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

No Author Given

No Institute Given

Abstract.

1 Introduction

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 $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ 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 $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ is called as the truth table of the Boolean function f, it corresponds to the ordered vectors of $\mathbb{F}_2^n$ as $v_0 = (0, 0, \ldots, 0), v_1 = (0, 0, \ldots, 1), \ldots, v_{2^n-1} = (1, 1, \ldots, 1)$. 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 $\mathsf{supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. Therefore, the Hamming weight of the Boolean function f, is 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 $\mathbb{F}_2[x_1, x_2, \ldots, x_n]/ < x_1^2 + x_1, x_2^2 + x_2, \ldots, x_n^2 + x_n >$, 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 also 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 $[m, n] = \{m, m + 1, \ldots, n\}$.

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 [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 [MZD18].

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

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

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

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:

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

Definition 8 (Krawtchouk Polynomial). *For a positive integer n, the Krawtchouk polynomial [MS78, Page 151] of degree k is given by*

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

Following the results in [DMS06, GM22], the following relations can be derived.

Theorem 1 (Krawtchouk Polynomials relations). *For integers $n > 0$, $0 \leq k \leq n$ and fixed $a \in \mathbb{F}_2^n$ such that $\mathsf{w_H}(a) = \ell$, the following relations hold.*

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

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

Definition 9 (Rotation Symmetric Boolean function). *A Boolean function f is rotation symmetric (RotS) if and only if for any $(x_1, x_2, \dots, x_n) \in \mathbb{F}_2^n$,*

$$f(\rho_n^k(x_1, x_2, \dots, x_n)) = f(x_1, x_2, \dots, x_n)$$

for every $1 \leq k \leq n$ where ρ_n is a cyclic shift permutation on n-elements i.e., $\rho_n(x_1, x_2, \dots, x_n) = (x_2, x_3, \dots, x_n, x_1)$ and $\rho_n^k = \rho_n \circ \rho_n^{k-1}$ for $k > 1$ i.e., the composition of ρ_n k times.Therefore, RotS Boolean functions have the same truth value for all vectors in every orbit obtained by the action of permutation group $\langle \rho_n \rangle$ on $\mathbb{F}_2^n$.

Let denote $P = \langle \rho_n \rangle$ be the cyclic permutation group generated by the permutation ρ_n. Applying Burnside's lemma, we can have the number of orbits obtained due the action of P on $\mathbb{F}_2^n$ is $g_n = \frac{1}{n} \sum_{t|n} \phi(t) 2^{n/t}$ [SM08]. Let $\mathcal{O} = \{\mathsf{O}_1, \mathsf{O}_2, \dots, \mathsf{O}_{g_n}\}$ be the set of orbits obtained due the action of P on $\mathbb{F}_2^n$. An orbit leader/representative ν_{O} is chosen for each orbit $\mathsf{O} \in \mathcal{O}$. The representatives can be chosen using some ordering, for example it may be the lexicographically smallest element in the orbit.

Definition 10 (2-Rotation Symmetric Boolean function). *A Boolean function f is 2-rotation symmetric (2-RotS) if and only if for every orbit $\mathsf{O} \in \mathcal{O}$ with representative element ν,*

$$f(\rho_n^{2i+1}(\nu)) = f(\nu); \quad f(\rho_n^{2i}(\nu)) = f(\nu) + 1 \text{ for every } 1 \leq i \leq \lfloor \frac{|\mathsf{O}|}{2} \rfloor.$$

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

A construction of a class of 2-RotS WPB Boolean functions is presented by Liu and Mesnager [LM19].

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.*

Since, n is the power of 2 in the construction proposed in Proposition 1, 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 have proposed an generalization of this concept to construct WAPB Boolean function on any n where n is a natural number in Section 4.

