Cryptography and Communications (2021) 13:909–926
https://doi.org/10.1007/s12095-021-00528-5

Some general properties of modified bent functions through addition of indicator functions

Nikolay Kolomeec[1]

Received: 21 October 2020 / Accepted: 9 August 2021 / Published online: 27 August 2021

Abstract
Properties of a secondary bent function construction that adds the indicator of an affine subspace of arbitrary dimension to a given bent function in n variables are obtained. Some results regarding normal and weakly normal bent functions are generalized. An upper bound for the number of generated bent functions is proven. This bound is attained if and only if the given bent function is quadratic. In certain cases, the addition of the indicator of an m-dimensional subspace, for different m, will not generate bent functions. Such examples are presented for any even $n \geq 10$. It is proven that there exists an infinite family of Maiorana–McFarland bent functions such that the numbers of generated bent functions differ for the bent function and its dual function.

Keywords Boolean functions · Bent functions · Affine functions · Balanced functions · Subspaces

Mathematics Subject Classification (2010) 06E30 · 94C10 · 94A60

1 Introduction

A bent function is a Boolean function in even number of variables that is at the maximal possible Hamming distance from the set of all affine Boolean functions. In other words, it has the best nonlinearity. Bent functions were introduced by O. Rothaus [26]. Since 1960, they have been actively researched. As extreme objects, they have many applications in various fields: algebra, coding theory, combinatorics, communication theory, cryptography.

This article belongs to the Topical Collection: *Boolean Functions and Their Applications V*
Guest Editors: Lilya Budaghyan, Claude Carlet, Tor Helleseth and Kaisa Nyberg

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075–15–2019–1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research.

✉ Nikolay Kolomeec
kolomeec@math.nsc.ru

[1] Sobolev Institute of Mathematics, Novosibirsk, Russia

Boolean functions with high nonlinearity are especially interesting for symmetric cryptography, since they help to resist linear cryptanalysis [23]. Useful information regarding bent functions can be found in reviews, dissertations and monographs [6, 7, 9–11, 14, 21, 25, 28].

This work is dedicated to the following secondary construction of bent functions. Let f be a given bent function in n variables and L be an affine subspace of $\mathbb{F}_2^n$. We consider all bent functions of the form $f \oplus \mathrm{Ind}_L$, where Ind_L is the indicator function of L. For the first time it was mentioned by J. Dillon [11] for $n/2$-dimensional subspaces. Later, C. Carlet [4] proved a criterion of "bentness" of $f \oplus \mathrm{Ind}_L$, where L is of arbitrary dimension. The most popular and well studied case is $\dim L = n/2$. In this case, the criterion transforms to the affinity of f on L. Also, the construction generates exactly all bent functions at the Hamming distance $2^{n/2}$ from the given one, which is the minimal possible distance between two distinct bent functions (see [17]). This connects the construction properties with the metric properties of the set of all bent functions (see, for instance, [16]). Note that this case was studied in terms of (weakly) normal bent functions, which means that a function is constant (resp. affine) on some $n/2$-dimensional affine subspace (see [3, 8, 13, 20]). It should be emphasized that the affinity on an affine subspace is an interesting property for cryptography by itself. Subspaces of large dimension deserve attention too. For instance, A. Canteaut and P. Charpin considered the case of $(n-2)$-dimensional subspaces in the function decomposition context [2]. Note that it is rather difficult to find a suitable affine subspace L such that $f \oplus \mathrm{Ind}_L$ is a bent function. Also, it is hard to determine which of bent function subclasses contain $f \oplus \mathrm{Ind}_L$ and which do not. Nevertheless, some results related to these problems have been obtained [3, 4, 22, 27].

In this work, we investigate the properties of the construction $f \oplus \mathrm{Ind}_L$, where L is an affine subspace of arbitrary dimension m. On the one hand, they are similar to the case of $m = n/2$. The construction properties are closely connected with the affinity of the dual function on affine subspaces. Some known results for $m = n/2$ are generalized for the case of arbitrary dimensions, for instance, an upper bound for the number of constructed bent functions [16], the use of the simplest iterative construction $f(x) \oplus y_1 y_2$ of bent functions [3, 8]. In certain cases, the addition of the indicator of an m-dimensional subspace, for different m, will not generate bent functions. Such examples are presented for any even $n \geq 10$. On the other hand, the numbers of generated bent functions may differ for some bent function f and its dual function $\widetilde{f}$, which is opposite to the case of $m = n/2$. Examples of such bent functions for any even $n \geq 8$ and $m = n-2$ are provided. Interestingly, these examples are Maiorana–McFarland bent functions [24].

The article is organized as follows. Section 2 contains basic definitions. In Section 3, the notion of a balanced representation of a bent function f by a linear subspace L is introduced. It means that f is either constant or balanced on each coset of L. This notion is directly connected with the criterion proven in [4]. Also, properties of such representations (Theorem 2) are considered. Note that bent functions [5, 24, 29] obtained by the concatenation of affine functions always have a balanced representation by some nontrivial linear subspace. In Section 4, we assume that $f \oplus \mathrm{Ind}_L$ is a bent function for some given bent function f and an affine subspace L and consider how to find affine subspaces L' and L'', where $L' \subset L \subset L''$, such that $f \oplus \mathrm{Ind}_{L'}$ and $f \oplus \mathrm{Ind}_{L''}$ are bent functions. Note that the conditions related to the existence of L' and L'' are, in general, not trivial. There is one simple case: we can always find an $n/2$-dimensional L' by an $(n/2+1)$-dimensional L. The case of $\dim L = n/2 + 1$ similarly to the case of $\dim L = n/2$ guarantees that the construction is symmetric for the bent function f and its dual function $\widetilde{f}$: $\mathrm{sup}(\widetilde{f} \oplus \widetilde{(f \oplus \mathrm{Ind}_L)})$ is an affine subspace too (Theorem 3). In other words, the dual functions of f and $f \oplus \mathrm{Ind}_L$ differ exactly on an affine subspace of dimension $\dim L$. Actually, the case of $\dim L = n/2 + 1$ is equivalent to applying the construction twice for some $n/2$-dimensional $L' \subset L$ and its shift $L \setminus L'$: $(f \oplus \mathrm{Ind}_{L'}) \oplus \mathrm{Ind}_{L\setminus L'} = f \oplus \mathrm{Ind}_L$, where $f \oplus \mathrm{Ind}_{L'}$ is bent. Hence, these two cases are practically similar. Let us denote by $\mathrm{BS}_m(f)$ the set of all bent functions of the form $f \oplus \mathrm{Ind}_L$, where L is m-dimensional. In Section 5, an upper bound for $\#\mathrm{BS}_m(f)$ is proven. This bound is attained for a nontrivial dimension if and only if the given bent function f is quadratic (Theorem 4). Also, it is shown how to choose a bent function f in n variables such that $\#\mathrm{BS}_m(f) = 0$, where $m = n-2, n-1, \ldots, k$. In light of A. Gorodilova's results [15], $k \le n/2 + 4$ for the dual function of a suitable Kasami [12, 19] bent function (Theorem 6). Thus, 0 is a tight lower bound for $\#\mathrm{BS}_m(f)$. Section 6 focuses on the simplest iterative construction $f_{+2}(x, y) = f(x) \oplus y_1 y_2$ of bent functions. It is proven (Theorem 8) that "bentness" of $f_{+2} \oplus \mathrm{Ind}_L$ for an m-dimensional affine subspace L implies "bentness" of $f \oplus \mathrm{Ind}_{L'}$ for some affine subspace L' of dimension $m-1$ or $m-2$. This fact generalizes the properties of normal bent functions [3]. It allows us to construct a bent function f such that $\#\mathrm{BS}_m(f) = 0$, where $m = n/2, n/2 + 1, n/2 + 2, n/2 + 3$ (the number of dimensions depends on the initial function; such example is based on the bent function found in [20]). Note that these dimensions complement the ones from Theorem 6. In addition, $\#\mathrm{BS}_n(f_{+2})$ is calculated by constant derivatives (Theorem 9) and it is shown that it is impossible to find $\#\mathrm{BS}_n(f_{+2})$ by $\#\mathrm{BS}_{n-2}(f)$. The counterexample is found in the Maiorana–McFarland class. Section 7 demonstrates an infinite family of Maiorana–McFarland bent functions f_n in n variables such that $\#\mathrm{BS}_{n-2}(f_n) \ne \#\mathrm{BS}_{n-2}(\widetilde{f_n})$, i. e. f and its dual $\widetilde{f}$ structurally differ. This can make it more difficult to determine the class containing $f \oplus \mathrm{Ind}_L$ even if f is a Maiorana–McFarland bent function.

2 Preliminaries

Let us denote the finite field with two elements by $\mathbb{F}_2$. *A Boolean function* in n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let $\langle x, y\rangle = x_1y_1 \oplus \ldots \oplus x_ny_n$, where $x, y \in \mathbb{F}_2^n$. Let us denote the characteristic Boolean function of a set $S \subseteq \mathbb{F}_2^n$ by Ind_S and *the derivative* of f *in the direction* α by $D_\alpha f$, $D_\alpha f(x) = f(x) \oplus f(x \oplus \alpha)$. Let $D_L f(x) = \bigoplus_{a\in L} f(x \oplus a)$, i. e. the derivative $D_L f = D_{a_1} D_{a_2} \ldots D_{a_k} f$, where $a_1, \ldots, a_k$ is a basis of L and L is a k-dimensional linear subspace of $\mathbb{F}_2^n$. We denote the cardinality of the set S by $\#S$, the set $\{x \oplus s \mid s \in S\}$ by $x \oplus S$ and the set $\{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ by $\sup(f)$. *The Hamming distance* between two Boolean functions in n variables is the number of arguments on which these functions differ. A function f is *balanced on a set* S if $\#(\sup(f) \cap S) = \frac{1}{2}\#S$.

