$\mathcal{S}_0$-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, GM23a, ZJZQ23, ZLC+23, GM23b, YCL+23].

In this article 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 [GM23b]), 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 [GM23a]), 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-variable classes. For 8 variables we selected some function from know families, *e.g.* [CMR17, LM19, TL19, GM23a, GM23b], and computed statistics over the properties in their classes. The result of these experiments is provided in the full version of the paper.

2 Preliminaries

For readability we use the notation $+$ instead of $\oplus$ to denote the addition in $\mathbb{F}_2$ and $\sum$ instead of $\bigoplus$. In addition to classic notations we denote by $[a, b]$ the subset of all integers between a and b: $\{a, a+1, \dots, b\}$.

For a vector $v \in \mathbb{F}_2^n$ we use $\mathsf{w_H}(v)$ to denote its Hamming weight $\mathsf{w_H}(v) = |\{i \in [1, n] \mid v_i = 1\}|$. For two vectors v and w of $\mathbb{F}_2^n$ we denote $\mathsf{d_H}(v, w)$ the Hamming distance between v and w, that is $\mathsf{d_H}(v, w) = \mathsf{w_H}(v + w)$.

2.1 Boolean functions and weightwise considerations

In this part we recall general concepts on Boolean functions and their weightwise properties we use in this article. For a deeper introduction on Boolean functions and their cryptographic parameters we refer to *e.g.* the book [Car21] and to [CMR17] for the weightwise properties, also called properties on the slices.

For $k \in [0, n]$ we denote $\mathsf{E}_{k,n}$ the set $\{x \in \mathbb{F}_2^n \mid \mathsf{w_H}(x) = k\}$ and call it slice of the Boolean hypercube (of dimension n). Accordingly, the Boolean hypercube is partitioned into $n + 1$ slices where the elements have the same Hamming weight.

Definition 1 (Boolean Function). *A Boolean function f in n variables is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. 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.*

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 $\mathsf{supp}(f) \cap \mathsf{E}_{k,n}$.

Definition 2 (Balancedness). *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 $|\mathsf{supp}_k(f)| = |\mathsf{supp}_k(f + 1)| = |\mathsf{E}_{k,n}|/2$.*

Definition 3 (Weightwise (Almost) Perfectly Balanced Function (WPB and WAPB)). *Let $m \in \mathbb{N}^*$ and f be a Boolean function in $n = 2^m$ variables. It will be 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:*

$$f(0, \cdots, 0) = 0, \quad \textit{and } f(1, \cdots, 1) = 1.$$

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:

$$|\mathsf{supp}_k(f)| = \begin{cases} |\mathsf{E}_{k,n}|/2 & \textit{if } |\mathsf{E}_{k,n}| \textit{ is even,} \\ (|\mathsf{E}_{k,n}| \pm 1)/2 & \textit{if } |\mathsf{E}_{k,n}| \textit{ is odd.} \end{cases}$$

The set of WAPB functions in n variables is denoted $\mathcal{WAPB}_n$.

Definition 4 (Walsh transform and restricted Walsh transform). *Let $f \in \mathcal{B}_n$ be a Boolean function, its Walsh transform W_f at $a \in \mathbb{F}_2^n$ is defined as:*

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

Let $f \in \mathcal{B}_n$, $S \subset \mathbb{F}_2^n$, its Walsh transform restricted to S at $a \in \mathbb{F}_2^n$ is defined as:

$$W_{f,S}(a) := \sum_{x \in S} (-1)^{f(x) + ax}.$$

For $S = \mathsf{E}_{k,n}$ we denote $W_{f,\mathsf{E}_{k,n}}(a)$ by $\mathcal{W}_{f,k}(a)$, and for $a = 0_n$ we denote $\mathcal{W}_{f,k}(a)$ as $\mathcal{W}_{f,k}(0)$.

Definition 5 (Nonlinearity and weightwise nonlinearity). *The nonlinearity* $\mathsf{NL}(f)$ *of a Boolean function* $f \in \mathcal{B}_n$*, where* n *is a positive integer, is the minimum Hamming distance between* f *and all the affine functions in* $\mathcal{B}_n$*:*

$$\mathsf{NL}(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} \{\mathsf{d_H}(f, g)\},$$

where $g(x) = a \cdot x + \varepsilon$, $a \in \mathbb{F}_2^n, \varepsilon \in \mathbb{F}_2$ *(where* $\cdot$ *is an inner product in* $\mathbb{F}_2^n$*, any choice of inner product will give the same value of* $\mathsf{NL}(f)$*)*

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* $\mathbb{F}_2^n$*. Accordingly:*

$$\mathsf{NL}_k(f) = \min_{g,\, \mathsf{deg}(g) \leq 1} |\mathsf{supp}_k(f + g)|.$$

Property 1 (Nonlinearity on the slice, adapted from [CMR17], Proposition 6). *Let* $n \in \mathbb{N}^*, k \in [0, n]$*, for every* n*-variable Boolean function* f *over* $\mathsf{E}_{k,n}$*:*

$$\mathsf{NL}_k(f) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f,k}(a)|}{2}.$$

Definition 6 (Non Perfect Balancedness ([GM23a])). *Let* $m \in \mathbb{N}^*$*,* $n = 2^m$*, and* f *an* n*-variable Boolean function, the non perfect balancedness of* f*, denoted* $\mathsf{NPB}(f)$ *is defined as:*

$$\mathsf{NPB}(f) = \min_{g \in \mathcal{WPB}_m} \mathsf{d_H}(f, g).$$

Property 2 (NPB and restricted Walsh transform ([GM23a], Proposition 2)). *Let* $m \in \mathbb{N}^*$*,* $n = 2^m$*, and* $f \in \mathcal{B}_n$*, the following holds on its non perfect balancedness:*

$$\mathsf{NPB}(f) = \frac{2 - \mathcal{W}_{f,0}(0) + \mathcal{W}_{f,n}(0)}{2} + \sum_{k=1}^{n-1} \frac{|\mathcal{W}_{f,k}(0)|}{2}.$$

Definition 7 (Algebraic Normal Form (ANF) and degree). *We call Algebraic Normal Form of a Boolean function* f *its* n*-variable polynomial representation over* $\mathbb{F}_2$ *(i.e. belonging to* $\mathbb{F}_2[x_1, \ldots, x_n]/(x_1^2 + x_1, \ldots, x_n^2 + x_n)$*):*

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq [1,n]} a_I \left(\prod_{i \in I} x_i \right)$$

where $a_I \in \mathbb{F}_2$*. The (algebraic) degree of* f*, denoted* $\mathsf{deg}(f)$ *is:*

$$\mathsf{deg}(f) = \max_{I \subseteq [1,n]} \{|I| \mid a_I = 1\} \textit{ if } f \textit{ is not null}, 0 \textit{ otherwise}.$$

Definition 8 (Algebraic Immunity (AI), and weightwise AI). *The Algebraic Immunity (AI) of a Boolean function* $f \in \mathcal{B}_n$*, denoted as* $\mathsf{AI}(f)$*, is defined as:*

$$\mathsf{AI}(f) = \min_{g \neq 0} \{\mathsf{deg}(g) \mid fg = 0 \textit{ or } (f + 1)g = 0\},$$

where $\mathsf{deg}(g)$ *is the algebraic degree of* g*. The function* g *is called an annihilator of* f *(or* $f + 1$*). Additionally we denote* $\mathsf{AN}(f) = \min_{g \neq 0}\{\mathsf{deg}(g) \mid fg = 0\}$*.*

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

Property 3. *If* $g \in \mathcal{B}_n^*$ *is an annihilator of* f *and* h *another function such that* $\mathsf{supp}(h) \subseteq \mathsf{supp}(g)$*, then* $hf = 0$*.*

2.2 Families of WPB functions

In this section we recall families of WPB functions exhibited in former works. These families will be used as examples of WPB functions with minimal or maximal parameters relatively to the degree or algebraic immunity.