3 Construction of WAPB Boolean functions using Group action

In this section we will present a construction of 2-RotS WAPB Boolean functions using a cyclic permutation group action. Let $G = \langle \pi \rangle$ be a cyclic subgroup of the symmetric group $\mathbb{S}_n$ on n elements. Let the group action of G 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 $O_\pi(x) = \{g(x) : g \in G\} = \{x, \pi(x), \pi^2(x), \dots, \pi^{l-1}(x)\}$ where l is the order of the permutation π. As

Construction 1 Construction of 2-RotS WAPB Boolean function

Input: $\pi \in \mathbb{S}_n$

Output: A 2-RotS WAPB Boolean function $f_\pi \in \mathcal{B}_n$

```
Initiate supp(f_π) = φ
t = 0
for k ← 0 to n do
    for i ← 1 to g_{k,n} do
        u = ν_{k,n,i}; l = |O_π(u)|
        if l is even then
            for j ← 1 to l/2 do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
        else
            u = π^t(u)
            for j ← 1 to ⌈(l−t)/2⌉ do
                supp(f_π).append(u)
                u ← π ∘ π(u)
            end for
            Update t ← 1 − t
        end if
    end for
end for
return f_π
```

$\mathsf{w_H}(\pi^i(x)) = \mathsf{w_H}(x)$ for $1 \leq i \leq l-1$, the group action G 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 $\mathsf{E}_{k,n}$ with some ordering. The construction of 2-RotS 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.

Example 1. Consider $n = 5$ and the permutation $\pi = \rho_n$ is the cyclic rotation. Then considering the orbits with representatives $00000, 00001, 00011, 00101, 00111, 01011, 01111, 11111$, we have the resultant function $f_{\rho_n} \in \mathcal{B}_5$ of Construction 1 as

$$\begin{aligned}\mathsf{supp}(f_{\rho_n}) =&\{00000, 00010, 01000, 00011, 01100, 10001, 01010, 01001,\\ &00111, 11100, 10011, 10110, 11010, 01111, 11101, 10111\}.\end{aligned}$$

is a 2-RotS WAPB Boolean function.

Theorem 2. *Nonlinearity and Weightwise nonlinearity bound.*

4 Extending Liu-Mesnager construction [LM19] for WAPB Boolean function

In this section, we present a class of 2-RotS 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 a WAPB Boolean functions. Let n be a positive integer with binary representation as

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

We denote $\mathsf{w_H}(n) = w$ i.e., the number of 1's in the binary representation of n. Consider the cyclic subgroup $G = \langle \psi \rangle$ of the symmetric group $\mathbb{S}_n$, where the disjoint cycle form of ψ contains cycles of length $n_1, n_2, \ldots, n_w$. Without loss of generality, we consider

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

Hence, for $x = (x_1, x_2, \ldots, x_n)$, we have

$$\psi(x) = (\rho_{n_1}(x_1, \ldots, x_{n_1}), \rho_{n_2}(x_{n_1+1}, \ldots, x_{n_1+n_2}), \ldots, \rho_{n_w}(x_{n-n_w+1}, \ldots, x_n)) \tag{3}$$

where ρ_{n_i} is the cyclic shift permutation on n_i elements. Here, $ord(\psi) = 2^{a_w} = n_w$. Hence, the cardinality of orbits obtained due the action of G 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 rest are of even cardinality.

Lemma 2. *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.,

$$\begin{aligned} &x_1 = x_2 = \ldots = x_{n_1}; \\ &x_{n_1+1} = x_{n_1+2} = \ldots = x_{n_1+n_2}; \\ &\vdots \\ &x_{n-n_w+1} = x_{n-n_w+2} = \ldots = x_n. \end{aligned} \tag{4}$$

As each partition of coordinates can be either 0 or 1, there are 2^w vectors x in $\mathbb{F}_2^n$ satisfying Equation 4 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 $x_i \leq y_i, \forall 1 \leq i \leq n$ i.e., $y_i = 1$ if $x_i = 1, \forall 1 \leq i \leq n$. 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 3. *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 4, 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 4. Hence, $|O_\psi(x)| > 1$. Hence, in this case there is no orbit of weight k and cardinality 1. □

Let denote $\mathcal{O}$ be the set of all orbits due the action of ψ on $\mathbb{F}_2^n$. Further, 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 cardinality odd. Hence from Equation 4, $\mathcal{O}_o = \{(x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n : x_1 = x_2 = \cdots = x_{n_1}; x_{n_1+1} = x_{n_1+2} = \cdots = x_{n_1+n_2}; \cdots; x_{(n-n_w)+1} = x_{(n-n_w)+2} = \cdots = x_n\}$. 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-RotS WAPB Boolean functions as other orbits are of even cardinality. Hence, we have the following result.

