A unified construction of weightwise perfectly balanced Boolean functions

Qinglan ZHAO[a], Mengran LI[a], Zhixiong CHEN[b], Baodong QIN[a], Dong ZHENG[a,c]

[a] *National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121*, China*

[b] *Fujian Key Laboratory of Financial Information Processing, Putian University, Putian* 351100*, China*

[c] *School of Computer, Qinghai Normal University, Xining* 810008*, China*

Abstract

At Eurocrypt 2016, Méaux et al. presented FLIP, a new family of stream ciphers that aimed to enhance the efficiency of homomorphic encryption frameworks. Motivated by FLIP, recent research has focused on the study of Boolean functions with good cryptographic properties when restricted to subsets of the space $\mathbb{F}_2^n$. If an n-variable Boolean function has the property of balancedness when restricted to each set of vectors with fixed Hamming weight between 1 and $n-1$, it is a weightwise perfectly balanced (WPB) Boolean function. In the literature, a few algebraic constructions of WPB functions are known, in which there are some constructions that use iterative method based on functions with low degrees of 1, 2, or 4. In this paper, we generalize the iterative method and contribute a unified construction of WPB functions based on functions with algebraic degrees that can be any power of 2. For any given positive integer d not larger than m, we first provide a class of 2^m-variable Boolean functions with a degree of 2^{d-1}. Utilizing these functions, we then present a construction of 2^m-variable WPB functions $g_{m;d}$. In particular, $g_{m;d}$ includes four former classes of WPB functions as special cases when $d = 1, 2, 3, m$. When d takes other integer values, $g_{m;d}$ has never appeared before. In addition, we prove the algebraic degree of the constructed WPB functions and compare the weightwise nonlinearity of WPB functions known so far in 8 and 16 variables.

Keywords: FLIP cipher, Weightwise perfectly balancedness, Boolean function, k-weight nonlinearity, Algebraic degree, Algebraic immunity

Email address: zhaoqinglan@foxmail.com (Qinglan ZHAO)

1. Introduction

FLIP, a newly introduced family of stream ciphers, was explored in the context of homomorphic encryption by Méaux et al. at Eurocrypt 2016 [11]. The FLIP cipher has three components: the key register, the permutation generator and the filter function. The key from the key register is permuted by the permutation generated by permutation generator. Then, the permuted key is filtered by the filter function to generate the key stream. All permuted keys have the same Hamming weight, which results in the input of the filter function being limited to a subset with the same Hamming weight in FLIP. In this context, Boolean functions with good cryptographic properties when restricted to subsets of the space $\mathbb{F}_2^n$ have attracted the attention of researchers.

In 2017, Carlet et al. [2] studied the main cryptographic properties of Boolean functions with limited inputs. They showed that balancedness, nonlinearity and algebraic immunity still play an important role in resisting the corresponding attacks on the system of FLIP ciphers. In particular, when studying the balancedness of those functions on some input set E in FLIP, they considered the change of the set E so that it can be applied to more application situations and extended to a new type of functions called weightwise perfectly balanced (WPB) Boolean functions. A WPB function is balanced on each subset $E_{n,i} = \{x \in \mathbb{F}_2^n | \mathrm{wt}(x) = i\}$, where $1 \leq i \leq n-1$ and $\mathrm{wt}(x)$ is the Hamming weight of x. Since then, there have been some research results on WPB functions. These works focus on the construction or other cryptographic properties of WPB functions such as nonlinearity and algebraic immunity. Next, we list some main known results of WPB functions.

- In 2017, Carlet et al. presented the first iterative construction for WPB functions in [2]. Additionally, they introduced an upper bound on the weightwise nonlinearity of Boolean functions with constrained inputs. Later, this bound was improved by Mesnager et al. in [15] in 2019.

- In 2018, a class of 2-rotation symmetric WPB functions was proposed by Liu and Mesnager in [8], and the lower bounds on k-weight nonlinearity of these functions they constructed were presented.

- In 2019, a new class of WPB Boolean functions with optimal algebraic immunity was constructed in [17] by Tang and Liu. Based on their results, Mesnager et al. derived two concrete constructions of optimal algebraically immune WPB functions in 2022 [14].

- In 2020 and 2021, four constructions were proposed by using the iterative method to modify the support of one class of linear functions [13], two classes

of different quadratic functions [7, 13] and one class of quartic functions [18], respectively.

- In 2021, in [16], Su discussed the lower bound on the weightwise nonlinearity of WPB functions with a straightforward algebraic normal form , which first introduced in paper [2].

- In 2022, Gini and Méaux studied theoretic bounds on the maximum and minimum of weightwise nonlinearity and algorithms to compute or estimate the distribution of weightwise nonlinearity in [4]. They also presented two constructions of WPB functions with prescribed weightwise nonlinearities. In [5], Gini and Méaux constructed a 16-variable WPB function with the highest observed weightwise nonlinearity to date by using combining functions with high weightwise nonlinearity on certain subsets. Very recently, Gini and Méaux released their new research that introduced upper and lower bounds for the nonlinearity of WPB functions and gave constructions of WPB functions with prescribed nonlinearity [6]. In addition they studied the distribution of nonlinearity on the set of WPB functions. In the same year, evolutionary algorithms were utilized on discovering WPB functions with high weightwise nonlinearity for 8 variables [9, 10], while their results are limited by computing power for larger values of the number of variables.

As mentioned above, the iterative method is used to construct WPB functions in [7, 13, 18] based on different functions with low algbraic degree of 1, 2 and 4. Motivated by these works, we present a unified construction of WPB functions utilizing the iterative method based on functions with algebraic degree that can be any power of 2. Given a positive integer d, we first give a class of 2^m-variable Boolean functions $f_{m;d}$ with algebraic degree 2^{d-1} for integer $m \geq d$. After that, a construction of 2^m-variable WPB functions denoted by $g_{m;d}$ is given by modifying the support of $f_{m;d}$. For any given d, there is a class of WPB functions $g_{m;d}$ related to d. The construction includes four existing classes of functions that appeared in [2, 7, 13, 18] as special cases when $d = 1, 2, 3, m$. Finally, there is a discussion about the algebraic degree of the newly constructed WPB functions, and the algebraic immunity and k-weight nonlinearity for WPB functions on small variables are also summarized at the end.

The remainder of our paper is organized as follows. Several significant preliminaries and basic definitions of Boolean functions are provided in Section 1. Then, we construct the Boolean functions $f_{m;d}$ with low degree 2^{d-1} in Section 3. The WPB functions $g_{m;d}$ are given by modifying the functions $f_{m;d}$ defined in Section 4. The cryptographic properties of the constructed WPB function, including k-weight non-

linearity and other important ones are summarized in this section. Finally, Section 5 summarizes the paper and continues the prospects.

