34])**.** *Let $\gcd(3,n) = 1$, $s \in \mathbb{N}$, $\gcd(s,n) = 1$, $d = 2^{2s} - 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. The Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent if and only if*

$$a \notin \langle \alpha^3 \rangle.$$

In [34], it was proved that there exist monomial bent functions with the Leander exponent $d = (2^s+1)^2$, and further result was given in [19]. It was shown in [19] that the Boolean function $Tr_1^n(ax^{(2^s+1)^2})$ on $\mathbb{F}_{2^n}$ is bent if and only if s is positive odd integer and there exist some $\rho \in \varepsilon\mathbb{F}_{2^s}^*$ and $\beta \in \mathbb{F}_{2^n}^*$ such that $a = \rho\beta^{(2^s+1)^2}$ holds, where $n = 4s$ and $\varepsilon \in \mathbb{F}_4 \setminus \mathbb{F}_2$. Note the fact, the condition that there exist some $\rho \in \varepsilon\mathbb{F}_{2^s}^*$ and $\beta \in \mathbb{F}_{2^n}^*$ with $\varepsilon \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and $n = 4s$ such that $a = \rho\beta^{(2^s+1)^2}$ is equivalent to $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \mathbb{F}_{2^s}^* \cdot \{x^{(2^s+1)^2} : x \in \mathbb{F}_{2^n}^*\}$. By Lemma 1 and $n = 4s$, $\{x^{(2^s+1)^2} : x \in \mathbb{F}_{2^n}^*\} = \langle \alpha^{2^s+1} \rangle$ holds. Since $\mathbb{F}_{2^s}^* = \langle \alpha^{(2^s+1)(2^{2s}+1)} \rangle$, we have $\mathbb{F}_{2^s}^* \subset \{x^{(2^s+1)^2} : x \in \mathbb{F}_{2^n}^*\}$. Therefore, $\mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \mathbb{F}_{2^s}^* \cdot \{x^{(2^s+1)^2} : x \in \mathbb{F}_{2^n}^*\} = \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$. Thus, Theorem 4.8 in [19] can be described equivalently and more succinctly as the following theorem.

Theorem 16 (Leander Case [19, 34])**.** *Let $s \in \mathbb{N}^*$, $n = 4s$, $d = (2^s+1)^2$ and $a \in \mathbb{F}_{2^n}^*$. Then the Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent if and only if*

$$s \text{ is odd and } a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle.$$

For the the Canteaut-Charpin-Kyureghyan exponent $d = 2^{2s} + 2^s + 1$, in [10, 19], it was shown that the Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent if and only if $a \in \{\rho : Tr_s^k(\rho) = 0, \rho \in \mathbb{F}_{2^k}^*\} \cdot \{x^d : x \in \mathbb{F}_{2^n}^*\}$, where the integer $s > 1$ and $n = 6s$. By Lemma 1, we describe this conclusion as the following theorem.

Theorem 17 (Canteaut-Charpin-Kyureghyan Case [10, 19])**.** *Let $s > 1$ be an integer, $n = 6s$, $d = 2^{2s} + 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. Then the Boolean function $Tr_1^n(ax^d)$ on $\mathbb{F}_{2^n}$ is bent if and only if*

$$a \in \{\rho : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle.$$

3.2.2 Characterizing the vectorial monomial bent functions with the known bent exponents

Based on the general constructions of vectorial monomial bent functions and the results of monomial bent functions, we characterize the vectorial monomial bent functions corresponding to the five known classes of bent exponents. The results of the constructions and the nonexistence of vectorial monomial bent functions are listed in Table 2 and Table 3 respectively. Among the constructions of vectorial Boolean bent functions, the constructions which reach maximal dimension of the output space, i.e., half of the dimension of the input

Table 1: The Known Monomial Bent Functions of the form $Tr_1^n(ax^d)$ [1]

Case	Exponent d	Condition-1	Condition-2 [2]	References
Gold	2^s+1	$s \in \mathbb{N}$	$a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle$	[34]
Dillon	$s(2^k-1)$	$\gcd(s, 2^k+1) = 1$	$K(a) = 0, a \in \mathbb{F}_{2^k}^*$	[18, 34]
		$s = 1$	$K(N_k^n(a)) = 0, a \in \mathbb{F}_{2^n}^*$	[32]
Kasami	$2^{2s} - 2^s + 1$	$s \in \mathbb{N}$, $\gcd(3, n) = 1$, $\gcd(s, n) = 1$	$a \notin \langle \alpha^3 \rangle$	[23, 34]
Leander	$(2^s+1)^2$	$s \in \mathbb{N}^*$, $n = 4s$	s odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$	[19, 34], Theorem 16
Canteaut-Charpin-Kyureghyan	$2^{2s} + 2^s + 1$	$s > 1$ integer, $n = 6s$	$a \in \{\rho : Tr_s^k(\rho) = 0, \rho \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$	[10, 19]

[1] $n = 2k$ and $a \in \mathbb{F}_{2^n}^*$.

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

space, are optimal. Thus, we list the results of the vectorial monomial bent functions of the form $Tr_k^n(ax^d)$ in Table 4.

According to Theorem 9 and Theorem 13-17, the following theorem can be obtained directly, which gives the vectorial monomial bent functions corresponding to the five known classes of bent exponents.

Theorem 18. *Let $m \mid n$, $a \in \mathbb{F}_{2^n}^*$ and one of the four conditions in Theorem 9 holds. For the (n, m)-function $Tr_m^n(ax^d)$, the following conclusions hold:*

(1) (Gold Case). *Let $s \in \mathbb{N}$ and $d = 2^s + 1$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle.$$

(2) (Dillon Case). *Let s be an integer and $d = s(2^k - 1)$.*

(2.1) *Let $\gcd(s, 2^k+1) = 1$ and $a \in \mathbb{F}_{2^k}^*$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$a \in \{\beta : K(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\}.$$

(2.2) *Let $s = 1$ and $a \in \mathbb{F}_{2^n}^*$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$a \in \{\beta : K(N_k^n(\beta)) = 0, \beta \in \mathbb{F}_{2^n}^*\}.$$

(3) (Kasami Case). *Let $\gcd(3, n) = 1$, $s \in \mathbb{N}$, $\gcd(s, n) = 1$ and $d = 2^{2s} - 2^s + 1$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$a \notin \langle \alpha^3 \rangle.$$

(4) (Leander Case). *Let $s \in \mathbb{N}^*$, $n = 4s$ and $d = (2^s + 1)^2$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$s \text{ is odd and } a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle.$$

(5) (Canteaut-Charpin-Kyureghyan Case). *Let $s > 1$ be an integer, $n = 6s$ and $d = 2^{2s} + 2^s + 1$. Then $Tr_m^n(ax^d)$ is bent if and only if*

$$a \in \{\rho : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle.$$

Although five classes of vectorial monomial bent functions are given in Theorem 18, the four conditions in Theorem 9 seem inconvenient to use directly. In order to construct vectorial monomial bent functions more practically, we further characterize the vectorial monomial bent functions corresponding to the five known classes of bent exponents.

We have a new sufficient and necessary condition for the vectorial monomial bent functions with the Gold exponent to be bent, which has less restrictions than that in Theorem 18.

Theorem 19 (Gold Case)**.** *Let $m \mid n$, $s \in \mathbb{N}$, $d = 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. The (n, m)-function $Tr_m^n(ax^d)$ is bent if and only if*

$$a \notin \langle \alpha^{\gcd(d,t)} \rangle.$$

Proof. By Theorem 13, the set of the coefficients such that $Tr_1^n(\beta x^d)$ on $\mathbb{F}_{2^n}$ is bent is

$$C = \{\beta \in \mathbb{F}_{2^n}^* : \beta \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle\}.$$

Then, by Theorem 12, we get that $Tr_m^n(ax^d)$ is bent if and only if

$$\begin{aligned} & a \cdot \mathbb{F}_{2^m}^* \subseteq \{\beta \in \mathbb{F}_{2^n}^* : \beta \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle\} \\ \Leftrightarrow \quad & a \cdot \mathbb{F}_{2^m}^* \cap \langle \alpha^{\gcd(d,2^n-1)} \rangle = \varnothing \\ \Leftrightarrow \quad & a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle \cdot \mathbb{F}_{2^m}^* \\ \Leftrightarrow \quad & a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle \cdot \langle \alpha^t \rangle \\ \Leftrightarrow \quad & a \notin \langle \alpha^{\gcd(t,\gcd(d,2^n-1))} \rangle \\ \Leftrightarrow \quad & a \notin \langle \alpha^{\gcd(d,t)} \rangle \end{aligned}$$

Given the above, the theorem is proved to be true. □

Remark 4. **(1)** *Here, we give an example that $Tr_m^n(ax^d)$ is a vectorial monomial bent function with a Gold exponent and the three conditions in Theorem 5 do not hold, which means that the three conditions in Theorem 5 are not necessary for $Tr_m^n(ax^d)$ to be bent. In Gold case, let $s = 3$, $m = 4$ and $n = 12$. Then $\gcd(d, t) = \gcd(2^s + 1, \frac{2^n-1}{2^m-1}) = \gcd(9, 273) = 3 \neq 1$. Thus, $\mathbb{F}_{2^n}^* \setminus \langle \alpha^{\gcd(d,t)} \rangle = \mathbb{F}_{2^{12}}^* \setminus \langle \alpha^3 \rangle \neq \varnothing$. For $\forall\ a \in \mathbb{F}_{2^{12}}^* \setminus \langle \alpha^3 \rangle$, by Theorem 19, we have $Tr_4^{12}(ax^9)$ is bent. However, $\gcd(\frac{d}{\gcd(d,t)}, 2^m - 1) = \gcd(3, 15) = 3 \neq 1$.*

(2) *Obviously, all the vectorial monomial bent functions constructed by item (1) of Theorem 18 can be constructed by Theorem 19. However, by item (1), we know that it is not vice-versa.*

Then we discuss the necessary and sufficient conditions for the (n, k)-function of the form $Tr_k^n(ax^d)$ with the Gold exponent to be bent. Before the discussion, the following lemma is given, which can be derived from Lemma 1 in [34].

Lemma 2. *Let $Tr_1^n(ax^d)$ be a monomial bent function. Then $\gcd(d, 2^k - 1) = 1$ if and only if $\gcd(d, 2^k + 1) \neq 1$.*

Corollary 2. *Let $m \mid n$, $s \in \mathbb{N}$, $d = 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. For the (n, k)-function $Tr_k^n(ax^d)$, the following three conditions are equivalent:*

(1) *$Tr_k^n(ax^d)$ is bent.*

(2) *$a \notin \langle \alpha^{\gcd(d,2^k+1)} \rangle$.*

(3) *$a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle$ and one of the four conditions in Theorem 9 with $m = k$ holds.*

Proof. By Theorem 19, the equivalence between item (1) and item (2) is trivial.

(2)⇒(3): Since $a \in \mathbb{F}_{2^n}^* \setminus \langle \alpha^{\gcd(d,2^k+1)} \rangle$ and $a \in \mathbb{F}_{2^n}^*$, we have that $a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle$ and $\gcd(d, 2^k + 1) \neq 1$. By Lemma 2, $\gcd(d, 2^k - 1) = 1$. According to Theorem 8, all the four conditions in Theorem 9 with $m = k$ hold.

(3)⇒(1): This follows from item (1) of Theorem 18.

Given the above, the corollary is proved to be true. □

Remark 5. **(1)** *If $Tr_1^n(ax^d)$ is a monomial bent function with a Gold exponent, by Theorem 13 and item (3) of Corollary 2, then every one of the four conditions in Theorem 9 with $m = k$ is also necessary for $Tr_k^n(ax^d)$ to be bent.*

(2) *Theorem 6 in [26] is a special case corresponding to item (3) of Corollary 2. Moreover, Corollary 2 indicates that the conditions $\gcd(2^s + 1, 2^n - 1) \mid (2^k + 1)$ and $a \notin \{x^{\gcd(d,2^n-1)} : x \in \mathbb{F}_{2^n}\}$ of Theorem 6 in [26] are also necessary for $Tr_k^n(ax^d)$ to be bent, which is unknown in [26].*

In order to discuss the vectorial monomial bent functions with the Dillon exponent, a lemma is given as follows.

Lemma 3. *Let $m \geq 2$, $m \mid n$, s be an integer, $\gcd(s, 2^k + 1) = 1$, $d = s(2^k - 1)$ and $Tr_1^n(ax^d)$ be a monomial bent function. Then one of the three conditions in Theorem 5 holds if and only if $m = 2$, $n \geq 6$ and $n \equiv 2 (\mathrm{mod}\ 4)$.*

Proof. Since $\gcd(s, 2^k + 1) = 1$, we have

$$\begin{aligned} & \gcd(d, 2^n - 1) \mid t \\ \Leftrightarrow \quad & (2^m - 1) \mid (2^k + 1) \\ \Leftrightarrow \quad & 2^m - 1 = \gcd(2^m - 1, 2^k + 1). \end{aligned}$$

Necessity: If $m \mid k$, then $\gcd(2^m - 1, 2^k + 1) = \gcd(2^m - 1, 2^m + 1) = 1$. Because $m \geq 2$, there is no m such that $2^m - 1 = \gcd(2^m - 1, 2^k + 1) = 1$. Then we have $m \nmid k$. According to Corollary 1 and $m \nmid k$, it is obtained that $m < k$.

By $m \geq 2$ and $m < k$, we have $n \geq 6$.

Since $m < k$, $\gcd(2^m - 1, 2^k + 1) = \gcd(2^m - 1, 2^{k \bmod m} + 1)$. And because $m \geq 2$, $m \nmid k$ and $2^m - 1 = \gcd(2^m - 1, 2^k + 1)$, we have that $m = 2$ and $k \equiv 1 (\mathrm{mod}\ 2)$, i.e., $n \equiv 2 (\mathrm{mod}\ 4)$.

