Designs, Codes and Cryptography (2021) 89:2697–2714
https://doi.org/10.1007/s10623-021-00943-y

Three classes of balanced vectorial semi-bent functions

WeiGuo Zhang[1,2] · **YuJuan Sun**[1,2] · **Enes Pasalic**[3]

Received: 3 January 2021 / Revised: 25 August 2021 / Accepted: 27 August 2021 /
Published online: 7 October 2021

Abstract
Semi-bent functions play an important role in symmetric ciphers and sequence designs. So far, there are few studies related to the construction of vectorial semi-bent functions even though lots of work has been done on single-output semi-bent functions. In this paper, three classes of balanced vectorial semi-bent functions are presented with varying cryptographic properties. The classes denoted $\mathcal{DC}$ and $\mathcal{DS}$ are constructed using disjoint codes and disjoint spectra functions, respectively. The former class has a useful provable property that its component functions do not admit linear structures. It is shown that the number of output bits of the constructed n-variable $\mathcal{DC}$ and $\mathcal{DS}$ vectorial functions can respectively reach $(n+1)/2$ and $n/3$. In addition, a construction method of semi-bent functions from $\mathbb{F}_2^{3n} \to \mathbb{F}_2^n$ by using almost bent (AB) functions on $\mathbb{F}_2^n$ is given.

Keywords Boolean functions · Disjoint codes · Disjoint spectra functions · Vectorial semi-bent functions · Fiestel ciphers

Mathematics Subject Classification 06E30 · 94A60

1 Introduction

Bent functions are one of the most interesting combinatorial objects since they achieve maximum nonlinearity [24,47]. Since the eighties, they have been extensively studied not

Communicated by C. Carlet.

✉ WeiGuo Zhang
zwg@xidian.edu.cn

YuJuan Sun
yjsun@xidian.edu.cn

Enes Pasalic
enes.pasalic6@gmail.com

1 State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China

2 State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China

3 University of Primorska, FAMNIT & IAM, Koper, Slovenia

only for their interesting algebraic properties, but also for their multiple applications in cryptography, combinational design, and coding theory, see [1,2,5,8,14,27,33,45] and the references therein. However, bent functions are not balanced and exist only when the number of variables is even, which makes them somewhat less applicable in the design of symmetric encryption schemes.

Semi-bent functions were introduced in 1994 by Chee et al. [19]. These functions f: $\mathbb{F}_2^n \to \mathbb{F}_2$ are characterized by the property that their Walsh spectrum values belong to the set $\{0, \pm 2^{\lfloor n/2 \rfloor + 1}\}$. Due to their almost optimal nonlinearity, semi-bent functions can resist linear approximation attacks [25,36] and fast correlation attacks [37] (assuming they possess a suitable resiliency order) when used in symmetric ciphers. Furthermore, semi-bent functions can be used to construct orthogonal variable spreading factor codes which are suitable for applications in synchronous CDMA communication systems [31,48,49].

The theory of semi-bent Boolean functions has been intensively studied in the literature. Even before the notion of semi-bent functions was formally introduced by Chee et al. [19], these objects had already been studied in 1960s by Gold [26] in sequence designs. In this direction, from the sequence design point of view, the main contributions are due to Niho [43], Helleseth [28,29], Boztaş and Kumar [3], Cusick and Dobbertin [21], Kumar and Helleseth [30], Canteaut et al. [6], Khoo et al. [34], etc. In 1992, Carlet [15] introduced and characterized a class of functions called partially-bent functions, which can be semi-bent and balanced. However, all partially bent functions that are semi-bent have 1 or 3 nonzero linear structures, which is regarded as a drawback from the cryptographic standpoint. Noticing that all quadratic Boolean functions are bent or partially bent, semi-bent quadratic Boolean functions are always partially bent. The quadratic case of semi-bent functions has been addressed in [18,35]. Furthermore, the most important contributions on theory and design of semi-bent functions can be found in [4,7,13,16,20,22,23,38–41,46,52–55].

It is worth noticing that all the above results are about single-output semi-bent functions. The notion of vectorial semi-bent functions is a natural generalization of single-output semi-bent functions. Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, with $1 < m \leq n$, be an (n, m) vectorial function defined by $F(x) = \big(f_1(x), \ldots, f_m(x)\big)$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ are Boolean mappings for $i = 1, \ldots, m$. The algebraic degree of F is defined as the maximum among the algebraic degrees of all non-zero linear combinations of the coordinate functions f_i of F. We call $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ a *vectorial semi-bent function* if all non-zero linear combinations of $f_1, \ldots, f_m$ are semi-bent functions. Furthermore, F is said to be balanced if

$$\big|\{x \in \mathbb{F}_2^n \mid F(x) = y\}\big| = 2^{n-m}$$

for any $y \in \mathbb{F}_2^m$, where $|S|$ is the cardinality of any set S.

However, to the best of our knowledge, there are few results related to the construction of vectorial semi-bent functions.

- Almost bent (AB) functions, $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, constitute the well-known class of vectorial semi-bent functions which exists only for odd n [17]. There are several generic classes of AB functions, mostly stemming from suitable power polynomials $F(x) = x^d$ over the finite field $\mathbb{F}_{2^n}$ (n is odd) for a suitably chosen exponent d, see e.g. [9,10,44].
- When $m < n$, more precisely, $m \leq \lfloor n/2 \rfloor + 1$, the other class of vectorial semi-bent functions can be obtained by the Maiorana-McFarland ($\mathcal{MM}$) construction technique. Johansson and Pasalic [32] constructed the $\mathcal{MM}$ class of balanced correlation immune plateaued functions, which can be vectorial semi-bent functions under certain conditions. Zhang et al. [49] showed that $(n, \lfloor n/2 \rfloor + 1)$ vectorial semi-bent functions (stemming

from the $\mathcal{MM}$ class) can be used to construct the orthogonal sequence sets suitable for applications in CDMA systems.

The main motivation of this work is to provide a greater variety of construction methods of vectorial semi-bent functions which do not necessarily stem from the $\mathcal{MM}$ class. In the first place, such functions can be used in Feistel-like block ciphers for specifying substitution boxes (S-boxes) as highly nonlinear mappings from $\mathbb{F}_2^n \to \mathbb{F}_2^m$ [42] (notice that S-boxes of Data Encryption Standard (DES) employ different mappings from $\mathbb{F}_2^6$ to $\mathbb{F}_2^4$, though none of the component functions used in S-boxes of DES is semi-bent), satisfying also other cryptographic criteria such as low differential uniformity and high algebraic degree. This approach has been recently employed in the design of certain block ciphers, which are more flexible with respect to the choice of input/output space dimensions n and m.

In this paper, we present three classes of balanced vectorial semi-bent functions, for odd n, with varying output space and algebraic degree. More precisely, using a suitable set of mutually disjoint codes (intersecting only at the all-zero vector), we specify the class $\mathcal{DC}$ of vectorial semi-bent functions (see Construction 1). Compared to the method of Johansson and Pasalic [32], which employs the concatenation of suitable linear functions on a small variable space (therefore apparently generating functions in $\mathcal{MM}$), our design employs a set of disjoint codes in a different manner. Namely, our construction technique implies that the component functions (non-zero linear combinations of the coordinate functions) are constant on these k-dimensional subspaces (deprived of the all-zero vector) corresponding to these disjoint codes. Therefore, our method rather resembles the partial spread construction of bent functions introduced by Dillon [24]. Thereafter, by employing disjoint spectra functions (see Definition 1), we propose the second class (named $\mathcal{DS}$) of vectorial semi-bent functions, see Construction 2. In this case, the component functions can be viewed as a concatenation of suitable disjoint spectra functions which in difference to the method in [32] are not linear. These methods are generic and can provide vectorial semi-bent functions of maximal algebraic degree. Furthermore, the members of class $\mathcal{DC}$ provably do not possess linear structures whereas there is no guarantee that vectorial semi-bent functions derived from the $\mathcal{MM}$ class (such as those proposed in [32]) share the same feature.

In Sect. 4, other cryptographic properties of the two classes are investigated. It is shown that these functions can achieve the maximum algebraic degree and posses quite good differential properties. An important problem of extending the output space of the proposed (n, m) semi-bent functions, thus building $(n, m + k)$ semi-bent functions for $1 \leq k \leq n - m$, is left open.