2. Perliminaries

Let $\mathbb{F}_2$ be a binary finite field with two elements 0 and 1, and let $\mathbb{F}_2^n$ be an n-dimension vector space on $\mathbb{F}_2$. We specify that an n-dimensional vector $x \in \mathbb{F}_2^n$ is denoted by $x = (x_1, x_2, \ldots, x_n)$ in the whole paper, and denote $\mathbf{1}_n = (1, 1, \ldots, 1) \in \mathbb{F}_2^n$, $\mathbf{0}_n = (0, 0, \ldots, 0) \in \mathbb{F}_2^n$. Moreover, the number of elements contained in $\mathrm{supp}(x) = \{1 \leq i \leq n | x_i = 1\}$ is named as the Hamming weight of x, which can be denoted by $\mathrm{wt}(x)$. For any integer $k \in [0, n]$, we define a subset of $\mathbb{F}_2^n$ as

$$E_{n,k} = \{x \in \mathbb{F}_2^n | \mathrm{wt}(x) = k\}. \tag{1}$$

Clearly, the union of all $E_{n,k}$ for $0 \leq k \leq n$ is $\mathbb{F}_2^n$.

An n-variable Boolean function f is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$. Its support is made up of all the vectors $x \in \mathbb{F}_2^n$ which satisfy $f(x) = 1$, i.e., $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. Likewise, $\mathrm{zeros}(f)$ is described as the set $\{x \in \mathbb{F}_2^n | f(x) = 0\}$. The number of vectors x in the $\mathrm{supp}(f)$ is regarded as the Hamming weight of Boolean function. A function $f \in \mathcal{B}_n$ is determined to be balanced only when $\mathrm{wt}(f) = 2^{n-1}$. The set of all the n-variable Boolean functions is denoted by $\mathcal{B}_n$.

For any $f \in \mathcal{B}_n$, it can be uniquely described by its algebraic normal form (ANF) as follows:

$$f(x) = \bigoplus_{\mu \in \mathbb{F}_2^n} c_\mu x^\mu, \tag{2}$$

where $c_\mu \in \mathbb{F}_2$, $\mu = (\mu_1, \mu_2, \ldots, \mu_n) \in \mathbb{F}_2^n$ and $x^\mu = x_1^{\mu_1} x_2^{\mu_2} \cdots x_n^{\mu_n}$.

The algebraic degree of the function f is equal to the maximum number of variables of a monomial with nonzero coefficient in its algebraic normal form (refer to (2)), which can be simply expressed as

$$\deg(f) = \max_{\mu \in \mathbb{F}_2^n} \{\mathrm{wt}(\mu) | c_\mu = 1\} \text{ if } f \text{ is not null, } 0 \text{ otherwise.} \tag{3}$$

As a special case, an affine function is one whose algebraic degree $\deg(f)$ is equal to or less than 1, and a linear function is an affine function whose constant term is zero.

The algebraic immunity is a property that can measure the capacity of the Boolean function to defend against algebraic attack.

Definition 1. ([12]) The algebraic immunity of $f \in \mathcal{B}_n$ can be expressed as

$$AI(f) = \min \{\deg(h) | f \cdot h = 0 \text{ or } (f \oplus 1) \cdot h = 0,\ 0 \neq h \in \mathcal{B}_n\}.$$

If $AI(f) = \left\lceil \frac{n}{2} \right\rceil$, we say that f has the optimal algebraic immunity([3]).

In the case where the inputs of $f \in \mathcal{B}_n$ are restrained to vectors with fixed Hamming weight k, there is a new description about the support, zero set and Hamming weight. As $E_{n,k}$ is mentioned in (1) and $0 \leq k \leq n$, the k-weight support is defined as $\mathrm{supp}_k(f) = \{x \in E_{n,k} | f(x) = 1\}$. Similarly to the description on the whole vector space, we can denote $\mathrm{zeros}_k(f) = \{x \in E_{n,k} | f(x) = 0\}$. The k-weight of f can also be described as

$$\mathrm{wt}_k(f) = |\mathrm{supp}_k(f)|. \tag{4}$$

Definition 2. For every integer $1 \leq k \leq n-1$, if the k-weight of $f \in \mathcal{B}_n$ satisfies $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$ and $f(\mathbf{0}_n) \neq f(\mathbf{1}_n)$, f is refered to as a weightwise perfectly balanced function.

In order to keep globally balaced for the function which has already satisfied the condition of $\mathrm{wt}_k(f) = \frac{1}{2}\binom{n}{k}$ with $1 \leq k \leq n-1$, there must be a difference between $f(\mathbf{0}_n)$ and $f(\mathbf{1}_n)$. Generally, in this paper we always discuss Boolean functions on 2^m variables with integer $m > 0$ since n-variable WPB Boolean functions arise only for n is a power of 2, as shown in [2] .

When E is a subset of $\mathbb{F}_2^n$, the smallest Hamming distance between a Boolean function f and affine function with limited inputs on E can be described by the restricted nonlinearity denoted by $\mathrm{NL}_E(f)$, which determines the ability to defend the affine approximation attack. Next, we introduce two known propositions about $\mathrm{NL}_E(f)$.

Proposition 1. *([2]) For every subset $E \subseteq \mathbb{F}_2^n$ and $f \in \mathcal{B}_n$, we obtain the following conclusion:*

$$\mathrm{NL}_E(f) = \frac{|E|}{2} - \frac{1}{2}\max_{\alpha \in \mathbb{F}_2^n} |\sum_{x \in E} (-1)^{f(x) \oplus \alpha \cdot x}|.$$

Proposition 2. *([2]) For every subset $E \subseteq \mathbb{F}_2^n$ and $f \in \mathcal{B}_n$, and $\lfloor \eta \rfloor$ is the maximum integer no larger than η, it is followed that*

$$\mathrm{NL}_E(f) \leq \left\lfloor \frac{|E|}{2} - \frac{\sqrt{|E|}}{2} \right\rfloor.$$

Note that $\mathrm{NL}_E(f)$ is the same as the classic one studied in the whole vector space if $E = \mathbb{F}_2^n$. Especially, according to the introduction of $\mathrm{NL}_E(f)$ above, we designate the k-weight nonlinearity of f as the weightwise nonlinearity for $E = E_{n,k}$ with $1 \leq k \leq n-1$, which is denoted by $\mathrm{NL}_{E_{n,k}}(f)$. In the following, in case of no confusion, it will be represented by $\mathrm{NL}_k(f)$.

3. A class of Boolean functions with degree 2^{d-1}

During this section, we will give a class of 2^m-variable functions which are going to be applied to construct WPB functions in the following section. From now on, for a vector $x = (x_1, x_2, \ldots, x_{2^m}) \in \mathbb{F}_2^{2^m}$, we denote $x' = (x_1, x_3, \ldots, x_{2^m-1})$, $x'' = (x_2, x_4, \ldots, x_{2^m}) \in \mathbb{F}_2^{2^{m-1}}$.

