Weightwise Almost Perfectly Balanced Functions, Construction From A Permutation Group Action View.

No Author Given

No Institute Given

Abstract. The construction of Boolean functions with good cryptographic properties over a subset of vectors with fixed Hamming weight is significant in lightweight stream ciphers like FLIP. We present a general idea to construct a class of Weightwise Almost Perfectly Balanced (WAPB) Boolean functions by using the action of a cyclic permutation group on $\mathbb{F}_2^n$. Further, considering a particular permutation group $\langle\psi_n\rangle$ (where ψ_n is a special type of permutation on n elements), we present a class of WAPB Boolean functions on n variables. This class generalizes the Weightwise Perfectly Balanced (WPB) Boolean function construction by Liu and Mesnager. Further, we studied the nonlinearity and weightwise nonlinearities of this class of functions.

Keywords: Boolean function, Weightwise perfectly balanced (WPB), Weightwise almost perfectly balanced (WAPB), Nonlinearity

1 Introduction

An n-variable Boolean function f is a mapping from the n-dimensional vector space $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ denotes a finite field with two elements $\{0, 1\}$. Depending upon the underlying algebraic structure, the symbol '+' is to indicate addition operations in $\mathbb{F}_2$, $\mathbb{F}_2^n$ and $\mathbb{R}$. The subsets of vectors with constant Hamming weight are denoted by $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathsf{w_H}(x) = k\}$ for $0 \le k \le n$. Typically, the cryptographic properties of Boolean functions are analyzed over the entire domain of vector space $\mathbb{F}_2^n$. The study of Boolean functions over restricted domains, specifically to the subsets of vectors with constant Hamming weight i.e., $\mathsf{E}_{k,n}$ for a specific k, has gained a considerable interest following the introduction of the stream cipher FLIP in 2016 [MJSC16]. In FLIP, the inputs to the filter function are from $\mathsf{E}_{\frac{n}{2},n}$. Further, this raises several questions concerning the characteristics of Boolean functions and their cryptographic properties. An initial cryptographic study of Boolean function in a restricted domain was undertaken by Carlet et al. in [CMR17]. In this paper, the authors introduced the concept of Weightwise Perfectly Balanced (WPB) Boolean functions in n variables which are balanced over $\mathsf{E}_{k,n}, 1 \le k \le n-1$. Such functions exist only when n is a power of two, otherwise, only functions that are *almost balanced* can exist. Here, *almost balanced* means that the counts of preimages of 0 and 1 differ by at most one. Functions that are almost balanced on each subset of constant Hamming weight are termed Weightwise Almost Perfectly Balanced (WAPB).

The first construction of Weightwise Perfectly Balanced (WPB) Boolean functions, presented in [CMR17] is based on the direct sum of four Boolean functions. The authors also proposed a recursive construction for Weightwise Almost Perfectly Balanced (WAPB) Boolean functions. In the same paper, the author established upper bounds on the nonlinearity and algebraic immunity of WPB/WAPB Boolean functions defined over $\mathsf{E}_{k,n}$. Subsequently, a numerous studies have been conducted within the framework of FLIP, focusing on optimizing Boolean functions for cryptographic criteria over restricted domains.

We present a brief summary of the advancements and further constructions of the families of WAPB functions introduced in previous studies. Tang and Liu [TL19] proposed a construction for a class of WAPB Boolean functions in even number of variables. These functions achieve optimal algebraic immunity over $\mathbb{F}_2^n$ and possess algebraic immunity greater than or equal to 2 on $\mathsf{E}_{k,n}$ for $3 \le k \le n-1$. A class of quadratic WAPB function was introduced in [LS20] to construct WPB functions by modifying the support of WAPB Boolean functions. In 2021, Mesnager and Su [MS21] derived a construction of n-variable WAPB Boolean functions for any positive integer n by algebraic normal form of a particular quadratic Boolean function.

Subsequetly, Zhu and Su in [ZS22] proposed an elegant constructon of WAPB functions by the direct sum of several known WPB Boolean functions. Guo and Su [GS22] introduced another class of WAPB Boolean functions on n-variables by modifying the support of quadratic Boolean functions. In [GM22b], a secondary construction of WAPB Boolean functions was introduced using Siegenthaler's construction. This approach allows to compute the nonlinearity bound over $\mathsf{E}_{k,n}$ of the resulting function to be determined using the known functions, enabling the generation of WAPB function with high nonlinearity over $\mathsf{E}_{k,n}$. Recent advancements have employed genetic algorithms (GA) to refine the properties of WPB in [MPJ$^+$22] and WAPB functions in [YCL$^+$23], specifically aiming to enhance their nonlinearity over $\mathsf{E}_{k,n}$. In [DM24], the author introduced a construction for a class of n-variable WAPB Boolean functions from the known support of an n_0-variable WAPB Boolean function where $n > n_0$. In [Méa24], the author proposed a construction for WAPB functions based on the concept of total order relations on vectors, aimed at simplifying implementation and also provide a recursive construction for WAPB Boolean function. Most studies primarily concentrate on WPB Boolean functions, which have been explored in [LM19, MS21, Su21, MPJ$^+$22, GM23c, GM23b, ZLC$^+$23, DM23, ZS23, ZJZQ23, GM23a]. Further, improved bounds on the nonlinearity and algebraic immunity of Boolean functions over restricted domains have been established in [MMM$^+$18, MSLZ22, GM22a, GM23c, GM23b].

To be cryptographic friendly, Boolean functions should be efficient to implement while achieving a balanced trade-off among various cryptographic criteria. However, these functions have not been comprehensively studied in terms of their cryptographic structures and properties, such as nonlinearity and algebraic immunity, both over $\mathbb{F}_2^n$ and over the set of vectors with constant Hamming weight. Moreover, Identifying such functions that closely approach the bounds established in previous research is also of significant importance. Therefore, analyzing the cryptographic properties and efficiency of WAPB Boolean functions is crucial for their potential application in ciphers like FLIP.

1.1 Our Contribution

Liu and Mesnager in [LM19] presented a class of WPB Boolean functions that are 2-rotation symmetric (see Proposition 1). These functions have the good nonlinearity and weightwise nonlinearities. However, their existence is restricted to cases where n is a power of 2. Furthermore, this class of functions of intresting algebraic structure as the truth values are invariant under 2-rotations(see Section 2.1). In this article, we introduce the general constructon of WAPB Boolean functions which is 2-invariant under any cyclic subgroup of symmetric group (i.e., $\langle\pi\rangle$ where $\pi \in \mathbb{S}_n$) on n elements. We also presented study of cryptographic properties for the cases of two different important permutations ψ and σ. In both cases, we generalize the construction to develop a class of WAPB Boolean functions for any number of variables. Hence, the Liu-Mesnager construction is the class of functions of our construction when n is power of 2.

Additionally, we propose new combinatorial identities for the binary Krawchouk polynomials of degree k to investigate the lower bounds on the nonlinearities of Boolean functions derived from this group action. Hereafter, we establish an improved bound on the nonlinearity over the set of vectors with Hamming weight 2 for the Liu-Mesnager [LM19] construction. Additionally, we provide strong bounds for the WAPB Boolean functions resulting from our proposed construction.

1.2 Organisation

The research objectives and our contributions are already outlined. The remaining part of the paper is organized as follows.

- Section 2 presents the required definitions and notations of a Boolean function and its critical cryptographic properties. Section 2.1 presents the definition and notations on π symmetric Boolean functions and 2-π symmetric Boolean functions. Some required known results and new results on Krawchouk polynomials are presents in Section 2.2.
- Section 3 contains a construction of 2-πS WAPB Boolean functions using the group action of a cyclic permutation group $P = \langle\pi\rangle$. Then some results on the lower bound of the nonlinearity and weightwise nonlinearities are presented.

- Section 4 and Section 5 presents the cryptographic studies for the special cases when $\pi = \psi$ and $\pi = \sigma$ where ψ and σ are distinct binary-cycle permutation and rotation permutation respectively. another main result of the paper.
- The paper is concluded in Section 6.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the vector space of dimension n over the binary field $\mathbb{F}_2$. For any two vectors $a = (a_1, a_2, \dots, a_n)$ and $b = (b_1, b_2, \dots, b_n)$ in $\mathbb{F}_2^n$, the dot product is defined as $a \cdot b = a_1b_1 + a_2b_2 + \cdots + a_nb_n \bmod 2$.

A Boolean function of n variables is a map from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ and $\mathcal{B}_n$ is the set of all n-variable Boolean functions. The 2^n-length binary sequence $(f(v_0), f(v_1), \dots, f(v_{2^n-1}))$ is called as the truth table of the Boolean function f, it corresponds to the ordered vectors of $\mathbb{F}_2^n$ as $v_0 = (0, 0, \dots, 0), v_1 = (0, 0, \dots, 1), \dots, v_{2^n-1} = (1, 1, \dots, 1)$. The Hamming weight of a vector $x \in \mathbb{F}_2^n$, denoted by $\mathsf{w_H}(x)$, is the number nonzero coordinates (i.e., 1s) in the vector x. The support of $f \in \mathcal{B}_n$, denoted by $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. The Hamming weight of the Boolean function f is the cardinality of $\mathsf{supp}(f)$ and is denoted by $\mathsf{w_H}(f)$. The function f is called balanced if $\mathsf{w_H}(f) = 2^{n-1}$. Let $f(x), g(x) \in \mathcal{B}_n$, then The Hamming distance between two Boolean functions $f, g \in \mathcal{B}_n$ is defined by $\mathsf{d_H}(f, g) = |\{x \in \mathbb{F}_2^n : f(x) \neq g(x)\}|$ i.e., $\mathsf{d_H}(f, g) = \mathsf{w_H}(f + g)$.

An n-variable Boolean function f can be expressed as a polynomial in the ring $\mathbb{F}_2[x_1, x_2, \dots, x_n]/ < x_1^2 + x_1, x_2^2 + x_2, \dots, x_n^2 + x_n >$, i.e. $f(x) = \sum\limits_{u \in \mathbb{F}_2^n} c_u x^{u_1} x^{u_2} \cdots x^{u_n}$, where c_u are the coefficients with a value in $\mathbb{F}_2$. It is called as the algebraic normal form or ANF and the number of variables in the highest order monomial with nonzero coefficient is called the *algebraic degree* of the function f, and denoted as $\deg(f)$. A function f is called as affine function if $f(x) = a \cdot x + b$ for $a \in \mathbb{F}_2^n$ and $b \in \mathbb{F}_2$. If $b = 0$, then f is called a linear Boolean function. $\mathcal{A}_n$ denotes the set of all n-variable affine functions.

Definition 1 (Walsh-Hadamard Transform). *The Walsh-Hadamard transform of a function on $\mathbb{F}_2^n$ is the map $W_f : \mathbb{F}_2^n \to \mathbb{R}$, defined by*

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

Definition 2 (Nonlinearity). *The nonlinearity of $f \in \mathcal{B}_n$ denoted as $\mathsf{NL}(f)$, is the minimum Hamming distance of f to any affine function. That is, $\mathsf{NL}(f) = \min\limits_{g \in \mathcal{A}_n} \mathsf{d_H}(f, g)$. It can be verified that $\mathsf{NL}(f) = 2^{n-1} - \frac{1}{2} \max\limits_{w \in \mathbb{F}_2^n} |W_f(w)|$.*

We denote $\mathsf{E}_{k,n} = \{x \in \mathbb{F}_2^n : \mathsf{w_H}(x) = k\}$ and $\mathsf{w}_{k,n}(f) = |\{x \in \mathsf{E}_{k,n} : f(x) = 1\}| = |\mathsf{supp}(f) \cap \mathsf{E}_{k,n}|$. Accordingly, the Hamming distance of two functions $f, g \in \mathcal{B}_n$ on $\mathsf{E}_{k,n}$ denoted as $d_{k,n}(f, g) = |\{x \in \mathsf{E}_{k,n} : f(x) \neq g(x)\}|$. The cryptographic criteria like balancedness, nonlinearity and algebraic immunity of a function f defined over $\mathbb{F}_2^n$ can also be defined, if we restrict f to the set $\mathsf{E}_{k,n}$. For two integers m, n with $m \leq n$, we define $[m, n] = \{m, m + 1, \dots, n\}$.

Definition 3 (Weightwise Almost Perfectly Balanced (WAPB)). *A Boolean function $f \in \mathcal{B}_n$ is said to be weightwise almost perfectly balanced (WAPB) if for all $k \in [0, n]$,*

$$\mathsf{w}_{k,n}(f) = \begin{cases} \frac{\binom{n}{k}}{2} & \text{if } \binom{n}{k} \text{ is even,} \\ \frac{\binom{n}{k} \pm 1}{2} & \text{if } \binom{n}{k} \text{ is odd.} \end{cases}$$

Definition 4 (Weightwise Perfectly Balanced (WPB)). *A Boolean function $f \in \mathcal{B}_n$ is said to be weightwise perfectly balanced (WPB) if for all $k \in [1, n-1]$,*

$$\mathsf{w}_{k,n}(f) = \frac{\binom{n}{k}}{2},$$

and $f(0, 0, \dots, 0) = 0 = 1 + f(1, 1, \dots, 1)$.

Using Lucas' Theorem *e.g.* [Fin47], we have that a WPB function exists only if, n is a power of 2. Hence, there are $\prod_{k=1}^{n-1}\binom{\binom{n}{k}}{\binom{n}{k}/2}$ WPB Boolean functions.