Definition 9 (CMR WAPB construction (adapted from [CMR17], Proposition 5)**).** *Let $n \in \mathbb{N}, n \geq 2$, the WAPB function f_n is recursively defined by $f_2(x_1, x_2) = x_1$ and for $n \geq 3$:*

$$f_n(x_1, \ldots, x_n) = \begin{cases} f_{n-1}(x_1, \ldots, x_{n-1}) & \text{if } n \text{ odd,} \\ f_{n-1}(x_1, \ldots, x_{n-1}) + x_{n-2} + \prod_{i=1}^{2^{d-1}} x_{n-i} & \text{if } n = 2^d; d > 1, \\ f_{n-1}(x_1, \ldots, x_{n-1}) + x_{n-2} + \prod_{i=1}^{2^d} x_{n-i} & \text{if } n = p \cdot 2^d; p \text{ odd.} \end{cases}$$

Re-indexing the variables the subfamily of WPB functions (the cases where n is a power of 2) can be written as:

$$f(x_1, x_2, \ldots, x_{2^m}) = \sum_{a=1}^{m} \sum_{i=1}^{2^{m-a}} \prod_{j=0}^{2^{a-1}-1} x_{i+j2^{m-a+1}}$$

Definition 10 (LM WPB construction (adapted from [LM19], Corollary 3.5)**).** *Let $n \in \mathbb{N}, n \geq 2$, we denote by Γ_n the set of all the coset leaders of the cyclotomic classes of 2 modulo $2^n - 1$ and by $o(j)$ the cardinality of the cyclotomic class of 2 modulo $2^n - 1$ containing j. Define $T_j : \mathbb{F}_{2^{o(j)}} \to \mathbb{F}_2$ the function $y \mapsto \sum_{i=0}^{o(j)-1} y^{2^i}$. For any fixed β primitive element of $\mathbb{F}_{2^2}$ and any given any function $\iota \colon \Gamma_n \setminus \{0\} \to \{1, 2\}$, the LM WPB function associate to ι is*

$$g_\iota(x) = \sum_{j \in \Gamma_n \setminus \{0\}} T_j(\beta^{\iota(j)} x^j).$$

Definition 11 (TL WPB construction (adapted from [TL19], Construction 1 **)).** *Let $m \in \mathbb{N}^*$ and $n = 2^m \geq 4$ be an integer. A TL WPB Boolean function h on n-variable is such that*

- $h(0_n) = 0$ *and* $h(1_n) = 1$
- $h(x, y) = 0$ *if* $\mathsf{w_H}(x) < \mathsf{w_H}(y)$, *where* $x, y \in \mathbb{F}_2^{m-1}$.
- $h(x, y) = 1$ *if* $\mathsf{w_H}(x) > \mathsf{w_H}(y)$, *where* $x, y \in \mathbb{F}_2^{m-1}$.
- *the cardinality of* $U_i = \mathsf{supp}(f) \cap \left\{(x, y) \in \mathbb{F}_2^{2^{m-1}} \times \mathbb{F}_2^{2^{m-1}} : \mathsf{w_H}(x) = \mathsf{w_H}(y) = i\right\}$ *is exactly* $\binom{2^{m-1}}{j}^2/2$ *for all* $0 < j < 2^{m-1}$.

Remark 1. Despite Definition 11 may appear quite different respect the original paper, it is equivalent when applying the constrains from the definitions we consider. Namely, here we consider only the case where n is a power of two. Referring to Construction 1 of [TL19], this implies that the coefficients $c_1, \ldots, c_{k-1}$ must be zero. Moreover, in [TL19] $f(0_n) = 0$ and $f(1_n) = 1$ is not required for weightwise perfectly balancedness, differently from Definition 3. This implies that in this context we can only instantiate the construction with $(-1, 0, .., 0, 1)$ as input sequence, *i.e.* as in Definition 11.

Property 4 (Properties of WPB families, [CMR17, LM19, TL19])**.** *Let $m \in \mathbb{N}^*$ and $n = 2^m$, the n-variable CMR function f_n, a n-variable LM function g_n AND a n-variable TL function h_n have the following properties:*

- $\mathsf{deg}(f_n) = \frac{n}{2}$,
- $\mathsf{deg}(g_n) = n - 1$,
- $\mathsf{AI}(h_n) = \frac{n}{2}$.

2.3 Symmetric Functions and Krawtchouk polynomials

The n-variable Boolean symmetric functions are those that are constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0, n]$. This class has been thoroughly studied in the context of cryptography, see *e.g.* [Car04, CV05, BP05, SM07, QFLW09, Méa19, Méa21, CM22]. The set of n-variable symmetric functions is denoted $\mathcal{SYM}_n$, and $|\mathcal{SYM}_n| = 2^{n+1}$. In this article we mainly consider two families of symmetric functions, which are both bases of the symmetric functions:

Definition 12 (Elementary symmetric functions). *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.*

Definition 13 (Slice indicator functions). *Let $k \in [0, n]$, the indicator function of the slice of weight k is defined as:*

$$\forall x \in \mathbb{F}_2^n, \quad \varphi_{k,n}(x) = 1 \textit{ if and only if } \mathsf{w_H}(x) = k.$$

Property 5 (Properties of elementary symmetric functions)**.** *Let $n \in \mathbb{N}^*$, and $d \in [0, n]$:*

- *The function $\sigma_{d,n}$ takes the value $\binom{k}{d} \mod 2$ on the elements of the slice $\mathsf{E}_{k,n}$.*
- *The function $\sigma_{2,n}$ takes the value 1 only on the slices $\mathsf{E}_{k,n}$ such that $k = 2 \mod 4$ or $k = 3 \mod 4$. Moreover, for n even, $\sigma_{2,n}$ is bent.*

Definition 14 (Threshold functions). *For any positive integers $d \leq n + 1$ we define the Boolean function $\mathsf{T}_{d,n}$ as follows:*

$$\forall x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n, \quad \mathsf{T}_{d,n}(x) = \begin{cases} 0 & \textit{if } \mathsf{w_H}(x) < d, \\ 1 & \textit{otherwise.} \end{cases}$$

Property 6 (Lucas' Theorem, *e.g.* [Fin47])**.** *Let $a, b, p \in \mathbb{N}$ be integers such that $a > b$ and p is a prime. Consider their p-adic expansions $a = \sum_{j=0}^{q} a_j p^j$ and $b = \sum_{j=0}^{q} b_j p^j$ such that $0 \leq a_j < p$ and $0 \leq b_j < p$ for each $j \in [0, q]$ and $a_q \neq 0$. Then*

$$\binom{a}{b} \equiv \prod_{j=0}^{q} \binom{a_j}{b_j} \pmod{p}.$$

Property 7 (Weightwise restricted Walsh transform and addition of symmetric function ([GM22b], Proposition 4))**.** *Let $n \in \mathbb{N}^*$, $k \in [0, n]$ and $f \in \mathcal{B}_n$, the following holds on $f + \varphi_{k,n}$*

$$\forall a \in \mathbb{F}_2^n, \forall i \in [0, n] \setminus \{k\}, \mathcal{W}_{f+\varphi_{k,n},i}(a) = \mathcal{W}_{f,i}(a), \textit{ and } \mathcal{W}_{f+\varphi_{k,n},k}(a) = -\mathcal{W}_{f,i}(a).$$

We give two results relatively to Krawtchouk Polynomials we will use in the article. We refer to *e.g.* [MS78] for more details on these polynomials and their properties.

Definition 15 (Krawtchouk Polynomials). *The Krawtchouk polynomial of degree k, with $0 \leq k \leq n$ is given by:* $\mathsf{K}_k(\ell, n) = \displaystyle\sum_{j=0}^{k} (-1)^j \binom{\ell}{j} \binom{n - \ell}{k - j}$.