Finally, a third method of using the so-called block functions of known AB functions is presented. This method employs a decomposition of the ambient space $\mathbb{F}_2^n$ as $\mathbb{F}_2^{n/3} \times \mathbb{F}_2^{n/3} \times \mathbb{F}_2^{n/3}$, for odd n divisible by 3. In this setup, any AB function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ can be viewed as $F = (F_1, F_2, F_3)$, where $F_i : \mathbb{F}_2^n \to \mathbb{F}_2^{n/3}$ and each F_i is necessarily a vectorial semi-bent function. We propose an efficient way of using the known AB permutations $F_1 : \mathbb{F}_2^{n/3} \to \mathbb{F}_2^{n/3}$ to define vectorial semi-bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^{n/3}$, which have different algebraic degree compared to F_1, see Proposition 2. For instance, using a Gold-like AB permutation $F_1(x) = x^{2^k+1}$ on $\mathbb{F}_{2^{n/3}}$, with $\gcd(k, n/3) = 1$, one can define $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{n/3}}$ as $F(x, y, z) = xy^{2^k+1} + yz^{2^k+1}$ which is shown to be vectorial semi-bent. This approach actually leaves an important open problem of specifying suitable block functions $F_1, F_2, F_3 : \mathbb{F}_2^n \to \mathbb{F}_2^{n/3}$ so that $F = (F_1, F_2, F_3)$ is an AB function, where each F_i is a vectorial semi-bent function. More precisely, given the possibility of specifying a vectorial semi-bent function F_1 as in Proposition 2, the question (which is intrinsically hard) of defining (using

for instance suitable modifications of F_1, F_2 and F_3 (thus extendability on a block level) so that $F = (F_1, F_2, F_3)$ is an AB function, is of great significance.

The rest of the paper is organized as follows. Section 2 provides the necessary notations and definitions related to vectorial semi-bent functions. Two constructions of balanced vectorial semi-bent functions are given in Sect. 3. In Sect. 5, we present an efficient technique of specifying vectorial semi-bent functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n/3}$, for odd n divisible by 3, based on the use of known AB functions on $\mathbb{F}_2^{n/3}$. Some concluding remarks are given in Sect. 6.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the cartesian product of n copies of $\mathbb{F}_2$, the prime field of characteristic 2. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is said to be a Boolean function in n variables. The set of all n-variable Boolean functions is denoted by $\mathcal{B}_n$. For any $x \in \mathbb{F}_2^n$, we write $x = (x_1, \ldots, x_n)$ where $x_i \in \mathbb{F}_2$. Any Boolean function $f \in \mathcal{B}_n$ has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called algebraic normal form (ANF),

$$f(x) = \sum_{I \subseteq \{1,\cdots,n\}} \lambda_I \prod_{i \in I} x_i, \quad \lambda_I \in \mathbb{F}_2.$$

The algebraic degree of f is the maximal value of $|I|$ such that $\lambda_I = 1$. The truth table of a Boolean function $f \in \mathcal{B}_n$ is a (0, 1)-sequence defined by

$$\overline{f} = \big(f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), \cdots, f(1, \ldots, 1, 1)\big).$$

The support of f is defined as $supp(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$. f is said to be balanced if $|supp(f)| = 2^{n-1}$ which is equivalent to the condition $W_f(\mathbf{0}_n) = 0$, where $\mathbf{0}_n$ denotes the zero vector of $\mathbb{F}_2^n$. Any linear function on $\mathbb{F}_2^n$ is denoted by $\alpha \cdot x = \alpha_1 x_1 + \cdots + \alpha_n x_n$, where $\alpha = (\alpha_1, \ldots, \alpha_n)$, $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$. The Walsh transform of $f \in \mathcal{B}_n$ at the point α is an integer valued function over $\mathbb{F}_2^n$ defined by

$$W_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+\alpha \cdot x}.$$

The Walsh spectrum of $f \in \mathcal{B}_n$, as a multi-set of values $W_f(\alpha)$ when $\alpha \in \mathbb{F}_2^n$, is given as

$$\widetilde{W}_f = \big(W_f(0, \ldots, 0, 0), W_f(0, \ldots, 0, 1), \ldots, W_f(1, \ldots, 1, 1)\big).$$

The Walsh support of $f \in \mathcal{B}_n$ is defined as $S_f = \{\omega \in \mathbb{F}_2^n \mid W_f(\omega) \neq 0\}$.

Definition 1 [51] A set of Boolean functions $\{f_1, f_2, \ldots, f_N\} \subset \mathcal{B}_n$ such that for any $\alpha \in \mathbb{F}_2^n$,

$$W_{f_i}(\alpha) \cdot W_{f_j}(\alpha) = 0, \quad 1 \leq i < j \leq N$$

is called a set of disjoint spectra functions of cardinality N.

Lemma 1 *An (n, m) vectorial Boolean function $F = (f_1, \ldots, f_m)$ is balanced if and only if all nonzero linear combinations of $f_1, \ldots, f_m$ are balanced functions, i.e. $W_{c \cdot F}(\mathbf{0}_n) = 0$ for any $c \in \mathbb{F}_2^{m*}$, where $\mathbb{F}_2^{m*} = \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$.*

The notion of semi-bent functions was introduced by Chee et al. [19], and it can be naturally extended to vectorial Boolean functions.

Definition 2 The function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called an (n, m) vectorial semi-bent function if $W_{c\cdot F}(\alpha) \in \{0, \pm 2^{\lfloor n/2 \rfloor + 1}\}$ for any $c \in \mathbb{F}_2^{m*}$ and $\alpha \in \mathbb{F}_2^n$. An (n, n) vectorial semi-bent function is called an almost bent (AB) function.

Definition 3 The autocorrelation function of a Boolean function $f \in \mathcal{B}_n$ at the point $\alpha \in \mathbb{F}_2^n$ is defined by

$$C_f(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+f(x+\alpha)}. \tag{1}$$

$\alpha \in \mathbb{F}_2^n$ is called a linear structure of f if $|C_f(\alpha)| = 2^n$.

3 $\mathcal{DC}$ and $\mathcal{DS}$ class vectorial semi-bent functions

In this section, we present two constructions of balanced (n, m) vectorial semi-bent functions based on, respectively, a set of disjoint codes and a set of disjoint spectra functions. It is shown that the number of output bits m of the functions obtained in Construction 1 and Construction 2 can respectively reach $(n + 1)/2$ and $n/3$. Before we describe the two constructions, we first introduce a construction method of a large set of disjoint codes.

Definition 4 A k-dimensional subspace C of $\mathbb{F}_2^n$ is called an $[n, k]$ linear code. The dual code of C is defined as $C^\perp = \{\alpha \in \mathbb{F}_2^n \mid \alpha \cdot x = 0, \text{ for any } x \in C\}$.

Definition 5 [32] A set of $[n, k]$ linear codes $\{C_1, C_2, \ldots, C_N\}$ such that

$$C_i \cap C_j = \{\mathbf{0}_n\}, \quad 1 \le i < j \le N$$

is called a set of (n, k) disjoint codes of cardinality N.

In what follows, a construction method of a set of (n, k) disjoint codes with cardinality 2^s is described, where $2 \le k \le n/2$.

Proposition 1 [50] *Let $n = s + k$ with $s \ge k \ge 2$. Let γ be a primitive element in $\mathbb{F}_{2^s}$, and $\{\gamma, \gamma^2, \ldots, \gamma^s\}$ be a basis of $\mathbb{F}_{2^s}$. Define a bijection $\pi : \mathbb{F}_{2^s} \mapsto \mathbb{F}_2^s$ by*

$$\pi(c_1\gamma + c_2\gamma^2 + \cdots + c_s\gamma^s) = (c_1, c_2, \ldots, c_s). \tag{2}$$

For $z \in \mathbb{F}_2^s$, let $G_z = (I_k, M_z)$ be the generator matrix of an (n, k) linear code C_z, where M_z is a zero matrix of size $k \times (n - k)$ if $z = \mathbf{0}_s$, or otherwise

$$M_z = \begin{pmatrix} \pi(\gamma^{[z]}) \\ \pi(\gamma^{[z]+1}) \\ \vdots \\ \pi(\gamma^{[z]+k-1}) \end{pmatrix}_{k \times s},$$

where $[z]$ denotes the integer representation of z. Then, $\{C_z \mid z \in \mathbb{F}_2^s\}$ is a set of (n, k) disjoint codes of cardinality 2^s.

Let E be an $[n, s]$ (canonical) linear code defined by

$$E = \{\mathbf{0}_k\} \times \mathbb{F}_2^s.$$

For the disjoint codes C_z in Proposition 1, one can easily verify that

$$E \cap C_z = \{\mathbf{0}_n\}, \text{ for } z \in \mathbb{F}_2^s. \tag{3}$$

Noticing $|E| + \sum_{z\in\mathbb{F}_2^s} |C_z^*| = 2^n$, where $C_z^* = C_z \setminus \{\mathbf{0}_n\}$, we then have

$$\Big(\bigcup_{z\in\mathbb{F}_2^s} C_z^*\Big) \cup E = \mathbb{F}_2^n. \tag{4}$$

$\mathbb{F}_2^n$ is now divided up into $2^s + 1$ disjoint sets: E, C_z^*, $z \in \mathbb{F}_2^s$. We remark that the specific $[n, s]$ linear code E will also play a role in Construction 1.

