$\mathcal{S}_0$-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more

Agnese Gini[$0009-0001-9565-380X$], Pierrick Méaux[$0000-0001-5733-4341$]

University of Luxembourg, Luxembourg
agnese.gini@uni.lu, pierrick.meaux@uni.lu

Abstract. We investigate the concept of $\mathcal{S}_0$ equivalent class, n-variable Boolean functions up to the addition of a symmetric function null in 0_n and 1_n, as a tool to study weightwise perfectly balanced functions. On the one hand we show that weightwise properties, such as being weightwise perfectly balanced, the weightwise nonlinearity and weightwise algebraic immunity, are invariants of these classes. On the other hand we analyze the variation of global parameters inside the same class, showing for example that there is always a function with high degree, algebraic immunity, or nonlinearity in the $\mathcal{S}_0$ equivalent class of a function. Finally, we discuss how these results extend to other equivalence relations and their applications in cryptography.

1 Introduction

Weightwise Perfectly Balanced (WPB) functions have been introduced by Carlet *et al.* in [CMR17] while studying the cryptographic properties of Boolean functions when the input is restricted to a subset of $\mathbb{F}_2^n$, motivated by the analysis of FLIP stream cipher [MJSC16]. These objects are the functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, such that $|\{x \in \mathsf{E}_{k,n} \mid f(x) = 0\}| = |\{x \in \mathsf{E}_{k,n} \mid f(x) = 1\}|$ for each $1 \leq k \leq n-1$ where the slice $\mathsf{E}_{k,n}$ denotes the set of $\mathbb{F}_2^n$ with all vectors of Hamming weight k, f globally balanced, and $f(0_n) = 0$. Since then, several articles studied the properties on restricted sets, and multiple articles focused on WPB functions such as [LM19, TL19, LS20, MS21, ZS21, MSL21, GS22, ZS22, MPJ$^+$22, GM22a, GM22b, MKCL22, MSLZ22, GM22c, ZJZQ23, ZLC$^+$23, GM23].

In this paper we study their parameters relatively to the concept of $\mathcal{S}_0$ equivalent class, which considers two n-variable Boolean functions being in the same class if they are equal up to the addition of a symmetric function null in 0_n and 1_n. The interest for WPB functions is that being WPB is an invariant of $\mathcal{S}_0$-classes. Hence, by stabilizing the WPB functions, the notion of $\mathcal{S}_0$-equivalence gives a new direction to find WPB functions.

Since for every practical application it is crucial to have a WPB function with both good weightwise and global parameters, this work aims to suggest a new strategy to construct a WPB function satisfying this assumption. Indeed, the results of this article imply that in order to find such a function, we can first search for one with suitable weightwise properties and later improve the global properties by looking directly inside its $\mathcal{S}_0$-class.

Indeed, in this paper we show that the weightwise parameters such as weightwise nonlinearity and weightwise algebraic immunity stay unchanged inside the $\mathcal{S}_0$-class. Then, we investigate the variation of the global parameters such as the degree, algebraic immunity and nonlinearity, inside an $\mathcal{S}_0$-class and we prove bounds on the maximal parameters in all classes. We demonstrate, for example, that from WPB functions with algebraic immunity as low as 2 (*e.g.* , in [GM23]), we can find a function with algebraic immunity at least $t+1$ in its $\mathcal{S}_0$-class provided $\log_2(n) \geq \log_2(2t+1) + t + 2$; while, for those whose nonlinearity is as low as $2^{n/2-1}$ (as exhibited in [GM22c]), we can find a function with nonlinearity at least $2^{n-2} - 2^{\frac{n}{2}-2}$ in its $\mathcal{S}_0$-class. We show that in every class we can find a function with degree $n-1$.

Using this framework are also able to prove that for every degree between $n/2$ and $n-1$ we can exhibit a WPB function with such a degree. Finally, we discuss how these results can be extended to other equivalence relations defined up to the addition of functions from of family $\mathcal{T}$. In different context of cryptography where a family $\mathcal{T}$ is easy to compute, and the addition is cheap, finding a Boolean function with good cryptographic parameters could then be reduced to finding the best function inside its $\mathcal{T}$-class.

