Quadratic almost bent functions - their partial characterization and design in the spectral domain

A. Bapić * S. Hodžić † E. Pasalic‡

Abstract

Quadratic AB (almost bent) functions are characterized by the property that the duals of their component functions are bent functions. We prove that these duals are also quadratic and illustrate that these bent duals may give rise to vectorial bent functions (in certain cases having a maximal output dimension). It is then natural to investigate when the linear combinations of quadratic bent duals again yields quadratic bent functions. A necessary and sufficient condition for ensuring bentness of these linear combinations is provided, by introducing a useful transform that acts on the Walsh spectrum of dual functions. Moreover, we provide a rather detailed analysis related to the structure of quadratic AB functions in the spectral domain, more precisely with respect to their Walsh supports, their intersection and restrictions of these bent duals to suitable subspaces. It turns out that the AB property is quite complicated even in the quadratic case. However, using the established facts in this article, we could for the first time provide the design of quadratic AB functions in the spectral domain by identifying (using computer simulations) suitable sets of bent dual functions which give rise to possibly new quadratic AB functions in a generic manner. Using a simple non-exhaustive search for suitable sets of defining bent duals $f_1, \ldots, f_5$ on $\mathbb{F}_2^4$, we could easily identify 60 quadratic AB functions $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$. It turns out that all these functions are CCZ-equivalent to the Gold AB function but none of these functions is a permutation. On the other hand, when $n = 7$, the same approach provides several AB functions which are **not** CCZ-equivalent to Gold functions.

1 Introduction

Mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ are called vectorial Boolean or (n, m)-functions. Any such function $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ can be represented in the form

$$F(x) = (f_1(x), f_2(x), \ldots, f_m(x)), \ x \in \mathbb{F}_2^n$$

where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \ldots, m$, are called *coordinate (Boolean) functions* of F and non-zero linear combinations of its coordinates $c \cdot F$ ($c \in \mathbb{F}_2^m \setminus \{\mathbf{0}_m\}$) are termed as *component functions*. When n is odd, (n, n)-functions that offer optimal resistance against both linear and differential cryptanalysis [13, 24] are called *almost bent* (AB) functions. There are a few known infinite families of AB functions and their complete classification seems to be elusive,

*University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: amar.bapic@famnit.upr.si
†University of Primorska, FAMNIT, Koper, Slovenia, e-mail: samir.hodzic@famnit.upr.si
‡University of Primorska, FAMNIT & IAM, Koper, Slovenia, e-mail: enes.pasalic6@gmail.com

see for instance [9] for the list of known ones. Another combinatorial object of particular importance in cryptography, coding and design theory, is a class of vectorial bent functions having the property that all the component functions are *bent* which are characterized by a unique feature of having a (uniform) flat Walsh spectrum. Nevertheless, it was shown by Nyberg [26] that vectorial bent functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ may only exist when $m \leq n/2$ and n is necessarily even.

Even though there is an extensive research on both these classes of functions, so far there has been no explicit connection between them. The main purpose of this article is to establish some (partial) connections and indicate the possibility of relating these structures through so-called duals of Boolean functions. The concept of dual was originally defined for bent functions but later it was generalized to the so-called plateaued Boolean functions. Employing the notion of dual of plateaued functions introduced in [20, 21], we provide some theoretical results that indicate certain regularity in the dual space of AB functions. More precisely, as already indicated in [20, 21], defining a dual of an s-plateaued function f on $\mathbb{F}_2^n$ (whose Walsh spectral values are in the set $\{0, \pm 2^{\frac{n+s}{2}}\}$) which distinguishes the signs of non-zero spectral values, conveys more information about a given function. Indeed, if we alternatively use the standard dual (which distinguishes zero and nonzero spectral values) in the quadratic case the dual functions become only trivial.

It is well-known that the class of Gold functions [19], defined in the univariate form over $\mathbb{F}_{2^n}$ as $F(x) = x^d$, with $d = 2^i+1$ and $\gcd(i, n) = 1$ for odd n, are AB functions. It was proved by Dobbertin (as reported in [9]) that all power APN functions are necessarily permutations in odd dimension, and 3-to-1 in even dimension. There has been an extensive research regarding the so-called CCZ equivalence (introduced in [10] and later named CCZ-equivalence in [4]) of known AB functions; and in particular the quadratic case received a lot of attention [1, 2, 4, 7, 17, 18]. This class of functions also exhibits nice combinatorial, algebraic or graph theoretic properties, though these features are generally non-constructive and to the best of our knowledge have not been helpful in specifying new classes of AB functions [3, 4, 7, 17, 18] Now, if F is represented as $F = (f_1, \ldots, f_n)$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, all the nonzero linear combinations of f_i (components of F) are quadratic semi-bent functions, thus their Walsh spectral values belong to $\{0, \pm 2^{\frac{n+1}{2}}\}$. Quite some research has been done in the field of quadratic semi-bent Boolean functions and for more details we refer to e.g. [25, 8, 14, 15]. Qu *et al.* [27] proved that all quadratic Boolean functions, as well as Maiorana-McFarland and partial spread bent functions can be represented as the sum of two bent functions. It is also known that all quadratic bent Boolean functions belong to the Maiorana-McFarland class of bent functions.

Leander and McGuire [23] considered the problem of constructing bent from semi-bent functions. In particular, it has been shown that two n-variable functions g and h (n odd) are semi-bent with complementary Walsh supports ($S_h \cap S_g = \emptyset$) if and only if the $(n+1)$-variable function $x \mapsto f(x, x_{n+1}) = g(x) + x_{n+1}h(x),\ x \in \mathbb{F}_2^n,\ x_{n+1} \in \mathbb{F}_2$ is bent. It is also known that the restrictions of an n-variable bent function to any hyperplane and to the complement of this hyperplane (viewed as $(n-1)$-Boolean functions) are semi-bent. For more details on the properties of semi-bent functions and their construction we refer to [25].

Because the components of Gold AB mappings are quadratic Boolean functions, their Walsh supports (a subset of $\mathbb{F}_2^n$ corresponding to nonzero spectral values) forms flats in $\mathbb{F}_2^n$ of even dimension, see [11]. This implies that the standard dual (which distinguishes the

zero and nonzero Walsh values) corresponds to an affine function. On the other hand, if we focus on the alternative definition of a dual, the situation is quite different. Since in the case of AB functions defined on $\mathbb{F}_2^n$, the cardinality of Walsh support of its component functions (which are all semi-bent) is exactly 2^{n-1}. Consequently, their duals can be defined on the ambient space $\mathbb{F}_2^{n-1}$ using some ordering (commonly lexicographic) to map bijectively the Walsh support as a subset of $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$, see [20, 21] and Section 3.

Moreover, for Gold AB functions which are quadratic, the fact that the Walsh supports of its component functions are affine subspaces implies (using the result in [20]) that their corresponding duals on $\mathbb{F}_2^{n-1}$ are bent functions. Hence, any Gold function $F = (f_1, \ldots, f_n)$ will give rise to a set of dual bent functions $\{f_1^*, \ldots, f_n^*\}$, where each $f_i^* : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$, and we prove that each f_i^* is necessarily quadratic, cf. Proposition 3.2. Moreover, these dual bent functions may build vectorial bent functions which we also confirm through simulations. Unfortunately, there is no clear structure which would indicate the choice of $\{f_1^*, \ldots, f_k^*\}$, where $k \leq (n-1)/2$, so that $F^* = (f_1^*, \ldots, f_k^*)$ is vectorial bent. This is especially true when the output bent dimension is maximal, thus when $k = (n-1)/2$, in which case such vectorial bent functions do not always exist. In this direction, considering quadratic semi-bent functions on $\mathbb{F}_2^n$, we derive a necessary and sufficient condition which ensures the bentness of the linear combinations of $f_1^*, \ldots, f_n^*$. This is achieved through a useful transform that acts on the Walsh spectrum of dual functions, but unfortunately the bent condition regarding the linear combinations of duals is non-constructive.

In the second part of this article, we further investigate the structure of the corresponding Walsh supports in the case of quadratic AB functions. Even though these Walsh supports are affine hyperplanes, the dimension of their intersection and the properties of the restrictions of dual functions have not been analyzed yet. More importantly, we consider the conditions imposed on dual bent functions (and their restrictions), say f^* and g^* on $\mathbb{F}_2^{n-1}$, so that the corresponding semi-bent functions f and g on $\mathbb{F}_2^n$ have the property that $f + g$ is again semi-bent. We provide a necessary and sufficient condition that $f + g$ is bent, which heavily depends on the properties of the restrictions of duals. However, using the established facts in this article, we could for the first time provide the design of quadratic AB functions in the spectral domain by identifying (using computer simulations) suitable sets of bent dual functions which give rise to possibly new quadratic AB functions in a generic manner. Using a simple non-exhaustive search for suitable sets of defining bent duals $f_1, \ldots, f_5$ on $\mathbb{F}_2^4$ we could easily identify 60 quadratic AB functions $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$. It turns out that all these functions are CCZ-equivalent to the Gold AB function but none of these functions is a permutation. On the other hand, when $n = 7$, the same approach provides several AB functions which are not CCZ-equivalent to Gold functions.

The rest of this article is organized as follows. In Section 2, we give some basic definitions related to Boolean functions. Using an alternative definition of a dual function of semi-bent functions, in Section 3 we provide a theoretical treatment concerning vectorial bentness of the dual functions. In Section 4, we consider the structure of dual bent functions and derive the necessary and sufficient conditions that two quadratic dual bent functions on $\mathbb{F}_2^{n-1}$ actually specify two quadratic semi-bent functions on $\mathbb{F}_2^n$ whose sum is again semi-bent. The design of semi-bent functions in the spectral domain is further discussed in Section 5, where we identify many quadratic AB functions by specifying suitable bent duals. Some concluding remarks are given in Section 6.

2 Definitions and terminology

The vector space $\mathbb{F}_2^n$ is the space of all n-tuples $x = (x_1, \ldots, x_n)$, where $x_i \in \mathbb{F}_2$. The all-zero vector is denoted by $\mathbf{0}_n$. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $\mathbb{F}_2^n$, the usual dot product over $\mathbb{F}_2$ is defined as $x \cdot y = x_1 y_1 \oplus \cdots \oplus x_n y_n$. The weight $\mathrm{wt}(x)$ of $x \in \mathbb{F}_2^n$ is computed as $\mathrm{wt}(x) = \sum_{i=1}^{n} x_i$. By "$\sum$" we denote the integer sum (without modulo evaluation), whereas "$\bigoplus$" denotes the sum evaluated modulo two.

The set of all Boolean functions in n variables, which is the set of mappings from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, is denoted by $\mathcal{B}_n$. The set of affine functions in n variables is given by $\mathcal{A}_n = \{a \cdot x \oplus b : a \in \mathbb{F}_2^n,\ b \in \{0,1\}\}$, and similarly $\mathcal{L}_n = \{a \cdot x : a \in \mathbb{F}_2^n\} \subset \mathcal{A}_n$ denotes the set of linear functions.

The *Walsh-Hadamard transform* (WHT) of a Boolean function f in n variables, and its inverse WHT, at any point $u \in \mathbb{F}_2^n$ are defined, respectively, by

$$W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x) \oplus u \cdot x}, \tag{1}$$

$$(-1)^{f(x)} = 2^{-n} \sum_{u \in \mathbb{F}_2^n} W_f(u) (-1)^{u \cdot x}. \tag{2}$$

The sequence of the 2^n *Walsh coefficients* given by (1), as u goes through $\mathbb{F}_2^n$ is called the *Walsh spectrum* of f, denoted by

$$\mathcal{W}_f = (W_f(u_0), \ldots, W_f(u_{2^n-1})),$$

where $u_0, \ldots, u_{2^n-1} \in \mathbb{F}_2^n$ are ordered lexicographically.

For an arbitrary Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$, the set of its values on $\mathbb{F}_2^n$ (*the truth table*) is defined as $T_f = (f(0, \ldots, 0, 0), f(0, \ldots, 0, 1), \ldots, f(1, \ldots, 1, 1))$. The corresponding (± 1)-*sequence of* f is defined as $\chi_f = ((-1)^{f(0,\ldots,0,0)}, (-1)^{f(0,\ldots,0,1)}, \ldots, (-1)^{f(1,\ldots,1,1)})$. A class of Boolean functions on $\mathbb{F}_2^n$ characterised by the property that their Walsh spectra is three-valued (more precisely taking values in $\{0, \pm 2^{\frac{n+s}{2}}\}$ for a positive integer $s < n$) are called *s-plateaued* functions [28]. In case $s = 1$ ($s = 2$) for n odd (n even), the functions are called *semi-bent*. For a bent Boolean function f defined on $\mathbb{F}_2^n$, its *dual* f^* is defined as a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, for which it holds that

$$(-1)^{f^*(x)} = 2^{-\frac{n}{2}} W_f(x), \quad x \in \mathbb{F}_2^n.$$

A standard way of defining the dual $\tilde{f} : \mathbb{F}_2^n \to \mathbb{F}_2$ of an s-plateaued Boolean function f on $\mathbb{F}_2^n$ is as follows:

$$\tilde{f}(x) = 2^{-\frac{n+s}{2}} |W_f(x)|, \quad x \in \mathbb{F}_2^n. \tag{3}$$

The *Sylvester-Hadamard* matrix of size $2^k \times 2^k$, is defined recursively as:

$$H_1 = (1),\ H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ H_{2^k} = \begin{pmatrix} H_{2^{k-1}} & H_{2^{k-1}} \\ H_{2^{k-1}} & -H_{2^{k-1}} \end{pmatrix}. \tag{4}$$

The i-th row of H_{2^k} we denote by $H_{2^k}^{(i)}$ ($i \in [0, 2^k - 1]$). Note that $H_{2^k}^{(i)} = ((-1)^{u_i \cdot x_0}, \ldots, (-1)^{u_i \cdot x_{2^k-1}}) = \chi_\ell$ ($x_j \in \mathbb{F}_2^k$) is a (± 1)-sequence of a linear function $\ell : \mathbb{F}_2^k \to \mathbb{F}_2$, where $\ell(x) = u_i \cdot x$ ($u_i, x \in \mathbb{F}_2^k$).