The degree of f ($\deg f$) is the degree of its *algebraic normal form* that is a representation of f as a polynomial over $\mathbb{F}_2$:

$$f(x_1, \ldots, x_n) = \bigoplus_{a\in\mathbb{F}_2^n} c_a x_1^{a_1} \ldots x_n^{a_n},\ c_a \in \mathbb{F}_2,\ \text{where}$$

$x_i^{a_i} \equiv x_i$ for $a_i = 1$ and $x_i^{a_i} \equiv 1$ for $a_i = 0$. A function is called *affine* if its degree is at most 1 and *quadratic* if its degree equals to 2. A function f is *affine on an affine subspace* L if $f(x) \oplus \langle a, x\rangle$ is constant on L for some $a \in \mathbb{F}_2^n$.

The Walsh–Hadamard transform of f is the mapping $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ such that

$$W_f(y) = \sum_{x\in\mathbb{F}_2^n} (-1)^{f(x)\oplus\langle y,x\rangle}.$$

The numbers $W_f(y)$ are called *the Walsh–Hadamard coefficients*. A Boolean function f in n variables, n is even, is *a bent function* if $|W_f(y)| = 2^{n/2}$ for all $y \in \mathbb{F}_2^n$. We denote by $\mathcal{B}_n$ the set of all bent functions in n variables. *The dual* function $\widetilde{f}$ is defined in the following way:

$$(-1)^{\widetilde{f}(y)} = 2^{-n/2} W_f(y),\ y \in \mathbb{F}_2^n.$$

The function $\widetilde{f}$ is a bent function too, and $\widetilde{\widetilde{f}} = f$ (see, for instance, [26]).

Two Boolean functions f, g in n variables are called *extended affinely equivalent* (*EA-equivalent*) if there exist an invertible n-by-n binary matrix A, a vector $b \in \mathbb{F}_2^n$ and an affine function ℓ in n variables such that

$$f(x) = g(xA \oplus b) \oplus \ell(x) \text{ for all } x \in \mathbb{F}_2^n.$$

Hereinafter, we suppose that n is even. In this work, we consider properties of a bent function construction $f \oplus \mathrm{Ind}_U$, where f is a given bent function in n variables and U is an affine subspace of arbitrary dimension. For $f \in \mathcal{B}_n$ and $0 \leq m \leq n$, we define

$$\mathrm{BS}_m(f) = \{f \oplus \mathrm{Ind}_U \mid U \text{ is an } m\text{-dimensional affine subspace of } \mathbb{F}_2^n\} \cap \mathcal{B}_n.$$

Note that for $f, g \in \mathcal{B}_n$ that are EA-equivalent $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(g)$ holds.

Necessary and sufficient conditions for $f \oplus \mathrm{Ind}_U$ to be a bent function were proven by C. Carlet [4].

Theorem 1 (C. Carlet, 1994) *Let $f \in \mathcal{B}_n$, $L \subseteq \mathbb{F}_2^n$ be a linear subspace and $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{a \oplus L}$ is a bent function if and only if any of the following equivalent conditions hold:*

1. *$D_\alpha f$ is balanced on $a \oplus L$ for all $\alpha \in \mathbb{F}_2^n \setminus L$;*
2. *$\widetilde{f}(x) \oplus \langle a, x \rangle$ is either constant or balanced on each coset of $L^\perp$.*

In the next section, additional details for the second condition of the criterion will be provided. They will be often used in the proofs.

Note that trivial subspace dimensions for $f \in \mathcal{B}_n$ are $n - 1$ and n. In these cases we just add an affine function to the bent function, i. e. the result is always a bent function too. It is also well known that $f \oplus \mathrm{Ind}_L$ is not a bent function if $\dim L < n/2$ (see [4]). Thus, we will focus on dimensions $n/2, n/2 + 1, \ldots, n - 2$.

3 A balanced representation

Let us introduce the following notion.

Definition 1 A Boolean function f in n variables has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$ if f is either constant or balanced on each coset of L.

Note that any function has a balanced representation by the 0-dimensional linear subspace. The same situation holds for a 1-dimensional linear subspace.

First of all, there are some additional details regarding balanced representations of bent functions. These statements mostly follow from Theorem 1 and [16].

Theorem 2 *Let $f \in \mathcal{B}_n$ and L be a linear subspace of* $\mathbb{F}_2^n$, $\dim L \leq n/2$. *Then the following holds.*

1. *Let f be constant on each of $a_1 \oplus L, \dots, a_m \oplus L$, where $a_1, \dots, a_m \in \mathbb{F}_2^n$, $m \in \mathbb{N}$, and be balanced on each other $a \oplus L$, where $a \in \mathbb{F}_2^n \setminus U$, $U = (a_1 \oplus L) \cup \ldots \cup (a_m \oplus L)$. Then $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$ and $\widetilde{f} \oplus \widetilde{f \oplus \mathrm{Ind}_U} = \mathrm{Ind}_{L^\perp}$.*
2. *f has a balanced representation by L if and only if f is constant on each of $2^{n-2\dim L}$ distinct cosets of L.*
3. *f cannot be constant on more than $2^{n-2\dim L}$ distinct cosets of L.*

Proof Starting with the first point, let us consider $W_f(x)$ and $W_{f\oplus\mathrm{Ind}_U}(x)$:

$$W_{f\oplus\mathrm{Ind}_U}(x) = \sum_{y\notin U}(-1)^{f(y)\oplus\langle x,y\rangle} + \sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle\oplus 1} =$$

$$W_f(x) - 2\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle} = W_f(x) - 2\sum_{i=1}^{m}\sum_{y\in a_i\oplus L}(-1)^{f(a_i)\oplus\langle x,y\rangle}.$$

Since the function $y \mapsto \langle x, y\rangle$ (here x is a fixed parameter) is balanced on any $a_i \oplus L$ if $x \notin L^\perp$, it holds that $W_f(x) = W_{f\oplus\mathrm{Ind}_U}(x)$ for $x \notin L^\perp$.

Next, let $x \in L^\perp$. In this case, we use the following:

$$W_{f\oplus\mathrm{Ind}_U}(x) = W_f(x) - 2\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle}.$$

It can be seen that $\sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle} = W_f(x)$. Indeed, $\langle x, z\rangle \equiv \text{const}$ on $z \in y \oplus L$, $y \notin U$, and, therefore, $f(z) \oplus \langle x, z\rangle$ is balanced on $y \oplus L$. Thus, $\sum_{y\notin U}(-1)^{f(y)\oplus\langle x,y\rangle} = 0$ and $W_f(x) = \sum_{y\in U}(-1)^{f(y)\oplus\langle x,y\rangle}$, i. e. $W_{f\oplus\mathrm{Ind}_U}(x) = -W_f(x)$. At the same time, $W_f(x) = \pm 2^{n/2}$. Consequently, $f \oplus \mathrm{Ind}_U$ is a bent function. Also, $W_{f\oplus\mathrm{Ind}_U}(x) = W_f(x)$ if and only if $x \notin L^\perp$. The first point is proven.

We can see that the first point implies that $m = 2^{n-2\dim L}$, since $\#L^\perp = 2^{n-\dim L}$ and it is well known that the duality mapping preserves the Hamming distance between bent functions (see, for instance, [4]). Some results related to this mapping can be found in [18]. This proves the first half of the second point. To complete the second point and to prove the third point, we refer to [16, Lemma 8]. □

Corollary 1 *Let f, $f \oplus \mathrm{Ind}_{a\oplus L} \in \mathcal{B}_n$, where L is a linear subspace of $\mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$. Then $\mathrm{sup}(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L})) = (a_1 \oplus L^\perp) \cup \ldots \cup (a_{2^{n-2\dim L^\perp}} \oplus L^\perp)$, where $f(x) \oplus \langle a, x\rangle$ is constant on each of $a_i \oplus L^\perp$ (each two of them are distinct). Note that this does not guarantee that $\mathrm{sup}(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$ is an affine subspace.*

The case of $\dim L = n/2$ is especially interesting for bent functions. A large class of normal bent functions for this representation was introduced by H. Dobbertin [13]. Also, any bent function represented by the concatenation of affine functions in k variables [5, 24, 29] has a balanced representation by some k-dimensional linear subspace.

Note that the algorithm described in [3] can find all balanced representations of bent functions $f(x) \oplus \langle a, x\rangle$ for all $a \in \mathbb{F}_2^n$, i. e. all elements of $\mathrm{BS}_m(\widetilde{f})$. Such algorithms have many applications (see, for instance, [1]).

4 Subspaces and superspaces of U where $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$

In this section, we consider a possibility to increase and decrease the dimension of a subspace by 1 which is suitable for the construction. Let us start with balanced representations.

Proposition 1 *Suppose that $f \in \mathcal{B}_n$ has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$. Then*

1. *f has a balanced representation by $L \cup (a \oplus L)$, where $a \in \mathbb{F}_2^n \setminus L$, if and only if $a \oplus U = U$, where U is the union of all cosets of L such that f is constant on each of them.*
2. *f has a balanced representation by $L_w = \{x \in L \mid \langle w, x\rangle = 0\}$, where $w \in \mathbb{F}_2^n L^{\perp}$, if and only if $f(x) \oplus \langle w, x\rangle$ has a balanced representation by L.*

Proof To prove the first point, it is enough to note that f is either constant or balanced on $L \cup (a \oplus L)$ if and only if there are no cases when f is constant on $x \oplus L$ and balanced on $a \oplus x \oplus L$. It is equivalent to $a \oplus U = U$.