Thus, $m = 2$, $n \geq 6$ and $n \equiv 2 (\mathrm{mod}\ 4)$.

Sufficiency: If $m = 2$, $n \geq 6$ and $n \equiv 2 (\mathrm{mod}\ 4)$, then $m \nmid k$ and $m < k$. Therefore, $\gcd(2^m - 1, 2^k + 1) = \gcd(2^m - 1, 2^{k \bmod m} + 1) = 2^m - 1$.

By Theorem 5, the lemma is proved to be true. □

By item (2) of Theorem 18 and Lemma 3, we can derive the following theorem.

Theorem 20 (Dillon Case). *Let $n \equiv 2 (\mathrm{mod}\ 4)$ and $n \geq 6$, s be an integer and $d = s(2^k - 1)$. For the $(n, 2)$-function $Tr_2^n(ax^d)$, the following conclusions hold:*

(1) *Let* $\gcd(s, 2^k+1) = 1$ *and* $a \in \mathbb{F}_{2^k}^*$. *Then* $Tr_2^n(ax^d)$ *is bent if and only if*

$$a \in \{\beta : K(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\}.$$

(2) *Let* $s = 1$ *and* $a \in \mathbb{F}_{2^n}^*$. *Then* $Tr_2^n(ax^d)$ *is bent if and only if*

$$a \in \{\beta : K(N_k^n(\beta)) = 0, \beta \in \mathbb{F}_{2^n}^*\}.$$

Remark 6. *According to Theorem 8 and Lemma 3, we have that all the vectorial monomial bent functions constructed by item (2) of Theorem 18 and by Theorem 20 are the same.*

It was shown by Theorem 10 in [48] that there does not exist a vectorial monomial bent functions of the form $Tr_k^n(ax^d)$ with the Dillon exponent $d = s(2^k-1)$, where $\gcd(s, 2^k+1) = 1$ and $a \in \mathbb{F}_{2^k}^*$. Here, we give an alternative proof of Theorem 10 in [48], and also prove the nonexistence of the vectorial monomial bent functions of the form $Tr_k^n(ax^d)$ with the Dillon exponent for $s = 1$ and $a \in \mathbb{F}_{2^n}^*$. Before the proof, a lemma is given as follows.

Lemma 4. *For* $\forall\ a \in \mathbb{F}_{2^n}^*$, $\{N_k^n(a\lambda) : \lambda \in \mathbb{F}_{2^k}^*\} = \mathbb{F}_{2^k}^*$.

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

Theorem 21. *Let s be an integer and $d = s(2^k-1)$. The following conclusions hold:*

(1) ([48]) *Let* $\gcd(s, 2^k+1) = 1$ *and* $a \in \mathbb{F}_{2^k}^*$. *Then there does not exist a vectorial monomial bent function of the form* $Tr_k^n(ax^d)$.

(2) *Let* $s = 1$ *and* $a \in \mathbb{F}_{2^n}^*$. *Then there does not exist a vectorial monomial bent function of the form* $Tr_k^n(ax^d)$.

Proof. Assume the contrary that such a vectorial monomial bent function $Tr_k^n(ax^d)$ exists.

(1) According to Theorem 1 and item (1) of Theorem 14, we have that $Tr_k^n(ax^d)$ is bent if and only if $K(a\lambda) = 0$ holds for all $\lambda \in \mathbb{F}_{2^k}^*$. Then,

$$\begin{aligned}
& \sum_{z\in\mathbb{F}_{2^k}} (-1)^{Tr_1^k(z^{2^k-2}+a\lambda z)} = 0 \text{ for all } \lambda \in \mathbb{F}_{2^k}^* \\
\Leftrightarrow\ & \sum_{z,y\in\mathbb{F}_{2^k}^*} (-1)^{Tr_1^k(z^{2^k-2}+y)} = -1 \\
\Leftrightarrow\ & \sum_{z\in\mathbb{F}_{2^k}^*} (-1)^{Tr_1^k(z^{2^k-2})} \sum_{y\in\mathbb{F}_{2^k}^*} (-1)^{Tr_1^k(y)} = -1 \\
\Leftrightarrow\ & (\sum_{z\in\mathbb{F}_{2^k}^*} (-1)^{Tr_1^k(z)})^2 = -1
\end{aligned}$$

This is obviously impossible.

(2) By Theorem 1 and item (2) of Theorem 14, we get that $Tr_k^n(ax^d)$ is bent if and only if $K(N_k^n(a\lambda))=0$ holds for all $\lambda\in\mathbb{F}_{2^k}^*$. By Lemma 4, we have

$$\begin{aligned}
&\sum_{z\in\mathbb{F}_{2^k}}(-1)^{Tr_1^k(z^{2^k-2}+z\cdot N_k^n(a\lambda))}=0 \text{ for all } \lambda\in\mathbb{F}_{2^k}^*\\
\Leftrightarrow\ &\sum_{z,y\in\mathbb{F}_{2^k}^*}(-1)^{Tr_1^k(z^{2^k-2}+y)}=-1\\
\Leftrightarrow\ &\sum_{z\in\mathbb{F}_{2^k}^*}(-1)^{Tr_1^k(z^{2^k-2})}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{Tr_1^k(y)}=-1\\
\Leftrightarrow\ &(\sum_{z\in\mathbb{F}_{2^k}^*}(-1)^{Tr_1^k(z)})^2=-1
\end{aligned}$$

This is also impossible.

The above impossible inductions mean that, the assumption of the existence of the vectorial monomial bent function $Tr_k^n(ax^d)$ is wrong. Hence the conclusions of the theorem hold. □

For the vectorial monomial bent functions with the Kasami exponent, we can derive the following theorem.

Theorem 22 (Kasami Case)**.** *Let $m\mid n$, $\gcd(3,n)=1$, $s\in\mathbb{N}$, $\gcd(s,n)=1$, $d=2^{2s}-2^s+1$ and $a\in\mathbb{F}_{2^n}^*$. For the (n,m)-function $Tr_m^n(ax^d)$, the following four conditions are equivalent:*

(1) *$Tr_m^n(ax^d)$ is bent.*

(2) *$a\notin\langle\alpha^{\gcd(3,t)}\rangle$.*

(3) *$a\notin\langle\alpha^3\rangle$ and m is odd.*

(4) *$a\notin\langle\alpha^3\rangle$ and one of the four conditions in Theorem 9 holds.*

Proof. By Theorem 12 and Theorem 15, the proof of the equivalence between item (1) and item (2) is similar to the proof of Theorem 19.

(2)⇒(3): It is easy to prove that,

$$\gcd(3,t)=\begin{cases}\gcd(3,2^m+1)=3, & m \text{ odd}, \ \frac{n}{m}\text{ even}\\ \qquad\qquad\qquad\quad 1, & m\text{ odd}, \ \frac{n}{m}\text{ odd}\\ \gcd(3,2^{m+1}+1)=3, & m\text{ even}, \ 0\equiv\frac{n}{m}(\text{mod } 3)\\ \qquad\qquad\qquad\quad 1, & m\text{ even}, \ 1\equiv\frac{n}{m}(\text{mod } 3)\\ \gcd(3,2^m+1)=1, & m\text{ even}, \ 2\equiv\frac{n}{m}(\text{mod } 3).\end{cases}$$

Because n is even, the case both m and $\frac{n}{m}$ are odd does not exist. Since $\gcd(3,n)=1$, the case $0\equiv\frac{n}{m}(\text{mod } 3)$ does not exist either.

Then we have

$$\gcd(3,t)=\begin{cases}3, & m\text{ odd}\\ 1, & m\text{ even}.\end{cases}$$

Because $a \in \mathbb{F}_{2^n}^*$ and $a \notin \langle \alpha^{\gcd(3,t)} \rangle$, we have $\langle \alpha^{\gcd(3,t)} \rangle \neq \mathbb{F}_{2^n}^*$. Then, $\gcd(3,t) \neq 1$, i.e., $\gcd(3,t) = 3$.

Therefore, m is odd.

(3)⇒(4): If m is odd, then $\gcd(3, 2^m - 1) = 1$. Since $\gcd(d, 2^n - 1) = 3$ (see the proof of Theorem 11 in [23]), we have $\gcd(d, 2^m - 1) = 1$.

By Theorem 8, we have that every one of the four conditions in Theorem 9 holds.

(4)⇒(1): This follows from item (3) of Theorem 18.

Consequently, the conclusion of the theorem have been proved to be true. □

Remark 7. **(1)** *If $Tr_1^n(ax^d)$ is a monomial bent function with a Kasami exponent, by Theorem 15 and item (4) of Theorem 22, then every one of the four conditions in Theorem 9 is also necessary for $Tr_m^n(ax^d)$ to be bent.*

(2) *According to item (4) of Theorem 22, we also know that the vectorial monomial bent functions constructed by item (3) of Theorem 18 and by Theorem 22 are the same.*

(3) *Since $\gcd(d, 2^n - 1) = 3$ in Kasami case, by Lemma 1, it is known that $\{x^{\gcd(d,2^n-1)} : x \in \mathbb{F}_{2^n}\} = \{x^3 : x \in \mathbb{F}_{2^n}\} = \langle \alpha^3 \rangle$, where d is a Kasami exponent. Then we have*

(3.1) *Theorem 2 in [55] is a special case corresponding to item (3) of Theorem 22 with s odd and $m = k$ odd. The conditions that k is odd and $a \notin \{x^3 : x \in \mathbb{F}_{2^n}\}$ of Theorem 2 in [55] are also necessary for $Tr_k^n(ax^d)$ to be bent, which is unknown in [55].*

(3.2) *Theorem 7 in [26] is a special case corresponding to item (4) of Theorem 22 with $m = k$. The conditions that $\gcd(d, 2^n - 1) \mid (2^k + 1)$ and $a \notin \{x^{\gcd(d,2^n-1)} : x \in \mathbb{F}_{2^n}\}$ of Theorem 7 in [26] are also necessary for $Tr_k^n(ax^d)$ to be bent, which is unknown in [26].*

(3.3) *Theorem 2 in [58] is a special case corresponding to item (3) of Theorem 22 for the case $n = 2^{s_1+1}k_1$ and $m = k_1$, where $s_1 \geq 0$ and k_1 is odd. The conditions that k_1 is odd and $a \notin \{x^3 : x \in \mathbb{F}_{2^n}\}$ of Theorem 2 in [58] are also necessary for $Tr_{k_1}^n(ax^d)$ to be bent, which is unknown in [58].*

According to item (3) of Theorem 22, the following corollary can be obtained.

Corollary 3. *Let $m \mid n$, $\gcd(3,n) = 1$, $s \in \mathbb{N}$, $\gcd(s,n) = 1$, $d = 2^{2s} - 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. If m is even, then there does not exist a vectorial monomial bent function of the form $Tr_m^n(ax^d)$.*

In order to discuss the vectorial monomial bent functions with the Leander exponent, a lemma is given as follows.

Lemma 5. *If s is a positive odd and $n = 4s$, then $\langle \alpha^{2^s+1} \rangle \cap \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle = \varnothing$.*

Proof. If s is a positive odd, then $\gcd(3, (2^s - 1)(2^{2s} + 1)) = 1$. Since the order of every element in $\mathbb{F}_4 \setminus \mathbb{F}_2$ is 3 and the order of every element in $\langle \alpha^{2^s+1} \rangle$ is $(2^s - 1)(2^{2s} + 1)$, we have that $\langle \alpha^{2^s+1} \rangle \cap \mathbb{F}_4 \setminus \mathbb{F}_2 = \varnothing$. Therefore, $\langle \alpha^{2^s+1} \rangle \cap \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle = \varnothing$. □

For the vectorial monomial bent functions with the Leander exponent, we have the following theorem.

Theorem 23 (Leander Case)**.** *Let $s \in \mathbb{N}^*$, $n = 4s$, $m \mid n$, $d = (2^s + 1)^2$ and $a \in \mathbb{F}_{2^n}^*$. For the (n, m)-function $Tr_m^n(ax^d)$, the following four conditions are equivalent:*

(1) *$Tr_m^n(ax^d)$ is bent.*

(2) *s is odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$ and m is odd.*

(3) *s is odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$ and $m \mid s$.*

(4) *s is odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$ and one of the four conditions in Theorem 9 holds.*

Proof. (1)⇒(2): According to Theorem 12 and Theorem 16, $Tr_m^n(ax^d)$ is bent if and only if

$$s \text{ is odd and } a \cdot \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle.$$

Thus, there exist some $\varepsilon \in \mathbb{F}_4 \setminus \mathbb{F}_2$ and $\tau \in \langle \alpha^{2^s+1} \rangle$ such that $a = \varepsilon \cdot \tau$.

If m is even, then $\mathbb{F}_4 \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^m}^*$. Therefore, $\varepsilon^2 \in \mathbb{F}_4 \setminus \mathbb{F}_2 \subseteq \mathbb{F}_{2^m}^*$. Let $\lambda = \varepsilon^2$. Then $a\lambda = \varepsilon^3 \tau = \tau \in \langle \alpha^{2^s+1} \rangle$. By Lemma 5, we have that $a\lambda \notin \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$. This contradicts $a \cdot \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$. Thus, m cannot be even, i.e., m is odd.

(2)⇔(3): Because s is odd and $m \mid 4s$, we have that m is odd if and only if $m \mid s$.

(3)⇒(4): Since $m \mid s$, we have $\gcd(d, 2^m - 1) = 1$. By Theorem 8, every one of the four conditions in Theorem 9 holds.

(4)⇒(1): This follows from item (4) of Theorem 18.