Boolean functions f and g in n variables are extended affine equivalent (EA-equivalent) if there exists a non-singular $n \times n$ matrix A over $\mathbb{F}_2$, binary vectors b and c of length n, and a constant $\lambda \in \mathbb{F}_2$, such that

$$g(x) = f(Ax \oplus b) \oplus c \cdot x \oplus \lambda,\ x \in \mathbb{F}_2^n,$$

where with Ax we denote matrix multiplication. only when considering affine equivalence, otherwise we use the standard notation for the dot product.

3 Vectorial bentness of duals for Gold-like functions

In this section, we analyse the duals of the Gold AB function $F(x) = x^d$ on $\mathbb{F}_2^n$ ($d = 2i + 1$, $\gcd(i, n) = 1$, n odd). For any nonzero $v \in \mathbb{F}_2^n$, we use $F_v(x) = v \cdot F(x)$, to denote the component functions of F. We notice that the property of being AB is characterized by the fact that all the component functions F_v are semi-bent.

In [11], it was proved that for any n, the Walsh support of any quadratic function on $\mathbb{F}_2^n$ is a flat on $\mathbb{F}_2^n$ of even dimension. Since all Gold functions are quadratic, the following proposition summarizes these observations and includes the Gold AB functions as a special case.

Proposition 3.1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an AB power mapping. Suppose that the Walsh supports S_i of the component functions F_v of F are affine hyperplanes on $\mathbb{F}_2^n$. Then the duals $\tilde{F}_v$ of the component functions F_v are linear functions on $\mathbb{F}_2^n$.*

The classical definition of a dual that we used above does not take into account the signs of Walsh coefficients. Therefore, another definition of a dual for an s-plateaued function f is introduced in [20], and it is described as follows.

With $S_f = \{\omega \in \mathbb{F}_2^n : W_f(\omega) \neq 0\}$ we denote the Walsh support of the function f. Its dual function f^* on S_f of cardinality 2^{n-s} is defined as $f^* : S_f \to \mathbb{F}_2$ by

$$W_f(\omega) = 2^{\frac{n+s}{2}}(-1)^{f^*(\omega)}, \tag{5}$$

for $\omega \in S_f$. To specify the dual function as $\overline{f}^* : \mathbb{F}_2^{n-s} \to \mathbb{F}_2$, we use the concept of the *lexicographic ordering*. That is, a subset $E = \{e_0, \ldots, e_{2^{n-s}-1}\} \subset \mathbb{F}_2^n$ is ordered lexicographically if $|e_i| < |e_{i+1}|$ for any $i \in [0, 2^{n-s} - 2]$, where $|e_i|$ denotes the integer representation of $e_i \in \mathbb{F}_2^n$. More precisely, for $e_i = (e_{i,1}, \ldots, e_{i,n})$ we have $|e_i| = \sum_{j=1}^{n} e_{i,j} 2^{n-j}$, thus having the most significant bit of e_i on the left-hand side. Now to define $f^* : S_f \to \mathbb{F}_2$ as a function from $\mathbb{F}_2^{n-s}$ to $\mathbb{F}_2$, we firstly impose an ordering on S_f as $S_f = z \oplus E = \{\omega_0, \ldots, \omega_{2^{n-s}-1}\}$ ($z \in S_f$), where E is lexicographically ordered and $\omega_i = z \oplus e_i$ ($i = 0, \ldots, 2^{n-s} - 1$). For instance, let an affine subspace $S_f \subset \mathbb{F}_2^3$ be given as

$$S_f = \{(0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1)\}.$$

By fixing $z = (0, 1, 1) \in S_f$, we have that the lexicographically ordered linear subspace E is given by

$$E = \{e_0, e_1, e_2, e_3\} = \{(0, 0, 0), (0, 0, 1), (1, 1, 0), (1, 1, 1)\},$$

and consequently S_f is "ordered" as $S_f = \{\omega_0, \omega_1, \omega_2, \omega_3\} = \{(0,1,1),(0,1,0),(1,0,1),(1,0,0)\}$.

By having S_f represented as $S_f = z \oplus E$, we can make a direct correspondence between $\mathbb{F}_2^{n-s}$ and S_f through E so that for the lexicographically ordered space $\mathbb{F}_2^{n-s} = \{x_0, x_1, \ldots, x_{2^{n-s}-1}\}$, we have

$$f^*(\omega_j) = f^*(z \oplus e_j) = \overline{f}^*(x_j), \quad x_j \in \mathbb{F}_2^{n-s},\ e_j \in E,\ j \in [0, 2^{n-s}-1]. \tag{6}$$

In the sequel, whenever we use this definition of dual of an s-plateaued function $f \in \mathcal{B}_n$, the notation $\overline{f}^*$ refers to a function defined on $\mathbb{F}_2^{n-s}$.

3.1 Alternative duals of Gold AB functions

Let us consider an AB function $F = (f_1, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ whose coordinate (semi-bent) functions f_i are all quadratic. From [11, Subsection 3.3.] it follows that their Walsh supports are affine hyperplanes (flats of dimension $n-1$). Following the result of Hodžić *et al.* [20] it is known that if the Walsh support S_f of a semi-bent bent function f is a flat in $\mathbb{F}_2^n$ (n odd), then f is a semi-bent and only if the dual $\overline{f}^*$ is bent on $\mathbb{F}_2^{n-1}$.

In the context of a vectorial AB function $F = (f_1, \ldots, f_n)$, we have that the definition of f_i^* as a function on $\mathbb{F}_2^{n-1}$ depends on the ordering of $S_{f_i} = z_i \oplus E_i \subset \mathbb{F}_2^n$, which is imposed by choice of the vector $z_i \in S_{f_i}$ and the lexicographic ordering of E_i. For different choices of $z_i \in S_{f_i}$, we actually have that the same dual f_i^* imposes different bent functions $\overline{f}_i^* : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$. Note that by [20, Theorem 3.1-(*ii*)] all these duals are bent functions. However, it is not clear what is happening with linear combinations of these functions. Therefore, we are interested in the following question:

Q1: Let $F = (f_1, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a quadratic AB function, where S_{f_i} are flats in $\mathbb{F}_2^n$. For which choice of $z_i \in S_{f_i}$ in the representation of $S_{f_i} = z_i \oplus E_i$ we have that the corresponding duals $\overline{f}_i^* : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ build a vectorial bent function $G = (\overline{f}_{i_1}^*, \ldots, \overline{f}_{i_t}^*) : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^t$ for some integers $1 \le i_1 < \ldots < i_t \le n$ $(1 \le t \le n)$?

Remark 1. *As noted in [11, Subsection 3.3.], the Walsh support of any quadratic function on $\mathbb{F}_2^n$ is a flat of $\mathbb{F}_2^n$ of even dimension. Conversely, any flat of $\mathbb{F}_2^n$ of even dimension is the Walsh support of a quadratic function. However, we note that there the exist plateaued functions with linear/affine Walsh supports which are not quadratic (cf. [21, Example 3.1]).*

In order to address the previous question, our goal is to analyse the linear combinations of duals $\overline{f}_i^*$ and the relation between the Walsh supports S_{f_i}. Firstly, we start by considering the sums of two functions $\overline{f}_i^* \oplus \overline{f}_j^*$, $1 \le i < j \le n$.

We recall that for a function $h(x) = f(x) \oplus g(x)$ defined on $\mathbb{F}_2^n$, by [15, Theorem 2.17.5] we have that

$$W_h(v) = 2^{-n} \sum_{x \in \mathbb{F}_2^n} W_f(x) W_g(x \oplus v),\ v \in \mathbb{F}_2^n. \tag{7}$$

Being motivated with this formula, we introduce the following notation. Let $f_1, \ldots, f_n : \mathbb{F}_2^n \to \mathbb{F}_2$ be semi-bent and $\overline{f}_1^*, \ldots, \overline{f}_n^* : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ their corresponding duals. For $W_i^* := W_{\overline{f}_i^*}$ and $W_j^* := W_{\overline{f}_j^*}$, we define

$$\Pi_{ij}(x) = 2^{-\frac{n-1}{2}} W_i^*(x) W_j^*(x),\ x \in \mathbb{F}_2^{n-1}. \tag{8}$$

Since the duals are bent, we have that $|W_i^*(x)| = |W_j^*(x)| = 2^{\frac{n-1}{2}}$, which implies that $\Pi_{ij}(x) = \pm 2^{\frac{n-1}{2}}$, for all $x \in \mathbb{F}_2^{n-1}$. Furthermore, for the coefficients $\Pi_{ij}(x)$ we can define their inverses $\Pi_{ij}^{-1}(x)$ as

$$\Pi_{ij}^{-1}(x) = 2^{-(n-1)} \sum_{y \in \mathbb{F}_2^{n-1}} \Pi_{ij}(y)(-1)^{x \cdot y},\ x \in \mathbb{F}_2^{n-1}. \tag{9}$$

We are interested in the sequence of coefficients $\{\Pi_{ij}(x_0), \ldots, \Pi_{ij}(x_{2^{n-1}-1})\}$ (with $\{x_0, \ldots, x_{2^{n-1}-1}\}$ representing lexicographically ordered $\mathbb{F}_2^{n-1}$). In this context, we would like to see whether some of these sequences (for some i and j) are corresponding to some bent functions defined on $\mathbb{F}_2^{n-1}$ (n odd). We introduce the following notation.

Spectral notation: Suppose we are given a sequence of integers $\mathcal{W} = (w_0, w_1, \ldots, w_{2^n-1})$ ($-2^n \leq w_i \leq 2^n$), which is not necessarily a Walsh spectrum of a Boolean function. In accordance to (2), we denote its inverse as $\mathcal{W}^{-1} = (w'_0, w'_1, \ldots, w'_{2^n-1})$, where

$$w'_k = 2^{-n} \sum_{i=0}^{2^n-1} w_i \cdot (-1)^{u_k \cdot x_i},\ 0 \leq k \leq 2^n - 1,$$

$u_k, x_i \in \mathbb{F}_2^n$ ordered lexicographically. With respect to this notation, we note the following:

- If for all $k \in \{0, 1, \ldots, 2^n - 1\}$ we have that $|w'_k| = 1$, then there exists some Boolean function f defined on $\mathbb{F}_2^n$ for which $w_i = W_f(u_i)$ ($u_i \in \mathbb{F}_2^n$), i.e., $\mathcal{W} = \mathcal{W}_f$.
- In addition to the previous comment, if n is even and all the values of $\mathcal{W}$ are $\pm 2^{\frac{n}{2}}$, the corresponding function f is bent.

In the following example, we show that certain sequences $\{\Pi_{ij}(x) : x \in \mathbb{F}_2^{n-1}\}$, depending on the indices i and j, actually correspond to some bent functions defined on $\mathbb{F}_2^{n-1}$, for a given Gold AB function F.

Example 3.1. *Let us consider the Gold function $F(x) = x^d$ defined on $\mathbb{F}_2^n$, where $(n, d) = (5, 5)$. In Table 1 and 2 we give the products $\Pi_{ij}(x)$ and their inverses $\Pi_{ij}^{-1}(x)$, where $1 \leq i < j \leq 5$ and $x \in \mathbb{F}_2^5$. We notice that for the pairs of indices $(i, j) \in \{(1, 2), (2, 3), (8, 5)\}$, it holds that $\Pi_{ij}^{-1}(x)$ are equal to ± 1 for all $x \in \mathbb{F}_2^5$. Notice that for $(n, d) = (5, 5)$ there are exactly three pairs $(\overline{f_i^*}, \overline{f_j^*})$ of bent vectorial functions mapping from $\mathbb{F}_2^4 \to \mathbb{F}_2^2$. The coordinates $\{i, j\}$ for which $\overline{f_{ij}^*} = \overline{f}_i^* \oplus \overline{f}_j^*$ is bent correspond to the coordinates for which the inverses $\Pi_{ij}^{-1}(x)$ have values ± 1 (Table 2). We obtained the same results for $(n, d) = (5, 3)$ and $(n, d) = (7, 9)$.*

Before we state the main results related to the previous observations, we provide the following two technical results. later.