Let us consider the second point. Since $w \notin L^{\perp}$, $L = L_w \cup (s \oplus L_w)$ for some $s \in L$ such that $\langle w, s\rangle = 1$. First of all, let $b \in U$. Then f is constant on $b \oplus L_w$ and $b \oplus s \oplus L_w$, i. e. U consists of $2 \cdot 2^{n-2\dim L}$ cosets of L_w. At the same time, $f(x) \oplus \langle w, x\rangle$ is not constant on $b \oplus L$ since $\langle w, b\rangle \neq \langle w, b \oplus s\rangle$.

Let $b \notin U$. Therefore, f is balanced on $b \oplus L$. As a consequence, f is constant on $b \oplus L_w$ if and only if f is constant on $b \oplus s \oplus L_w = (b \oplus L) \setminus (b \oplus L_w)$. Note that $f(x) \oplus \langle w, x\rangle = f(x) \oplus \langle w, b\rangle$ for $x \in b \oplus L_w$ and $f(x) \oplus \langle w, x\rangle = f(x) \oplus \langle w, b\rangle \oplus 1$ for $x \in b \oplus s \oplus L_w$. It implies that $f(x) \oplus \langle w, x\rangle$ is constant on $b \oplus L$ if and only if f is constant on $b \oplus L_w$ and $b \oplus s \oplus L_w$.

Hence, f is constant on $2^{n-2\dim L_w} = 2 \cdot 2^{n-2\dim L} + 2 \cdot 2^{n-2\dim L}$ distinct cosets of L_w if and only if $f(x) \oplus \langle w, x\rangle$ is constant on $2^{n-2\dim L}$ distinct cosets of L. Theorem 2 completes the proof. □

The following property follows from the previous proposition. Theorem 1 and bent function distance properties can also provide it.

Proposition 2 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$, where L is an affine subspace of $\mathbb{F}_2^n$. Let $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{L \cup (a \oplus L)} \in \mathcal{B}_n$ if and only if $f \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_n$.*

Proof Without loss of generality, we assume that L is a linear subspace. Otherwise, we can consider $f(x \oplus b)$ instead of f, where $b \in L$. If $a \in L$, the statement is obvious. Let $a \notin L$. First of all, Theorem 1 provides that $\tilde{f}$ has a balanced representation by $L^{\perp}$. Next, $(L \cup (a \oplus L))^{\perp} = \{x \in L^{\perp} \mid \langle a, x\rangle = 0\} = (L^{\perp})_a$, where $(L^{\perp})_a$ is defined in the second point of Proposition 1. According to this point, $\tilde{f}$ has a balanced representation by $(L^{\perp})_a$ if and only if $\tilde{f}(x) \oplus \langle a, x\rangle$ has a balanced representation by $L^{\perp}$. Theorem 1 completes the proof. □

Let us rewrite the first point of Proposition 1 in terms of the construction.

Proposition 3 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$, where L is an affine subspace of $\mathbb{F}_2^n$. Let $a \in \mathbb{F}_2^n$ and $L_a = \{x \in L \mid \langle a, x\rangle = 0\}$. Then $f \oplus \mathrm{Ind}_{L_a} \in \mathcal{B}_n$ if and only if $D_a \tilde{f} \equiv D_a(\widetilde{f \oplus \mathrm{Ind}_L})$.*

Proof It is easy to see that $D_a\widetilde{f} \equiv D_a(\widetilde{f \oplus \mathrm{Ind}_L})$ is equivalent to $a \oplus U = U$, where $U = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$. Without loss of generality, we can assume that L is a linear subspace, similarly to Proposition 2. Let $L' = \{x \in L \mid \langle a, x\rangle = 0\}$. If $L' = L$, the statement is obvious: it means that $a \in L^{\perp}$ and we know that U is the union of cosets of $L^{\perp}$. In other cases, either $L_a = L'$ or $L_a = L \setminus L'$, where $\dim L' = \dim L - 1$. According to Proposition 1, $\widetilde{f}$ has a balanced representation by $L'^{\perp} = L^{\perp} \cup (a \oplus L^{\perp})$ if and only if $a \oplus U = U$. Thus, $f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n$ if and only if $a \oplus U = U$. In light of Proposition 2, it does not matter whether $L_a = L'$ or $L_a = L \setminus L'$. □

Note that Propositions 1, 2 and 3 give nontrivial conditions to increase and decrease the dimension of a subspace. It looks like it is rather hard to construct a subspace or a superspace of the given one. In other words, nonempty $\mathrm{BS}_m(f)$, in general, does not guarantee that $\mathrm{BS}_{m+1}(f)$ and $\mathrm{BS}_{m-1}(f)$ are nonempty too. It is confirmed by the computational experiments and by the results obtained in Sections 5.1 and 6.2 that are dedicated to bent functions with empty $\mathrm{BS}_m(f)$.

It is known [4] that the set $\sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$ is always an affine subspace for f, $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$ and an $n/2$-dimensional U. Next, we prove that the same is true for an $(n/2 + 1)$-dimensional subspace.

Theorem 3 *Let* $f \in \mathcal{B}_n$ *and* $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$*, where* U *is an affine subspace of* $\mathbb{F}_2^n$ *of dimension at most* $n/2 + 1$*. Then* $\sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$ *is an affine subspace too.*

Proof The case of $\dim U = n/2$ is obvious. Suppose that $\dim U = n/2 + 1$. By Theorem 1, let us move to a balanced representation by $L^{\perp}$ for $g(x) = \widetilde{f}(x) \oplus \langle a, x\rangle$, where $a \oplus L = U$, L is a linear subspace. According to Corollary 1, we have $2^{n-2\dim L^{\perp}} = 2^2 = 4$ "constant" cosets C_1, C_2, C_3, C_4 of $L^{\perp}$, i. e. $C_1 \cup C_2 \cup C_3 \cup C_4 = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_U}))$. Without loss of generality, we can suppose that $g|_{C_1} \equiv g|_{C_2}$. By Theorem 2, the function g has a balanced representation by the affine subspace $C_1 \cup C_2$ of dimension $n/2$. But Proposition 1 provides that there exists $a \notin L^{\perp}$ such that $a \oplus (C_1 \cup C_2 \cup C_3 \cup C_4) = C_1 \cup C_2 \cup C_3 \cup C_4$. Since $a \notin L^{\perp}$, it holds $a \oplus C_{i_1} = C_{i_2}$ and $a \oplus C_{i_3} = C_{i_4}$ for some $\{i_1, i_2, i_3, i_4\} = \{1, 2, 3, 4\}$. It means that $a \oplus (C_{i_1} \cup C_{i_3}) = C_{i_2} \cup C_{i_4}$. Since $C_{i_1} \cup C_{i_3}$ is an affine subspace, $(C_{i_1} \cup C_{i_3}) \cup (C_{i_2} \cup C_{i_4}) = C_1 \cup C_2 \cup C_3 \cup C_4$ is an affine subspace too. □

An important corollary of the theorem is the following proposition.

Proposition 4 *Let* $f \in \mathcal{B}_n$ *and* $f \oplus \mathrm{Ind}_L \in \mathcal{B}_n$*, where* L *is an* $(n/2+1)$*-dimensional affine subspace of* $\mathbb{F}_2^n$*. Then there exists an* $n/2$*-dimensional affine subspace* $L' \subset L$ *such that* $f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n$*.*

Proof Due to Theorem 3, let $U = \sup(\widetilde{f} \oplus (\widetilde{f \oplus \mathrm{Ind}_L}))$ be a coset of a linear subspace U'. Since $L^{\perp} \subset U'$, Proposition 3 gives us that $f \oplus \mathrm{Ind}_{L_a} \in \mathcal{B}_n$, where $a \in U'$ and $a \notin L^{\perp}$. In this case $\dim L_a = n/2$. □

Proposition 4 claims that the case of $(n/2+1)$-dimensional L is equivalent to applying the construction twice for some $n/2$-dimensional $L' \subset L$ (that always exists by the proposition) and its shift $L \setminus L'$, i. e.

$$(f \oplus \mathrm{Ind}_{L'}) \oplus \mathrm{Ind}_{L \setminus L'} = f \oplus \mathrm{Ind}_L, \text{ where } f \oplus \mathrm{Ind}_{L'} \in \mathcal{B}_n.$$

5 Bounds for #BS$_m$(f)

The following theorem estimates #BS$_m(f)$. It generalizes the upper bound from [16] that works for $m = n/2$.

Theorem 4 *For $f \in \mathcal{B}_n$ and $m \geq n/2$, it holds*

$$\#\mathrm{BS}_m(f) \leq 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{2m-n+2i}-1}{2^i-1}.$$

Moreover, for $m \leq n-2$, the bound is attained if and only if f is quadratic.

Proof To prove the bound, we refer to [16, Theorem 2]. In the first part of that theorem, the following was shown:

$$\#D^s(g) \leq 2^n \prod_{t=0}^{s-1} \frac{2^{n-2t}-1}{2\cdot(2^{t+1}-1)} = \#D^s(h),$$

where $g, h \in \mathcal{B}_n$, h is quadratic, $D^s(g)$ is the set of all s-dimensional affine subspaces such that g is affine on each of them.

Let $U \in D^s(g)$, i. e. $g(x) \oplus \langle a, x\rangle$ is constant on U for some $a \in \mathbb{F}_2^n$. Next, we define $\mathrm{nc}_g(U) = \#\{b \oplus U \mid g(x) \oplus \langle a, x\rangle \text{ is constant on } b \oplus U, b \in \mathbb{F}_2^n\}$.