Property 8 (Krawtchouk polynomials relations)**.** *Let $n \in \mathbb{N}^*$ and $k \in [0, n]$, the following relations hold:*

1. $\mathsf{K}_k(\ell, n) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{a \cdot x}$, *where $a \in \mathbb{F}_2^n$ and $\ell = \mathsf{w_H}(a)$,*
2. *Proposition 5 [DMS06] For n even, $k \in [0, n]$,*

$$\mathsf{K}_k(n/2, n) = \begin{cases} 0 & \textit{if } k \textit{ is odd}, \\ (-1)^{k/2} \dbinom{n/2}{k/2} & \textit{if } k \textit{ is even}. \end{cases}$$

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

In this section we introduce the notion of $\mathcal{S}_0$ equivalent relation and we prove a few properties of sets of equivalent functions. Let $n = 2^m$ for $m \in \mathbb{N}^+$ and consider the set of symmetric functions null in 0_n and 1_n:

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

In this section we analyses the properties of sets of Boolean functions in $\mathcal{B}_n$ up to addition of an element of $\mathcal{S}_0$:

Definition 16 **($\mathcal{S}_0$-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 $\mathcal{S}_0(f)$.*

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 (Definition 13).

2. *$|\mathcal{S}_0| = 2^{n-1}$.*
3. *For all $f \in \mathcal{B}_n$, $\mathcal{S}_0(f) = f + \mathcal{S}_0$ and $|\mathcal{S}_0(f)| = 2^{n-1}$.*

Proof. Boolean symmetric functions are those constant on each slice $\mathsf{E}_{k,n}$ for $k \in [0, n]$. Since by definition every function $\sigma \in \mathcal{S}_0$ is such that $\sigma(0_n) = \sigma(1_n) = 0$, it can be uniquely written $\sigma = \sum_{k=1}^{n-1} a_k \varphi_{k,n}$ with $a_k \in \mathbb{F}_2$ for $k \in [1, n-1]$. Additionally, this establishes a bijection between $\mathbb{F}_2^{n-1}$ and

$$\mathcal{S}_0(f) = \{f + \sigma \colon \sigma \in \mathcal{S}_0\} = f + \mathcal{S}_0.$$

Therefore, $|\mathcal{S}_0| = 2^{n-1}$ and $|\mathcal{S}_0(f)| = 2^{n-1}$. □

From the first point of Lemma 1 we can deduct that being $\mathcal{S}_0$-equivalent is an equivalence relation. Indeed, we have that $f \in \mathcal{S}_0(f)$ (reflexivity), since the null function belongs to $\mathcal{S}_0$. If $g \in \mathcal{S}_0(()f)$, there exists $\sigma \in \mathcal{S}_0$ such that $g = f + \sigma$, then $f = g + \sigma$ and $f \in \mathcal{S}_0(g)$ (symmetry). Finally, if $g = f + \sigma$ $h = g + \sigma'$ for $\sigma, \sigma' \in \mathcal{S}_0$, we have that $h = f + \sigma + \sigma'$ and $h \in \mathcal{S}_0(f)$, since $\sigma + \sigma' \in \mathcal{S}_0$ (transitivity).

From Lemma 1 we can derive an efficient constructive method to compute one or more $\mathcal{S}_0$-classes. Namely, for a fixed n we can first precompute the set $\mathcal{S}_0$, and then compute the class $\mathcal{S}_0(f)$ as $f + \mathcal{S}_0$. The set $\mathcal{S}_0$ can be generated via slice indicator functions as suggested by Lemma 1. When $n = 2^m > 1$, this space can be also generated via elementary symmetric functions (Definition 12):

Lemma 2. *Let $m \in \mathbb{N}^*$ and $n = 2^m$. We denote by $\sigma_{d,n}$ the n-variable elementary symmetric function of degree d. For all $d \in [1, n-1]$, $\sigma_{d,n} \in \mathcal{S}_0$.*

Proof. On the slice 0 the function $\sigma_{d,n}$ takes the value $\binom{0}{d}$ from Property 5 Item 1. This implies that is 0 since $d > 0$. Similarly, on the slice n, the function $\sigma_{d,n}$ takes the value $\binom{n}{d} \mod 2$, that is 0 since $n = 2^m > 1$ and $d \in [1, n-1]$. □

Proposition 1. *Let $m \in \mathbb{N}^*$ and $n = 2^m$. Then, $\mathcal{S}_0 = \langle \sigma_{d,n} \colon d \in [1, n-1] \rangle_{\mathbb{F}_2}$.*

Proof. Lemma 2 implies that $\langle \sigma_{d,n} \colon d \in [1, n-1] \rangle_{\mathbb{F}_2}$ is a subspace of $\mathcal{S}_0$. Since the elementary symmetric functions have distinct degree, they are also linearly independent. This is sufficient to prove the equality. □

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 2. *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 $v = (v_1, \ldots, v_{n-1})$ 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.*

Proof. Let $f \in \mathcal{WAPB}_n$ and $g \in \mathcal{S}_0(f)$ such that $g = f + \sigma = f + \sum_{k=1}^{n-1} a_i \varphi_{k,n}$. Then, for all $k \in [1, n-1]$ we have $|\mathsf{supp}_k(g)| = |\mathsf{supp}_k(f + \varphi_{k,n})|$. If $\mathsf{E}_{k,n}$ is even, then $|\mathsf{supp}_k(g)| = |\mathsf{supp}_k(f)| = |\mathsf{E}_{k,n}|/2$. If $\mathsf{E}_{k,n}$ is odd, $|\mathsf{supp}_k(g)| = |\mathsf{supp}_k(f)| = |\mathsf{E}_{k,n}|/2 \pm 1/2$. This implies $\mathcal{S}_0(f) \subseteq \mathcal{WAPB}_n$.

Additionally, since $\sigma(0_n) = \sigma(1_n) = 0$, we obtain $g(0_n) = f(0_n)$ and $g(1_n) = f(1_n)$. This implies that if $f \in \mathcal{WPB}_m$, then $g \in \mathcal{WPB}_m$ too. Namely, $\mathcal{S}_0(f) \subseteq \mathcal{WPB}_m$.

Finally, consider a tuple $v = (v_1, \ldots, v_{n-1})$ such that $\forall k \in [1, n-1]$, $v_k \in \mathsf{E}_{k,n}$. If we set $b_k = f(v_k) + 1 \in \{0, 1\}$ for all $k \in [1, n-1]$, we obtain a function $\sigma_v = \sum_{k=1}^{n-1} b_k \varphi_{k,n} \in \mathcal{S}_0$. Hence, we can define $g_v = f + \sigma_v$. By construction $g_v(v_k) = f(v_k) + \sigma_v(v_k) = f(v_k) + b_k = 1$ and $g_v \in \mathcal{S}_0(f)$. Moreover, since the coefficients b_k uniquely identify σ_v, such g_v is unique. □

As a consequence of Proposition 2 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 weightwise nonlinearity and weightwise 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 $\mathsf{NL}_k(f) = \mathsf{NL}_k(g)$.*

Proof. Any symmetric function in $\mathcal{S}_0$ can be written as sum of slice indicator functions with index in $[1, n-1]$ (see Lemma 1). Therefore, if $\sigma = f + g$ there exist $b_1, \ldots, b_{n-1} \in \mathbb{F}_2$ such that $\sigma = \sum_{k=1}^{n-1} b_k \varphi_{k,n}$. Applying recursively Property 7 we obtain from Property 1 that for all $a \in \mathbb{F}_2^n$ and for all $k \in [0, n]$ we have $|\mathcal{W}_{g,k}(a)| = |\mathcal{W}_{f,k}(a)|$. This is sufficient to conclude that, for all $k \in [0, n]$:

$$\mathsf{NL}_k(f) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f,k}(a)|}{2} = \mathsf{NL}_k(g).$$

□

Theorem 2. *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 $\mathsf{AI}_k(f) = \mathsf{AI}_k(g)$.*