Definition 5 (Restricted Walsh Transform). *Let f be an n-variable Boolean function, then its Walsh transform $\mathcal{W}_{f,k}(a)$ is defined as:*

$$\mathcal{W}_{f,k}(a)=\sum_{x\in\mathsf{E}_{k,n}}(-1)^{f(x)+a\cdot x}.$$

Definition 6 (Weightwise Nonlinearity). *The nonlinearity of $f\in\mathcal{B}_n$ over $\mathsf{E}_{k,n}$, denoted as $\mathsf{NL}_k(f)$, is the Hamming distance of f to the set of all affine functions $\mathcal{A}_n$ when evaluated over $\mathsf{E}_{k,n}$. That is, $\mathsf{NL}_k(f)=\min_{g\in\mathcal{A}_n}d_{k,n}(f,g)=\min_{g\in\mathcal{A}_n}\mathsf{w}_{k,n}(f+g)$.*

The following identity and upper bound on the nonlinearity of a Boolean function over $\mathsf{E}_{k,n}$ can be derived. The upper bound is further improved by Mesnager et al. in [MZD19].

Lemma 1 ([CMR17], Propositions 4 and 5). *If $f\in\mathcal{B}_n$ then for $k\in[0,n]$,*

$$\mathsf{NL}_k(f)=\frac{|\mathsf{E}_{k,n}|}{2}-\frac{1}{2}\max_{a\in\mathbb{F}_2^n}|\mathcal{W}_{f,k}(a)|,\ \textit{and}$$

$$\mathsf{NL}_k(f)\le\frac{1}{2}[|\mathsf{E}_{k,n}|-\sqrt{|\mathsf{E}_{k,n}|}]=\frac{1}{2}[\binom{n}{k}-\sqrt{\binom{n}{k}}].$$

[**DKD:** Do we need to put the definition of $\mathsf{AI}(f)$ and $\mathsf{AI}_k(f)$?]

Definition 7 (Algebraic immunity and weightwise algebraic immunity). *The algebraic immunity of a Boolean function $f\in\mathcal{B}_n$, denoted as $\mathsf{AI}(f)$, is defined as:*

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

where $\mathsf{deg}(g)$ is the algebraic degree of g. The function g is called an annihilator of f (or $f+1$).

The weightwise algebraic immunity of $f\in\mathcal{B}_n$ for $k\in[0,n]$, denoted as $\mathsf{AI}_k(f)$, is defined as:

$$\mathsf{AI}_k(f)=\min_{g\neq 0\ \text{over}\ \mathsf{E}_{k,n}}\{\mathsf{deg}(g)\mid fg=0\text{ or }(f+1)g=0\}.$$

2.1 Permutation symmetric Boolean functions

We denote $\mathbb{S}_n$ by the symmetric group on n elements. For a permutation $\pi\in\mathbb{S}_n$, the action of permutation group $P=\langle\pi\rangle$ on $\mathbb{F}_2^n$ makes a partition of $\mathbb{F}_2^n$, called orbits. The set of orbits is denoted as $\mathcal{O}$. For $x\in\mathbb{F}_2^n$, we denote the orbit containing x as $O_\pi(x)=\{y\in\mathbb{F}_2^n\mid\pi^k(y)=x\text{ for some }k\in\mathbb{Z}\}$. Now we define two special permutations as follows.

1. **Rotation (or, cyclic) permutation (σ)**: The permutation $\sigma\in\mathbb{S}_n$ is called rotation permutation if $\sigma((x_1,x_2,\ldots,x_n))=(x_n,x_1,\ldots,x_{n-1})$ for every $(x_1,x_2,\ldots,x_n)\in\mathbb{F}_2^n$. We denote the rotation permutation on n elements by σ (or, σ_n to specify the number n). The cyclic group $P=\langle\sigma\rangle$ is called rotation symmetric group.
2. **Distinct binary-cycle permutation(ψ)**: Let n be a positive integer with the unique binary representation as

$$n=n_1+n_2+\cdots+n_w\text{ where }n_1=2^{a_1},n_2=2^{a_2},\ldots,n_w=2^{a_w}\text{ and }0\le a_1<a_2<\cdots<a_w.\quad(1)$$

A permutation $\psi \in \mathbb{S}_n$ is called a distinct binary-cycle permutation if its disjoint cycle form contains cycles of length $n_1, n_2, \ldots, n_w$. We name the permutation by distinct binary-cycle permutation as the length of each cycle is a power of 2 and the lengths of cycles are distinct. We denote the permutation on n elements by ψ (or, ψ_n to specify the number n). Without loss of generality, we consider

$$\psi = (x_1, x_2, \ldots, x_{n_1})(x_{n_1+1}, x_{n_1+2}, \ldots, x_{n_1+n_2}) \cdots (x_{n-n_w+1}, x_{n-n_w+2}, \ldots, x_n) = \sigma_{n_1}\sigma_{n_2}\cdots\sigma_{n_w}. \quad (2)$$

Note that, $\sigma = \psi$ when $n = 2^m$ is a power of 2. For $\pi \in \mathbb{S}_n$, we define π symmetric Boolean functions and 2-π symmetric Boolean functions as follows.

Definition 8 (π Symmetric Boolean function (πS)). *Let $\pi \in \mathbb{S}_n$ be a permutation on n elements with order $o(\pi)$. A Boolean function f is π symmetric (in short, πS) if and only if for any $(x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$,*

$$f(\pi^k(x_1, x_2, \ldots, x_n)) = f(x_1, x_2, \ldots, x_n) \text{ for every } 1 \le k \le o(\pi)$$

where $\pi^k = \pi \circ \pi^{k-1}$ for $k > 1$ and $\pi^1 = \pi$. Therefore, πS Boolean functions have the same truth value for all vectors in every orbit obtained by the action of permutation group $P = \langle\pi\rangle$ on $\mathbb{F}_2^n$.

For $\pi = \sigma$, the σS Boolean functions are known as Rotation Symmetric Boolean functions(in short, RotS). The σS Boolean functions are very well studied functions in the literature [PQ99, CS02, SM08]. However, no study on ψS Boolean functions is available in the literature. When n is power of 2, the class of σS Boolean functions and the class of ψS Boolean functions are same.

Definition 9 (2-π Symmetric Boolean function(2-πS)). *Let $\pi \in \mathbb{S}_n$ be a permutation on n elements and $\mathcal{O}$ be the set of all orbits due to the group action of $P = \langle\pi\rangle$ on $\mathbb{F}_2^n$. A Boolean function f is 2-π symmetric (in short, 2-πS) if and only if for every orbit $\mathsf{O} \in \mathcal{O}$ with a fixed representative element ν_{O},*

$$f(\pi^{2i}(\nu_{\mathsf{O}})) = f(\nu_{\mathsf{O}}); \quad f(\pi^{2i+1}(\nu_{\mathsf{O}})) = f(\nu_{\mathsf{O}}) + 1 \text{ for every } 0 \le i < \lfloor \frac{|\mathsf{O}|}{2} \rfloor.$$

Note that, if $|\mathsf{O}|$ is odd then $f(\pi^{|\mathsf{O}|-1}(\nu_{\mathsf{O}}))$ can be any value from $\mathbb{F}_2$.

Therefore, 2-πS Boolean functions have the alternative truth value for the lexicograpphically ordered vectors in every orbit obtained by the action of permutation group $P = \langle\pi\rangle$ on $\mathbb{F}_2^n$. As example, a 2-RotS Boolean function (i.e., 2-σS) on $n = 5$ satisfies $f(00001) = f(00100) = f(10000)$ and $f(00010) = f(01000) = 1 + f(00001)$ for the orbit $\{00001, 00010, \ldots, 10000\}$ with representative 00001.

A construction of a class of 2-σS WPB Boolean functions, when n is a power of 2, is presented by Liu and Mesnager [LM19] as follows.

Proposition 1. *[LM19] For a Boolean function $f \in \mathcal{B}_n$ with n is power of 2, if $f(x^2) = f(x) + 1$ holds for all $x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$, then f is WPB.*

The Boolean function proposed in Proposition 1 is 2-σS. Since, n is the power of 2 in the construction, the cardinality of all orbits in $\mathbb{F}_{2^n} \setminus \{0, 1\}$ are even. Therefore, $f(x^2) = f(x) + 1, x \in \mathbb{F}_{2^n} \setminus \{0, 1\}$ is well defined and hence, the truth value 1 and 0 can be assigned alternatively to the half of the vectors in the each orbit. This can not be assigned when n is not a power of 2 as there are some orbits with cardinality odd and hence the $f(x^2) = f(x) + 1$ can not be defined. However, we propose a generalization of this concept to construct WAPB Boolean function on any n where n is a natural number in Section 4. When n is power of 2, the class of 2-σS Boolean functions and the class of 2-ψS Boolean functions are the same.

Moreover, in the specific case of Proposition 1, the function is also σ^2-symmetric (σ^2S), as it takes the same value on each orbit under σ^2. This property, however, is only achievable when n is a power of 2.

2.2 Some Results on Krawtchouk Polynomials

We present some results on Krawtchouk polynomials and sequences which are useful for later results, and can be of independent interest.

Definition 10 (Krawtchouk polynomial). *For a positive integer n, the Krawtchouk polynomial [MS78, Page 151] of degree k is given by*

$$\mathsf{K}_k(x,n) = \sum_{j=0}^{k} (-1)^j \binom{x}{j}\binom{n-x}{k-j} \text{ for } k = 0, 1, \dots n.$$

Some nice properties of the Krawtchouk polynomials from [DMS06, Proposition 4, Corollary 1] are presented in the following Proposition.

Proposition 2. *1.* $\mathsf{K}_0(l,n) = 1, \mathsf{K}_1(l,n) = n - 2l$.

2. $\mathsf{K}_k(l,n) = (-1)^l \mathsf{K}_{n-k}(l,n)$ *(that implies,* $\mathsf{K}_{\frac{n}{2}}(l,n) = 0$ *for n even and l odd).*

3. $\mathsf{K}_k(l,n) = (-1)^k \mathsf{K}_k(n-l,n)$, *(that implies,* $\mathsf{K}_k(\frac{n}{2},n) = 0$ *for n even and k odd).*

4. For n odd, $|\mathsf{K}_k(1,n)| \geq |\mathsf{K}_k(l,n)|$ *where* $0 \leq k \leq n$ *and* $1 \leq l \leq n-1$,

5. For n even, $|\mathsf{K}_k(1,n)| \geq |\mathsf{K}_k(l,n)|$ *where* $0 \leq k \leq n$ *and* $1 \leq l \leq n-1$ *except* $k = \frac{n}{2}$ *or* $l = \frac{n}{2}$.

6. $(n-l)\mathsf{K}_k(l+1,n) = (n-2k)\mathsf{K}_k(l,n) - l\mathsf{K}_k(l-1,n)$.

The following relations are derived from some results in [DMS06, GM22a],

Proposition 3 (Krawtchouk polynomials relations). *For integers $n > 0$, $k \in [0,n]$ and fixed $a \in \mathbb{F}_2^n$ such that $\mathsf{w}_\mathsf{H}(a) = \ell$, the following relations hold.*

1. $\sum\limits_{x \in \mathsf{E}_{k,n}} (-1)^{a.x} = \mathsf{K}_k(\ell,n)$.

2. If $l_{a,b}(x) = a \cdot x + b$, *where* $a \in \mathbb{F}_2^n, b \in \mathbb{F}_2$, *be an affine Boolean function then*

$$\mathsf{w}_{k,n}(l_{a,b}) = \frac{1}{2}(|\mathsf{E}_{k,n}| - (-1)^b \mathsf{K}_k(\ell,n)).$$

Now we present some results on the sequences from Krawtchouk polynomial.

Lemma 2. *Let n be a positive integer and $k \in [0,n]$. Then*

1. $\mathsf{K}_k(1,n) \geq 0$ *if* $k \leq \lfloor \frac{n}{2} \rfloor$ *and* $\mathsf{K}_k(1,n) < 0$ *if* $k > \lfloor \frac{n}{2} \rfloor$.
In particular, $\mathsf{K}_k(1,n) = 0$ *if n is even and* $k = \frac{n}{2}$.

2. $\mathsf{K}_k(2,n) \geq 0$ *if and only if* $k \leq \frac{n}{2} - \frac{\sqrt{n}}{2}$ *or,* $k \geq \frac{n}{2} + \frac{\sqrt{n}}{2}$.
In particular, $\mathsf{K}_k(2,n) = 0$ *if n is an even square integer and* $k = \frac{n}{2} \pm \frac{\sqrt{n}}{2}$.

3. $\mathsf{K}_k(l+1,n) + \mathsf{K}_k(l,n) = 2\mathsf{K}_k(l,n-1)$ *and* $\mathsf{K}_k(l+1,n) - \mathsf{K}_k(l,n) = -2\mathsf{K}_{k-1}(l,n-1)$.

4. $\mathsf{K}_k(l,n) + \mathsf{K}_{k-1}(l,n) = \mathsf{K}_k(l,n+1)$ *and* $\mathsf{K}_k(l,n) - \mathsf{K}_{k-1}(l,n) = \mathsf{K}_k(l+1,n+1)$.

Proof. 1. The proof can be derived from the expression $\mathsf{K}_k(1,n) = \binom{n-1}{k} - \binom{n-1}{k-1}$.

2. $\mathsf{K}_k(2,n) = \binom{n-2}{k} - 2\binom{n-2}{k-1} + \binom{n-2}{k-2} = \frac{(n-2)!((2k-n)^2-n)}{k!(n-k)!}$.
Hence, $\mathsf{K}_k(2,n) \geq 0 \iff (2k-n)^2 - n \geq 0 \iff (2k-n)^2 \geq n \iff 2k - n \geq \sqrt{n}$ or, $2k - n \leq -\sqrt{n} \iff k \geq \frac{n}{2} + \frac{\sqrt{n}}{2}$ or, $k \leq \frac{n}{2} - \frac{\sqrt{n}}{2}$. The particular case follows similarly.