Lemma 3.1. *Let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a bent Boolean function (n is even).*

(a) *The derivatives $\Delta_a f$, $a \neq \mathbf{0}$, are all distinct.*

(b) *Suppose that for all $a \in \mathbb{F}_2^{n*}$ the derivatives of f are affine of the form $\Delta_a f(x) = u_a \cdot x \oplus c_a$, where $u_a \in \mathbb{F}_2^n$, $c_a \in \mathbb{F}_2$. If $\Delta_a f \neq \Delta_b f$, then $u_a \neq u_b$.*

i	j	$\Pi_{ij}(x),\ x \in \mathbb{F}_2^{n-1}$
1	2	$(8,8,8,-8,8,8,-8,8,-8,8,-8,-8,-8,8,8,8)$
1	3	$(8,8,8,-8,8,-8,8,8,-8,-8,-8,8,-8,8,-8,-8)$
1	4	$(8,8,8,-8,8,8,-8,8,8,-8,-8,-8,-8,8,-8,-8)$
1	5	$(8,-8,-8,8,8,-8,-8,8,8,8,-8,-8,8,8,-8,-8)$
2	3	$(8,8,8,8,8,-8,-8,8,8,-8,8,-8,8,8,-8,-8)$
2	4	$(8,8,8,8,8,8,8,8,8,-8,-8,8,8,8,8,-8,-8)$
2	5	$(8,-8,-8,-8,8,-8,8,8,-8,8,8,8,-8,8,-8,-8)$
3	4	$(8,8,8,8,8,-8,-8,8,-8,8,8,-8,8,8,8,8)$
3	5	$(8,-8,-8,-8,8,8,-8,8,-8,-8,8,-8,-8,8,8,8)$
4	5	$(8,-8,-8,-8,8,-8,8,8,8,-8,8,8,-8,8,8,8)$

Table 1: Products of the Walsh transforms W_i^* and W_j^* for $(n,d) = (5,5)$ and $1 \le i < j \le 5$

i	j	$\Pi_{ij}^{-1}(x),\ x \in \mathbb{F}_2^{n-1}$
1	2	$(1,-1,1,-1,-1,1,1,-1,1,1,1,1,1,1,-1,-1)$
1	3	$(0,0,0,0,0,0,0,0,2,2,0,0,0,0,2,-2)$
1	4	$(0,0,2,0,0,2,0,0,2,0,0,0,0,0,0,-2)$
1	5	$(0,0,2,2,0,0,0,0,0,0,-2,2,0,0,0,0)$
2	3	$(1,1,1,1,1,1,-1,-1,1,-1,-1,1,1,-1,1,-1)$
2	4	$(2,0,0,0,0,0,-2,0,2,0,0,0,0,0,2,0)$
2	5	$(0,0,0,0,0,0,0,0,0,0,2,0,2,-2,0,2,0)$
3	4	$(2,0,0,0,0,0,0,-2,0,0,0,2,2,0,0,0)$
3	5	$(0,0,0,0,-2,2,0,0,0,0,2,2,0,0,0,0)$
4	5	$(1,1,-1,1,-1,1,1,1,-1,1,1,1,-1,-1,1,-1)$

Table 2: Inverses of the products given in Table 1

Proof. (a) Let $a \neq b$, and suppose that $\Delta_a f(x) = \Delta_b f(x)$. Then,

$$\begin{aligned}\Delta_a f(x) = \Delta_b f(x) &\Leftrightarrow f(x) \oplus f(x \oplus a) = f(x) \oplus f(x \oplus b)\\ &\Leftrightarrow f(x \oplus a) \oplus f(x \oplus b) = 0\\ &\Leftrightarrow f(x \oplus a) \oplus f(x \oplus a \oplus (a \oplus b)) = 0\\ &\Leftrightarrow \Delta_{a \oplus b} f(x \oplus a) = 0,\end{aligned}$$

for all $x \in \mathbb{F}_2^n$, which contradicts with the balance of the derivatives of $f(x \oplus a)$.

(b) Let $a \neq b$. Suppose that $\Delta_a f(x) = u \cdot x \oplus c_1$ and $\Delta_b f(x) = u \cdot x \oplus c_2$. We have that

$$\begin{aligned}&\Delta_a f(x) = u \cdot x \oplus c_1\\ \Leftrightarrow &\Delta_a f(x) = \Delta_b f(x) \oplus c_2 \oplus c_1\\ \Leftrightarrow &\Delta_{a \oplus b} f(x) = c_1 \oplus c_2.\end{aligned}$$

Similarly as in (a), we would obtain that $\Delta_{a \oplus b} f(x) = c_1 \oplus c_2$ for all $x \in \mathbb{F}_2^n$, which contradicts to the fact that derivatives $\Delta_{a \oplus b} f(x)$ (with $a \neq b$) are balanced. Hence, distinct derivatives have distinct linear terms. $\square$

Proposition 3.2. *Let $F = (f_1, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a Gold AB function. Then the duals $\overline{f}_i^* : \mathbb{F}_2^{n-1} \to \mathbb{F}_2$ of the coordinate functions $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$ are quadratic bent functions.*

Proof. Since F is a Gold AB function, for any non-zero vector $c \in \mathbb{F}_2^n$ we denote by $f(x) = c \cdot F(x)$, $x \in \mathbb{F}_2^n$. By relation (2) and $W_f(u) = 2^{\frac{n+1}{2}}(-1)^{f^*(u)}$, at any $u \in \mathbb{F}_2^n$ we have that

$$\sum_{\omega \in S_f} (-1)^{f^*(\omega) \oplus u \cdot \omega} = 2^{\frac{n-1}{2}}(-1)^{f(u)}, \tag{10}$$

where $S_f = z \oplus E$ is the Walsh support of f and $E = \{e_0, \ldots, e_{2^{n-1}-1}\}$ is a lexicographically ordered linear subspace of $\mathbb{F}_2^n$, thus any $\omega \in S_f$ can be written as $\omega = z \oplus e_i$ for some $e_i \in E$ and fixed $z \in S_f$. Using [20, Lemma 3.1], we have that $\mathcal{L}_{n-1} \subseteq T_\ell = \{(u \cdot e_0, \ldots, u \cdot e_{2^{n-1}-1}) : u \in \mathbb{F}_2^n\}$, which means that T_ℓ contains truth tables of all linear functions in $n-1$ variables $\mathcal{L}_{n-1}$ (clearly T_ℓ is a multi-set of linear functions). We recall that AB Gold functions have quadratic component (semi-bent) functions $c \cdot F$, and its Walsh supports are affine subspaces of dimension $n-1$ (see [11, Section 3.3.1]). By identifying a subset $R \subset \mathbb{F}_2^n$ of those u which give distinct linear functions in T_ℓ so that $\mathcal{L}_{n-1} = \{(u \cdot e_0, \ldots, u \cdot e_{2^{n-1}-1}) : u \in R\}$, then R is a linear subspace of dimension $n-1$.

Thus, for arbitrary vector $u \in R$ the relation (10) is equivalent to

$$\sum_{e \in E} (-1)^{f^*(z \oplus e) \oplus u \cdot e} = W_{\overline{f}^*}(\vartheta_u) = 2^{\frac{n-1}{2}}(-1)^{f(u) \oplus u \cdot z}, \quad (\vartheta_u \in \mathbb{F}_2^{n-1}),$$

where $\overline{f}^*(x_i) = f^*(z \oplus e_i)$ with $x_i \in \mathbb{F}_2^{n-1}$ denotes the dual of f viewed as a function on $\mathbb{F}_2^{n-1}$, and for $\vartheta_u \in \mathbb{F}_2^{n-1}$ it holds that $(\vartheta_u \cdot x_0, \ldots, \vartheta_u \cdot x_{2^{n-1}-1}) = (u \cdot e_0, \ldots, u \cdot e_{2^{n-1}-1})$. Furthermore, by [20, Theorem 3.1-(ii)] we have that $\overline{f}^*$ is a bent function in $n-1$ variables (n odd), and thus $W_{\overline{f}^*}(\vartheta_u) = 2^{\frac{n-1}{2}}(-1)^{g(\vartheta_u)}$ implies that g (being the dual of $\overline{f}^*$) is also a bent function on $\mathbb{F}_2^{n-1}$.

Using the inequality that relates the degrees of a bent function and its dual [8] (recall $\overline{f}^*, g$ are defined on $\mathbb{F}_2^{n-1}$), we have that

$$\frac{n-1}{2} - \deg(\overline{f}^*) \geq \frac{\frac{n-1}{2} - \deg(g)}{\deg(g) - 1}.$$

However, using the fact that g is actually a restriction of the function f to R and $W_{\overline{f}^*}(\vartheta_u) = 2^{\frac{n-1}{2}}(-1)^{g(\vartheta_u)} = 2^{\frac{n-1}{2}}(-1)^{f(u) \oplus u \cdot z}$, then f being quadratic implies that $\deg(g) \leq 2$. Note that here the term $u \cdot v$ in $f(u) \oplus u \cdot z$ is viewed as a linear function due to the fact that R is a linear space ([20, Lemma 3.1]). Clearly, g being bent means exactly that $\deg(g) = 2$. Thus, we have that $\frac{n-1}{2} - \deg(\overline{f}^*) \geq \frac{n-1}{2} - 2$, which gives that $\deg(\overline{f}^*) \leq 2$. Using the fact that $\overline{f}^*$ is bent, we have that $\deg(\overline{f}^*) = 2$, and thus we get that f^* is a quadratic bent function. □

3.2 Characterizing the bentness of the sum of bent duals

We again focus on quadratic semi-bent functions regardless of whether these constitute AB functions or not. Since their duals are quadratic bent functions it is natural to consider the problem of determining the conditions for preserving the bentness of the sum of these duals. The bentness of the function $\overline{f}_i^* \oplus \overline{f}_j^*$ is characterized with the following result.

Theorem 3.1. *Let $f_1, \ldots, f_k$ be quadratic semi-bent functions on $\mathbb{F}_2^n$, n odd, and $\overline{f}_1^*, \ldots, \overline{f}_k^*$ their corresponding duals on $\mathbb{F}_2^{n-1}$. Then, $\overline{f}_{ij}^* = \overline{f}_i^* \oplus \overline{f}_j^*$, $1 \leq i < j \leq k$, is bent if and only if $|\Pi_{ij}^{-1}(u)| = 1$ for all $u \in \mathbb{F}_2^{n-1}$.*

Proof. Let $u \neq 0$ be fixed.

$$\begin{aligned}
\Pi_{ij}^{-1}(u) &= 2^{-(n-1)} \sum_{x \in \mathbb{F}_2^{n-1}} \Pi_{ij}^*(x)(-1)^{x \cdot u} = 2^{-\frac{3}{2}(n-1)} \sum_{x \in \mathbb{F}_2^{n-1}} W_i^*(x) \cdot W_j^*(x)(-1)^{x \cdot u} \\
&= 2^{-\frac{3}{2}(n-1)} \sum_{x \in \mathbb{F}_2^{n-1}} \left(\sum_{y \in \mathbb{F}_2^{n-1}} (-1)^{f_i^*(y) \oplus y \cdot x} \right) \cdot \left(\sum_{z \in \mathbb{F}_2^{n-1}} (-1)^{f_j^*(z) \oplus z \cdot x} \right) (-1)^{x \cdot u} \\
&= 2^{-\frac{3}{2}(n-1)} \sum_{x,y,z \in \mathbb{F}_2^{n-1}} (-1)^{f_i^*(y) \oplus f_j^*(z)} (-1)^{x \cdot (y \oplus z \oplus u)} \\
&= 2^{-\frac{3}{2}(n-1)} \sum_{y,z \in \mathbb{F}_2^{n-1}} (-1)^{f_i^*(y) \oplus f_j^*(z)} \sum_{x \in \mathbb{F}_2^{n-1}} (-1)^{x \cdot (y \oplus z \oplus u)} \\
&= 2^{-\frac{n-1}{2}} \sum_{y \in \mathbb{F}_2^{n-1}} (-1)^{f_i^*(y) \oplus f_j^*(y \oplus u)} = 2^{-\frac{n-1}{2}} \sum_{y \in \mathbb{F}_2^{n-1}} (-1)^{f_i^*(y) \oplus f_i^*(y \oplus u) \oplus f_{ij}^*(y \oplus u)} \\
&= 2^{-\frac{n-1}{2}} \sum_{y \in \mathbb{F}_2^{n-1}} (-1)^{\Delta_u f_i^*(y) \oplus f_{ij}^*(y \oplus u)} = (\star)
\end{aligned}$$

Since the derivatives $\Delta_u f_i^*$ of the duals are all affine, we can write them as $\Delta_u f_i^* = a_u \cdot x \oplus c_u$ for some $a_u \in \mathbb{F}_2^{n-1}, c_u \in \mathbb{F}_2$. Thus,

$$\begin{aligned}
(\star) &= 2^{-\frac{n-1}{2}} \sum_{y \in \mathbb{F}_2^{n-1}} (-1)^{a_u \cdot y \oplus c_u \oplus f_{ij}^*(y \oplus u)} = 2^{-\frac{n-1}{2}} \sum_{x \in \mathbb{F}_2^{n-1}} (-1)^{a_u \cdot (x \oplus u) \oplus c_u \oplus f_{ij}^*(x)} \\
&= 2^{-\frac{n-1}{2}} \sum_{x \in \mathbb{F}_2^{n-1}} (-1)^{a_u \cdot x \oplus (a_u \cdot u \oplus c_u) \oplus f_{ij}^*(x)} = 2^{-\frac{n-1}{2}} \cdot (-1)^{a_u \cdot u \oplus c_u} \sum_{x \in \mathbb{F}_2^{n-1}} (-1)^{a_u \cdot x \oplus f_{ij}^*(x)},
\end{aligned}$$

so, for all $u \neq 0$,

$$\Pi_{ij}^{-1}(u) = \pm 2^{-\frac{n-1}{2}} \cdot W_{f_{ij}^*}(a_u). \tag{11}$$

If $u = 0$, then

$$\Pi_{ij}^{-1}(0) = 2^{-(n-1)} \sum_{x \in \mathbb{F}_2^{n-1}} \Pi_{ij}(x) \overset{(8),(9)}{=} 2^{-\frac{n-1}{2}} W_{f_{ij}^*}(0) \tag{12}$$

From Lemma 3.1, we know that all the derivatives are distinct and have distinct linear terms. That is, if u goes through $\mathbb{F}_2^{n-1}$, then a_u will also go through the whole vector space, with possibly a different ordering. Hence, from (11) and (12), it follows:

$$|\Pi_{ij}^{-1}(u)| = 1, \forall u \in \mathbb{F}_2^{n-1} \Leftrightarrow |W_{f_{ij}^*}(a_u)| = 2^{\frac{n-1}{2}}, \forall a_u \in \mathbb{F}_2^{n-1}.$$

□

Corollary 1. *Let $f_1, \ldots, f_k$ be quadratic semi-bent functions on $\mathbb{F}_2^n$, n odd, and $\overline{f}_1^*, \ldots, \overline{f}_k^*$ their corresponding duals on $\mathbb{F}_2^{n-1}$. Then, $\overline{f}^*_{i_1 \ldots i_l} = \overline{f}^*_{i_1} \oplus \cdots \oplus \overline{f}^*_{i_l}$, $\{i_1, \ldots, i_l\} \subseteq \{1, \ldots, k\}$, is bent if and only if $|\Pi^{-1}_{i_1 \ldots i_l}(u)| = 1$, for all $u \in \mathbb{F}_2^{n-1}$.*

Proof. We prove the statement with induction over l. For $l = 2$ the statement follows from Theorem 3.1. Let us suppose that the statement holds for $l - 1$. We have that

$$\overline{f}^*_{i_1 \ldots i_l} = \overline{f}^*_{i_1} \oplus \ldots \oplus \overline{f}^*_{i_l} = \overline{f}^*_{i_1 \ldots i_{l-1}} \oplus \overline{f}^*_{i_l}.$$

Using Theorem 3.1 and the inductive hypothesis the result follows. □

Corollary 2. *Let $F(x) = x^d$, $d = 2^i + 1$, $\gcd(i, n) = 1$, $1 \leq i \leq \frac{n-1}{2}$, be the Gold function defined on $\mathbb{F}_{2^n}$. With $f_1, \ldots, f_n$ we denote its coordinate functions and with $\overline{f}_1^*, \ldots, \overline{f}_n^*$ their corresponding duals defined on $\mathbb{F}_2^{n-1}$. Then, $\overline{f}^*_{ij} = \overline{f}^*_i \oplus \overline{f}^*_j$, $1 \leq i < j \leq n$, is bent if and only if $|\Pi^{-1}_{ij}(u)| = 1$, for all $u \in \mathbb{F}_2^{n-1}$.*

Proof. Since the coordinates of the Gold function are quadratic, their Walsh supports all affine hyperplanes of even dimension $n - 1$ [11] and since the duals are quadratic as well by Proposition 3.2, their derivatives must be affine [16, Proposition 2.1]. Thus the conditions of Theorem 3.1 are satisfied and the result follows. □

Similarly as Theorem 3.1 was stated in terms of bentness of $\overline{f}^*_{ij}$, we now consider the case when these sums are s-plateaued.