Given the above, the theorem is proved to be true. □

Remark 8. (1) *If $Tr_1^n(ax^d)$ is a monomial bent function with a Leander exponent, by Theorem 16 and item (4) of Theorem 23, then every one of the four conditions in Theorem 9 is also necessary for $Tr_m^n(ax^d)$ to be bent.*

(2) *According to item (4) of Theorem 23, we also know that the vectorial monomial bent functions constructed by item (4) of Theorem 18 and by Theorem 23 are the same.*

(3) *In [55], it was claimed that, if $s > 1$ is odd, $n = 4s$ and $d = (2^s + 1)^2$, then the (n, s)-function $Tr_s^n(ax^d)$ is bent for any $a \in \mathbb{F}_{2^s}^* \setminus \mathbb{F}_{2^2}$. That is Theorem 3 in [55]. However, it is wrong. The reason is as follows.*

According to Lemma 5, we know that $\mathbb{F}_{2^s}^* \cap \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle = \varnothing$. By item (2) of Theorem 23, we have that such (n, s)-function $Tr_s^n(ax^d)$ is not bent for any $a \in \mathbb{F}_{2^s}^*$.

According to item (2) and item (3) of Theorem 23, we have the following corollary.

Corollary 4. *Let $s \in \mathbb{N}^*$, $n = 4s$, $m \mid n$, $d = (2^s + 1)^2$ and $a \in \mathbb{F}_{2^n}^*$. If m is even or $m \nmid s$, then there does not exist a vectorial monomial bent function of the form $Tr_m^n(ax^d)$.*

For the vectorial monomial bent functions with the Canteaut-Charpin-Kyureghyan exponent, we have the following theorem.

Theorem 24 (Canteaut-Charpin-Kyureghyan Case)**.** *Let $s > 1$ be an integer, $n = 6s$, $d = 2^{2s} + 2^s + 1$ and $a \in \mathbb{F}_{2^n}^*$. If $m \mid 2s$, then the (n, m)-function $Tr_m^n(ax^d)$ is bent if and only if*

$$a \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle.$$

Proof. Note that $m \mid 2s$ if and only if $(2^m-1) \mid (2^{2s}-1)$. Since $2^n-1 = d(2^{2s}-1)(2^{2s}-2^s+1)$, we have $d \mid t$. Thus, $\gcd(d, 2^n-1) \mid t$. By item (5) of Theorem 18, the conclusion holds. □

Remark 9. **(1)** *According to the proof of Theorem 24, we have that the vectorial monomial bent functions constructed by item (5) of Theorem 18 include all of those constructed by Theorem 24.*

(2) *In [55], it was claimed that, if $s > 1$ is an odd integer, $n = 6s$ and $d = 2^{2s}+2^s+1$, then the $(n, 2s)$-function $Tr_{2s}^n(ax^d)$ and the (n, s)-function $Tr_s^n(ax^d)$ are bent for $a \in \mathbb{F}_{2^{2s}}^*$, respectively $a \in \mathbb{F}_{2^s}^*$, satisfying $Tr_s^{3s}(a^3) = 0$. That is Theorem 4 in [55]. However, there is no such vectorial monomial bent function. The reasons are as follows.*

Since s is odd, $\gcd(d, 2^{2s}-1) = 1$. If $Tr_{2s}^n(ax^d)$ with $a \in \mathbb{F}_{2^{2s}}^*$ is bent, then there exists some $\beta \in \mathbb{F}_{2^{2s}}^*$ such that $Tr_{2s}^n((\beta x)^d)$ is bent. Since $Tr_{2s}^n((\beta x)^d)$ and $Tr_{2s}^n(x^d)$ are linear equivalent, $Tr_{2s}^n(x^d)$ is bent. Then $Tr_1^n(x^d)$ is bent. However $Tr_s^{3s}(1) = 1 \neq 0$. This contradicts Theorem 3 in [10]. Thus, we have that such $(n, 2s)$-function $Tr_{2s}^n(ax^d)$ is not bent for any $a \in \mathbb{F}_{2^{2s}}^*$.

The reason for the nonexistence of such vectorial monomial bent functions of the form $Tr_s^n(ax^d)$ for any $a \in \mathbb{F}_{2^s}^*$ is similar to the above.

(3) *Theorem 3 in [58] is a special case of Theorem 24 with $m = 2s$ and $a \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\}$.*

However, whether all the vectorial monomial bent functions constructed by item (5) of Theorem 18 can be constructed by Theorem 24 or not is unknown. We leave this as an open problem.

Open Problem 3. *It is not yet known whether item (5) of Theorem 18 and Theorem 24 construct the same vectorial monomial bent functions.*

We conclude that no vectorial monomial bent function with the Canteaut-Charpin-Kyureghyan exponent has the optimal dimension of the output space, i.e., half of the dimension of the input space.

Theorem 25. *Let $s > 1$ be an integer, $n = 6s$, $d = 2^{2s}+2^s+1$ and $a \in \mathbb{F}_{2^n}^*$. There is no vectorial monomial bent function of the form $Tr_k^n(ax^d)$.*

Proof. Trivially, according to Theorem 17, the (n, k)-function $Tr_k^n(ax^d)$ is not bent for $a \notin \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$. In the following, we discuss the case $a \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$.

For $\forall\ a \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$, there are some $\mu_1 \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\}$ and some $\beta_1 \in \mathbb{F}_{2^n}^*$ such that $a = \mu_1 \beta_1^d$. According to Theorem 1 and Theorem 17, $Tr_k^n(ax^d)$ is bent if and only if $\mu_1 \lambda \beta_1^d \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$ for all $\lambda \in \mathbb{F}_{2^k}^*$.

Let $\mu_2 = \mu_1 \lambda$. Because of $\mu_1 \in \mathbb{F}_{2^k}^*$ and the ergodicity of λ over $\mathbb{F}_{2^k}^*$, we have that $\mu_1 \lambda \beta_1^d \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$ for all $\lambda \in \mathbb{F}_{2^k}^*$, is equivalent to, $\mu_2 \beta_1^d \in \{\mu : Tr_s^k(\mu) = 0, \mu \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$ for all $\mu_2 \in \mathbb{F}_{2^k}^*$. Thus, $Tr_k^n(ax^d)$ is bent if and only if $Tr_1^n(\mu_2 \beta_1^d x^d)$ is bent for all $\mu_2 \in \mathbb{F}_{2^k}^*$.

Since $Tr_1^n(\mu_2 x^d)$ is linear equivalent to $Tr_1^n(\mu_2 \beta_1^d x^d)$, we have that $Tr_k^n(ax^d)$ is bent if and only if $Tr_1^n(\mu_2 x^d)$ is bent for all $\mu_2 \in \mathbb{F}_{2^k}^*$.

Considering the equivalence induced by replacing μ_2 with $\mu_2\beta^d$ for all $\beta \in \mathbb{F}_{2^n}^*$, then $Tr_k^n(ax^d)$ is bent if and only if $Tr_1^n(a'x^d)$ is bent for all $a' \in \mathbb{F}_{2^k}^* \cdot \langle \alpha^d \rangle$, where $a' = \mu_2\beta^d$. Since $\gcd(d, 2^k+1) = 1$, we have $\mathbb{F}_{2^k}^* \cdot \langle \alpha^d \rangle = \mathbb{F}_{2^n}^*$. If $Tr_k^n(ax^d)$ is bent, then $Tr_1^n(a'x^d)$ is bent for all $a' \in \mathbb{F}_{2^n}^*$. This contradicts Theorem 17. Hence $Tr_k^n(ax^d)$ cannot be bent.

Given the above, the conclusion of the theorem holds. □

Table 2: The Known Vectorial Monomial Bent Functions of the form $Tr_m^n(ax^d)$ [1]

Case	Exponent d	Condition-1	Condition-2	Condition-3	Reference
Gold	2^s+1	$s \in \mathbb{N}$	$a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle$ [2]	Condition-C	Theorem 18
			$a \notin \langle \alpha^{\gcd(d,t)} \rangle$ [2]	–	Theorem 19
Dillon	$s(2^k-1)$	$\gcd(s, 2^k+1) = 1$	$K(a) = 0, a \in \mathbb{F}_{2^k}^*$ [2]	Condition-C	Theorem 18
				$m = 2$, $n \equiv 2 (\bmod\ 4)$	Theorem 20
		$s = 1$	$K(N_k^n(a)) = 0$, $a \in \mathbb{F}_{2^n}^*$ [2]	Condition-C	Theorem 18
				$m = 2$, $n \equiv 2 (\bmod\ 4)$	Theorem 20
Kasami	$2^{2s} - 2^s + 1$	$s \in \mathbb{N}$, $\gcd(3, n) = 1$, $\gcd(s, n) = 1$	$a \notin \langle \alpha^{\gcd(3,t)} \rangle$ [2]	–	Theorem 22
			$a \notin \langle \alpha^3 \rangle$ [2]	m is odd [2]	
				Condition-C[3,2]	
Leander	$(2^s+1)^2$	$s \in \mathbb{N}^*$, $n = 4s$	s odd, $a \in \mathbb{F}_4 \setminus \mathbb{F}_2 \cdot \langle \alpha^{2^s+1} \rangle$ [2]	m is odd [2]	Theorem 23
				$m \mid n$ [2]	
				Condition-C [2]	
Canteaut-Charpin-Kyureghyan	$2^{2s} + 2^s + 1$	$s > 1$ integer, $n = 6s$	$a \in \{\rho : Tr_s^k(\rho) = 0$, $\rho \in \mathbb{F}_{2^k}^*\} \cdot \langle \alpha^d \rangle$ [2]	Condition-C	Theorem 18
				$m \mid 2s$	Theorem 24

[1] $n = 2k$ and $a \in \mathbb{F}_{2^n}^*$.
[2] Necessary and sufficient conditions for $Tr_m^n(ax^d)$ to be bent.
[3] Every one of the four conditions in Theorem 9.

Table 3: The Nonexistence of the Vectorial Monomial Bent Functions of the form $Tr_m^n(ax^d)$ [1]

Case	Exponent d	Condition-1	m [2]	References
Dillon	$s(2^k-1)$	$\gcd(s, 2^k+1) = 1$	k	[48], Theorem 21
		$s = 1$	k	Theorem 21
Kasami	$2^{2s} - 2^s + 1$	$s \in \mathbb{N}$, $\gcd(3, n) = 1$, $\gcd(s, n) = 1$	m even	Corollary 3
Leander	$(2^s+1)^2$	$s \in \mathbb{N}^*$, $n = 4s$	m even	Corollary 4
			$m \nmid s$	
Canteaut-Charpin-Kyureghyan	$2^{2s} + 2^s + 1$	$s > 1$ integer, $n = 6s$	k	Theorem 25

[1] $n = 2k$ and $a \in \mathbb{F}_{2^n}^*$.
[2] If m is the value in this column, there does not exist the vectorial monomial bent functions of the form $Tr_m^n(ax^d)$.

Table 4: The Vectorial Monomial Bent Functions of the form $Tr_k^n(ax^d)$ [1]

<table>
<tr><th>Case</th><th>Exponent d</th><th>Condition-1</th><th colspan="2">Condition-2</th><th>E.[4]</th><th>References</th></tr>
<tr><td rowspan="2">Gold</td><td rowspan="2">2^s+1</td><td rowspan="2">$s \in \mathbb{N}$</td><td colspan="2">$a \notin \langle \alpha^{\gcd(d,2^k+1)} \rangle$ [2]</td><td rowspan="2">Yes</td><td rowspan="2">Corollary 2</td></tr>
<tr><td>$a \notin \langle \alpha^{\gcd(d,2^n-1)} \rangle$[2]</td><td>Condition-D[3,2]</td></tr>
<tr><td rowspan="2">Dillon</td><td rowspan="2">$s(2^k-1)$</td><td>$\gcd(s,2^k+1)=1$</td><td colspan="2">$a \in \mathbb{F}_{2^k}^*$</td><td rowspan="2">No</td><td>[48],
Theorem 21</td></tr>
<tr><td>$s=1$</td><td colspan="2">–</td><td>Theorem 21</td></tr>
<tr><td rowspan="3">Kasami</td><td rowspan="3">$2^{2s}-2^s+1$</td><td rowspan="3">$s \in \mathbb{N}$,
$\gcd(3,n)=1$,
$\gcd(s,n)=1$</td><td colspan="2">$a \notin \langle \alpha^{\gcd(3,2^k+1)} \rangle$ [2]</td><td rowspan="3">Yes</td><td rowspan="3">Theorem 22</td></tr>
<tr><td rowspan="2">$a \notin \langle \alpha^3 \rangle$ [2]</td><td>k is odd [2]</td></tr>
<tr><td>Condition-D[2]</td></tr>
<tr><td>Leander</td><td>$(2^s+1)^2$</td><td>$s \in \mathbb{N}^*$, $n=4s$</td><td colspan="2">–</td><td>No</td><td>Corollary 4</td></tr>
<tr><td>Canteaut-
Charpin-
Kyureghyan</td><td>$2^{2s}+2^s+1$</td><td>$s>1$ integer,
$n=6s$</td><td colspan="2">–</td><td>No</td><td>Theorem 25</td></tr>
</table>

[1] $n=2k$ and $a \in \mathbb{F}_{2^n}^*$.
[2] Necessary and sufficient conditions for $Tr_k^n(ax^d)$ to be bent.
[3] Every one of the four conditions in Theorem 9 with $m=k$.
[4] The existence of the vectorial monomial bent functions of the form $Tr_k^n(ax^d)$.

4 The vectorial Boolean bent functions with multiple trace terms

The Boolean bent functions with multiple trace terms have been researched in a large number of public literatures [7, 9, 14, 18, 20, 24, 25, 29, 33, 35, 41–44, 47, 59, 62]. However, the discussions of the vectorial Boolean bent functions with multiple trace terms are rare, only few can be found in [48, 49, 58].

In this section, we investigate the constructions of the vectorial Boolean bent functions with multiple trace terms.

4.1 General constructions of the vectorial Boolean bent functions with multiple trace terms

This subsection discusses general constructions of the vectorial Boolean bent functions with multiple trace terms, and answers Open Problem 1 in [48] (named Open Problem 4 in this paper).

In order to gain general constructions of the vectorial Boolean bent functions with multiple trace terms, we give the following theorem, which can be obtained by Theorem 2 directly.