3. We have,

$$\begin{aligned}
\mathsf{K}_k(l+1,n)+\mathsf{K}_k(l,n) &= \sum_{j=0}^{k}(-1)^j\binom{l+1}{j}\binom{n-l-1}{k-j}+\sum_{j=0}^{k}(-1)^j\binom{l}{j}\binom{n-l}{k-j}\\
&= \sum_{j=0}^{k}(-1)^j\left[\binom{l+1}{j}\binom{n-l-1}{k-j}+\binom{l}{j}\binom{n-l}{k-j}\right]\\
&= \sum_{j=0}^{k}(-1)^j\left[\binom{l+1}{j}\binom{n-l-1}{k-j}+\binom{l}{j}\left(\binom{n-l-1}{k-j}+\binom{n-l-1}{k-j-1}\right)\right]\\
&= \sum_{j=0}^{k}(-1)^j\left[\left(\binom{l+1}{j}+\binom{l}{j}\right)\binom{n-l-1}{k-j}+\binom{l}{j}\binom{n-l-1}{k-j-1}\right]\\
&= \sum_{j=0}^{k}(-1)^j\left[\left(\binom{l+1}{j}+\binom{l}{j}\right)\binom{n-l-1}{k-j}\right]+\sum_{j=1}^{k+1}(-1)^{j-1}\binom{l}{j-1}\binom{n-l-1}{k-j}\\
&= \sum_{j=0}^{k}(-1)^j\left[\left(\binom{l+1}{j}+\binom{l}{j}\right)\binom{n-l-1}{k-j}\right]+\sum_{j=0}^{k}(-1)^{j-1}\binom{l}{j-1}\binom{n-l-1}{k-j}\\
&= \sum_{j=0}^{k}(-1)^j\left(\binom{l+1}{j}+\binom{l}{j}-\binom{l}{j-1}\right)\binom{n-l-1}{k-j}\\
&= 2\sum_{j=0}^{k}(-1)^j\binom{l}{j}\binom{n-l-1}{k-j}=2\mathsf{K}_k(l,n-1).
\end{aligned}$$

The second part of this item can be proven using a similar technique as above.

4. These equalities can be proved by adding and subtracting the equalities in Item 3 respectively.

□

We present the minimum of the sequence $\mathsf{K}_k(l,n), 0\le l\le n$ for a fixed k and n in the following theorem.

Theorem 1. *1. Let $n=2m+1$ be an odd integer for some $m\in\mathbb{Z}^+$. Then for $k\in[0,n]$*

$$\min_{0\le l\le n-1}\mathsf{K}_k(l,n)=\begin{cases}\mathsf{K}_k(n-1,n)=-\mathsf{K}_k(1,n) & \textit{for } k\in[0,\frac{n-1}{2}] \textit{ and odd},\\ \mathsf{K}_k(1,n) & \textit{for } k\in[\frac{n+1}{2},n].\end{cases}$$

In particular (when $k=m$), $\min\limits_{0\le l\le n-1}\mathsf{K}_m(l,n)=\mathsf{K}_m(2,n)=-\mathsf{K}_m(1,n)$.

2. Let $n=2m$ be an even integer for some $m\in\mathbb{Z}^+$.
Then for $k\in[m+1,n]$ and even, $\min\limits_{0\le l\le n}\mathsf{K}_k(l,n)=\mathsf{K}_k(1,n)$.
Moreover,
(a) $\min\limits_{0\le l\le n}\mathsf{K}_m(l,n)=\mathsf{K}_m(2,n)$ if m is even,
(b) for $n\ge 10$, $\min\limits_{0\le l\le n}\mathsf{K}_{m-1}(l,n)=\mathsf{K}_{m-1}(2,n)$ if m is odd.

3. $\min\limits_{0\le l\le n}\mathsf{K}_2(l,n)=-\lfloor\frac{n}{2}\rfloor$.

4. $\max\limits_{0\le l\le n}\mathsf{K}_k(l,n)=\mathsf{K}_k(0,n)=\binom{n}{k}$.

5. $\mathsf{K}_k(n,n)=\begin{cases}\max\limits_{0\le l\le n}\mathsf{K}_k(l,n) & \textit{if } k \textit{ is even},\\ \min\limits_{0\le l\le n}\mathsf{K}_k(l,n) & \textit{if } k \textit{ is odd}.\end{cases}$

Proof. 1. From Proposition 2[Item 4], for $k \in [0, n]$, we have $|\mathsf{K}_k(1,n)| \geq |\mathsf{K}_k(l,n)|$ for all $l \in [1, n-1]$. For $k \in [\frac{n+1}{2}, n]$, $\mathsf{K}_k(1,n) < 0$ (from Lemma 2[Item 1]), we have $\min_{1 \leq l \leq n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$.

   Furthermore, k being an odd integer in $[0, \frac{n-1}{2}]$, using Proposition 2[Item 3], we have $\mathsf{K}_k(1,n) = -\mathsf{K}_k(n-1,n)$. Hence, for $k \in [0, \frac{n-1}{2}]$, since $\mathsf{K}_k(1,n) \geq 0$ (from Lemma 2[Item 1]), we get $\max_{1 \leq l \leq n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$ i.e., $\min_{1 \leq l \leq n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(n-1,n)$.

   Since $\mathsf{K}_k(0,n) = \binom{n}{k} > 0$, we have $\min_{0 \leq l \leq n-1} \mathsf{K}_k(l,n) = \min_{1 \leq l \leq n-1} \mathsf{K}_k(l,n)$ and it proves the result of the first part of the item.

   Since $n = 2m+1$, we have from Lemma 2[Item 3 and Item 1] that $\mathsf{K}_m(2,n) + \mathsf{K}_m(1,n) = 2\mathsf{K}_m(1,n-1) = 0$. It implies $\mathsf{K}_m(2,n) = -\mathsf{K}_m(1,n) \leq 0$.

   Since $\mathsf{K}_m(0,n) = \binom{n}{m} > 0$, we obtain $\min_{0 \leq l \leq n} \mathsf{K}_m(l,n) = \min_{1 \leq l \leq n-1} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n)$ (from Proposition 2[Item 4]). Accordingly, the second part of this item is proven.

2. Since $k \geq m+1$, from Proposition 2[Item 5], we have $|\mathsf{K}_k(1,n)| \geq |\mathsf{K}_k(l,n)|$ for $l \in [1, n-1]$. As $\mathsf{K}_k(1,n) \leq 0$ (from Lemma 2[Item 1]) and $\mathsf{K}_k(0,n) = \mathsf{K}_k(n,n) = \binom{n}{k} > 0$, $\min_{0 \leq l \leq n} \mathsf{K}_k(l,n) = \min_{1 \leq l \leq n-1} \mathsf{K}_k(l,n) = \mathsf{K}_k(1,n)$. Hence, the first part is proven.

   Additionally, from Lemma 2[Item 2]), we have $\mathsf{K}_m(2,n) \leq 0$ since $m = \frac{n}{2}$.

   (a) Here we consider the case $m = \frac{n}{2}$ even. We show $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l,n)|$ for $1 \leq l \leq n-1$. At first, we use induction on l to show it for l even and $2 \leq l \leq \frac{n}{2}$.

   For $l = 2$, it is direct since $|\mathsf{K}_m(2,n)| = |\mathsf{K}_m(l,n)|$.

   Then, assume that $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l,n)|$ for some even l and $2 \leq l \leq \frac{n}{2} - 2$. Then, we need to prove that $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l+2,n)|$. From Proposition 2[Item 6], for $2 \leq l \leq \frac{n-4}{2} = \frac{n}{2} - 2$, we have:

$$\begin{aligned}
(n-(l+1))\mathsf{K}_m(l+2,n) &= (n-2m)\mathsf{K}_m(l+1,n) - (l+1)\mathsf{K}_m(l,n) \\
&= -(l+1)\mathsf{K}_m(l,n), \text{ since } n = 2m \\
\implies |(n-l-1)\mathsf{K}_m(l+2,n)| &= |-(l+1)\mathsf{K}_m(l,n)| \\
\implies |\mathsf{K}_m(l+2,n)| &= \frac{l+1}{n-l-1}|\mathsf{K}_m(l,n)| \leq |\mathsf{K}_m(l,n)| \leq |\mathsf{K}_m(2,n)| \text{ since } \frac{l+1}{n-l-1} \leq 1.
\end{aligned}$$

   Therefore, $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l,n)|$ for all $2 \leq l \leq \frac{n}{2}$ and even. From Proposition 2[Item 2], $\mathsf{K}_m(l,n) = 0$ for l odd. Hence, $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l,n)|$ for all $1 \leq l \leq \frac{n}{2}$. Further, from Proposition 2[Item 3], $\mathsf{K}_m(l,n) = \mathsf{K}_m(n-l,n)$ as m even. Hence, $|\mathsf{K}_m(2,n)| \geq |\mathsf{K}_m(l,n)|$ for all $1 \leq l \leq n-1$. Therefore, as $\mathsf{K}_m(2,n) < 0$ and $\mathsf{K}_m(0,n) = \mathsf{K}_m(n,n) = \binom{n}{m} > 0$, $\min_{0 \leq l \leq n} \mathsf{K}_m(l,n) = \min_{1 \leq l \leq n-1} \mathsf{K}_m(l,n) = \mathsf{K}_m(2,n)$ for m even.

   (b) Now we focus on the case $m = \frac{n}{2}$ odd. At first, we show that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$ using induction on l.

   For $l = 2$, we have $|\mathsf{K}_{m-1}(2,n)| = |\mathsf{K}_{m-1}(l,n)|$.

   Then, we prove the property for $l = 3$ i.e. $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$. This is needed since (as we will see later) the induction has a recursion with depth two. It can be checked from Lemma 2[Item 2] that $\mathsf{K}_{m-1}(2,n) \leq 0$ for $n \geq 4$. To prove $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$, we need to show that $\mathsf{K}_{m-1}(2,n) \leq \mathsf{K}_{m-1}(3,n) \leq -\mathsf{K}_{m-1}(2,n)$ i.e., $\mathsf{K}_{m-1}(3,n) - \mathsf{K}_{m-1}(2,n) \geq 0$ and $\mathsf{K}_{m-1}(3,n) + \mathsf{K}_{m-1}(2,n) \leq 0$.

   From Lemma 2[Item 3 and Item 1], we have $\mathsf{K}_{m-1}(3,n) + \mathsf{K}_{m-1}(2,n) = 2\mathsf{K}_{m-1}(2,n-1) = 2\left(2\mathsf{K}_{m-1}(1,n-2) - \mathsf{K}_{m-1}(1,n-1)\right) = -2\mathsf{K}_{m-1}(1,n-1) \leq 0$.

   Similarly, $\mathsf{K}_{m-1}(3,n) - \mathsf{K}_{m-1}(2,n) = -2\mathsf{K}_{m-2}(2,n-1) \geq 0$ if $m-2 \geq \frac{n-1-\sqrt{n-1}}{2}$ *i.e.*, if $n \geq 10$ (Lemma 2[Item 2]). Hence, $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(3,n)|$ if $n \geq 10$.

   Assume that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l-1,n)|$ and $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for some $3 \leq l \leq \frac{n}{2} - 1$. Then, we need to prove that $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l+1,n)|$.

Using Proposition 2[Item 6], we have

$$\begin{aligned}(n-l)\mathsf{K}_{m-1}(l+1,n) &= (n-2(m-1))\mathsf{K}_{m-1}(l,n) - l\mathsf{K}_{m-1}(l-1,n)\\ &= 2\mathsf{K}_{m-1}(l,n) - l\mathsf{K}_{m-1}(l-1,n)\\ \implies (n-l)|\mathsf{K}_{m-1}(l+1,n)| &\leq 2|\mathsf{K}_{m-1}(l,n)| + l|\mathsf{K}_{m-1}(l-1,n)| \leq (2+l)|\mathsf{K}_{m-1}(2,n)|\\ \implies |\mathsf{K}_{m-1}(l+1,n)| &\leq \frac{l+2}{n-l}|\mathsf{K}_{m-1}(2,n)|\\ \implies |\mathsf{K}_{m-1}(l+1,n)| &\leq |\mathsf{K}_{m-1}(2,n)| \qquad \text{as } \frac{l+2}{n-l} \leq 1 \text{ for } 2 \leq l \leq \frac{n}{2}-1.\end{aligned}$$

Hence, $|\mathsf{K}_{m-1}(2,n)| \geq |\mathsf{K}_{m-1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$.
Then, $|\mathsf{K}_{m+1}(2,n)| \geq |\mathsf{K}_{m+1}(l,n)|$ for $2 \leq l \leq \frac{n}{2}$ since $|\mathsf{K}_{m+1}(l,n)| = |\mathsf{K}_{m-1}(l,n)|$ (from Proposition 2[Item 2]).
Now, we show that $\min\limits_{0\leq l\leq n} \mathsf{K}_{m+1}(l,n) = \mathsf{K}_{m+1}(1,n)$. From Lemma 2[Item 3 and Item 1], we have $\mathsf{K}_{m+1}(2,n) - \mathsf{K}_{m+1}(1,n) = -2\mathsf{K}_m(1,n-1) > 0$. Similarly, $\mathsf{K}_{m+1}(2,n) + \mathsf{K}_{m+1}(1,n) = 2\mathsf{K}_{m+1}(1,n-1) \leq 0$. That implies $-\mathsf{K}_{m+1}(1,n) \leq \mathsf{K}_{m+1}(2,n) < \mathsf{K}_{m+1}(1,n)$ *i.e.*, $|\mathsf{K}_{m+1}(2,n)| \leq |\mathsf{K}_{m+1}(1,n)|$.
From Lemma 2[Item 1], we have $\mathsf{K}_{m+1}(1,n) \leq 0$. Accordingly, $\min\limits_{0\leq l\leq n} \mathsf{K}_{m+1}(l,n) = \mathsf{K}_{m+1}(1,n)$.