Proof. For $k = 0, n$, the restrictions of f and g on the slices coincide by definition of $\mathcal{S}_0$. Consequently, they have the same restricted algebraic immunity. Let us consider $k \in [1, n-1]$ and h a Boolean function non null on $\mathsf{E}_{k,n}$ and such that either $(fh)_{|\mathsf{E}_{k,n}} = 0$ or $((1+f)h)_{|\mathsf{E}_{k,n}} = 0$. Denoting $\sigma = f + g \in \mathcal{S}_0$, we have that there exist unique coefficients $b_1, \ldots, b_{n-1} \in \mathbb{F}_2$ such that $\sigma = \sum_{j=1}^{n-1} b_j \varphi_{j,n}$. Then, considering the case $(fh)_{|\mathsf{E}_{k,n}} = 0$ without lost of generality, we can write:

$$g \cdot h \cdot \varphi_{k,n} = (f + \sigma) \cdot h \cdot \varphi_{k,n} = (\sum_{j=1}^{n-1} b_j \varphi_{j,n}) \cdot h \cdot \varphi_{k,n} = b_k \cdot h \cdot \varphi_{k,n},$$

$$(1 + g) \cdot h \cdot \varphi_{k,n} = (f + \sigma + 1) \cdot h \cdot \varphi_{k,n} = (\sum_{j=1}^{n-1} (b_j + 1) \varphi_{j,n}) \cdot h \cdot \varphi_{k,n} = (b_k + 1) \cdot h \cdot \varphi_{k,n}.$$

Since for every Boolean function f we have that $(f \cdot \varphi_{k,n})_{|\mathsf{E}_{k,n}} = f_{|\mathsf{E}_{k,n}}$, and b_k is a binary value we obtain that one between $(gh)_{|\mathsf{E}_{k,n}} = 0$ and $((1+g)h)_{|\mathsf{E}_{k,n}} = 0$ must be zero. This implies that $\mathsf{AI}_k(f) = \mathsf{AI}_k(g)$. □

While functions in the same $\mathcal{S}_0$-class have the same weightwise nonlinearities and 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 17. *Let $m \in \mathbb{N}^*$ and $n = 2^m$, we define:*

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

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

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

Remark 2. From Lemma 1 we have that $\mathcal{S}_0$ is a vector space, hence a group. $\mathcal{S}_0$-class can be interpreted as orbits of Boolean functions respect to the action of $\mathcal{S}_0$ over the set $\mathcal{B}_n$:

$$\begin{aligned} \Sigma \colon \mathcal{S}_0 \times \mathcal{B}_n &\to \mathcal{B}_n \\ (\sigma, f) &\mapsto f + \sigma \end{aligned}$$

In these terms, Proposition 2 implies that both the subset of weightwise almost perfectly balanced functions and weightwise perfectly balanced functions are stable under the action of $\mathcal{S}_0$. Notice that $\mathcal{SYM}_n$ is also stabilized.

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 18 (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:*

$$\sigma\mathsf{deg}(f) = \begin{cases} \max D_f & \text{if } D_f \neq \emptyset \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 3. *Let $m \in \mathbb{N}^*$ and $n = 2^m$. Let f, g $\mathcal{S}_0$-equivalent Boolean functions in n variables. Then, $\sigma\mathsf{deg}(f) = \sigma\mathsf{deg}(g)$.*

Proof. If $\sigma\mathsf{deg}(f) = 0$, for every $d \in [0, n]$ the ANF of f contains either all monomials of degree d or none. Namely, $f \in \mathcal{SYM}_n$ and $f + \sigma \in \mathcal{SYM}_n$ for every $\sigma \in \mathcal{S}_0$. This implies if $g \in \mathcal{S}_0(f)$, $\sigma\mathsf{deg}(g) = \sigma\mathsf{deg}(f) = 0$. Suppose now $\sigma\mathsf{deg}(f) > 0$. Let f_{ds} be the sum of monomials in f of degree up to $\sigma\mathsf{deg}(f)$. Since $\sigma\mathsf{deg}(f)$ is the maximum $d \in \mathbb{N}^*$ such that the ANF of f does not contain all the monomials of degree d, there exist $b_{\sigma\mathsf{deg}(f)}, \dots, b_n \in \mathbb{F}_2$ such that

$$f = f_{ds} + \sum_{k=\sigma\mathsf{deg}(f)+1}^{n} b_k \sigma_{k,n}.$$

From Proposition 1 we can write any $\sigma \in \mathcal{S}_0$ as $\sum_{k=1}^{n-1} a_k \sigma_{k,n}$. Then,

$$g = f + \sigma = \underbrace{f_{ds} + \sum_{k=1}^{\sigma\mathsf{deg}(f)} a_k \sigma_{k,n}}_{g_{ds}} + \sum_{k=\sigma\mathsf{deg}(f)+1}^{n} (a_k + b_k)\sigma_{k,n}. \tag{1}$$

This implies that $\sigma\mathsf{deg}(g) = \mathsf{deg}(g_{ds}) = \mathsf{deg}(f_{ds}) = \sigma\mathsf{deg}(f)$. □

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 a Boolean function of n variables 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 $\mathsf{deg}(g) = \delta$.*

Proof. Let f_{ds} be the sum of monomials in f of degree up to $\sigma\mathsf{deg}(f) > 0$. Repeating the arguments of the proof of Lemma 3 to get Equation (1), we have that every $g \in \mathcal{S}_0(f)$ can be uniquely written as

$$g = \underbrace{f_{ds} + \sum_{k=1}^{\sigma\mathsf{deg}(f)} a_k\sigma_{k,n}}_{g_{ds}} + \sum_{k=\sigma\mathsf{deg}(f)+1}^{n-1} c_k\sigma_{k,n}.$$

for some fixed $a_k, c_k \in \mathbb{F}_2$. This implies that $\mathsf{deg}(g)$ cannot be smaller than $\mathsf{deg}(f_{ds}) = \sigma\mathsf{deg}(f)$. Moreover, we have exactly $2^{\sigma\mathsf{deg}(f)}$ possible values for $g_{ds} \in \mathcal{S}_0(f)$. All functions of degree δ for $\sigma\mathsf{deg}(f) < \delta < n$ are of the form $g_{ds} + \sum_{k=\sigma\mathsf{deg}(f)}^{\delta-1} c_k\sigma_{k,n} + \sigma_{\delta,n}$. Hence, we obtain $2^{\delta-1}$ functions of such degree in $\mathcal{S}_0(f)$. □

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, based on the 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 the function $f_{n,d}$ as :*

$$f_{n,d} = \begin{cases} f_n & \textit{as in Definition 9 if } d = \frac{n}{2}, \\ f_n + \sigma_{d,n} & \textit{if } \frac{n}{2} < d < n. \end{cases}$$

The function $f_{n,d}$ is weightwise perfectly balanced and $\mathsf{deg}(f_{n,d}) = d$.

Proof. Since, for all d, $f_{n,d} \in \mathcal{S}_0(f_n)$ and $f_n \in \mathcal{WPB}_m$, the function $f_{n,d}$ is weightwise perfectly balanced from Proposition 2. If $d = n/2$ then $f_{n,d} = f_n$ hence $\mathsf{deg}(f_{n,n/2}) = n/2$ by Property 4, otherwise $\mathsf{deg}(f_{n,d}) = \mathsf{deg}(\sigma_{d,n}) = d$. □

4.1 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 2. 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:

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

We prove now that a WPB function have degree $n-1$ with probability greater than $1/2$. First, notice that the following property implies $D_{d,m} = \theta_{d,m} = 0$ for $d < n/2$:

Property 9 (Proposition 4 from [CMR17])**.** *If f is a weightwise perfectly balanced Boolean function of n variables, then the ANF of f contains at least one monomial of degree $n/2$.*

From Property 4 we know that $\theta_{n/2,m} > 0$. Hence, the number of WPB functions of minimal degree is a multiple of $2^{n/2}$.