Theorem 3.2. *Let $f_1, \ldots, f_k$ be quadratic semi-bent functions on $\mathbb{F}_2^n$, n odd, and $\overline{f}_1^*, \ldots, \overline{f}_k^*$ their corresponding duals on $\mathbb{F}_2^{n-1}$. Then, $\overline{f}^*_{ij} = \overline{f}^*_i \oplus \overline{f}^*_j$, $1 \leq i < j \leq k$, is s-plateaued, $s \geq 2$ even, if and only if $|\Pi^{-1}_{ij}(u)| \in \{0, 2^{s/2}\}$ for all $u \in \mathbb{F}_2^{n-1}$.*

Proof. The proof follows directly from the assumptions of the theorem and the equalities (11) and (12). □

Remark 2. *Since quadratic functions are either bent or plateaued (those with 3 values in the spectrum) [12], Theorems 3.1 and 3.2 are providing the characterization of the sum of two bent duals $\overline{f}^*_i \oplus \overline{f}^*_j$, in terms of notation (8)-(9), obtained from quadratic semi-bent functions in odd dimension.*

3.3 Identifying bent spaces via duals of Gold AB components

In this section, we provide some observations regarding the maximum dimension of vectorial bent spaces obtained by considering the bent duals of Gold AB components. The main conclusion is that there is no obvious connection between the vectorial semi-bent space and its corresponding dual bent space. At least, it can be deduced that reaching the maximal dimension of a vectorial dual bent space, given by the Nyberg's bound, is not possible for larger ambient spaces.

Suppose that $F = (f_1, \ldots, f_n) : \mathbb{F}_2^n \to \mathbb{F}_2$ is a Gold AB function, and let

$$\beta_k = \#\{F^*_{i_1, \ldots, i_k} : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^k \mid F^*_{i_1, \ldots, i_k} \text{ is bent}\}$$

denote the number of bent k-vectorial Boolean functions $F^*_{i_1,\ldots,i_k} = (\overline{f}^*_{i_1}, \ldots, \overline{f}^*_{i_k}) : \mathbb{F}_2^{n-1} \to \mathbb{F}_2^k$, $\{i_1, \ldots, i_k\} \subset \{1, \ldots, n\}$, $\#\{i_1, \ldots, i_k\} \leq (n-1)/2$, composed of the bent duals $\overline{f}^*_1, \ldots, \overline{f}^*_n$. In Table 3, we give some computational results on β_k obtained using the mathematical software Sage.

Remark 3.1. *We note here that all bent functions $\overline{f}^*_i$ above are defined with respect to the lexicographically ordered $S_{f_i} = \{\omega_0, \ldots, \omega_{2^{n-1}-1}\}$ as $\overline{f}^*_i(x_j) = f^*_i(\omega_j)$ ($j \in [0, 2^{n-1}-1]$). The bentness of these functions holds due to [22, Proposition V.4] and [20, Theorem 3.1-(ii)], since by [22, Proposition V.4] we have that for the lexicographically ordered affine subspace $S_{f_i} = \{\omega_0, \ldots, \omega_{2^{n-1}-1}\}$ it holds that $E = \omega_0 \oplus S_{f_i} = \{\boldsymbol{0}_n, e_1, \ldots, e_{2^{n-1}-1}\}$ with $e_j = \omega_0 \oplus \omega_j$ ($j \in [0, 2^{n-1}-1]$) is ordered lexicographically.*

We use the abbreviation DNE=Does Not Exist for the cases where the number of bent coordinates is larger than Nyberg's bound. As shown in Table 3, bent vectorial Boolean

n	d	β_2	β_3	β_4	β_5
5	3	5	DNE	DNE	DNE
5	5	3	DNE	DNE	DNE
7	3	13	4	DNE	DNE
7	5	7	1	DNE	DNE
7	9	13	6	DNE	DNE
9	3	14	1	0	DNE
9	5	19	6	0	DNE
9	17	15	1	0	DNE
11	3	25	8	0	0
11	5	28	8	0	0
11	9	36	20	1	0
11	17	29	18	0	0
11	33	30	13	1	0

Table 3: Number of bent k-vectorial Boolean functions obtained from the duals of Gold AB coordinates

functions that reach the Nyberg's bound do not always exist (cf. the columns corresponding to β_4 and β_5). This motivates the following question.

Q2: What is the largest k for which a bent k-vectorial function $(\overline{f}^*_{i_1}, \ldots, \overline{f}^*_{i_k})$ exists? Does the choice of $z \in S_{f_i}$ in the definition of $\overline{f}^*_i$ affect the existence of these functions?

Example 3.2. *Let us consider $F(x) = x^5$ defined on $\mathbb{F}_{2^5}$. For each coordinate f_i of $F = (f_1, \ldots, f_5)$ we are able to define 16 bent functions $\overline{f}^*_{i,z}$ on $\mathbb{F}_2^4$ for a different choice of $z \in S_{f_i}$ via (6). The entry (i, j) in Table 4 represents the set of functions*

$$\{\overline{f}^*_{ij,\{z_i,z_j\}} = \overline{f}^*_{i,z_i} \oplus \overline{f}^*_{j,z_j} \ : \ z_i \in S_{f_i}, z_j \in S_{f_j}, \ 1 \leq i < j \leq 5\}.$$

We note that since there are 16 choices for z_i and z_j, there are maximally 256 possibilities for the functions $\overline{f}^*_{ij,\{z_i,z_j\}}$ for each pair (i, j).

(i,j)	β_2	(i,j)	β_2	(i,j)	β_2	(i,j)	β_2
$(1,2)$	256	$(2,3)$	256	$(3,8)$	0	$(8,5)$	256
$(1,3)$	0	$(2,8)$	0	$(3,5)$	0		
$(1,8)$	0	$(2,5)$	0				
$(1,5)$	0						

Table 4: Number of bent functions $\overline{f}^*_{ij,\{z_i,z_j\}}$ on $\mathbb{F}_2^4$

Comparing Tables 2 and 4, we observe that the duals of coordinates whose sum is bent, were not affected by the choice of the vector $z \in S_f$ in (6). Thus, the choice of z in the support does not affect the existence of bent vectorial Boolean functions. The same observations apply to other Gold AB functions in dimensions $n = 7$ and $n = 9$ for different β_k.

Regarding the question **Q1**, the observations presented in this section indicate that the bentness of linear combinations $\overline{f}^*_{i_1} \oplus \ldots \oplus \overline{f}^*_{i_k}$ (for some $i_j \in \{1, \ldots, n\}$) is not expected so easily, even if the functions $\overline{f}^*_i$ are quadratic. In the following section, we focus on the analysis of a sum of two semi-bent functions from the spectral point of view.

4 Characterizing semi-bentness in the spectral domain

In this subsection, we provide the spectral analysis of the sum of two quadratic semi-bent functions f and g (as components of an AB permutation) in odd number of variables, whose Walsh supports are affine subspaces. The case of non-quadratic semi-bent functions and the case when the Walsh supports are non-affine sets is left as an interesting topic for further investigation. The structure of this section is briefly summarized as follows:

We firstly show that if f and g are semi-bent such that $f \oplus g$ is semi-bent, then it necessarily holds that $\dim(S_f \cap S_g) = n - 2$, and thus it is not possible that $S_f = S_g$ or $S_f \cap S_g = \emptyset$ (Theorem 4.1). Based on this fact, we then show that $f \oplus g$ is semi-bent if and only if the functions $\varphi_u : S_f \setminus (S_f \cap S_g) \to \mathbb{F}_2$, if $u \in S_g$, and $\psi_u : S_f \cap S_g \to \mathbb{F}_2$, if $u \in \mathbb{F}_2^n \setminus S_g$, defined by

$$\varphi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega), \;\; \omega \in S_f \setminus (S_f \cap S_g),$$
$$\psi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega), \;\; \omega \in S_f \cap S_g,$$

are either balanced, or have weights $2^{n-3} \pm 2^{\frac{n-1}{2}-1}$ (Proposition 4.2). Here f^* and g^* are the duals of f and g respectively, defined by (5). We note that $\#(S_f \setminus (S_f \cap S_g)) = \#(S_f \cap S_g) = 2^{n-2}$. Furthermore, unlike in the case of (6), we are not concerned with the ordering of the $(n-2)$-dimensional affine subspaces $S_f \cap S_g$ and $S_f \setminus (S_f \cap S_g)$, since we are not able to fully analyze their structure further as Boolean functions defined on $\mathbb{F}_2^{n-2}$.

Remark 4.1. *Throughout the subsequent subsections, by "an affine subspace" we mean a proper coset of a linear subspace which does not contain the all-zero vector.*

We start with the following well-known result in linear algebra.

Proposition 4.1. *Let R and Q be two affine subspaces in $\mathbb{F}_2^n$ of dimension $n-1$. Then the following three cases occur:*

(i) R and Q are equal, i.e. $R = Q$.

(ii) R and Q are parallel, i.e. $R \cap Q = \emptyset$.

(iii) $\dim(R \cap Q) = n - 2$.

Let $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ (n odd) be two different semi-bent functions. For any vector $u \in \mathbb{F}_2^n$, we have the following computation:

$$\begin{aligned} W_{f\oplus g}(u) &= \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus g(x)\oplus u\cdot x} \overset{(2)}{=} 2^{-2n} \sum_{x\in\mathbb{F}_2^n} \sum_{\omega\in S_f} \sum_{z\in S_g} W_f(\omega) W_g(z) (-1)^{\omega\cdot x\oplus z\cdot x\oplus u\cdot x} \\ &= 2^{-2n} \sum_{\omega\in S_f} \sum_{z\in S_g} W_f(\omega) W_g(z) \sum_{x\in\mathbb{F}_2^n} (-1)^{x\cdot(\omega\oplus z\oplus u)} \\ &= \begin{cases} 2^{-n} \sum\limits_{\omega\in S_f:\ z=u\oplus\omega\in S_g} W_f(\omega) W_g(z), & u \in S_f \oplus S_g \\ 0, & u \notin S_f \oplus S_g. \end{cases} \end{aligned} \tag{13}$$

Applying Proposition 4.1 we have the following result.

Theorem 4.1. *Let $f, g, f\oplus g : \mathbb{F}_2^n \to \mathbb{F}_2$ (n odd) be semi-bent functions, whose Walsh supports are affine subspaces. Then:*

(i) It is not possible that $S_f = S_g$ or $S_f \cap S_g = \emptyset$, thus it necessarily holds that $\dim(S_f \cap S_g) = n - 2$.

(ii) It holds that $S_f \oplus S_g = \mathbb{F}_2^n$.

Proof. (i) Assume that $S_f \cap S_g = \emptyset$, then one of the sets S_f or S_g is a linear subspace (recall $\dim(S_f) = n - 1$), which contradicts the assumption that S_f and S_g are affine subspaces.

On the other hand, let us assume that $S_f = S_g$. By representing $S_f = S_g = v \oplus S$, for some linear subspace $S \subset \mathbb{F}_2^n$ ($\dim(S) = n - 1$) and $v \notin S$, we have that $S_f \oplus S_g = S$ and thus for every $u \notin S$ by relation (13) we have that $W_{f\oplus g}(u) = 0$. In addition, since $f \oplus g$ is balanced ($\mathbf{0}_n \notin S_{f\oplus g}$), then for $u = \mathbf{0}_n \in S$ we have that

$$W_{f\oplus g}(\mathbf{0}_n) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus g(x)} = 0.$$

Hence, we have that for at least $2^{n-1} + 1 = \#(\mathbb{F}_2^n \setminus S \cup \{\mathbf{0}_n\})$ vectors u it holds that $W_{f\oplus g}(u) = 0$. Using the fact that $|W_{f\oplus g}(u)| \in \{0, 2^{\frac{n+1}{2}}\}$ for all $u \in \mathbb{F}_2^n$, we have that

$$\sum_{u\in\mathbb{F}_2^n} W_{f\oplus g}^2(u) \leq (2^{n-1} - 1) \cdot 2^{n+1} = 2^{2n} - 2^{n+1} < 2^{2n},$$

which contradicts the Parseval's identity stating that $\sum_{u\in\mathbb{F}_2^n} W_{f\oplus g}^2(u) = 2^{2n}$. Therefore, it holds that $S_f = S_g$ is not possible. And finally, by Proposition 4.1-(iii) we have that $\dim(S_f \cap S_g) = n - 2$.