We complement our investigation performing experimental analyses on equivalence classes for WPB functions in a small number of variables. Specifically, we are able to provide an exhaustive taxonomy of 4-variables classes. For 8-variables we selected some function from know families, *e.g.* [CMR17, LM19, TL19, GM22c, GM23], and computed statistics over the properties in their classes. The result of these experiments is provided in the full version of the paper.

2 Some preliminaries

A *Boolean function* f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. We recall here general concepts on Boolean functions and their weightwise properties, we refer to *e.g.* [Car21] and to [CMR17] respectively for further details. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$, and we denote $\mathcal{B}_n^*$ the set without the null function. We call *Algebraic Normal Form* of a Boolean n-variable polynomial representation over $\mathbb{F}_2$ (*i.e.* in $\mathbb{F}_2[x_1, \dots, x_n]/(x_1^2 + x_1, \dots, x_n^2 + x_n)$): $f(x_1, \dots, x_n) = \sum_{I \subseteq [1,n]} a_I \left(\prod_{i \in I} x_i\right)$ where $a_I \in \mathbb{F}_2$. The *(algebraic) degree* of f, denoted $\mathsf{deg}(f)$ is $\mathsf{deg}(f) = \max_{I \subseteq [1,n]}\{|I| \mid a_I = 1\}$ if f is not null, 0 otherwise.

To denote when a property or a definition is restricted to a slice we use the subscript k. For example, for a n-variable Boolean function f we denote its support $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ and we denote $\mathsf{supp}_k(f)$ its support restricted to a slice, that is $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

A Boolean function $f \in \mathcal{B}_n$ is called *balanced* if $|\mathsf{supp}(f)| = 2^{n-1} = |\mathsf{supp}(f+1)|$. For $k \in [0, n]$ the function is said *balanced on the slice* k if $||\mathsf{supp}_k(f)| - |\mathsf{supp}_k(f+1)|| \leq 1$. In particular when $|\mathsf{E}_{k,n}|$ is even $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f+1)| = |\mathsf{E}_{k,n}|/2$.

Let $m \in \mathbb{N}^*$ and $n = 2^m$, f is called *weightwise perfectly balanced* (WPB) if, for every $k \in [1, n-1]$, f is balanced on the slice k, that is $\forall k \in [1, n-1]$, $|\mathsf{supp}_k(f)| = \binom{n}{k}/2$, and $f(0_n) = 0$ and $f(1_n) = 1$. The set of WPB functions in 2^m variables is denoted $\mathcal{WPB}_m$. When n is not a power of 2, other weights than $k = 0$ and n give slices of odd cardinality, in this case we call $f \in \mathcal{B}_n$ *weightwise almost perfectly balanced* (WAPB) if $|\mathsf{supp}_k(f)|$ is either $|\mathsf{E}_{k,n}|/2$ if $|\mathsf{E}_{k,n}|$ is even, or $(|\mathsf{E}_{k,n}| \pm 1)/2$, otherwise. The set of WAPB functions in n variables is denoted $\mathcal{WAPB}_n$. The first WAPB family of function has been exhibited in [CMR17, Proposition 5] and it is usually referred as CMR functions.

The *nonlinearity* $\mathsf{NL}(f)$ of $f \in \mathcal{B}_n$ is the minimum Hamming distance between f and all the affine functions in $\mathcal{B}_n$, *i.e.* $\mathsf{NL}(f) = \min_{g,\, \mathsf{deg}(g) \leq 1}\{\mathsf{d_H}(f, g)\}$. For $k \in [0, n]$ we denote NL_k the *nonlinearity on the slice* k, the minimum Hamming distance between f restricted to $\mathsf{E}_{k,n}$ and the restrictions to $\mathsf{E}_{k,n}$ of affine functions over $\mathbb{F}_2^n$, *i.e.* $\mathsf{NL}_k(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} |\mathsf{supp}_k(f + g)|$.