Assuming that d is a positive integer, for any integer $m \geq d$, we define $f_{m;d} \in \mathcal{B}_{2^m}$ with the form

$$f_{m;d}(x) = \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{m-t+1}}. \tag{5}$$

From the ANF of $f_{m;d}$, we can easily get $\deg(f_{m;d}) = 2^{d-1}$.

Example 1. The ANF of $f_{m;d}$ are listed if $d = 1, 2$, and 3 as follows:

- $f_{m;1}(x) = x_1 \oplus x_2 \oplus \ldots \oplus x_{2^{m-1}}, \quad m \geq 1.$
- $f_{m;2}(x) = x_1 \oplus x_2 \oplus \ldots \oplus x_{2^{m-1}} \oplus x_1 x_{1+2^{m-1}} \oplus x_2 x_{2+2^{m-1}} \oplus \ldots \oplus x_{2^{m-2}} x_{3\cdot 2^{m-2}}, \quad m \geq 2.$
- $f_{m;3}(x) = \bigoplus_{i=1}^{2^{m-1}} x_i \oplus \bigoplus_{i=1}^{2^{m-2}} x_i x_{i+2^{m-1}} \oplus \bigoplus_{i=1}^{2^{m-3}} x_i x_{i+2^{m-2}} x_{i+2^{m-1}} x_{i+3\cdot 2^{m-2}}, \quad m \geq 3.$

Obviously, $f_{m;1}(x)$, $f_{m;2}(x)$ and $f_{m;3}(x)$, as special cases of $f_{m;d}$ when $d = 1, 2, 3$, have been used as low-degree functions to construct WPB functions in [7, 13, 18] and their k-weight have been analyzed in these three papers respectively. Now we will discuss the k-weight of $f_{m;d}$ for any positive integer d, which is a little more complicated. Before our discussion, we will introduce two known lemmas of combinatorial numbers that will be utilized in the subsequent proof.

Lemma 1. *(Pascal's rule) Assuming m and n are two nonnegative integers, we have*

$$\binom{m}{n} = \binom{m-1}{n} + \binom{m-1}{n-1}.$$

Lemma 2. *Chu-Vandermonde's indentity, adapted from [1], Eq.(7.16)) Assuming a, b and n are three nonnegative integers, the following is true.*

$$\binom{a+b}{n} = \sum_{i=0}^{n} \binom{a}{n} \binom{b}{n-i}.$$

Next we discuss the properties of functions $f_{m;d}(x)$ defined in (5) according to the value of m.

Lemma 3. *Let $f_{m;d}(x)$ be defined in (5). We have*

$$\begin{cases} f_{d;d}(x) = f_{d-1;d-1}(x') \oplus f_{d-1;d-1}(x'') \oplus x_1 x_3 \dots x_{2^d-1}, & \text{if } m = d \geq 1, \\ f_{m;d}(x) = f_{m-1;d}(x') \oplus f_{m-1;d}(x''), & \text{if } m > d \geq 1. \end{cases} \tag{6}$$

Proof. (1) Firstly we consider the case of $m = d$. For a given positive integer d, we have the following equation,

$$\begin{aligned} & f_{d-1;d-1}(x_1, x_3, \dots, x_{2^d-1}) \oplus f_{d-1;d-1}(x_2, x_4, \dots, x_{2^d}) \\ &= \bigoplus_{t=1}^{d-1} \bigoplus_{i=1}^{2^{d-t-1}} \prod_{s=0}^{2^{t-1}-1} x_{(2i-1)+s\cdot 2^{d-t+1}} \oplus \bigoplus_{t=1}^{d-1} \bigoplus_{i=1}^{2^{d-t-1}} \prod_{s=0}^{2^{t-1}-1} x_{(2i)+s\cdot 2^{d-t+1}} \\ &= \bigoplus_{t=1}^{d-1} \bigoplus_{i=1}^{2^{d-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{d-t+1}}. \end{aligned}$$

Therefore it can be seen that

$$\begin{aligned} f_{d;d}(x_1, x_2, \dots, x_{2^d}) &= \bigoplus_{t=1}^{d-1} \bigoplus_{i=1}^{2^{d-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{d-t+1}} \oplus \bigoplus_{t=d}^{d} \bigoplus_{i=1}^{2^{d-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{d-t+1}} \\ &= \bigoplus_{t=1}^{d-1} \bigoplus_{i=1}^{2^{d-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{d-t+1}} \oplus \prod_{s=0}^{2^{d-1}-1} x_{1+s\cdot 2} \\ &= f_{d-1;d-1}(x') \oplus f_{d-1;d-1}(x'') \oplus x_1 x_3 \dots x_{2^d-1}. \end{aligned}$$

(2) If $m > d$, from the definition of $f_{m;d}(x)$, we have

$$\begin{aligned} & f_{m-1;d}(x') \oplus f_{m-1;d}(x'') \\ &= \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t-1}} \prod_{s=0}^{2^{t-1}-1} x_{(2i-1)+s\cdot 2^{m-t+1}} \oplus \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t-1}} \prod_{s=0}^{2^{t-1}-1} x_{(2i)+s\cdot 2^{m-t+1}} \\ &= \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t}} \prod_{s=0}^{2^{t-1}-1} x_{i+s\cdot 2^{m-t+1}} \\ &= f_{m;d}(x_1, x_2, \dots, x_{2^m}) \\ &= f_{m;d}(x). \end{aligned}$$

The proof is finished. □

By Lemma 3, we can easily get the conclusion that in order to make $f_{m;d}(x) = 1$, there is an only way to do it, that is, to ensure the value of $f_{m-1;d}(x')$ is not equal to $f_{m-1;d}(x'')$ for $m > d$. Therefore, the k-weight support of $f_{m;d}(x)$ for $m > d$ is

$$\begin{aligned}\mathrm{supp}_k(f_{m;d}(x)) = &\bigcup_{a=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x' \in \mathrm{supp}_a(f_{m-1;d}), x'' \in \mathrm{zeros}_{k-a}(f_{m-1;d})\right\} \cup \\ &\bigcup_{a=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x'' \in \mathrm{supp}_{k-a}(f_{m-1;d}), x' \in \mathrm{zeros}_a(f_{m-1;d})\right\}.\end{aligned} \tag{7}$$

Lemma 4. *If $m > d$, the k-weight of $f_{m;d}(x)$ defined in (5) satisfies*

$$\mathrm{wt}_k(f_{m;d}) = 2\sum_{a=0}^{k} \mathrm{wt}_a(f_{m-1;d}) \left[\binom{2^{m-1}}{k-a} - \mathrm{wt}_{k-a}(f_{m-1;d})\right], \tag{8}$$

where $0 \le k \le 2^m$.