Theorem 1 gives us that $\#\mathrm{BS}_{n-s}(\widetilde{g}) = \#P^s(g)$, where

$$P^s(g) = \{a \oplus L^\perp \mid a \in \mathbb{F}_2^n, L \text{ is a linear subspace of dimension } s$$
$$\text{and the function } g(x) \oplus \langle a, x\rangle \text{ has a balanced representation by } L\}.$$

Note that $a \oplus L^\perp = b \oplus L^\perp$ if and only if $\langle a, x\rangle \oplus \langle b, x\rangle$ is constant on $u \oplus L$, $a, b, u \in \mathbb{F}_2^n$. In other words, if $g(x) \oplus \langle a, x\rangle$ is constant on $u \oplus L$, then $g(x) \oplus \langle b, x\rangle$ is constant on $u \oplus L$ if and only if $a \oplus L^\perp = b \oplus L^\perp$. In light of Theorem 2, it implies that $\#P^s(g) = 2^{2s-n}\#\{U \in D^s(g) \mid \mathrm{nc}_g(U) = 2^{n-2s}\}$. Therefore, $\#\mathrm{BS}_{n-s}(\widetilde{g}) = \#P^s(g) \leq 2^{2s-n}\#D^s(g)$. According to [16, Proposition 4], $\mathrm{nc}_h(U) = 2^{n-2\dim U}$ for any $U \in D^s(h)$, i. e. $\#\mathrm{BS}_{n-s}(\widetilde{h}) = 2^{2s-n}\#D^s(h)$. As a result,

$$\#\mathrm{BS}_m(\widetilde{g}) \leq 2^{2(n-m)-n}\#D^{n-m}(g) \leq 2^{2(n-m)-n}2^n \prod_{t=0}^{n-m-1} \frac{2^{n-2t}-1}{2\cdot(2^{t+1}-1)} =$$

$$2^{n-m} \prod_{i=1}^{n-m} \frac{2^{n-2i+2}-1}{2^i-1} = 2^{n-m} \prod_{i=1}^{n-m} \frac{2^{n-2(n-m-i+1)+2}-1}{2^i-1} = \#\mathrm{BS}_m(\widetilde{h}).$$

It is more difficult to prove that the bound is attained only by quadratic functions for any $m \leq n-2$. The second part of the proof of [16, Theorem 2] gives us that $\#D^s(g) < \#D^s(h)$ if there exists $U \in D^2(g)$ such that $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$, where $s > 2$. Let us prove the existence of such U by contradiction. Note that we exclude the case of $\#D^2(g) = 0$ since it is straightforward.

Let g be not quadratic. Suppose that $\mathrm{nc}_g(U) = 2^{n-2\cdot 2}$ for any $U \in D^2(g)$. We consider any $U \in D^2(g)$, $U = u \oplus L$, where L is a linear subspace, $u \in \mathbb{F}_2^n$. Since $\mathrm{nc}_g(u \oplus L) = 2^{n-2\cdot 2}$, Theorem 2 provides that $g_a(x) = g(x) \oplus \langle a, x\rangle$ for some $a \in \mathbb{F}_2^n$ has a balanced representation by L, i. e. g_a is either constant or balanced on each coset of L. But any function balanced on 2-dimensional subspace is affine on it (see, for instance, [16, Proposition 2]). Thus, g_a is affine on each coset of L. As a consequence, $g(x) = g_a(x) \oplus \langle a, x\rangle$ is affine on each coset of L as well. Hence, g is completely affinely decomposable of order 2.

Recall that g is completely affinely decomposable of order 2 if 1) g is affine on at least one 2-dimensional affine subspace; 2) if g is affine on a 2-dimensional affine subspace, then g is affine on any its coset as well. It is known [16, Theorem 1] that only affine and quadratic functions can satisfy these conditions, which contradicts the choice of g.

Thus, there exists $U \in D^2(g)$ such that $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$. In other words, $\#D^s(g) < \#D^s(h)$ for any $s > 2$. It implies that $\#\mathrm{BS}_m(\widetilde{g}) < \#\mathrm{BS}_m(\widetilde{h})$ for any $m < n-2$. Let us consider $s = 2$. Since $\mathrm{nc}_g(U) < 2^{n-2\cdot 2}$, it can be seen that $\#\mathrm{BS}_{n-2}(\widetilde{g}) = \#P^2(g) < 2^{2\cdot 2-n}\#D^2(g) \leq 2^{2\cdot 2-n}\#D^2(h) = \#\mathrm{BS}_{n-2}(\widetilde{h})$. Finally, we choose $\widetilde{f}$ as g since f is quadratic if and only if $\widetilde{f}$ is quadratic. The same is true for h. □

5.1 Bent functions with $\#\mathrm{BS}_m(f) = 0$

Let us show that $\#\mathrm{BS}_m(f) = 0$ for some $f \in \mathcal{B}_n$ and some m. First of all, the following necessary condition for derivatives holds.

Lemma 1 *Let $f \in \mathcal{B}_n$ and the function $f(x) \oplus \langle w, x\rangle$, $w \in \mathbb{F}_2^n$, have a balanced representation by a linear subspace L, $\dim L \geq 2$. Then $D_L f \equiv 0$.*

Proof First of all, $D_L\langle w, x\rangle \equiv 0$ since $\dim L \geq 2$. Next, let us recall that $D_L f(x) = \bigoplus_{a\in L} f(x \oplus a)$. Since f is either constant or balanced on a fixed $x \oplus L$, the number of ones among $f(x \oplus a)$, $a \in L$, is either 0 or $2^{\dim L-1}$ or $2^{\dim L}$, i. e. it is always even. Therefore, $D_L f(x) = 0$ for any $x \in \mathbb{F}_2^n$. □

This subsection focuses on *the Kasami* bent functions. It was proven [12, 19] that the functions of the form $f(x) = \mathrm{tr}(\alpha x^{2^{2k}-2^k+1})$ are bent, where

- $\alpha, x \in \mathbb{F}_{2^n}$, $\mathbb{F}_{2^n}$ is the field with 2^n elements and n is even;
- $\mathrm{tr}(y) = y^{2^0} + y^{2^1} + \ldots + y^{2^{n-1}}$, $y \in \mathbb{F}_{2^n}$, $\mathrm{tr}(y)$ always belongs to $\mathbb{F}_2$;
- $0 < k < n$ and $\gcd(k, n) = 1$;
- $\alpha \notin \{y^3 \mid y \in \mathbb{F}_{2^n}\}$. Note that $\{y^3 \mid y \in \mathbb{F}_{2^n}\} \neq \mathbb{F}_{2^n}$ if n is even.

These functions are called the Kasami bent functions. Though they map $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, we can fix a basis of $\mathbb{F}_{2^n}$ (since it is a vector space over $\mathbb{F}_2$) and consider them as Boolean functions. It is well known that $\deg f = k+1$ for $0 < k < n/2$ and $\deg f = n-k+1$ for $n/2 < k < n$.

In A. Gorodilova's work [15] the properties of $D_L f$ of the Kasami functions were studied. We note the following result.

Theorem 5 (A. Gorodilova, 2013) *Let f be a Kasami bent function in n variables of degree t, $n \geq 8$ is even. Then $D_L f \not\equiv 0$ for any k-dimensional linear subspace L, where*

$$k \leq \begin{cases} t-2, & \text{if } 4 \leq t \leq (n+3)/3; \\ t-3, & \text{if } (n+3)/3 < t \leq n/2. \end{cases}$$

These derivatives for 2-dimensional L were also studied in [27]: using the derivatives, D. Sharma et al. proved that a nonquadratic Kasami bent function does not belong to the Maiorana–McFarland class.

In light of these results, it is not difficult to prove that

Theorem 6 *There exists a Kasami bent function f in n variables such that $\#\mathrm{BS}_m(\widetilde{f}) = 0$, where*

$$n - 2 \geq m \geq \begin{cases} n/2 + 3, & \textit{if } 4 \mid n \textit{ or } n = 10; \\ n/2 + 4, & \textit{otherwise.} \end{cases}$$

Proof Recall that there exists a Kasami bent function in n variables of degree $n/2$ if $4 \mid n$ and of degree $n/2 - 1$ for other even n. In the first case, $\gcd(n, n/2 - 1) = 1$ allows us to construct a Kasami bent function f of degree $n/2$. In the second case, $\gcd(n, n/2-2) = 1$ and, similarly, there exists a Kasami function f of degree $n/2 - 1$. According to Lemma 1 and Theorem 5, these Kasami functions (even if we add an affine function) cannot have a nontrivial balanced representation by a subspace of dimension at most $n/2-3$ and $n/2-4$ respectively. The case of $n = 10$ satisfies $4 \leq t \leq (10 + 3)/3$ case of Theorem 5 and can be considered as the first case. Thus, Theorem 1 provides that $\#\mathrm{BS}_m(\widetilde{f}) = 0$, where $n - 2 \geq m \geq n - (n/2 - 3)$ for the first case and $n - 2 \geq m \geq n - (n/2 - 4)$ for the second case. □

Let us note that in Section 6.2 we consider bent functions $f \in \mathcal{B}_n$ such that $\#\mathrm{BS}_m\,(f) = 0$ for $m \leq n/2 + 3$. In some sense, these examples complement Theorem 6: in this section we focus on $m = n - 2, n - 3, \ldots$, in Section 6.2 we focus on $m = n/2, n/2 + 1, \ldots$. Unfortunately, at the moment there is no example of a bent function $f \in \mathcal{B}_n$, where n is arbitrary, such that $\#\mathrm{BS}_m(f) = 0$ for any $m \leq n - 2$.