Proposition 2. *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, $\psi = \rho_n$ 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-RotS WAPB Boolean function using $\psi \in \mathbb{S}_n$

Input: $\psi \in \mathbb{S}_n$ as in Equation 2
Output: A 2-RotS WAPB Boolean function $f_\psi \in \mathcal{B}_n$
For every orbit O in $\mathbb{F}_2^n$ due to the action of $G = \langle\psi\rangle$, 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 to make f balanced.
end if
return f_ψ

[**PM:** For construction 2, I propose the following modifications:

- in input we add a representative ν_i
- in input we add a binary vector v of length the number of orbits.
- then, for every orbit f takes the value v_i on ν_i, and we keep "f satisfies $f_\psi(\psi(x)) = 1 + f(x)$ for $x \in \mathsf{O}$"
- we withdraw the last part, forcing f_ψ to be balanced.

The advantage of the extra inputs would be to define more easily each function later on (if we use an order to list the representatives, we can identify a function in n variables only from the the vector v). Regarding the balancedness, WAPB functions are not required to be balanced, so we would have a more general description (I do not think the balancedness is used in the proofs after). We would make a remark on the restriction that is sufficient to be balanced, or even than the weight of f is determined by the weight of v restricted to the orbits of size 1.]

Theorem 3. *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 3, we have

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

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

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 $\rho_{n_i}^k = \gcd(n_i, k)$ for $1 \le i \le w$ and $1 \le k \le n_w$. So, the length of each permutation cycle in $\rho_{n_i}^k$ 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. $\rho_{n_i}^k$ 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

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

□

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

Proposition 3. *For $n \ge 2$ as in Equation 1, let $\psi \in \mathbb{S}_n$ be the permutation as defined in Equation 2.Then*

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

Proof. Now for any $x = (x_1, x_2, \ldots, x_n), c = (c_1, c_2, \ldots, c_n) \in \mathbb{F}_2^n$, [**DKD:** need to write $\psi(x)$ in proper order]

$$\begin{aligned} c \cdot (x + \psi(x)) &= c_1(x_1 + x_{n_1}) + c_2(x_2 + x_1) + \cdots + c_{n_1}(x_{n_1} + x_{n_1-1}) \\ &\quad + c_{n_1+1}(x_{n_1+1} + x_{n_1+n_2}) + \cdots + c_{n_1+n_2}(x_{n_1+n_2} + x_{n_1+n_2-1}) \\ &\quad + \cdots \\ &\quad + c_{n-n_w+1}(x_{n-n_w+1} + x_n) + \cdots + c_n(x_n + x_{n-1}) \\ \implies c \cdot (x + \psi(x)) &= (c_1 + c_2)x_1 + (c_2 + c_3)x_2 + \cdots + (c_{n_1} + c_1)x_{n_1} \\ &\quad + (c_{n_1+1} + c_{n_1+2})x_{n_1+1} + \cdots + (c_{n_1+n_2} + c_{n_1+1})x_{n_1+n_2} \\ &\quad + \cdots \\ &\quad + (c_{n-n_w+1} + c_{n-n_w+2})x_{n-n_w+1} + \cdots + (c_n + c_{n-n_w+1})x_n \qquad (5) \\ \implies c \cdot (x + \psi(x)) &= (c + \psi^{-1}(c)) \cdot x. \end{aligned}$$

Therefore, $c \cdot (x + \psi(x))$ is a linear Boolean function on n variables. Here, $c \cdot (x + \psi(x))$ is the zero Boolean function if and only if $c_1 = c_2 = \ldots = c_{n_1}$; $c_{n_1+1} = c_{n_1+2} = \cdots = c_{n_1+n_2}; \ldots ; c_{(n-n_w)+1} = c_{(n-n_w)+2} = \cdots = c_n$ i.e., $c \in \mathcal{O}_o$. Hence,

$$|\{x \in \mathbb{F}_2^n : c \cdot (x + \psi(x)) = 1\}| = \mathsf{w_H}(c \cdot (x + \psi(x))) = \begin{cases} 2^{n-1} & \text{if } c \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 0 & \text{if } c \in \mathcal{O}_o \end{cases} \qquad (6)$$

Now further, if $x = (x_1, x_2, \ldots, x_n) \in \mathcal{O}_o$, then $\psi(x) = x$ and that implies $c \cdot (x + \psi(x)) = 0$. Hence,

$$\begin{aligned} & |\{x \in \mathcal{O}_o : c \cdot (x + \psi(x)) = 0\}| = |\mathcal{O}_o| = 2^w \\ \implies & |\{x \in \mathcal{O}_o : c \cdot (x + \psi(x)) = 1\}| = 0. \end{aligned} \qquad (7)$$

Now combining Equation 6 and Equation 7 we have the desired result

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

□

Theorem 4. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. Then* $\mathsf{NL}(f_\psi) \geq 2^{n-2} - 2^{w-1}$.