Theorem 26. *Let the Boolean function $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ on $\mathbb{F}_{2^n}$ be bent, where $a_i \in \mathbb{F}_{2^n}^*$ for $i=1,2,\cdots,j$. Then the (n,m)-function $Tr_m^n(\sum_{i=1}^{j} a_i x^{d_i})$ is bent if $Tr_1^n(\lambda \sum_{i=1}^{j} a_i x^{d_i})$ is linear equivalent to $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ for all $\lambda \in \mathbb{F}_{2^m}^*$.*

Given a Boolean bent function $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ on $\mathbb{F}_{2^n}$, where $a_i \in \mathbb{F}_{2^n}^*$ for $i=1,2,\cdots,j$, to construct vectorial Boolean bent functions by Theorem 26, it is the principal concern that ensuring the linear equivalence between $Tr_1^n(\lambda \sum_{i=1}^{j} a_i x^{d_i})$ and $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ for all $\lambda \in \mathbb{F}_{2^m}^*$. We give four conditions which will be used to meet the condition that $Tr_1^n(\lambda \sum_{i=1}^{j} a_i x^{d_i})$ is linear equivalent to $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ for all $\lambda \in \mathbb{F}_{2^m}^*$.

Before that, the following lemma is given.

Lemma 6. *Let $m \mid n$ and $d \in \mathbb{Z}^*$. For $\forall\ \beta \in \mathbb{F}_{2^n}^*$, then $\beta^u = 1$ if one of the following four conditions holds:*

(1) $u = \frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1-1}}$ *and* $\beta^d \in \mathbb{F}_{2^m}^*$.

(2) $u = \frac{v_2(2^n-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}$.

(3) $u = \frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3-1}}$ *and* $\gcd(\frac{d^{l_3}}{\gcd(d^{l'_3},t)}, 2^m-1) = 1$, $\beta^d \in \mathbb{F}_{2^m}^*$.

(4) $u = \frac{v_4(2^n-1)\gcd(d^{l'_4},t)}{d^{l_4}}$ *and* $\gcd(\frac{d^{l_4}}{\gcd(d^{l'_4},t)}, 2^m-1) = 1$,

where v_ϱ are some integers such that u is integer and $l_\varrho \in \mathbb{N}^*$ for $\varrho = 1,2,3,4$, $l'_3, l'_4 \in \mathbb{N}^*$, $l_3 \geq l'_3$ and $l_4 \geq l'_4$.

Proof. (1) Let $\lambda = \beta^d$. Then $\lambda \in \mathbb{F}_{2^m}^*$. For $u = \frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1-1}}$, we have

$$\begin{aligned}
\beta^u &= \beta^{\frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1-1}}}\\
&= \beta^{d\cdot\frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1}}}\\
&= \lambda^{\frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1}}}\\
&\quad (\because\ \gcd(\frac{d^{l_1}}{\gcd(d^{l_1},2^m-1)}, 2^m-1) = 1,\ \therefore\ \exists\ \gamma \in \mathbb{F}_{2^m}^*\ s.t.\ \lambda = \gamma^{\frac{d^{l_1}}{\gcd(d^{l_1},2^m-1)}})\\
&= (\gamma^{\frac{d^{l_1}}{\gcd(d^{l_1},2^m-1)}})^{\frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1}}}\\
&= \gamma^{v_1(2^m-1)}\\
&= 1.
\end{aligned}$$

(2) Let $\sigma = \beta^t$. Then $\sigma \in \mathbb{F}_{2^m}^*$. For $u = \frac{v_2(2^n-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}$, we have

$$\begin{aligned}
\beta^u &= \beta^{\frac{v_2(2^n-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}}\\
&= \beta^{t\cdot\frac{v_2(2^m-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}}\\
&= \sigma^{\frac{v_2(2^m-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}}\\
&\quad (\because\ \gcd(\frac{d^{l_2}}{\gcd(d^{l_2},2^m-1)}, 2^m-1) = 1,\ \therefore\ \exists\ \gamma \in \mathbb{F}_{2^m}^*\ s.t.\ \sigma = \gamma^{\frac{d^{l_2}}{\gcd(d^{l_2},2^m-1)}})\\
&= (\gamma^{\frac{d^{l_2}}{\gcd(d^{l_2},2^m-1)}})^{\frac{v_2(2^m-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}}\\
&= \gamma^{v_2(2^m-1)}\\
&= 1.
\end{aligned}$$

(3) Let $\lambda = \beta^d$. Then $\lambda \in \mathbb{F}_{2^m}^*$. For $u = \frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3-1}}$, we have

$$\begin{aligned}
\beta^u &= \beta^{\frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3-1}}} \\
&= \beta^{d\cdot\frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3}}} \\
&= \lambda^{\frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3}}} \\
&\quad (\because\ \gcd(\frac{d^{l_3}}{\gcd(d^{l'_3},t)}, 2^m-1) = 1,\ \therefore\ \exists\ \gamma \in \mathbb{F}_{2^m}^*\ s.t.\ \lambda = \gamma^{\frac{d^{l_3}}{\gcd(d^{l'_3},t)}}) \\
&= \left(\gamma^{\frac{d^{l_3}}{\gcd(d^{l'_3},t)}}\right)^{\frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d^{l_3}}} \\
&= \gamma^{v_3(2^m-1)} \\
&= 1.
\end{aligned}$$

(4) Let $\sigma = \beta^t$. Then $\sigma \in \mathbb{F}_{2^m}^*$. For $u = \frac{v_4(2^n-1)\gcd(d^{l'_4},t)}{d^{l_4}}$, we have

$$\begin{aligned}
\beta^u &= \beta^{\frac{v_4(2^n-1)\gcd(d^{l'_4},t)}{d^{l_4}}} \\
&= \beta^{t\cdot\frac{v_4(2^m-1)\gcd(d^{l'_4},t)}{d^{l_4}}} \\
&= \sigma^{\frac{v_4(2^m-1)\gcd(d^{l'_4},t)}{d^{l_4}}} \\
&\quad (\because\ \gcd(\frac{d^{l_4}}{\gcd(d^{l'_4},t)}, 2^m-1) = 1,\ \therefore\ \exists\ \gamma \in \mathbb{F}_{2^m}^*\ s.t.\ \sigma = \gamma^{\frac{d^{l_4}}{\gcd(d^{l'_4},t)}}) \\
&= \left(\gamma^{\frac{d^{l_4}}{\gcd(d^{l'_4},t)}}\right)^{\frac{v_4(2^m-1)\gcd(d^{l'_4},t)}{d^{l_4}}} \\
&= \gamma^{v_4(2^m-1)} \\
&= 1.
\end{aligned}$$

Given the above, the theorem is proved to be true. □

If $\gcd(\frac{d^l}{\gcd(d^{l'},t)}, 2^m-1) = 1$ with $l \geq l'$ holds, by Theorem 8, then every one of the three conditions in Theorem 5 holds. By item (1) of Theorem 5 and Lemma 6, we have the following theorem.

Theorem 27. *Let $m \mid n$ and $d \in \mathbb{Z}^*$. For $\forall\ \lambda \in \mathbb{F}_{2^m}^*$, then there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^d = \beta^{d+u}$ if one of the following four conditions holds:*

(1) $u = \frac{v_1(2^m-1)\gcd(d^{l_1},2^m-1)}{d^{l_1-1}}$ *and one of the three conditions in Theorem 5 holds,*

(2) $u = \frac{v_2(2^n-1)\gcd(d^{l_2},2^m-1)}{d^{l_2}}$ *and one of the three conditions in Theorem 5 holds,*

(3) $u = \frac{v_3(2^m-1)\gcd(d^{l'_3},t)}{d_1^{l_3-1}}$ *and* $\gcd(\frac{d_1^{l_3}}{\gcd(d^{l'_3},t)}, 2^m-1) = 1,$

(4) $u = \frac{v_4(2^n-1)\gcd(d^{l'_4},t)}{d^{l_4}}$ *and* $\gcd(\frac{d^{l_4}}{\gcd(d^{l'_4},t)}, 2^m-1) = 1,$

where v_ϱ are some integers such that u is integer and $l_\varrho \in \mathbb{N}^*$ for $\varrho = 1, 2, 3, 4$, $l'_3, l'_4 \in \mathbb{N}^*$, $l_3 \geq l'_3$ and $l_4 \geq l'_4$.

The general constructions of the vectorial Boolean bent functions with multiple trace terms corresponding to the four conditions in Theorem 27 can be obtained as the following theorem.

Theorem 28. *Let $m \mid n$ and*

$$u_i = \begin{cases} \frac{s_i(2^m-1)\gcd(d_1^{l_i}, 2^m-1)}{d_1^{l_i-1}}, & i = 2, \cdots, j_1 \\ \frac{s_i(2^n-1)\gcd(d_1^{l_i}, 2^m-1)}{d_1^{l_i}}, & i = j_1+1, \cdots, j_2 \\ \frac{s_i(2^m-1)\gcd(d_1^{l'_i}, t)}{d_1^{l_i-1}}, & i = j_2+1, \cdots, j_3 \\ \frac{s_i(2^n-1)\gcd(d_1^{l'_i}, t)}{d_1^{l_i}}, & i = j_3+1, \cdots, j, \end{cases}$$

where $l_i, l'_i \in \mathbb{N}^*$, $l_i \geq l'_i$ and s_i are some integers such that u_i is integer. Let the Boolean function $Tr_1^n(a_1x^{d_1} + \sum_{i=2}^{j} a_ix^{d_1+u_i})$ on $\mathbb{F}_{2^n}$ be bent, where $a_i \in \mathbb{F}_{2^n}^*$ for $i = 1, 2, \cdots, j$. Then the (n, m)-function

$$Tr_m^n(a_1x^{d_1} + \sum_{i=2}^{j} a_ix^{d_1+u_i})$$

is bent if one of the following two conditions holds:

(1) *$j \geq j_2 + 1$ and $\gcd(\frac{d_1^{l_i}}{\gcd(d_1^{l'_i}, t)}, 2^m - 1) = 1$ for $i = j_2 + 1, j_2 + 2, \cdots, j,$.*

(2) *$j \leq j_2$ and the three conditions in Theorem 5 with $d = d_1$ holds.*

Proof. Since the proofs of the two items are similar, we only give the proof of item (1).

If $\gcd(\frac{d_1^{l_i}}{\gcd(d_1^{l'_i}, t)}, 2^m - 1) = 1$ with $l_i \geq l'_i$ holds for some i, by Theorem 8, then every one of the three conditions in Theorem 5 with $d = d_1$ holds. By item (1) of Theorem 5, there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^{d_1}$ for all $\lambda \in \mathbb{F}_{2^m}^*$. According to Theorem 27, for every $\lambda \in \mathbb{F}_{2^m}^*$, we know that there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^{d_1+u_i}$ for $i = 2, 3, \cdots, j$.

By Definition 5, we have that there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that

$$Tr_1^n(a_1\lambda x^{d_1} + \sum_{i=2}^{j} a_i\lambda x^{d_1+u_i}) = Tr_1^n(a_1(\beta x)^{d_1} + \sum_{i=2}^{j} a_i(\beta x)^{d_1+u_i})$$

is linear equivalent to $Tr_1^n(a_1x^{d_1} + \sum_{i=2}^{j} a_ix^{d_1+u_i})$ for all $\lambda \in \mathbb{F}_{2^m}^*$. According to Theorem 26, the (n, m)-function $Tr_m^n(a_1x^{d_1} + \sum_{i=2}^{j} a_ix^{d_1+u_i})$ is bent.

Given the above, the theorem is proved to be true. □

In [48], on the premise that x^{d_1} is a permutation of $\mathbb{F}_{2^m}$, i.e., $\gcd(d_1, 2^m - 1) = 1$, A.Muratović-Ribić et al. presented a general construction of the bent (n, m)-functions of the form $Tr_m^n(a_1x^{d_1} + \sum_{i=2}^{j} a_ix^{d_1+v_i(2^m-1)})$, and left an open problem as follows.

Open Problem 4 (named Open problem 1 in [48])**.** *Let $n \geq 4$, $m \mid n$ and $m \leq k$. Let x^{d_1} be a permutation of $\mathbb{F}_{2^m}$ and $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$ be a Boolean bent function, where $d_i = d_1 + v_i(2^m - 1)$ for $i = 2, \cdots, j$ and some integers $v_i \geq 0$. Then the function $Tr_m^n(\sum_{i=1}^{j} a_i x^{d_i})$ is a vectorial bent function.*

It is interest to prove a similar result to the above result for the functions of the form $Tr_1^n(\sum_{i=1}^{j} a_i x^{d_i})$, if x^{d_1} is not a permutation over $\mathbb{F}_{2^m}$.

To answer Open Problem 4 in detail, we should discuss the relations between every one of the four conditions in Theorem 27 and the condition that $u = v(2^m - 1)$, $\gcd(d, 2^m - 1) = 1$.

Before that, a lemma is given as follows.

Lemma 7. *Let $m \mid n$, $d \in \mathbb{Z}^*$ and denote*

$S_1 = \{\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}} + \theta_1(2^n - 1) \in \mathbb{Z} : v_1, \theta_1 \in \mathbb{Z}, l_1 \in \mathbb{N}^*\}$,

$S_2 = \{\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}} + \theta_2(2^n - 1) \in \mathbb{Z} : v_2, \theta_2 \in \mathbb{Z}, l_2 \in \mathbb{N}^*\}$,

$S_3 = \{\frac{v_3(2^m-1)\gcd(d^{l'_3}, t)}{d_1^{l_3-1}} + \theta_3(2^n - 1) \in \mathbb{Z} : v_3, \theta_3 \in \mathbb{Z}, \gcd(\frac{d_1^{l_3}}{\gcd(d^{l'_3}, t)}, 2^m - 1) = 1, l_3, l'_3 \in \mathbb{N}^*, l_3 \geq l'_3\}$,

$S_4 = \{\frac{v_4(2^n-1)\gcd(d^{l'_4}, t)}{d^{l_4}} + \theta_4(2^n - 1) \in \mathbb{Z} : v_4, \theta_4 \in \mathbb{Z}, \gcd(\frac{d^{l_4}}{\gcd(d^{l'_4}, t)}, 2^m - 1) = 1, l_4, l'_4 \in \mathbb{N}^*, l_4 \geq l'_4\}$,

$S_5 = \{v_5(2^m - 1) + \theta_5(2^n - 1) : v_5, \theta_5 \in \mathbb{Z}, \gcd(d, 2^m - 1) = 1\}$.