6 $\mathrm{BS}_m(f_{+2})$ for the iteratively constructed bent function f_{+2}

Let us consider the simplest iterative construction of a bent function f_{+2} by $f \in \mathcal{B}_n$:

$$f_{+2}(x_1, \ldots, x_{n+2}) = f(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Recall that $f_{+2} \in \mathcal{B}_{n+2}$ if and only if $f \in \mathcal{B}_n$. Also, it holds

$$\widetilde{f_{+2}}(x_1, \ldots, x_{n+2}) = \widetilde{f}(x_1, \ldots, x_n) \oplus x_{n+1}x_{n+2}.$$

Since f and f_{+2} have different number of variables, let us define

$$\mathrm{pj}_n(x) = (x_1, \ldots, x_n) \text{ and } \mathrm{pj}_n(S) = \{\mathrm{pj}_n(x) \mid x \in S\},$$

where $x \in \mathbb{F}_2^{n+2}$ and $S \subseteq \mathbb{F}_2^{n+2}$. Also, $\mathbb{F}_2^n(S) = \{x \in \mathbb{F}_2^n \mid (x, 0, 0) \in S\}$.

In this section, we establish the connection between $\mathrm{BS}_{m-1}(f)$, $\mathrm{BS}_{m-2}(f)$ and $\mathrm{BS}_m(f_{+2})$.

6.1 Balanced representations of iteratively constructed functions

Recall that $f \in \mathcal{B}_n$ is normal if it has a balanced representation by some $n/2$-dimensional L. Hence, the result of this subsection (Theorem 7 and the bellow proposition) is a generalization of the normal bent function property "f is normal if and only if f_{+2} is normal" which was proven in [3] (see also [8]).

Proposition 5 *Let $f \in \mathcal{B}_n$ have a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^n$. Then the bent function f_{+2} has balanced representations by*

1. $L_0 = \{(x, 0, 0) \mid x \in L\}$, *i. e.* $\dim L_0 = \dim L$;
2. $L_1 = \{(x, y, 0) \mid x \in L, y \in \mathbb{F}_2\}$, *i. e.* $\dim L_1 = \dim L + 1$.

Let us establish which balanced representations of f exist if we have some balanced representation of f_{+2}.

Theorem 7 *Let $f \in \mathcal{B}_n$ and suppose that f_{+2} has a balanced representation by a linear subspace $L \subseteq \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$, where $\dim L - 1 \leq \dim L' \leq \dim L$, such that f has a balanced representation by L'. Moreover, $\mathbb{F}_2^n(L) \subseteq L' \subseteq \mathrm{pj}_n(L)$ holds.*

Proof Let $x = (x_1, \dots, x_{n+2}) \in \mathbb{F}_2^{n+2}$. For convenience, we rename the variables of both functions, that is, consider $f(x_3, \dots, x_{n+2})$ and $f_{+2}(x) = x_1x_2 \oplus f(x_3, \dots, x_{n+2})$, where the function f is defined on the set

$$\Gamma = \{\widetilde{x} \mid x \in \mathbb{F}_2^{n+2}\} \subseteq \mathbb{F}_2^{n+2}, \ \widetilde{x} = (0, 0, x_3, \dots, x_{n+2}).$$

We work with $\mathbb{F}_2^n(L)$ and $\mathrm{pj}_n(L)$ taking into account the new notation, i. e. $\mathrm{pj}_n(x) = \widetilde{x} \in \Gamma$ and $\mathbb{F}_2^n(L) = L \cap \Gamma$.

Suppose that f_{+2} has a balanced representation by a $(t+1)$-dimensional subspace $L \subseteq \mathbb{F}_2^{n+2}$. By Theorem 2, it is constant on each of $s^1 \oplus L, \dots, s^m \oplus L$ which are distinct, $s^1, \dots, s^m \in \mathbb{F}_2^{n+2}$ and $m = 2^{n-2t}$. Let $L' = L \cap \Gamma$. Since $\dim \Gamma = n$, then $\dim L' \in \{t+1, t, t-1\}$.

Case 1 $\dim L' = t + 1$. Therefore, $L = L' \subseteq \Gamma$, i. e. any coset of L' either belongs to Γ or does not intersect with Γ. Since $f(a \oplus x) = f_{+2}(a \oplus x)$ for all $x \in L', a \in \Gamma$, the function f is either constant or balanced on each coset of L' which belongs to Γ. Hence, it has balanced representation by $L' = L$. Moreover, $L' = \mathbb{F}_2^n(L)$ holds.

Case 2 $\dim L' = t$. Then for some fixed $\alpha \in L \setminus L'$ we can represent any $x \in L$ as $x = x' \oplus y\alpha$, where $x' \in L'$, $y \in \mathbb{F}_2$. Fixing some $s \in \mathbb{F}_2^{n+2}$, it holds

$$\begin{aligned} f_{+2}(s \oplus y\alpha \oplus x') \ &= \ f(\widetilde{s} \oplus y\widetilde{\alpha} \oplus x') \oplus (s_1 \oplus y\alpha_1)(s_2 \oplus y\alpha_2) = f(\widetilde{s} \oplus y\widetilde{\alpha} \oplus x') \\ &\oplus(\alpha_1 s_2 \ \oplus \ \alpha_2 s_1 \oplus \alpha_1\alpha_2)y \oplus s_1s_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2. \end{aligned} \tag{1}$$

Let us consider $S = (s^1 \oplus L) \cup \ldots \cup (s^m \oplus L)$. It is obvious that $\#S = m2^{t+1}$. Note that if f_{+2} is constant on $s \oplus L$, $s \in S$, then f_{+2} is constant on $a \oplus s \oplus L$ for $a = (\alpha_1, \alpha_2, 0, \dots, 0) \in \mathbb{F}_2^{n+2}$ too. Indeed, $(\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2)y = (\alpha_1(s_2 \oplus \alpha_2) \oplus \alpha_2(s_1 \oplus \alpha_1) \oplus \alpha_1\alpha_2)y$ for any $y \in \mathbb{F}_2$, that is why (1) gives us

$$\begin{gathered} f_{+2}(s \oplus a \oplus y\alpha \oplus x') = f_{+2}(s \oplus y\alpha \oplus x') \oplus \\ \alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2. \end{gathered}$$

At the same time, Theorem 2 claims that the bent function f_{+2} cannot be constant on more than m distinct cosets. Therefore, $a \oplus S = S$. Since $a \in L \setminus L'$, it holds $(\alpha_1, \alpha_2) \neq (0, 0)$. Let us consider two subcases.

Case 2.1 $a \in L$. In this case we can suppose that $\alpha = a$. Then, fixing some $s \in S$, equality (1) transforms to

$$\begin{aligned} f_{+2}(s) = f_{+2}(s \oplus y\alpha \oplus x') = f(\widetilde{s} \oplus x') \oplus (\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2)y \\ \oplus s_1s_2 \text{ for all } x' \in L' \text{ and } y \in \mathbb{F}_2. \end{aligned} \tag{2}$$

On the one hand, f is constant on each $u \oplus L'$, where $u \in \widetilde{S} = \{\widetilde{s} \mid s \in S\}$. On the other hand, $f(\widetilde{s} \oplus x')$ does not depend on y. It means that $\alpha_1 s_2 \oplus \alpha_2 s_1 \oplus \alpha_1\alpha_2 = 0$ for all

$s \in S$. Thus, for two elements of $\mathbb{F}_2^2$ given as (s_1, s_2), the equality does not hold. Therefore, $\#\widetilde{S} \geq \#S/2 = m2^t$. But in this case we have at least $m = m2^t/2^{\dim L'}$ distinct cosets of L' such that f is constant on each of them. By Theorem 2, f has a balanced representation by t-dimensional L'. Note that $\mathbb{F}_2^n(L) = L' = \mathrm{pj}_n(L)$ holds.

Case 2.2 $a \notin L$. Let us consider $L'' = L \cup (a \oplus L)$, $\dim L'' = t + 2$. Since $a \oplus S = S$, the first point of Proposition 1 provides that f_{+2} has a balanced representation by L''. To conclude the case, it is enough to note that any element $x \in L''$ can be represented as $x = x' \oplus \alpha y \oplus az = x' \oplus y(\alpha \oplus a) \oplus (z \oplus y)a = x' \oplus y\beta \oplus z'a$, where $\beta = \alpha \oplus a \in \Gamma$, $x' \in L'$, $y, z' \in \mathbb{F}_2$. Hence, we obtain that f_{+2} has a balanced representation by $(t+2)$-dimensional L''. At the same time, $\dim L'' \cap \Gamma = t + 1$ and $a \in L''$. It means that we can apply the case 2.1 to the subspace L'' and the element a. As a result, the function f has a balanced representation by $(t + 2 - 1)$-dimensional $L' \cup (\beta \oplus L') = U$. Also, $\mathbb{F}_2^n(L) \subset U \subseteq \mathrm{pj}_n(L)$ holds.

Case 3 $\dim L' = t - 1$. In this case there exist $\alpha, \beta \in L \setminus L'$ such that $(\alpha_1, \alpha_2) = (1, 0)$ and $(\beta_1, \beta_2) = (0, 1)$. Any element $x \in s^i \oplus L$, $i \in \{1, \ldots, m\}$, can be represented as $x = s^i \oplus x' \oplus y\alpha \oplus z\beta$, where $x' \in L'$, $y, z \in \mathbb{F}_2$. Without loss of generality, let us suppose that $s^i \in \Gamma$ (otherwise, we can consider $s^i \oplus \alpha$, $s^i \oplus \beta$ or $s^i \oplus \alpha \oplus \beta$ instead of s^i). Next, for any fixed $i \in \{1, \ldots, m\}$ it holds

$$f(s^i) = f_{+2}(s^i) = f_{+2}(s^i \oplus x) = f_{+2}(s^i \oplus x' \oplus y\alpha \oplus z\beta) = \\ f(s^i \oplus x' \oplus y\widetilde{\alpha} \oplus z\widetilde{\beta}) \oplus yz \text{ for all } x' \in L' \text{ and } y, z \in \mathbb{F}_2. \quad (3)$$

Thus, f is constant on each of $s^i \oplus L'$, $s^i \oplus \widetilde{\alpha} \oplus L'$, $s^i \oplus \widetilde{\beta} \oplus L'$ and $s^i \oplus \widetilde{\alpha} \oplus \widetilde{\beta} \oplus L'$.