Proof. Let $a \in \mathbb{F}_2^n$ and $\psi \in \mathbb{S}_n$ be the permutation defined as in Equation 2. As $\mathsf{w_H}(n) = w$, from Lemma 2 there are 2^w orbits with cardinality 1 and remaining orbits are of even cardinality. Then the Walsh spectrum of f_ψ at a is as follows.

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

$$\implies |W_{f_\psi}(a)| \leq |\sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}} (-1)^{f_\psi(x)+a\cdot x}| + |\sum_{\mathsf{O}\in\mathcal{O}_o} \sum_{x\in\mathsf{O}} (-1)^{f_\psi(x)+a\cdot x}|. \tag{8}$$

Since the number of orbits of cardinality odd (i.e., 1) is 2^w, we have a bound for second sum as

$$|\sum_{\mathsf{O}\in\mathcal{O}_o} \sum_{x\in\mathsf{O}} (-1)^{f_\psi(x)+a\cdot x}| \leq 2^w. \tag{9}$$

Now we will work on the first sum.

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

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

$$\begin{aligned}
\sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}} (-1)^{f_\psi(x)+a\cdot x} &= \frac{1}{2}\Bigg[\sum_{\mathsf{O}\in\mathcal{O}_e}\Bigg(\sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=0} (-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}) \\
&\qquad + \sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1} (-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\Bigg)\Bigg] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1} (-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\right] \\
&= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1} 2\times(-1)^{f_\psi(x)+a\cdot x}\right] = \sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}:a\cdot(x+\psi(x))=1} (-1)^{f_\psi(x)+a\cdot x} \\
&= \sum_{x\in\mathbb{F}_2^n\setminus\mathsf{O}_o:a\cdot(x+\psi(x))=1} (-1)^{f_\psi(x)+a\cdot x}.
\end{aligned}$$

Now, using the Proposition 3, we have an upper bound to the sum

$$\left|\sum_{\mathsf{O}\in\mathcal{O}_e} \sum_{x\in\mathsf{O}} (-1)^{f_\psi(x)+a\cdot x}\right| = \left|\sum_{x\in\mathbb{F}_2^n\setminus\mathsf{O}_o:a\cdot(x+\psi(x))=1} (-1)^{f_\psi(x)+a\cdot x}\right| \leq \begin{cases} 2^{n-1} & \text{if } a \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 0 & \text{if } a \in \mathcal{O}_o. \end{cases} \tag{10}$$

Hence, from Equation 8, Equation 9 and Equation 10, we have

$$|W_{f_\psi}(a)| \le \begin{cases} 2^{n-1} + 2^w & \text{if } a \in \mathbb{F}_2^n \setminus \mathcal{O}_o \\ 2^w & \text{if } a \in \mathcal{O}_o \end{cases} \tag{11}$$

Hence, the nonlinearity of f_ψ satisfies

$$\mathsf{NL}(f_\psi) = 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |W_{f_\psi}(a)| \;\ge\; 2^{n-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n}\{2^{n-1}+2^w, 2^w\} \;=\; 2^{n-1} - 2^{n-2} - 2^{w-1}$$
$$\implies \mathsf{NL}(f_\psi) \ge 2^{n-2} - 2^{w-1}.$$

□

In the following table we have presented the maximum and minimum nonlinearity among all f_ψ for the number of variables $n = \{4, 5, \dots, 10\}$ along with the upperbound of balanced Boolean functions and lowerbound of f_ψ as per Theorem 4. We have searched all such Boolean functions for $n \le 6$ and from 2^{20} randomly chosen such Boolean functions for $n > 6$.