Then the following conclusions hold:

(1) $S_1 \supset S_5$.

(2) $S_2 \not\subseteq S_5$ *and* $S_2 \not\supseteq S_5$.

(3) $S_3 \supset S_5$.

(4) $S_4 \not\subseteq S_5$ *and* $S_4 \not\supseteq S_5$.

Proof. (1) For $\forall$ $\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}} + \theta_1(2^n - 1) \in S_1$, if $\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}} + \theta_1(2^n - 1) \in S_5$, then there exist some $\theta \in \mathbb{Z}$ such that $\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}}$ can be represented in the form $v_5(2^m - 1) + \theta(2^n - 1)$ and

$$v_5 = \frac{v_1 \gcd(d^{l_1}, 2^m - 1)}{d^{l_1-1}} - \theta t.$$

Note that there exist some $\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}} + \theta_1(2^n - 1) \in S_1$ such that some $\frac{v_1 \gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}}$ are not integer. If $S_1 \subseteq S_5$, then there exists some $\frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}}$ such that some $v_5 = \frac{v_1 \gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}} - \theta t$ are not integer. This contradicts $v_5 \in \mathbb{Z}$. Therefore, $S_1 \not\subseteq S_5$.

If $\gcd(d, 2^m - 1) = 1$, by Theorem 8, every one of the three conditions in Theorem 5 holds, and $\frac{d^{l_1-1}}{\gcd(d^{l_1}, 2^m-1)} = d^{l_1-1}$. For $\gcd(d, 2^m - 1) = 1$ and $\forall\ v_5$ identified as in S_5, let the integer $v_1 = v_5 \cdot \frac{d^{l_1-1}}{\gcd(d^{l_1}, 2^m-1)}$. Then $v_5(2^m - 1) = \frac{v_1(2^m-1)\gcd(d^{l_1}, 2^m-1)}{d^{l_1-1}}$. Therefore, $S_1 \supseteq S_5$. Thus, $S_1 \supset S_5$.

(2) For $\forall\ \frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}} + \theta_2(2^n - 1) \in S_2$, if $\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}} + \theta_2(2^n - 1) \in S_5$, then there exist some $\theta \in \mathbb{Z}$ such that $\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}}$ can be represented in the form $v_5(2^m - 1) + \theta(2^n - 1)$ and

$$v_5 = \frac{v_2 t \gcd(d^{l_2}, 2^m - 1)}{d^{l_2}} - \theta t.$$

Note that there exist some $\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}} + \theta_2(2^n - 1) \in S_2$ such that some $\frac{v_2 t \gcd(d^{l_2}, 2^m-1)}{d^{l_2}}$ are not integer. If $S_2 \subseteq S_5$, then there exist some $\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}}$ such that some $v_5 = \frac{v_2 t \gcd(d^{l_2}, 2^m-1)}{d^{l_2}} - \theta t$ are not integer. This contradicts $v_5 \in \mathbb{Z}$. Therefore, $S_2 \not\subseteq S_5$.

For $\forall\ v_5(2^m - 1) + \theta_5(2^n - 1) \in S_5$, if $v_5(2^m - 1) + \theta_5(2^n - 1) \in S_2$, then there exist some $\theta \in \mathbb{Z}$ such that $v_5(2^m - 1)$ can be represented in the form $\frac{v_2(2^n-1)\gcd(d^{l_2}, 2^m-1)}{d^{l_2}} + \theta(2^n - 1)$ and

$$v_2 = \frac{v_5 d^{l_2}}{t \gcd(d^{l_2}, 2^m - 1)} - \theta \cdot \frac{d^{l_2}}{\gcd(d^{l_2}, 2^m - 1)}.$$

Note that $\frac{d^{l_2}}{\gcd(d^{l_2}, 2^m-1)}$ is integer and there exist some $v_5(2^m - 1) + \theta_5(2^n - 1) \in S_2$ such that some $\frac{v_5 d^{l_2}}{t \gcd(d^{l_2}, 2^m-1)}$ are not integer. If $S_2 \supseteq S_5$, then there exist some $v_5(2^m - 1)$ such that some $v_2 = \frac{v_5 d^{l_2}}{t \gcd(d^{l_2}, 2^m-1)} - \theta \cdot \frac{d^{l_2}}{\gcd(d^{l_2}, 2^m-1)}$ are not integer. This contradicts $v_2 \in \mathbb{Z}$. Therefore, $S_2 \not\supseteq S_5$.

Item (3) can be proved by the similar method of item (1), and item (4) can be proved by the similar method of item (2). □

By Theorem 8 and Lemma 7, we can derive the following theorem.

Theorem 29. *Let v be integer and the other parameters be identified with them in Theorem 27. Then the following conclusions hold:*

(1) *Each of item (1) and item (3) in Theorem 27 includes the condition that $u = v(2^m - 1)$, $\gcd(d, 2^m - 1) = 1$ as a special case.*

(2) *Each of item (2) and item (4) in Theorem 27 is neither sufficient and nor necessary for the condition that $u = v(2^m - 1)$, $\gcd(d, 2^m - 1) = 1$ to hold.*

Remark 10. *Let v be integer and the other parameters be identified with them in Theorem 27. The reason why the four conditions in Theorem 27 and the condition $u = v(2^m - 1)$, $\gcd(d, 2^m - 1) = 1$ can educe bent (n, m)-functions is that they make there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^d = \beta^{d+u}$ for all $\lambda \in \mathbb{F}_{2^m}^*$.*

There are some other conditions, which are neither sufficient and nor necessary for the condition $u = v(2^m - 1)$, $\gcd(d, 2^m - 1) = 1$ to hold, can also ensure that there exist some $\beta \in \mathbb{F}_{2^n}^*$ such that $\lambda = \beta^d = \beta^{d+u}$ for all $\lambda \in \mathbb{F}_{2^m}^*$. But they are special cases of item (1) *or item (3) of Theorem 27. Three such examples are given as follows, where v'_ϱ are some integers such that u is integer for $\varrho = 1, 2, 3$ and $l \in \mathbb{N}^*$:*

(1) $u = \frac{v'_1(2^m-1)d^2}{\gcd(d,2^m-1)}$ *and one of the three conditions in Theorem 5 holds.*

(2) $u = \frac{v'_2(2^m-1)d^2}{\gcd(d,t)}$ *and one of the three conditions in Theorem 5 holds.*

(3) $u = \frac{v'_3(2^n-1)}{d^{l-1}}$ *and one of the three conditions in Theorem 5 with $d = d^l$ holds.*

By the similar method of the proof of Lemma 7, it can be proved that each of item (1) and item (3) of Theorem 27 includes the above three items as special cases.

Anwsers to Open Problem 4. *By Theorem 8 and Theorem 29, we have that Theorem 28 gives answers to Open Problem 4.*

Similarly to Theorem 12, by Theorem 1, the (n,m)-function of the form $Tr_m^{n_1}(\sum_{i=1}^{j_1} a_i x^{d_i}) + Tr_m^{n_2}(\sum_{j_1+1}^{j_2} a_i x^{d_i}) + \cdots + Tr_m^{n_r}(\sum_{i=j_{r-1}+1}^{j} a_i x^{d_i})$ is bent if and only if the Boolean function $Tr_1^{n_1}(\sum_{i=1}^{j_1} a_i \lambda x^{d_i}) + Tr_1^{n_2}(\sum_{j_1+1}^{j_2} a_i \lambda x^{d_i}) + \cdots + Tr_1^{n_r}(\sum_{i=j_{r-1}+1}^{j} a_i \lambda x^{d_i})$ is bent for all $\lambda \in \mathbb{F}_{2^m}^*$, where $a_i \in \mathbb{F}_{2^n}^*$ for $i = 1, 2, \cdots, j$. A similar idea was also used in [5, 58]. For the convenience of discussion, we list this fact as the following theorem.

Theorem 30. *Let $m \mid n$, $n_\varrho \in \mathbb{N}^*$ and $m \mid n_\varrho$ for $\varrho = 1, 2, \cdots, \varsigma$, $a_i \in \mathbb{F}_{2^n}^*$ for $i = 1, 2, \cdots, j$, and denote*

$$C = \{(\beta_1, \beta_2, \cdots, \beta_j) \in (\mathbb{F}_{2^n}^*)^r \ for\ i = 1, 2, \cdots, j : f(x)\ is\ bent\},$$

where $f(x)$ is the Boolean function on $\mathbb{F}_{2^n}$ of the form

$$Tr_1^{n_1}(\sum_{i=1}^{j_1} \beta_i x^{d_i}) + Tr_1^{n_2}(\sum_{j_1+1}^{j_2} \beta_i x^{d_i}) + \cdots + Tr_1^{n_\varsigma}(\sum_{i=j_{\varsigma-1}+1}^{j} \beta_i x^{d_i}).$$

Then the (n,m)-function

$$F(x) = Tr_m^{n_1}(\sum_{i=1}^{j_1} a_i x^{d_i}) + Tr_m^{n_2}(\sum_{j_1+1}^{j_2} a_i x^{d_i}) + \cdots + Tr_m^{n_\varsigma}(\sum_{i=j_{\varsigma-1}+1}^{j} a_i x^{d_i})$$

is bent if and only if

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

4.2 Explicit constructions of the vectorial Boolean bent functions with multiple trace terms

This subsection focuses on the explicit constructions of vectorial Boolean bent functions with multiple trace terms.

4.2.1 The Boolean bent functions with multiple trace terms

We recall some constructions of the Boolean bent functions with multiple trace terms, which will be used in the explicit constructions of the vectorial Boolean bent functions with multiple trace terms.

A positive integer d (in the sense of modulo 2^n-1) is named as a *Niho exponent* and x^d a *Niho power function* if the restriction of x^d to $\mathbb{F}_{2^k}$ is linear [25, 50], i.e., $d \equiv 2^s (\bmod\ 2^k-1)$ for some nonnegative integer $s<n$. A bent function is named as a *Niho bent function* if the exponents of all its non-constant terms are Niho exponents, when it is viewed in the univariate representation.

When considering $Tr_1^n(x^d)$, without loss of generality, we assume that the Niho exponent d is in the *normalized form* [33], i.e., with $s=0$. Then the Niho exponent d can be represented uniquely [33] as

$$d=(2^k-1)l+1,$$

where $2 \leq l \leq 2^k$. If l for the definition of the Niho exponent is written as a fraction, then l is in the sense of modulo 2^k+1. For example, $l=\frac{1}{2}=2^{k-1}+1$, i.e., $2l \equiv 1(\bmod\ 2^k+1)$. Note that the monomial bent functions with a Niho exponent for $l=\frac{1}{2}$, i.e., $Tr_1^n(ax^{2^k+1})$, where $a \in \mathbb{F}_{2^k}^*$, is a special case of the monomial bent functions with the Gold exponent for $s=k$ (see Theorem 13).

In [24, 25], three infinite classes of binomial Niho bent functions were obtained. Later, an infinite class of the Boolean bent functions on $\mathbb{F}_{2^n}$ with 2^{r-1} Niho exponents for any integer $r>1$ and $\gcd(r,k)=1$ was presented in [33], which is a generalization of one class of the binomial Niho bent functions in [24, 25]. Further study on the Boolean bent functions on $\mathbb{F}_{2^n}$ with 2^{r-1} Niho exponents can be found in [7, 9, 14], where $r>1$ and $\gcd(r,k)=1$. In [35], up to the EA-equivalence, an equivalent form of the construction as in [33] was presented.

Theorem 31 ([35]). *Let $i,r \in \mathbb{N}^*$, $r<k$, $\gcd(r,k)=1$, $l_i \equiv \frac{i}{2^r}(\bmod\ 2^k+1)$ and $a \in \mathbb{F}_{2^n}^*$. Then the Boolean function*

$$Tr_1^n(ax^{(2^k-1)\frac{1}{2}+1}+(a+a^{2^k})\sum_{i=1}^{2^{r-1}-1} x^{(2^k-1)l_i+1})$$

on $\mathbb{F}_{2^n}$ is bent if $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

The quadratic functions which are the sums of some trace functions with Gold exponents were studied in several papers [20, 31, 37, 60, 62]. In [29], four infinite classes of the Boolean bent functions with some Gold exponents were introduced, and can be described as the following theorem.

Theorem 32 ([29]). *Let $e \in \mathbb{N}^*$, $e \mid n$, $\zeta=\frac{n}{e}$ be even, $\zeta_0, j, l \in \mathbb{N}^*$, ζ_0 be the maximum odd divisor of ζ, $1 \leq j \leq \frac{\zeta}{2}-1$ and $a \in \mathbb{F}_{2^e}^*$. For the Boolean functions on $\mathbb{F}_{2^n}$ below, the following conclusions hold:*

(1) $\sum_{i=0}^{\frac{\zeta}{2}-1} Tr_1^n(ax^{2^{ei}+1})+Tr_1^k(ax^{2^k+1})$ *is bent.*

(2) $\sum_{i=0}^{j} Tr_1^n(ax^{2^{eli}+1})+Tr_1^k(ax^{2^k+1})$ *is bent if and only if* $\gcd((2j+1)l,\zeta_0)=\gcd(l,\zeta_0)$.