We consider the subspace $L'' = L' \cup (\widetilde{\alpha} \oplus \widetilde{\beta} \oplus L')$. Let us show that $\dim L'' = t$. It is equivalent to $\widetilde{\alpha} \oplus \widetilde{\beta} \notin L'$. Indeed, fixing $x' = 0$, (3) provides that

$$f(s^i) = f_{+2}(s^i) = f_{+2}(s^i \oplus \alpha \oplus \beta) = f(s^i \oplus \widetilde{\alpha} \oplus \widetilde{\beta}) \oplus 1,$$

but f is constant on $s^i \oplus L'$. It means that $\widetilde{\alpha} \oplus \widetilde{\beta} \notin L'$.

Next, we prove that f is constant on each of $s^i \oplus \widetilde{\alpha} \oplus L''$. Note that $s^i \oplus \widetilde{\alpha} \oplus L'' = (s^i \oplus \widetilde{\alpha} \oplus L') \cup (s^i \oplus \widetilde{\beta} \oplus L')$. According to (3),

$$f(s^i \oplus \widetilde{\alpha}) = f_{+2}(s^i \oplus \alpha) = f_{+2}(s^i \oplus \beta) = f(s^i \oplus \widetilde{\beta}).$$

At the same time, f is constant on both $s^i \oplus \widetilde{\alpha} \oplus L'$ and $s^i \oplus \widetilde{\beta} \oplus L'$, i. e. it is constant on their union.

The rest of the case is to prove that all $s^i \oplus \widetilde{\alpha} \oplus L''$ are distinct. Suppose that $s^i \oplus \widetilde{\alpha} \oplus s^j \oplus \widetilde{\alpha} = s^i \oplus s^j \in L''$ for $i \neq j$, where $i, j \in \{1, \ldots, m\}$. But $s^i \oplus s^j \notin L' \subseteq L$ by the choice. Therefore, $s^i \oplus s^j \in \widetilde{\alpha} \oplus \widetilde{\beta} \oplus L'$. In other words, $s^i = s^j \oplus \widetilde{\alpha} \oplus \widetilde{\beta} \oplus x'$, $x' \in L'$. By (3) and the definition of f_{+2}, we obtain that

$$f_{+2}(s^i) = f_{+2}(s^i \oplus y\alpha \oplus z\beta) = f(s^i \oplus y\widetilde{\alpha} \oplus z\widetilde{\beta}) \oplus yz = \\ f(s^j \oplus (y \oplus 1)\widetilde{\alpha} \oplus (z \oplus 1)\widetilde{\beta} \oplus x') \oplus (y \oplus 1)(z \oplus 1) \oplus y \oplus z \oplus 1 = \\ f_{+2}(s^j \oplus (y \oplus 1)\alpha \oplus (z \oplus 1)\beta \oplus x') \oplus y \oplus z \oplus 1 \text{ for all } y, z \in \mathbb{F}_2.$$

But $f_{+2}(s^j \oplus (y \oplus 1)\alpha \oplus (z \oplus 1)\beta \oplus x') = f_{+2}(s^j)$. Hence, $f_{+2}(s^i) = f_{+2}(s^j) \oplus y \oplus z \oplus 1$ for all $y, z \in \mathbb{F}_2$, which is a contradiction. As a result, any two of $s^i \oplus \widetilde{\alpha} \oplus L''$ are distinct and f is constant on each of them. By Theorem 2, f has a balanced representation by L''. Note that $\mathbb{F}_2^n(L) \subset L'' \subset \mathrm{pj}_n(L)$ holds. □

6.2 The connection between $\mathrm{BS}_{m-1}(f)$, $\mathrm{BS}_{m-2}(f)$ and $\mathrm{BS}_m(f_{+2})$

Recall that Theorem 1 gives us the connection between an affine subspace U, for which $f \oplus \mathrm{Ind}_U$ is a bent function, and the balanced representation of the bent function $\widetilde{f}$. It means that the results obtained in Section 6.1 can help us to establish the connection between the sets $\mathrm{BS}_m(f)$ and $\mathrm{BS}_k(f_{+2})$.

Proposition 6 *Let $f \in \mathcal{B}_n$ and $f \oplus \mathrm{Ind}_U \in \mathcal{B}_n$, where U is an affine subspace of $\mathbb{F}_2^n$. Then both $f_{+2} \oplus \mathrm{Ind}_{U_1}$ and $f_{+2} \oplus \mathrm{Ind}_{U_2}$ are bent functions, where*

1. $U_1 = \{(x, y, 0) \mid x \in U, y \in \mathbb{F}_2\}$, *i. e.* $\dim U_1 = \dim U + 1$;
2. $U_2 = \{(x, y, z) \mid x \in U, y, z \in \mathbb{F}_2\}$, *i. e.* $\dim U_2 = \dim U + 2$.

Theorem 8 *Let $f_{+2} \in \mathcal{B}_{n+2}$ and $f_{+2} \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_{n+2}$, where $L \subseteq \mathbb{F}_2^{n+2}$ is a linear subspace, $a \in \mathbb{F}_2^{n+2}$. Then there exists a linear subspace $L' \subseteq \mathbb{F}_2^n$, where* $\dim L - 2 \leq \dim L' \leq \dim L - 1$, *such that $f \oplus \mathrm{Ind}_{\mathrm{pj}_n(a) \oplus L'} \in \mathcal{B}_n$. Moreover, $\mathbb{F}_2^n(L) \subseteq L' \subseteq \mathrm{pj}_n(L)$ holds.*

Proof By Theorem 1, $f_{+2} \oplus \mathrm{Ind}_{a \oplus L} \in \mathcal{B}_{n+2}$ if and only if $\widetilde{f}(x) \oplus \langle a, x\rangle$ has a balanced representation by $L^{\perp}$. Let us consider $f_{+2}(x \oplus a)$ instead of f_{+2}:

$$f_{+2}(x \oplus a) = f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a)) \oplus (x_{n+1} \oplus a_{n+1})(x_{n+2} \oplus a_{n+2}).$$

Since $(x_{n+1} \oplus a_{n+1})(x_{n+2} \oplus a_{n+2}) = x_{n+1}x_{n+2} \oplus a_{n+2}x_{n+1} \oplus a_{n+1}x_{n+2} \oplus a_{n+1}a_{n+2}$, we can exclude $\ell(x) = a_{n+2}x_{n+1} \oplus a_{n+1}x_{n+2} \oplus a_{n+1}a_{n+2}$ from $f_{+2}(x \oplus a)$: indeed, $g \oplus \mathrm{Ind}_U \in \mathcal{B}_{n+2}$ if and only if $g \oplus \ell \oplus \mathrm{Ind}_U \in \mathcal{B}_{n+2}$.

It means that $f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a)) \oplus x_{n+1}x_{n+2}$ has a balanced representation by $L^{\perp}$. According to Theorem 7, $f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a))$ has a balanced representation by L', where $\mathbb{F}_2^n(L^{\perp}) \subseteq L' \subseteq \mathrm{pj}_n(L^{\perp})$. Again, it implies that $f(\mathrm{pj}_n(x) \oplus \mathrm{pj}_n(a)) \oplus \mathrm{Ind}_{L'^{\perp}}(x)$ is a bent function. Consequently, $f \oplus \mathrm{Ind}_{\mathrm{pj}_n(a) \oplus L'^{\perp}}$ is a bent function too, where $(\mathrm{pj}_n(L^{\perp}))^{\perp} \subseteq L'^{\perp} \subseteq (\mathbb{F}_2^n(L^{\perp}))^{\perp}$.

To complete the proof, it is necessary to check the bounds for $L'^{\perp}$. The dimensions obviously satisfy the conditions. Next,

$$\begin{aligned}(\mathrm{pj}_n(L^{\perp}))^{\perp} = \{x \in \mathbb{F}_2^n \mid \langle x, y\rangle = 0 \text{ for any } y \in \mathrm{pj}_n(L^{\perp})\} =\\ \{x \in \mathbb{F}_2^n \mid \langle (x, 0, 0), y\rangle = 0 \text{ for any } y \in L^{\perp}\} =\\ (L^{\perp})^{\perp} \cap \{(x, 0, 0) \mid x \in \mathbb{F}_2^n\} = \mathbb{F}_2^n(L).\end{aligned}$$

We obtain that $(\mathrm{pj}_n(L))^{\perp} = (\mathrm{pj}_n((L^{\perp})^{\perp}))^{\perp} = \mathbb{F}_2^n(L^{\perp})$ from the above equality, i. e. $(\mathbb{F}_2^n(L^{\perp}))^{\perp} = \mathrm{pj}_n(L)$. As a result, $\mathbb{F}_2^n(L) \subseteq L'^{\perp} \subseteq \mathrm{pj}_n(L)$ holds. □

Theorem 8 allows us to preserve k zero values starting with $n/2$: if

$$\#\mathrm{BS}_{n/2}(f) = \#\mathrm{BS}_{n/2+1}(f) = \ldots = \#\mathrm{BS}_{n/2+k-1}(f) = 0, \text{ then}$$
$$\#\mathrm{BS}_{n/2+1}(f_{+2}) = \#\mathrm{BS}_{n/2+2}(f_{+2}) = \ldots = \#\mathrm{BS}_{n/2+k}(f_{+2}) = 0.$$

Computational experiments show that for the non-weakly normal bent function $f_{10} \in \mathcal{B}_{10}$ found in [20, Fact 14] the following holds.

