FURTHER PROPERTIES OF SEVERAL CLASSES OF BOOLEAN FUNCTIONS WITH OPTIMUM ALGEBRAIC IMMUNITY

CLAUDE CARLET, XIANGYONG ZENG, CHUNLEI LI AND LEI HU

Abstract. Thanks to a method proposed by Carlet, several classes of balanced Boolean functions with optimum algebraic immunity are obtained. By choosing suitable parameters, for even $n \geq 8$, the balanced n-variable functions can have nonlinearity $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + 2\binom{n-2}{\frac{n}{2}-2}/(n-2)$, and for odd n, the functions can have nonlinearity $2^{n-1} - \binom{n-1}{\frac{n-1}{2}} + \Delta(n)$, where the function $\Delta(n)$ is described in Theorem 4.4. The algebraic degree of some constructed functions is also discussed.

1. Introduction

Boolean functions have important applications in the combiner model and the filter model of stream ciphers. A function used in such an application should mainly possess balancedness, a high algebraic degree, a high nonlinearity and, in the case of the combiner model, a high correlation immunity. Recently, by finding a way of solving some of the overdefined systems of multivariate equations whose unknowns are the secret key bits, the algebraic attacks have allowed cryptanalysing several stream ciphers; they may also represent a thread for block ciphers [1, 7, 9, 10, 8, 15, 18]. A high algebraic immunity was proposed as a necessary (not sufficient) property for Boolean functions used in stream ciphers: for a given Boolean function f on n variables, any Boolean function g such that $f * g = 0$ or $(1 + f) * g = 0$ should have high algebraic degree [9, 18], where $*$ is the multiplication of functions inherited from multiplication in $\mathbb{F}_2$, the finite field with two elements.

The research of Boolean functions that can resist algebraic attacks has not given fully satisfactory results. Since a difference of only 1 between the algebraic immunities of two functions can make a crucial difference with respect to algebraic attacks, it is an important topic to construct Boolean functions with optimum algebraic immunity. But these functions must also satisfy the other criteria recalled above for being likely to be used in stream ciphers.

There are two main ways to construct Boolean functions achieving optimum algebraic immunity. The first one consists in an iterative construction of a $2k$-variable Boolean function with algebraic immunity k [12]. The constructed functions were further studied in [6], where it is shown that their algebraic degrees are close to $2k$ but their nonlinearity is $2^{n-1} - \binom{n-1}{\frac{n}{2}}$, which is insufficient. Moreover, they are not balanced. The second way is based on modifying symmetric functions [13, 2]. Speaking concretely, up to affine equivalence, the obtained functions of n-variable are symmetric on the set consisting of all elements with weight not equal to $\lfloor \frac{n+1}{2} \rfloor$ in $\mathbb{F}_2^n$ [13, 2]. These functions are almost symmetric. Furthermore, their nonlinearities

Key words and phrases. Boolean function, algebraic immunity, nonlinearity, balancedness, Krawtchouk polynomial.

C. Carlet is with MAATICAH, Université Paris VIII, 93526 Saint-Denis Cedex, France (e-mail: claude.carlet@inria.fr).

X. Zeng and C. Li are with the Faculty of Mathematics and Computer Science, Hubei University, Wuhan 430062, China (e-mail: xzeng@hubu.edu.cn).

L. Hu is with the State Key Laboratory of Information Security (Graduate School of Chinese Academy of Sciences), Beijing, 100049, China (e-mail: hu@is.ac.cn).

are not exceeding $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. The Boolean functions with optimum algebraic immunity, in odd number of variables, are also considered in [16], and some necessary conditions that these functions have a possibility to achieve high nonlinearities are presented.

Recently, Carlet [4] introduced a general method for proving that a given function, in any number of variables, has a prescribed algebraic immunity. Two algorithms were also presented to search balanced Boolean functions with optimum algebraic immunity. A new infinite class of such functions was given and their Walsh transforms were studied. But the problem of determining, for every n, the nonlinearities of the constructed functions (or of a part of them) was left open.

In the present paper, several infinite classes of balanced Boolean functions are constructed, based on Carlet's method. Thus, all these functions have optimum algebraic immunity. Furthermore, by choosing suitable parameters, we show that some infinite classes of balanced functions can have nonlinearity significantly larger than $2^{n-1} - \binom{n-1}{\lfloor \frac{n}{2} \rfloor}$. The nonlinearity is measured by applying properties of Krawtchouk polynomials to analyze the Walsh transform. The algebraic degree of some functions in even numbers of variables is also analyzed.

The remainder of this paper is organized as follows. Section 2 gives some definitions and preliminaries. Sections 3 presents a construction of Boolean functions with optimum algebraic immunity, in even number of variables. The nonlinearity of the constructed functions is calculated. Furthermore, the algebraic degree for some functions is considered. Section 4 determines the nonlinearity for a class of Boolean functions with optimum algebraic immunity, in odd number of variables. Section 5 concludes the study.

2. Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$, and B_n the set of n-variable Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. The basic representation of a Boolean function $f(x_1, \cdots, x_n)$ is by the output column of its truth table, i.e., a binary string of length 2^n,

$$f = [f(0, 0, \cdots, 0), f(1, 0, \cdots, 0), f(0, 1, \cdots, 0), f(1, 1, \cdots, 0), \cdots, f(1, 1, \cdots, 1)].$$

The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function $f \in B_n$ is the weight of this string, that is, the size of the support $\mathrm{supp}(f) = \{x \in \mathbb{F}_2^n \mid f(x) = 1\}$ of the function. The Hamming distance $d(f, g)$ between two Boolean functions f and g is the Hamming weight of their difference $f + g$ (by abuse of notation, we use $+$ to denote the addition on $\mathbb{F}_2$, i.e., the XOR). We say that a Boolean function f is *balanced* if its truth table contains an equal number of 1's and 0's, that is, if its Hamming weight equals 2^{n-1}.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form* (ANF),

$$f(x_1, \cdots, x_n) = \sum_{I \subseteq \{1,2,\cdots,n\}} a_I \prod_{i \in I} x_i,$$

where the a_I's are in $\mathbb{F}_2$. The *algebraic degree*, $\deg(f)$, is the number of variables in the highest order term with non zero coefficient. A Boolean function is affine if it has degree at most 1. The set of all affine functions is denoted by A_n.

Boolean functions used in cryptographic systems must have high nonlinearity to withstand linear and correlation attacks [14, 11]. The *nonlinearity* of an n-variable function f is its distance from the set of all n-variable affine functions, i.e.,

$$nl(f) = \min_{g \in A_n} (d(f, g)).$$

This parameter can be expressed by means of the Walsh transform. Let $x = (x_1, \cdots, x_n)$ and $\lambda = (\lambda_1, \cdots, \lambda_n)$ both belong to $\mathbb{F}_2^n$ and $\lambda \cdot x = \lambda_1 x_1 + \cdots + \lambda_n x_n$. Let $f(x)$ be a Boolean function in n variables. The *Walsh transform* of $f(x)$ is an integer valued function over $\mathbb{F}_2^n$ which is defined as

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

A Boolean function f is balanced if and only if $W_f(0) = 0$. The nonlinearity of f can also be given by

$$nl(f) = 2^{n-1} - \frac{1}{2}\max_{\lambda\in\mathbb{F}_2^n} |W_f(\lambda)|.$$

Any Boolean function should have also high algebraic degree to be cryptographically secure [14, 19]. In fact, it must keep high degree even if a few output bits are modified. In other words, it must have high nonlinearity profile [5].

For an n-variable Boolean function f, different scenarios related to low degree multiples of f have been studied in [9, 18]. This led to the following definition.