The *algebraic immunity* (AI) of a Boolean function $f \in \mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as: $\mathsf{AI}(f) = \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0\}$. The function g is called an *annihilator* of f (or $f + 1$). The *weightwise algebraic immunity* on the slice $\mathsf{E}_{k,n}$, denoted by $\mathsf{AI}_k(f)$, is defined as: $\min\{\mathsf{deg}(g) \mid fg = 0 \text{ or } (f+1)g = 0 \text{ over } \mathsf{E}_{k,n}\}$ where g is non null on $\mathsf{E}_{k,n}$.

The n-variable Boolean symmetric functions are those that are constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0, n]$. The set of n-variable symmetric functions is denoted $\mathcal{SYM}_n$. Let $i \in [0, n]$, the *elementary symmetric function* of degree i in n variables, denoted $\sigma_{i,n}$, is the function which ANF contains all monomials of degree i and no monomials of other degrees; while, the *indicator functions* of the slice of weight k is the such that $\forall x \in \mathbb{F}_2^n$, $\varphi_{k,n}(x) = 1$ if and only if $\mathsf{w_H}(x) = k$.

3 The $\mathcal{S}_0$-equivalence relation

For a fixed $n = 2^m$ we consider the set of symmetric functions null in 0_n and 1_n:

$$\mathcal{S}_0 = \{\sigma \in \mathcal{SYM}_n \colon \sigma(0_n) = \sigma(1_n) = 0\}\,,$$

and the sets of Boolean functions in $\mathcal{B}_n$ up to addition of an element of $\mathcal{S}_0$:

Definition 1 **($\mathcal{S}_0$-equivalent functions).** *Let $m \in \mathbb{N}^*$ and $f, g \in \mathcal{B}_n$ Boolean functions in $n = 2^m$ variables. f, g are called $\mathcal{S}_0$-equivalent if there exists a symmetric function $\sigma \in \mathcal{S}_0$ such that $f = g + \sigma$. We call $\mathcal{S}_0$-class of f the set of functions $\mathcal{S}_0$-equivalent to f and we denote it by $\mathcal{S}_0(f)$.*

Remark 1. Being $\mathcal{S}_0$-equivalent is an equivalence relation.

Lemma 1. *Let $m \in \mathbb{N}^*$ and $n = 2^m$,*

1. *$\mathcal{S}_0$ is a $\mathbb{F}_2$-vector space of dimension $n - 1$. In particular, $\mathcal{S}_0 = \langle \varphi_{k,n} \colon k \in [1, n-1] \rangle_{\mathbb{F}_2}$where we denote by $\varphi_{k,n}$'s the slice indicator functions.*

2. *For all $f \in \mathcal{B}_n$, $\mathcal{S}_0(f) = f + \mathcal{S}_0$ and $|\mathcal{S}_0(f)| = 2^{n-1}$.*
3. *$\mathcal{S}_0 = \langle \sigma_{d,n} \colon d \in [1, n-1] \rangle_{\mathbb{F}_2}$ where we denote by $\sigma_{d,n}$'s the elementary symmetric functions.*

Both $\mathcal{S}_0$-classes of weightwise almost perfectly balanced functions and weightwise perfectly balanced functions consist of functions having the same W(A)PB property.

Proposition 1. *Let $m \in \mathbb{N}^*$ and $n = 2^m$,*

1. *For all $f \in \mathcal{WAPB}_n$, $\mathcal{S}_0(f) \subseteq \mathcal{WAPB}_n$.*
2. *For all $f \in \mathcal{WPB}_m$, $\mathcal{S}_0(f) \subseteq \mathcal{WPB}_m$.*
3. *Let $v = (v_1, \dots, v_{n-1})$ be a tuple such that $\forall k \in [1, n-1]$, $v_k \in \mathsf{E}_{k,n}$. For any $f \in \mathcal{B}_n$, there exists a unique $g_v \in \mathcal{S}_0(f)$ such that for all $k \in [1, n-1]$, $g_v(v_k) = 1$. We call g_v the canonical representative of its class respectively to v.*