Fact 1 For an affine subspace $U \subseteq \mathbb{F}_2^{10}$, $\dim U \leq 8$, $f_{10} \oplus \mathrm{Ind}_U \notin \mathcal{B}_{10}$ holds.

Together with Theorem 8, it implies the following:

Corollary 2 *For any $n \geq 10$, there exists a bent function $f \in \mathcal{B}_n$ such that $f \oplus \mathrm{Ind}_U \notin \mathcal{B}_n$ for any affine subspace $U \subseteq \mathbb{F}_2^n$ of dimension at most $n/2 + 3$.*

Remark 1 We do not consider the more general iterative construction $h(x, y) = f(x) \oplus g(y)$, where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^t$, for which we have the same "normal" property [8]: if g is normal, then h is normal if and only if f is normal. It is more difficult and $D_{(a,0)}D_{(0,b)}\widetilde{h} \equiv 0$ for any $a \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2^t$. According to Proposition 7 (see Section 6.3), $\mathrm{BS}_{n+t-2}(\widetilde{h})$ is always nonempty.

6.3 Exact number of functions in $\mathrm{BS}_n(f_{+2})$

Despite the bounds from Theorem 8, it seems impossible to obtain $\#\mathrm{BS}_m(f_{+2})$ by $\#\mathrm{BS}_{m-1}(f)$ and $\#\mathrm{BS}_{m-2}(f)$. Theorem 9 and computational experiments will clearly show this. The next proposition follows from [2, Theorem 8]. It can be proven directly by the second point of Theorem 1.

Proposition 7 (A. Canteaut, P. Charpin, 2003) *Let $f \in \mathcal{B}_n$, L be an $(n-2)$-dimensional linear subspace of $\mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$. Then $f \oplus \mathrm{Ind}_{a \oplus L}$ is a bent function if and only if $D_{L^\perp}\widetilde{f} \equiv 0$.*

Let us introduce

$$K_c(f) = \#\{\text{2-dimensional linear subspace } L \mid D_L f \equiv c\},\ c \in \mathbb{F}_2.$$

Proposition 7 implies that $\#\mathrm{BS}_{n-2}(\widetilde{f}) = 4K_0(f)$.

Theorem 9 *For any $f \in \mathcal{B}_n$ it holds*

$$\begin{aligned} K_0(f_{+2}) &= 10K_0(f) + 6K_1(f) + 3 \cdot 2^n - 3, \\ K_1(f_{+2}) &= 6K_0(f) + 10K_1(f) + 3 \cdot 2^n - 2. \end{aligned}$$

Proof Let us work with a Gauss–Jordan basis (GJB) of a 2-dimensional linear subspace of $\mathbb{F}_2^{n+2}$ (see, for instance, [3]). We need to define $\mathrm{lead}(a) = i$ such that $a_i = 1$ and $a_j = 0$ for all $j < i$, where $i, j \in \{1, \dots, n+2\}$. A pair of nonzero $a, b \in \mathbb{F}_2^{n+2}$ is a GJB of the linear subspace $\{0, a, b, a \oplus b\}$ if $\mathrm{lead}(a) > \mathrm{lead}(b)$ and $b_{\mathrm{lead}(a)} = 0$. For any linear subspace there exists a unique GJB.

Let $a = (a', \alpha), b = (b', \beta) \in \mathbb{F}_2^{n+2}$, where $a', b' \in \mathbb{F}_2^n$, $\alpha, \beta \in \mathbb{F}_2^2$. We note the following examples of GJBs:

$$\begin{array}{c|cccc|cc} \mathrm{b} & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline \mathrm{a} & 0 & 0 & 0 & 1 & 1 & 0 \end{array}, \quad \begin{array}{c|cccc|cc} \mathrm{b} & 0 & 1 & 1 & 0 & 1 & 0 \\ \hline \mathrm{a} & 0 & 0 & 0 & 0 & 0 & 1 \end{array}.$$

In the first example, $\mathrm{lead}(a) = 4$, $\mathrm{lead}(b) = 2$. Also, a', b' are linearly independent, α, β are linearly dependent. In the second example, $\mathrm{lead}(a) = 6$, $\mathrm{lead}(b) = 2$. Also, a', b' are linearly dependent, α, β are linearly independent.

Let us count the number of GJBs a, b that correspond to $D_L f \equiv c$, $c \in \mathbb{F}_2$. Firstly, it is easy to see that $D_L f_{+2}(x) = D_{a'}D_{b'}f(x_1, \dots, x_n) \oplus D_\alpha D_\beta x_{n+1}x_{n+2}$. Note that $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv d$, where $d \in \mathbb{F}_2$. It means that $D_L f_{+2} \equiv c$ if and only if $D_{a'}D_{b'}f \equiv c \oplus d$. Also, the following holds:

1. $D_\alpha D_\beta x_{n+1}x_{n+2} \equiv 1$ if and only if α, β are linearly independent;

2. $D_{a'} D_{b'} f \equiv 0$ for linearly dependent a', b'.

Next, we calculate $K_0(f_{+2})$. All the desired subspaces satisfy one of the independent cases:

Case 1 a' and b' are linearly independent. There are two subcases here:

Case 1.1 $D_{a'} D_{b'} f \equiv 0$ and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 0$. There are $K_0(f)$ possibilities to choose a GJB a', b'. According to point 1, any linearly dependent α, β can be chosen, there are exactly 10 such pairs. We obtain $10K_0(f)$ GJBs.

Case 1.2 $D_{a'} D_{b'} f \equiv 1$ and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 1$. Similarly to the previous case, there are $6K_1(f)$ distinct GJBs, since α, β are linearly independent; there are exactly 6 such pairs (α, β).

Case 2 a' and b' are linearly dependent (it holds $D_{a'} D_{b'} f \equiv 0$ by point 2) and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 0$. To form a GJB (a, b) by linearly dependent a', b', $a' = 0$ is necessary. Any nonzero vector can be chosen as b' (we do not consider $b' = 0$ since α, β are linearly dependent too). Next, any of 3 nonzero elements can be chosen as α: $(1, 0)$, $(0, 1)$ or $(1, 1)$. But $\beta_{\mathrm{lead}(\alpha)} = 0 \neq \alpha_{\mathrm{lead}(\alpha)}$, it means that the only way is $\beta = (0, 0)$. Finally, we have $3(2^n - 1)$ distinct GJBs. It means that $K_0(f_{+2}) = 10K_0(f) + 6K_1(f) + 3 \cdot 2^n - 3$.

We calculate $K_1(f_{+2})$ in the same way:

Case 1 a' and b' are linearly independent. Thus, there are two subcases:

Case 1.1 $D_{a'} D_{b'} f \equiv 0$ and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 1$, there are $6K_0(f)$ GJBs.

Case 1.2 $D_{a'} D_{b'} f \equiv 1$ and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 0$, there are $10K_1(f)$ GJBs.

Case 2 a' and b' are linearly dependent and $D_\alpha D_\beta x_{n+1} x_{n+2} \equiv 1$, i. e. α, β are linearly independent by point 1. Similarly to $K_0(f_{+2})$, $a' = 0$ is necessary. If $b' = 0$, the only way to choose (a, b) is $\alpha = (1, 0)$ and $\beta = (0, 1)$. Also, any $b' \neq 0$ can be chosen. In this case there are 3 possibilities for α: $(1, 0)$, $(0, 1)$ or $(1, 1)$. Since $\beta_{\mathrm{lead}(\alpha)} = 0$, the only way to choose linearly independent α, β is to set the rest non-leading coordinate of β to 1. Finally, we have $3(2^n - 1) + 1$ distinct GJBs.

As a result, $K_1(f_{+2}) = 6K_0(f) + 10K_1(f) + 3 \cdot 2^n - 2$. □

It can be seen that $K_0(f_{+2})$ and, as a result, $\#\mathrm{BS}_n(\widetilde{f_{+2}})$, depend on $K_0(f)$ and $K_1(f)$. Also, bounds from Theorem 8 bind $\mathrm{BS}_n(\widetilde{f_{+2}})$ only with $\mathrm{BS}_{n-2}(\widetilde{f})$: we do not consider $\mathrm{BS}_{n-1}(\widetilde{f})$ since it is trivial and has the same structure for any bent function f. Unfortunately, it looks like $K_1(f)$ has no direct connection to $\#\mathrm{BS}_{n-2}(\widetilde{f})$. Computational experiments for Maiorana–McFarland bent functions confirm this:

Fact 2 Let $f_8^i(x, y) = \langle x, \pi_i(y) \rangle$, $x, y \in \mathbb{F}_2^4$, $i \in \{1, 2\}$, and π_i be defined by

y	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$\pi_1(y)$	0100	1001	1010	0011	0101	0111	1011	1101	1100	1110	0010	1111	0001	0110	1000	0000 .
$\pi_2(y)$	0100	1001	1010	0011	1011	0111	0101	1100	1110	1101	0010	1111	0001	1000	0000	0110

Then $\#\mathrm{BS}_6(\widetilde{f_8^1}) = \#\mathrm{BS}_6(\widetilde{f_8^2})$, but $\#\mathrm{BS}_8(\widetilde{f^1_{8+2}}) \neq \#\mathrm{BS}_8(\widetilde{f^2_{8+2}})$:

	deg	K_0	K_1
f_8^1	4	43	40 .
f_8^2	4	43	64

Thus, it is not sufficient to know $\#\mathrm{BS}_{n-2}(f)$ to calculate $\#\mathrm{BS}_n(f_{+2})$. Nevertheless, Theorem 9 allows us to construct an infinite family of bent functions with $\#\mathrm{BS}_{n-2}(f) \neq \#\mathrm{BS}_{n-2}(\widetilde{f})$.