Lemma 4. *Let $m \in \mathbb{N}$, $m \geq 3$, $n = 2^m$ and $d \in [n/2, n-2]$ the following holds: $\theta_{n-1,m} \geq \theta_{d,m}$.*

Proof. If $\theta_{d,m} = 0$ then $\theta_{n-1,m} \geq \theta_{d,m}$ so we focus on the case $\theta_{d,m} > 0$. First, for each function WPB f with $\sigma\mathsf{deg}(f) = d$ we create a WPB function g such that $\sigma\mathsf{deg}(g) = n-1$. Since f is WPB, for all $k \in [1, n-1]$ we have $|\mathsf{supp}_k(f)| = |\mathsf{E}_{k,n}|/2$, therefore on the slice $n-1$, $|\mathsf{supp}_{n-1}(f)| = n/2 = |\mathsf{supp}_{n-1}(f+1)|$, and there exist pairs of elements $(u,v) \in \mathsf{E}^2_{n-1,n}$ such that $f(u) = 0$ and $f(v) = 1$. For an element $a \in \mathbb{F}_2^n$ we denote x^a the monomial defined by $x^a = \prod_{i \in \mathsf{supp}(a)} x_i$. Since u and v belongs to $\mathsf{E}_{n-1,n}$, the monomials x^u and x^v have degree $n-1$. In the following we consider the properties of the function $g = f + x^u + x^v$.

We recall that in the ANF of f there are all or none of the monomials of degree $n-1$ since $\sigma\mathsf{deg}(f) = d$. This implies that the degree of g is $n-1$ since it has 2 degree-$n-1$ monomials of difference with f and $2 < |\mathsf{E}_{n-1,n}| = n$ when $n \geq 2$. With the same argument $\sigma\mathsf{deg}(g) = n-1$. Then, we show that g is WPB. Since only the ANF of degree at least $n-1$ differs between f and g, the two functions have the same support on all slices of Hamming weight lower than $n-1$. On the slice $\mathsf{E}_{n-1,n}$, we have $\mathsf{supp}_{n-1}(g) = \{\mathsf{supp}_{n-1}(f) \cup \{u\}\} \setminus \{v\}$, therefore $|\mathsf{supp}_{n-1}(g)| = |\mathsf{supp}_{n-1}(f)| = n/2$. On the last slice, $g(1_n) = f(1_n) + x^u(1_n) + x^v(1_n) = 1+1+1 = 1$, it allows to conclude, g is WPB.

Finally, by construction each pair (u,v) gives a different function g from a function f since g has the same support on all the slices of weight lower than $n-1$, and only $2 < n/2$ modifications on the slice $n-1$. It allows to conclude $\theta_{n-1,m} \geq \theta_{d,m}$. Note that, if $m = 2$, $|\mathsf{E}_{n-1,n}| = 4$ and in this case f and $f + \sigma_{3,4}$ can lead to the same function g for different pairs (u,v).

□

As a consequence, we can also show that more than half of the WPB functions have degree $n-1$:

Theorem 4. *Let $m \in \mathbb{N}, m \geq 3$, $n = 2^m$, the probability of a WPB function from $\mathcal{WPB}_m$ having degree $n-1$ is:*

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

Proof. The number of n-variable WPB functions of degree $n-1$ is:

$$D_{n-1,m} = 2^{n-2}\theta_{n-1,m} + 2^{n-2} \cdot \sum_{k=0}^{n-1} \theta_{k,m} = 2^{n-2}\theta_{n-1,m} + 2^{n-2}\frac{|\mathcal{WPB}_m|}{|\mathcal{S}_0|}.$$

Therefore, the probability that a WPB function has degree $n-1$ is:

$$\frac{D_{n-1,m}}{|\mathcal{WPB}_m|} = \frac{2^{n-2}\theta_{n-1,m}}{|\mathcal{WPB}_m|} + 2^{n-2}\frac{1}{|\mathcal{S}_0|} = \frac{2^{n-2}\theta_{n-1,m}}{|\mathcal{WPB}_m|} + \frac{1}{2} > \frac{1}{2}$$

since $\theta_{n-1} > 0$ using Lemma 4. □

Experimental degree distribution in $\mathcal{WPB}_m$ for $m \in [2,4]$. 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. Following the same principle as in [GM22a, GM23a], we exhausted $\mathcal{WPB}_2$ to collect the distribution of the degree, while we sampled uniformly at random WPB functions in 8 and 16 variables and we extrapolated an approximation of the distribution of the degree for these cases. See Figure 1, Figure 2 and Table 3, respectively.

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

In this section we show that 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 function by exhausting the parameters of all the elements of the class when the number of variables is limited (up to 16), or by using more complex methods to increase specific parameters while staying in the class.

x	2	3
$p_{\mathsf{deg}}(x)\%$	13.333	86.667
#	96	624

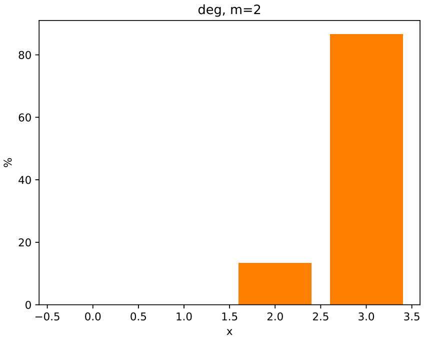

Fig. 1. Degree distribution in $\mathcal{WPB}_2$.

x	6	7
$\tilde{p}_{\mathsf{deg}}(x)\%$	0.782	99.218
#	65905	8361615

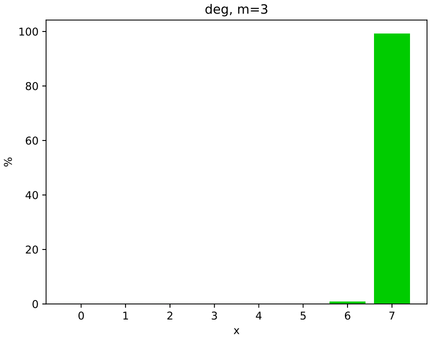

Fig. 2. Approximation of the degree distribution in $\mathcal{WPB}_3$ via sampling elements of $\mathcal{WPB}_3$ uniformly at random. The sample size is larger than 2^{23}.

5.1 Algebraic immunity inside an $\mathcal{S}_0$ class

In this part we focus on the $\mathsf{mAI}\mathcal{S}_0(m)$ parameter (Definition 17). In [GM23b], 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 [GM23b], 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 5. *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 :*

- $\mathsf{AI}(s_i) > 2t$,
- $\mathsf{AI}(s_i + s_j) > 2t$, *for all $i \neq j$,*

then for all $f \in \mathcal{B}_n$ there exists $g \in \mathcal{S}_0(f)$ such that $\mathsf{AI}(g) \geq t + 1$.

Proof. We prove the result by contradiction. Assume that all elements in $\mathcal{S}_0(f)$ have algebraic immunity at most t, then we consider the function f and the 2^t functions $f + s_i$ where s_i are the ones defined in the statement. We denote f by f_0, and f_i with $i \in [1, 2^t]$ the other functions. Since the AI of these functions is at most t, for each one of them we can take an annihilator g_i of f_i or annihilator of $f_i + 1$, such that $\deg(g_i) \leq t$ and $g_i \neq 0$.

Then, we have that each sum $f_i + f_j$ with $0 \leq i < j \leq 2^t$ is equal to a function s_j or $s_i + s_j$, and $(g_i \cdot g_j)(f_i + f_j + \varepsilon) = 0$ where $\varepsilon \in \{0, 1\}$. By construction $g_i \cdot g_j$ has degree at most $2t$ so it can only be null since the algebraic immunity of $f_i + f_j$ is greater than $2t$. All the products $g_i \cdot g_j$ being null means that the support of all the g_i, $i \in [0, 2^t]$ are disjoints. Since the g_i are non null functions of degree at most t their support have size at least 2^{n-t} and $(2^t + 1)2^{n-t} > 2^n$ which leads to a contradiction.

x	14	15
$\tilde{p}_{\mathsf{deg}}(x)\%$	0.003	99.997
$\#$	17	641007

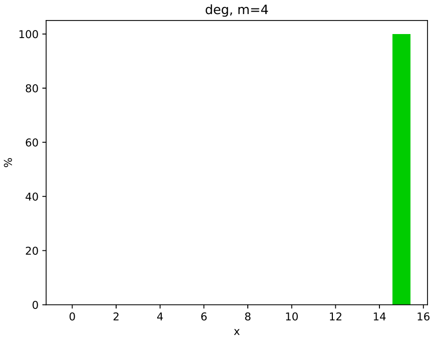

Fig. 3. Approximation of the degree distribution in $\mathcal{WPB}_4$ via sampling elements of $\mathcal{WPB}_4$ uniformly at random. The sample size is larger than 2^{19}.