Proof. Assume that $k - a = b$. By (7), we have

$$\begin{aligned}\mathrm{supp}_k(f_{m;d}) = &\bigcup_{a=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x' \in \mathrm{supp}_a(f_{m-1;d}), x'' \in \mathrm{zeros}_{k-a}(f_{m-1;d})\right\} \cup \\ &\bigcup_{b=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x'' \in \mathrm{supp}_b(f_{m-1;d}), x' \in \mathrm{zeros}_{k-b}(f_{m-1;d})\right\} \\ = &\bigcup_{a=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x' \in \mathrm{supp}_a(f_{m-1;d}), x'' \in \mathrm{zeros}_{k-a}(f_{m-1;d})\right\} \cup \\ &\bigcup_{a=0}^{k} \left\{x \in \mathbb{F}_2^{2^m} | x'' \in \mathrm{supp}_a(f_{m-1;d}), x' \in \mathrm{zeros}_{k-a}(f_{m-1;d})\right\},\end{aligned}$$

By the k-weight definition in (4), it follows that

$$\begin{aligned}\mathrm{wt}_k(f_{m;d}) &= |\mathrm{supp}_k(f_{m;d})| \\ &= 2\sum_{a=0}^{k} \mathrm{wt}_a(f_{m-1;d}) \left[\binom{2^{m-1}}{k-a} - \mathrm{wt}_{k-a}(f_{m-1;d})\right].\end{aligned}$$

The proof is finished. □

Corollary 1. *Let $f_{d;d}(x_1, x_2, \ldots, x_{2^d})$ be defined in (5). We have the following conclusions.*

(1-1) When $d \geq 1$, $f_{d;d}(\mathbf{1}_{2^d}) = 1$ and $f_{d;d}(\mathbf{0}_{2^d}) = 0$.

(1-2) When $x' = \mathbf{1}_{2^{d-1}}$ and $d \geq 2$, $f_{d;d}(x) = 1$ if and only if $f_{d-1;d-1}(x'') = 1$.

(1-3) When $x' \neq \mathbf{1}_{2^{d-1}}$ and $d \geq 2$, $f_{d;d}(x) = 1$ if and only if $f_{d-1;d-1}(x') = f_{d-1;d-1}(x'') \oplus 1$.

Proof. It can be proved by Lemma 3 easily when $m = d$. □

For the sake of the verification of the k-weight of the function $f_{m;d}$ which is described in (5) when $m = d$, from Corollary 1, we give the following two equations about $f_{d;d}(x_1, x_2, \ldots, x_{2^d})$:

$$|\left\{x \in \text{zeros}(f_{d;d}) | \text{wt}(x) = 2^d\right\}| = |\left\{x \in \text{supp}(f_{d;d}) | \text{wt}(x) = 0\right\}| = 0 \tag{9}$$

and

$$|\left\{x \in \text{supp}(f_{d;d}) | \text{wt}(x) = 2^d\right\}| = |\left\{x \in \text{zeros}(f_{d;d}) | \text{wt}(x) = 0\right\}| = 1. \tag{10}$$

Now the k-weight of $f_{m;d}(x)$ defined in (5) is given as follows.

Theorem 1. *The k-weight of $f_{m;d}(x)$ defined in (5) is*

$$\text{wt}_k(f_{m;d}) = \begin{cases} \frac{1}{2}\binom{2^m}{k}, & k \not\equiv 0 (\text{mod } 2^d), \\ \frac{1}{2}\binom{2^m}{k} - \frac{(-1)^{\frac{k}{2^d}}}{2}\binom{2^{m-d}}{\frac{k}{2^d}}, & k \equiv 0 (\text{mod } 2^d), \end{cases} \tag{11}$$

where $0 \leq k \leq 2^m$.

Proof. Our proof will be accomplished based on mathematical induction on m in two cases (1) $m = d$ and (2) $m > d$.

(1) To begin with we focus on the first case where $m = d$. In [2], Carlet et al. introduced a class of WPB functions which is the same class as $f_{d;d}$, and proved k-weight of $f_{d;d}(x)$ satisfying the equation in (11). The detailed proof can be found in [2].

(2) Now we start to prove that (11) holds for another case with $m > d$ for a given d. Let us assume (11) is true for $m - 1$, that is to say,

$$\text{wt}_k(f_{m-1;d}) = \begin{cases} \frac{1}{2}\binom{2^{m-1}}{k}, & k \not\equiv 0 (\text{mod } 2^d), \\ \frac{1}{2}\binom{2^{m-1}}{k} - \frac{(-1)^{\frac{k}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k}{2^d}}, & k \equiv 0 (\text{mod } 2^d), \end{cases} \tag{12}$$

where $0 \le k \le 2^{m-1}$. According to the value of k, the value of $\mathrm{wt}_k(f_{m;d})$ for $0 \le k \le 2^m$ can be considered in the following two cases.

(2-1) When $k \not\equiv 0 (\mathrm{mod}\ 2^d)$, we can get that $k-a \not\equiv 0 (\mathrm{mod}\ 2^d)$ when $a \equiv 0 (\mathrm{mod}\ 2^d)$, or $a \not\equiv 0 (\mathrm{mod}\ 2^d)$ when $k-a \equiv 0 (\mathrm{mod}\ 2^d)$. So we have

$$
\begin{aligned}
\mathrm{wt}_k(f_{m;d}) &= 2\sum_{a=0}^{k} \mathrm{wt}_a(f_{m-1;d}) \left[\binom{2^{m-1}}{k-a} - \mathrm{wt}_{k-a}(f_{m-1;d}) \right] \\
&= 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \frac{1}{2}\binom{2^{m-1}}{a} \left[\binom{2^{m-1}}{k-a} - \frac{1}{2}\binom{2^{m-1}}{k-a} \right] + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \left[\frac{1}{2}\binom{2^{m-1}}{a} - \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{a}{2^d}} \right] \frac{1}{2}\binom{2^{m-1}}{k-a} + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\equiv 0(\mathrm{mod}\ 2^d)}} \frac{1}{2}\binom{2^{m-1}}{a} \left[\binom{2^{m-1}}{k-a} - \frac{1}{2}\binom{2^{m-1}}{k-a} + \frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k-a}{2^d}} \right] \\
&= 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \frac{1}{2}\binom{2^{m-1}}{a} \frac{1}{2}\binom{2^{m-1}}{k-a} + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \left[\frac{1}{2}\binom{2^{m-1}}{a} \frac{1}{2}\binom{2^{m-1}}{k-a} - \frac{1}{2}\binom{2^{m-1}}{k-a} \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{a}{2^d}} \right] + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\equiv 0(\mathrm{mod}\ 2^d)}} \left[\frac{1}{2}\binom{2^{m-1}}{a} \frac{1}{2}\binom{2^{m-1}}{k-a} + \frac{1}{2}\binom{2^{m-1}}{a} \frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k-a}{2^d}} \right] \\
&= 2\sum_{a=0}^{k} \frac{1}{2}\binom{2^{m-1}}{a} \frac{1}{2}\binom{2^{m-1}}{k-a} \\
&= \frac{1}{2}\binom{2^m}{k},
\end{aligned}
$$

where the first, second, and last equations is true because of (8), (12) and Lemma 2

, respectively.