Definition 2.1. *For $f \in B_n$, define $AN(f) = \{g \in B_n \,|\, f * g = 0\}$. Any function $g \in AN(f)$ is called an annihilator of f. The algebraic immunity of f is the minimum degree of all the nonzero annihilators of f and of all those of $f + 1$. We denote it by $AI(f)$.*

Notation:

- W^d: the set of all elements with Hamming weight d in $\mathbb{F}_2^n$;
- $W^{<d} = W^0 \cup \cdots \cup W^{d-1}$, $W^{>d} = W^{d+1} \cup \cdots \cup W^n$, $W^{\le d} = W^{<d} \cup W^d$, $W^{\ge d} = W^{>d} \cup W^d$;
- $\mathrm{supp}(\alpha) = \{1 \le i \le n \,|\, \alpha_i = 1\}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$;
- $\alpha \preceq \beta$: $\mathrm{supp}(\alpha) \subseteq \mathrm{supp}(\beta)$;
- $C_\alpha = \{x \in \mathbb{F}_2^n \,|\, x \preceq \alpha\}$ for $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_2^n$;
- $x \oplus y = (x_1 + y_1, x_2 + y_2, \cdots, x_n + y_n)$ where $x = (x_1, x_2, \cdots, x_n)$, $y = (y_1, y_2, \cdots, y_n) \in \mathbb{F}_2^n$;
- $\overline{E} = \{\overline{x} \,|\, x \in E\}$ for any subset E of $\mathbb{F}_2^n$, where $\overline{x} = (x_1 + 1, x_2 + 1, \cdots, x_n + 1)$ is the bitwise complement of $x = (x_1, x_2, \cdots, x_n)$.

For a fixed $\lambda \in \mathbb{F}_2^n$ with $\mathrm{wt}(\lambda) = k$, we have

$$\sum_{\mathrm{wt}(x)=i} (-1)^{\lambda\cdot x} = \sum_{j=0}^{i} (-1)^j \tbinom{k}{j}\tbinom{n-k}{i-j} = K_i(k, n), \tag{1}$$

where $K_i(x, n)$ is the Krawtchouk polynomial [17].

Proposition 2.2. *The Krawtchouk polynomials have the following properties.*

1. $K_0(k, n) = 1$, $K_1(k, n) = n - 2k$;
2. $(n - k)K_i(k + 1, n) = (n - 2i)K_i(k, n) - kK_i(k - 1, n)$;
3. $K_i(k, n) = (-1)^i K_i(n - k, n)$;
4. $\binom{n}{k}K_i(k, n) = \binom{n}{i}K_k(i, n)$.

The following lemmas will be used to prove the results in the paper. Lemma 1 is presented as a problem in page 153 of [17]. A proof is provided for completeness.

Lemma 2.3. *The equality*

$$\sum_{i=0}^{r} K_i(k, n) = K_r(k - 1, n - 1) \tag{2}$$

holds for $0 \le r \le n$ *and* $n, k \ge 1$.

Proof: This lemma will be proved by induction on the integer $r \ge 0$.

For $r = 0$, $K_0(k, n) = K_0(k - 1, n - 1) = 1$.

Suppose that $\sum\limits_{i=0}^{t} K_i(k,n) = K_t(k-1,n-1)$ holds for $0 \leq t \leq r-1$.

Then, we have:

$$\begin{array}{rl} & \sum\limits_{i=0}^{r} K_i(k,n) \\ = & \sum\limits_{i=0}^{r-1} K_i(k,n) + K_r(k,n) \\ = & K_{r-1}(k-1,n-1) + K_r(k,n) \\ = & \sum\limits_{j=0}^{r-1}(-1)^j\binom{k-1}{j}\binom{n-k}{r-1-j} + \sum\limits_{j=0}^{r}(-1)^j\binom{k}{j}\binom{n-k}{r-j} \\ = & \sum\limits_{j=0}^{r-1}(-1)^j\binom{k-1}{j}\binom{n-k}{r-1-j} + \binom{k}{0}\binom{n-k}{r} + \sum\limits_{j=1}^{r}(-1)^j[\binom{k-1}{j-1} + \binom{k-1}{j}]\binom{n-k}{r-j} \\ = & \sum\limits_{j=0}^{r-1}(-1)^j\binom{k-1}{j}\binom{n-k}{r-1-j} + \sum\limits_{j=1}^{r}(-1)^j\binom{k-1}{j-1}\binom{n-k}{r-j} + \sum\limits_{j=0}^{r}(-1)^j\binom{k-1}{j}\binom{n-k}{r-j} \\ = & \sum\limits_{j=0}^{r-1}(-1)^j\binom{k-1}{j}\binom{n-k}{r-1-j} + \sum\limits_{j=0}^{r-1}(-1)^{j+1}\binom{k-1}{j}\binom{n-k}{r-1-j} + \sum\limits_{j=0}^{r}(-1)^j\binom{k-1}{j}\binom{n-k}{r-j} \\ = & \sum\limits_{j=0}^{r}(-1)^j\binom{k-1}{j}\binom{n-k}{r-j} \\ = & K_r(k-1,n-1). \end{array}$$

Thus, Equality (2) holds for all $0 \leq r \leq n$. □

Lemma 2.4. *Let n and k be even and such that $2 \leq k \leq n-2$. Then:*

$$\begin{array}{rl} & K_{\frac{n}{2}-1}(k,n-1) \\ = & -K_{\frac{n}{2}-1}(k-1,n-1) \\ = & (-1)^{\frac{k}{2}}\binom{n-1}{\frac{n}{2}-1}(k-1)(k-3)\cdots 3\cdot 1/[(n-1)(n-3)\cdots(n-k+1)]. \end{array} \qquad (3)$$

Furthermore, $|K_{\frac{n}{2}-1}(i,n-1)| \leq |K_{\frac{n}{2}-1}(2,n-1)| = \binom{n-1}{\frac{n}{2}-1}/(n-1)$ for all i with $1 \leq i \leq n-2$.

Proof: We will prove the result by induction on k.

By Proposition 2.2, Equality 4., one has

$$K_{\frac{n}{2}-1}(0,n-1) = \binom{n-1}{\frac{n}{2}-1}K_0(\tfrac{n}{2}-1,n-1) = \binom{n-1}{\frac{n}{2}-1}.$$

Similarly, by Proposition 2.2, Equalities 4. and 1., it can be proven that

$$K_{\frac{n}{2}-1}(1,n-1) = \binom{n-1}{\frac{n}{2}-1}K_1(\tfrac{n}{2}-1,n-1)/\binom{n-1}{1} = \binom{n-1}{\frac{n}{2}-1}/(n-1).$$

Then, by Proposition 2.2, Equality 2., one has

$$\begin{array}{rcl} K_{\frac{n}{2}-1}(2,n-1) & = & [K_{\frac{n}{2}-1}(1,n-1) - K_{\frac{n}{2}-1}(0,n-1)]/(n-2) \\ & = & [\binom{n-1}{\frac{n}{2}-1}/(n-1) - \binom{n-1}{\frac{n}{2}-1}]/(n-2) \\ & = & -\binom{n-1}{\frac{n}{2}-1}/(n-1). \end{array}$$

Thus, the result holds for $k=2$. When $n=4$, Equality (3) has been proven to be true. When $n \geq 6$, suppose that Equality (3) holds for all even j with $2 \leq j \leq k$, where the integer k satisfies $2 \leq k \leq n-4$. Then, by Proposition 2.2, Equality 2., one has

$$\begin{array}{rl} & K_{\frac{n}{2}-1}(k+1,n-1) \\ = & [K_{\frac{n}{2}-1}(k,n-1) - kK_{\frac{n}{2}-1}(k-1,n-1)]/(n-1-k) \\ = & (-1)^{\frac{k}{2}}\binom{n-1}{\frac{n}{2}-1}(k+1)(k-1)\cdots 3\cdot 1/[(n-1)(n-3)\cdots(n-k-1)]. \end{array}$$