3. We have:

$$\mathsf{K}_k(l,n) = \sum_{j=0}^{k}(-1)^j\binom{l}{j}\binom{n-l}{k-j} = \sum_{j=0}^{k}\binom{l}{j}\binom{n-l}{k-j} - 2\sum_{\substack{j=0\\ j \text{ odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j} = \binom{n}{k} - 2\sum_{\substack{j=0\\ j \text{ odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j}. \quad (3)$$

Hence, $\mathsf{K}_2(l,n) = \binom{n}{2} - 2\binom{l}{1}\binom{n-l}{1} = \binom{n}{2} - 2l(n-l)$. For real value of l, the function $\mathsf{K}_2(l,n)$ has minima at $l = \frac{n}{2}$ as $\frac{d(\mathsf{K}_2(l,n))}{dl} = 4l - 2n = 0$ at $l = \frac{n}{2}$ and $\frac{d^2(\mathsf{K}_2(l,n))}{dl^2} = 4 > 0$. Since ℓ in a positive integer, we have $\min\limits_{0\leq l\leq n} \mathsf{K}_2(l,n)$ is $\binom{n}{2} - 2(\frac{n}{2})^2 = -\frac{n}{2}$ when n is even. For n is odd, it can be checked that $\mathsf{K}_2(l,n)$ has minimum at $l = \frac{n-1}{2}$ and $l = \frac{n+1}{2}$ with value $\min\limits_{0\leq l\leq n} \mathsf{K}_2(l,n) = \binom{n}{2} - 2\frac{n-1}{2}\frac{n+1}{2} = -\frac{n-1}{2}$. Hence, combining both the cases, we have $\min\limits_{0\leq l\leq n} \mathsf{K}_2(l,n) = -\lfloor\frac{n}{2}\rfloor$.

4. From Equation 3, we have $\mathsf{K}_k(l,n) = \binom{n}{k} - 2\sum\limits_{\substack{j=0\\ j:\text{odd}}}^{k}\binom{l}{j}\binom{n-l}{k-j} \leq \binom{n}{k} = \mathsf{K}_k(0,n)$. It finishes the demonstration of the item.

5. From Proposition 2[Item 3], we have $\mathsf{K}_k(n,n) = (-1)^k\mathsf{K}_k(0,n)$. Hence, for k is even, $\mathsf{K}_k(n,n) = \mathsf{K}_k(0,n)$ is maximum in $\mathsf{K}_k(l,n), l \in [0,n]$. Like Equation 3, we have $\mathsf{K}_k(l,n) = 2\sum\limits_{\substack{j=0\\ j:\text{even}}}^{k}\binom{l}{j}\binom{n-l}{k-j} - \binom{n}{k} \geq -\binom{n}{k} = -\mathsf{K}_k(0,n)$. Hence, for odd k, we have $\mathsf{K}_k(n,n) = -\mathsf{K}_k(0,n) \leq \mathsf{K}_k(l,n)$ for $l \in [0,n]$.

□

3 Construction of WAPB Boolean functions using Group action

In this section we present a construction of 2-πS WAPB Boolean functions using the group action of a cyclic permutation group $P = \langle\pi\rangle$. Let $P = \langle\pi\rangle$ be a cyclic subgroup of the symmetric group $\mathbb{S}_n$ on n elements. Let the group action of P on $\mathbb{F}_2^n$ partitions the set into g_n number of orbits. The orbit generated by $x \in \mathbb{F}_2^n$ is denoted as $O_\pi(x) = \{\pi^i(x) : 0 \leq i < o(\pi)\}$. Since $\mathsf{w_H}(\pi^i(x)) = \mathsf{w_H}(x)$ for $0 \leq i < o(\pi)$, the group action P splits each $\mathsf{E}_{k,n}$ into orbits and let $g_{k,n}$ be the number of orbits in $\mathsf{E}_{k,n}$. Denote $\nu_{k,n,i}$ be the orbit representative of i-th orbit in $\mathsf{E}_{k,n}$ with some ordering. A construction of 2-πS WAPB Boolean functions is presented in Construction 1.

Construction 1 ensures a balanced WAPB Boolean function. The binary variable t indicates whether the partially constructed is balanced (when $t = 0$) or having an extra 1 (when $t = 1$) during each iteration of orbits.

Construction 1 Construction of a 2-πS WAPB Boolean function

```
Input: $\pi \in \mathbb{S}_n$
Output: A 2-$\pi$S WAPB Boolean function $f_\pi \in \mathcal{B}_n$
  Initiate $\mathsf{supp}(f_\pi) = \emptyset$
  $t = 0$
  for $k \leftarrow 0$ to $n$ do
      for $i \leftarrow 1$ to $g_{k,n}$ do
          $u = \nu_{k,n,i}$; $l = |O_\pi(u)|$
          if $l$ is even then
              for $j \leftarrow 1$ to $\frac{l}{2}$ do
                  $\mathsf{supp}(f_\pi)$.append($u$)
                  $u \leftarrow \pi \circ \pi(u)$
              end for
          else
              $u = \pi^t(u)$
              for $j \leftarrow 1$ to $\lceil \frac{l-t}{2} \rceil$ do
                  $\mathsf{supp}(f_\pi)$.append($u$)
                  $u \leftarrow \pi \circ \pi(u)$
              end for
              Update $t \leftarrow 1 - t$
          end if
      end for
  end for
  return $f_\pi$
```

Example 1. Consider $n = 5$ and the permutation $\pi = \sigma$ is the rotation permutation. Then considering the orbits with representatives $00000, 00001, 00011, 00101, 00111, 01011, 01111, 11111$, we have the resultant function $f_\sigma \in \mathcal{B}_5$ of Construction 1 as $\mathsf{supp}(f_\sigma) = \{00000, 00010, 01000, 00011, 01100, 10001, 01010, 01001, 00111, 11100, 10011, 10110, 11010, 01111, 11101, 10111\}$. Hence, f_σ is a 2-RotS (*i.e.*, 2-σS) WAPB Boolean function.

Given a permutation $\pi \in \mathbb{S}_n$, let denote $\mathcal{O}_e$ and $\mathcal{O}_o$ be the set of orbits of even cardinality and odd cardinality of the group action $P = \langle \pi \rangle$ on $\mathbb{F}_2^n$ respectively. Further, let denote $\mathcal{O}_k$ be the set of orbits of cardinality k for $k \in [0, n]$. Here, $\mathcal{O}_1$ is the set of orbits of cardinality 1. Since every orbit in $\mathcal{O}_1$ contains exactly one element, abusing the notation, we also denote $\mathcal{O}_1 = \{x \in \mathbb{F}_2^n \,|\, x = \pi(x)\}$(i.e., the set of vectors in $\mathbb{F}_2^n$ of orbit length 1).

Theorem 2. *For $\pi \in \mathbb{S}_n$ where $n \in \mathbb{Z}^+$, let $\mathcal{O}_1 = \{x \in \mathbb{F}_2^n : \pi(x) = x\}$. Then, for $c \in \mathbb{F}_2^n$ and $k \in [0, n]$,*

1. $|\{x \in \mathbb{F}_2^n \setminus \mathcal{O}_1 : c \cdot (x + \pi(x)) = 1\}| = \begin{cases} 2^{n-1} & \textit{if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_1 \\ 0 & \textit{if } c \in \mathcal{O}_1. \end{cases}$
2. $|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_1 : c \cdot (x + \pi(x)) = 1\}| = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n))$, *where* $l = \mathsf{w_H}(c + \pi^{-1}(c))$.

Proof. Now for any $x = (x_1, x_2, \ldots, x_n), c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$,

$$c \cdot (x + \pi(x)) = c \cdot x + c \cdot \pi(x) = c \cdot x + \pi^{-1}(c) \cdot x = (c + \pi^{-1}(c)) \cdot x. \tag{4}$$

Therefore, $c \cdot (x + \pi(x))$ is a linear Boolean function on n variables. Then $c \cdot (x + \pi(x))$ is the zero Boolean function if and only if $c = \pi^{-1}(c)$ i.e., $c \in \mathcal{O}_1$. Hence,

$$|\{x \in \mathbb{F}_2^n : c \cdot (x + \pi(x)) = 1\}| = \mathsf{w_H}(c \cdot (x + \pi(x))) = \begin{cases} 2^{n-1} \text{ if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_1 \\ 0 \qquad \text{if } c \in \mathcal{O}_1. \end{cases} \tag{5}$$

Further, if $x \in \mathcal{O}_1$, then $\pi(x) = x$ and that implies $c \cdot (x + \pi(x)) = 0$. Hence,

$$\begin{aligned} &|\{x \in \mathcal{O}_1 : c \cdot (x + \pi(x)) = 0\}| = |\mathcal{O}_1| \\ \Longrightarrow\ &|\{x \in \mathcal{O}_1 : c \cdot (x + \pi(x)) = 1\}| = 0. \end{aligned} \tag{6}$$

Now, combining Equation 5 and Equation 6 we have the desired result of Item 1

$$|\{x \in \mathbb{F}_2^n \setminus \mathcal{O}_1 : c \cdot (x + \pi(x)) = 1\}| = \begin{cases} 2^{n-1} & \text{if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_1 \\ 0 & \text{if } c \in \mathcal{O}_1. \end{cases}$$

Moreover, as $c \cdot (x + \pi(x)) = (c + \pi^{-1}(c)) \cdot x$ is linear in $\mathsf{E}_{k,n}$, using Proposition 3, we have

$$|\{x \in \mathsf{E}_{k,n} : c \cdot (x + \pi(x)) = 1\}| = \mathsf{w}_{k,n}((c + \pi^{-1}(c)) \cdot x) = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n))$$

where $l = \mathsf{w_H}(c + \pi^{-1}(c))$. If $x \in \mathcal{O}_1$ then $c \cdot (x + \pi(x)) = 0$.
Hence, $|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_1 : c \cdot (x + \pi(x)) = 1\}| = \dfrac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l, n))$. □

Theorem 3. *Let n be a positive integer and $\pi \in \mathbb{S}_n$. Then $\mathsf{NL}(f_\pi) \geq 2^{n-2} - \dfrac{|\mathcal{O}_o|}{2}$.*

Proof. Here $\mathcal{O}_e, \mathcal{O}_o$ and $\mathcal{O}_1$ are the set of orbits of even cardinalty, odd cardinality and single elements of the group action $G = \langle \pi \rangle$ on $\mathbb{F}_2^n$ respectively. Then the Walsh spectrum of f_π at $a \in \mathbb{F}_2^n$ is as follows.

$$W_{f_\pi}(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f_\pi(x) + a\cdot x} = \sum_{\mathsf{O} \in \mathcal{O}} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} = \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_o} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} \tag{7}$$

$$\begin{aligned} \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} &= \frac{1}{2}\left[\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(\pi(x)) + a\cdot \pi(x)}\right] \\ &= \frac{1}{2}\left[\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} + (-1)^{f_\pi(\pi(x)) + a\cdot \pi(x)}\right] \\ &= \frac{1}{2}\left[\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x)} \Big((-1)^{a\cdot x} - (-1)^{a\cdot \pi(x)}\Big)\right] \qquad (\text{as } f_\pi(\pi(x)) = 1 + f_\pi(x)). \end{aligned}$$

There are some vectors x in even orbits such that $((-1)^{a\cdot x} - (-1)^{a\cdot\pi(x)}) = 0$ i.e., $a \cdot (x + \pi(x)) = 0$. As these vectors contributes 0 to the sum, we now remove them in the equation. Hence, we have

$$\begin{aligned} \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} &= \frac{1}{2}\left[\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O} : a\cdot(x+\pi(x))=1} (-1)^{f_\pi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\pi(x)})\right] \\ &= \frac{1}{2}\left[\sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O} : a\cdot(x+\pi(x))=1} 2 \times (-1)^{f_\pi(x) + a\cdot x}\right] = \sum_{\mathsf{O} \in \mathcal{O}_e} \sum_{x \in \mathsf{O} : a\cdot(x+\pi(x))=1} (-1)^{f_\pi(x) + a\cdot x} \end{aligned} \tag{8}$$

$$\begin{aligned} \text{Similarly, } \sum_{\mathsf{O} \in \mathcal{O}_o} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} &= \sum_{\mathsf{O} \in \mathcal{O}_o \setminus \mathcal{O}_1} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_1} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x) + a\cdot x} \\ &= \sum_{\mathsf{O} \in \mathcal{O}_o \setminus \mathcal{O}_1} \sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_\mathsf{O})) + a\cdot\pi^i(\nu_\mathsf{O})} + \sum_{\mathsf{O} \in \mathcal{O}_1} (-1)^{f_\pi(\nu_\mathsf{O}) + a\cdot\nu_\mathsf{O}} \end{aligned} \tag{9}$$

where ν_{O} is the orbit representative of the orbit O. Then, for an orbit $\mathsf{O} \in \mathcal{O}_o \setminus \mathcal{O}_1$, if $f(\pi^{|\mathsf{O}|-1}(\nu_{\mathsf{O}})) = 1 + f(\pi^{|\mathsf{O}|-2}(\nu_{\mathsf{O}})) = f(\nu_{\mathsf{O}})$, we have

$$\begin{aligned}
\sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})} &= \frac{1}{2}\left(\sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})} + \sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})}\right) \\
&= \frac{1}{2}\left(\sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})} + \sum_{i=1}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})}\right) + \frac{(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}}{2} \\
&= \frac{1}{2}\left(\sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})} + \sum_{i=1}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))+a\cdot\pi^i(\nu_{\mathsf{O}})} + (-1)^{1+f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}\right) \\
&\qquad + \frac{(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}} - (-1)^{1+f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}}{2} \\
&= \frac{1}{2}\left(\sum_{i=0}^{|O|-1} (-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))}\left((-1)^{a\cdot\pi^i(\nu_{\mathsf{O}})} - (-1)^{a\cdot\pi^{i+1}(\nu_{\mathsf{O}})}\right)\right) + (-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}. \qquad (10)
\end{aligned}$$