(2-2) When $k \equiv 0 (\mathrm{mod}\ 2^d)$, we can get that $a \equiv 0 (\mathrm{mod}\ 2^d)$ if and only if $k-a \equiv 0 (\mathrm{mod}\ 2^d)$, or $a \not\equiv 0 (\mathrm{mod}\ 2^d)$ if and only if $k-a \not\equiv 0 (\mathrm{mod}\ 2^d)$. Hence we have

$$
\begin{aligned}
\mathrm{wt}_k(f_{m;d}) &= 2\sum_{a=0}^{k} \mathrm{wt}_a(f_{m-1;d}) \left[\binom{2^{m-1}}{k-a} - \mathrm{wt}_{k-a}(f_{m-1;d}) \right] \\
&= 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \frac{1}{2}\binom{2^{m-1}}{a} \left[\binom{2^{m-1}}{k-a} - \frac{1}{2}\binom{2^{m-1}}{k-a} \right] + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\equiv 0(\mathrm{mod}\ 2^d)}} \left[\frac{1}{2}\binom{2^{m-1}}{a} - \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-1-d}}{\frac{a}{2^d}} \right] \left[\frac{1}{2}\binom{2^{m-1}}{k-a} + \frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-1-d}}{\frac{k-a}{2^d}} \right] \\
&= 2 \sum_{\substack{0\le a\le k \\ a\not\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\not\equiv 0(\mathrm{mod}\ 2^d)}} \frac{1}{2}\binom{2^{m-1}}{a}\frac{1}{2}\binom{2^{m-1}}{k-a} + \\
&\quad 2 \sum_{\substack{0\le a\le k \\ a\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\equiv 0(\mathrm{mod}\ 2^d)}} \left[\frac{1}{2}\binom{2^{m-1}}{a}\frac{1}{2}\binom{2^{m-1}}{k-a} + \frac{1}{2}\binom{2^{m-1}}{a}\frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k-a}{2^d}} - \right. \\
&\quad \left. \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{a}{2^d}}\frac{1}{2}\binom{2^{m-1}}{k-a} - \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{a}{2^d}}\frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k-a}{2^d}} \right] \\
&= 2\sum_{a=0}^{k} \frac{1}{2}\binom{2^{m-1}}{a}\frac{1}{2}\binom{2^{m-1}}{k-a} - 2 \sum_{\substack{0\le a\le k \\ a\equiv 0(\mathrm{mod}\ 2^d) \\ k-a\equiv 0(\mathrm{mod}\ 2^d)}} \frac{(-1)^{\frac{a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{a}{2^d}}\frac{(-1)^{\frac{k-a}{2^d}}}{2}\binom{2^{m-d-1}}{\frac{k-a}{2^d}} \\
&= \frac{1}{2}\binom{2^m}{k} - \frac{(-1)^{\frac{k}{2^d}}}{2}\binom{2^{m-d}}{\frac{k}{2^d}},
\end{aligned}
$$

where (8), (12) and Lemma 2 support the first, second, and last equations, respectively.

The proof is finished. □

From Theorem 1, we see that $f_{m;d}(x) \in \mathcal{B}_{2^m}$ defined in (5) are not WPB functions.

In the next section, we will use this class of functions to construct 2^m-variable WPB functions.

4. WPB Boolean functions

According to the discussion in Section 3, we give a modification on the support of $f_{m;d}(x) \in \mathcal{B}_{2^m}$ defined in (5) to construct the WPB functions. We also demonstrate the algebraic degree of the new constructed WPB functions. At the end of this section the k-weight nonlinearity and algebraic immunity for functions in a small number of variables are listed.

4.1. The construction of WPB functions

Construction 1. *Let $d \geq 1$ be a given integer. For any positive integer m, we define Boolean function $g_{m;d}(x) \in \mathcal{B}_{2^m}$ with the form*

$$g_{m;d}(x) = \begin{cases} f_{m;m}(x), & \text{if } \ m \leq d, \\ f_{m;d}(x) \oplus g_{m-d;d}(\bar{x}) \prod_{i=1}^{\sum_{t=1}^{d} 2^{m-t}} (x_i \oplus x_{i+2^{m-d}} \oplus 1), & \text{if } \ m > d, \end{cases}$$

where $f_{m;m}(x)$ and $f_{m;d}(x) \in \mathcal{B}_{2^m}$ are of the form in (5), and $x = (x_1, x_2, \ldots, x_{2^m}) \in \mathbb{F}_2^{2^m}$, $\bar{x} = (x_1, x_2, \ldots, x_{2^{m-d}}) \in \mathbb{F}_2^{2^{m-d}}$.

For convenience, from now on we denote $\bar{x} = (x_1, x_2, \ldots, x_{2^{m-d}}) \in \mathbb{F}_2^{2^{m-d}}$ if $m > d$.

Note that 2^m-variable Boolean functions $\prod_{i=1}^{\sum_{t=1}^{d} 2^{m-t}} (x_i \oplus x_{i+2^{m-d}} \oplus 1) = 1$ if and only if $x_j = x_{j+2^{m-d}} = x_{j+2^{m-d+1}} = \cdots = x_{j+\sum_{t=1}^{d} 2^{m-t}}$ for all $1 \leq j \leq 2^{m-d}$.

Lemma 5. *The k-weight support of $g_{m;d}(x)$ defined in Construction 1 for $m > d$ can be described as*

$$\mathrm{supp}_k(g_{m;d}) = \begin{cases} \mathrm{supp}_k(f_{m;d}), & k \not\equiv 0 (\mathrm{mod}\ 2^d), \\ \mathrm{supp}_k(f_{m;d}) \cup \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d}) \in \mathbb{F}_2^{2^m} | \bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\} \backslash & \\ \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d}) \in \mathbb{F}_2^{2^m} | \bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}), \mathrm{wt}(\bar{x}) \ \textit{is odd}\}, & k \equiv 0 (\mathrm{mod}\ 2^d), \end{cases}$$

where $0 \leq k \leq 2^m$.

Proof. According to the value of k, here are two cases on the k-weight support of the function $g_{m;d}(x)$, which are described as follows.

(1) When $k \not\equiv 0 (\mathrm{mod}\ 2^d)$, we have

$$\begin{aligned}\mathrm{supp}_k(g_{m;d}) &= \mathrm{supp}_k(f_{m;d}) \cup \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\}\backslash \\ &\quad \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}), f_{m;d}(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d}) = 1\} \\ &= \mathrm{supp}_k(f_{m;d}),\end{aligned}$$

where the second equation is true because it is easy to get the conclusion that $\frac{k}{2^d}$ is not an integer and the set $\{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\}$ is empty when $k \not\equiv 0 (\mathrm{mod}\ 2^d)$.