(3) $\sum\limits_{i=0}^{\frac{\zeta}{2}-1} Tr_1^n(ax^{2^{ei}+1}) + \sum\limits_{i=0}^{j} Tr_1^n(ax^{2^{eli}+1}) + Tr_1^k(ax^{2^k+1})$ *is bent if and only if* $\gcd((2j+1)l, \zeta_0) = \gcd(l, \zeta_0)$.

(4) $Tr_1^n(ax^{2^{el}+1}) + Tr_1^n(ax^{2^{3el}+1}) + Tr_1^k(ax^{2^k+1})$ *is bent if and only if* $\gcd(3l, \zeta_0) = \gcd(5l, \zeta_0) = \gcd(l, \zeta_0)$.

In [36], the functions which are the sums of the trace functions with Dillon exponents were investigated. An infinite class of Boolean bent functions as the following theorem was obtained in [36].

Theorem 33 ([36])**.** *Let* $1 \le s \le k-1$, $\gcd(s-1, m) = 1$ *and* $a \in \mathbb{F}_{2^k}^*$. *Then the Boolean function*

$$\sum_{i=1}^{2^{k-s}} Tr_1^n(ax^{(2i-1)(2^k-1)})$$

on $\mathbb{F}_{2^n}$ *is bent if and only if*

$$\sum_{z \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k(a^{2^{s-1}} z^{2^{s-1}-1} + z)} = 0.$$

A corollary of Theorem 33 was also given in [36], which shows that then the Boolean function $\sum_{i=1}^{2^{k-2}} Tr_1^n(ax^{(2i-1)(2^k-1)})$ on $\mathbb{F}_{2^n}$ is bent if $a \in \mathbb{F}_{2^k} \setminus \{0,1\}$. Note the fact that, for $a \in \mathbb{F}_{2^k}$, $\sum_{z \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k((a^2+1)z)} = 0$ if and only if $a \in \mathbb{F}_{2^k} \setminus \{1\}$. Thus, by Theorem 33, for $a \in \mathbb{F}_{2^k}$, we have that $a \in \mathbb{F}_{2^k} \setminus \{0,1\}$ is also necessary for the Boolean function $\sum_{i=1}^{2^{k-2}} Tr_1^n(ax^{(2i-1)(2^k-1)})$ on $\mathbb{F}_{2^n}$ to be bent.

Corollary 5. *Let* $a \in \mathbb{F}_{2^k}^*$. *Then the Boolean function*

$$\sum_{i=1}^{2^{k-2}} Tr_1^n(ax^{(2i-1)(2^k-1)})$$

on $\mathbb{F}_{2^n}$ *is bent if and only if* $a \in \mathbb{F}_{2^k} \setminus \{0,1\}$.

4.2.2 Constructing the vectorial Boolean bent functions with multiple trace terms

Based on the above, we discuss the explicit constructions of the vectorial Boolean bent functions with multiple trace terms. Six new infinite classes of the explicit constructions of such bent (n,m)-functions are obtained, i.e., one classes with 2^{r-1} Niho exponents, where $r < k$ and $\gcd(r,k) = 1$, four classes with some Gold exponents and one classes with 2^{k-2} Dillon exponents. Besides, the nonexistence of the bent (n,k)-functions of the form $\sum_{i=1}^{2^{k-2}} Tr_k^n(ax^{(2i-1)(2^k-1)})$ is shown, where $a \in \mathbb{F}_{2^k}^*$. The known vectorial Boolean bent functions with multiple trace terms are listed in Table 5.

An infinite class of the bent (n,m)-functions with 2^{r-1} Niho exponents is given as the following theorem, where $r > 1$ and $\gcd(r,k) = 1$.

Theorem 34. *Let $m \mid k$, $i, r \in \mathbb{N}^*$, $r < k$, $\gcd(r, k) = 1$, $l_i \equiv \frac{i}{2^r} (\bmod\ 2^k + 1)$ and $a \in \mathbb{F}_{2^n}^*$. Then the (n, m)-function*

$$Tr_m^n(ax^{(2^k-1)\frac{1}{2}+1} + (a + a^{2^k}) \sum_{i=1}^{2^{r-1}-1} x^{(2^k-1)l_i+1})$$

is bent if $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$.

Proof. Since $m \mid k$, $\mathbb{F}_{2^m}^* \subseteq \mathbb{F}_{2^k}^*$. For $\forall\ a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, we have $a \cdot \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$. By Theorem 30 and Theorem 31, the conclusion holds. □

Four infinite classes of the vectorial Boolean bent functions which are the sums of some trace functions with Gold exponents can be derived as the following theorem.

Theorem 35. *Let $e \in \mathbb{N}^*$, $e \mid n$, $\zeta = \frac{n}{e}$ be even, $\zeta_0, j, l \in \mathbb{N}^*$, ζ_0 be the maximum odd divisor of ζ, $1 \leq j \leq \frac{\zeta}{2} - 1$ and $a \in \mathbb{F}_{2^e}^*$. For the (n, m)-functions below, if $m \mid e$, then the following conclusions hold:*

(1) $\sum_{i=0}^{\frac{\zeta}{2}-1} Tr_m^n(ax^{2^{ei}+1}) + Tr_m^k(ax^{2^k+1})$ *is bent.*

(2) $\sum_{i=0}^{j} Tr_m^n(ax^{2^{eli}+1}) + Tr_m^k(ax^{2^k+1})$ *is bent if and only if* $\gcd((2j + 1)l, \zeta_0) = \gcd(l, \zeta_0)$.

(3) $\sum_{i=0}^{\frac{\zeta}{2}-1} Tr_m^n(ax^{2^{ei}+1}) + \sum_{i=0}^{j} Tr_m^n(ax^{2^{eli}+1}) + Tr_m^k(ax^{2^k+1})$ *is bent if and only if* $\gcd((2j +1)l, \zeta_0) = \gcd(l, \zeta_0)$.

(4) $Tr_m^n(ax^{2^{el}+1}) + Tr_m^n(ax^{2^{3el}+1}) + Tr_m^k(ax^{2^k+1})$ *is bent if and only if* $\gcd(3l, \zeta_0) = \gcd(5l, \zeta_0) = \gcd(l, \zeta_0)$.

Proof. Since $\frac{n}{d}$ is even, we have that $m \mid k$ if $m \mid n$. By Theorem 30 and Theorem 32, the conclusions of this theorem hold. □

An infinite class of the bent (n, m)-functions with 2^{k-2} Niho bent exponents is given as the following theorem.

Theorem 36. *Let $m \mid k$ and $a \in \mathbb{F}_{2^k}^*$. Then the (n, m)-function*

$$\sum_{i=1}^{2^{k-2}} Tr_m^n(ax^{(2i-1)(2^k-1)})$$

is bent if and only if $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m}$.

Proof. Since $m \mid k$ and $a \in \mathbb{F}_{2^k}^*$, we have that $a \cdot \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_{2^k}^*$. Note that, for $\forall\ a \in \mathbb{F}_{2^k}^*$, $\{1\} \notin a \cdot \mathbb{F}_{2^m}^*$ if and only if $a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m}$. By Theorem 30 and Corollary 5, the conclusion holds. □

Remark 11. *In [58], it was claimed that, if $a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$, then the (n,k)-function $F(x) = \sum_{i=1}^{2^{k-2}} Tr_k^n(ax^{(2i-1)(2^k-1)})$ is bent. That is Theorem 4 in [58]. However, it is wrong. Here, we give a counter example.*

Let $k = 2$. Then $F(x) = Tr_2^4(ax^3)$. According to item (2) of Theorem 21, we have that $Tr_2^4(ax^3)$ is not bent.

If $m = k$, then $\mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m} = \varnothing$. Thus, by Theorem 36, we have the following corollary.

Corollary 6. *Let $a \in \mathbb{F}_{2^k}^*$. Then there does not exist a bent (n,k)-function of the form*

$$\sum_{i=1}^{2^{k-2}} Tr_k^n(ax^{(2i-1)(2^k-1)}).$$

Table 5: The Known Bent (n,m)-functions [1] with Multiple Trace Terms

Expression	Condition-1	Condition-2	Condition-3	References
$Tr_k^n(a_1x^{(2^k-1)\frac{1}{2}+1}$ $+a_2x^{(2^k-1)l+1})$	$(a_1 + a_1^{2^k})^2 = a_2^{2^k+1}$	$l = 3$	$a_2 \in \langle \alpha^{\gcd(5,t)} \rangle$, $k \equiv 2 (\mathrm{mod}\ 4)$	[48]
			$a_2 \in \mathbb{F}_{2^n}^*$, $k \not\equiv 2 (\mathrm{mod}\ 4)$	
		$l = \frac{1}{4}$, k odd	$a_1, a_2 \in \mathbb{F}_{2^n}^*$	
		$l = \frac{1}{6}$, k even		
$Tr_k^n(\sum_{i=1}^{2^k} a_ix^{i(2^k-1)})$	a_i characterized by Corollary 2 in [49]	–	–	[49]
$Tr_m^n(ax^{(2^k-1)\frac{1}{2}+1}$ $+(a+a^{2^k})$ $\cdot \sum_{i=1}^{2^{r-1}-1} x^{(2^k-1)l_i+1})$	$i, r \in \mathbb{N}^*$, $r < k$, $\gcd(r,k) = 1$, $l_i \equiv \frac{i}{2^r}(\mathrm{mod}\ 2^k+1)$, $m \mid k$	–	$a \in \mathbb{F}_{2^n} \setminus \mathbb{F}_{2^k}$	Theorem 34
$\sum_{i=0}^{\frac{\zeta}{2}-1} Tr_m^n(ax^{2^{ei}+1})$ $+Tr_m^k(ax^{2^k+1})$	$e \in \mathbb{N}^*$, $e \mid n$, $\zeta = \frac{n}{e}$ even $a \in \mathbb{F}_{2^e}^*$, $m \mid e$	–	–	Theorem 35
$\sum_{i=0}^{j} Tr_m^n(ax^{2^{eli}+1})$ $+Tr_m^k(ax^{2^k+1})$		$\zeta_0, j, l \in \mathbb{N}^*$ ζ_0 be the maximum odd divisor of ζ, $1 \leq j \leq \frac{\zeta}{2} - 1$	$\gcd((2j+1)l, \zeta_0)$ $= \gcd(l, \zeta_0)$ [2]	
$\sum_{i=0}^{\frac{\zeta}{2}-1} Tr_m^n(ax^{2^{ei}+1})$ $+\sum_{i=0}^{j} Tr_m^n(ax^{2^{eli}+1})$ $+Tr_m^k(ax^{2^k+1})$				
$Tr_m^n(ax^{2^{el}+1})$ $+Tr_m^n(ax^{2^{3el}+1})$ $+Tr_m^k(ax^{2^k+1})$			$\gcd(3l, \zeta_0)$ $= \gcd(5l, \zeta_0)$ $= \gcd(l, \zeta_0)$ [2]	
$\sum_{i=1}^{2^{k-2}} Tr_m^n(ax^{(2i-1)(2^k-1)})$	$a \in \mathbb{F}_{2^k}^*$, $m \mid k$	–	$a \in \mathbb{F}_{2^k} \setminus \mathbb{F}_{2^m}$ [2]	Theorem 36

[1] $n = 2k$.
[2] Necessary and sufficient conditions for the vectorial Boolean bent function to be bent.

5 $\mathcal{H}$ vectorial functions

In [45], S. Mesnager introduced an infinite class of vectorial Boolean bent functions of the form $yG(zy^{2^k-2})$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and G is an o-polynomial on $\mathbb{F}_{2^k}$, and called it as $\mathcal{H}$ vectorial functions. This section further characterizes $\mathcal{H}$ vectorial functions.

5.1 $\mathcal{H}$ functions

In this subsection, we recall some results of $\mathcal{H}$ functions, which will be used to characterize $\mathcal{H}$ vectorial functions.

In [22], a class of Boolean bent functions named as H functions was introduced, which is based on the *Desarguesian spread* [12, 46]. A set $E = \{E_1, E_2, \cdots, E_j\}$, which is a set of the k-dimensional subspaces of $\mathbb{F}_{2^n}$, is referred to as a *k-spread* of $\mathbb{F}_{2^n}$ if

$$E_{i_1} \bigcap_{i_1 \neq i_2,\ i_1, i_2 = 1, 2, \cdots, j} E_{i_2} = \{0\} \text{ and } \bigcup_{i=1}^{j} E_i = \mathbb{F}_{2^n}.$$

The Desarguesian k-spread of $\mathbb{F}_{2^n}$ is the set $\{(0, y), y \in \mathbb{F}_{2^k}\}$ and $\{(z, \nu z), z \in \mathbb{F}_{2^k}\}$, where $\nu \in \mathbb{F}_{2^k}$.

In [22], H functions are defined in the bivariate representation as $Tr_1^k(z + yG(zy^{2^k-2}))$, where $(y, z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and G is a permutation on $\mathbb{F}_{2^k}$ with $G(z) + z \neq 0$ and $G(z) + \nu z$ is two-to-one for all $\nu \in \mathbb{F}_{2^k}$. In [16], it was pointed out that the condition $G(z) + z \neq 0$, which makes H functions to be a subclass of $\mathcal{PS}$ functions [22], is not necessary for $Tr_1^k(z + yG(zy^{2^k-2}))$ to be bent. A development of H functions named as $\mathcal{H}$ functions was introduced in [16], whose bivariate representation [45] is $Tr_1^k(\nu z + yG(zy^{2^k-2}))$, with $(y, z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $\nu \in \mathbb{F}_{2^k}$ and G being an o-polynomial on $\mathbb{F}_{2^k}$. Note that all the known o-polynomials were listed in Table 1 of [45].

Definition 7 ([16])**.** *A permutation polynomial G on $\mathbb{F}_{2^k}$ is called an oval polynomial (o-polynomial), if the function*

$$z \in \mathbb{F}_{2^k} \mapsto \begin{cases} \frac{G(z+\gamma)+G(\gamma)}{z}, & if\ z \neq 0 \\ 0, & if\ z = 0 \end{cases}$$

is a permutation on $\mathbb{F}_{2^k}$ for all $\gamma \in \mathbb{F}_{2^k}$.