If $f(\pi^{|\mathsf{O}|-1}(\nu_{\mathsf{O}})) = f(\pi^{|\mathsf{O}|-2}(\nu_{\mathsf{O}})) = 1 + f(\nu_{\mathsf{O}})$, consider $\hat{\nu_{\mathsf{O}}} = \pi^{-1}(\nu_{\mathsf{O}})$ as the representative element. We have now the earlier situation with the representative element $\hat{\nu_{\mathsf{O}}}$ i.e., $f(\pi^{|\mathsf{O}|-1}(\hat{\nu_{\mathsf{O}}})) = 1 + f(\pi^{|\mathsf{O}|-2}(\hat{\nu_{\mathsf{O}}})) = f(\hat{\nu_{\mathsf{O}}})$. Hence we will have Equation 10 for the representative element $\hat{\nu_{\mathsf{O}}}$. Hence, Equation 9 becomes

$$\begin{aligned}
\sum_{\mathsf{O}\in\mathcal{O}_o}\sum_{x\in\mathsf{O}}(-1)^{f_\pi(x)+a\cdot x} &= \frac{1}{2}\sum_{\mathsf{O}\in\mathcal{O}_o\setminus\mathcal{O}_1}\left(\sum_{i=0}^{|O|-1}(-1)^{f_\pi(\pi^i(\nu_{\mathsf{O}}))}\left((-1)^{a\cdot\pi^i(\nu_{\mathsf{O}})} - (-1)^{a\cdot\pi^{i+1}(\nu_{\mathsf{O}})}\right)\right) + \sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}} \\
&= \frac{1}{2}\sum_{\mathsf{O}\in\mathcal{O}_o\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}}(-1)^{f_\pi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\pi(x)}\right) + \sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}} \\
&= \frac{1}{2}\sum_{\mathsf{O}\in\mathcal{O}_o\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}:a(x+\pi(x))=1} 2\times(-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}} \\
&= \sum_{\mathsf{O}\in\mathcal{O}_o\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}:a(x+\pi(x))=1}(-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}. \qquad (11)
\end{aligned}$$

Now substituting the values in Equation 8 and Equation 11 in Equation 7, we have:

$$\begin{aligned}
W_{f_\pi}(a) &= \sum_{\mathsf{O}\in\mathcal{O}\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}:a(x+\pi(x))=1}(-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}} \\
\implies |W_{f_\pi}(a)| &\leq |\sum_{\mathsf{O}\in\mathcal{O}\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}:a(x+\pi(x))=1}(-1)^{f_\pi(x)+a\cdot x}| + |\sum_{\mathsf{O}\in\mathcal{O}_o}(-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot\nu_{\mathsf{O}}}| \\
&\leq |\sum_{\mathsf{O}\in\mathcal{O}\setminus\mathcal{O}_1}\sum_{x\in\mathsf{O}:a(x+\pi(x))=1}(-1)^{f_\pi(x)+a\cdot x}| + |\mathcal{O}_o| \\
\implies |W_{f_\pi}(a)| &\leq \begin{cases} 2^{n-1} + |\mathcal{O}_o| & \text{if } a \in \mathbb{F}_2^n \setminus \mathcal{O}_1 \\ |\mathcal{O}_o| & \text{if } a \in \mathcal{O}_1. \end{cases} \qquad \text{(from Theorem 2).}
\end{aligned}$$

Hence, the nonlinearity of f_π satisfies

$$\mathsf{NL}(f_\pi) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}|W_{f_\pi}(a)| \;\geq\; 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\{2^{n-1} + |\mathcal{O}_o|, |\mathcal{O}_o|\} \;=\; 2^{n-1} - 2^{n-2} - \frac{|\mathcal{O}_o|}{2}$$

$$\implies \mathsf{NL}(f_\pi) \geq 2^{n-2} - \frac{|\mathcal{O}_o|}{2}.$$

□

For a permutation $\pi \in \mathbb{S}_n$, we denote $\mathcal{O}_{e,k}, \mathcal{O}_{o,k}$ and $\mathcal{O}_{1,k}$ by the sets of all orbits of cardinality even, odd and one of the group action $P = \langle \pi \rangle$ on $\mathsf{E}_{k,n}$, respectively.

Theorem 4. *Let $\pi \in \mathbb{S}_n$ for some $n \in \mathbb{Z}^+$. Then*

$$\mathsf{NL}_k(f_\pi) \geq \frac{1}{4}\left(\binom{n}{k} - 2|\mathcal{O}_{o,k}| + \min_{\substack{2 \leq l \leq n \\ l \ even}} \mathsf{K}_k(l,n)\right).$$

Proof. The restricted Walsh spectrum of f_π at $a \in \mathbb{F}_2^n$ is

$$\mathcal{W}_{f_\pi,k}(a) = \sum_{x \in \mathsf{E}_{k,n}} (-1)^{f_\pi(x)+a\cdot x} = \sum_{\mathsf{O} \in \mathcal{O}_{e,k}} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_{o,k}} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x)+a\cdot x}. \tag{12}$$

Following a similar process as in the proof of Theorem 3, we have

$$\sum_{\mathsf{O} \in \mathcal{O}_{e,k}} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x)+a\cdot x} = \sum_{\mathsf{O} \in \mathcal{O}_{e,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x} \tag{13}$$

and

$$\sum_{\mathsf{O} \in \mathcal{O}_{o,k}} \sum_{x \in \mathsf{O}} (-1)^{f_\pi(x)+a\cdot x} = \sum_{\mathsf{O} \in \mathcal{O}_{o,k} \setminus \mathcal{O}_{1,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_{o,k}} (-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot \nu_{\mathsf{O}}}, \tag{14}$$

where ν_{O} is the orbit representative of the orbit O. Hence, substituting the values in Equation 13 and Equation 14 in Equation 12, we have

$$\begin{aligned}
\mathcal{W}_{f_\pi,k}(a) &= \sum_{\mathsf{O} \in \mathcal{O}_{e,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_{o,k} \setminus \mathcal{O}_{1,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_{o,k}} (-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot \nu_{\mathsf{O}}} \\
&= \sum_{\mathsf{O} \in \mathcal{O}_{k} \setminus \mathcal{O}_{1,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x} + \sum_{\mathsf{O} \in \mathcal{O}_{o,k}} (-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot \nu_{\mathsf{O}}} \\
\implies |\mathcal{W}_{f_\pi,k}(a)| &\leq |\sum_{\mathsf{O} \in \mathcal{O}_{k} \setminus \mathcal{O}_{1,k}} \sum_{\substack{x \in \mathsf{O} \\ a\cdot(x+\pi(x))=1}} (-1)^{f_\pi(x)+a\cdot x}| + |\sum_{\mathsf{O} \in \mathcal{O}_{o,k}} (-1)^{f_\pi(\nu_{\mathsf{O}})+a\cdot \nu_{\mathsf{O}}}| \\
&\leq \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) + |\mathcal{O}_{o,k}|,
\end{aligned}$$

where the last equation comes from Theorem 2.

Hence, the restricted nonlinearity of f_π satisfies

$$\begin{aligned}
\mathsf{NL}_k(f_\pi) = \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{2}\max_{a \in \mathbb{F}_2^n} |\mathcal{W}_{f_\pi,k}(a)| &\geq \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{4}\max_{a \in \mathbb{F}_2^n} (|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n) + 2|\mathcal{O}_{o,k}|) \\
\implies \mathsf{NL}_k(f_\pi) \geq \frac{1}{4}\left(|\mathsf{E}_{k,n}| - 2|\mathcal{O}_{o,k}| + \min_{a \in \mathbb{F}_2^n} \mathsf{K}_k(l,n)\right) &= \frac{1}{4}\left(\binom{n}{k} - 2|\mathcal{O}_{o,k}| + \min_{0 \leq l \leq n} \mathsf{K}_k(l,n)|\right).
\end{aligned}$$

Further, $l = \mathsf{w_H}(a + \pi^{-1}(a))$ is always even as $\mathsf{w_H}(a) = \mathsf{w_H}(\pi^{-1}(a))$. Hence, we have

$$\mathsf{NL}_k(f_\pi) \geq \frac{1}{4}\left(\binom{n}{k} - 2|\mathcal{O}_{o,k}| + \min_{\substack{0 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l,n)\right).$$

Using Theorem 1[Item 4], we have further,

$$\mathsf{NL}_k(f_\pi) \geq \frac{1}{4}\left(\binom{n}{k} - 2|\mathcal{O}_{o,k}| + \min_{\substack{2 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l,n)\right).$$

□

In the following sections we study 2-πS WAPB Boolean functions for two different permutations $\psi, \sigma \in \mathbb{S}_n$ for any positive integer n. Here, σ is the rotation permutation and ψ is the distinct binary-cycle permutation as defined in Section 4. Both functions generalize the Liu-Mesnager construction [LM19] of WPB Boolean functions on $n = 2^m$ variables.

4 Construction and Study of 2-ψS WAPB Boolean functions

In this section, we present a class of 2-ψS WAPB Boolean function which is a special case of the construction presented in Section 3. This construction extends the idea of Liu-Mesnager construction [LM19] to generate WAPB Boolean functions. As Liu-Mesnager construction outputs a WPB Boolean function, the form of n (the number of variable) needs to be a power of 2. However, in our case, the number of variables n can be any positive integer for generating WAPB Boolean functions.

Let n be a positive integer with binary representation as $n = n_1 + n_2 + \cdots + n_w$ as defined in Equation 1. We denote $\mathsf{w_H}(n) = w$ i.e., the number of 1's in the binary representation of n. For $x = (x_1, x_2, \ldots, x_n)$, we have

$$\psi(x) = (\sigma_{n_1}(x_1, \ldots, x_{n_1}), \sigma_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \sigma_{n_w}(x_{n-n_w+1}, \ldots, x_n)) \tag{15}$$

where σ_{n_i} is the rotation permutation on n_i elements. Here, $ord(\psi) = 2^{a_w} = n_w$. Hence, the cardinality of orbits obtained due the action of $P = \langle\psi\rangle$ on $\mathbb{F}_2^n$ are of power of 2 i.e., $|O_\psi(x)| = 2^l$ where $0 \leq l \leq a_w$ for $x \in \mathbb{F}_2^n$. Hence, there are some orbits of cardinality 1 and the remainings are of even cardinality.

Lemma 3. *Let n be a positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. Then there are 2^w orbits of cardinality 1 where $w = \mathsf{w_H}(n)$.*

Proof. For a vector $x \in \mathbb{F}_2^n$ is having an orbit of cardinality 1 i.e., $|O_\psi(x)| = 1$ if and only if the coordinates of x present in the cycles are of same value i.e.,

$$x_1 = x_2 = \ldots = x_{n_1}; \qquad x_{n_1+1} = x_{n_1+2} = \ldots = x_{n_1+n_2}; \qquad \cdots, \qquad x_{n-n_w+1} = x_{n-n_w+2} = \ldots = x_n. \tag{16}$$

As each partition of coordinates can be either 0 or 1, there are 2^w vectors x in $\mathbb{F}_2^n$ satisfying Equation 16 and hence $|O_\psi(x)| = 1$. □

Since every orbit contains the vectors of same weight, we denote the weight of an orbit is the weight of vectors in the orbit i.e., $\mathsf{w_H}(O_\psi(x)) = \mathsf{w_H}(x)$ for $x \in \mathbb{F}_2^n$. Further, for $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_2^n$, we say y covers x (i.e., $x \preceq y$), if $x_i \leq y_i$ for $1 \leq i \leq n$ i.e., $y_i = 1$ if $x_i = 1$ for $1 \leq i \leq n$. Similarly, given two positive integers n and k with binary representation $n = 2^{a_1} + 2^{a_2} + + \cdots + 2^{a_w}$ and $k = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_t}$, we denote $k \preceq n$ if $\{b_1, b_2, \ldots, b_t\} \subseteq \{a_1, a_2, \ldots, a_w\}$.

Lemma 4. *Let n be a positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. For $k \in [0, n]$, the number of orbits of weight k and cardinality 1 is 1 if $k \preceq n$, otherwise it is 0.*

Proof. Let $k = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_t}$ where $0 \leq b_1 < b_2 < \cdots < b_t$.
Case I: Let $k \preceq n$ i.e., $\{b_1, b_2, \ldots, b_t\} \subseteq \{a_1, a_2, \ldots, a_w\}$. Since the only way of writing k as sum of powers of 2 is $k = 2^{b_1} + 2^{b_2} + \cdots + 2^{b_t}$ and satisfying the condition in Equation 16, there is only one vector x with $\mathsf{w_H}(x) = k$ and $|O_\psi(x)| = 1$. In this case, the coordinates of x in the partitions of cardinality $2^{b_1}, 2^{b_2}, \ldots, 2^{b_t}$ are having value 1 and other coordinates have value 0.
Case II: Let $k \not\preceq n$, then $\{b_1, b_2, \ldots, b_t\} \not\subseteq \{a_1, a_2, \ldots, a_w\}$. Therefore, if $\mathsf{w_H}(x) = k$, the nonzero coordinates of x can not be partitioned of (distinct) sizes from the set $\{2^{a_1}, 2^{a_2}, \ldots, 2^{b_w}\}$. As a result, the coordinates of x will not satisfy the Equation 16. Hence, $|O_\psi(x)| > 1$. Hence, in this case there is no orbit of weight k and cardinality 1. □

We denote $\mathcal{O}_o$ be the set of orbits of odd cardinality (i.e., here 1) and $\mathcal{O}_e$ be the set of orbits of even cardinality. Since the cardinality of all orbits of carinality odd is 1, abusing the notation, we also denote $\mathcal{O}_o$ as the set of all vectors belonging in the orbits of odd cardinality. Hence from Equation 16, $\mathcal{O}_o = \{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n : x_1 = x_2 = \cdots = x_{n_1}; \quad x_{n_1+1} = x_{n_1+2} = \cdots = x_{n_1+n_2}; \quad \cdots; \; x_{(n-n_w)+1} = x_{(n-n_w)+2} = \cdots = x_n\}$. For example, if $n = 6$, there are there are $2^{\mathsf{w_H}(6)} = 2^2 = 4$ orbits of weight 1 and $\mathcal{O}_o = \{000000, 000011, 111100, 111111\}$.