n	4	5	6	7	8	9	10
Number of functions	$2^4 \times \binom{2}{1} = 2^5$	$2^8 \times \binom{4}{2} = 3 \times 2^9$	$2^{18} \times \binom{4}{2} = 3 \times 2^{19}$	$2^{36} \times \binom{8}{4} = 35 \times 2^{37}$	$2^{34} \times \binom{2}{1} = 2^{35}$	$2^{68} \times \binom{4}{2} = 3 \times 2^{69}$	$2^{138} \times \binom{4}{2} = 3 \times 2^{139}$
Max Nonlinearity	4	12	26	56	116	236	480
% functions at max nl	100	22.917	0.651042	0.304318	0.008297	0.072575	0.013638
Nonlinearity upper bound	4	12	26	56	116	240	492
Min Nonlinearity	4	6	14	28	64	192	328
% functions at min nl	100	4.17	0.260417	0.014687	0.006199	0.000191	2^{-20}
Nonlinearity lower bound	3	6	14	28	63	144	254

Now we will study the weightwise nonlinearity of f_ψ.

Lemma 4. *For $n \ge 2$ as in Equation 1, let $\psi \in \mathbb{S}_n$ be the permutation as defined in Equation 2.Then*

$$|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_o : c\cdot(x+\psi(x)) = 1\}| = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)),$$

where $l = \mathsf{w_H}(c + \psi^{-1}(c))$.

Proof. Let $x = (x_1, x_2, \dots, x_n) \in \mathsf{E}_{k,n}$ and $c = (c_1, c_2, \dots, c_n) \in \mathbb{F}_2^n$. Then as in Equation 5, we have

$$c\cdot(x+\psi(x)) = (c+\psi^{-1}(c))\cdot x$$

is a linear function on n variable defined over the slice $\mathsf{E}_{k,n}$. Therefore, using Theorem 1, we have

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

where $l = \mathsf{w_H}(c+\psi^{-1}(c))$. If $x \in \mathsf{E}_{k,n}$ and $|\mathcal{O}_\psi(x)| = 1$ i.e., $x \in \mathsf{E}_{k,n} \cap \mathcal{O}_o$ then $c\cdot(x+\psi(x)) = 0$. Hence,

$$|\{x \in \mathsf{E}_{k,n} \setminus \mathcal{O}_o : c\cdot(x+\psi(x)) = 1\}| = \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)).$$

□

Theorem 5. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

$$\mathsf{NL}_k(f_\psi) \;\geq\; \begin{cases} \frac{1}{4}\left(\binom{n}{k} + \min\limits_{0\leq l\leq n} \mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \frac{1}{4}\left(\binom{n}{k} + \min\limits_{0\leq l\leq n} \mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}$$

Proof. Let $\mathcal{O}_k$ be the set of all orbits of the group action $G = \langle\psi\rangle$ on $\mathsf{E}_{k,n}$. Let $\mathcal{O}_{e,k}$ and $\mathcal{O}_{o,k}$ be the set of all orbits in $\mathcal{O}_k$ of cardinality even and cardinality odd respectively.
The restricted Walsh spectrum of f_ψ at $a \in \mathbb{F}_2^n$ is as follows.

$$\begin{aligned} \mathcal{W}_{f_\psi,k}(a) &= \sum_{x\in\mathsf{E}_{k,n}} (-1)^{f_\psi(x)+a\cdot x} = \sum_{\mathsf{O}\in\mathcal{O}_k}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} \\ &= \sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_{o,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} \\ \implies |\mathcal{W}_{f_\psi,k}(a)| &\leq |\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| + |\sum_{\mathsf{O}\in\mathcal{O}_{o,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| \\ &= \begin{cases} |\sum\limits_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum\limits_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| & \text{if } k \not\preceq n \\ |\sum\limits_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum\limits_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x}| + 1 & \text{if } k \preceq n. \end{cases} \end{aligned} \tag{12}$$

$$\begin{aligned} \sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + \sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(\psi(x))+a\cdot\psi(x)}\right] \\ &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} + (-1)^{f_\psi(\psi(x))+a\cdot\psi(x)}\right] \\ &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)+a\cdot x} - (-1)^{f_\psi(x)+a\cdot\psi(x)}\right] \qquad (\text{as } f_\psi(\psi(x)) = 1 + f_\psi(x)) \\ &= \frac{1}{2}\left[\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f_\psi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)\right] \\ &= \frac{1}{2}\left[\sum_{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o}(-1)^{f_\psi(x)}\left((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}\right)\right]. \end{aligned} \tag{13}$$