The following formula is similarly obtained.

$$\begin{array}{rl} & K_{\frac{n}{2}-1}(k+2,n-1) \\ = & (-1)^{\frac{k}{2}+1}\binom{n-1}{\frac{n}{2}-1}(k+1)(k-1)\cdots 3\cdot 1/[(n-1)(n-3)\cdots(n-k-1)]. \end{array}$$

By Equality (3), for even $2\le k\le n-4$, one has

$$|K_{\frac{n}{2}-1}(k,n-1)|/|K_{\frac{n}{2}-1}(k+2,n-1)| = (n-k-1)/(k+1).$$

Thus, for even $2\le i\le j\le n-2$, it can be proven that

$$|K_{\frac{n}{2}-1}(2,n-1)| \ge |K_{\frac{n}{2}-1}(i,n-1)| \ge |K_{\frac{n}{2}-1}(j,n-1)|$$

when $j\le n/2-1$, and

$$|K_{\frac{n}{2}-1}(i,n-1)| \le |K_{\frac{n}{2}-1}(j,n-1)| \le |K_{\frac{n}{2}-1}(n-2,n-1)|$$

when $i\ge n/2-1$. Since $|K_{\frac{n}{2}-1}(2,n-1)| = |K_{\frac{n}{2}-1}(n-2,n-1)|$, one has

$$|K_{\frac{n}{2}-1}(i,n-1)| \le |K_{\frac{n}{2}-1}(2,n-1)|$$

for even $2\le i\le n-2$. Furthermore, for odd $1\le i\le n-3$, by Equality (3), one has

$$|K_{\frac{n}{2}-1}(i,n-1)| = |K_{\frac{n}{2}-1}(i+1,n-1)| \le |K_{\frac{n}{2}-1}(2,n-1)|.$$

Thus, for $1\le i\le n-2$, $|K_{\frac{n}{2}-1}(i,n-1)| \le |K_{\frac{n}{2}-1}(2,n-1)|$.

The proof is completed. □

Lemma 2.5. *For $1\le i\le\lfloor\frac{n-1}{2}\rfloor$ and $1\le r\le n-1$, $|K_i(r,n)|\le K_i(1,n)$.*

Proof: From Corollary 1 in [13], we only need to show the inequality $|K_i(r,n)|\le K_i(1,n)$ holds for $r=n/2$ when n is even. By Proposition 5 in [13],

$$K_i(n/2,n) = \begin{cases} 0, & \text{for odd } i, \\ (-1)^{i/2}\binom{n/2}{i/2}, & \text{for even } i. \end{cases}$$

By Proposition 2.2, one has $K_i(1,n)=(n-2i)\binom{n}{i}/n$ and for even $i\le n/2-1$,

$$\begin{array}{rcl} K_i(1,n) & = & (n-2i)\binom{n}{i}/n = (n-2i)\binom{n-1}{i-1}/i \\ & \ge & 2\binom{n-1}{i-1}/i > 2^2\binom{n-2}{i-2}/i > \cdots > 2^{i/2}\binom{n-i/2}{i/2}/i \\ & > & 2^{i/2}\binom{n/2}{i/2}/i \ge \binom{n/2}{i/2}. \end{array}$$

This finishes the proof. □

Lemma 2.6. *Let n be odd, for odd $3\le t\le n-2$,*

$$|K_{\frac{n-1}{2}}(t-1,n-1)| \le |K_{\frac{n-1}{2}}(2,n-1)| = \binom{n-1}{\frac{n-1}{2}}/(n-2).$$

Proof. By Proposition 2.2, Equality 4., and Proposition 5 in [13], for odd t, one has

$$|K_{\frac{n-1}{2}}(t-1,n-1)| = \binom{n-1}{\frac{n-1}{2}}|K_{t-1}(\tfrac{n-1}{2},n-1)|/\binom{n-1}{t-1} = \binom{n-1}{\frac{n-1}{2}}\binom{\frac{n-1}{2}}{\frac{t-1}{2}}/\binom{n-1}{t-1}.$$

Then,

$$\begin{array}{rl} & |K_{\frac{n-1}{2}}(t+1,n-1)|/|K_{\frac{n-1}{2}}(t-1,n-1)| \\ = & \binom{\frac{n-1}{2}}{\frac{t+1}{2}}\binom{n-1}{t-1}/[\binom{\frac{n-1}{2}}{\frac{t-1}{2}}\binom{n-1}{t+1}] \\ = & t/(n-1-t). \end{array}$$

This implies

$$\begin{array}{l}|K_{\frac{n-1}{2}}(t+1,n-1)|-|K_{\frac{n-1}{2}}(t-1,n-1)|\le 0 \text{ for } t\le (n-1)/2\\ |K_{\frac{n-1}{2}}(t+1,n-1)|-|K_{\frac{n-1}{2}}(t-1,n-1)|\ge 0 \text{ for } t\ge (n-1)/2.\end{array}$$

Thus, for odd $3\le t\le n-2$, $|K_{\frac{n-1}{2}}(t-1,n-1)|\le |K_{\frac{n-1}{2}}(2,n-1)|$. □

Lemma 2.7. *Let $E\subseteq \mathbb{F}_2^n$ and the Boolean function $\varphi_0(x)$ be balanced on E. Then for any Boolean function $\varphi(x)$, one has*

$$|\sum_{x\in E}(-1)^{\varphi_0(x)+\varphi(x)}|\le |E|-|\sum_{x\in E}(-1)^{\varphi(x)}|.$$

Proof: Let $E_1=E\cap \mathrm{supp}(\varphi)$ and $E_0=E\setminus E_1$. Since φ_0 is balanced on E, one has

$$\begin{array}{rcl}\sum\limits_{x\in E}(-1)^{\varphi_0(x)+\varphi(x)} &=& \sum\limits_{x\in E_0}(-1)^{\varphi_0(x)}-\sum\limits_{x\in E_1}(-1)^{\varphi_0(x)}\\ &=& 2\sum\limits_{x\in E_0}(-1)^{\varphi_0(x)}-\sum\limits_{x\in E}(-1)^{\varphi_0(x)}\\ &=& 2\sum\limits_{x\in E_0}(-1)^{\varphi_0(x)}\\ &=& -2\sum\limits_{x\in E_1}(-1)^{\varphi_0(x)}.\end{array}$$

This implies

$$|\sum_{x\in E}(-1)^{\varphi_0(x)+\varphi(x)}|\le \min\{2|E_0|,\,2|E_1|\}.$$

On the other hand, one has

$$|E|-|\sum_{x\in E}(-1)^{\varphi(x)}|=\min\{2|E_0|,\,2|E_1|\}$$

since $\sum\limits_{x\in E}(-1)^{\varphi(x)}=|E_0|-|E_1|$. □

3. A construction of Boolean functions with optimum algebraic immunity, in even number of variables

Throughout this section, n is always assumed to be even. Let T, S, U and V denote four subsets of $\mathbb{F}_2^n$, more concretely, $T=\{\alpha_1,\ldots,\alpha_l\}\subseteq W^{<\frac{n}{2}}$, $S=\{\beta_1,\ldots,\beta_s\}\subseteq W^{>\frac{n}{2}}$, $U=\{u_1,\ldots,u_l\}\subseteq W^{\frac{n}{2}}$, and $V=\{v_1,\ldots,v_s\}\subseteq W^{\frac{n}{2}}$. These sets will be used to construct Boolean functions with desired properties.