By choosing such permutation ψ for Construction 1, we have every slice $\mathsf{E}_{k,n}$, $0 \leq k \leq n$, contains at most one orbit of odd cardinality (and i.e., 1). Therefore, it becomes easy to construct 2-ψS WAPB Boolean functions as other orbits are of even cardinality. Hence, we have the following result.

Theorem 5. *Let n be a positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. For a Boolean function $f_\psi \in \mathcal{B}_n$, if $f_\psi(\psi(x)) = 1 + f_\psi(x)$ holds for all $x \in \mathbb{F}_2^n \setminus \mathcal{O}_o$ where $\mathcal{O}_o$ is the set of vectors whose orbit cardinality is 1, then f_ψ is WAPB.*

Hence, when $n = 2^m$, a power of 2, $\psi = \sigma$ and Construction 1 on input $\psi \in \mathbb{S}_n$ results the 2-RotS WPB Boolean function by Liu and Mesnager [LM19]. A simplified version of Construction 1 is presented in Construction 4 for input ψ.

Construction 2 Construction of 2-ψS WAPB Boolean function using $\psi \in \mathbb{S}_n$

```
Input: $\psi \in \mathbb{S}_n$ as in Equation 2
Output: A 2-$\psi$S WAPB Boolean function $f_\psi \in \mathcal{B}_n$
  For every orbit $\mathsf{O}$ in $\mathbb{F}_2^n$ due to the action of $P = \langle \psi \rangle$, do the following:
  if $|\mathsf{O}|$ is even then
      $f$ satisfies $f_\psi(\psi(x)) = 1 + f(x)$ for $x \in \mathsf{O}$
  end if
  if $|\mathsf{O}| = 1$ then
      assign $f_\psi(x) = 0$ or 1.
  end if
  return $f_\psi$
```

Theorem 6. *The number of orbits generated due the action of ψ on $\mathbb{F}_2^n$ is*

$$g_n = \frac{1}{n_w} \sum_{k=1}^{n_w} 2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}.$$

Proof. As $ord(\psi) = 2^{a_w} = n_w$, let denote $G =< \psi >= \{\psi_n^1, \psi_n^2, \ldots, \psi_n^{n_w}\}$ where $\psi_n^1 = \psi$ and $\psi_n^i = \psi \circ \psi_n^{i-1}$ for $i \geq 2$. From the disjoint cycle form of ψ as in Equation 15, we have

$$\psi(x) = (\sigma_{n_1}(x_1, \ldots, x_{n_1}), \sigma_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \sigma_{n_w}(x_{n-n_w+1}, \ldots, x_n))$$

where σ_{n_i} is the rotation permutation on n_i elements. Hence, we denote, $\psi_n = (\sigma_{n_1}, \sigma_{n_2}, \ldots, \sigma_{n_w})$ and for positive integers k, we have $\psi_n^k = (\sigma_{n_1}^k, \sigma_{n_2}^k, \ldots, \sigma_{n_w}^k)$.

Now to apply Burnside's lemma, for every $k \in \{1, 2, \ldots, n_w\}$, we need to compute the number of fixed vectors $z \in \mathbb{F}_2^n$ by ψ_n^k i.e., $\psi_n^k(z) = z$. That is, for every $k \in \{1, 2, \ldots, n_w\}$, we need to compute the number of vectors $z \in \mathbb{F}_2^n$ such that $\rho_{n_1}^k(z_1) = z_1, \rho_{n_2}^k(z_2) = z_2, \ldots, \rho_{n_w}^k(z_w) = z_w$ where $z = (z_1, z_2, \ldots, z_w)$ and $z_1 \in \mathbb{F}_2^{n_1}, z_2 \in \mathbb{F}_2^{n_2}, \ldots, z_w \in \mathbb{F}_2^{n_w}$.

Here, the number of permutation cycles in $\sigma_{n_i}^k = \gcd(n_i, k)$ for $1 \leq i \leq w$ and $1 \leq k \leq n_w$. So, the length of each permutation cycle in $\sigma_{n_i}^k$ is $\frac{n_i}{\gcd(n_i,k)}$. Therefore, the total number of permutation cycles in ψ^k is

$$\gcd(n_1, k) + \gcd(n_2, k) + \cdots + \gcd(n_w, k).$$

As every permutation cycle fixes all 0's or all 1's, each permutation cycle has two choices. $\sigma_{n_i}^k$ fixes $2^{\gcd(n_i,k)}$ number of $z_i \in \mathbb{F}_2^{n_i}$. Therefore, ψ^k fixes $2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}$ number of $z \in \mathbb{F}_2^n$. Hence, by using the Burnside Lemma, the number of orbits is

$$g_n = \frac{1}{n_w}\sum_{\pi \in G} |fix_{\mathbb{F}_2^n}(\pi)| = \frac{1}{n_w}\sum_{k=1}^{n_w} 2^{\gcd(n_1,k)+\gcd(n_2,k)+\cdots+\gcd(n_w,k)}. \qquad \square$$

The representative of each orbit can be be assigned 0 or 1 and accordingly other vectors in the orbit are assigned. Hence, there are 2^{g_n} WAPB 2-ψS Boolean functions on n variables. Further, we can count the number of balanced WAPB 2-ψS Boolean functions on n variables. There are 2^w many orbits of cardinality 1 and remaining $g_n - 2^w$ orbits are having cardinality even. Further, 2^{w-1} orbits from the 2^w orbits of cardinality 1 are to be assigned 1 to make f_ψ balanced. Hence $\binom{2^w}{2^{w-1}} \times 2^{g_n - 2^w}$ balanced WAPB 2-ψS Boolean functions can be generated using Construction 4. Now we will study some cryptographic properties of the function $f_\psi \in \mathcal{B}_n$.

Theorem 7. *Let $\psi \in \mathbb{S}_n$ as in Equation 2 with $\mathsf{w_H}(n) = w$. Then $\mathsf{NL}(f_\psi) \geq 2^{n-2} - 2^{w-1}$.*

Proof. As $\mathsf{w_H}(n) = w$, from Lemma 3 there are 2^w orbits with cardinality 1 and remaining orbits are of even cardinality (i.e., $|\mathsf{O}_o| = |\mathsf{O}_1| = 2^w$). Then from Theorem 3, the nonlinearity bound of f_ψ is

$$\mathsf{NL}(f_\psi) \geq 2^{n-2} - \frac{|\mathsf{O}_o|}{2} = 2^{n-2} - 2^{w-1}.$$

$\square$

The following corollary presents a nonlinearity bound for the 2-ψS WPB Boolean function which resembles with the WPB Boolean function by Liu and Mesnager [LM19].

Corollary 1. *Let $n = 2^m$ be a positive integer. Then $\mathsf{NL}(f_\psi) \geq 2^{n-2} - 1$.*

In Table 4, we have presented the maximum and minimum nonlinearity among all f_ψ for the number of variables $n = \{4, 5, \ldots, 10\}$ along with the upperbound of balanced Boolean functions and lowerbound of f_ψ as per Theorem 7. We have searched all such balanced Boolean functions for $n \leq 6$ and from $70 \times 2^{20}, 2 \times 2^{25}, 6 \times 2^{23}, 6 \times 2^{23}$ randomly chosen such Boolean functions for $n = 7, 8, 9, 10$ respectively.

n	4	5	6	7	8	9	10
Number of functions	$2^4 \times \binom{2}{1}$ $= 2^5$	$2^8 \times \binom{4}{2}$ $= 6 \times 2^9$	$2^{18} \times \binom{4}{2}$ $= 6 \times 2^{19}$	$2^{36} \times \binom{8}{4}$ $= 70 \times 2^{37}$	$2^{34} \times \binom{2}{1}$ $= 2^{35}$	$2^{68} \times \binom{4}{2}$ $= 6 \times 2^{69}$	$2^{138} \times \binom{4}{2}$ $= 6 \times 2^{139}$
Max nl by experiment	4	12	26	56	116	238	480
% functions at max nl	100	22.92	0.65	4.3×10^{-3}	4.6×10^{-3}	1.6×10^{-5}	2.4×10^{-3}
Nonlinearity upper bound of balanced functions [SZZ95]	4	12	28	58	118	244	494
Min Nonlinearity	4	6	14	28	64	144	328
% functions at min nl	100	4.17	0.26	2.3×10^{-4}	3.3×10^{-3}	3.2×10^{-5}	1.6×10^{-5}
Average nl by experiment	4.0	9.79	21.83	47.35	106.01	220.58	453.49
Nonlinearity lower bound by Theorem 7	3	6	14	28	63	144	254

Table 1. Percentage of $f_\psi \in \mathcal{B}_n$ satisfying lower bound and upper value of $\mathsf{NL}(f_\psi)$

Now we will study the weightwise nonlinearity of f_ψ.

Theorem 8. *Let $n \geq 2$ be a positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

$$\mathsf{NL}_k(f_\psi) \ \geq \ \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min\limits_{\substack{2\leq l\leq n\\ l \text{ even}}} \mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min\limits_{\substack{2\leq l\leq n\\ l \text{ even}}} \mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Proof. From Lemma 4, we have $|\mathcal{O}_{o,k}| = |\mathcal{O}_{1,k}| = 1$ if $k \preceq n$ else it is 0. Hence from Theorem 4, we have

$$\mathsf{NL}_k(f_\psi) \geq \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\leq l\leq n\\ l \text{ even}}} \mathsf{K}_k(l,n)\right) + \varepsilon,$$

where $\varepsilon = 0$ if $k \not\preceq n$ and -2 otherwise. □

We can discard the case $l = n$ from finding minimum in $\mathsf{K}_k(l,n)$ for some cases.

Corollary 2. *Let $n \geq 2$ be a positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. If k is even or n is odd then:*

$$\mathsf{NL}_k(f_\psi) \ \geq \ \frac{1}{4}\left(\binom{n}{k} + \min_{\substack{2\leq l\leq n-1\\ l \text{ even}}} \mathsf{K}_k(l,n)\right) + \varepsilon,$$

where $\varepsilon = 0$ if $k \not\preceq n$ and -2 otherwise. Otherwise (i.e., k is odd and n is even), $\mathsf{NL}_k(f_\psi) \geq 0$.

Proof. If n is odd then $\mathsf{K}_k(n,n)$ is not included in the minimum finding as l has to be even. Further, from Theorem 1[Item 5], if k is even then $\max\limits_{0\leq l\leq n} \mathsf{K}_k(l,n) = \mathsf{K}_k(n,n)$. Hence we are done for the case k is even or n is odd.

If k is odd and n is even, then $\min\limits_{\substack{2\leq l\leq n\\ l \text{ even}}} \mathsf{K}_k(l,n) = \mathsf{K}_k(n,n) = -\binom{n}{k}$. Further, in this case $k \not\preceq n$. Hence, $\mathsf{NL}_k(f_\psi) \geq 0$, which is infact always true. □

Now, substituting the results of Theorem 1[Item 1 and Item 2] in Corollary 8, we have nonlinearity bounds for particular values of k.

Theorem 9. *1. If n is odd then*

$$\mathsf{NL}_k(f_\psi) \ \geq \ \begin{cases} \frac{1}{2}\binom{n-1}{k-1} & \text{if } k \in [0, \frac{n-1}{2}], \text{ odd and } k \not\preceq n \\ \frac{1}{2}\left(\binom{n-1}{k-1} - 1\right) & \text{if } k \in [0, \frac{n-1}{2}], \text{ odd and } k \preceq n \\ \frac{1}{2}\binom{n-1}{k} & \text{if } k \in [\frac{n+1}{2}, n] \text{ and } k \not\preceq n \\ \frac{1}{2}\left(\binom{n-1}{k} - 1\right) & \text{if } k \in [\frac{n+1}{2}, n] \text{ and } k \preceq n. \end{cases}$$

2. If n is even and $k \in [\frac{n}{2}+1, n]$ is even then

$$\mathsf{NL}_k(f_\psi) \ \geq \ \begin{cases} \frac{1}{2}\binom{n-1}{k} & \text{if } k \not\preceq n \\ \frac{1}{2}\left(\binom{n-1}{k} - 1\right) & \text{if } k \preceq n. \end{cases}$$

k	2	3	4	5	6	7	8	9	10
n	n-2	n-3	n-4	n-5	n-6	n-7	n-8	n-9	n-10
15	24	0	330	0	1215	0	-	-	-
	0	45	0	500	0	1506	-	-	-
16	28	0	443	0	1931	0	3003	-	-
	8	0	228	0	1502	0	-	-	-
17	32	0	580	0	3003	0	5720	-	-
	0	60	0	910	0	4004	0	-	-
18	36	0	750	0	4550	0	10725	0	-
	8	0	340	0	3094	0	9724	0	-
19	40	0	950	0	6650	0	18343	0	-
	0	76	0	1530	0	9282	0	21879	-
20	45	0	1190	0	9524	0	30719	0	43758
	10	0	484	0	5814	0	25194	0	43758

Table 2. Values of the lower bound of $\mathsf{NL}_k(f_\psi)$ as per Theorem 8

Since $\mathsf{E}_{\lfloor \frac{n}{2} \rfloor, n}$ is a largest slice among all slices $\mathsf{E}_{k,n}, k \in [0, n]$, studying the nonlinearity at this domain is useful for cryptographic purpose. The cipher FLIP also uses the domain $\mathsf{E}_{\frac{n}{2},n}$ for its design. We have the nonlinearity bounds for the largest slice (*i.e.*, $k = \lfloor \frac{n}{2} \rfloor$) in the following theorem.