Example 1 Let $n = 5$ and $k = 2$. Let γ be a root of the prime polynomial $z^3 + z + 1$. By (2), we have $\pi(\gamma) = (100)$, $\pi(\gamma^2) = (010)$, $\pi(\gamma^3) = (001)$, $\pi(\gamma^4) = (110)$, $\pi(\gamma^5) = (011)$, $\pi(\gamma^6) = (111)$, $\pi(\gamma^7) = \pi(1) = (101)$. We have

$C_{000} = \{00000, 10000, 01000, 11000\}$, $C_{001} = \{00000, 10100, 01010, 11110\}$,
$C_{010} = \{00000, 10010, 01001, 11011\}$, $C_{011} = \{00000, 10001, 01110, 11111\}$,
$C_{100} = \{00000, 10110, 01011, 11101\}$, $C_{101} = \{00000, 10011, 01111, 11100\}$,
$C_{110} = \{00000, 10111, 01101, 11010\}$, $C_{111} = \{00000, 10101, 01100, 11001\}$,
and $E = \{00000, 00100, 00010, 00001, 00110, 00101, 00011, 00111\}$.

Then $\{C_z \mid z \in \mathbb{F}_2^3\}$ is a set of $(5, 2)$ disjoint codes. Moreover, (3) and (4) hold, that is $\{E, C_{000}^*, \ldots, C_{111}^*\}$ partitions $\mathbb{F}_2^5$.

Remark 1 Notice that when $k = s = n/2$ this method essentially provides a (well-known approach of designing) full spread of $\mathbb{F}_2^n$, for even n, as a collection of disjoint $(n/2)$-dimensional subspaces of $\mathbb{F}_2^n$ of cardinality $2^{n/2+1}$.

Let $s = k+1$ in Proposition 1, which consequently gives 2^{k+1} many (n, k) disjoint codes $C_z, z \in \mathbb{F}_2^{k+1}$. Note that $C_z^\perp$ and $C_{z'}^\perp$ are two $[n, k+1]$ linear codes. Now, suppose that $C_z^\perp$ and $C_{z'}^\perp$ can be generated by the bases $\{e_1, e_2, \ldots, e_{k+1}\}$ and $\{w_1, w_2, \ldots, w_{k+1}\}$, respectively. Then $e_1, e_2, \ldots, e_{k+1}, w_1, w_2, \ldots, w_{k+1}$ must be linearly dependent (since $2k + 2 > n$), which implies

$$C_z^{\perp *} \cap C_{z'}^{\perp *} \neq \emptyset,$$

for any $z \neq z'$. The following lemma shows a relationship between $C_z^\perp$ and $C_{z'}^\perp$, which will be useful in proving the main result of Construction 1.

Lemma 2 *Let $n = s + k$ with $s = k + 1$. Let $\{C_z \mid z \in \mathbb{F}_2^{k+1}\}$ be a set of (n, k) disjoint codes as in Proposition 1. Then, we have $|C_z^{\perp *} \cap C_{z'}^{\perp *}| = 1$ for any $z \neq z'$.*

Proof Noticing $(C_z + C_{z'})^\perp \subseteq C_z^\perp$ and $(C_z + C_{z'})^\perp \subseteq C_{z'}^\perp$, we have

$$(C_z + C_{z'})^\perp \subseteq C_z^\perp \cap C_{z'}^\perp. \tag{5}$$

On the other hand, for any $\alpha \in C_z^\perp \cap C_{z'}^\perp$, we have $\alpha \cdot x = 0$ and $\alpha \cdot x' = 0$, where $x \in C_z$ and $x' \in C_{z'}$. It then follows that $\alpha \cdot (x + x') = 0$, for any $x \in C_z$ and $x' \in C_{z'}$. This means $\alpha \in (C_z + C_{z'})^\perp$. Since α is arbitrary, we obtain

$$C_z^\perp \cap C_{z'}^\perp \subseteq (C_z + C_{z'})^\perp. \tag{6}$$

Combining (5) and (6), we have

$$C_z^\perp \cap C_{z'}^\perp = (C_z + C_{z'})^\perp. \tag{7}$$

Since C_z and $C_{z'}$ are (n,k) disjoint codes, we obtain

$$\dim(C_z + C_{z'}) = 2k.$$

By (7), we have

$$\dim(C_z^{\perp} \cap C_{z'}^{\perp}) = 1.$$

This proves $|C_z^{\perp *} \cap C_{z'}^{\perp *}| = 1$. □

3.1 $\mathcal{DC}$ class of vectorial semi-bent functions

The Partial Spread ($\mathcal{PS}$) class of bent functions was introduced in [24] by Dillon. The support of an n-variable bent function in $\mathcal{PS}$ is the union of $2^{n/2-1}$ or $2^{n/2-1}+1$ disjoint $(n/2)$-dimensional subspaces of $\mathbb{F}_2^n$, which means that the intersection of any two of these subspaces is $\{\mathbf{0}_n\}$. Obviously, the expression of "disjoint $(n/2)$-dimensional subspaces" are equivalent to that of "$(n, n/2)$ disjoint codes".

However, the regular $\mathcal{PS}$ construction technique cannot be applied when n is an odd number. To provide a method similar to the $\mathcal{PS}$-type construction in general, for odd n, we face the following problems:

(1) Since we cannot get bent functions when n is odd, the question is whether we can construct a class of semi-bent functions through (n,k) disjoint codes?
(2) Can this generalized $\mathcal{PS}$ construction be adopted for the purpose of designing vectorial semi-bent functions? How to guarantee that the constructed vectorial semi-bent functions are balanced?

We now give a construction method for balanced vectorial semi-bent functions, thus answering affirmatively the above raised questions. For $n = 2k+1$, we first design an $(n, k+1)$ unbalanced vectorial semi-bent function H, where the support of $c \cdot F$, $c \in \mathbb{F}_2^{k+1*}$, is a union of (n,k) disjoint codes of cardinality 2^k. Then H is transformed to a balanced vectorial semi-bent function F by adding a carefully selected linear $(n, k+1)$ vectorial function L. We call this class of functions *disjoint codes* ($\mathcal{DC}$) class of vectorial semi-bent functions.

Construction 1 *($\mathcal{DC}$ class) Let $n = s + k$ with $s = k+1$. Let $\{C_z \mid z \in \mathbb{F}_2^s\}$ be a set of (n,k) disjoint codes constructed as in Proposition 1. Let $E = \{\mathbf{0}_k\} \times \mathbb{F}_2^s$ and $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$. An (n,s) vectorial Boolean function H is defined as*

$$H(x) = \begin{cases} z & \text{if } x \in C_z^*,\ z \in \mathbb{F}_2^s \\ \mathbf{0}_s & \text{if } x \in E. \end{cases} \tag{8}$$

For $c \in \mathbb{F}_2^{s*}$, let $h_c = c \cdot H$ and

$$U_c = \{\omega \mid W_{h_c}(\omega) = 0,\ \omega \in \mathbb{F}_2^n\}. \tag{9}$$

For $i = 1, \ldots, s$, assume there exist $\theta_i \in \mathbb{F}_2^n$ such that $\theta_c = \sum_{i=1}^{s} c_i \theta_i \in U_c$ for any $c \in \mathbb{F}_2^{s*}$, and define

$$L(x) = (\theta_1 \cdot x, \theta_2 \cdot x, \ldots, \theta_s \cdot x).$$

An (n,s) vectorial Boolean function F is then specified as $F(x) = H(x) + L(x)$.

Theorem 1 *Let $F(x)$ be an (n,s) function specified as in Construction 1. Then, $F(x)$ is an (n,s) balanced vectorial semi-bent function without nonzero linear structures.*

Proof Note that $\{C_z^* \mid z \in \mathbb{F}_2^s\}$ is a set of (n, k) disjoint codes, and E, C_z^*, $z \in \mathbb{F}_2^s$, is a partition of $\mathbb{F}_2^n$. For any $c \in \mathbb{F}_2^{s*}$, we have

$$W_{h_c}(\alpha) = \sum_{x \in \mathbb{F}_2^n} (-1)^{h_c(x)+\alpha \cdot x} = S_{1(\alpha)} + S_{2(\alpha)},$$

where

$$S_1(\alpha) = \sum_{z \in \mathbb{F}_2^s} \sum_{x \in C_z^*} (-1)^{c \cdot z + \alpha \cdot x}$$

and

$$S_2(\alpha) = \sum_{x \in E} (-1)^{\alpha \cdot x}.$$

Notice that extending the sum $\sum_{x \in C_z} (-1)^{c \cdot z + \alpha \cdot x}$ in $S_1(\alpha)$ to include $x = \mathbf{0_s}$ does not change its value since for $x = \mathbf{0_s}$ we have $S_1^{x=\mathbf{0_s}}(\alpha) = \sum_{z \in \mathbb{F}_2^s} (-1)^{c \cdot z} = 0$. Therefore,

$$S_1(\alpha) = \sum_{z \in \mathbb{F}_2^s} (-1)^{c \cdot z} \sum_{x \in C_z} (-1)^{\alpha \cdot x}.$$