Construction 1: Define $f\in B_n$ as follows

$$f(x)=\begin{cases}0, & x\in W^{<\frac{n}{2}}\cup S\cup U\setminus T,\\ a_x, & x\in W^{\frac{n}{2}}\setminus U\cup V,\\ 1, & x\in W^{>\frac{n}{2}}\cup T\cup V\setminus S,\end{cases}\tag{4}$$

where $a_x\in\{0,1\}$.

When the sets T, S, U and V satisfy the following conditions

$$\begin{array}{l}U\cap V=\emptyset,\\ \forall 1\le i\le l,\ \alpha_i\preceq u_i,\ \text{ and } \forall 1\le j<i\le l,\ \alpha_i\not\preceq u_j,\\ \forall 1\le i\le s,\ v_i\preceq \beta_i,\ \text{ and } \forall 1\le j<i\le s,\ v_i\not\preceq \beta_j,\end{array}\tag{5}$$

the function f defined by (4) is a special case of Carlet's method [4].

Proposition 3.1. *([4]) Let n be even and let $a^1, \cdots, a^{\binom{n}{n/2}}$ be an ordering of the set of all vectors of weight $n/2$ in $\mathbb{F}_2^n$. For every $i \in \{1, 2, \cdots, \binom{n}{n/2}\}$, let us denote by A_i the flat $\{x \in \mathbb{F}_2^n \,|\, \mathrm{supp}(a^i) \subseteq \mathrm{supp}(x)\}$ and by A'_i the vector space $\{x \in \mathbb{F}_2^n \,|\, \mathrm{supp}(x) \subseteq \mathrm{supp}(a^i)\}$. Let I, J and K be three disjoint subsets of $\{1, 2, \cdots, \binom{n}{n/2}\}$. Assume that, for every $i \in I$, there exists a vector $b^i \neq a^i$ such that $b^i \in A_i \setminus \cup_{i' \in I: i' < i} A_{i'}$. Assume that, for every $i \in J$, there exists a vector $c^i \neq a^i$ such that $c^i \in A'_i \setminus \cup_{i' \in J: i' < i} A'_i$. Then the function whose support equals:*

$$\{x \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x) > n/2\} \cup \{c^i, i \in J\} \cup \{a^i, i \in I \cup K\} \setminus \{b^i, i \in I\}$$

has algebraic immunity $n/2$.

Let $\{a^i,\, i \in I\} = V = \{v_1, \ldots, v_s\}$ and $\{b^i,\, i \in I\} = S = \{\beta_1, \ldots, \beta_s\}$. Then, for every $i \in I$, $b^i \neq a^i$ and $b^i \in A_i \setminus \cup_{i' \in I: i' < i} A_{i'}$. Similarly, let $\{a^i,\, i \in J\} = U = \{u_1, \ldots, u_l\}$ and $\{c^i,\, i \in J\} = T = \{\alpha_1, \ldots, \alpha_l\}$. Then, $c^i \neq a^i$ and $c^i \in A'_i \setminus \cup_{i' \in J: i' < i} A'_i$. Let $\{a^k,\, k \in K\} = \{x \in W^{\frac{n}{2}} \,|\, a_x = 1, x \notin U \cup V\}$. Then, the function defined in Proposition 3.1 has the same support as the function f defined as in Construction 1. This shows f is included in the class of functions described as Proposition 3.1 if T, S, U and V satisfy the conditions in (5).

By Proposition 3.1 and the above analysis, the following result is obtained. A simpler proof is also presented here.

Corollary 3.2. *Let $f \in B_n$ be defined by (4). If the sets T, S, U and V satisfy the conditions in (5), then $AI(f) = n/2$.*

Proof: We first prove that any nonzero annihilator of $f + 1$ has algebraic degree $\geq n/2$.

Suppose $g \in B_n$ is a nonzero annihilator of $f + 1$. Then, for any element μ of $U \cup W^{<\frac{n}{2}} \backslash T$, one has $g(\mu) = 0$. Let $g(x) = \sum_{\nu \in \mathbb{F}_2^n} \widetilde{g}_\nu x^\nu$ be the algebraic normal form (ANF) of g. Thus, $\widetilde{g}_\nu = \bigoplus_{\mu \preceq \nu} g(\mu)$.

If there exists some element $\alpha \in T$ such that $g(\alpha) = 1$, denote $i_0 = \min\{i \,|\, g(\alpha_i) = 1\}$, then $\widetilde{g}_{u_{i_0}} = g(\alpha_{i_0}) = 1$, i.e., $\deg(g) \geq n/2$. Otherwise, one has $g(\alpha_1) = g(\alpha_2) = \cdots = g(\alpha_l) = 0$, then $\widetilde{g}_\nu = 0$ for all $\nu \in W^{<\frac{n}{2}}$. This implies $\deg(g) \geq n/2$.

Now we show that f has no annihilator of degree $< n/2$.

Suppose h is a nonzero annihilator of f, then, for any element μ of $V \cup W^{>\frac{n}{2}} \backslash S$, one has $h(\mu) = 0$. Set $h'(x) = h(x \oplus 1)$, then $h'(x) = 0$ for $x \in \overline{V} \cup W^{<\frac{n}{2}} \backslash \overline{S}$. Similarly, it can be proven that $\deg(h') \geq n/2$. Since h and h' have the same algebraic degree, one has $\deg(h) \geq n/2$.

Therefore, $AI(f) = n/2$ follows above facts. □

When the sets T, S, U and V are pairwise disjoint, by (4), the Walsh spectrum of f can be calculated as follows.

$$\begin{aligned} W_f(\lambda) &= \sum_{x \in W^{<\frac{n}{2}} \backslash T} (-1)^{\lambda \cdot x} + \sum_{x \in S \cup U} (-1)^{\lambda \cdot x} + \sum_{x \in W^{\frac{n}{2}} \backslash U \cup V} (-1)^{a_x + \lambda \cdot x} \\ &\quad + \sum_{x \in W^{>\frac{n}{2}} \backslash S} (-1)^{\lambda \cdot x + 1} + \sum_{x \in T \cup V} (-1)^{\lambda \cdot x + 1} \\ &= \sum_{x \in W^{<\frac{n}{2}}} (-1)^{\lambda \cdot x} + 2 \sum_{x \in T} (-1)^{\lambda \cdot x + 1} + \sum_{x \in U} (-1)^{\lambda \cdot x} + \sum_{x \in V} (-1)^{\lambda \cdot x + 1} \\ &\quad + \sum_{x \in W^{\frac{n}{2}} \backslash U \cup V} (-1)^{a_x + \lambda \cdot x} + \sum_{x \in W^{>\frac{n}{2}}} (-1)^{\lambda \cdot x + 1} + 2 \sum_{x \in S} (-1)^{\lambda \cdot x}. \end{aligned} \tag{6}$$

The main purpose of this section is to study the cryptographical properties such as nonlinearity and balancedness for some Boolean functions in Construction 1, by imposing additional restrictions on the sets T, S, U, V and Boolean values of a_x for $x \in W^{\frac{n}{2}} \setminus U \cup V$.

3.1. **Nonlinearity and balancedness of the constructed functions.** By choosing suitable sets T, S, U and V, and restricting $a_x = a_{\overline{x}}$ on $W^{\frac{n}{2}} \setminus U \cup V$, this subsection studies the nonlinearity and balancedness for several infinite classes of functions based on Construction 1.

Case 1. $S = \overline{T}$ and $V = \overline{U}$.

In this case, by (4), the function f can be written as

$$f(x) = \begin{cases} 0, & x \in W^{<\frac{n}{2}} \cup \overline{T} \cup U \setminus T, \\ a_x, & x \in W^{\frac{n}{2}} \setminus U \cup \overline{U}, \\ 1, & x \in W^{>\frac{n}{2}} \cup T \cup \overline{U} \setminus \overline{T}, \end{cases} \tag{7}$$

where $a_x = a_{\overline{x}} \in \{0, 1\}$.