Here, $\mathcal{O}_o$ is the set of vectors with orbit cardinalty 1. The vectors x for which $((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)}) = 0$ i.e., $a\cdot(x+\psi(x)) = 0$ have contribution 0 to the sum in Equation 13. Hence, we have

$$\sum_{\mathsf{O}\in\mathcal{O}_{e,k}}\sum_{x\in\mathsf{O}}(-1)^{f(x)+a\cdot x} = \frac{1}{2}\left[\sum_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o \\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)}((-1)^{a\cdot x} - (-1)^{a\cdot\psi(x)})\right] = \sum_{\substack{x\in\mathsf{E}_{k,n}\setminus\mathcal{O}_o \\ a\cdot(x+\psi(x))=1}}(-1)^{f_\psi(x)+a\cdot x}.$$

Hence from Equation 12 and Lemma 4, we have

$$
\begin{aligned}
|\mathcal{W}_{f_\psi,k}(a)| &\leq \begin{cases} |\displaystyle\sum_{\substack{x\in \mathsf{E}_{k,n}\setminus \mathcal{O}_o \\ a\cdot(x+\psi(x))=1}} (-1)^{f_\psi(x)+a\cdot x}| & \text{if } k \not\preceq n \\ |\displaystyle\sum_{\substack{x\in \mathsf{E}_{k,n}\setminus \mathcal{O}_o \\ a\cdot(x+\psi(x))=1}} (-1)^{f_\psi(x)+a\cdot x}| + 1 & \text{if } k \preceq n. \end{cases} \\
&= \begin{cases} \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) & \text{if } k \not\preceq n \\ \frac{1}{2}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) + 1 & \text{if } k \preceq n. \end{cases}
\end{aligned} \tag{14}
$$

where $l = \mathsf{w_H}(a + \psi^{-1}(a))$. Hence, the nonlinearity of f_ψ satisfies

$$
\begin{aligned}
\mathsf{NL}_k(f_\psi) &= \frac{|\mathsf{E}_{k,n}|}{2} - \frac{1}{2}\max_{a\in\mathbb{F}_2^n} |\mathcal{W}_{f_\psi,k}(a)| \geq \begin{cases} \dfrac{|\mathsf{E}_{k,n}|}{2} - \dfrac{1}{4}\displaystyle\max_{a\in\mathbb{F}_2^n}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) & \text{if } k \not\preceq n \\ \dfrac{|\mathsf{E}_{k,n}|}{2} - \dfrac{1}{4}\displaystyle\max_{a\in\mathbb{F}_2^n}(|\mathsf{E}_{k,n}| - \mathsf{K}_k(l,n)) - \dfrac{1}{2} & \text{if } k \preceq n \end{cases} \\
&= \begin{cases} \dfrac{|\mathsf{E}_{k,n}|}{4} + \dfrac{1}{4}\displaystyle\min_{0\leq l\leq n} \mathsf{K}_k(l,n) & \text{if } k \not\preceq n \\ \dfrac{|\mathsf{E}_{k,n}|}{4} + \dfrac{1}{4}\displaystyle\min_{0\leq l\leq n} \mathsf{K}_k(l,n) - \dfrac{1}{2} & \text{if } k \preceq n \end{cases} \\
&= \begin{cases} \dfrac{1}{4}\left(\dbinom{n}{k} + \displaystyle\min_{0\leq l\leq n} \mathsf{K}_k(l,n)\right) & \text{if } k \not\preceq n \\ \dfrac{1}{4}\left(\dbinom{n}{k} + \displaystyle\min_{0\leq l\leq n} \mathsf{K}_k(l,n) - 2\right) & \text{if } k \preceq n. \end{cases}
\end{aligned}
$$

$\square$

n \ k	2	3	4	5	6	7	8	9	10
	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 1. A lower bound of $\mathsf{NL}_k(f_\psi)$ as per Theorem 5