Theorem 10. *1. If $n = 2m+1$ is odd then*

$$\mathsf{NL}_m(f_\psi) \;\geq\; \begin{cases} \dfrac{1}{2}\dbinom{n-1}{m-1} & \text{if } m \not\preceq n \text{ (i.e., } n \text{ is not of the form } 2^t - 1\text{);} \\ \dfrac{1}{2}\left(\dbinom{n-1}{m-1} - 1\right) & \text{if } m \preceq n \text{ (i.e., } n \text{ is of the form } 2^t - 1\text{).} \end{cases}$$

2. If $n = 2m$ is even then

(a) $\mathsf{NL}_m(f_\psi) \;\geq\; \binom{n-2}{m}$ if m is even.

(b) $\mathsf{NL}_{m-1}(f_\psi) \;\geq\; \frac{1}{2}\left(\binom{n-2}{m-1} + \binom{n-2}{m-3}\right)$ if m is odd and $n \geq 10$.

Now, we study the restricted nonlinearity $\mathsf{NL}_2(f_\psi)$.
We denote by NL_k^n the minimum $\min\{\mathsf{NL}_k^n(f_\psi) \mid f_\psi \in \mathcal{B}_n$ constructed as in Theorem 5$\}$.

Theorem 11. *Let $n \geq 2$ be an positive integer and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

$$\mathsf{NL}_2(f_\psi) \;\geq\; \lfloor \frac{(n-1)^2}{8} \rfloor.$$

Moreover, if $n = 2^m$ for $m \geq 1$, $\quad \dfrac{n(n-2)}{8} \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n} \leq \cdots.$
For generalization, if $n = 2^{a_w} + 2^{a_{w-1}} + \cdots + 2^{a_1}$ for $a_w > a_{w-1} > \cdots > a_1 \geq 0$ as defined in Equation1,

$$\lfloor \frac{(n-1)^2}{8} \rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n} \leq \cdots.$$

Proof. From Theorem 1, we have $\min\limits_{0 \leq l \leq n} \mathsf{K}_2(l, n) = -\lfloor \frac{n}{2} \rfloor$. Using it in Theorem 8 we have,

$$\mathsf{NL}_2(f_\psi) \;\geq\; \begin{cases} \frac{1}{4}\left(\binom{n}{2} - \lfloor \frac{n}{2} \rfloor\right) & \text{if } 2 \not\preceq n \\ \frac{1}{4}\left(\binom{n}{2} - \lfloor \frac{n}{2} \rfloor - 2\right) & \text{if } 2 \preceq n. \end{cases}$$

Therefore, for $2 \not\preceq n$, we have $\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even } (i.e., n = 4t \text{ form}) \\ \frac{(n-1)^2}{8} & \text{if } n \text{ is odd } (i.e., n = 4t+1 \text{ form}), \end{cases}$
and for $2 \preceq n$, we have $\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} - \frac{1}{2} & \text{if } n \text{ is even } (i.e., n = 4t+2 \text{ form}) \\ \frac{(n-1)^2}{8} - \frac{1}{2} & \text{if } n \text{ is odd } (i.e., n = 4t+3 \text{ form}). \end{cases}$
We can check that for n even, $\frac{n(n-2)}{8}$ is always an integer and for n odd, $\frac{(n-1)^2}{8}$ is an integer if and only if $2 \not\preceq n$. Hence, combining the cases, we have

$$\mathsf{NL}_2(f_\psi) \geq \begin{cases} \frac{n(n-2)}{8} & \text{if } n \text{ is even} \\ \lfloor \frac{(n-1)^2}{8} \rfloor & \text{if } n \text{ is odd.} \end{cases}$$

Further, as $\frac{(n-1)^2}{8} = \frac{n(n-2)}{8} + \frac{1}{8}$, $\lfloor \frac{(n-1)^2}{8} \rfloor = \frac{n(n-2)}{8}$ when n is even. Hence, $\mathsf{NL}_2(f_\psi) \geq \lfloor \frac{(n-1)^2}{8} \rfloor$.

To prove the second part of the theorem, we use the technique followed in the proof of [LM19, Theorem-3.14]. It can be checked that $\mathsf{NL}_R(f) \leq \mathsf{NL}_E(f)$ if $R \subseteq E$. When $n = 2^m$, for a fixed integer $j \in [1, m]$, consider the set

$$R_j = \{(y, y) : y \in \mathbb{F}_2^{\frac{n}{2}}, \mathsf{w_H}(y) = 2^{j-1}\} = \{(y, y) : y \in \mathsf{E}_{2^{j-1}, \frac{n}{2}}\} \subseteq \mathsf{E}_{2^j, n}.$$

It can be checked that for $x = (y, y) \in R_j$, the orbit containing x, $\mathsf{O}_{\psi_n}(x) = \{(z, z) : z \in \mathsf{O}_{\psi_{\frac{n}{2}}}(y)\}$. Then for a WPB $f \in \mathcal{B}_n$ satisfying Theorem 5, we have a WPB $g \in \mathcal{B}_{\frac{n}{2}}$ such that $g(y) = f(x)$ for all $y \in \mathbb{F}_2^{\frac{n}{2}}$. This implies,

$$\mathsf{NL}_2^{\frac{n}{2}}(g) = \mathsf{NL}_{\mathsf{E}_{2, \frac{n}{2}}}(g) = \mathsf{NL}_{R_2}(f) \leq \mathsf{NL}_{\mathsf{E}_{4,n}}(f) = \mathsf{NL}_4^n(f). \tag{17}$$

The equality $\mathsf{NL}_{\mathsf{E}_{2, \frac{n}{2}}}(g) = \mathsf{NL}_{R_2}(f)$ can be proved as follows.

$$\begin{aligned} \mathsf{NL}_{R_2}(f) = \frac{|R_2|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \sum_{x \in R_2} (-1)^{f(x) + a.x} &= \frac{|\mathsf{E}_{2, \frac{n}{2}}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \sum_{y \in \mathsf{E}_{2, \frac{n}{2}}} (-1)^{g(y) + a.(y,y)} \\ &= \frac{|\mathsf{E}_{2, \frac{n}{2}}|}{2} - \frac{1}{2} \max_{a \in \mathbb{F}_2^n} \sum_{y \in \mathsf{E}_{2, \frac{n}{2}}} (-1)^{g(y) + (a_l + a_r).y} \quad \text{where } a = (a_l, a_r) \text{ with } a_l, a_r \in \mathbb{F}_2^{\frac{n}{2}} \\ &= \frac{|\mathsf{E}_{2, \frac{n}{2}}|}{2} - \frac{1}{2} \max_{b \in \mathbb{F}_2^{\frac{n}{2}}} \sum_{y \in \mathsf{E}_{2, \frac{n}{2}}} (-1)^{g(y) + b.y} = \mathsf{NL}_{\mathsf{E}_{2, \frac{n}{2}}}(g). \end{aligned}$$

Let the $\mathsf{NL}_4^n = \min\limits_{f \in \mathcal{B}_n \text{WPB}} \mathsf{NL}_4^n(f) = \mathsf{NL}_4^n(\hat{f})$ for a Boolean function $\hat{f} \in \mathcal{B}_n$. Then there is a WPB $\hat{g} \in \mathcal{B}_{\frac{n}{2}}$ such that $\mathsf{NL}_2^{\frac{n}{2}}(\hat{g}) \leq \mathsf{NL}_4^n(\hat{f})$. Hence, $\mathsf{NL}_2^{\frac{n}{2}} \leq \mathsf{NL}_2^{\frac{n}{2}}(\hat{g}) \leq \mathsf{NL}_4^n(\hat{f}) = \mathsf{NL}_4^n$.

Then, it can be generalized (by proving $\mathsf{NL}_{\mathsf{E}_{2^t, \frac{n}{2}}}(g) = \mathsf{NL}_{R_{t+1}}(f)$) as

$$\lfloor \frac{(n-1)^2}{8} \rfloor = \frac{n(n-2)}{8} \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n} \leq \cdots.$$

Consider $n = n_w + n_{w-1} + \cdots + n_1 = 2^{a_w} + 2^{a_{w-1}} + \cdots + 2^{a_1}$ such that $a_w > a_{w-1} > \cdots > a_1 \geq 0$ as defined in Equation 1. Let $y \in \mathsf{E}_{2,n}$ for $y = y_{n_w} y_{n_{w-1}} \ldots y_{n_1}$ where $y_{n_i} = (y_{n_{i+1}+1}, y_{n_{i+1}+2}, \ldots, y_{n_{i+1}+n_i})$ and $\mathsf{w_H}(y) = 2$. Let us define:

$$R = \{(y_{n_w}, y_{n_w})(y_{n_{w-1}}, y_{n_{w-1}}) \ldots (y_{n_1}, y_{n_1}) : y = y_{n_w} y_{n_{w-1}} \ldots y_{n_1} \in \mathbb{F}_2^n \text{ and } \mathsf{w_H}(y) = 2\} \subseteq \mathsf{E}_{4,2n}.$$

For $x = (y_{n_w}, y_{n_w})(y_{n_{w-1}}, y_{n_{w-1}}) \ldots (y_{n_1}, y_{n_1}) \in R$, we have

$$\mathsf{O}_{\psi_n}(x) = \{(z_{n_w}, z_{n_w})(z_{n_{w-1}}, z_{n_{w-1}}) \ldots (z_{n_1}, z_{n_1}) : z_{n_w} z_{n_{w-1}} \ldots z_{n_1} \in \mathsf{O}_{\psi_{\frac{n}{2}}}(y)\}.$$

Using similar technique as in the previous case, for a $f \in \mathcal{B}_{2n}$ satisfying Theorem 5, we have a WAPB $g \in \mathcal{B}_n$ such that $\forall y \in \mathbb{F}_2^n$, $g(y) = f(x)$ for $x \in R$. This implies, $\mathsf{NL}_2^n(g) = \mathsf{NL}_R(f) \leq \mathsf{NL}_{\mathsf{E}_{4,2n}}(f) = \mathsf{NL}_4^{2n}(f)$. This implies, $\mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n}$. If we generalize the result, we have

$$\lfloor \frac{(n-1)^2}{8} \rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n}.$$

□

Thus, the above theorem provides a better lower bound for the weightwise nonlinearity $\mathsf{NL}_k(f_\psi)$, as proven in the article [LM19], recalled in the following proposition.

Proposition 4. *[LM19][Theorem 3.14] For any $n = 2^m \geq 8$ and f_ψ be a WPB Boolean function as defined in 1, then*

$$\mathsf{NL}_{2^i}^{(n)}(f_\psi) \;\geq\; \begin{cases} 5, & \text{if } 1 \leq i \leq m-3, \\ 6, & \text{if } i = m-2, \\ 19, & \text{if } i = m-1. \end{cases}$$

5 Construction and Study of 2-σS (i.e., 2-RotS) WAPB Boolean functions

In this section, we present a class of 2-σS WAPB Boolean function which is another special case of the construction presented in Section 3. Since $\sigma \in \mathbb{S}_n$ is the rotation permutation, these functions are also known as 2-RotS WAPB Boolean functions. When n is a power of 2, the construction matches the Liu-Mesnager construction [LM19] to generate WPB Boolean functions. Now to study nonlinearity bound in Theorem 3, we need to count the number of orbits of odd cardinality due to the group action of $C_n = \langle \sigma_n \rangle$ on $\mathbb{F}_2^n$. For a positive integer n, we denote n_0 as the largest odd integer that divides n i.e., $n_0 = \frac{n}{2^t}$ for largest integer t such that $\frac{n}{2^t}$ is an integer.

Proposition 5. *[SM08] Let $C_n = \langle \sigma_n \rangle$ for $\sigma_n \in \mathbb{S}_n$ be the cyclic group of rotation permutations acting on $\mathbb{F}_2^n$. Then the number of orbits induced on $\mathbb{F}_2^n$ is given by $g_n = \frac{1}{n} \sum\limits_{t \mid n} \phi(t) 2^{\frac{n}{t}}$, where $\phi(t)$ is Euler's phi-function.*

Lemma 5. *Let $d \mid n$ for positive integers d and n. Let $C_n = \langle \sigma_n \rangle$ for $\sigma_n \in \mathbb{S}_n$ and $C_d = \langle \sigma_d \rangle$ for $\sigma_d \in \mathbb{S}_d$. For $v \in \mathbb{F}_2^d$, $|\mathsf{O}_{\sigma_d}(v)| = |\mathsf{O}_{\sigma_n}(\hat{v})|$ where $\hat{v} = (v, v, \ldots, v) \in \mathbb{F}_2^n$.*

Proof. For $v \in \mathbb{F}_2^d$, it can be verified that $\sigma_n(\hat{v}) = \sigma_n(v, v, \ldots, v) = (\sigma_d(v), \sigma_d(v), \ldots, \sigma_d(v))$.