(2) When $k \equiv 0 (\mathrm{mod}\ 2^d)$, we have

$$\begin{aligned}\mathrm{supp}_k(g_{m;d}) &= \mathrm{supp}_k(f_{m;d}) \cup \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\}\backslash \\ &\quad \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}), f_{m;d}(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d}) = 1\} \\ &= \mathrm{supp}_k(f_{m;d}) \cup \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\}\backslash \\ &\quad \{(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d})|\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}), \mathrm{wt}(\bar{x}) \text{ is odd}\},\end{aligned}$$

where the last equation is supported by the following conlusion:

$$\begin{aligned}f_{m;d}(\underbrace{\bar{x}, \bar{x}, \ldots, \bar{x}}_{d}) &= \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t}} x_i x_{i+2^{m-t+1}} x_{i+2\cdot 2^{m-t+1}} \cdots x_{i+(2^{t-1}-1)\cdot 2^{m-t+1}} \\ &= \bigoplus_{t=1}^{d} \bigoplus_{i=1}^{2^{m-t}} x_i \\ &= \bigoplus_{i=1}^{2^{m-d}} x_i \\ &\equiv \mathrm{wt}(\bar{x}) (\mathrm{mod}\ 2).\end{aligned}$$

The proof is finished. □

Corollary 2. *If $m > d$, the k-weight of $g_{m;d}(x)$ defined in Construction 1 is*

$$\mathrm{wt}_k(g_{m;d}) = \begin{cases} \mathrm{wt}_k(f_{m;d}), & k \not\equiv 0 (\mathrm{mod}\ 2^d), \\ \mathrm{wt}_k(f_{m;d}) + \mathrm{wt}_{\frac{k}{2^d}}(g_{m-d;d}) - & \\ 2|\{\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}) | \mathrm{wt}(\bar{x}) \ \textit{is odd}\}|, & k \equiv 0 (\mathrm{mod}\ 2^d), \end{cases} \tag{13}$$

where $0 \le k \le 2^m$ and $\bar{x} = (x_1, x_2, \ldots, x_{2^{m-d}}) \in \mathbb{F}_2^{2^{m-d}}$.

Theorem 2. *$g_{m;d} \in \mathcal{B}_{2^m}$ defined in Construction 1 is a 2^m-variable WPB function.*

Proof. Our proof will be accomplished based on the mathematical induction on m.

From the result of k-weight in Theorem 1, firstly, the fact that $g_{1;d}$ and $g_{2;d}$ are WPB functions is obvious. Moreover, we can see that the proof of the k-weight of $g_{m;d}$ for the case of $1 \le m \le d$ is as same as the proof of $f_{m;d}$ when $m = d$ in Theorem 1. Therefore, when $1 \le m \le d$, the function $g_{m;d}$ is WPB since $\mathrm{wt}_k(g_{m;d}) = \frac{1}{2}\binom{2^m}{k}$.

Next, we assume that $g_{m-d;d}(\bar{x})$ is a WPB function for $m > d$, i.e. $\mathrm{wt}_0(g_{m-d;d}) = 0$, $\mathrm{wt}_{2^{m-d}}(g_{m-d;d}) = 1$, and

$$\mathrm{wt}_k(g_{m-d;d}) = \frac{1}{2}\binom{2^{m-d}}{k}, \tag{14}$$

where $1 \le k \le 2^{m-d} - 1$, .

In what follows, for $m > d$, we calculate the k-weight of $g_{m;d}(x)$ defined in Construction 1 with $0 \le k \le 2^m$.

(1) If $k \not\equiv 0 (\mathrm{mod}\ 2^d)$, by (13), we have

$$\mathrm{wt}_k(g_{m;d}) = \mathrm{wt}_k(f_{m;d}) = \frac{1}{2}\binom{2^m}{k}.$$

(2) If $k \equiv 0 (\mathrm{mod}\ 2^d)$, by (13), the k-weight of $g_{m;d}(x)$ is represented as

$$\mathrm{wt}_k(g_{m;d}) = \mathrm{wt}_k(f_{m;d}) + \mathrm{wt}_{\frac{k}{2^d}}(g_{m-d;d}) - 2|\{\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}) | \mathrm{wt}(\bar{x}) \text{ is odd}\}|.$$

Now we discuss the value of $\mathrm{wt}_k(g_{m;d})$ according to the value of k.

(2-1) If $1 \le k \le 2^m - 1$ and $\frac{k}{2^d}$ is odd, then we get

$$\begin{aligned} \mathrm{wt}_k(g_{m;d}) &= \mathrm{wt}_k(f_{m;d}) + \mathrm{wt}_{\frac{k}{2^d}}(g_{m-d;d}) - 2|\mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})| \\ &= \frac{1}{2}\binom{2^m}{k} - \frac{(-1)^{\frac{k}{2^d}}}{2}\binom{2^{m-d}}{\frac{k}{2^d}} + \frac{1}{2}\binom{2^{m-d}}{\frac{k}{2^d}} - 2 \times \frac{1}{2}\binom{2^{m-d}}{\frac{k}{2^d}} \\ &= \frac{1}{2}\binom{2^m}{k}, \end{aligned}$$

where the first equation is true as we can get that $\{\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d})\}$ is actually equal to $\{\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}) | \mathrm{wt}(\bar{x}) \text{ is odd}\}$ due to the condition that $\frac{k}{2^d}$ is odd. Furthermore, (11) and (14) support the second equation and the condition that $\frac{k}{2^d}$ is odd also supports the last equation.

(2-2) If $1 \leq k \leq 2^m - 1$ and $\frac{k}{2^d}$ is even, we have

$$\begin{aligned}\mathrm{wt}_k(g_{m;d}) &= \mathrm{wt}_k(f_{m;d}) + \mathrm{wt}_{\frac{k}{2^d}}(g_{m-d;d}) \\ &= \frac{1}{2}\binom{2^m}{k} - \frac{(-1)^{\frac{k}{2^d}}}{2}\binom{2^{m-d}}{\frac{k}{2^d}} + \frac{1}{2}\binom{2^{m-d}}{\frac{k}{2^d}} \\ &= \frac{1}{2}\binom{2^m}{k},\end{aligned}$$

Since $\frac{k}{2^d}$ is even, we can get $\left\{\bar{x} \in \mathrm{supp}_{\frac{k}{2^d}}(g_{m-d;d}) | \mathrm{wt}(\bar{x}) \text{ is odd}\right\} = \phi$, the first equation is true. Furthermore, (11) and (14) support the second equation and the last equation holds for $\frac{k}{2^d}$ is even .