□

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 5 in $\mathcal{S}_0$. We recall necessary results for it:

Property 10 (Adapted from [MT21], Proposition 12)**.** *Let $k, d \in \mathbb{N}$, let $f \in \mathcal{B}_n$ such that $\mathsf{AI}(f) = k$, and $h \in \mathcal{B}_n$ such that $\mathsf{w_H}(h) < \min(2^{n-k}, 2^{d+1} - 1)$, then $|\mathsf{AI}(f + h) - \mathsf{AI}(f)| \leq d$.*

Property 11 (AI of threshold functions, *e.g.* [CM22], Proposition 3)**.** *Let $n \in \mathbb{N}$, $d \in [1, n]$, the threshold function $\mathsf{T}_{d,n}$ has the following algebraic immunity: $\mathsf{AI}(\mathsf{T}_{d,n}) = \min(d, n - d + 1)$.*

Proposition 3. *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 $\mathsf{AI}(f) \geq 2^{m-r} - 1$.

Proof. First, we prove that for $r < m$, $\mathsf{AI}(\sigma_{2^m - 2^{m-r}, 2^m}) \geq 2^{m-r}$. Note that, from Property 5, $\sigma_{2^m - 2^{m-r}, 2^m}$ takes the value $\binom{k}{2^m - 2^{m-r}} \mod 2$ on the slice $\mathsf{E}_{k,n}$, that is, 0 for $k < 2^m - 2^{m-r}$, 1 for $k \in [2^m - 2^{m-r}, 2^m - 1]$ and 0 for $k = 2^m$ from Lucas' Theorem (see Property 6). Therefore, $\sigma_{2^m - 2^{m-r}, 2^m} = \mathsf{T}_{2^m - 2^{m-r}, 2^m} + \mathsf{T}_{2^m, 2^m}$ by Definition 14. Then, for $r > 1$, using Property 10, since $\mathsf{w_H}(\mathsf{T}_{2^m, 2^m}) = 1$, and since from Property 11 we get $\mathsf{AI}(\mathsf{T}_{2^m - 2^{m-r}, 2^m}) = 2^{m-r} + 1$, we can conclude $\mathsf{AI}(\sigma_{2^m - 2^{m-r}, 2^m}) \geq 2^{m-r}$. For $r = 1$, we get $\sigma_{2^m - 2^{m-r}, 2^m} = \sigma_{2^{m-1}, 2^m}$ and in this case its AI is 2^{m-1} from Property 5.

Then, we consider any function f with at least two $\sigma_{i, 2^m}$ functions in their ANF, and consider the smaller value of i. We write f as $f = \sigma_{2^m - 2^s, 2^m} + g$ where:

- $m - 1 \geq s > m - r$.
- g's ANF contains only monomials of degree greater than $2^m - 2^{s-1}$.

For any non null function h of degree at most $2^{m-r} - 1$ we consider the degree of $h \cdot f = h \cdot \sigma_{2^m - 2^s, 2^m} + h \cdot g$. Since $\mathsf{AI}(\sigma_{2^m - 2^s, 2^m}) \geq 2^{m-r}$ we have that $h \cdot \sigma_{2^m - 2^s, 2^m} \neq 0$ and all monomials of this product have degree in the range $[2^m - 2^s, 2^m - 2^s + 2^{m-r} - 1]$, hence they cannot be canceled by the monomials from the product $h \cdot g$, therefore $h \cdot f \neq 0$. Similarly for $1 + f$, writing it as $1 + \sigma_{2^m - 2^s, 2^m} + g$ we obtain that the product by any non null function h of degree at most $2^{m-r} - 1$ has a non null parts in its ANF (in the range of degrees $[2^m - 2^s, 2^m - 2^s + 2^{m-r} - 1]$). Therefore, we can conclude $\mathsf{AI}(f) \geq 2^{m-r} - 1$. □

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* $\mathsf{mAI}\mathcal{S}_0(m) \geq t + 1$.

Proof. First, to apply Lemma 5 we need 2^t functions s_i from $\mathcal{S}_0$ that have AI greater than $2t$ and such that each sum of 2 functions also has AI greater than $2t$. We take as functions s_i symmetric functions that can be written as $s_i = \sum_{j=1}^{r} v_j \sigma_{2^m - 2^{m-j}, 2^m}$ where:

- $r = t + 1$ if t is even, $r = t + 2$ otherwise,
- $v \in \mathbb{F}_2^n$, $\mathsf{w_H}(v)$ is odd.

Since r is odd we have $N = \sum_{k=0, k \text{ odd}}^{r} \binom{r}{k} = 2^{r-1}$, and by construction $N \geq 2^t$, therefore there are at least 2^t such functions s_i (provided m is bigger than r). Since each function s_i is the sum of an odd number of elementary functions of degree between 2^{m-1} and $2^m - 2^{m-r}$ we obtain that each sum of pair can be written as $s_i + s_j = \sum_{j=1}^{r} v_j \sigma_{2^m - 2^{m-j}, 2^m}$, where $\mathsf{w_H}(v) > 0$ and $\mathsf{w_H}(v)$ is even. Then, applying Proposition 3 all functions s_i and $s_i + s_j$ for $i \neq j$ have AI at least $2^{m-r} - 1$. Taking $m > \log(2t+1) + t + 1 + (t \mod 2)$ we get $m > \log(2t+1) + r$ that is $2^{m-r} - 1 > 2t$, thereafter we can apply Lemma 5 and conclude $\mathsf{mAI}\mathcal{S}_0(m) \geq t + 1$.

□

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 $m_5 = 11$.

Remark 3. In fact, the proof of Theorem 5 can be applied to any function, and not only WPB functions; by construction there is always a function with this lower bound on the algebraic immunity inside an $\mathcal{S}_0$ class.

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.

5.2 Nonlinearity inside an $\mathcal{S}_0$-class

In this part we focus on $\mathsf{mNL}\mathcal{S}_0(m)$, as defined in Definition 17. In [GM23a], 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:*

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

Proof. For any $f \in \mathcal{WPB}_m$, we show that at least one function between f and $f + \sigma_{2,2^m}$ has nonlinearity equal to or greater than $B = 2^{n-2} - 2^{\frac{n}{2}-2}$. If $\mathsf{NL}(f) \geq B$ the property holds, hence we focus on the case $\mathsf{NL}(f) < B$. In this case, we can write f as $(f + \ell) + \ell$ where ℓ is the best affine approximation of f (or one of the best if multiple functions reach the same minimal distance), that is such that $\mathsf{d_H}(f, \ell) = \mathsf{NL}(f)$, which implies $\mathsf{w_H}(f + \ell) < B$. We take $g = f + \sigma_{2,2^m}$ which is in the $\mathcal{S}_0$-class of f, we can write g as $\ell + (f + \ell) + \sigma_{2,2^m}$. Since the nonlinearity is an extended affine equivalent criteria we have $\mathsf{NL}(g(x)) = \mathsf{NL}(g(x) + a \cdot x + \varepsilon)$ (for all $a \in \mathbb{F}_2^n$ and $\varepsilon \in \{0,1\}$), and in particular $\mathsf{NL}(g) = \mathsf{NL}(f + \ell + \sigma_{2,2^m})$. Then, since $\sigma_{2,2^m}$ is a bent function (see Property 5) its distance to the closest affine function is $2^{n-1} - 2^{n/2-1}$, hence for any affine function ℓ' we have the triangular inequality $\mathsf{d_H}(\ell', \sigma_{2,2^m}) \leq \mathsf{d_H}(\ell', f + \ell + \sigma_{2,2^m}) + \mathsf{d_H}(f + \ell + \sigma_{2,2^m}, \sigma_{2,2^m})$. Thereafter, $\mathsf{d_H}(f + \ell + \sigma_{2,2^m}, \ell') \geq 2^{n-1} - 2^{n/2-1} - \mathsf{w_H}(f + \ell)$, which implies $\mathsf{NL}(g) \geq 2^{n-1} - 2^{n/2-1} - \mathsf{NL}(f)$. It allows us to conclude $\mathsf{NL}(g) \geq 2^{n-1} - 2^{n/2-1} - B$, that is $\mathsf{NL}(g) \geq B$.