Since the Boolean function $Tr_1^k(\nu z)$ is linear and the bentness of $\mathcal{H}$ functions is our main concern, here, we describe $\mathcal{H}$ functions as follows.

$\mathcal{H}$ functions ([16, 45])**.** *The Boolean function*

$$Tr_1^k(yG(zy^{2^k-2}))$$

is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$, where $(y, z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Two o-polynomials G and G' are called *projectively equivalent* [6] if $G^\alpha = \frac{G(z)+G(0)}{G(1)+G(0)}$ and $G'^\alpha = \frac{G'(z)+G'(0)}{G'(1)+G'(0)}$ define equivalent hyperovals. In [16], five projectively equivalent o-polynomials of an o-polynomial G on $\mathbb{F}_{2^k}$ were given, i.e., $\mu G(z) + \nu$, $G(\mu z + \nu)$, $zG(z^{2^k-2})$, $(G(z^{2^s}))^{2^{k-s}}$ and $G^{-1}(z)$, where $\mu \in \mathbb{F}_{2^k}^*$, $\nu \in \mathbb{F}_{2^k}$, $s \in \mathbb{N}$ and G^{-1} denotes the compositional inverse of G. The $\mathcal{H}$ functions corresponding to G, $\mu G(z) + \nu$, $G(\mu z + \nu)$, $zG(z^{2^k-2})$ and $(G(z^{2^s}))^{2^{k-s}}$ are EA-equivalent [16, 45]. However, in general, $Tr_1^k(yG^{-1}(zy^{2^k-2}))$ is not EA-equivalent to the $\mathcal{H}$ functions corresponding to G, $\mu G(z) + \nu$, $G(\mu z + \nu)$, $zG(z^{2^k-2})$ and $(G(z^{2^s}))^{2^{k-s}}$ [16, 45].

For the composite functions of the above five projectively equivalent o-polynomials of an o-polynomial G, the projectively equivalence is preserved. The $\mathcal{H}$ functions educed by these composite functions may be EA-equivalent or EA-inequivalent. Therefore, the classification of these composite functions is interesting. In [6], by the transformations related to a group of order 24, the classification of some of these composite functions was studied.

The above five projectively equivalent o-polynomials of the o-polynomial G on $\mathbb{F}_{2^k}$ and some of their composite functions can be divided into four classes, which were discussed in [6, 16]. We let the four classes be denoted by

$$S_{G(z)}, S_{G^{-1}(z)}, S_{(zG(z^{2^k-2}))^{-1}} \text{ and } S_{(z+zG(y^{2^k-2}+1))^{-1}},$$

and summarize the classification as Table 6. Note that, in Table 6, except $(G(z^{2^s}))^{2^{k-s}}$, all the other projectively equivalent o-polynomials of G can be obtained by compounding $\mu G(z)+\nu$, $G(\mu z+\nu)$, $zG(z^{2^k-2})$ and $G^{-1}(z)$.

Table 6: The Known Classification of the Projectively Equivalent o-polynomials of the o-polynomial G on $\mathbb{F}_{2^k}$

(a) The o-polynomials in $S_{G(z)}$

Elements	Ref.
$G(z)$	–
$(G(z^{2^s}))^{2^{k-s}}$ [1]	[16]
$\mu G(z)+\nu$ [2]	[16]
$G(\mu z+\nu)$ [2]	[16]
$zG(z^{2^k-2})$	[6, 16]
$G(z+1)+1$	[6]
$z(G(z^{2^k-2}+1)+1)$	[6]
$z+(z+1)G(z(z+1)^{2^k-2})$	[6]
$(z+1)G((z+1)^{2^k-2})+1$	[6]

[1] $s \in \mathbb{N}$.
[2] $\mu \in \mathbb{F}_{2^k}^*$ and $\nu \in \mathbb{F}_{2^k}$.

(b) The o-polynomials in $S_{G^{-1}(z)}$

Elements	Ref.
$G^{-1}(z)$	[16]
$zG^{-1}(z^{2^k-2})$	[6]
$G^{-1}(z+1)+1$	[6]
$z(G^{-1}(z^{2^k-2}+1)+1)$	[6]
$z+(z+1)G^{-1}(z(z+1)^{2^k-2})$	[6]
$(z+1)G^{-1}((z+1)^{2^k-2})+1$	[6]

(c) The o-polynomials in $S_{(zG(z^{2^k-2}))^{-1}}$

Elements	Ref.
$(zG(z^{2^k-2}))^{-1}$	[6]
$(zG^{-1}(z^{2^k-2}))^{-1}$	[6]
$(z(z^{2^k-2}+(z^{2^k-2}+1)G((z+1)^{2^k-2}))^{-1})^{-1}$	[6]
$((z+1)G((z+1)^{2^k-2})+1)^{-1}$	[6]
$((z+1)G^{-1}((z+1)^{2^k-2})+1)^{-1}$	[6]
$(z(z^{2^k-2}+(z^{2^k-2}+1)G^{-1}((z+1)^{2^k-2}))^{-1})^{-1}$	[6]

(d) The o-polynomials in $S_{(z+zG(z^{2^k-2}+1))^{-1}}$

Elements	Ref.
$(z+zG(z^{2^k-2}+1))^{-1}$	[6]
$(z+zG^{-1}(z^{2^k-2}+1))^{-1}$	[6]
$(z+(z+1)G^{-1}(z(z+1)^{2^k-2}))^{-1}$	[6]
$z(z^{2^k-2}+(z^{2^k-2}+1)G^{-1}((z+1)^{2^k-2}))^{-1}$	[6]
$(z+(z+1)G(z(z+1)^{2^k-2}))^{-1}$	[6]
$z(z^{2^k-2}+(z^{2^k-2}+1)G((z+1)^{2^k-2}))^{-1}$	[6]

The $\mathcal{H}$ functions are EA-equivalent [6, 16] if the corresponding o-polynomials are in the same class S_i, where $i \in \{G(z),\ G^{-1}(z),\ (zG(z^{2^k-2}))^{-1}, (z+zG(z^{2^k-2}+1))^{-1}\}$. On the other hand, the o-polynomials in different S_i may induce EA-inequivalent $\mathcal{H}$ functions [6, 16].

For the convenience of discussion, we list the above fact as the following theorem.

Theorem 37 ([6, 16]). *Let G be an o-polynomial on $\mathbb{F}_{2^k}$,*

$$i_1, i_2 \in \{G(z), G^{-1}(z), (zG(z^{2^k-2}))^{-1}, (z+zG(z^{2^k-2}+1))^{-1}\},$$

$G_1 \in S_{i_1}$ and $G_2 \in S_{i_2}$. Then the two $\mathcal{H}$ functions $Tr_1^k(yG_1(zy^{2^k-2}))$ and $Tr_1^k(yG_2(zy^{2^k-2}))$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$,

(1) *are EA-equivalent if $i_1 = i_2$;*

(2) *may be EA-inequivalent if $i_1 \neq i_2$.*

5.2 Characterizing $\mathcal{H}$ vectorial functions

In order to characterize $\mathcal{H}$ vectorial functions, we give the following theorem that can be obtained by Theorem 2 directly.

Theorem 38. *Let $m \mid k$ and the Boolean function $Tr_1^k(yG(zy^{2^k-2}))$ be bent, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and G is a function on $\mathbb{F}_{2^k}$. Then the vectorial Boolean function $Tr_m^k(yG(zy^{2^k-2}))$ is bent if $Tr_1^k(\lambda yG(zy^{2^k-2}))$ is EA-equivalent to $Tr_1^k(yG(zy^{2^k-2}))$ for all $\lambda \in \mathbb{F}_{2^m}^*$.*

Note that, if G is an o-polynomial on $\mathbb{F}_{2^k}$, then $\mu G(z)+\nu \in S_{G(z)}$ (see Table 6 (a)), where $\mu \in \mathbb{F}_{2^k}^*$ and $\nu \in \mathbb{F}_{2^k}$. By Theorem 37, we have that the Boolean functions $Tr_1^k(yG(zy^{2^k-2}))$ and $Tr_1^k(\lambda yG(zy^{2^k-2}))$ are EA-equivalent for all $\lambda \in \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_{2^k}^*$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and G is an o-polynomial on $\mathbb{F}_{2^k}$. Thus, according to the definition of $\mathcal{H}$ functions and Theorem 38, the following theorem can be derived, which is the generalization of S. Mesnager's $\mathcal{H}$ vectorial functions, i.e., Theorem 1 in [45].

Theorem 39 (**$\mathcal{H}$ vectorial functions**)**.** *Let $m \mid k$. Then the vectorial Boolean function*

$$Tr_m^k(yG(zy^{2^k-2}))$$

is bent if and only if G is an o-polynomial on $\mathbb{F}_{2^k}$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Then we discuss the EA-equivalent relations among the $\mathcal{H}$ vectorial functions induced by the projectively equivalent o-polynomials.

Before the discussion, a theorem is presented as follows.

Theorem 40. *Let G, G' be two (k,m)-functions. Then $Tr_1^k(G)$ and $Tr_1^k(G')$ are EA-equivalent if and only if there exist some affine permutation A_2 on $\mathbb{F}_{2^k}$ and some affine (k,m)-function A_3 such that $G' = G \circ A_2 + A_3$.*

Proof. The sufficiency is obvious. In the following, we prove the necessity.

By Definition 5, $Tr_1^m(G)$ and $Tr_1^m(G')$ are EA-equivalent if and only if there exist some affine permutation A_2 on $\mathbb{F}_{2^k}$ and some affine Boolean function g on $\mathbb{F}_{2^k}$ such that $Tr_1^m(G'(z)) = Tr_1^m(G(A_2(z))) + g(z)$.

For the affine Boolean function g on $\mathbb{F}_{2^k}$, there exists some affine function $P(z) \in \mathbb{F}_{2^k}[z]$ such that $g(z) = Tr_1^k(P(z)) = Tr_1^m \circ Tr_m^k(P(z))$. Let $A_3(z) = Tr_m^k(P(z))$. Then A_3 is an affine (k,m)-function.

Thus, $Tr_1^m(G'(z)) = Tr_1^m(G(A_2(z)))+Tr_1^m(A_3(z))$, i.e., $Tr_1^m(G'(z)+G(A_2(z))+A_3(z)) \equiv 0$. Then $G'(z) = G(A_2(z)) + A_3(z)$.

Given the above, the conclusion holds. □

By Definition 5 and Theorem 40, the following corollary can be obtained.

Corollary 7. *Let G and G' be two (k,m)-functions. If $Tr_1^m(G)$ and $Tr_1^m(G')$ are EA-equivalent, then G and G' are EA-equivalent.*

By Theorem 37, Theorem 39 and Corollary 7, we have the following theorem.

Theorem 41. *Let $m \mid k$, G be an o-polynomial on $\mathbb{F}_{2^k}$,*

$$i_1, i_2 \in \{G(z), G^{-1}(z), (zG(z^{2^k-2}))^{-1}, (z + zG(z^{2^k-2}+1))^{-1}\},$$

$G_1 \in S_{i_1}$ and $G_2 \in S_{i_2}$. Then the two $\mathcal{H}$ vectorial functions $Tr_m^k(yG_1(zy^{2^k-2}))$ and $Tr_m^k(yG_2(zy^{2^k-2}))$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$,

(1) *are EA-equivalent if $i_1 = i_2$;*

(2) *may be EA-inequivalent if $i_1 \neq i_2$.*

Remark 12. *Theorem 41 includes Proposition 2 in [45] as special cases.*

The restrictions of $\mathcal{H}$ functions to all the elements of the Desarguesian spread are linear [16], which indicates that the restrictions of $\mathcal{H}$ functions to the vector space $\omega\mathbb{F}_{2^k}$ are linear for all $\omega \in \mathbb{F}_{2^n}^*$. According to this fact, it was shown in [16] that, when viewed in the univariate representation, $\mathcal{H}$ functions are the Niho Boolean bent functions. Then whether $\mathcal{H}$ vectorial functions viewed in the univariate representation are the Niho vectorial Boolean bent functions or not is also interesting.

By the similar method to the proof of Lemma 4 in [16], the following lemma can be obtained.

Lemma 8. *Let $F(x) = \sum_{i=0}^{2^n-1} a_i x^i$ be a vectorial Boolean function on $\mathbb{F}_{2^n}$, where $a_i \in \mathbb{F}_{2^n}$ for $i = 1, 2, \cdots, j$. The restriction of F to the vector space $\omega\mathbb{F}_{2^k}$ is linear for all $\omega \in \mathbb{F}_{2^n}^*$ if and only if $i \equiv 2^s (\mathrm{mod}\ 2^k - 1)$ for all $a_i \neq 0$ and $i = 1, 2, \cdots, 2^n - 1$, where s is some nonnegative integer and $s < n$.*

It is obvious that the restrictions of $\mathcal{H}$ vectorial functions to all the elements of the Desarguesian spread are linear. Similarly to $\mathcal{H}$ functions, we know that the restrictions of $\mathcal{H}$ vectorial functions to the vector space $\omega\mathbb{F}_{2^k}$ are linear for all $\omega \in \mathbb{F}_{2^n}^*$. By the definition of the Niho bent functions and Lemma 8, we have the following conclusion.

Theorem 42. *$\mathcal{H}$ vectorial functions viewed in univariate representation are Niho vectorial Boolean bent functions.*

6 $\mathcal{H}$-like vectorial functions

In this section, we present a new infinite class of vectorial Boolean bent functions and call it as $\mathcal{H}$-like vectorial functions, which includes $\mathcal{H}$ vectorial functions as a subclass. $\mathcal{H}$-like vectorial functions drive from $\mathcal{H}$-like functions that is a generalization of $\mathcal{H}$ functions.