We have

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

Hence, $\mathsf{K}_2(l,n) = \binom{n}{2} - 2\sum_{\substack{j=0\\ j:\text{odd}}}^{2}\binom{l}{j}\binom{n-l}{2-j} = \binom{n}{2} - 2\binom{l}{1}\binom{n-l}{1} = \binom{n}{2} - 2l(n-l)$. 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 $\frac{d^2(\mathsf{K}_2(l,n))}{dl^2} = 4 > 0$. In our case, as $l = \mathsf{w_H}(a+\psi^{-1}(a))$ for $a \in \mathbb{F}_2^n$ is an integer, we have $\min_{0\le l\le n}\mathsf{K}_2(l,n)$ 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 $\min_{0\le l\le n}\mathsf{K}_2(l,n) = \binom{n}{2} - 2\frac{n-1}{2}\frac{n+1}{2} = -\frac{n-1}{2}$. Hence, combining both the cases, we have $\min_{0\le l\le n}\mathsf{K}_2(l,n) = -\lfloor\frac{n}{2}\rfloor$. Further, denote $\mathsf{NL}_k^n = \min\{\mathsf{NL}_k^n(f_\psi) | f_\psi \in \mathcal{B}_n \text{constructed as in Proposition 2}\}$.

Theorem 6. *Let $n \geq 2$ be an positive integer as in Equation 1 and $\psi \in \mathbb{S}_n$ as in Equation 2. Then*

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

Moreover, if $n = 2^m$ for $m \geq 1$, $\quad \dfrac{n(n-2)}{8} \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^in} \leq \cdots,$ *and 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 1,* $\left\lfloor\dfrac{(n+1)(n-4)+n}{8}\right\rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^in} \leq \cdots.$

Proof. Using the $\min_{0\le l\le n}\mathsf{K}_2(l,n)$ in Theorem 5 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 $\mathsf{NL}_2(f_\psi) \geq \begin{cases}\frac{n(n-2)}{8} & \text{if } n \text{ is even} \\ \frac{(n-1)^2}{8} & \text{if } n \text{ is odd,}\end{cases}$

and for $2 \preceq n$, we have $\mathsf{NL}_2(f_\psi) \geq \begin{cases}\frac{n(n-2)}{8} - \frac{1}{2} & \text{if } n \text{ is even} \\ \frac{(n-1)^2}{8} - \frac{1}{2} & \text{if } n \text{ is odd.}\end{cases}$

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 iff $2 \not\preceq n$. Hence, combining the cases, we have

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

For proof of the second part of the theorem, we apply the technique followed in the proof of [LM19, Theorem-3.14]. If $R \subseteq E$, then $\mathsf{NL}_R(f) \leq \mathsf{NL}_E(f)$. When $n = 2^m$, for a fixed integer $j \in [1,m]$, consider the set

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

It can be checked that for $x = (y,y) \in R$, $\mathsf{O}_x = \{(z,z) : z \in \mathsf{O}_y\}$. Then for a WPB $f \in \mathcal{B}_n$ satisfying Proposition 2, 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,

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

Then we have the generalised result as

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

Now 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 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,

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

Now 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

$$\mathsf{O}_x = \{(z_{n_w}, z_{n_w})(z_{n_{w-1}}, z_{n_{w-1}}) \ldots (z_{n_1}, z_{n_1}) : z_{n_w} z_{n_{w-1}} \ldots z_{n_1} \in \mathsf{O}_y\}$$

Then for a $f \in \mathcal{B}_{2n}$ satisfying Proposition 2, 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, $\mathsf{NL}_2^n(g) = \mathsf{NL}_R(f) \leq \mathsf{NL}_{\mathsf{E}_{4,2n}}(f) = \mathsf{NL}_4^{2n}(f)$. If we generalised the result,

$$\left\lfloor \frac{(n+1)(n-4)+n}{8} \right\rfloor \leq \mathsf{NL}_2^n \leq \mathsf{NL}_4^{2n} \leq \mathsf{NL}_8^{2^2 n} \leq \cdots \leq \mathsf{NL}_{2^{i+1}}^{2^i n}.$$

□

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

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

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

Corollary 1.

References

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.

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.

GM22. Agnese Gini and Pierrick Méaux. On the weightwise nonlinearity of weightwise perfectly balanced functions. *Discret. Appl. Math.*, 322:320–341, 2022.

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

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

MZD18. Sihem Mesnager, Zhengchun Zhou, and Cunsheng Ding. On the nonlinearity of boolean functions with restricted input. *Cryptography and Communications*, Mar 2018.

SM08. Pantelimon Stanica and Subhamoy Maitra. Rotation symmetric boolean functions - count and cryptographic properties. *Discret. Appl. Math.*, 156(10):1567–1580, 2008.