(2-3) If $k = 0$, we get $\mathrm{wt}_0(f_{m;d}) = \frac{1}{2}\binom{2^m}{0} - \frac{(-1)^0}{2}\binom{2^{m-d}}{0} = 0$ by Theorem 1, and $\mathrm{wt}_0(g_{m-d;d}) = 0$ by (14). Hence we have

$$\mathrm{wt}_0(g_{m;d}) = \mathrm{wt}_0(f_{m;d}) + \mathrm{wt}_0(g_{m-d;d}) = 0.$$

(2-4) If $k = 2^m$, which implies $\frac{k}{2^d} = 2^{m-d}$ is even when $m > d$, by Theorem 1, we have $\mathrm{wt}_{2^m}(f_{m;d}) = \frac{1}{2}\binom{2^m}{2^m} - \frac{(-1)^{2^{m-d}}}{2}\binom{2^{m-d}}{2^{m-d}} = 0$ and $\mathrm{wt}_{2^{m-d}}(g_{m-d;d}) = 1$. Then we get

$$\mathrm{wt}_{2^m}(g_{m;d}) = \mathrm{wt}_{2^m}(f_{m;d}) + \mathrm{wt}_{2^{m-d}}(g_{m-d;d}) - 2|\left\{\mathrm{supp}_{2^{m-d}}(g_{m-d;d}) | \mathrm{wt}(\bar{x}) \text{ is odd}\right\}| = 1.$$

In summary, by the definition of the WPB functions, we get that $g_{m;d}(x)$ defined in Construction 1 is WPB. □

Remark 1. The functions $g_{m;d}$ we defined in Construction 1 are WPB functions with unified structure including four special cases constructed in the previously published papers. Specifically, if $d = 1$, we can check $g_{m;1}$ in Construction 1 is the WPB function f_m defined by Theorem 4 in [13]; if $d = 2$, $g_{m;2}$ is the function $g_{2^{q+2}}$ defined by (9) in [7]; and if $d = 3$, $g_{m;3}$ we proposed is equal to the g_m defined by (11) in [18]. In addition, if d equals to m, the function $g_{m;m}$ we defined has the same form as the function given in [16] which first appeared in [2]. If d takes the other values, $g_{m;d}$ defined in Construction 1 represents new classes of 2^m-variable WPB functions that have never been noted.

4.2. The algebraic degree of WPB function

Theorem 3. *The algebraic degree of the $g_{m;d} \in \mathcal{B}_{2^m}$ defined as Construction 1 is*

$$\deg(g_{m;d}) = \begin{cases} 2^m - 2^{d-1}, & a = 0, \\ 2^m - 2^{a-1}, & 1 \le a \le d-1, \end{cases} \tag{15}$$

where $m \equiv a \pmod d$, $0 \le a \le d-1$.

Proof. Our proof will be accomplished based on the mathematical induction on m.

(1)Firstly we consider the case of $1 \le m \le d$. The proof of algebraic degree of $g_{m;d}$ for $1 \le m \le d$ has been given in [2].

(2) Now, let us prove that (15) holds for $m > d$. Assuming (15) holds for $m-d$, it is followed

$$\deg(g_{m-d;d}) = \begin{cases} 2^{m-d} - 2^{d-1}, & a = 0, \\ 2^{m-d} - 2^{a-1}, & 1 \le a \le d-1, \end{cases} \tag{16}$$

where $m \equiv a \pmod d$, $0 \le a \le d-1$, since $m - d \equiv m \equiv a \pmod d$.

Thereupon, by Construction 1, we have

$$\begin{aligned} \deg(g_{m;d}) &= \max\{\deg(f_{m;d}), \deg(g_{m-d;d}) + \deg(\prod_{i=1}^{\sum_{t=1}^{d} 2^{m-t}} (x_i \oplus x_{i+2^{m-d}} \oplus 1))\} \\ &= \deg(g_{m-d;d}) + \deg(\prod_{i=1}^{\sum_{t=1}^{d} 2^{m-t}} (x_i \oplus x_{i+2^{m-d}} \oplus 1)) \\ &= \deg(g_{m-d;d}) + (2^d - 1) \times 2^{m-d} \\ &= \begin{cases} 2^{m-d} - 2^{d-1} + 2^m - 2^{m-d}, & a = 0, \\ 2^{m-d} - 2^{a-1} + 2^m - 2^{m-d}, & 1 \le a \le d-1, \end{cases} \\ &= \begin{cases} 2^m - 2^{d-1}, & a = 0, \\ 2^m - 2^{a-1}, & 1 \le a \le d-1, \end{cases} \end{aligned}$$

where $m \equiv a \pmod d$ and the second equation is true since $\deg(f_{m;d}) = 2^{d-1}$ for $m > d$.

The proof is finished.

□

4.3. The k-weight nonlinearity and algebraic immunity of WPB function

In what follows, we give a comparison of the k-weight nonlinearity of WPB Boolean functions in Construction 1 with other constructions [4, 5, 8, 14] in 8 and 16 variables, as shown in Table 1 and Table 2. The lower bound and upper bound of [4] in Table 1 and 2 denote the lower and upper bounds of the maximum of the k-weight nonlinearity of all WPB functions over $E_{2^m,k}$, respectively, and the lower bound of cons-1 in [8] denotes the minimum value of the k-weight nonlinearity distribution of the functions they constructed. As mentioned in Remark 1, the functions $g_{m;1}$, $g_{m;2}$ and $g_{m;m}$ in Construction 1 with $m = 3, 4$ appeared in [13], [7] and [2], respectively, and the function $g_{4;3}$ in Construction 1 was defined in [18]. For $g_{3;1}$, $g_{4;1}$, $g_{4;2}$ and $g_{4;3}$, we compute and list their k-weight nonlinearities which were not exhibited before. From these two tables, we can see that the k-weight nonlinearity of functions in Construction 1 still is below the lower bound of the maximum value given in [4]. So far, the k-weight nonlinearity of h_{16} in [5] is the highest known.

Table 1: A comparison of k-weight nonlinearities of 8-variable WPB functions

Construction	NL_2	NL_3	NL_4	NL_5	NL_6
$g_{3;1}$ [13]	2	0	3	0	2
$g_{3;2}$ [7]	2	12	19	12	2
$g_{3;3}$ [2]	2	12	19	12	6
f [8]	$\{6, 9\}$	$\{0, 8, 14, 16, 18, 20, 21, 22\}$	$\{19, 22, 23, 24, 25, 26, 27\}$	$\{0, 8, 14, 16, 18, 20, 21, 22\}$	$\{6, 9\}$
f_3 [14]	2	8	8	8	2
g_3 [14]	6	8	26	8	6
Construction 2 [4]	2	10	14	10	2
the lower bound [4]	6	16	21	12	6
the upper bound [4]	11	24	30	24	11

At the end of this section, we list the algebraic immunity of $g_{m;d}$ in Construction 1 and the optimal algebraic immunity when $m = 2, 3, 4$ and $d = 1, 2, 3$, respectively as shown in Table 3. As we can see, the WPB functions we defined in Construction 1 have the optimal algebraic immunity only when $m = 2$, while in other cases, they do not reach the optimal algebraic immunity. Therefore, we also need to do further work to follow the algebraic immunity of WPB functions.