7 $\mathrm{BS}_m(f)$ and $\mathrm{BS}_m(\widetilde{f})$

In this section, we construct bent functions such that $\#\mathrm{BS}_m(f) \neq \#\mathrm{BS}_m(\widetilde{f})$.

Theorem 3 shows that the case of $m = n/2 + 1$ is very similar to the case of $m = n/2$: $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(\widetilde{f})$ for $m \leq n/2 + 1$. As a consequence, we have $\#\mathrm{BS}_m(f) = \#\mathrm{BS}_m(\widetilde{f})$ for any $f \in \mathcal{B}_2 \cup \mathcal{B}_4 \cup \mathcal{B}_6$ and any m. It seems that the simplest example of f such that $\#\mathrm{BS}_m(f) \neq \#\mathrm{BS}_m(\widetilde{f})$ can be found in $\mathcal{B}_8$ for $m = 6$. Computational experiments show that the following fact holds.

Fact 3 Let $\xi_8(x, y) = \langle x, \pi(y)\rangle$, where $x, y \in \mathbb{F}_2^4$, and π be defined by

y	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$\pi(y)$	1001	1010	0100	0011	0101	0111	1011	1101	1100	1110	0010	1111	0001	0110	1000	0000 .

Then $\#\mathrm{BS}_6(\xi_8) \neq \#\mathrm{BS}_6(\widetilde{\xi_8})$. More precisely, ξ_8 and $\widetilde{\xi_8}$ have

	deg	K_0	K_1
ξ_8	4	75	80 .
$\widetilde{\xi_8}$	4	59	64

Now, Fact 3 and Theorem 9 allow us to construct an infinite family of Maiorana–McFarland functions f_{2k} such that $\#\mathrm{BS}_{2k-2}(f_{2k}) \neq \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$. Also, it implies that f_{2k} and $\widetilde{f_{2k}}$ are not EA-equivalent.

Corollary 3 $\#\mathrm{BS}_{2k-2}(f_{2k}) < \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$ *holds, where the function* $f_{2k} \in \mathcal{B}_{2k}$, $k \geq 4$, *is defined by*

$$f_{2k}(x) = \xi_8(x_1, \ldots, x_8) \oplus x_9x_{10} \oplus x_{11}x_{12} \oplus \ldots \oplus x_{2k-1}x_{2k}, \ x \in \mathbb{F}_2^{2k}.$$

Proof It is easy to show by induction that $K_0(\widetilde{f_{2k}}) < K_0(f_{2k})$ and $K_1(\widetilde{f_{2k}}) < K_1(f_{2k})$. The base of the induction is the function $f_8 = \xi_8$, the induction step is provided by Theorem 9. It means that $\#\mathrm{BS}_{2k-2}(f_{2k}) = 4K_0(\widetilde{f_{2k}}) < 4K_0(f_{2k}) = \#\mathrm{BS}_{2k-2}(\widetilde{f_{2k}})$. □

Thus, unlike $m \leq n/2 + 1$, we obtain that $\#\mathrm{BS}_m(f)$ and $\#\mathrm{BS}_m(\widetilde{f})$ may not be equal. As a consequence, $\sup(\widetilde{f} \oplus \widetilde{(f \oplus \mathrm{Ind}_U)})$ may not be an affine subspace.

8 Conclusion

We have considered several properties of the bent function secondary construction $f \oplus \mathrm{Ind}_L$, where f is a bent function in n variables and L is an affine subspace of arbitrary dimension. In particular, $\#\mathrm{BS}_m(f)$, where $\mathrm{BS}_m(f)$ is the set of all bent functions of the form $f \oplus \mathrm{Ind}_L$ for an m-dimensional L, has been estimated. A relationship between considered subspaces in the simplest iterative construction has been established. Examples of the "most difficult" bent functions that have empty $\mathrm{BS}_m(f)$, for different m, have been provided. It has been found that the construction properties for arbitrary subspaces are quite similar to the case of $n/2$-dimensional subspaces, thus, we have generalized some known facts. At the same time, arbitrary dimensions have some specific properties that make the construction interesting.

Note that we have not provided an example of a bent function f in n variables, where n is arbitrary, such that $\mathrm{BS}_m(f)$ is empty for any $m \leq n - 2$. It is a topic for future research.

Acknowledgements We would like to thank C. Carlet and anonymous reviewers for the valuable comments. We also thank A. Gorodilova and V. Idrisova for their suggestions and helpful discussions.

References

1. Bonnetain, X., Perrin, L., Tian, S.: Anomalies and vector space search: tools for S-Box analysis. In: Galbraith, S., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. ASIACRYPT 2019. Lecture Notes in Computer Science, 11921, pp. 196–223. Springer, Cham (2019)
2. Canteaut, A., Charpin, P.: Decomposing bent functions. IEEE Trans. Inform. Theory **49**(8), 2004–2019 (2003)
3. Canteaut, A., Daum, M., Dobbertin, H., Leander, G.: Finding nonnormal bent functions. Discrete Appl. Math. **154**(2), 202–218 (2006)
4. Carlet, C.: Two new classes of bent functions. In: Helleseth, T. (ed.) Advances in Cryptology — EUROCRYPT '93. EUROCRYPT 1993. Lecture Notes in Computer Science, 765, pp. 77–101. Springer, Berlin, Heidelberg (1994)
5. Carlet, C.: On the confusion and diffusion properties of Maiorana–McFarland's and extended Maiorana–McFarland's functions, Special Issue "Complexity Issues in Coding Theory and Cryptography" dedicated to Prof. Harald Niederreiter on the occasion of his 60th birthday. J. Complexity **20**, 182–204 (2004)
6. Carlet, C.: Boolean functions for cryptography and error correcting code. In: Crama, Y., Hammer, P.L. (eds.) Boolean models and methods in mathematics, computer science, and engineering, pp. 257–397. Cambridge University Press, Cambridge (2010)
7. Carlet, C.: Boolean functions for cryptography and coding theory. Cambridge University Press, Cambridge (2021)
8. Carlet, C., Dobbertin, H., Leander, G.: Normal extensions of bent functions. IEEE Trans. Inform. Theory **50**(11), 2880–2885 (2004)
9. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**(1), 5–50 (2016)
10. Cusick, T.W., Stanica, P. Cryptographic Boolean functions and applications, 2nd. Acad. Press. Elsevier, Amsterdam (2009)
11. Dillon, J.: Elementary Hadamard Difference Sets, PhD. dissertation. College Park, Univ Maryland (1974)
12. Dillon, J.F., Dobbertin, H.: New cyclic difference sets with singer parameters. Finite Fields Their Appl. **10**, 342–389 (2004)
13. Dobbertin, H.: Construction of bent functions and balanced Boolean functions with high nonlinearity. In: Preneel, B. (ed.) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science, 1008, pp. 61–74. Springer, Berlin, Heidelberg (1995)
14. Helleseth, T., Kholosha, A.: Bent functions and their connections to combinatorics. In: Blackburn, S., Gerke, S., Wildon, M. (eds.) Surveys in Combinatorics 2013 (London Mathematical Society Lecture Note Series), pp. 91–126. Cambridge University Press, Cambridge (2013)

15. Frolova, A.: The essential dependence of Kasami bent functions on the products of variables. J. Appl. Ind. Math. **7**, 166–176 (2013)
16. Kolomeec, N.: The graph of minimal distances of bent functions and its properties. Des Codes Cryptogr **85**(3), 395–410 (2017)
17. Kolomeec, N.A., Pavlov, A.V.: Bent functions on the minimal distance. In: 2010 IEEE Region 8 international conference on computational technologies in electrical and electronics engineering (SIBIRCON), pp. 145–149 (2010)
18. Kutsenko, A.: The group of automorphisms of the set of self-dual bent functions. Cryptogr. Commun. **12**(5), 881–898 (2020)
19. Langevin, P., Leander, G.: Monomial bent function and Stickelberger's theorem. Finite Fields Their Appl. **14**, 727–742 (2008)
20. Leander, G., McGuire, G.: Construction of bent functions from near-bent functions. J. Combin. Theory. Ser. A **116**(4), 960–970 (2009)
21. Logachev, O.A., Salnikov, A.A., Yashchenko, V.V.: Boolean functions in coding theory and cryptography american mathematical society (2012)
22. Mandal, B., Stanica, P., Gangopadhyay, S., Pasalic, E.: An analysis of the $\mathcal{C}$ class of bent functions. Fundamenta Informaticae **146**, 271–292 (2016)
23. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) Advances in cryptology – EUROCRYPT '93. EUROCRYPT 1993. lecture notes in computer science, 765, pp. 386–397. Springer, Berlin (1994)
24. McFarland, R.L.: A family of difference sets in non-cyclic groups. J. Combin. Theory. Ser. A **15**, 1–10 (1973)
25. Mesnager, S., functions, B.ent.: Fundamentals and results. Springer, Berlin (2016)
26. Rothaus, O.: On bent functions. J. Combin. Theory. Ser. A **20**(3), 300–305 (1976)
27. Sharma, D., Gangopadhyay, D.: On Kasami bent function, Cryptology ePrint Archive, Report 2008/426. http://eprint.iacr.org/2008/426.pdf (2008)
28. Tokareva, N.: Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, Amsterdam (2015)
29. Yashchenko, V.: On the propagation criterion for Boolean functions and on bent functions. Probl. Peredachi Inf. **33**(1), 75–86 (1997). (in Russian)