(ii) The fact that $S_f \oplus S_g = \mathbb{F}_2^n$ follows directly since $S_f \cup E = \mathbb{F}_2^n$ and $S_f \cap E = \emptyset$. $\square$

Theorem 4.1-(ii) implies that the second case in (13), that is the case when $u \notin S_f \oplus S_g$, never occurs. This motivates us to further investigate the relation (13) with respect to the Walsh supports S_f and S_g. The main goal now is to find a precise description of vectors $u \in \mathbb{F}_2^n$ and $\omega \in S_f$ for which $z = u \oplus \omega \in S_g$. Based on this analysis, we will later investigate the duals f^* and g^*.

Analyzing further (13): Let S_f and S_g be represented as

$$S_f = \tau \oplus E \text{ and } S_g = \mu \oplus T,$$

where $E, T \subset \mathbb{F}_2^n$ are linear subspaces and $\tau \notin E$, $\mu \notin T$. Since by Theorem 4.1-(i) we have that $S_f \cap S_g \neq \emptyset$ with $\dim(S_f \cap S_g) = n-2$, let $\Lambda \subset T$ be a set for which it holds that

$$\Lambda = S_f \cap T.$$

Clearly, the set Λ has also the property that $S_f = \Lambda \cup (S_f \cap S_g)$ and $\Lambda \cap (S_f \cap S_g) = \emptyset$. Since S_f, S_g are affine subspaces, it holds that $S_f \cap S_g$ is also a linear or affine space. Thus, by $\dim(S_f \cap S_g) = n-2$ we have that Λ is either a linear or affine space with dimension $n-2$. We distinguish the following two cases:

Case I: Let $u \in S_g = \mu \oplus T$. This means that u can be written as $u = \mu \oplus t_u$, for some $t_u \in T$. By $\Lambda = S_f \cap T$ we have that

$$u \oplus \omega = \begin{cases} \mu \oplus t_u \oplus \omega \in \mu \oplus T = S_g, & \text{when } \omega \in \Lambda, \\ \mu \oplus t_u \oplus (\mu \oplus t_\omega) \in T, & \text{when } \omega = \mu \oplus t_\omega \in S_f \backslash \Lambda = S_f \cap S_g. \end{cases} \tag{14}$$

Here, t_u and t_ω are some vectors from T used to represent the vectors u and $\omega \in S_f$. From (14) we have that $u \oplus \omega \in S_g$ only in the case when $\omega \in \Lambda$, which means that (13) can be further written as

$$\begin{aligned} W_{f \oplus g}(u) &= 2^{-n} \sum_{\omega \in \Lambda \subset S_f:\ z = u \oplus \omega \in S_g} W_f(\omega) W_g(z) \\ &= 2 \sum_{\omega \in \Lambda \subset S_f} (-1)^{f^*(\omega) \oplus g^*(u \oplus \omega)}, \end{aligned} \tag{15}$$

where in the last step we used $W_f(\omega) = 2^{\frac{n+1}{2}}(-1)^{f^*(\omega)}$ and $W_g(u \oplus \omega) = 2^{\frac{n+1}{2}}(-1)^{g^*(u \oplus \omega)}$. It is important to note that the value $g^*(u \oplus \omega)$ in (15) is well defined for every $\omega \in \Lambda$, since by (14) we have that $u \oplus \Lambda \subset S_g$ (recall that g^* is a mapping defined on S_g).

Case II: Let $u \in T = \mathbb{F}_2^n \setminus S_g$. Similarly, we have that

$$u \oplus \omega \in \begin{cases} T, & \text{when } \omega \in \Lambda, \\ S_g, & \text{when } \omega \in S_f \backslash \Lambda. \end{cases} \tag{16}$$

Consequently, by (16) the relation (13) can be written as

$$W_{f \oplus g}(u) = 2 \sum_{\omega \in S_f \backslash \Lambda} (-1)^{f^*(\omega) \oplus g^*(u \oplus \omega)}, \tag{17}$$

where $S_f \backslash \Lambda = S_f \cap S_g$.

To unify **Cases I** and **II**, we finally have that (13) (with respect to $u \in \mathbb{F}_2^n$) is given as

$$W_{f\oplus g}(u) = \begin{cases} 2 \sum\limits_{\omega \in \Lambda \subset S_f} (-1)^{f^*(\omega)\oplus g^*(u\oplus\omega)}, & u \in S_g,\ \Lambda = S_f \setminus (S_f \cap S_g), \\ 2 \sum\limits_{\omega \in S_f \backslash \Lambda = S_f \cap S_g} (-1)^{f^*(\omega)\oplus g^*(u\oplus\omega)}, & u \in T = \mathbb{F}_2^n \setminus S_g. \end{cases} \tag{18}$$

Remark 4.2. *In (18), we have that the semi-bentness of $f \oplus g$ depends on functions $f^*(\omega) \oplus g^*(u \oplus \omega)$, where ω are either from $\Lambda = S_f \setminus (S_f \cap S_g)$ or $S_f \backslash \Lambda = S_f \cap S_g$. Due to the influence of the vector $u \in \mathbb{F}_2^n$, it is not clear whether the function $g^*(u \oplus \omega)$ in (18) represents the restrictions of the dual g^* to $S_f \cap S_g$ and $S_g \setminus (S_f \cap S_g)$, or not.*

Assuming that $W_{f\oplus g}(u) \in \{0, \pm 2^{\frac{n+1}{2}}\}$ holds for all $u \in \mathbb{F}_2^n$, from (18) we conclude that

$$\sum_{\omega \in \Lambda \subset S_f} (-1)^{f^*(\omega)\oplus g^*(u\oplus\omega)}, \sum_{\omega \in S_g \backslash \Lambda} (-1)^{f^*(\omega)\oplus g^*(u\oplus\omega)} \in \{0, \pm 2^{\frac{n-1}{2}}\},\ \ \forall u \in \mathbb{F}_2^n.$$

Since $\dim(\Lambda) = \dim(S_g \backslash \Lambda) = n - 2$, this does not imply that the functions $\omega \in \Lambda \to f^*(\omega) \oplus g^*(u \oplus \omega)$ and $\omega \in S_f \backslash \Lambda \to f^*(\omega) \oplus g^*(u \oplus \omega)$ are semi-bent on $\mathbb{F}_2^{n-2}$. At least, we can provide the following characterization of these functions.

Proposition 4.2. *Let $f, g, f \oplus g : \mathbb{F}_2^n \to \mathbb{F}_2$ (n odd) be semi-bent functions, whose Walsh supports are affine subspaces. In addition, let S_g be represented as $S_g = \mu \oplus T$, where $T \subset \mathbb{F}_2^n$ is a linear subspace and $\mu \notin T$. Denoting by $\Lambda = S_f \cap T$ ($\dim(\Lambda) = n - 2$), it holds that the functions*

$$\varphi_u : \Lambda \to \mathbb{F}_2,\ \varphi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega)\ \text{ for }\ u \in S_g,$$
$$\psi_u : S_f \backslash \Lambda \to \mathbb{F}_2,\ \psi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega)\ \text{ for }\ u \in \mathbb{F}_2^n \setminus S_g,$$

are either balanced, or have weights $2^{n-3} \pm 2^{\frac{n-1}{2}-1}$.

Proof. One proves the statement by using the fact that $W_{f\oplus g}(u) \in \{0, \pm 2^{\frac{n+1}{2}}\}$, the relation (18), and the fact that for any Boolean function $g \in \mathcal{B}_m$ it holds that $wt(g) = 2^{m-1} - \frac{1}{2} W_g(\mathbf{0}_m)$. □

In the following example, we briefly indicate what kind of structure the function φ_u may possess (similarly one can consider the function ψ_u).

Example 4.1. *Let $F(x) = x^d$ ($d = 2^k + 1$, $gcd(n, k) = 1$, $k \leq (n-1)/2$) be a Gold AB function defined on $\mathbb{F}_{2^n}$ whose components are denoted by F_i and its corresponding Walsh support by S_i, $i \in \{1, \ldots, 2^n - 1\}$. Moreover, by F_i^* we denote the duals of F_i defined with (5).*

Since S_i are affine subspaces for all $i \in \{1, \ldots, 2^n - 1\}$, we can represent the affine subspace $\Lambda = \{\lambda_0, \ldots, \lambda_{2^{n-2}-1}\} = S_i \backslash (S_i \cap S_j) = S_i \backslash S_j$ ($1 \leq i < j \leq 2^n - 1$) as $\Lambda = \alpha + \Gamma$ with $\lambda_k = \alpha + \gamma_k$, where $\Gamma = \{\gamma_0, \ldots, \gamma_{2^{n-2}-1}\}$ is a lexicographically ordered $(n-2)$-dimensional

linear subspace. Clearly, Λ (and thus α and Γ) depends on indices i and j. Now, by defining the function $\varphi_{i,j,u} : S_i \setminus (S_i \cap S_j) \to \mathbb{F}_2$ as a function in $n-2$ variables as

$$\overline{\varphi}_{i,j,u}(x_k) = \varphi_u(\lambda_k) = \varphi_u(\alpha + \gamma_k) = F_i^*(\lambda_k) \oplus F_j^*(u \oplus \lambda_k), \;\; u \in S_j,$$

where $k \in [0, 2^{n-2}-1]$ and $\mathbb{F}_2^{n-2} = \{x_0, \ldots, x_{2^{n-2}-1}\}$ is lexicographically ordered. Using `Sage` *(for any d described above) we observe that for $n = 5$ the functions $\overline{\varphi}_{ij,u}$ are either linear or semi-bent, while for $n = 7, 9$ they are either semi-bent or 3-plateaued (the non-zero Walsh coefficients are $\pm 2^{\frac{(n-2)+3}{2}} = \pm 2^{\frac{n+1}{2}}$).*

Remark 4.3. *The previous example indicates that the functions φ_u and ψ_u seem to have a plateaued-like spectrum, at least for quadratic AB functions. However, due to the presence of the vector u in their definition, the properties of these functions remain unclear and thus a more rigorous theoretical analysis is required.*

5 Designing quadratic AB functions in the spectral domain

In this section, we specify a search technique for finding quadratic AB functions (the design being performed in the spectral domain), which turns out to be quite successful. More precisely, we demonstrate the existence of many different bent duals $(\tilde{f}_1, \ldots, \tilde{f}_n)$, used to specify the coordinate functions $f_1, \ldots, f_n$ of F, so that F is a quadratic AB function. For $n = 5$, the AB functions constructed in this way turn out to be CCZ-equivalent to Gold functions. Nevertheless, in this case, none of the found functions is a permutation which is the property of Gold AB monomials. On the other hand, when $n = 7$, the same approach provides several AB functions which are **not** CCZ-equivalent to Gold functions.

Notation: Throughout the section, we denote by $f_1, \ldots, f_n : \mathbb{F}_2^n \to \mathbb{F}_2$ and $F_i = v_i \cdot (f_1, \ldots, f_n)$ the coordinate and component functions, respectively, of a given Gold function, where $\mathbb{F}_2^n = \{v_0, v_1, \ldots, v_{2^n-1}\}$ is ordered lexicographically. The corresponding Walsh supports of F_i will be denoted by S_i. The Walsh support of a coordinate function f_i will be denoted by S_{f_i}.

In the following example, we observe that the cardinalities of intersections of the Walsh supports of component functions of $F(x) = x^5$, for $n = 5, 7, 9$, follow certain patterns.

Example 5.1. *Let $f_1, \ldots, f_5 : \mathbb{F}_2^5 \to \mathbb{F}_2$ be the coordinate function of the Gold function $F(x) = x^5 : \mathbb{F}_{2^5} \to \mathbb{F}_{2^5}$. We observe that the following intersections of k-tuples of the Walsh supports satisfy the following (with $1 \le i_1 < \cdots < i_k \le 5$)*

$$|\cap_{k=1}^{2} S_{f_{i_k}}| = 8, \qquad |\cap_{k=1}^{4} S_{f_{i_k}}| = 2,$$
$$|\cap_{k=1}^{3} S_{f_{i_k}}| = 4, \qquad |\cap_{i=1}^{5} S_{f_i}| = 1.$$

Hence, the cardinalities of these intersections are of the form 2^{5-m}, where the parameter m is the number of intersected Walsh supports. Similarly, one can verify that the same pattern holds for the remaining Gold AB functions when $n = 5, 7, 9$.

While Proposition 4.1 regards the dimension of intersection of two linear/affine subspaces of dimension $n-1$ (n odd), in the following result we describe the dimension of intersection of more than two affine subspaces.

Proposition 5.1. *Let $S_1, \ldots, S_n$ be affine subspaces in $\mathbb{F}_2^n$ of dimension $n-1$ such that $\dim(S_i \cap S_j) = n-2$ for all $1 \leq i < j \leq n$. With $\mathcal{S}_{i_1,\ldots,i_c} = S_{i_1} \cap \cdots \cap S_{i_c}$ we denote the intersection of $c \geq 2$ arbitrary (fixed) affine subspaces $S_{i_1}, \ldots, S_{i_c}$, where $1 \leq i_1 < \cdots < i_c \leq n$. Then*

$$\dim(\mathcal{S}_{i_1,\ldots,i_{c-1},i_c}) \in \{\dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}), \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) - 1\}. \tag{19}$$

Proof. We prove the statement by the mathematical induction. Using the given assumptions and Theorem 4.1 we have that $\dim(S_i \cap S_j) = n-2$ ($1 \leq i < j \leq n$), and thus (19) holds for $c = 2$. Suppose that (19) holds for some $c > 2$. In order to prove that (19) holds for some $c+1$, that is,

$$\dim(\mathcal{S}_{i_1,\ldots,i_c,i_{c+1}}) \in \{\dim(\mathcal{S}_{i_1,\ldots,i_c}), \dim(\mathcal{S}_{i_1,\ldots,i_c}) - 1\},$$

we compute the following:

$$\begin{aligned} n \geq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}} \oplus S_{i_c}) &= \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) + \dim(S_{i_c}) - \dim(\mathcal{S}_{i_1,\ldots,i_c}) \\ &\Rightarrow \dim(\mathcal{S}_{i_1,\ldots,i_c}) \geq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) + (n-1) - n \\ &\Rightarrow \dim(\mathcal{S}_{i_1,\ldots,i_c}) \geq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) - 1. \end{aligned}$$

On the other hand, $\mathcal{S}_{i_1,\ldots,i_{c-1},i_c} \subseteq \mathcal{S}_{i_1,\ldots,i_{c-1}}$ implies that $\dim(\mathcal{S}_{i_1,\ldots,i_{c-1},i_c}) \leq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}})$. Hence,

$$\dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) \geq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1},i_c}) \geq \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) - 1,$$

and thus it holds that

$$\dim(\mathcal{S}_{i_1,\ldots,i_{c-1},i_c}) \in \{\dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}), \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) - 1\},$$

which completes the proof. □

Referring to Example 5.1 and Proposition 5.1, we state the following conjecture that addresses the gold AB function of the form $F(x) = x^{2^s+1}$ ($n = 2k+1$, $1 \leq s \leq k$, $\gcd(s,n) = 1$), which specifies (19) more precisely.