Let $\underline{1}$ denote the full one vector in $\mathbb{F}_2^n$. By Equality (6), one has

$$\begin{aligned} W_f(\lambda) &= \sum_{x \in W^{<\frac{n}{2}}} [(-1)^{\lambda\cdot x} + (-1)^{\lambda\cdot(x\oplus\underline{1})+1}] + 2\sum_{x\in T}[(-1)^{\lambda\cdot x+1} + (-1)^{\lambda\cdot(x\oplus\underline{1})}] \\ &\quad + \sum_{x\in U}[(-1)^{\lambda\cdot x} + (-1)^{\lambda\cdot(x\oplus\underline{1})+1}] + \sum_{x\in A\setminus U}[(-1)^{a_x+\lambda\cdot x} + (-1)^{a_x+\lambda\cdot(x\oplus\underline{1})}] \\ &= \begin{cases} 2\sum\limits_{x\in W^{<\frac{n}{2}}}(-1)^{\lambda\cdot x} - 4\sum\limits_{x\in T}(-1)^{\lambda\cdot x} + 2\sum\limits_{x\in U}(-1)^{\lambda\cdot x}, & \text{for odd } \mathrm{wt}(\lambda), \\ 2\sum\limits_{x\in A\setminus U}(-1)^{a_x+\lambda\cdot x}, & \text{otherwise}, \end{cases} \end{aligned} \tag{8}$$

where the second equal sign holds since $a_x = a_{\overline{x}}$, and A is a subset of $W^{\frac{n}{2}}$ satisfying

$$A \supset U,\ A \cup \overline{A} = W^{\frac{n}{2}},\ \text{and } A \cap \overline{A} = \emptyset. \tag{9}$$

For any fixed nonzero element u in $W^{<\frac{n}{2}}$, take

$$T = \{x \,|\, \mathrm{wt}(x) = n/2 - \mathrm{wt}(u),\ \mathrm{supp}(x) \cap \mathrm{supp}(u) = \emptyset\},\ U = \{x \,|\, \mathrm{wt}(x) = n/2,\ u \preceq x\}. \tag{10}$$

In fact, U can also be written as $U = \{x \oplus u \,|\, x \in T\}$. This shows U is completely determined by T and u. Thus, $V = \overline{U} = \{\overline{x} \oplus u \,|\, x \in T\}$ and then $U \cap V = \emptyset$ since $T \cap \overline{T} = \emptyset$. Furthermore, T, S, U and V satisfy the conditions in (5). Therefore, by Corollary 3.2, $AI(f) = n/2$.

When U is defined as in Equality (10) and $V = \overline{U}$, the function f defined in (7) is exactly the function $f_{u,L}$ in Corollary 3 [4] with additional condition $a_x = a_{\overline{x}}$. Its nonlinearity can be determined by the following theorem.

Theorem 3.3. *Let* $\mathrm{wt}(u) = k \le n/2 - 1$ *and the sets* T, U *be defined by Equality (10). Then, the nonlinearity of the function* $f(x)$ *defined in (7) is*

$$nl(f) = \begin{cases} 2^{n-1} - 2\binom{n-1}{\frac{n}{2}-1}, & k = 1, \\ 2^{n-1} - (3n-4)\binom{n-1}{\frac{n}{2}-1}/(2n-2), & k = 2, \\ 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k), & k \ge 3. \end{cases}$$

Proof: The Walsh spectrum of f is considered as follows.

For odd $\mathrm{wt}(\lambda) = t$, without loss of generality, we can assume $u = (1, \cdots, 1, 0, \cdots, 0) \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$. Then, the sets T and U can be expressed as

$$\begin{cases} T = \{(0, 0, \cdots, 0, x'') \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x'') = \frac{n}{2} - k\}, \\ U = \{(1, 1, \cdots, 1, x'') \in \mathbb{F}_2^n \,|\, \mathrm{wt}(x'') = \frac{n}{2} - k\} \end{cases}$$

where $x'' \in \mathbb{F}_2^{n-k}$. For $\lambda = (\lambda', \lambda'') \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$ with $\mathrm{wt}(\lambda'') = s$, one has $t - s \leq k$ and $s \leq \min\{t, n-k\}$, i.e., $\max\{0, t-k\} \leq s \leq \min\{t, n-k\}$. Then,

$$\sum_{x \in T} (-1)^{\lambda \cdot x} = \sum_{\mathrm{wt}(x'') = \frac{n}{2} - k} (-1)^{\lambda'' \cdot x''} = K_{\frac{n}{2}-k}(s, n-k),$$

and

$$\sum_{x \in U} (-1)^{\lambda \cdot x} = (-1)^{\mathrm{wt}(\lambda')} \sum_{\mathrm{wt}(x'') = \frac{n}{2} - k} (-1)^{\lambda'' \cdot x''} = (-1)^{t-s} K_{\frac{n}{2}-k}(s, n-k).$$

By Lemma 2.3 and Equality (8), one has

$$W_f(\lambda) = \begin{cases} 2K_{\frac{n}{2}-1}(t-1, n-1) - 2K_{\frac{n}{2}-k}(s, n-k), & \text{for odd } s, \\ 2K_{\frac{n}{2}-1}(t-1, n-1) - 6K_{\frac{n}{2}-k}(s, n-k), & \text{for even } s \end{cases} \tag{11}$$

where $\max\{0, t-k\} \leq s \leq \min\{t, n-k\}$.

For convenience, we denote in the sequel:

$$W(t, s, k) = \begin{cases} 2K_{\frac{n}{2}-1}(t-1, n-1) - 2K_{\frac{n}{2}-k}(s, n-k), & \text{for odd } s, \\ 2K_{\frac{n}{2}-1}(t-1, n-1) - 6K_{\frac{n}{2}-k}(s, n-k), & \text{for even } s. \end{cases} \tag{12}$$

When $t = 1$, the value of $|W_f(\lambda)|$ is $|W(1,1,k)|$ or $|W(1,0,k)|$. By Equality (12) and Proposition 2.2, Equalities 1. and 4.,

$$\begin{cases} |W(1,1,1)| = (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1), \\ |W(1,0,1)| = 4\binom{n-1}{\frac{n}{2}-1} \end{cases}$$

for $k = 1$,

$$\begin{cases} |W(1,1,2)| = (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1), \\ |W(1,0,2)| = (n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) \end{cases}$$

for $k = 2$, and

$$\begin{cases} |W(1,1,k)| = 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k), \\ |W(1,0,k)| = 2\binom{n-1}{\frac{n}{2}-1} - 6\binom{n-k}{\frac{n}{2}-k} \end{cases}$$

for $k \geq 3$. Thus, one has

$$\max_{t=1} |W_f(\lambda)| = \begin{cases} |W(1,0,1)|, & k = 1, \\ |W(1,1,k)|, & k \geq 2. \end{cases} \tag{13}$$

since $2k\binom{n-k}{\frac{n}{2}-k}/(n-k) < 6\binom{n-k}{\frac{n}{2}-k}$ holds for $3 \leq k < n/2$.