As a consequence of Proposition 1 we obtain that $\mathcal{S}_0$-classes form a partition of $\mathcal{WAPB}_n$ and $\mathcal{WPB}_m$ and that for every tuple v we can represent the partition using canonical representatives. We prove that $\mathcal{S}_0$-equivalent classes have invariant restricted weightwise nonlinearity and restricted algebraic immunity:

Theorem 1. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $f, g \in \mathcal{B}_n$ $\mathcal{S}_0$-equivalent functions. For every $k \in [0, n]$ it holds $\mathsf{NL}_k(f) = \mathsf{NL}_k(g)$.*

Theorem 2. *Let $m \in \mathbb{N}^*$, $n = 2^m$ and $f, g \in \mathcal{WPB}_m$ $\mathcal{S}_0$-equivalent functions. For every $k \in [0, n]$ it holds $\mathsf{AI}_k(f) = \mathsf{AI}_k(g)$.*

While functions in the same $\mathcal{S}_0$-class have the same restricted weightwise nonlinearities and restricted algebraic immunities, they do not necessarily share the global properties such as the degree, nonlinearity and algebraic immunity. Working with $\mathcal{S}_0$-classes provides us a different principle for the construction of new functions. In fact, suppose we have a WPB function h with certain NL_k 's and AI_k 's and we are interested in increasing, for instance, its algebraic immunity, we can start our search for a new function inside $\mathcal{S}_0(h)$. Additionally, if h is a WPB function, we are guaranteed to obtain a function that is also WPB.

In the rest of this article we study the behavior of degree, nonlinearity and algebraic immunity inside $\mathcal{S}_0$-classes. Specifically, we are interested in the following edge quantities for WPB functions that characterize the best guaranteed value, for degree, algebraic immunity and nonlinearity, achievable by modifying a function in $\mathcal{WPB}_m$, while staying within its $\mathcal{S}_0$-class:

Definition 2. *Let $m \in \mathbb{N}^*$ and $n = 2^m$, we define:*

$$\mathsf{mdeg}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{deg}(g),$$

$$\mathsf{mAI}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{AI}(g),$$

$$\mathsf{mNL}\mathcal{S}_0(m) = \min_{f \in \mathcal{WPB}_m} \max_{g \in \mathcal{S}_0(f)} \mathsf{NL}(g).$$

4 Degree in $\mathcal{S}_0$-classes

In this part we study the potential algebraic degree inside $\mathcal{S}_0$-classes. We prove that we can preview the behavior of the degree inside the $\mathcal{S}_0$-class $\mathcal{S}_0(f)$ by looking at the ANF of f. As a consequence, we show that for any value between $n/2$ and $n-1$ (included) there exist WPB functions reaching this degree. The proof is constructive, we exhibit a new family of WPB functions with prescribed degree for all $n = 2^m$ (with $m \in \mathbb{N}^*$).

Definition 3 (Sigma-degree $\sigma\mathsf{deg}(f)$). *Let $n \in \mathbb{N}^*$, and $f \in \mathcal{B}_n$. Let D_f be the set of $d \in [1, n-1]$ such that the ANF of f contains at least a degree d monomial but not all of them. We define: $\sigma\mathsf{deg}(f) = \max D_f$ if $D_f \neq \emptyset, 0$ otherwise.*

Lemma 2. *Let $m \in \mathbb{N}^*$ and $n = 2^m$. Let f, g $\mathcal{S}_0$-equivalent Boolean functions in n variables. Then, $\sigma\mathsf{deg}(f) = \sigma\mathsf{deg}(g)$.*

Hence, $\sigma\mathsf{deg}(f)$ is an invariant of the $\mathcal{S}_0$-class and it is in fact the minimum degree in the class when f is not a symmetric function:

Theorem 3. *Let $m \in \mathbb{N}^*$ and $n = 2^m$. Let $f \in \mathcal{B}_n$ such that $f \notin \mathcal{SYM}_n$ and $\delta \in \mathbb{N}$.*

- *there exist exactly $2^{\sigma\mathsf{deg}(f)}$ functions $g \in \mathcal{S}_0(f)$ such that $\mathsf{deg}(g) = \sigma\mathsf{deg}(f)$.*
- *if $\sigma\mathsf{deg}(f) < \delta < n$, there exist exactly $2^{\delta-1}$ functions $g \in \mathcal{S}_0(f)$ such that $\mathsf{deg}(g) = \delta$.*
- *if $\delta < \sigma\mathsf{deg}(f)$, there does not exist $g \in \mathcal{S}_0(f)$ such that $\mathsf{deg}(g) = \delta$.*

Therefore, in the $\mathcal{S}_0$ class of every WPB function there exists at least a function of degree $n-1$, *i.e.* the minimum of the maximal degree inside an $\mathcal{S}_0$-class of $\mathcal{WPB}_m$ is $n-1$:

Corollary 1. *Let $m \in \mathbb{N}^*$. $\mathsf{mdeg}\mathcal{S}_0(m) = n - 1$.*

We can specialize the argument of Theorem 3 to explicitly construct WPB functions having for degree any value between $n/2$ and $n-1$ included, from CMR family.

Corollary 2 (WPB functions with prescribed degree). *Let $m \in \mathbb{N}^*$, $n = 2^m$, and $d \in [\frac{n}{2}, n-1]$. We define $f_{n,n/2} = f_n$ as in [CMR17, Proposition 5], and for all $\frac{n}{2} < d < n$, $f_{n,d} = f_n + \sigma_{d,n}$. The function $f_{n,d}$ is weightwise perfectly balanced and $\mathsf{deg}(f_{n,d}) = d$.*

Degree distribution in $\mathcal{WPB}_m$. Let $m \in \mathbb{N}^*$ and $n = 2^m$. We observe that $\mathcal{S}_0$-classes form a partition of $\mathcal{WPB}_m$ from Proposition 1. Denoting by $\theta_{d,m}$ the number of $\mathcal{S}_0$-classes such that $\sigma\mathsf{deg}(f) = d$ and setting $D_{d,m} = |\{f \in \mathcal{WPB}_m\colon \deg f = d\}|$, from Theorem 3 we have that:

$$D_{d,m} = 2^d \cdot \theta_{d,m} + 2^{d-1} \cdot \sum_{k=0}^{d-1} \theta_{k,m} = 2^{d-1} \cdot \theta_{d,m} + 2^{d-1} \cdot \sum_{k=0}^{d} \theta_{k,m}.$$

Theorem 4. *Let $m \in \mathbb{N}^*$, $n = 2^m$, the probability of a WPB function from $\mathcal{WPB}_m$ having degree $n-1$ is:*

$$\frac{D_{n-1,m}}{|\mathcal{WPB}_m|} = \frac{2^{n-2}\theta_{n-1,m}}{|\mathcal{WPB}_m|} + \frac{1}{2} > 1/2. \tag{1}$$

Practical experiments. To complement this investigation on the degree, we perform an experimental study of the degree distribution for WPB functions in a small number of variables. The results will be displayed in the full version of the paper.

5 Minimal parameters inside the $\mathcal{S}_0$-classes of WPB functions

For a WPB function reaching a very small algebraic immunity or nonlinearity, there always exists a function with better parameters in its $\mathcal{S}_0$-class. On the experimental side, it allows to optimize the parameters of a WPB while staying in the class.