Conjecture 1. *Let $f_1, \ldots, f_n$ be the coordinate functions of the Gold function $F(x) = x^{2^s+1}$ defined on $\mathbb{F}_{2^n}$, where $n = 2k+1$ and $1 \leq s \leq k$ with $\gcd(s,n) = 1$. Let also S_i denote the Walsh support of f_i, $i = 1, \ldots, n$. Let $\mathcal{S}_{i_1,\ldots,i_c} = S_{i_1} \cap \cdots \cap S_{i_c}$ be the intersection of c arbitrary (fixed) affine subspaces $S_{i_1}, \ldots, S_{i_c}$, where $1 \leq i_1 < \cdots < i_c \leq n$. Then, it holds that*

$$\dim(\mathcal{S}_{i_1,\ldots,i_c}) = \dim(\mathcal{S}_{i_1,\ldots,i_{c-1}}) - 1. \tag{20}$$

Remark 5.1. *We observe that intersection of the Walsh supports of the coordinate functions of $F(x) = x^{2^i+1}$ ($n = 2k+1$, $1 \leq i \leq k$, $\gcd(i,n) = 1$), for $n \in \{5, 7, 9, 11\}$, always satisfies the relation* (20)*. For a graphical representation, we refer to Figure 1 given in Appendix,*

cf. Section 6.1. On the other hand, for the quadratic AB function $F(x) = x^3 + Tr(x^9)$ [5] (CCZ-inequivalent to the Gold function for $n \geq 6$) for $n \in \{9, 11\}$, these intersections are not uniform as in the Gold case and they generally correspond to (19)*. A precise description of the intersection structure of the Walsh supports for different (in)equivalent AB functions is an interesting research challenge.*

5.1 Constructing AB functions on $\mathbb{F}_2^5$

In the following example, we construct five semi-bent functions using the so-called spectral approach which has been described by [21, Theorem 3.1]. We notice that any semi-bent function with linear/affine Walsh support necessarily has a bent dual (in lower number of variables).

Example 5.2. *With $T_1, \ldots, T_5$ we denote the truth tables of five bent functions in four variables. It turns out that these five bent functions (found by a computer search) will give rise to an AB function defined on $\mathbb{F}_2^5$.*

$$\begin{aligned}
T_1 &= (0,0,0,1,0,0,1,0,1,1,0,1,0,0,0,1)\\
T_2 &= (1,0,1,0,1,1,1,1,1,1,0,0,1,0,0,1)\\
T_3 &= (0,1,1,0,1,0,1,0,0,0,0,0,1,1,0,0)\\
T_4 &= (0,0,1,0,1,0,1,1,0,0,0,1,1,0,0,0)\\
T_5 &= (0,0,0,1,0,0,0,1,1,0,1,1,0,1,0,0)
\end{aligned}$$

From Example 5.1 and Figure 1, we see that the Walsh support of any Gold coordinate behaves in a special manner. More precisely, if $S_1, \ldots, S_5$ are the Walsh supports as in Example 5.1, then we can represent $\bigcup_{i=1}^5 S_i$ as a disjoint union of sets E_I of the form

$$E_I = \bigcap_{i \in I} S_i \setminus \bigcup_{j \in N \setminus I} S_j, \tag{21}$$

where $\emptyset \neq I \in \mathcal{P}(N)$ and $N = \{1, 2, \ldots, 5\}$ (for a graphical representation see Figure 1 in Appendix). Here, $\mathcal{P}(N)$ denotes the set of all non-empty different subsets of the set N. Moreover, there are $2^5 - 1$ choices for E_I since this is exactly the number of non-empty sets in $\mathcal{P}(N)$. Hence, for the sets E_I, where $I \in \mathcal{P}(N)$ we have that

$$\bigcup_{i=1}^{5} S_i = \bigcup_{\emptyset \neq I \in \mathcal{P}(N)} E_I,\ |E_I| = 1,\ E_I \cap E_J = \emptyset\ (I \cap J = \emptyset). \tag{22}$$

In addition, we observe that the affine hyperplanes S_i (from Example 5.1) are given as $S_i = \{x = (x_1, \ldots, x_5) \in \mathbb{F}_2^5 : x_i = 1\}$, $i = 1, \ldots, 5$, and they satisfy (22)*.*

Using the method proposed in [21, Theorem 3.1], we can construct a semi-bent function f_i from T_i and S_i ($i = 1, \ldots, 5$) as follows. For instance, let us construct the function f_1 from T_1 and S_1, as the construction of $f_2, \ldots, f_5$ goes similarly. Firstly, we note that $S_1, \ldots, S_5$ are ordered lexicographically. Let $S_1 = s_0 \oplus L = \{s_0, s_1, \ldots, s_{2^4-1}\} \subset \mathbb{F}_2^5$, where

$L = \{0, e_1, \ldots, e_{2^4-1}\} \subset \mathbb{F}_2^5$ is a linear subspace and let $\{x_0, \ldots, x_{2^4-1}\} = \mathbb{F}_2^4$ be ordered lexicographically. Let the spectrum $W_1 : \mathbb{F}_2^5 \to \mathbb{Z}$ be defined as

$$W_1(u) = \begin{cases} (-1)^{T_1(x_i)} \cdot 2^{\frac{5+1}{2}}, & u = s_0 \oplus e_i \in S_1, \\ 0, & u \notin S_1. \end{cases}$$

By applying the inverse Walsh-Hadamard transform (2) to the spectrum $\mathcal{W}_1 = \{W_1(x) : x \in \mathbb{F}_2^5\}$, we obtain the truth table of f_1 (clearly having $\mathcal{W}_1 = \mathcal{W}_{f_1}$), cf. Algorithm 1. Using the same approach we obtain the truth tables of $f_2, \ldots, f_5$, which are given as:

$$\begin{aligned}
T_{f_1} &= (0,1,0,1,0,1,1,0,1,0,0,1,1,0,1,0,0,1,1,0,0,1,0,1,0,1,0,1,1,0),\\
T_{f_2} &= (1,1,0,0,1,1,0,0,0,1,1,0,1,0,0,1,1,1,0,0,0,0,1,1,0,1,1,0,0,1,1,0),\\
T_{f_3} &= (0,1,1,0,1,0,0,1,0,0,0,0,1,1,1,1,1,1,0,0,0,0,1,1,1,0,1,0,0,1,0,1),\\
T_{f_4} &= (0,1,0,1,0,0,0,0,1,0,1,0,1,1,1,1,1,1,0,0,0,1,1,0,0,0,1,1,1,0,0,1),\\
T_{f_5} &= (0,0,0,1,1,1,0,1,0,0,0,1,0,0,1,0,1,1,1,0,0,0,1,0,1,1,1,0,1,1,0,1).
\end{aligned}$$

Using Sage*, we confirm that $F = (f_1, \ldots, f_5)$ is an AB function CCZ-equivalent to the Gold function. Using the primitive polynomial $p(x) = x^5 + x^2 + 1$ and the generating element a for which $p(a) = 0$, the univariate form of the function F is given by:*

$$\begin{aligned}
F(x) \;=\; & (a^3+a)x^{24} + (a^4+a^3+a^2+a+1)x^{20} + (a^2+a+1)x^{18} + (a^4+a+1)x^{17} \\
& + (a^4+a^3+a^2+a)x^{16} + (a^3+1)x^{12} + x^{10} + (a^4+a+1)x^9 + (a^4+a^2)x^8 \\
& + (a^4+a^3+a)x^6 + (a^4+a^3)x^5 + a^4x^4 + (a^4+a+1)x^3 + (a^4+a)x^2 + (a^3+a^2+a)x + a
\end{aligned}$$

More formally, given an affine Walsh support and a bent dual function, the process of deriving semi-bent functions is specified in Algorithm 1 below. On the other hand, the search for suitable bent duals that specify an AB function is summarized in Algorithm 2.

Algorithm 1 Construction of semi-bent functions via bent functions and Walsh supports

Input: bent function f in n variables, n-dimensional affine subspace S.
Output: semi-bent function g in $n+1$ variables with Walsh support S.
SemibentFromBent(S, f, n)

1: $A = [x.base(10)$ **for** $x \in S]$
2: $W_f = [0$ **for** $i \in range(n+1)]$
3: **for** $x \in A$ **do**
4: $\quad W_f(x) = (-1)^{f(A.index(x))} \cdot 2^{\frac{n+1}{2}}$
5: **end for**
6: **return** $g =$**invWHT**(W_f)

The above example is a special instance of a computer search for suitable duals performed on a pool of 20 random bent functions in 4 variables, which gives $\binom{20}{5} = 15504$ possibilities to select five bent duals for the coordinate functions. In this search, the five Walsh supports of the coordinate functions are defined as above, i.e., as

$$S_i = \{x = (x_1, \ldots, x_5) \in \mathbb{F}_2^5 : x_i = 1\},\ i = 1, \ldots, 5.$$

Algorithm 2 List of AB functions defined on $\mathbb{F}_2^{n+1}$ from $(\mathcal{T}, \mathcal{S})$

Input: $(n, \mathcal{T}, \mathcal{S})$, where $\mathcal{T}$ is the list of truth tables of bent functions in n variables and $\mathcal{S} = \{S_1, \ldots, S_n\}$ are n-dimensional subspaces of $\mathbb{F}_2^{n+1}$.

Output: List of AB functions $F : \mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$ whose coordinates have Walsh supports in $\mathcal{S}$ and their duals are in $\mathcal{T}$.

```
C = Combinations(T, n + 1)
for c ∈ C do
    L = [ ]
    for i ∈ range(n + 1) do
        f = SemibentFromBent(S[i], T[c[i]], n)
        L.append(f)
    end for
    if isAB(L) then
        A.append(L)
    end if
end for
return A
```

Thus, we obtain 15504 pairs (T, S), where $T = \{T_1, \ldots, T_5\}$ are five bent functions in 4 variables and $S = \{S_1, \ldots, S_5\}$ are the previously defined Walsh supports. This search method is described in Algorithm 2. Among the 15504 pairs (T, S), there are exactly 60 pairs (T, S) that specify AB functions. Nevertheless, all these AB functions (listed in Appendix-Section 6.2) are CCZ-equivalent to some Gold function, which seems to be a consequence of the small ambient space. It is interesting to notice that none of the listed functions is a permutation even though the Gold AB functions are bijective mappings (any monomial AB function is necessarily a permutation).

On the other hand, one may attempt to use equivalent bent duals $T' = \{T'_1, \ldots, T'_5\}$ of bent functions $T = \{T_1, \ldots, T_5\}$. In this context, by constructing semi-bent functions out of pairs (T', S) (where $S = \{S_1, \ldots, S_5\}$), we could observe that the AB property is rather sensitive to such a transformation, and quite remarkably none of the vectorial functions constructed from (T', S) was an AB function.

Remark 5.2. *When considering the function $F(x) = x^3 + Tr(x^9),\ x \in \mathbb{F}_{2^9}$, we noticed that the intersections are not as uniform as in the Gold case. That is, if $S_1, \ldots, S_9$ are the Walsh supports of the coordinate functions, then for $I \in \mathcal{P}(N),\ N = \{1, \ldots, 9\}$, we have that*

$$|E_I| \in \{0, 2\},\ E_I \cap E_J = \emptyset\ (I \cap J = \emptyset), \tag{23}$$

where E_I is defined by (21).

In the previous example, we have fixed the Walsh supports $S = \{S_1, \ldots, S_5\}$ that satisfy the "uniform" intersection (corresponding to (22)) and we searched for bent functions T such that the sets of duals $T = \{T_1, \ldots, T_5\}$ and Walsh supports S (briefly denoted by a pair (T, S)) gives us an AB function. Let us now consider an example for the second case, i.e. when the sets E_I satisfy (23). We define the Walsh supports to be

$$S_i = \{x = (x_1, \ldots, x_5) \in \mathbb{F}_2^5 : x_i \oplus x_{i+1 \mod 5} = 1\},\ i = 1, \ldots, 5.$$

These supports obviously satisfy (23). Using Sage and the previously described method, we have taken 20 random bent functions in 4 variables and considered all possible 5-tupples, i.e. $\binom{20}{5}$ possibilities for T. In total, we were able to find 44 pairs (T, S) for which the constructed vectorial function is AB. Furthermore, all the functions are CCZ-equivalent to some Gold function.

Remark 5.3. *Using* Sage*, for the component functions of the AB functions listed in Appendix-Sections 6.2, we note that the functions $\psi_{u,i,j}$ and $\varphi_{u,i,j}$ (as described in Example 4.1) are semi-bent Boolean functions in 3 variables for any choice of Walsh supports S_i, S_j and of components f_i, f_j of F.*

5.2 Constructing AB functions on $\mathbb{F}_2^7$

For $n = 7$, by using Algorithm 2, we were able to find suitable pairs of Walsh supports and bent functions in six variables, such that the resulting mappings are AB functions on $\mathbb{F}_2^7$. Similarly as before, the Walsh supports behave in a pattern identical to (22) and (23). Furthermore, using the mathematical software Magma, it could be confirmed that the obtained AB functions are not CCZ-equivalent to the Gold AB function. In Appendix - Section 6.3, we list these AB functions. However, a much rigorous theoretical approach is needed to have a better understanding of these intersections, that is, to find explicit conditions for (T, S) such that the constructed vectorial bent function is always AB and hopefully CCZ-inequivalent to the Gold function. We leave this investigation as an open problem for further research.