When $3 \leq t \leq n-1$, the maximal value of $|W_f(\lambda)|$ can be studied by the following analysis. If $k = 1$, then $2 \leq s \leq t$. By Lemma 2.4 and Equality (11), for odd $3 \leq s \leq t$,

$$\begin{aligned} |W_f(\lambda)| &\leq 2|K_{\frac{n}{2}-1}(t-1, n-1)| + 2|K_{\frac{n}{2}-1}(s, n-1)| \\ &< 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 2\binom{n-1}{\frac{n}{2}-1} \\ &= 2n\binom{n-1}{\frac{n}{2}-1}/(n-1), \end{aligned}$$

and for even $2 \leq s \leq t-1$,

$$\begin{aligned} |W_f(\lambda)| &\leq 2|K_{\frac{n}{2}-1}(t-1, n-1)| + 6|K_{\frac{n}{2}-1}(s, n-1)| \\ &\leq 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-1}{\frac{n}{2}-1}/(n-1) \\ &= 8\binom{n-1}{\frac{n}{2}-1}/(n-1). \end{aligned}$$

Thus, for $k = 1$,

$$\max_{t \geq 3} |W_f(\lambda)| < 4\binom{n-1}{\frac{n}{2}-1} = |W(1,0,1)|. \tag{14}$$

For $k \geq 2$, by Lemma 2.4 and Equality (11), one has

$$\begin{array}{rcl}|W_f(\lambda)| & \leq & 2|K_{\frac{n}{2}-1}(t-1,n-1)| + 6|K_{\frac{n}{2}-k}(s,n-k)| \\ & \leq & 2|K_{\frac{n}{2}-1}(2,n-1)| + 6K_{\frac{n}{2}-k}(0,n-k) \\ & = & 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k}.\end{array}$$

More concretely, by Proposition 2.2 and Lemma 2.4, for $k = 2$, $1 \leq s \leq \min\{t, n-k\}$, one has

$$\begin{array}{l} |W(n-1,n-k,k)| \\ = |2K_{\frac{n}{2}-1}(n-2,n-1) - 6K_{\frac{n}{2}-k}(n-k,n-k)| \\ = |2(-1)^{\frac{n}{2}-1}K_{\frac{n}{2}-1}(1,n-1) - 6(-1)^{\frac{n}{2}-k}K_{\frac{n}{2}-k}(0,n-k)| \\ = 2K_{\frac{n}{2}-1}(1,n-1) + 6K_{\frac{n}{2}-k}(0,n-k) \\ = 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k},\end{array}$$

and for $k \geq 3$, $\max\{0, t-k\} \leq s \leq \min\{t, n-k\}$, one has

$$|W(3,0,k)| = |2K_{\frac{n}{2}-1}(2,n-1) - 6K_{\frac{n}{2}-k}(0,n-k)| = 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k}.$$

The three above equations imply

$$\max_{3\leq t\leq n-1} |W_f(\lambda)| = 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k} \tag{15}$$

for $k \geq 2$.

Therefore, when $k = 1$, by Equality (13) and by (14), one has

$$\max_{\text{odd wt}(\lambda)} |W_f(\lambda)| = |W(1,0,1)| = 4\binom{n-1}{\frac{n}{2}-1}. \tag{16}$$

When $k = 2$, by Equality (13) and Equality (15), one has

$$\begin{cases} \max\limits_{t=1} |W_f(\lambda)| = (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1), \\ \max\limits_{t\geq 3} |W_f(\lambda)| = (3n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1), \end{cases}$$

and then,

$$\max_{\text{odd wt}(\lambda)} |W_f(\lambda)| = (3n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1). \tag{17}$$

When $k \geq 3$, since

$$\begin{array}{rl} & |W(1,1,k)| - [2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k}] \\ = & (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) - (6n-4k)\binom{n-k}{\frac{n}{2}-k}/(n-k) \\ = & 2\binom{n-1}{\frac{n}{2}-1}[(n-2)/(n-1) - (3n-2k)(n/2-1)\cdots(n/2-k+1)/((n-k)(n-1) \\ & \qquad \cdots(n-k+1))] \\ \geq & 2\binom{n-1}{\frac{n}{2}-1}[(n-2)/(n-1) - 4(n/2-1)(n/2-2)/((n-1)(n-2))] \\ = & 4\binom{n-1}{\frac{n}{2}-1}/(n-1) > 0, \end{array}$$

by Equality (13) and Equality (15), one has

$$\max_{\text{odd wt}(\lambda)} |W_f(\lambda)| = |W(1,1,k)| = 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k). \tag{18}$$

On the other hand, for even $\text{wt}(\lambda)$, by Equality (8), one has

$$\max_{\lambda} |W_f(\lambda)| = 2\max_{\lambda} |\sum_{x\in A\setminus U} (-1)^{a_x+\lambda\cdot x}| \leq 2[\binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}] < |W(1,1,k)|.$$

Thus, according to the maximal value of $|W_f(\lambda)|$ for odd $\mathrm{wt}(\lambda)$, one has

$$\max_{\lambda\in\mathbb{F}_2^n}|W_f(\lambda)| = \max_{\text{odd } \mathrm{wt}(\lambda)}|W_f(\lambda)|. \tag{19}$$

From the analysis above, for $k=1$, by Equality (16) and Equality (19), one has

$$nl(f) = 2^{n-1} - |W(1,0,1)|/2 = 2^{n-1} - 2\binom{n-1}{\frac{n}{2}-1}.$$

For $k=2$, by Equality (17) and Equality (19), one has

$$nl(f) = 2^{n-1} - (3n-4)\binom{n-1}{\frac{n}{2}-1}/(2n-2).$$

For $k\geq 3$, by Equality (18) and Equality (19), one has

$$nl(f) = 2^{n-1} - |W(1,1,k)|/2 = 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k).$$

The proof is finished by the analysis above. □

Remark 1: By Theorem 3.3, the nonlinearity of f is related to the Hamming weight of the vector u. More precisely, $nl(f) < 2^{n-1} - \binom{n-1}{\frac{n}{2}-1}$ for $\mathrm{wt}(u)=1$, or 2, and $nl(f) > 2^{n-1} - \binom{n-1}{\frac{n}{2}-1}$ for $\mathrm{wt}(u)\geq 3$. Let $\Gamma_k = k\binom{n-k}{\frac{n}{2}-k}/(n-k)$. Then, $\Gamma_k/\Gamma_{k+1} = k(n-k-1)/[(n/2-k)(k+1)] > 1$ for all k, $3\leq k\leq n/2-2$. Thus, taking $\mathrm{wt}(u)=3$, by Theorem 3.3, f can obtain a nonlinearity $nl(f) = 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + 3\binom{n-3}{\frac{n}{2}-3}/(n-3)$.

According to the Boolean values of a_x, two sets L_0 and L_1 are defined as

$$L_0 = \{x\in W^{\frac{n}{2}} \mid a_x = 0\}\setminus U\cup\overline{U},\ L_1 = \{x\in W^{\frac{n}{2}} \mid a_x = 1\}\setminus U\cup\overline{U}.$$

Let

$$\Theta_k = |W^{\frac{n}{2}}\backslash U\cup\overline{U}|/2 = \binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}. \tag{20}$$

To ensure that f defined by (7) is balanced, the Boolean values a_x are required to be balanced on the set $W^{\frac{n}{2}}\backslash U\cup\overline{U}$, i.e., $|L_0| = |L_1| = \Theta_k$. In this case, the integer Θ_k must be even since $a_x = a_{\bar{x}}$. However, when Θ_k is odd, an nonlinear function f_0 obtained by slightly modifying f can be balanced.