We now consider two cases with respect to whether α belongs to $E^\perp$ or not.
Case 1: $\alpha \notin E^\perp$. By Lemma 2, there exists exactly two different vectors z and z' in $\mathbb{F}_2^s$ such that $\alpha \in C_z^{\perp *}$ and $\alpha \in C_{z'}^{\perp *}$. So, when $\alpha \notin E^\perp$, we have

$$\begin{aligned} S_1(\alpha) &= (-1)^{c \cdot z} \sum_{x \in C_z} (-1)^{\alpha \cdot x} + (-1)^{c \cdot z'} \sum_{x \in C_{z'}} (-1)^{\alpha \cdot x} \\ &= \left((-1)^{c \cdot z} + (-1)^{c \cdot z'} \right) 2^k \\ &= \begin{cases} 0 & \text{if } c \cdot z \neq c \cdot z' \\ \pm 2^s & \text{if } c \cdot z = c \cdot z'. \end{cases} \end{aligned}$$

For any $\alpha \notin E^\perp$, noticing $\sum_{x \in E} (-1)^{\alpha \cdot x} = 0$, we have $S_2(\alpha) = 0$. So,

$$W_{h_c}(\alpha) \in \{0, \pm 2^s\}, \text{ for } \alpha \notin E^\perp. \tag{10}$$

Case 2: $\alpha \in E^\perp$. In this case, when $\alpha \neq 0$, we have

$$\sum_{x \in C_z} (-1)^{\alpha \cdot x} = 0$$

for any $z \in \mathbb{F}_2^s$, which implies $S_1(\alpha) = 0$. When $\alpha \neq 0$, one obtains

$$S_1(\alpha) = \sum_{z \in \mathbb{F}_2^s} (-1)^{c \cdot z} \sum_{x \in C_z} (-1)^0 = 2^k \sum_{z \in \mathbb{F}_2^s} (-1)^{c \cdot z} = 0.$$

On the other hand,

$$S_2(\alpha) = \sum_{x \in E} (-1)^{\alpha \cdot x} = 2^s, \text{ for } \alpha \in E^\perp.$$

Therefore,

$$W_{h_c}(\alpha) = 2^s, \text{ for } \alpha \in E^\perp. \tag{11}$$

Combining (10) and (11), we conclude that

$$W_{h_c}(\alpha) \in \{0, \pm 2^s\}, \text{ for } \alpha \in \mathbb{F}_2^n,$$

which implies H is an (n, s) vectorial semi-bent function. By (11),

$$W_{h_c}(\mathbf{0}_n) = 2^s, \text{ for any } c \in \mathbb{F}_2^{s*}.$$

According to Lemma 1, H is not balanced. In what follows, we show that H can be transformed to a balanced vectorial semi-bent function by applying an affine transformation to it.

Note that $\theta_i \in U_i$, $i = 1, 2, \ldots, s$, which implies $f_i(x) = h_i(x) + \theta_i \cdot x$ is balanced. For $c \in \mathbb{F}_2^{s*}$, let $f_c(x) = \sum_{i=1}^{s} c_i f_i(x)$. Obviously,

$$f_c(x) = h_c(x) + \theta_c \cdot x,$$

where $h_c = c \cdot H$ and $\theta_c = \sum_{i=1}^{s} c_i \theta_i$. Note that $\theta_c \in U_c$ always holds, where $U_c = \{\theta \mid W_{h_c}(\theta) = 0\}$. This means that f_c is balanced, for any $c \in \mathbb{F}_2^{s*}$. By Lemma 1,

$$\big(f_1(x), \ldots, f_s(x)\big) = H(x) + L(x) = F(x)$$

is balanced. Note that

$$W_{f_c}(\alpha) \in \{0, \pm 2^s\}, \text{ for } \alpha \in \mathbb{F}_2^n$$

still holds. This proves that $F(x)$ is a balanced (n, s) semi-bent function.

Next we show $F(x)$ has no nonzero linear structures. Let $c \in \mathbb{F}_2^{s*}$ and $\alpha \in {C_z}^*$. When $x \in {C_z}^*$, we have $x + \alpha \in {C_z}^*$. By (8), $h_c(x) = h_c(x + \alpha)$. When $x \in {C_{z'}}^*$, $z' \neq z$, $\alpha + C_{z'}$ is a coset of $C_{z'}$ and have no common vectors with $C_{z'}$. Notice that two different elements x' and x'' in $\alpha + C_{z'}$ must lie in two different disjoint codes. Then, the 2^s distinct elements of $\alpha + C_{z'}$ are evenly distributed in the 2^s disjoint codes. So, $h_c(x + \alpha)$ is not a constant when $x \in {C_z}^*$. Noticing that, by (8), $h_c(\alpha)$ is a constant function on C_z^*, we have $h_c(\alpha) + h_c(x + \alpha)$ is not a constant. This proves that F has no nonzero linear structures. □

Example 2 Let $\{C_z \mid z \in \mathbb{F}_2^3\}$ be a set of (5, 3) disjoint codes constructed as in Example 1. Let $E = \{\mathbf{0}_2\} \times \mathbb{F}_2^3$. We first construct an unbalanced (5, 3) vectorial semi-bent function

$$H(x) = \big(h_1(x), h_2(x), h_3(x)\big),$$

where, by (8),

$$h_1(x) = \begin{cases} 1 \text{ if } x \in C_z^*, \ z \in \{100, 101, 110, 111\} \\ 0 \text{ if } x \in C_z^*, \ z \in \{000, 001, 010, 011\}, \text{ or } x \in E \end{cases}$$

$$h_2(x) = \begin{cases} 1 \text{ if } x \in C_z^*, \ z \in \{010, 011, 110, 111\} \\ 0 \text{ if } x \in C_z^*, \ z \in \{000, 001, 100, 101\}, \text{ or } x \in E \end{cases}$$

and

$$h_3(x) = \begin{cases} 1 \text{ if } x \in C_z^*, \ z \in \{001, 011, 101, 111\} \\ 0 \text{ if } x \in C_z^*, \ z \in \{000, 010, 100, 110\}, \text{ or } x \in E. \end{cases}$$

We then get the truth tables of h_1, h_2 and h_3 as follows:

$\overline{h_1}$=(0 0 0 0 0 0 0 0 0 0 0 0 1 1 1 0 1 0 0 0 1 0 1 1 1 0 1 1 0 1 1 0 0),

$\overline{h_2}$=(0 0 0 0 0 0 0 0 0 0 1 0 0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 1 1 0 0 0 1), *and*

$\overline{h_3}$=(0 0 0 0 0 0 0 0 0 0 0 1 0 1 0 1 1 0 1 0 1 1 1 0 0 0 1 0 0 1 0 1 1).

Select $\theta_1 = (01101)$, $\theta_2 = (00010)$ and $\theta_3 = (00001)$.

It can be checked that for any $c \in \mathbb{F}_2^{3*}$, we always have $\theta_c \in U_c$, where $\theta_c = c_1\theta_1 + c_2\theta_2 + c_3\theta_3$ and U_c is defined as in (9). Let

$$L(x) = \big(l_1(x), l_2(x), l_3(x)\big)$$

where $l_1(x) = \theta_1 \cdot x = x_2 + x_3 + x_5$, $l_2(x) = \theta_2 \cdot x = x_4$ and $l_3(x) = \theta_3 \cdot x = x_5$. The truth tables of l_1, l_2 and l_3 are as follows:

$\overline{l_1}$=*(0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1),*
$\overline{l_2}$=*(0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1),* and
$\overline{l_3}$=*(0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1).*

Let $f_i(x) = h_i(x) + l_i(x)$, $i = 1, 2, 3$. Then the truth tables of f_1, f_2 and f_3 are as follows:

$\overline{f_1}$=*(0 1 0 1 1 0 1 0 1 0 1 1 1 0 0 0 0 1 0 0 1 1 0 1 1 1 1 0 0 1 0 0 1),*
$\overline{f_2}$=*(0 0 1 1 0 0 1 1 0 1 1 1 1 1 1 0 1 0 1 0 1 0 1 1 0 0 1 0 0 0 0 1 0),* and
$\overline{f_3}$=*(0 1 0 1 0 1 0 1 0 1 1 1 1 1 1 1 0 0 0 0 0 1 0 0 1 0 0 0 0 1 1 1 1 0).*

The Walsh spectra of f_c, $c \in \mathbb{F}_2^{3*}$, are as follows:

$\widetilde{W}_{f_{100}}$=*(0 0 −8 −8 0 8 0 8 0 8 0 8 8 8 8 0 0 0 −8 8 0 −8 8 8 −8 0 0 0 0 0 8 −8 0),*
$\widetilde{W}_{f_{010}}$=*(0 8 8 8 0 8 0 0 0 0 8 0 0 0 0 −8 −8 0 8 −8 0 −8 8 8 8 −8 8 0 0 0 −8 0),*
$\widetilde{W}_{f_{001}}$=*(0 8 0 0 8 8 8 0 8 8 0 −8 0 −8 −8 8 −8 8 0 8 −8 0 0 0 0 8 0 0 0 0 0 −8),*
$\widetilde{W}_{f_{110}}$=*(0 0 0 −8 8 0 −8 8 0 0 8 8 0 0 8 8 8 0 8 −8 8 −8 −8 0 8 0 −8 0 0 0 0 0 8),*
$\widetilde{W}_{f_{101}}$=*(0 8 −8 8 8 0 −8 −8 8 8 0 0 0 8 0 8 8 0 −8 0 0 0 8 0 0 0 −8 0 8 −8 8 0 0 0),*
$\widetilde{W}_{f_{011}}$=*(0 8 0 8 8 8 0 0 −8 0 0 8 0 0 0 0 8 −8 8 8 0 −8 −8 0 0 0 −8 8 −8 0 8 0),*
$\widetilde{W}_{f_{111}}$=*(0 0 8 −8 0 0 8 −8 8 8 0 0 8 0 8 8 0 −8 −8 0 0 0 0 8 8 0 8 −8 0 0 −8 8 0).*

Note that $W_{f_c}(\mathbf{0}_5) = 0$ for any $c \in \mathbb{F}_2^{3*}$. We have $\big(f_1(x), f_2(x), f_3(x)\big) = F(x) + L(x)$ is a $\mathcal{DC}$ type balanced $(5, 3)$ vectorial semi-bent function.

Remark 2 There seem to be many different choices (verified by computer simulations) to specify the elements $\theta_1, \ldots, \theta_s$ that satisfy the condition in Construction 1 so that $\theta_c = \sum_{i=1}^{s} c_i\theta_i \in U_c$, for any $c \in \mathbb{F}_2^{s*}$. However, specifying these selections precisely appears to be quite hard. We leave this interesting question as an open problem.

3.2 $\mathcal{DS}$ class vectorial semi-bent functions

We now present our second construction method which uses a set of disjoint spectra functions obtained from an AB permutation and a set of disjoint codes. The resulting balanced vectorial semi-bent functions are then derived by using a suitable concatenation of these disjoint spectra functions. We refer to this class as to *disjoint spectra* ($\mathcal{DS}$) class vectorial semi-bent functions.

Construction 2 *($\mathcal{DS}$ class) Let $n = 2s + k$, where $s \geq k$ and k is odd. Let $x \in \mathbb{F}_2^k$ and $y, z \in \mathbb{F}_2^s$. Let*

$$G(x) = \big(g_1(x), \ldots, g_k(x)\big)$$

be an AB permutation on $\mathbb{F}_2^k$. Let H be an $(s + k, k)$ vectorial function defined as

$$H(x, y) = \big(h_1(x, y), \ldots, h_k(x, y)\big),$$

where $h_i(x, y) = g_i(x)$, $i = 1, 2, \ldots, k$. For $z \in \mathbb{F}_2^s$, let

$$A_z = \begin{pmatrix} I_k & M_z \\ \mathbf{0} & R_z \end{pmatrix} \tag{12}$$

where M_z is defined as in Proposition 1 and R_z is any $s \times s$ invertible binary matrix. We construct an (n, k) vectorial function as follows:

$$F(x, y, z) = H\big((x, y) \cdot (A_z^T)^{-1}\big). \tag{13}$$

Notice that the function F defined by (13) can be viewed as a concatenation of different linear transforms of $H(x, y)$ performed on the variable space (x, y) through the invertible matrices $A_z^{T^{-1}}$. The main design rationale, which ensures the semi-bentness of the components of F, is that any component function $c \cdot H\big((x, y) \cdot (A_z^T)^{-1}\big)$ builds a set of disjoint spectra functions when z ranges through $\mathbb{F}_2^s$.

Theorem 2 *Let F be an (n, k) function defined by means of Construction 2. Then, F is a balanced (n, k) vectorial semi-bent function.*

Proof For any $c \in \mathbb{F}_2^{k*}$, let $h_c = c \cdot H$ and $g_c = c \cdot G$. Let $\alpha \in \mathbb{F}_2^k$ and $\beta \in \mathbb{F}_2^s$. We have

$$\begin{aligned} W_{h_c}(\alpha, \beta) &= \sum_{y \in \mathbb{F}_2^s} (-1)^{\beta \cdot y} \sum_{x \in \mathbb{F}_2^k} (-1)^{g_c(x) + \alpha \cdot x} \\ &= \begin{cases} 2^s \cdot W_{g_c}(\alpha), & \beta = \mathbf{0}_s \\ 0, & \beta \neq \mathbf{0}_s. \end{cases} \end{aligned} \tag{14}$$

Noticing that G is an AB function, we have

$$W_{g_c}(\alpha) \in \{0, \pm 2^{(k+1)/2}\}.$$

By (14),

$$W_{h_c}(\alpha, \beta) \in \{0, \pm 2^{(n+1)/2}\}.$$

Let $\{C_z \mid z \in \mathbb{F}_2^s\}$ be a set of $(s + k, k)$ disjoint codes as in Proposition 1. Noticing G is a permutation, we have $W_{g_c}(\mathbf{0}_k) = 0$. Thus,

$$S_{h_c} = S_{g_c} \times \{\mathbf{0}_s\} \subset C_{\mathbf{0}_s}^*. \tag{15}$$

From (12), the upper section of A_z is just the generator matrix G_z of C_z. This implies

$$C_z = C_{\mathbf{0}_s} \cdot A_z. \tag{16}$$

For a fixed $z \in \mathbb{F}_2^{s*}$, let

$$H^{(z)}(x, y) = H\big((x, y) \cdot (A_z^T)^{-1}\big). \tag{17}$$

Obviously, $H^{(\mathbf{0}_s)}(x, y) = H\big((x, y) \cdot A_{\mathbf{0}_s}^{-1}\big) = H(x, y)$. For $c \in \mathbb{F}_2^{k*}$, let $h_c^{(z)} = c \cdot H^{(z)}$. By (17),

$$h_c^{(z)}(x, y) = h_c\big((x, y) \cdot (A_z^T)^{-1}\big).$$

We have

$$W_{h_c^{(z)}}(\alpha, \beta) = W_{h_c}\big((\alpha, \beta) \cdot A_z\big).$$

By (16),

$$S_{h_c^{(z)}} \subset C_z^*.$$

Let $f_c = c \cdot F, c \in \mathbb{F}_2^{k*}$. By (13), f_c is a concatenation of the 2^s functions $h_c^{(z)}, z \in \mathbb{F}_2^s$. For $\alpha \in \mathbb{F}_2^k$, $\beta \in \mathbb{F}_2^s$, and $\gamma \in \mathbb{F}_2^s$, we have

$$\begin{aligned} W_{f_c}(\alpha, \beta, \gamma) &= \sum_{(x,y,z)\in\mathbb{F}_2^n} (-1)^{f_c(x,y,z)+(\alpha,\beta,\gamma)\cdot(x,y,z)} \\ &= \sum_{z\in\mathbb{F}_2^s} (-1)^{\gamma\cdot z} \sum_{(x,y)\in\mathbb{F}_2^{k+s}} (-1)^{h_c^{(z)}(x,y)+(\alpha,\beta)\cdot(x,y)} \\ &= \sum_{z\in\mathbb{F}_2^s} (-1)^{\gamma\cdot z} W_{h_c^{(z)}}(\alpha, \beta). \end{aligned}$$

Note that $\{C_z \mid z \in \mathbb{F}_2^s\}$ is a set of disjoint codes. By Definition 1,

$$\{h_c^{(z)}(x, y) \mid z \in \mathbb{F}_2^s\} \subset \mathcal{B}_{s+k}$$

is a set of disjoint spectra functions. We then have

$$W_{h_c^{(z)}}(\alpha, \beta) \cdot W_{h_c^{(z')}}(\alpha, \beta) = 0, \text{ for } z \neq z'.$$

We then have $W_{f_c}(\alpha, \beta, \gamma) \in \{0, \pm 2^{(n+1)/2}\}$. This proves that f is semi-bent. By (15), $W_{h_c^{(z)}}(\mathbf{0}_{k+s}) = 0$ for any $z \in \mathbb{F}_2^s$. So, $W_{f_c}(\mathbf{0}_n) = 0$, which implies that f_c is balanced. By Lemma 1, we have that F is balanced. □