Similarly as in the case when $n = 5$ (cf. Remark 5.3), we observe that the functions $\psi_{u,i,j}$ and $\phi_{u,i,j}$ (for $n = 7$) are semi-bent functions in 5 variables. However, this holds only for those functions whose Walsh supports are affine subspaces. For some of the AB functions listed in the Appendix-Section 6.3, we observe that the Walsh-supports are linear subspaces. Because of this, we need to redefine the functions ψ_u and φ_u in Proposition 4.2, so that they are well-defined mappings.

Using similar observations as in (14) and (16), the mappings φ_u and ψ_u can be redefined as follows:

$$\begin{aligned} \varphi_u : S_f \backslash \Lambda \to \mathbb{F}_2,\ \varphi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega) \ \text{ for } \ u \in S_g, \\ \psi_u : \Lambda \to \mathbb{F}_2,\ \psi_u(\omega) = f^*(\omega) \oplus g^*(u \oplus \omega) \ \text{ for } \ u \in \mathbb{F}_2^n \setminus S_g, \end{aligned}$$

Notice that the only difference between the above definition of φ_u and ψ_u and those given in Proposition 4.2 is that we switched the domains of the functions. Again, using Sage, we could confirm that in the case of linear Walsh supports, the functions $\psi_{u,i,j}$ and $\varphi_{u,i,j}$ (as described in Example 4.1 and defined as above) are semi-bent functions in five variables for any choice of Walsh supports S_i, S_j and of components f_i, f_j of F, where F is from the list of AB functions in Appendix-Section 6.3.

6 Conclusions

In this article, we employed the concept of dual of s-plateaued functions introduced in [20, 21] to analyze the structure of quadratic AB functions and to address the problem of designing AB functions in the dual (spectral) domain. It turns out that even the quadratic case (along

with the fact that the corresponding Walsh supports are affine hyperplanes) is quite complicated. Nevertheless, the presented results are quite promising and there seems to be a greater potential in this approach which can eventually be further developed to efficiently deal with the quadratic case.

Acknowledgment: Amar Bapić is supported in part by the Slovenian Research Agency (research program P1-0404 and Young Researchers Grant). Samir Hodžić is supported by a grant from the Independent Research Fund Denmark for Technology and Production, grant no. 8022-00348A. Enes Pasalic is partly supported by the Slovenian Research Agency (research program P1-0404 and research projects J1-9108, J1-1694), and the European Commission for funding the InnoRenew CoE project (Grant Agreement no. 739574) under the Horizon2020 Widespread-Teaming program and the Republic of Slovenia (Investment funding of the Republic of Slovenia and the European Union of the European regional Development Fund).

References

[1] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. *Designs, Codes and Cryptography* 49(1-3), pp. 273-288, 2008.

[2] L. Budaghyan, C. Carlet, P. Felke and G. Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. *IEEE International Symposium on Information Theory*, pp. 2637-2641, 2006.

[3] L. Budaghyan, C. Carlet and G. Leander. Two classes of quadratic APN binomials inequivalent to power functions. *IEEE Trans. on Inform. Theory* 54(9): 4218–4229, 2008.

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

[5] L. Budaghyan, C. Carlet and G. Leander. Constructing new APN functions from known ones. *Finite Fields and Applications*, 15(2): 150–159, 2009.

[6] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine. On cryptographic properties of the cosets of $R(1, m)$. *IEEE Trans. on Inform. Theory*, 47(4): 1494–1513, 2001.

[7] M. Calderini, L. Budaghyan and C. Carlet. On known constructions of APN and AB functions and their relation to each other. *IACR Cryptology ePrint Archive*, 2020:1444, 2020.

[8] C. Carlet. *Boolean Functions for Cryptography and Error-Correcting Codes*, pages 257–397. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010.

[9] C. Carlet. *Vectorial Boolean Functions for Cryptography*, pages 398–470. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2010.

[10] 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.

[11] C. Carlet and S. Mesnager. On the supports of the walsh transforms of boolean functions. *IACR Cryptology ePrint Archive*, 2004:256, 2004.

[12] C. Carlet and E. Prouff. On plateaued functions and their constructions. In T. Johansson, editor, *Fast Software Encryption*, pages 54–73, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[13] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In A. De Santis, editor, *Advances in Cryptology — EUROCRYPT'94*, pages 356–365, Berlin, Heidelberg, 1995. Springer Berlin Heidelberg.

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

[15] T. Cusick and P. Stănică. *Cryptographic Boolean Functions and Applications: Second edition*. Academic Press, 2017.

[16] M. Duan, X. Lai, M. Yang, X. Sun, and B. Zhu. Distinguishing properties of higher order derivatives of boolean functions. *IACR Cryptology ePrint Archive*, 2010:417, 01 2010.

[17] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory* 52(2): 744–747, 2006.

[18] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. *Advances in Mathematics of Communications*, 3(1): 59–81, 2009.

[19] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14(1): 154–156, 1968.

[20] S. Hodžić, E. Pasalic, and Y. Wei. A general framework for secondary constructions of bent and plateaued functions. *CoRR*, abs/1809.07390, 2018.

[21] S. Hodžić, E. Pasalic, Y. Wei, and F. Zhang. Designing plateaued boolean functions in spectral domain and their classification. *IEEE Trans. on Inform. Theory*, 65(9): 5865–5879, 2019.

[22] S. Hodžić, P. Horak, E. Pasalic. Characterization of basic 5-value spectrum functions through Walsh-Hadamard transform. *IEEE Trans. on Inform. Theory*, 67(2): 1038–1053, 2021.

[23] G. Leander and G. McGuire. Construction of bent functions from near-bent functions. *Journal of Combinatorial Theory, Series A*, 116(4):960 – 970, 2009.

[24] M. Matsui. Linear cryptanalysis method for DES cipher. In *Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of of Cryptographic Techniques, Lofthus, Norway, May 23-27, 1993, Proceedings*, pages 386–397, 1993.

[25] S. Mesnager. *Bent Functions: Fundamentals and Results*. Springer Publishing Company, Incorporated, 1st edition, 2016.

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

[27] L. Qu, S. Fu, Q. Dai and C. Li. When a Boolean Function can be Expressed as the Sum of two Bent Functions. *IACR Cryptology ePrint Archive*, 2014:048, 2014.

[28] Y. Zheng and X. Zhang. On plateaued functions. *IEEE Trans. on Inform. Theory*, 47(3): 1215 – 1223, 2001.

Appendix

6.1 Intersection of the Walsh supports for the Gold coordinate functions

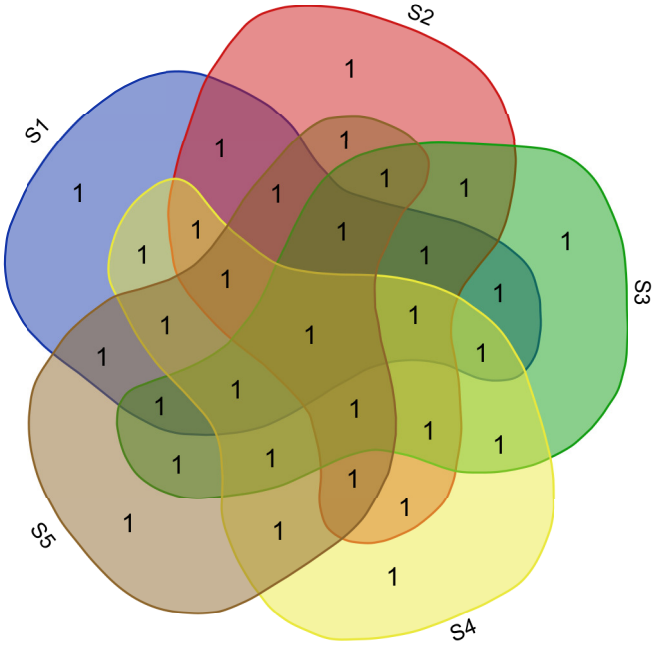

Figure 1: Graphical representation of the intersection of Walsh supports of the coordinate functions f_i for the Gold function $F(x) = x^d$ on $\mathbb{F}_{2^5}$, $d = 3, 5$

6.2 A list of AB functions constructed by the spectral method for $n = 5$

The functions $F : \mathbb{F}_2^5 \to \mathbb{F}_2^5$ below are specified as integer outputs when the input x goes through $\mathbb{F}_2^5$ ordered lexicographically.

$(2, 15, 4, 25, 22, 19, 1, 20, 9, 2, 10, 17, 15, 12, 29, 14, 30, 31, 17, 0, 0, 9, 30, 7, 20, 19, 30, 9, 24, 23, 3, 28)$
$(18, 31, 4, 25, 22, 3, 17, 20, 9, 18, 26, 17, 15, 12, 13, 30, 14, 15, 17, 0, 0, 25, 14, 7, 20, 3, 14, 9, 24, 23, 19, 12)$
$(18, 23, 12, 17, 6, 19, 1, 12, 9, 10, 18, 9, 15, 28, 13, 6, 6, 7, 17, 8, 24, 9, 22, 31, 28, 27, 14, 17, 16, 7, 27, 20)$
$(26, 31, 4, 17, 6, 27, 9, 4, 1, 2, 26, 9, 15, 20, 5, 14, 14, 7, 25, 0, 16, 1, 22, 23, 20, 27, 6, 25, 24, 15, 27, 28)$
$(2, 15, 20, 29, 6, 19, 17, 0, 29, 22, 30, 17, 27, 8, 25, 14, 30, 27, 5, 4, 16, 13, 10, 19, 0, 3, 14, 9, 12, 23, 3, 28)$
$(18, 15, 20, 29, 6, 3, 17, 0, 13, 22, 30, 17, 27, 24, 25, 14, 14, 27, 5, 4, 16, 29, 10, 19, 16, 3, 14, 9, 12, 7, 3, 28)$
$(26, 15, 20, 5, 6, 11, 9, 0, 5, 6, 30, 25, 11, 16, 17, 14, 14, 19, 13, 20, 16, 21, 18, 19, 16, 27, 6, 9, 28, 15, 11, 28)$
$(10, 23, 24, 29, 22, 3, 13, 0, 17, 10, 2, 1, 31, 12, 5, 14, 22, 15, 9, 8, 8, 25, 30, 23, 8, 23, 22, 17, 4, 19, 19, 28)$
$(26, 7, 24, 13, 6, 3, 13, 0, 1, 10, 18, 17, 15, 28, 21, 14, 6, 31, 9, 24, 24, 25, 30, 23, 24, 23, 6, 1, 20, 3, 3, 28)$
$(10, 31, 20, 17, 22, 9, 9, 6, 17, 0, 10, 11, 31, 4, 5, 14, 30, 7, 9, 0, 0, 19, 22, 21, 6, 27, 20, 25, 10, 29, 25, 30)$
$(26, 15, 16, 13, 6, 9, 5, 2, 1, 0, 26, 19, 15, 20, 29, 14, 6, 23, 9, 16, 16, 27, 22, 21, 26, 31, 4, 9, 30, 1, 9, 30)$
$(18, 31, 8, 29, 30, 1, 21, 18, 9, 16, 18, 19, 7, 12, 13, 30, 14, 7, 17, 0, 8, 19, 6, 5, 18, 15, 12, 9, 22, 25, 25, 14)$
$(0, 21, 30, 27, 22, 11, 9, 4, 27, 8, 16, 19, 31, 4, 21, 30, 28, 13, 11, 10, 8, 17, 30, 23, 4, 19, 6, 1, 2, 29, 1, 14)$
$(0, 5, 18, 31, 14, 27, 21, 8, 27, 24, 24, 19, 23, 4, 29, 6, 20, 21, 3, 10, 16, 1, 14, 23, 8, 15, 14, 1, 14, 25, 1, 30)$
$(12, 13, 18, 27, 2, 27, 21, 4, 19, 20, 28, 19, 31, 0, 25, 14, 20, 17, 15, 2, 16, 13, 2, 23, 8, 11, 2, 9, 14, 21, 13, 30)$