□

Remark 4. As for the bound on $\mathsf{mAI}\mathcal{S}_0(m)$ in section 5.1, the proof of Theorem 6 also hold for functions that are not WPB.

5.3 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 5 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.

6 $\mathcal{S}_0$-classes of WPB functions

In this part we experimentally compute the parameters of WPB functions within their $\mathcal{S}_0$-class. In Section 6.1 we determine the parameters for all $\mathcal{S}_0$-classes of $\mathcal{WPB}_2$ since there are only 90. In Section 6.2 we exhibit the parameters of one part of the $\mathcal{S}_0$-classes of $\mathcal{WPB}_3$ only, since there are too man to exhaust all parameters. We focus on the $\mathcal{S}_0$-classes of WPB functions exhibited in former works.

6.1 $\mathcal{S}_0$ taxonomy of $\mathcal{WPB}_2$

The size of $\mathcal{S}_0$ in 4 variables is 8 and $|\mathcal{WPB}_2| = 720$, then the $\mathcal{S}_0$-equivalence relation produces a partition of $\mathcal{WPB}_2$ in 90 $\mathcal{S}_0$-classes. We further divide the classes according to the value that can be obtained as NL_2, nonlinearity and degree within the same classes and summarize the result in Table 1. We recall that all functions in degree 4 have algebraic immunity 2. We can observe that only less than 14% of $\mathcal{S}_0$-classes contain functions with all the possible values of degree and NL, and these classes only contain functions with null weightwise nonlinearity.

$\mathsf{NL}_2, \mathsf{NL}, \mathsf{deg}$	$\#\ \mathcal{S}_0$-classes
$1, \{2,4\}, \{3\}$	12
$1, \{4\}, \{3\}$	30
$1, \{4\}, \{2,3\}$	12
$0, \{2,4\}, \{2,3\}$	12
$0, \{2,4\}, \{3\}$	24

Table 1.

6.2 Selection of $\mathcal{S}_0$-classes in $\mathcal{WPB}_3$

We computed $\mathcal{S}_0$-classes of some known constructions in 8 variables. The properties of these formerly studied functions are summarized in Table 2, then we investigate the parameters inside their $\mathcal{S}_0$-classes in dedicated tables.

- The algebraic normal form of CMR function (Definition 9) in 8 variables is $f_8 = x_1 + x_2x_3 + x_2 + x_4x_5x_6x_7 + x_4x_5 + x_4 + x_6$. We collect the distribution of degree, algebraic immunity and nonlinearities of its $\mathcal{S}_0$-class in Table 3.
- The family of 8-variable WPB functions introduced in [LM19] (see Definition 10) have good restricted nonlinearities. We study here the $\mathcal{S}_0$-class some of these function, too. Specifically, we consider the function referred as l in [GM22b] and two other elements sampled uniformly at random by this family that we denote by l', l''. See Table 4.
- Selecting arbitrary sets U_i as in Definition 11 we obtain distinct functions from the TL family ([TL19]). We construct the $\mathcal{S}_0$-class of four functions a_1, a_2, a_3, a_4 uniformly sampling U_i in 8 variables. See Table 5.
- The family of WPB functions with high nonlinearity constructed in [GM23a] has algebraic immunity 2 [GM23b]. We summarize the properties of the $\mathcal{S}_0$-class of three functions sampled from this family with different nonlinearity. See Table 6.2, Table 6 and Figure 4.
- Every function in the *porcelain* family described in [GM23b] has algebraic immunity 2. We summarize the property of the $\mathcal{S}_0$-class of three functions p_1, p_2, p_3 sampled from this family with different nonlinearity. See Table 7.
- We collect the data also for three functions g_1, g_2, g_3 sampled uniformly at random from $\mathcal{WPB}_3$. See Table 8. For these functions we observe that all the $\mathcal{S}_0$-equivalent functions have degree 7 and algebraic immunity 4.

	deg	AI	NL	NL$_2$	NL$_3$	NL$_4$	NL$_5$	NL$_6$	Reference
f_8	4	4	88	2	12	19	12	6	[CMR17]
l	7	4	108	6	21	27	22	9	[LM19]
l'	7	4	96	9	8	19	20	6	[LM19]
l''	7	4	104	9	16	19	16	6	[LM19]
a_1	7	4	88	8	8	22	8	7	[TL19]
a_2	7	4	88	6	8	22	8	6	[TL19]
a_3	7	4	88	6	8	20	8	7	[TL19]
a_4	7	4	90	6	8	24	8	7	[TL19]
s_{112}	7	2	112	2	0	3	0	2	[GM23a]
s_{114}	7	2	114	2	0	3	0	2	[GM23a]
s_{116}	7	2	116	2	0	3	0	2	[GM23a]
p_1	7	2	64	6	19	21	11	3	[GM23b]
p_2	7	2	76	6	14	20	11	6	[GM23b]
p_3	7	2	82	7	15	18	14	6	[GM23b]
g_1	7	4	106	7	17	21	18	7	SUR
g_2	7	4	104	7	15	19	19	7	SUR
g_3	7	4	104	5	18	23	17	6	SUR

Table 2. Criteria of some 8-variable WPB functions from known constructions, referred in the last column. SUR corresponds to functions sampled uniformly at random.

NL	84	88	92	96	100	104
#	8	68	16	20	4	12

deg	4	5	6	7
#	16	16	32	64

AI	3	4
#	36	92

Table 3. Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(f_8)$.

	NL	96	100	104	106	108	110	112
$\mathcal{S}_0(l)$	#	0	0	4	16	24	48	36
$\mathcal{S}_0(l')$	#	16	0	48	12	40	8	4
$\mathcal{S}_0(l'')$	#	16	4	80	8	0	20	0

deg	7
#	128
#	128
#	128

AI	3	4
#	0	128
#	0	128
#	14	114

Table 4. Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(l)$, $\mathcal{S}_0(l')$ and $\mathcal{S}_0(l'')$.

	AI	3	4
$\mathcal{S}_0(a_1)$	#	64	64
$\mathcal{S}_0(a_2)$	#	64	64
$\mathcal{S}_0(a_3)$	#	64	64
$\mathcal{S}_0(a_4)$	#	64	64

deg	7
#	128
#	128
#	128
#	128

NL	80	88	90	92	94	96	98	100	102
#	16	36	8	6	16	22	14	8	2
#	16	36	10	10	12	32	12	0	0
#	16	36	10	10	18	36	2	0	0
#	16	34	6	8	14	34	4	6	6

Table 5. Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(a_1)$, $\mathcal{S}_0(a_2)$, $\mathcal{S}_0(a_3)$ and $\mathcal{S}_0(a_4)$.

	AI	2	3	4
$\mathcal{S}(s_{112})$	#	24	96	8
$\mathcal{S}(s_{114})$	#	32	88	8
$\mathcal{S}(s_{116})$	#	32	88	8

deg	7
#	128
#	128
#	128

	NL	8	16	24	32	40	48	56	64	72	88	90	92	94	96	104	110	112	114	116
$\mathcal{S}_0(s_{112})$	#	4	8	4	8	16	8	4	16	12	16	2	2	2	10	4	8	4	0	0
$\mathcal{S}_0(s_{114})$	#	4	8	4	8	16	8	4	16	12	16	2	4	2	8	4	8	2	2	0
$\mathcal{S}_0(s_{116})$	#	4	8	4	8	16	8	4	16	12	16	4	4	0	8	4	8	0	0	4

Table 6. Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(s_{112})$, $\mathcal{S}_0(s_{114})$ and $\mathcal{S}_0(s_{116})$.