Algebraic immunity inside an $\mathcal{S}_0$ class. In this part we focus on the $\mathsf{mAI}\mathcal{S}_0(m)$ parameter (Definition 2). In [GM23], the minimal AI that a WPB function can have is proven to be 2. In the following we show that $\mathsf{mAI}\mathcal{S}_0(m) > 2$ (for $m \geq 6$), which means that for such WPB functions exhibited in [GM23], there always exist functions with better AI in their $\mathcal{S}_0$-class, more adequate to be used in a cipher. We begin by demonstrating a general lemma:

Lemma 3. *Let $m \in \mathbb{N}^*$ and $n = 2^m$, let $t \in \mathbb{N}^*$, if there exist 2^t functions s_i in $\mathcal{S}_0$ such that $\mathsf{AI}(s_i) > 2t$, and $\mathsf{AI}(s_i + s_j) > 2t$ for all $i \neq j$, then for all $f \in \mathcal{B}_n$ there exists $g \in \mathcal{S}_0(f)$ such that $\mathsf{AI}(g) \geq t + 1$.*

Then, we need a result on the AI of some symmetric functions, to show the existence of 2^t functions satisfying the conditions of Lemma 3 in $\mathcal{S}_0$.

Proposition 2. *Let $m \in \mathbb{N}^*$ and $n = 2^m$, let $r \in \mathbb{N}^*$, $r < m$, for all vector $v \in (\mathbb{F}_2^r)^*$ the symmetric function f defined as: $f = \sum_{i=1}^{r} v_i \sigma_{2^m - 2^{m-i}, 2^m}$ is such that* $\mathsf{AI}(f) \geq 2^{m-r} - 1$.

It allows to derive a first lower bound on $\mathsf{mAI}\mathcal{S}_0(m)$:

Theorem 5 (Lower bound on $\mathsf{mAI}\mathcal{S}_0(m)$). *Let $t, m \in \mathbb{N}$, $t \geq 2$, if $m > \log(2t+1) + t + 1 + (t \mod 2)$ then* $\mathsf{mAI}\mathcal{S}_0(m) \geq t + 1$.

Taking the first m satisfying the condition of Theorem 5, $m_t = \lfloor \log(2t+1) \rfloor + t + 2 + (t \mod 2)$, the first values are $m_2 = 6$, $m_3 = 8$, $m_4 = 9$, and $m_5 = 11$.

Theorem 5 shows that for $m \geq 6$ there are functions with AI at least 3 in each $\mathcal{S}_0$-class of $\mathcal{WPB}_m$. An interesting research direction is to determine if $\mathsf{mAI}\mathcal{S}_0(m) = 2^{m-1}$. If it holds, there are functions with optimal AI in each $\mathcal{S}_0$-class, and then finding a WPB function with good AI together with good NL_k and AI_k boils down to determining the adequate representative. If it does not hold, it is appealing to characterize the classes where optimal AI is not reachable.

Nonlinearity inside an $\mathcal{S}_0$-class. In this part we focus on $\mathsf{mNL}\mathcal{S}_0(m)$, as defined in Definition 2. In [GM22c], WPB functions with a nonlinearity as low as $2^{n/2-1}$ have been exhibited. In this part we demonstrate that $\mathsf{mNL}\mathcal{S}_0(m) \geq 2^{n-2} - 2^{\frac{n}{2}-2}$.

Theorem 6 (Lower bound on $\mathsf{mNL}\mathcal{S}_0(m)$). *Let $m \in \mathbb{N}$, $m \geq 2$ and $n = 2^m$, the following holds:*

$$\mathsf{mNL}\mathcal{S}_0(m) \geq 2^{n-2} - 2^{\frac{n}{2}-2}.$$

6 Beyond parameters in $\mathcal{S}_0$-classes

These results have more implications for cryptographic applications: for example in the (improved) filter permutator context [MJSC16, MCJS19], for hybrid homomorphic encryption, there are efficient ways to evaluate symmetric functions (as illustrated in [HMR20]), and doing one addition is cheap, therefore it is interesting to consider the best function in the $\mathcal{S}_0$-class of a filter function. In that case, for all contexts where adding one function is cheap, the hunt for optimized functions could be split into finding a cheap function to evaluate, and then determining the one with best cryptographic parameters in its $\mathcal{T}$-class. The $\mathcal{T}$-class would be the class given by an equivalence relation up to the addition of a fixed family of functions, at the same time efficiently computable in the context and enabling good cryptographic parameters.