The function $f_0\in B_n$ is defined as

$$f_0(x) = \begin{cases} 0, & x\in W^{<\frac{n}{2}}\cup\overline{T}_0\cup U_0\setminus T_0,\\ a_x, & x\in W^{\frac{n}{2}}\setminus U_0\cup\overline{U}_0,\\ 1, & x\in W^{>\frac{n}{2}}\cup T_0\cup\overline{U}_0\setminus\overline{T}_0,\end{cases} \tag{21}$$

where $a_x = a_{\overline{x}}\in\{0,1\}$, and the sets T_0 and U_0 are defined by

$$T_0 = \begin{cases} T, & \text{for even } \Theta_k,\\ T\backslash\{x_0\}, & \text{otherwise}\end{cases} \quad\text{and } U_0 = \begin{cases} U, & \text{for even } \Theta_k,\\ U\setminus\{u\oplus x_0\}, & \text{otherwise}\end{cases} \tag{22}$$

where x_0 is any one element of T. Similarly to the analysis after Equality (10), the pairwise disjoint sets T_0 and U_0 satisfy the conditions in (5), and $AI(f_0) = n/2$ by Corollary 3.2. With T_0 and U_0 in (22), one has $|W^{\frac{n}{2}}| - 2|U_0|\equiv 0 \pmod 4$. Then, f_0 is balanced if and only if a_x is balanced on the set $W^{\frac{n}{2}}\backslash U_0\cup\overline{U}_0$, which is easily satisfied when T_0 and U_0 are defined by (22). In this case, let $W_1\cup\overline{W}_1 = W^{\frac{n}{2}}\setminus U_0\cup\overline{U}_0$ and $W_1\cap\overline{W}_1 = \emptyset$. Then the set W_1 is divided into two disjoint subsets W_2 and W_3 such that $|W_2| = |W_3|$. On the set $W^{\frac{n}{2}}\backslash U_0\cup\overline{U}_0$, define the Boolean values a_x as

$$a_x = \begin{cases} b, & x\in W_2\cup\overline{W}_2,\\ b+1, & x\in W_3\cup\overline{W}_3\end{cases}$$

where $b\in\{0,1\}$.

Theorem 3.4. *Let u be any element of $W^{<\frac{n}{2}}$ such that $3 \leq \mathrm{wt}(u) = k \leq n/2-1$. If a_x is balanced on the set $W^{\frac{n}{2}}\backslash U_0 \cup \overline{U}_0$, then the function $f_0(x)$ defined in Equality (21) is balanced and its nonlinearity satisfies*

$$nl(f_0) = \begin{cases} 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k), & \text{for even } \Theta_k, \\ 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k) - 1, & \text{otherwise.} \end{cases}$$

Proof: By the analysis after (22), f_0 is balanced.

For even Θ_k, the proof follows from Theorem 3.3. Let us consider the case Θ_k odd.

When $\mathrm{wt}(\lambda) = t$ is odd, one has

$$\begin{cases} \sum\limits_{x\in T_0}(-1)^{\lambda\cdot x} = \sum\limits_{x\in T}(-1)^{\lambda\cdot x} - (-1)^{\lambda\cdot x_0} = K_{\frac{n}{2}-k}(s, n-k) - (-1)^{\lambda\cdot x_0}, \\ \sum\limits_{x\in U_0}(-1)^{\lambda\cdot x} = \sum\limits_{x\in T_0}(-1)^{\lambda\cdot(x\oplus u)} = (-1)^{t-s}[K_{\frac{n}{2}-k}(s, n-k) - (-1)^{\lambda\cdot x_0}] \end{cases}$$

where $\max\{0, t-k\} \leq s \leq \min\{t, n-k\}$. By Equality (8), the Walsh transform of $f_0(x)$ is calculated as

$$W_{f_0}(\lambda) = \begin{cases} 2K_{\frac{n}{2}-1}(t-1, n-1) - 2K_{\frac{n}{2}-k}(s, n-k) + 2(-1)^{\lambda\cdot x_0}, & \text{for odd } s, \\ 2K_{\frac{n}{2}-1}(t-1, n-1) - 6K_{\frac{n}{2}-k}(s, n-k) + 6(-1)^{\lambda\cdot x_0}, & \text{otherwise.} \end{cases} \tag{23}$$

Thus, for $k \geq 3$, by Equality (13), one has $\max\limits_{\lambda} |W_{f_0}(\lambda)| = |W(1,1,k)| + 2$ for $\mathrm{wt}(\lambda) = 1$ and by Equality (12) and Equality (15), $\max\limits_{\lambda} |W_{f_0}(\lambda)| \leq |W(3,0,k)| + 6$ for odd $3 \leq \mathrm{wt}(\lambda) \leq n-1$.

For even $\mathrm{wt}(\lambda)$, one has

$$\max_{\lambda} |W_{f_0}(\lambda)| = \max_{\lambda} |2\textstyle\sum_{x\in A\backslash U}(-1)^{a_x+\lambda\cdot x}| \leq 2(\binom{n-1}{\frac{n}{2}} - \binom{n-k}{\frac{n}{2}-k} + 1) \leq |W(1,1,k)|.$$

Similarly to the analysis in the proof of Theorem 3.3, one has

$$\begin{aligned} \max_{\lambda\in\mathbb{F}_2^n} |W_{f_0}(\lambda)| &= \max\{|W(1,1,k)| + 2, |W(3,0,k)| + 6\} \\ &= |W(1,1,k)| + 2 \\ &= 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k) + 2, \end{aligned}$$

which implies

$$nl(f_0) = 2^{n-1} - \max_{\lambda\in\mathbb{F}_2^n} |W_{f_0}(\lambda)|/2 = 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k) - 1.$$

The above analysis finishes the proof. □

Remark 2: To obtain balanced Boolean functions with high nonlinearities and optimum algebraic immunity, we only use the vector u with Hamming weight $3 \leq \mathrm{wt}(u) \leq n/2-1$. In this case, the resulting function f_0 has almost the same nonlinearity as f.

Notice that all elements in the set T defined by Equality (10) have the same Hamming weight $n/2-k$. Does there exist a set T, consisting of elements with different weights, such that the function f or f_0 has high nonlinearity? The following results provide an answer to this question.

For a fixed nonzero element $v_1 \in W^{<\frac{n}{2}}$ with $\mathrm{supp}(v_1) = \{i_1, i_2, \cdots, i_k\}$, take $v_2 \in W^{\leq\frac{n}{2}}$ with $\mathrm{supp}(v_2) = \{i_1, i_2, \cdots, i_k, i_{k+1}\}$. Denote

$$T^i = \{x \,|\, \mathrm{wt}(x) = n/2 - \mathrm{wt}(v_i),\ \mathrm{supp}(x) \cap \mathrm{supp}(v_2) = \emptyset\},\ U^i = \{x \oplus v_i \,|\, x \in T^i\} \tag{24}$$

for $i = 1, 2$. Two sets T and U are defined as

$$T = T^1 \cup T^2,\ U = U^1 \cup U^2.$$

Let the elements $x_1, x_2, \cdots, x_{|T|}$ of T be sorted by increasing Hamming weight. Correspondingly, the elements $y_1, y_2, \cdots, y_{|U|}$ of U are listed as: for $1 \le j \le |T|$, $y_j = x_j \oplus v_i$ if $x_j \in T^i$ $(i = 1, 2)$. From the definition above, it can be verified T and U satisfy the conditions in Equality (5). Furthermore, $S = \overline{T}$ and $V = \overline{U}$ also satisfy the conditions in Equality (5). Thus, by Corollary 2, one has $AI(f) = n/2$.

Denote

$$P = \{x \,|\, \mathrm{wt}(x) = n/2 - \mathrm{wt}(v_1),\ \mathrm{supp}(x) \cap \mathrm{supp}(v_1) = \emptyset\},\ P^2 = \{x \in P \,|\, x_{i_{k+1}} = 1\}, \tag{25}$$

then $T^1 = P \setminus P^2$. Moreover, the sets T and U can be expressed as

$$T = P \cup T^2 \setminus P^2 \text{ and } U = \{x \oplus v_1 \,|\, x \in P\}. \tag{26}$$

Note that the sets P, U are exactly the sets T and U given in Equality (10) when $v_1 = u$.