Example 3 Let $n = 9$ with $s = k = 3$. Let $x, y, z \in \mathbb{F}_2^3$. Let $G(x) = (g_1(x), g_2(x), g_3(x))$ be an AB permutation on $\mathbb{F}_2^3$ with

$$\overline{g_1} = (01010110), \quad \overline{g_2} = (00110101), \quad \overline{g_2} = (01111000).$$

Then $H(x, y) = \big(h_1(x, y), h_2(x, y), h_2(x, y)\big) = \big(g_1(x), g_2(x), g_3(x)\big)$ is a balanced (6, 3) vectorial function. Let $\{C_z \mid z \in \mathbb{F}_2^3\}$ be a set of (6, 3) disjoint codes obtained by means of Proposition 1. Set $R_z = M_z$ for $z \in \mathbb{F}_2^{3*}$. Then, we have

$$A_{000} = \begin{pmatrix} 100\ 100 \\ 010\ 010 \\ 001\ 001 \\ 000\ 100 \\ 000\ 010 \\ 000\ 001 \end{pmatrix}, A_{001} = \begin{pmatrix} 100\ 100 \\ 010\ 010 \\ 001\ 001 \\ 000\ 100 \\ 000\ 010 \\ 000\ 001 \end{pmatrix}, A_{010} = \begin{pmatrix} 100\ 010 \\ 010\ 001 \\ 001\ 110 \\ 000\ 010 \\ 000\ 001 \\ 000\ 110 \end{pmatrix}, A_{011} = \begin{pmatrix} 100\ 001 \\ 010\ 110 \\ 001\ 011 \\ 000\ 001 \\ 000\ 110 \\ 000\ 011 \end{pmatrix},$$

$$A_{100} = \begin{pmatrix} 100\ 110 \\ 010\ 011 \\ 001\ 111 \\ 000\ 110 \\ 000\ 011 \\ 000\ 111 \end{pmatrix}, A_{101} = \begin{pmatrix} 100\ 011 \\ 010\ 111 \\ 001\ 101 \\ 000\ 011 \\ 000\ 111 \\ 000\ 101 \end{pmatrix}, A_{110} = \begin{pmatrix} 100\ 111 \\ 010\ 101 \\ 001\ 100 \\ 000\ 111 \\ 000\ 101 \\ 000\ 100 \end{pmatrix}, A_{111} = \begin{pmatrix} 100\ 101 \\ 010\ 100 \\ 001\ 010 \\ 000\ 101 \\ 000\ 100 \\ 000\ 010 \end{pmatrix}.$$

For $z \in \mathbb{F}_2^3$, let $H^{(z)}(x, y) = H\big((x, y)\cdot(A_z^T)^{-1}\big)$. The eight balanced (6, 3) vectorial functions $H^{(z)}, z \in \mathbb{F}_2^3$, have the property that $\{c \cdot H^{(z)} \mid z \in \mathbb{F}_2^3\}$ is a set of disjoint spectra functions for any $c \in \mathbb{F}_2^{3*}$. Then we can get the $\mathcal{DS}$ type balanced (9, 3) vectorial semi-bent function

$$F(x, y, z) = \big(f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)\big) = H\big((x, y) \cdot (A_z^T)^{-1}\big).$$

Note that $f_c = c \cdot F$ can be regarded as the concatenation of $H^{(z)}$, $z \in \mathbb{F}_2^3$. We get the truth tables of F in a hexadecimal format as follows:

f_1 : 0000007F7F7F7F0074335A620B4C251D174B654668341A39ADB6F195D2C98EEA
D9EC9ED4A693E1ABCEBCA7AAB1C3D8D5BAD38F99C5ACF0E6634D78291C320756
f_2 : 00007F00007F7F7F635632784D071C29CED5C3A7BCD8B1AA173934654B1A6846
741D4C5A33250B62BAE6AC8FD3F0C599D9AB939EECE1A6D4ADEAC9F1B68ED295
f_3 : 007F7F007F007F00D9A6D4ABE19E93ECADD295EA8EF1C9B6631C29560778324D
BAC599E6F08FACD3176846391A65344BCEB1AAD5D8A7C3BC740B621D255A4C33.

4 Other cryptographic properties of the $\mathcal{DC}$ and $\mathcal{DS}$ class

We have already mentioned that the method of Johansson-Pasalic [32] may admit linear structures depending on the selection of disjoint codes, whereas the members of our $\mathcal{DC}$ class provably cannot possess linear structures. We recall that the component functions of an (n, m) function are actually a concatenation of 2^d linear t-resilient functions in $n - d$ variables which are derived from an (several) $[n - d, m, t + 1]$ linear code(s). Therefore, the (n, m) functions in [32] strictly belong to the $\mathcal{MM}$ class of functions. In difference to this approach (of concatenating linear functions), our method has similarities to the $\mathcal{PS}$ class of Boolean bent functions. Indeed, Construction 1 specifies both the coordinate and component functions to be constant on disjoint k-dimensional subspaces of $\mathbb{F}_2^n$ corresponding to the codes C_z in Construction 1. This is structurally different approach compared to the method in [32], but nevertheless proving the EA-inequivalence between the classes is quite difficult. We also notice that the disjoint codes employed in [32] are found using a computer search, whereas the set of codes in Proposition 1 is specified in an exact manner. As mentioned in the introduction, the component functions in Construction 2 can be viewed as a concatenation of suitable disjoint spectra functions which in difference to the method in [32] are not linear.

In what follows, we discuss other cryptographic properties of the two classes.

4.1 Algebraic degree

In general, for the same n, the dimension of the output space of $\mathcal{DC}$ functions is larger compared to the class $\mathcal{DS}$. The upper bounds on the algebraic degrees of $\mathcal{DC}$ and $\mathcal{DS}$ balanced vectorial semi-bent functions are both $(n + 1)/2$. The bounds are tight, which have been confirmed by simulations (the algebraic degrees of the constructed functions in Example 2 and Example 3 are 3 and 5, respectively), and essentially this is the maximum degree of AB functions as proved by Carlet et al. [11].

In difference to the $\mathcal{DC}$ class, whose algebraic degree is harder to analyse theoretically, for functions that belong to $\mathcal{DS}$ (generated by Construction 2) we deduce the following. Noticing that $G(x)$ is an AB function on $\mathbb{F}_2^k$ and $H(x, y) = G(x)$, where $H : \mathbb{F}_2^{s+k} \to \mathbb{F}_2^k$, we have $\deg(H) = \deg(G) \leq (k + 1)/2$. For any $c \in \mathbb{F}_2^{k*}$, the component function $f_c = c \cdot F$ in Construction 2 is in nature the concatenation of $h_c^{(u)} = c \cdot H^{(u)}$, when u goes through $\mathbb{F}_2^s$. It implies that

$$\deg(F) = \max_{c \in \mathbb{F}_2^{k*}} \deg(f_c) \leq s + (k + 1)/2 = (n + 1)/2.$$

Table 1 Differential properties of the (5,3) function F in Example 2

c	0	2	4	6	8
$\big\vert\{(a,b) \mid \delta_F(a,b)=c\}\big\vert$	744	84	108	28	28

Table 2 Differential properties of the (9,3) function F in Example 3

c	0	48	64	80	112
$\big\vert\{(a,b) \mid \delta_F(a,b)=c\}\big\vert$	257572	84	3836	112	28

4.2 Differential properties

Let F be an (n,m) function. For any $a \in \mathbb{F}_2^{n*}$ and $b \in \mathbb{F}_2^m$, we denote by

$$\delta_F(a,b) = \big\vert\{x \in \mathbb{F}_2^n \mid F(x+a)+F(x)=b\}\big\vert.$$

A mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ has a uniform differential distribution if any differential $F(x+a)+F(x)=b$ has exactly 2^{n-m} solutions, which is only achieved by vectorial bent functions for suitable n and m. In this context, an element $a \in \mathbb{F}_2^{n*}$ is called a linear structure of F if for some $b \in \mathbb{F}_2^m$ we have $\delta_F(a,b)=2^n$. Hence, for non-bent (n,m) functions good differential properties are achieved by those functions whose

$$\max_{(a,b)\in\mathbb{F}_2^{n*}\times\mathbb{F}_2^m} \delta_F(a,b) \le 2^{n-m+1}.$$

We now provide simulation results related to the functions specified in Example 2 and Example 3. For the sake of brevity, we present the tables below in a compact form by counting all the pairs (a,b) that have the same value $\delta_F(a,b)$.

In both cases, $\max_{(a,b)\in\mathbb{F}_2^{n*}\times\mathbb{F}_2^m} \delta_F(a,b) \le 2^{n-m+1}$ which is especially true for the function F in Example 3, which seems to be "closer" to a uniform distribution than the one in Example 2. An exact theoretical analysis of the differential properties appears to be difficult.