Different results we presented can be generalized to $\mathcal{T}$-classes, in particular denoting $\mathsf{mdeg}\mathcal{T}$, $\mathsf{mAI}\mathcal{T}$ and $\mathsf{mNL}\mathcal{T}$, the minimum over the maximum degree, AI and nonlinearity parameter inside a $\mathcal{T}$-class:

- Similarly to Corollary 1, denoting by D the maximum degree of functions inside $\mathcal{T}$, we obtain that $\mathsf{mdeg}\mathcal{T} \geq D$.
- Lemma 3 can be generalized to any family $\mathcal{T}$, hence for any family $\mathcal{T}$ with functions with high AI and such that the sum of two elements still have high AI, we can obtain a bound on $\mathsf{mAI}\mathcal{T}$ similarly to the one of Theorem 5.
- The bound on $\mathsf{mNL}\mathcal{S}_0(m)$ from Theorem 6 comes from the fact that a bent function belongs to $\mathcal{S}_0$. Then, the same bound applies for each family $\mathcal{T}$ containing a bent function. More generally, denoting B the maximal nonlinearity for a function in $\mathcal{T}$, the bound $\mathsf{mNL}\mathcal{T} \geq B/2$ holds.

Acknowledgments. The two authors were supported by the ERC Advanced Grant no. 787390.

References

BP05. An Braeken and Bart Preneel. On the algebraic immunity of symmetric boolean functions. In *Progress in Cryptology - INDOCRYPT 2005, 6th International Conference on Cryptology in India, Bangalore, India, December 10-12, 2005, Proceedings*, pages 35–48, 2005.

Car04. Claude Carlet. On the degree, nonlinearity, algebraic thickness, and nonnormality of boolean functions, with developments on symmetric functions. *IEEE Trans. Information Theory*, pages 2178–2185, 2004.

Car21. Claude Carlet. *Boolean Functions for Cryptography and Coding Theory*. Cambridge University Press, 2021.

CM22. Claude Carlet and Pierrick Méaux. A complete study of two classes of boolean functions: direct sums of monomials and threshold functions. *IEEE Transactions on Information Theory*, 68(5):3404–3425, 2022.

CMR17. Claude Carlet, Pierrick Méaux, and Yann Rotella. Boolean functions with restricted input and their robustness; application to the FLIP cipher. *IACR Trans. Symmetric Cryptol.*, 2017(3), 2017.

CV05. Anne Canteaut and Marion Videau. Symmetric boolean functions. *IEEE Trans. Information Theory*, pages 2791–2811, 2005.

DMS06. Deepak Kumar Dalai, Subhamoy Maitra, and Sumanta Sarkar. Basic theory in construction of boolean functions with maximum possible annihilator immunity. *Designs, Codes and Cryptography*, 2006.

Fin47. N. J. Fine. Binomial coefficients modulo a prime. *The American Mathematical Monthly*, 54(10):589–592, 1947.

GM22a. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 322:320–341, 2022.

GM22b. Agnese Gini and Pierrick Méaux. Weightwise almost perfectly balanced functions: Secondary constructions for all n and better weightwise nonlinearities. In Takanori Isobe and Santanu Sarkar, editors, *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

GM22c. Agnese Gini and Pierrick Maux. Weightwise perfectly balanced functions and nonlinearity. Cryptology ePrint Archive, Paper 2022/1777, 2022.

GM23. Agnese Gini and Pierrick Maux. On the algebraic immunity of weightwise perfectly balanced functions. Cryptology ePrint Archive, Paper 2023/495, 2023. `https://eprint.iacr.org/2023/495`.

GS22. Xiaoqi Guo and Sihong Su. Construction of weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 307:102–114, 2022.

HMR20. Clément Hoffmann, Pierrick Méaux, and Thomas Ricosset. Transciphering, using filip and TFHE for an efficient delegation of computation. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 39–61. Springer, 2020.