	AI	2	3	4
$\mathcal{S}_0(p_1)$	#	4	56	68
$\mathcal{S}_0(p_2)$	#	4	56	68
$\mathcal{S}_0(p_3)$	#	4	58	66

deg	7
#	128
#	128
#	128

	NL	64	66	70	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100	102	104	106	108	110
$\mathcal{S}_0(p_1)$	#	2	2	4	4	0	2	4	2	2	6	6	6	16	14	20	6	12	0	8	0	8	2	2
$\mathcal{S}_0(p_2)$	#	0	0	0	2	6	6	4	6	6	2	6	6	14	4	16	8	6	20	6	10	0	0	0
$\mathcal{S}_0(p_3)$	#	0	0	2	4	2	4	8	4	2	6	6	2	6	14	10	12	10	6	8	16	6	0	0

Table 7. Distribution of nonlinearities, degree and algebraic immunity in $\mathcal{S}_0(p_1)$, $\mathcal{S}_0(p_2)$ and $\mathcal{S}_0(p_3)$.

7 Conclusions and open questions

In this article we introduced the notion of $\mathcal{S}_0$-equivalent class for Boolean functions in $2^m > 1$ variables. Namely, we consider the partition of the Boolean functions space by collecting in the same class functions which addition is a symmetric function null in 0_n and 1_n.

First, we studied invariant properties of these classes. We proved that if a function is either WPB or WAPB, the same holds for all the functions in its class. Additionally, $\mathcal{S}_0$-equivalent functions have the same weightwise nonlinearity and weightwise algebraic immunity.

Then, we studied the behavior of the degree, nonlinearity and algebraic immunity inside $\mathcal{S}_0$-classes and determine bounds for edge quantities like the best guaranteed value, for the degree, algebraic immunity and nonlinearity, achievable by modifying a function in $\mathcal{WPB}_m$, while staying within its $\mathcal{S}_0$-class, *i.e.* $\mathsf{mdeg}\mathcal{S}_0(m), \mathsf{mAI}\mathcal{S}_0(m)$ and $\mathsf{mNL}\mathcal{S}_0(m)$. Specifically, for the degree we proved the distribution of degree inside a class of a WPB function is determined by its sigma-degree $\sigma\mathsf{deg}(f)$, which is another invariant of the class deduct from the ANF of the function. As a corollary, we also showed that for any value between $n/2$ and $n-1$ (included) there exist WPB functions

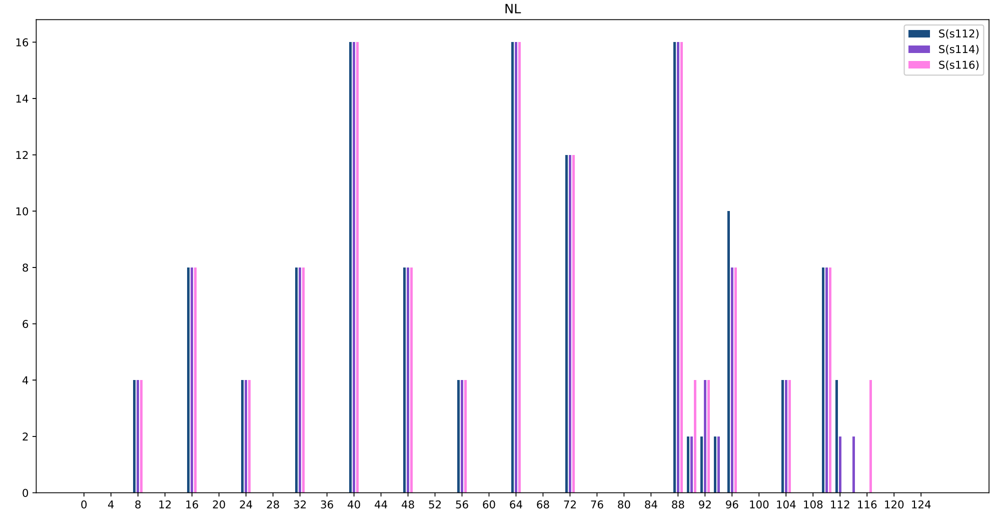

Fig. 4. Display of nonlinearity's distribution in Table 6

	NL	94	96	98	100	102	104	106	108	110
$\mathcal{S}_0(g_1)$	#	2	6	14	4	24	34	30	14	0
$\mathcal{S}_0(g_2)$	#	0	2	14	8	52	24	26	2	0
$\mathcal{S}_0(g_3)$	#	0	0	8	8	24	48	34	4	2

Table 8. Distribution of nonlinearities in $\mathcal{S}_0(g_1)$, $\mathcal{S}_0(g_2)$ and $\mathcal{S}_0(g_3)$.

reaching this degree, explicitly exhibiting a new family of WPB functions with prescribed degree for all $n = 2^m$. Additionally, we used this results to infer properties of the degree distribution in $\mathcal{WPB}_m$ and prove that more than half of the functions in this set have degree exactly $n-1$. Then, analyzing the algebraic immunity and nonlinearity of certain symmetric functions we derived lower bounds for both $\mathsf{mAI}\mathcal{S}_0(m)$ and $\mathsf{mNL}\mathcal{S}_0(m)$. It demonstrated that there are always $\mathcal{S}_0$-equivalent functions with better AI and nonlinearity than the one with minimal parameters exhibited in former works. Moreover, the proofs of these bounds hold for functions that are not WPB. We also discussed how the concept of $\mathcal{S}_0$-class can be generalized and how the results on $\mathsf{mdeg}\mathcal{S}_0(m)$, $\mathsf{mAI}\mathcal{S}_0(m)$ and $\mathsf{mNL}\mathcal{S}_0(m)$ can be extended.

Finally, we presented experimental results. In Section 6 we provided an exhaustive taxonomy of 4-variable classes. While, for 8 variables we analyzed $\mathcal{S}_0$-classes of some function from know families, *e.g.* [CMR17, LM19, TL19, GM23a, GM23b]

Regarding open questions and future possible directions:

- In Section 5.3, we outline a possible extension to other equivalence relations defined up to the addition of functions from a family $\mathcal{T}$. Indeed, we suggest that for cryptographic application 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 observe our work suggests a new strategy to construct a WPB function with good cryptographic criteria. Indeed, being weightwise properties invariant in $\mathcal{S}_0$-classes, as soon as we identify a function having good weightwise properties, we can then improve the global properties by looking directly inside its $\mathcal{S}_0$-class. $\mathsf{mdeg}\mathcal{S}_0(m)$, $\mathsf{mAI}\mathcal{S}_0(m)$ and $\mathsf{mNL}\mathcal{S}_0(m)$ express the best guaranteed value, for degree, algebraic immunity and nonlinearity, achievable by using this strategy. Therefore, it would be good to improve our bounds on these quantities. For instance, as we point out, it would be interesting to determine if $\mathsf{mAI}\mathcal{S}_0(m) = 2^{m-1}$, since it would imply that there are functions with optimal AI in each $\mathcal{S}_0$-class.

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.

GM23a. Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In Said El Hajji, Sihem Mesnager, and El Mamoun Souidi, editors, *Codes, Cryptology and Information Security*, pages 338–359, Cham, 2023. Springer Nature Switzerland.

GM23b. Agnese Gini and Pierrick Méaux. 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.

Méa19. Pierrick Méaux. On the fast algebraic immunity of majority functions. In Peter Schwabe and Nicolas Thériault, editors, *Progress in Cryptology - LATINCRYPT*, volume 11774 of *LNCS*, pages 86–105. 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 for the application of evolutionary algorithms in the seek of optimal boolean functions for cryptography. 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 1–8. 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.

YCL$^+$23. Lili Yan, Jingyi Cui, Jian Liu, Guangquan Xu, Lidong Han, Alireza Jolfaei, and Xi Zheng. Iga: An improved genetic algorithm to construct weightwise (almost) perfectly balanced boolean functions with high weightwise nonlinearity. In *Proceedings of the 2023 ACM Asia Conference on Computer and Communications Security*, ASIA CCS '23, page 638–648, New York, NY, USA, 2023. Association for Computing Machinery.

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.