(0, 7, 30, 21, 6, 17, 17, 10, 29, 28, 22, 27, 25, 8, 27, 6, 22, 19, 5, 12, 24, 13, 2, 27, 10, 9, 12, 3, 6, 21, 9, 22)
(28, 15, 18, 13, 8, 3, 15, 8, 1, 4, 26, 19, 5, 24, 23, 6, 2, 27, 13, 24, 20, 21, 18, 31, 24, 23, 2, 1, 30, 9, 13, 22)
(6, 19, 28, 29, 16, 13, 11, 2, 25, 14, 6, 5, 31, 0, 1, 10, 26, 9, 9, 14, 14, 21, 28, 19, 4, 21, 18, 23, 0, 25, 23, 26)
(3, 26, 29, 20, 23, 4, 1, 2, 28, 1, 7, 10, 27, 12, 8, 15, 27, 10, 1, 0, 12, 23, 30, 21, 2, 23, 29, 24, 6, 25, 17, 30)
(15, 2, 29, 4, 19, 20, 17, 2, 16, 13, 23, 30, 15, 24, 24, 27, 19, 18, 9, 28, 4, 15, 14, 17, 14, 31, 1, 4, 26, 1, 5, 10)
(17, 26, 15, 20, 5, 20, 3, 2, 14, 1, 21, 10, 11, 30, 8, 13, 11, 8, 17, 2, 30, 7, 28, 21, 18, 21, 13, 26, 22, 11, 17, 28)
(25, 10, 23, 16, 7, 28, 25, 22, 0, 1, 11, 30, 29, 20, 6, 27, 11, 18, 9, 4, 20, 5, 6, 3, 22, 29, 17, 14, 10, 9, 29, 10)
(25, 26, 7, 16, 7, 28, 9, 6, 0, 1, 27, 14, 13, 20, 6, 11, 11, 2, 25, 4, 20, 5, 22, 19, 22, 29, 1, 30, 26, 9, 29, 26)
(25, 10, 19, 20, 5, 30, 31, 16, 4, 5, 11, 30, 25, 16, 6, 27, 11, 18, 9, 4, 20, 5, 6, 3, 16, 27, 23, 8, 14, 13, 25, 14)
(25, 26, 3, 20, 5, 30, 15, 0, 4, 5, 27, 14, 9, 16, 6, 11, 11, 2, 25, 4, 20, 5, 22, 19, 16, 27, 7, 24, 30, 13, 25, 30)
(17, 18, 11, 28, 21, 14, 31, 16, 12, 29, 19, 22, 9, 0, 6, 27, 11, 10, 25, 12, 12, 21, 14, 3, 16, 3, 7, 0, 22, 29, 17, 14)
(17, 18, 15, 24, 21, 14, 27, 20, 8, 25, 19, 22, 13, 4, 6, 27, 11, 10, 25, 12, 12, 21, 14, 3, 20, 7, 3, 4, 18, 25, 21, 10)
(13, 0, 31, 6, 19, 20, 17, 2, 16, 13, 23, 30, 13, 26, 26, 25, 17, 16, 11, 30, 4, 15, 14, 17, 14, 31, 1, 4, 24, 3, 7, 8)
(1, 18, 31, 20, 31, 14, 8, 1, 26, 15, 20, 25, 23, 0, 16, 31, 31, 4, 13, 14, 2, 27, 25, 24, 5, 24, 7, 2, 11, 20, 0, 7)
(17, 18, 15, 24, 21, 14, 26, 21, 8, 25, 18, 23, 13, 4, 6, 27, 11, 10, 25, 12, 12, 21, 15, 2, 21, 6, 3, 4, 19, 24, 20, 11)
(7, 18, 29, 28, 17, 12, 10, 3, 24, 15, 6, 5, 31, 0, 0, 11, 27, 8, 9, 14, 14, 21, 29, 18, 5, 20, 19, 22, 1, 24, 22, 27)
(15, 18, 29, 28, 17, 4, 10, 3, 16, 15, 6, 5, 31, 8, 0, 11, 19, 8, 9, 14, 14, 29, 29, 18, 13, 20, 19, 22, 1, 16, 22, 27)
(16, 13, 23, 26, 6, 3, 16, 5, 11, 16, 24, 19, 31, 28, 29, 14, 13, 28, 2, 3, 17, 24, 15, 22, 21, 2, 14, 9, 11, 4, 1, 30)
(0, 29, 23, 26, 22, 3, 0, 5, 27, 0, 8, 3, 31, 12, 13, 14, 29, 12, 2, 3, 1, 24, 31, 22, 5, 18, 30, 25, 11, 20, 17, 30)
(24, 29, 7, 22, 6, 27, 8, 1, 7, 4, 28, 11, 11, 16, 1, 14, 13, 0, 30, 7, 17, 4, 19, 18, 17, 26, 6, 25, 31, 12, 25, 30)
(12, 29, 19, 26, 26, 3, 12, 13, 19, 4, 28, 19, 23, 8, 17, 22, 21, 8, 14, 11, 1, 20, 19, 30, 9, 18, 2, 1, 15, 28, 13, 6)
(16, 23, 15, 20, 6, 17, 0, 11, 13, 12, 22, 11, 9, 24, 11, 6, 7, 2, 20, 13, 25, 12, 19, 26, 27, 24, 12, 19, 23, 4, 25, 22)
(16, 15, 31, 12, 14, 1, 0, 3, 13, 4, 22, 19, 1, 24, 27, 14, 15, 18, 4, 21, 25, 20, 19, 18, 19, 24, 12, 11, 23, 12, 9, 30)
(20, 11, 31, 12, 10, 5, 0, 3, 9, 0, 22, 19, 5, 28, 27, 14, 11, 22, 4, 21, 29, 16, 19, 18, 23, 28, 12, 11, 19, 8, 9, 30)
(16, 7, 27, 20, 6, 3, 20, 9, 11, 26, 16, 25, 31, 28, 29, 6, 7, 20, 0, 11, 27, 26, 5, 28, 25, 12, 14, 3, 7, 0, 9, 22)
(4, 19, 31, 28, 18, 15, 8, 1, 27, 14, 4, 5, 31, 0, 1, 10, 27, 8, 8, 15, 15, 22, 29, 16, 5, 20, 18, 23, 3, 24, 21, 26)
(20, 3, 31, 12, 0, 15, 10, 1, 9, 12, 22, 23, 13, 16, 19, 10, 11, 26, 8, 29, 29, 20, 31, 18, 21, 22, 2, 5, 19, 8, 5, 26)
(16, 31, 6, 29, 23, 0, 17, 18, 13, 20, 30, 19, 9, 8, 10, 31, 14, 11, 20, 5, 0, 29, 10, 3, 18, 1, 13, 10, 31, 20, 16, 15)
(16, 7, 30, 21, 7, 0, 17, 10, 13, 28, 22, 27, 25, 24, 26, 7, 6, 19, 4, 13, 24, 29, 2, 27, 26, 9, 13, 2, 7, 4, 8, 23)
(16, 23, 14, 21, 23, 0, 17, 26, 13, 28, 22, 27, 9, 8, 10, 23, 6, 3, 20, 13, 8, 29, 2, 11, 26, 9, 13, 2, 23, 20, 24, 7)
(24, 11, 18, 21, 7, 12, 29, 2, 5, 20, 26, 31, 25, 16, 22, 11, 10, 19, 8, 5, 20, 21, 6, 19, 18, 9, 5, 10, 15, 12, 8, 31)
(24, 11, 22, 17, 7, 12, 25, 6, 1, 16, 26, 31, 29, 20, 22, 11, 10, 19, 8, 5, 20, 21, 6, 19, 22, 13, 1, 14, 11, 8, 12, 27)
(24, 11, 18, 21, 5, 30, 31, 16, 5, 4, 10, 31, 25, 16, 6, 27, 10, 19, 8, 5, 20, 5, 6, 3, 16, 27, 23, 8, 15, 12, 24, 15)
(16, 19, 10, 29, 21, 14, 31, 16, 13, 28, 18, 23, 9, 0, 6, 27, 10, 11, 24, 13, 12, 21, 14, 3, 16, 3, 7, 0, 23, 28, 16, 15)
(24, 11, 22, 17, 5, 30, 27, 20, 1, 0, 10, 31, 29, 20, 6, 27, 10, 19, 8, 5, 20, 5, 6, 3, 20, 31, 19, 12, 11, 8, 28, 11)
(24, 9, 22, 19, 5, 30, 27, 20, 3, 2, 8, 29, 29, 22, 6, 25, 8, 17, 10, 7, 20, 7, 6, 1, 20, 29, 19, 14, 11, 8, 28, 11)
(4, 17, 30, 23, 25, 14, 11, 0, 27, 10, 20, 25, 21, 6, 18, 29, 24, 5, 14, 15, 4, 27, 26, 25, 4, 29, 7, 2, 11, 16, 0, 7)
(4, 13, 27, 10, 27, 16, 20, 7, 24, 5, 22, 19, 4, 27, 26, 29, 29, 16, 7, 18, 8, 7, 2, 21, 3, 26, 8, 9, 21, 14, 14, 13)
(20, 25, 15, 30, 27, 4, 16, 19, 8, 21, 22, 23, 4, 11, 10, 25, 9, 0, 19, 6, 12, 23, 6, 1, 23, 14, 8, 13, 17, 26, 30, 9)
(12, 1, 31, 6, 19, 20, 17, 2, 17, 12, 23, 30, 13, 26, 26, 25, 17, 16, 10, 31, 5, 14, 15, 16, 14, 31, 0, 5, 25, 2, 6, 9)
(8, 13, 23, 14, 30, 17, 25, 10, 20, 1, 26, 19, 0, 31, 22, 21, 21, 24, 11, 26, 0, 7, 6, 29, 14, 19, 1, 0, 25, 14, 14, 5)
(14, 19, 28, 29, 16, 5, 11, 2, 17, 14, 7, 4, 30, 9, 1, 10, 18, 9, 8, 15, 14, 29, 29, 18, 12, 21, 18, 23, 1, 16, 22, 27)
(6, 19, 28, 29, 17, 12, 10, 3, 24, 15, 6, 5, 30, 1, 1, 10, 26, 9, 8, 15, 14, 21, 29, 18, 5, 20, 19, 22, 0, 25, 23, 26)
(14, 19, 28, 29, 17, 4, 10, 3, 16, 15, 6, 5, 30, 9, 1, 10, 18, 9, 8, 15, 14, 29, 29, 18, 13, 20, 19, 22, 0, 17, 23, 26)
(7, 16, 29, 18, 26, 15, 8, 5, 24, 9, 19, 26, 23, 4, 20, 31, 25, 2, 14, 13, 7, 30, 24, 25, 2, 31, 4, 1, 14, 17, 0, 7)
(7, 18, 29, 16, 24, 15, 10, 5, 26, 9, 17, 26, 23, 6, 20, 29, 25, 2, 14, 13, 7, 30, 24, 25, 0, 29, 6, 3, 12, 19, 2, 5)

6.3 A list of AB functions constructed by the spectral method for $n = 7$

A list of AB functions with the intersection of their coordinate Walsh supports corresponding to (22):

(0, 1, 14, 25, 84, 71, 106, 111, 44, 27, 100, 69, 57, 28, 65, 114, 118, 117, 52, 33, 60, 45, 78, 73, 111, 90, 107, 72, 100, 67, 80, 97, 117, 58, 66, 27, 110, 51, 105, 34, 67, 58, 50, 93, 25, 114, 88, 37, 12, 65, 119, 44, 9, 86, 66, 11, 15, 116, 50, 95, 75, 34, 70, 57, 72, 67, 61, 32, 104, 113, 45, 34, 71, 122, 116, 95, 38, 9, 37, 28, 95, 86, 102, 121, 97, 122, 104, 101, 101, 90, 26, 51, 26, 55, 85, 110, 32, 101, 108, 63, 79, 24, 51, 114, 53, 70, 63, 90, 27, 122, 33, 86, 56, 127, 56, 105, 73, 28, 121, 58, 24, 105, 94, 57, 40, 75, 94, 43)

(0, 1, 68, 85, 112, 119, 42, 61, 113, 32, 33, 96, 35, 116, 109, 42, 126, 107, 10, 15, 92, 79, 54, 53, 10, 79, 106, 63, 10, 73, 116, 39, 54, 61, 54, 45, 69, 72, 91, 70, 123, 32, 111, 36, 42, 119, 32, 109, 70, 89, 118, 121, 103, 126, 73, 64, 14, 65, 42, 117, 13, 68, 55, 110, 127, 24, 60, 75, 25, 120, 68, 53, 92, 107, 11, 44, 24, 41, 81, 112, 29, 110, 110, 13, 41, 92, 68, 33, 59, 24, 92, 111, 45, 8, 84, 97, 43, 70, 44, 81, 78, 37, 87, 44, 52, 9, 39, 10, 115, 72, 126, 85, 71, 62, 112, 25, 112, 15, 89, 54, 93, 116, 126, 71, 72, 103, 117, 74)

A list of AB functions with the intersection of their coordinate Walsh supports corresponding to (23):

(0, 0, 28, 24, 86, 70, 122, 110, 82, 112, 67, 101, 124, 78, 93, 107, 114, 116, 34, 32, 58, 44, 90, 72, 107, 79, 54, 22, 91, 111, 54, 6, 119, 61, 59, 117, 30, 68, 98, 60, 30, 118, 95, 51, 15, 119, 126, 2, 92, 16, 92, 20, 43, 119, 27, 67, 126, 16, 115, 25, 113, 15, 76, 54, 98, 126, 10, 18, 101, 105, 61, 53, 85, 107, 48, 10, 42, 4, 127, 85, 46, 52, 10, 20, 55, 61, 35, 45, 82, 106, 123, 71, 51, 27, 42, 6, 124, 42, 68, 22, 68, 2, 76, 14, 112, 4, 69, 53, 48, 84, 53, 85, 105, 57, 29, 73, 79, 15, 11, 79, 46, 92, 87, 33, 112, 18, 57, 95)

(0, 1, 40, 57, 88, 95, 12, 27, 68, 89, 122, 119, 125, 102, 63, 52, 38, 51, 108, 105, 80, 67, 102, 101, 115, 122, 47, 54, 100, 107, 68, 91, 87, 114, 66, 119, 10, 41, 99, 80, 31, 38, 28, 53, 35, 28, 92, 115, 10, 59, 125, 92, 121, 78, 114, 85, 83, 126, 50, 15, 65, 106, 92, 103, 112, 39, 77, 10, 58, 107, 123, 58, 29, 86, 54, 109, 54, 123, 97, 60, 47, 108, 112, 35, 75, 14, 104, 61, 83, 12, 26, 85, 86, 15, 99, 42, 126, 13, 126, 29, 49, 68, 77, 40, 31, 112, 9, 118, 49, 88, 91, 34, 90, 61, 56, 79, 59, 90, 37, 84, 42, 81, 94, 53, 42, 87, 34, 79)

(0, 1, 118, 103, 106, 109, 78, 89, 80, 31, 25, 70, 77, 4, 86, 15, 60, 41, 84, 81, 52, 39, 14, 13, 28, 71, 75, 0, 99, 62, 102, 43, 34, 25, 83, 120, 12, 49, 47, 2, 99, 22, 45, 72, 58, 73, 38, 69, 80, 127, 63, 0, 28, 53, 33, 24, 97, 0, 49, 64, 90, 61, 88, 47, 102, 83, 37, 0, 71, 116, 86, 117, 90, 33, 38, 77, 12, 113, 34, 79, 49, 16, 108, 93, 114, 85, 125, 74, 125, 18, 31, 96, 73, 32, 121, 0, 108, 99, 40, 55, 9, 0, 31, 6, 65, 0, 58, 107, 83, 20, 122, 45, 117, 110, 47, 36, 114, 111, 122, 119, 40, 125, 77, 8, 88, 11, 111, 44)