LM19. Jian Liu and Sihem Mesnager. Weightwise perfectly balanced functions with high weightwise nonlinearity profile. *Des. Codes Cryptogr.*, 87(8):1797–1813, 2019.

LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced boolean functions with high weightwise nonlinearity. *Discret. Appl. Math.*, 279:218–227, 2020.

MCJS19. Pierrick Méaux, Claude Carlet, Anthony Journault, and François-Xavier Standaert. Improved filter permutators for efficient FHE: better instances and implementations. In Feng Hao, Sushmita Ruj, and Sourav Sen Gupta, editors, *Progress in Cryptology - INDOCRYPT*, volume 11898 of *LNCS*, pages 68–91. Springer, 2019.

Méa21. Pierrick Méaux. On the fast algebraic immunity of threshold functions. *Cryptogr. Commun.*, 13(5):741–762, 2021.

MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 311–343. Springer, Heidelberg, May 2016.

MKCL22. Sara Mandujano, Juan Carlos Ku Cauich, and Adriana Lara. Studying special operators fortheapplication ofevolutionary algorithms intheseek ofoptimal boolean functions forcryptography. In Obdulia Pichardo Lagunas, Juan Martínez-Miranda, and Bella Martínez Seis, editors, *Advances in Computational Intelligence*, pages 383–396, Cham, 2022. Springer Nature Switzerland.

MPJ$^+$22. Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced boolean functions. In *2022 IEEE Congress on Evolutionary Computation (CEC)*, page 18. IEEE Press, 2022.

MS78. F.J. MacWilliams and N.J.A. Sloane. *The Theory of Error-Correcting Codes*. North-holland Publishing Company, 2nd edition, 1978.

MS21. Sihem Mesnager and Sihong Su. On constructions of weightwise perfectly balanced boolean functions. *Cryptography and Communications*, 2021.

MSL21. Sihem Mesnager, Sihong Su, and Jingjing Li. On concrete constructions of weightwise perfectly balanced functions with optimal algebraic immunity and high weightwise nonlinearity. *Boolean Functions and Applications*, 2021.

MSLZ22. Sihem Mesnager, Sihong Su, Jingjing Li, and Linya Zhu. Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity. *Cryptogr. Commun.*, 14(6):1371–1389, 2022.

MT21. Sihem Mesnager and Chunming Tang. Fast algebraic immunity of boolean functions and LCD codes. *IEEE Trans. Inf. Theory*, 67(7):4828–4837, 2021.

QFLW09. Longjiang Qu, Keqin Feng, Feng Liu, and Lei Wang. Constructing symmetric boolean functions with maximum algebraic immunity. *IEEE Transactions on Information Theory*, 55:2406–2412, 05 2009.

SM07. Palash Sarkar and Subhamoy Maitra. Balancedness and correlation immunity of symmetric boolean functions. *Discrete Mathematics*, pages 2351 – 2358, 2007.

TL19. Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced boolean functions with optimal algebraic immunity. *Cryptogr. Commun.*, 11(6):1185–1197, 2019.

ZJZQ23. Qinglan Zhao, Yu Jia, Dong Zheng, and Baodong Qin. A new construction of weightwise perfectly balanced functions with high weightwise nonlinearity. *Mathematics*, 11(5), 2023.

ZLC$^+$23. Qinglan Zhao, Mengran Li, Zhixiong Chen, Baodong Qin, and Dong Zheng. A unified construction of weightwise perfectly balanced boolean functions. Cryptology ePrint Archive, Paper 2023/460, 2023. `https://eprint.iacr.org/2023/460`.

ZS21. Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced boolean functions. *Advances in Mathematics of Communications*, 0:–, 2021.

ZS22. Linya Zhu and Sihong Su. A systematic method of constructing weightwise almost perfectly balanced boolean functions on an arbitrary number of variables. *Discrete Applied Mathematics*, 314:181–190, 2022.