If $|\mathsf{O}_{\sigma_d}(v)| = k \implies \sigma_d^k(v) = v \implies (\sigma_d^k(v), \sigma_d^k(v), \ldots, \sigma_d^k(v)) = (v, v, \ldots, v) \implies \sigma_n^k(\hat{v}) = \hat{v} \implies |\mathsf{O}_{\sigma_n}(\hat{v})| \mid k$. Further, if $|\mathsf{O}_{\sigma_n}(\hat{v})| = l \implies \sigma_n^l(\hat{v}) = \hat{v} \implies (\sigma_d^l(v), \sigma_d^l(v), \ldots, \sigma_d^l(v)) = (v, v, \ldots, v) \implies \sigma_d^l(v) = v \implies |\mathsf{O}_{\sigma_d}(v)| \mid l$. Therefore, $|\mathsf{O}_{\sigma_d}(v)| = |\mathsf{O}_{\sigma_n}(\hat{v})|$ for every $v \in \mathbb{F}_2^d$. □

Theorem 12. *For $\sigma_n \in \mathbb{S}_n$, the number of orbits of odd cardinality due to the action of $C_n = \langle \sigma_n \rangle$ on $\mathbb{F}_2^n$ is given by $g_{n,odd} = g_{n_0}$.*

Proof. For $d \mid n$, it can be easily checked that if $|\mathsf{O}_{\sigma_n}(x)| = d$ for an $x \in \mathbb{F}_2^n$ then there is a $v \in \mathbb{F}_2^d$ such that such that $x = (v, v, \ldots, v)$ and $|\mathsf{O}_{\sigma_d}(v)| = d$ in $\mathbb{F}_2^d$. Every odd divisor d of n is also an divisor of n_0 and viceversa. Hence, for $d \mid n$ and d is odd, $|\mathsf{O}_{\sigma_n}(x)| = d$ for an $x \in \mathbb{F}_2^n$ iff there is a $v \in \mathbb{F}_2^d$ such that $x = (v, v, \ldots, v)$ and $|\mathsf{O}_{\sigma_d}(v)| = d$ iff $|\mathsf{O}_{\sigma_{n_0}}(y)| = d$ where $y = (v, v, \ldots, v) \in \mathbb{F}_2^{n_0}$. Therefore $g_{n,odd} = g_{n_0}$. □

Corollary 3. *For $\sigma_n \in \mathbb{S}_n$, the number of 2-$\sigma_n$S WAPB functions is X and the number of balanced 2-σS WAPB functions is Y.*

Theorem 13. *Let $\sigma_n \in \mathbb{S}_n$ for a positive integer n. Then $\mathsf{NL}(f_{\sigma_n}) \geq 2^{n-2} - \frac{g_{n_0}}{2}$.*

Proof. From Theorem 3, we have

$$\mathsf{NL}(f_{\sigma_n}) \geq 2^{n-2} - \frac{|\mathsf{O}_o|}{2} = 2^{n-2} - \frac{g_{n,odd}}{2} = 2^{n-2} - \frac{g_{n_0}}{2}.$$

□

As g_n is an even integer [CI18], the bound is always an integer. When $n = 2^m$ is a power of 2, the nonlinearity bound $\mathsf{NL}(f_{\sigma_n}) \geq 2^{n-2} - 1$ as $g_{n_0} = g_1 = 2$. As $f_{\sigma_n} = f_{\psi_n}$ when n is a power of 2, the nonlinearity bound $\mathsf{NL}(f_{\sigma_n})$ matches with the result in Corollary 1.

n	4	5	6	7	8	9	10
Max nl by experiment	4	12	26	54	116	232	480
% functions at max nl	100	2.34	6.51	8.2×10^{-3}	3.8×10^{-3}	8.5×10^{-4}	9.5×10^{-5}
Nonlinearity upper bound of balanced functions [SZZ95]	4	12	28	58	118	244	494
Min nl by experiment	4	6	14	34	64	188	334
% functions at min nl	100	0.52	1.04	3.1×10^{-6}	3.2×10^{-3}	9.5×10^{-5}	9.5×10^{-5}
Average nl by experiment	4.0	9.59	22.05	48.51	106.01	220.18	460.45
Nonlinearity lower bound by Theorem 13	3	4	14	22	63	98	252

Table 3. Percentage of $f_\sigma \in \mathcal{B}_n$ satisfying lower bound and upper value of $\mathsf{NL}(f_\sigma)$

Theorem 14. *For $\sigma_n \in \mathbb{S}_n$ and $k \in [0, n]$, the number of orbits due to the action of $C_n = \langle \sigma_n \rangle$ on $\mathsf{E}_{k,n}$ is given by*

$$g_{k,n} = \frac{1}{n} \sum_{\{\sigma_n^i \in C_n : o(\sigma_n^i) | k\}} \binom{\gcd(n,i)}{\frac{k}{o(\sigma_n^i)}},$$

where $o(\sigma_n^i) = \frac{n}{\gcd(n,i)}$ is the order of σ_n^i.

Proof. For $1 \leq i \leq o(\sigma_n)$, denote $F_i = \{x \in \mathsf{E}_{k,n} : \sigma_n^i(x) = x\}$ be the set of fixed elements of σ_n^i in $\mathsf{E}_{k,n}$. To apply Burnside's Lemma for counting the number of orbits, we need to determine $|F_i|$. Observe that $o(\sigma_n^i) = \frac{n}{\gcd(n,i)}$. Hence, the number of disjoint cycles in σ_n^i is $\gcd(n,i)$, with each cycle having length $o(\sigma_n^i) = \frac{n}{\gcd(n,i)}$. A vector $x \in \mathbb{F}_2^n$ is fixed by σ_n^i if each cycle in x must be all 0 or all 1. For x being in $\mathsf{E}_{k,n}$, $o(\sigma_n^i) \mid k$ and there are $\frac{k}{o(\sigma_n^i)}$ cycles in x contain all 1 and remaining cycles contain all 0. Thus, there are $|F_i| = \binom{\gcd(n,i)}{\frac{k}{o(\sigma^i)}}$. Hence, applying Burnside's Lemma, we have

$$g_{k,n} = \frac{1}{n} \sum_{\sigma_n^i \in C_n} |F_i| = \frac{1}{n} \sum_{\{\sigma_n^i \in C_n : o(\sigma_n^i) | k\}} \binom{\gcd(n,i)}{\frac{k}{o(\sigma_n^i)}}.$$

□

Lemma 6. *For $\sigma_n \in \mathbb{S}_n$, the number of orbits of odd cardinality due to the action of $C_n = \langle \sigma_n \rangle$ on $\mathsf{E}_{k,n}$ is given by*

$$g_{k,n,odd} = \begin{cases} 0 & \textit{if } 2^e \nmid k \\ g_{\frac{k}{2^e}, n_0} & \textit{if } 2^e \mid k, \end{cases}$$

where n_0 is the largest odd intger that divides n and $2^e = \frac{n}{n_0}$ i.e., e is the largest integer such that 2^e divides n.

Proof. As in the proof of Theorem 12, for $d \mid n$, if $|\mathsf{O}_{\sigma_n}(x)| = d$ for an $x \in \mathsf{E}_{k,n}$ then there is a $v \in \mathbb{F}_2^d$ such that such that $x = (v, v, \ldots, v)$ with $|\mathsf{O}_{\sigma_d}(v)| = d$ in $\mathbb{F}_2^d$ and $\mathsf{w}_\mathsf{H}(v) = \frac{k}{n/d} = \frac{kd}{n}$. Thus, in this case, $\frac{n}{d} \mid k$ and hence $v \in \mathsf{E}_{\frac{kd}{n},d}$.
For any odd divisor d of n, if $\frac{n}{d} \mid k$ then $2^e \mid k$. That is, if $2^e \nmid k$ then $\frac{n}{d} \nmid k$ for every odd divisor d of n and that implies $g_{k,n,odd} = 0$.
Now consider the case $2^e \mid k$. Every odd divisor d of n is also an divisor of n_0 and viceversa. Further, for any odd integer d of n, if $\frac{n}{d} \nmid k$ then $\frac{n_0}{d} \nmid \frac{k}{2^e}$ and viceversa. Hence, $|\mathsf{O}_{\sigma_n}(x)| = d$ for an $x \in \mathsf{E}_{k,n}$ with d is odd, $d \mid n$ and $\frac{n}{d} \mid k$ iff there is a $v \in \mathsf{E}_{\frac{kd}{n},d}$ such that $x = (v, v, \ldots, v)$ and $|\mathsf{O}_{\sigma_d}(v)| = d$ iff $|\mathsf{O}_{\sigma_{n_0}}(y)| = d$ where $y = (v, v, \ldots, v) \in \mathsf{E}_{\frac{k}{2^e},n_0}$. Therefore, $g_{k,n,odd} = g_{\frac{k}{2^e},n_0}$. □

Theorem 15. *Let $n \geq 2$ be a positive integer and $\sigma_n \in \mathbb{S}_n$ be the rotation permutation. Then*

$$\mathsf{NL}_k(f_{\sigma_n}) \geq \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min\limits_{\substack{2 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l,n)\right) & \text{if } 2^e \nmid k \\ \frac{1}{4}\left(\binom{n}{k} - 2g_{\frac{k}{2^e},n_0} + \min\limits_{\substack{2 \leq l \leq n \\ l \text{ even}}} \mathsf{K}_k(l,n)\right) & \text{if } 2^e \mid k, \end{cases}$$

where n_0 is the largest odd intger that divides n and $2^e = \frac{n}{n_0}$

The proof of the theorem can directly be obtained by substituting the value of $|\mathcal{O}_{o,k}| = g_{k,n,odd}$ from Lemma 6 in Theorem 4.

6 Conclusion

References

CI18. Lavinia C. Ciungu and Miodrag C. Iovanov. On the matrix of rotation symmetric boolean functions. *Discrete Mathematics*, 341(12):3271–3280, 2018.

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.

CS02. Thomas W. Cusick and Pantelimon Stanica. Fast evaluation, weights and nonlinearity of rotation-symmetric functions. *Discrete Mathematics*, 258(1-3):289–301, 2002.

DM23. Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced Boolean functions with high weightwise nonlinearity. In *8th International Workshop on Boolean Functions and their Applications (BFA)*, 2023.

DM24. Deepak Kumar Dalai and Krishna Mallick. A class of weightwise almost perfectly balanced Boolean functions. *Advances in Mathematics of Communications*, 18(2):480–504, 2024.

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*, 40:41–58, 2006.

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

GM22a. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 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 *Progress in Cryptology - INDOCRYPT*, volume 13774 of *Lecture Notes in Computer Science*, pages 492–514. Springer, 2022.

GM23a. Agnese Gini and Pierrick Méaux. S_0-equivalent classes, a new direction to find better weightwise perfectly balanced functions, and more. *IACR Cryptol. ePrint Arch.*, page 1101, 2023.

GM23b. Agnese Gini and Pierrick Méaux. On the algebraic immunity of weightwise perfectly balanced functions. In *LATINCRYPT*, volume 14168 of *Lecture Notes in Computer Science*, pages 3–23. Springer, 2023.

GM23c. Agnese Gini and Pierrick Méaux. Weightwise perfectly balanced functions and nonlinearity. In *Codes, Cryptology and Information Security*, volume 13874 of *Lecture Notes in Computer Science*, pages 338–359. Springer, 2023.

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.

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

LS20. Jingjing Li and Sihong Su. Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity. *Discrete Applied Mathematics*, 279:218–227, 2020.

Méa24. Pierrick Méaux. Weightwise (almost) perfectly balanced functions based on total orders. *IACR Cryptol. ePrint Arch.*, page 647, 2024.

MJSC16. Pierrick Méaux, Anthony Journault, François-Xavier Standaert, and Claude Carlet. Towards stream ciphers for efficient FHE with low-noise ciphertexts. In *Advances in Cryptology - EUROCRYPT*, volume 9665 of *Lecture Notes in Computer Science*, pages 311–343. Springer, 2016.

MMM$^+$18. Subhamoy Maitra, Bimal Mandal, Thor Martinsen, Dibyendu Roy, and Pantelimon Stanica. Tools in analyzing linear approximation for boolean functions related to FLIP. In *Progress in Cryptology - INDOCRYPT 2018*, pages 282–303, 2018.

MPJ$^+$22. Luca Mariot, Stjepan Picek, Domagoj Jakobovic, Marko Djurasevic, and Alberto Leporati. Evolutionary construction of perfectly balanced Boolean functions. In *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*, 13(6):951–979, 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. *Cryptography and Communications*, 14(6):1371–1389, 2022.

MZD19. Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of Boolean functions with restricted input. *Cryptography and Communications*, 11(1):63–76, 2019.

PQ99. Josef Pieprzyk and Cheng Xin Qu. Fast hashing and rotation-symmetric functions. *Journal of Universal Computer Science*, 5:20–31, 1999.

SM08. Pantelimon Stanica and Subhamoy Maitra. Rotation symmetric Boolean functions - count and cryptographic properties. *Discrete Applied Mathematics*, 156(10):1567–1580, 2008.

Su21. Sihong Su. The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions. *Discrete Applied Mathematics*, 297:60–70, 2021.

SZZ95. Jennifer Seberry, Xian-Mo Zhang, and Yuliang Zheng. Nonlinearity and propagation characteristics of balanced boolean functions. *Inf. Comput.*, 119(1):1–13, 1995.

TL19. Deng Tang and Jian Liu. A family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity. *Cryptography and Communications*, 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 *ACM Asia Conference on Computer and Communications Security*, page 638–648. Association for Computing Machinery, 2023.

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. *Discrete Applied Mathematics*, 337:190–201, 2023.

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.

ZS23. Rui Zhang and Sihong Su. A new construction of weightwise perfectly balanced Boolean functions. *Advances in Mathematics of Communications*, 17(4):757–770, 2023.