4.3 Extendability problem

It is an interesting problem to investigate the concept of extendability for both the proposed classes. In other words, given the existence of vectorial semi-bent functions of a certain output dimension m the question is whether these (n,m) functions can be extended to $(n,m+k)$ semi-bent functions for some $1 \le k \le n-m$. Nevertheless, there is no known technique of verifying whether these classes are *non-extendable* in the sense that there do not exist suitable Boolean semi-bent functions (of cardinality k) so that $(n,m+k)$ semi-bent function can be built. This problem is intrinsically hard and in our opinion of utmost importance for gaining a better understanding of these objects. A related question in this context is whether the coordinates of (n,m) functions (either in $\mathcal{DC}$ or $\mathcal{DS}$) belong to the set of component functions of some known AB functions, which also appears to be difficult.

5 Vectorial semi-bent functions from AB permutations

When n is even, Carlet [12] proposed a method of using two suitable vectorial bent functions (which we call *block components*) $F_1, F_2 : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$, to define vectorial semi-bent

functions on $\mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ in the $\mathcal{MM}$ class (using the finite field representation). The semi-bent property of

$$F(x, y) = \big(F_1(x, y), F_2(x, y)\big) = \big(x\pi(y) + \phi(y), x\pi^{2^i}(y) + \psi(y)\big),$$

where $\phi, \psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ are arbitrary, π is a permutation on $\mathbb{F}_{2^m}$ and $\gcd(i, m) = 1$, relies on the fact that the absolute values of the Walsh spectra of the component functions $u \cdot F_1 + v \cdot F_2$ are at most 2^{m+1}, using the vector space representation so that $F : \mathbb{F}_2^{2m} \to \mathbb{F}_2^{2m}$, see Carlet [12]. This property is a consequence of the fact that the equation $u\pi(y) + v\pi^{2^i}(y) = a$ has at most two solutions for $u, v, a \in \mathbb{F}_{2^m}$.

For odd $n \equiv 0 \pmod 3$ one can consider

$$F(x, y, z) = (F_1(x, y, z), F_2(x, y, z), F_3(x, y, z)),$$

where $F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^{\frac{n}{3}}}$ and clearly $n \equiv 0 \pmod 3$. Then, F is an AB function if and only if

$$W_F(a, b, c) = \sum_{x \in \mathbb{F}_{2^{\frac{n}{3}}}} \sum_{y \in \mathbb{F}_{2^{\frac{n}{3}}}} \sum_{z \in \mathbb{F}_{2^{\frac{n}{3}}}} (-1)^{Tr_1^{\frac{n}{3}}\left(uF_1(x,y,z)+vF_2(x,y,z)+wF_3(x,y,z)+ax+by+cz\right)}$$
$$\in \{0, \pm 2^{\frac{n+1}{2}}\},$$

for all $(a, b, c) \in (\mathbb{F}_{2^{\frac{n}{3}}})^3$, where $Tr_1^{\frac{n}{3}}(uF_1 + vF_2 + wF_3)$ specifies the component functions of F. Here, $Tr_1^{\frac{n}{3}}(\cdot)$ denotes the absolute trace function defined as

$$Tr_1^{\frac{n}{3}}(x) = \sum_{i=0}^{n/3-1} x^{2^i}, \quad \text{for any } x \in \mathbb{F}_{2^{\frac{n}{3}}}.$$

Nevertheless, in difference to the even n case described above, the specification of AB functions using the block components F_1, F_2 and F_3 appears to be a difficult task, see also Remark 4 below. Instead, we demonstrate the possibility of specifying vectorial $(n, n/3)$ semi-bent functions. The following result gives us a possibility to lift up the semi-bent property from a subfield to extension fields, thus specifying vectorial semi-bent functions $F : (\mathbb{F}_{2^k})^3 \to \mathbb{F}_{2^k}$.

Proposition 2 *Let $n = 3k$, where k is odd. Define $F_1 : (\mathbb{F}_{2^k})^3 \to \mathbb{F}_{2^k}$ as*

$$F_1(x, y, z) = x\pi(y) + y\pi(z),$$

where π is an AB permutation on $\mathbb{F}_{2^k}$. Then, the function F_1 is a vectorial (n, k) semi-bent function.

Proof We compute the extended Walsh spectra of uF_1, $u \neq 0$ as follows :

$$W_{uF_1}(a, b, c) = \sum_{y \in \mathbb{F}_{2^k}} \sum_{z \in \mathbb{F}_{2^k}} \sum_{x \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k\left(u(x\pi(y)+y\pi(z))+ax+by+cz\right)} =$$
$$= \sum_{y \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k(by)} \sum_{z \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k\left(uy\pi(z)+cz\right)} \sum_{x \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k\left((u\pi(y)+a)x\right)}.$$

Since for any other y the function $(u\pi(y) + a)x$ is balanced so that

$$\sum_{x \in \mathbb{F}_{2^k}} (-1)^{Tr_1^k\left((u\pi(y)+a)x\right)} = 0,$$

unless $u\pi(y) = a$ in which case

$$\sum_{x\in\mathbb{F}_{2^k}} (-1)^{Tr_1^k\left((u\pi(y)+a)x\right)} = 2^k,$$

we have

$$W_{uF_1}(a,b,c) = 2^k \sum_{y\in\mathbb{F}_{2^k}:y=\pi^{-1}(a/u)} (-1)^{Tr_1^k(by)} \sum_{z\in\mathbb{F}_{2^k}} (-1)^{Tr_1^k\left(uy\pi(z)+cz\right)}.$$

Since by assumption π is an AB function

$$\sum_{z\in\mathbb{F}_{2^k}} (-1)^{Tr_1^k\left(uy\pi(z)+cz\right)} \in \{0, \pm 2^{\frac{k+1}{2}}\},$$

we have

$$W_{uF_1}(a,b,c) \in \{0, \pm 2^k 2^{\frac{k+1}{2}}\} = \{0, \pm 2^{\frac{n+1}{2}}\},$$

that is F_1 is an (n,k) vectorial semi-bent function. □

Remark 3 The algebraic degree of F_1 defined in Proposition 2 is obviously $\deg(F_1) = \deg(\pi) + 1$. Notice that any AB function $F : \mathbb{F}_2^{3k} \to \mathbb{F}_2^{3k}$ can be represented as $F = (F_1, F_2, F_3)$, where $F_i : \mathbb{F}_2^{3k} \to \mathbb{F}_2^k$, which naturally gives rise to F_i which are vectorial semi-bent functions. However, if degree of an AB function π is the same on $\mathbb{F}_{2^k}$ and on $\mathbb{F}_{2^{3k}}$ then Proposition 2 generates EA-inequivalent functions.

Remark 4 Due to symmetry, it is clear that one can for instance define $F_2(x,y,z) = y\pi(x) + x\pi(z)$ and $F_3(x,y,z) = z\pi(y) + y\pi(x)$, which are also semi-bent vectorial functions. However, the analysis of the Walsh coefficients of $uF_1 + vF_2 + wF_3$ becomes complicated and non-exhaustive attempts to specify an AB function $F = (F_1, F_2, F_3)$ using F_i derived from the same AB function π on $\mathbb{F}_2^k$ have failed.

Clearly, the above approach in general does not yield vectorial semi-bent functions of maximal algebraic degree but is very efficient from the implementation point of view since most of the known AB functions are power monomials implying that $F_1(x,y,z) = zy^d + yx^d$ for a suitably chosen d. Nevertheless, the main interest of the proposed method is a further investigation of the structure $F = (F_1, F_2, F_3)$ for the known AB functions and the possibility of extending functions $F : (\mathbb{F}_{2^{n/3}})^3 \to \mathbb{F}_{2^{n/3}}$ in Proposition 2 on a block/coordinate level.

6 Concluding remarks

In this paper, using different design rationales, three constructions of vectorial semi-bent functions are presented. These classes of functions can be potentially used for implementing S-boxes in Feistel-like block ciphers. Moreover, these functions (depending on the choice of input parameters) can possess good cryptographic properties such as high algebraic degree, the absence of linear structures and quite satisfactory differential properties. The extendability problem, related to the increase of the output space, is left as an interesting research challenge.

Acknowledgements WeiGuo Zhang is supported by the National Natural Science Foundation of China (No. 61972303). Enes Pasalic is supported in part by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694, N1-0159, J1-2451).