5. Conclusion

Inspired by the works on the constructions of WPB functions in [7, 13, 16, 18], in this paper, a unified construction of WPB functions including their four classes of

Table 2: A comparison of k-weight nonlinearities of 16-variable WPB functions

Construction	NL_2	NL_3	NL_4	NL_5	NL_6	NL_7	NL_8	NL_9	NL_{10}	NL_{11}	NL_{12}	NL_{13}	NL_{14}
$g_{4;1}$ [13]	4	0	14	0	28	0	35	0	28	0	14	0	14
$g_{4;2}$ [7]	4	56	350	1312	3176	4782	5443	4782	3176	1312	350	56	4
$g_{4;3}$ [18]	4	56	350	1288	3108	4774	5539	4902	3228	1664	638	152	12
$g_{4;4}$ [2]	4	56	350	1288	3108	4774	5539	4902	3236	1672	654	152	28
the lower bound of cons-1 in [8]	5	144	472	1056	2184	1296	2184	1296	2184	1056	472	144	5
h_{16} [5]	28	172	688	1884	3629	5103	5567	5103	3629	1884	688	172	28
Construction 2 [4]	6	52	226	682	1500	2502	3002	2502	1500	682	226	52	6
the lower bound [4]	34	222	803	2016	3774	5443	6141	5443	3774	2016	803	222	34
the upper bound [4]	54	268	888	2150	3959	5666	6378	5666	3959	2150	888	268	54

Table 3: The algebraic immunity of $g_{m;d}$ in Construction 1

d	m	algebraic immunity of $g_{m;d}$	optimal algebraic immunity
1 [13]	2	2	2
	3	3	4
	4	3	8
2 [7]	2	2	2
	3	3	4
	4	3	8
3 [18]	2	2	2
	3	3	4
	4	3	8

WPB functions as special cases is contributed. First, we provide a construction of functions with provable k-weight. We then modify the support of these functions and provide a unified construction of WPB functions that contains an infinite number of WPB function classes. We also analyze the algebraic degree of the newly constructed WPB functions and compare the k-weight nonlinearities of WPB functions in 8 and 16 variables. For larger number of variables, we have not got the k-weight nonlinearity. As far as we know, only Gini and Méaux constructed WPB functions with proven weightwise nonlinearity [4] up to now. How to theoretically prove the k-weight nonlinearity of the WPB functions is still a challenging problem. In the future we will devote ourselves to constructing WPB functions with the provable k-weight nonlinearity in theory.

Acknowledgements

This work was supported by National Natural Science Foundation of China (Grant Nos.61902314 and 62072371), Basic Research Program of Qinghai Province (Grant No.2020-ZJ-701).

References

[1] R. Askey, Orthogonal polynomials and special functions, SIAM, 1975.

[2] C. Carlet, P. Méaux, Y. Rotella, Boolean functions with restricted input and their robustness; application to the FLIP cipher, IACR Trans. Symmetric Cryptol. 2017 (3) (2017) 192–227.

[3] N. T. Courtois, W. Meier, Algebraic attacks on stream ciphers with linear feedback, in: Advances in Cryptology – EUROCRYPT 2003, Springer, Heidelberg, 2003, pp. 345–359.

[4] A. Gini, P. Méaux, On the weightwise nonlinearity of weightwise perfectly balanced functions, Discrete Appl. Math. 322 (2022) 320–341.

[5] A. Gini, P. Méaux, Weightwise almost perfectly balanced functions: secondary constructions for all n and better weightwise nonlinearities, in: Progress in Cryptology – INDOCRYPT 2022, Springer, Cham, 2022, pp. 492–514.

[6] A. Gini, P. Méaux, Weightwise perfectly balanced functions and nonlinearity, Cryptology ePrint Archive, (2022), https://eprint.iacr.org/2022/1777.

[7] J. Li, S. Su, Construction of weightwise perfectly balanced Boolean functions with high weightwise nonlinearity, Discrete Appl. Math. 279 (2020) 218–227.

[8] J. Liu, S. Mesnager, Weightwise perfectly balanced functions with high weightwise nonlinearity profile, Des. Codes Cryptogr. 87 (8) (2019) 1797–1813.

[9] S. Mandujano, J. Carlos Ku Cauich, A. Lara1, Studying special operators for the application of evolutionary algorithms in the seek of optimal Boolean functions for cryptography, in: Advances in Computational Intelligence, Springer, Cham, 2022, pp. 383–396.

[10] L. Mariot, S. Picek, D.Jakobovic M. Djurasevic, A. Leporati, Evolutionary construction of perfectly balanced Boolean functions, in: 2022 IEEE Congress on Evolutionary Computation, IEEE, Italy, 2022, pp. 1–8.

[11] P. Méaux, A. Journault, F.-X. Standaert, C. Carlet, Towards stream ciphers for efficient fhe with low-noise ciphertexts, in: Advances in Cryptology – EUROCRYPT 2016, Springer, Heidelberg, 2016, pp. 311–343.

[12] W. Meier, E. Pasalic, C.Carlet. Algebraic attacks and decomposition of Boolean functions, in: Advances in Cryptology - EUROCRYPT 2004, Springer, Heidelberg, 2004, pp. 474-491.

[13] S. Mesnager, S. Su, On constructions of weightwise perfectly balanced Boolean functions, Cryptogr. Commun. 13 (6) (2021) 951–979.

[14] S. Mesnager, S. Su, J. Li, Concrete constructions of weightwise perfectly balanced (2-rotation symmetric) functions with optimal algebraic immunity and high weightwise nonlinearity, Cryptogr. Commun. (2022) 1–19.

[15] S. Mesnager, Z. Zhou, C. Ding, On the nonlinearity of Boolean functions with restricted input, Cryptogr. Commun. 11 (1) (2019) 63–76.

[16] S. Su, The lower bound of the weightwise nonlinearity profile of a class of weightwise perfectly balanced functions, Discrete Appl. Math. 297 (2021) 60–70.

[17] D. Tang, J. Liu, A family of weightwise (almost) perfectly balanced Boolean functions with optimal algebraic immunity, Cryptogr. Commun. 11 (6) (2019) 1185–1197.

[18] R. Zhang, S. Su, A new construction of weightwise perfectly balanced Boolean functions, Adv. Math. Commun. (2021). doi:10.3934/amc.2021020, in press.