$\mathcal{H}$ functions is associated to the Desarguesian spread, while many other k-spreads of $\mathbb{F}_{2^n}$ exist [12, 21, 30]. In [12], C. Carlet generalized $\mathcal{H}$ functions into a new class of Boolean bent functions named $\mathcal{H}$-like functions by using several other classes of k-spreads, especially, André's spread. André's k-spread is the set $\{(0,y), y \in \mathbb{F}_{2^k}\}$ and $\{(z, \nu z^{2^{k\Phi(\nu)}}), z \in \mathbb{F}_{2^k}\}$, where $\nu \in \mathbb{F}_{2^k}$, $l \mid k$, $\Phi = \phi \circ N_l^k$ and ϕ is any function from $\mathbb{F}_{2^l}$ to $\mathbb{Z}_{\frac{k}{l}}$. In other word, Φ can be any function from $\mathbb{F}_{2^k}$ to $\mathbb{Z}_{\frac{k}{l}}$ such that it is constant on every multiplicative coset of the subgroup of order $\frac{2^k-1}{2^l-1}$ of $\mathbb{F}_{2^k}^*$ [12].

For the $\mathcal{H}$-like functions related to André's spreads, φ-polynomial plays a basic role.

Definition 8 ([12]). *Let $l \in \mathbb{N}^*$, $l \mid k$, Φ be a function from $\mathbb{F}_{2^k}$ to $\mathbb{Z}_{\frac{k}{l}}$ and constant on every multiplicative coset of the subgroup of order $\frac{2^k-1}{2^l-1}$ of $\mathbb{F}_{2^k}^*$. A permutation polynomial V on $\mathbb{F}_{2^k}$ is called a φ-polynomial if for every $b_1 \in \mathbb{F}_{2^k}^*$ and every $b_2 \in \mathbb{F}_{2^k}$, there exist two solutions or none of the equation*

$$V(z) + (b_1 z)^{2^{k-l\Phi(z)}} = b_2.$$

The $\mathcal{H}$-like functions related to André's k-spread are as follows.

Theorem 43 ([12]). *Let $l \in \mathbb{N}^*$, $l \mid k$, Φ be a function from $\mathbb{F}_{2^k}$ to $\mathbb{Z}_{\frac{k}{l}}$ and constant on every multiplicative coset of the subgroup of order $\frac{2^k-1}{2^l-1}$ of $\mathbb{F}_{2^k}^*$. The Boolean function*

$$Tr_1^k(yV(zy^{2^k-2^{l\Phi(zy^{2^k-2})}})),$$

is bent if and only if V is a φ-polynomial corresponding to Φ, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

In the following theorem, we show that, if an integer-valued function Φ on $\mathbb{F}_{2^k}$ is a constant in $\mathbb{Z}_{\frac{k}{l}}$, then multiplying the corresponding φ-polynomial by any element of $\mathbb{F}_{2^k}^*$ is still a φ-polynomial.

Theorem 44. *Let $l \in \mathbb{N}^*$, $l \mid k$, $c \in \mathbb{Z}_{\frac{k}{l}}$, $\Phi \equiv c$ be a constant function on $\mathbb{F}_{2^k}$ and V be the corresponding φ-polynomial. Then μV is a φ-polynomial corresponding to $\Phi \equiv c$ for all $\mu \in \mathbb{F}_{2^k}^*$.*

Proof. For $\forall\ \mu, b_1 \in \mathbb{F}_{2^k}^*$ and $\forall\ b_2 \in \mathbb{F}_{2^k}$, we have

$$\begin{aligned} & V(z) + (b_1 z)^{2^{k-lc}} = b_2 \\ \Leftrightarrow\ & \mu V(z) + \mu(b_1 z)^{2^{k-lc}} = b_2\mu \\ \Leftrightarrow\ & \mu V(z) + (\mu^{2^{lc}} b_1 z)^{2^{k-lc}} = b_2\mu \end{aligned}$$

Let $b_1' = \mu^{2^{lc}} b_1$ and $b_2' = b_2\mu$. Because V is a φ-polynomial corresponding to $\Phi \equiv c$, we know that $\mu V(z) + (b_1' z)^{2^{k-lc}} = b_2'$ has two solutions or none. For every $\mu \in \mathbb{F}_{2^k}^*$, by $\gcd(2^{lc}, 2^k - 1) = 1$ and the arbitrariness of b_1 and b_2, we have that b_1' and b_2' can traverse $\mathbb{F}_{2^k}^*$ and $\mathbb{F}_{2^k}$ respectively. By Definition 8, μV is a φ-polynomial corresponding to $\Phi \equiv c$. □

By Theorem 43 and Theorem 44, we have that $Tr_m^k(y\lambda V(zy^{2^k-2^{lc}}))$ belongs to $\mathcal{H}$-like functions for all $\lambda \in \mathbb{F}_{2^m}^* \subseteq \mathbb{F}_{2^k}^*$ if V is a φ-polynomial on $\mathbb{F}_{2^k}$ corresponding to $\Phi \equiv c$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and $c \in \mathbb{Z}_{\frac{k}{l}}$. Thus, according to Theorem 3, we obtain a new infinite class of vectorial Boolean bent functions, and call it as $\mathcal{H}$-like vectorial functions.

Theorem 45 (**$\mathcal{H}$-like vectorial functions**). *Let $l \in \mathbb{N}^*$, $l \mid k$, $m \mid k$, $c \in \mathbb{Z}_{\frac{k}{l}}$ and $\Phi \equiv c$ be a constant function on $\mathbb{F}_{2^k}$. Then the vectorial Boolean function*

$$Tr_m^k(yV(zy^{2^k-2^{lc}}))$$

is bent if and only if V is a φ-polynomial corresponding to $\Phi \equiv c$, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$.

Remark 13. *Note that o-polynomials belong to φ-polynomials [12], and are equivalent to 0-polynomials, i.e., the φ-polynomials corresponding to $\Phi(z) \equiv 0$. Therefore, we have that $\mathcal{H}$ vectorial functions form a subclass of $\mathcal{H}$-like vectorial functions.*

7 Conclusions

In this paper, we studied new primary constructions of vectorial Boolean bent functions about four types, i.e., vectorial monomial bent functions, vectorial Boolean bent functions with multiple trace terms, $\mathcal{H}$ vectorial functions and $\mathcal{H}$-like vectorial functions.

We give answers to one open problem (see Open Problem 1) proposed by E. Pasalic et al. in [55]. More precisely, when $Tr_1^n(ax^d)$ is a monomial bent function, several conditions which are much closer to the sufficient and necessary conditions for $Tr_m^n(ax^d)$ to be bent than the condition that $\gcd(d, 2^m-1)=1$ are given. We also characterize the vectorial monomial bent functions corresponding to the five known classes of bent exponents, and list the results in Table 2, Table 3 and Table 4.

We provide answers to one open problem (see Open Problem 4) proposed by A. Muratović-Ribić in [48]. That is, several similar results to Theorem 1 in [48] with $\gcd(d_1, 2^m-1) \neq 1$ are presented. We also obtain six infinite classes of the vectorial Boolean bent functions with multiple trace terms, and list them in Table 5. Besides, the nonexistence of the bent (n,k)-functions of the form $\sum_{i=1}^{2^k-2} Tr_k^n(ax^{(2i-1)(2^k-1)})$ is proved, where $a \in \mathbb{F}_{2^k}^*$.

$\mathcal{H}$ vectorial functions, which are the vectorial Boolean bent functions of the form $Tr_m^k(yG(zy^{2^k-2})$ with $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and G being an o-polynomial on $\mathbb{F}_{2^k}$, are further characterized.

The vectorial Boolean bent functions of the form $Tr_m^k(yV(zy^{2^k-2^{lc}}))$ are derived, where $(y,z) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $l \mid k$, $c \in \mathbb{Z}_{\frac{k}{l}}$ and V is a φ-polynomial on $\mathbb{F}_{2^k}$ corresponding to $\Phi \equiv c$, and named as $\mathcal{H}$-like vectorial functions. Furthermore, $\mathcal{H}$-like vectorial functions includes $\mathcal{H}$ vectorial functions as a subclass.

References

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

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

[3] L. Budaghyan. *Construction and Analysis of Cryptographic Functions.* Springer, 2015.

[4] L. Budaghyan and C. Carlet. CCZ-equivalence of single and multi-output boolean functions. In *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq*, volume 9, pages 43–54, 2010.

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

[6] L. Budaghyan, C. Carlet, T. Helleseth, and A. Kholosha. On o-equivalence of Niho bent functions. In *Arithmetic of Finite Fields*, pages 155–168. Springer, 2014.

[7] L. Budaghyan, C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager. Further results on Niho bent functions. *IEEE Transactions on Information Theory*, 58(11):6979–6985, 2012.

[8] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.

[9] L. Budaghyan, A. Kholosha, C. Carlet, and T. Helleseth. Niho bent functions from quadratic o-monomials. In *Information Theory (ISIT), 2014 IEEE International Symposium on*, pages 1827–1831. IEEE, 2014.

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

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

[12] C. Carlet. More $\mathcal{PS}$ and $\mathcal{H}$-like bent functions. Cryptology ePrint Archive, Report 2015/168, 2015.

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

[14] C. Carlet, T. Helleseth, A. Kholosha, and S. Mesnager. On the dual of bent functions with 2^r Niho exponents. 2011 IEEE International Symposium on Information Theory Proceedings (ISIT), 2011.

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

[16] C. Carlet and S. 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.

[17] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In *Advances in CryptologyEUROCRYPT'94*, pages 356–365. Springer, 1995.

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

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

[20] P. Charpin, E. Pasalic, and C. Tavernier. On bent and semi-bent quadratic boolean functions. *IEEE Transactions on Information Theory*, 51(12):4286–4298, 2005.

[21] P. Dembowski. *Finite geometries*, volume 44. Springer Science & Business Media, 1968.

[22] J. F. Dillon. *Elementary Hadamard difference sets.* PhD thesis, University of Maryland, College Park., 1974.

[23] J. F. Dillon and H. Dobbertin. New cyclic difference sets with singer parameters. *Finite Fields and Their Applications*, 10(3):342–389, 2004.

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

[25] H. Dobbertin, G. Leander, A. Canteaut, C. Carlet, P. Felke, and P. Gaborit. Construction of bent functions via Niho power functions. *Journal of Combinatorial Theory, Series A*, 113(5):779–798, 2006.

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

[27] M. Hermelin, J. Y. Cho, and K. Nyberg. Statistical tests for key recovery using multidimensional extension of Matsuis algorithm 1. In *EUROCRYPT*, 2009.

[28] H. D. Hollmann and Q. Xiang. On binary cyclic codes with few weights. In *Finite Fields and Applications*, pages 251–275. Springer, 2001.

[29] H. Hu and D. Feng. On quadratic bent functions in polynomial forms. *IEEE transactions on information theory*, 53(7):2610–2615, 2007.

[30] N. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes.* CRC Press, 2007.

[31] K. Khoo, G. Gong, and D. R. Stinson. A new characterization of semi-bent and bent functions on finite fields*. *Designs, Codes and Cryptography*, 38(2):279–295, 2006.

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

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

[34] N. G. Leander. Monomial bent functions. *IEEE transactions on information theory*, 52(2):738–743, 2006.

[35] N. Li, T. Helleseth, A. Kholosha, and X. Tang. On the Walsh transform of a class of functions from Niho exponents. *IEEE transactions on information theory*, 59(7):4662–4667, 2013.

[36] N. Li, T. Helleseth, X. Tang, and A. Kholosha. Several new classes of bent functions from Dillon exponents. *IEEE Transactions on Information Theory*, 59(3):1818–1831, 2013.

[37] N. Li, X. Tang, and T. Helleseth. New constructions of quadratic bent functions in polynomial form. *IEEE Transactions on Information Theory*, 60(9):5760–5767, 2014.

[38] Y. Lou, H. Han, C. Tang, Z. Wu, and M. Xu. Constructing vectorial boolean functions with high algebraic immunity based on group decomposition. *International Journal of Computer Mathematics*, (ahead-of-print):1–12, 2014.

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

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

[41] S. 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.

[42] S. Mesnager. Hyper-bent Boolean functions with multiple trace terms. In *Arithmetic of Finite Fields*, pages 97–113. Springer, 2010.

[43] S. 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.

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

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

[46] S. Mesnager. Bent functions from spreads. *Contemporary Mathematics*, 632:295–316, 2015.

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

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

[49] A. Muratović-Ribić, E. Pasalic, and S. Bajric. Vectorial hyperbent trace functions from the $\mathcal{PS}_{ap}$ class-their exaxt number and specification. *IEEE transactions on information theory*, 60(7):4408–4413, 2014.

[50] Y. Niho. Multi-valued cross-correlation functions between two maximal linear recursive sequences. Technical report, DTIC Document, 1972.

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

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

[53] K. Nyberg. Differentially uniform mappings for cryptography. In *Advances in cryptologyEurocrypt93*, pages 55–64. Springer, 1994.

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

[55] E. Pasalic and W.-G. Zhang. On multiple output bent functions. *Information Processing Letters*, 112(21):811–815, 2012.

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

[57] T. Satoh, T. Iwata, and K. Kurosawa. On cryptographically secure vectorial Boolean functions. In *Advances in Cryptology-ASIACRYPT99*, pages 20–28. Springer, 1999.

[58] C. Tang, Y. Qi, and M. Xu. Multiple output bent functions characterized by families of bent functions. *Journal of Cryptologic Research*, 1(4):321–326, 2014.

[59] C. Tang, Y. Qi, M. Xu, B. Wang, and Y. Yang. A new class of hyper-bent boolean functions in binomial forms. *arXiv preprint arXiv:1112.0062*, 2011.

[60] M. WenPing, L. MoonHo, and F. Zhang. A new class of bent functions. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 88(7):2039–2040, 2005.

[61] A. M. Youssef and G. Gong. Hyper-bent functions. In *EUROCRYPT 2001*, page 406.

[62] N. Y. Yu and G. Gong. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7):3291–3299, 2006.