References

1. Assmus E.F., Key J.D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).
2. Beth T., Jungnickel D., Lenz H.: Design Theory, vol. 1. Cambridge University Press, Cambridge (1999).
3. Boztaş S., Kumar P.V.: Binary sequences with Gold-like correlation but larger linear span. IEEE Trans. Inf. Theory **40**, 532–537 (1994).
4. Canteaut A., Carlet C., Charpin P., Fontaine C.: On cryptographic properties of the cosets of $R(1, m)$. IEEE Trans. Inf. Theory **47**, 1494–1513 (2001).
5. Canteaut A., Charpin P.: Decomposing bent functions. IEEE Trans. Inf. Theory **49**, 2004–2019 (2003).
6. Canteaut A., Charpin P., Dobbertin H.: Binary m-sequences with three-valued crosscorrelation: a proof of Welch's conjecture. IEEE Trans. Inf. Theory **46**, 4–8 (2000).
7. Cao X., Chen H., Mesnager S.: Further results on semi-bent functions in polynomial form. Adv. Math. Commun. **10**, 725–741 (2016).
8. Carlet C.: Boolean functions for cryptography and error correcting codes. In: Crama Y., Hammer P. (eds.) Boolean Methods and Models, pp. 257–397. Cambridge University Press, Cambridge (2010).
9. Carlet C.: Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge (2021).
10. Carlet C.: Vectorial Boolean functions for cryptography. In: Crama Y., Hammer P. (eds.) Boolean Methods and Models, pp. 398–469. Cambridge University Press, Cambridge (2010).
11. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–156 (1998).
12. Carlet C.: Boolean and vectorial plateaued functions, and APN functions. IEEE Trans. Inf. Theory **61**, 6272–6289 (2015).
13. Carlet C., Gao G., Liu W.: Results on constructions of rotation symmetric bent and semi-bent functions. In: International Conference on Sequences and Their Applications-SETA 2014, vol. 8865, pp. 21–23. LNCS. Springer, Berlin (2014).
14. Carlet C., Mesnager S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**, 257–397 (2016).
15. Carlet C.: Partially bent functions. In: Advances in Cryptology-CRYPTO'92, vol. 740, pp. 280–291. LNCS. Springer, Berlin (1993).
16. Carlet C., Mesnager S.: On semibent Boolean functions. IEEE Trans. Inf. Theory **58**, 3287–3292 (2012).
17. Chabaud F., Vaudenay S.: Links between differential and linear cryptanalysis. In: Advances in Cryptology-EUROCRYPT'94, vol. 950, pp. 356–365. LNCS. Springer, Berlin (1995).
18. Charpin P., Pasalic E., Tavernier C.: On bent and semi-bent quadratic Boolean functions. IEEE Trans. Inf. Theory **51**, 4286–4298 (2005).
19. Chee S., Lee S., Kim K.: Semi-bent functions. In: Advances in Cryptology-ASIACRYPT'94, vol. 917, pp. 107–118. LNCS. Springer, Berlin (1994).
20. Chen H., Cao X.: Some semi-bent functions with polynomial trace form. J. Syst. Sci. Complex. **27**, 777–784 (2014).
21. Cusick T.W., Dobbertin H.: Some new three-valued cross-correlation functions for binary m-sequences. IEEE Trans. Inf. Theory **42**, 1238–1240 (1996).
22. Dempwolff U., Neumann T.: Geometric and design-theoretic aspects of semibent functions (I). Des. Codes Cryptogr. **57**, 373–381 (2010).
23. Dempwolff U.: Geometric and design-theoretic aspects of semibent functions (II). Des. Codes Cryptogr. **62**, 241–252 (2012).
24. Dillon J.F.: Elementary Hadamard difference sets, Ph.D. Dissertation, Fac. Graduate School. University of Maryland, College Park (1974).
25. Ding C., Xiao G.-Z., Shan W.: The Stability Theory of Stream Ciphers, LNCS, vol. 561. Springer, Berlin (1991).
26. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inf. Theory **IT–14**, 154–156 (1968).
27. Helleseth T., Kumar P.V.: Sequences with low correlation, Chapter 21. In: Pless V.S., Huffman W.C., Brualdi R.A. (eds.) Handbook of Coding Theory, Part 3: Applications, pp. 1765–1853. Elsevier, Amsterdam (1998).
28. Helleseth T.: Some results about the cross-correlation function between two maximal linear sequences. Discret. Math. **16**, 209–232 (1976).
29. Helleseth T.: Correlation of m-sequences and related topics. In: Ding C., Helleseth T., Niederreiter H. (eds.) Sequences and their Applications, Discrete Mathematics and Theoretical Computer Science, pp. 49–66. Springer, London (1999).

30. Helleseth T., Kumar P.V.: In: Sequences with low correlation. In: Pless V.S., Huffman W.C., Brualdi R.A. (eds.) Handbook of Coding Theory, Part 3: Applications, vol. ch. 21. Elsevier, Amsterdam (1998).
31. Hunt F.H., Smith D.H.: The construction of orthogonal variable spreading factor codes from semi-bent functions. IEEE Trans. Wirel. Commun. **11**, 2970–2975 (2012).
32. Johansson T., Pasalic E.: A construction of resilient functions with high nonlinearity. IEEE Trans. Inf. Theory **49**, 494–501 (2003).
33. Karpovsky M.G., Kulikowski K.J., Wang Z.: On-line self error detection with equal protection against all errors. Int. J. Highly Reliab. Electron. Syst. Des. **124–130** (2008).
34. Khoo K., Gong G., Stinson D.R.: A new family of Gold-like sequences, In: IEEE International Symposium on Information Theory, pp. 181, Lausanne, Switzerland (2002).
35. Khoo K., Gong G., Stinson D.R.: A new characterization of semibent and bent functions on finite fields. Des. Codes Cryptogr. **38**, 279–295 (2006).
36. Matsui M.: Linear cryptanalysis method for DES cipher. In: Advances in Cryptology-EUROCRYPT'93, vol. 765, pp. 386–397. LNCS. Springer, Berlin (1994).
37. Meier W., Staffelbach O.: Fast correlation attacks on certain stream ciphers. J. Cryptol. **1**, 159–176 (1989).
38. Mesnager S.: Semi-bent functions from Dillon and Niho exponents, Kloosterman sums and Dickson polynomials. IEEE Trans. Inf. Theory **57**, 7443–7458 (2011).
39. Mesnager S.: Semi-bent functions with multiple trace terms and hyperelliptic curves. In: Proceeding of International Conference on Cryptology and Information Security in Latin America, vol. 7533, pp. 18–36. Latincrypt 2012, (Lecture Notes in Computer Science). Springer, Berlin (2012).
40. Mesnager S.: Semi-bent Functions from Oval Polynomials, vol. 8308, pp. 1–15. Springer, Berlin (2013).
41. Mesnager S., Zhang F.: On constructions of bent, semi-bent and five valued spectrum functions from old bent functions. Adv. Math. Commun. **11**, 339–345 (2017).
42. Nachef V., Patarin J., Volte E.: Feistel Ciphers Security—Proofs and Cryptanalysis. Springer, Berlin (2017).
43. Niho Y.: Multi-valued cross-correlation functions between two maximal linear recursive sequences, Ph.D. dissertation, Univ. Sothern Calif, Los Angeles (1972).
44. Nyberg K.: Differentially uniform mappings for cryptography. In: Advances in Cryptology-EUROCRYPT'93, vol. **765**, pp. 55–64. LNCS. Springer, Berlin (1994).
45. Olsen J.D., Scholtz R.A., Welch L.R.: Bent function sequences. IEEE Trans. Inf. Theory **28**, 858–864 (1982).
46. Pasalic E., Gangopadhyay S., Zhang W.-G., Bajric S.: Design methods for semi-bent functions. Inf. Process. Lett. **143**, 61–70 (2019).
47. Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A **20**, 300–305 (1976).
48. Smith D.H., Hunt F.H., Perkins S.: Exploiting spatial separations in CDMA systems with correlation constrained sets of Hadamard matrices. IEEE Trans. Inf. Theory **56**, 5757–5761 (2010).
49. Zhang W.-G., Xie C.-L., Pasalic E.: Large sets of orthogonal sequences suitable for applications in CDMA systems. IEEE Trans. Inf. Theory **62**, 3757–3767 (2016).
50. Zhang W.-G., Pasalic E.: Constructions of resilient S-boxes with strictly almost optimal nonlinearity through disjoint linear codes. IEEE Trans. Inf. Theory **60**, 1638–1651 (2014).
51. Zhang W.-G., Xiao G.-Z.: Constructions of almost optimal resilient Boolean functions on large even number of variables. IEEE Trans. Inf. Theory **55**, 5822–5831 (2009).
52. Zhao Q.-L., Zheng D.: Two classes of rotation symmetric semi-bent functions. Sci. China Inf. Sci. **60**, 068103:1-068103:3 (2017).
53. Zheng Y., Zhang X.-M.: Plateaued functions, In: Varadharajan V., Mu Y. (eds.) Information and Communication Security, ICICS 1999, LNCS, vol. 1726, pp. 284-300, Springer, Berlin (1999).
54. Zheng Y., Zhang X.-M.: On plateaued functions. IEEE Trans. Inf. Theory **47**, 1215–1223 (2001).
55. Zheng Y., Zhang X.-M.: Relationships between bent functions and complementary plateaued functions, In: Song J. (eds.) Information Security and Cryptology—ICISC'99. ICISC 1999, vol. 1787, pp. 60-75, Springer, Berlin (2000).