The nonlinearity of f is determined in the following theorem.

Theorem 3.5. *For $2 \le k \le n/2 - 2$, let $f \in B_n$ be defined in Equality (7) with $T = T^1 \cup T^2$ and $U = U^1 \cup U^2$, where T^i and U^i $(i = 1, 2)$ are given in Equality (24). Then its nonlinearity is*

$$nl(f) = \ 2^{n-1} - \tbinom{n-1}{\frac{n}{2}-1} + k\tbinom{n-k}{\frac{n}{2}-k}/(n-k).$$

Proof: The Walsh spectrum of f is considered as follows.

Without loss of generality, we can assume that $\mathrm{supp}(v_1) = \{1, 2, \cdots, k\}$ and $\mathrm{supp}(v_2) = \{1, 2, \cdots, k, k+1\}$, by Equality (26), it is true that

$$\begin{aligned} \sum_{x\in T} (-1)^{\lambda\cdot x} &= \sum_{x\in P} (-1)^{\lambda\cdot x} + \sum_{x\in T^2} (-1)^{\lambda\cdot x} - \sum_{x\in P^2} (-1)^{\lambda\cdot x} \\ &= \sum_{x\in P} (-1)^{\lambda\cdot x} + \sum_{x\in T^2} (-1)^{\lambda\cdot x} - (-1)^{\lambda_{k+1}} \sum_{x\in T^2} (-1)^{\lambda\cdot x}. \end{aligned}$$

Moreover, for $\lambda = (\lambda', \lambda'') \in \mathbb{F}_2^k \times \mathbb{F}_2^{n-k}$ with $\mathrm{wt}(\lambda'') = s$, $\sum\limits_{x\in T^2} (-1)^{\lambda\cdot x} = K_{\frac{n}{2}-k-1}(s-1, n-k-1)$ when $\lambda_{k+1} = 1$.

When $\mathrm{wt}(\lambda) = t$ is odd, since the set P, U can be regarded as T and U defined in Equality (10) where $u = v_1$, by Equalities (8), (11) and (12), one has

$$\begin{aligned} W_f(\lambda) &= 2 \sum_{x\in W^{<\frac{n}{2}}} (-1)^{\lambda\cdot x} - 4 \sum_{x\in T} (-1)^{\lambda\cdot x} + 2 \sum_{x\in U} (-1)^{\lambda\cdot x} \\ &= 2 \sum_{x\in W^{<\frac{n}{2}}} (-1)^{\lambda\cdot x} - 4 \sum_{x\in P} (-1)^{\lambda\cdot x} + 2 \sum_{x\in U} (-1)^{\lambda\cdot x} \\ &\qquad -4[\sum_{x\in T^2} (-1)^{\lambda\cdot x} - (-1)^{\lambda_{k+1}} \sum_{x\in T^2} (-1)^{\lambda\cdot x}] \\ &= \begin{cases} W(t, s, k), & \lambda_{k+1} = 0 \\ W(t, s, k) - 8K_{\frac{n}{2}-k-1}(s-1, n-k-1), & \lambda_{k+1} = 1 \end{cases} \end{aligned} \tag{27}$$

where $\max\{0, t-k\} \le s \le \{t, n-k\}$.

For $t = 1$, the integer s may take 0 or 1. Then, $W_f(\lambda) = W(1, 0, k)$ when $s = 0$, and $W_f(\lambda)$ is equal to $W(1, 1, k)$ or $W(1, 1, k) - 8\tbinom{n-k-1}{\frac{n}{2}-k-1}$ when $s = 1$. Thus, by Equality (13), it can be verified that

$$\max_{\mathrm{wt}(\lambda)=1} |W_f(\lambda)| = |W(1, 1, k)| = 2\tbinom{n-1}{\frac{n}{2}-1} - 2k\tbinom{n-k}{\frac{n}{2}-k}/(n-k). \tag{28}$$

For $3 \leq t \leq n-1$, when $k=2$, one has $n \geq 8$. If $\lambda_{k+1}=0$, then $t-2 \leq s \leq \min\{t, n-3\}$. By Equalities (27) and (12), and by Lemmas 2.4 and 2.5, one has

$$\begin{array}{rcl} |W_f(\lambda)| & \leq & 2|K_{\frac{n}{2}-1}(t-1,n-1)| + 6|K_{\frac{n}{2}-2}(s,n-2)| \\ & \leq & 2|K_{\frac{n}{2}-1}(2,n-1)| + 6|K_{\frac{n}{2}-2}(1,n-2)| \\ & = & 8\binom{n-1}{\frac{n}{2}-1}/(n-1) < (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) \\ & = & |W(1,1,2)|. \end{array}$$

If $\lambda_{k+1}=1$, then $t-2 \leq s \leq \min\{t, n-2\}$. By Equalities (27) and (12), for odd s, one has

$$\begin{array}{rcl} |W_f(\lambda)| & \leq & 2|K_{\frac{n}{2}-1}(t-1,n-1)| + 2|K_{\frac{n}{2}-2}(s,n-2)| + 8|K_{\frac{n}{2}-3}(s-1,n-3)| \\ & \leq & 2|K_{\frac{n}{2}-1}(2,n-1)| + 2|K_{\frac{n}{2}-2}(1,n-2)| + 8|K_{\frac{n}{2}-3}(0,n-3)| \\ & = & 4\binom{n-1}{\frac{n}{2}-1}/(n-1) + 8\binom{n-3}{\frac{n}{2}-3} = (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) \\ & = & |W(1,1,2)|, \end{array}$$

and for even $s=t-1$, the fact

$$|W_f(\lambda)| = |2K_{\frac{n}{2}-1}(t-1,n-1) - 6K_{\frac{n}{2}-2}(t-1,n-2) - 8K_{\frac{n}{2}-3}(t-2,n-3)| \leq |W(1,1,2)|$$

will be proved by the three cases (i), (ii) and (iii) as follows.

(i) For $t=3$, since $K_{\frac{n}{2}-1}(2,n-1)<0$, $K_{\frac{n}{2}-2}(2,n-2)<0$ and $K_{\frac{n}{2}-3}(1,n-3)>0$, one has

$$\begin{array}{rcl} |W_f(\lambda)| & = & |2K_{\frac{n}{2}-1}(2,n-1) - 6K_{\frac{n}{2}-2}(2,n-2) - 8K_{\frac{n}{2}-3}(1,n-3)| \\ & \leq & 2|K_{\frac{n}{2}-1}(2,n-1)| + 8|K_{\frac{n}{2}-3}(1,n-3)| \\ & < & 2|K_{\frac{n}{2}-1}(2,n-1)| + 8|K_{\frac{n}{2}-3}(0,n-3)| \\ & = & (2n-6)\binom{n-1}{\frac{n}{2}-1}/(n-1) < |W(1,1,2)|. \end{array}$$

(ii) For $5 \leq t \leq n-3$, by Lemmas 2.4 and 2.5, one has

$$\begin{array}{rcl} |W_f(\lambda)| & \leq & 2|K_{\frac{n}{2}-1}(t-1,n-1)| + 6|K_{\frac{n}{2}-2}(t-1,n-2)| + 8|K_{\frac{n}{2}-3}(t-2,n-3)| \\ & < & 2|K_{\frac{n}{2}-1}(4,n-1)| + 6|K_{\frac{n}{2}-2}(1,n-2)| + 8|K_{\frac{n}{2}-3}(1,n-3)| \\ & = & 12\binom{n-1}{\frac{n}{2}-1}/(n-1) \leq (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) = |W(1,1,2)|. \end{array}$$

(iii) For $t=n-1$, one has

$$\begin{array}{rcl} |W_f(\lambda)| & = & |2K_{\frac{n}{2}-1}(n-2,n-1) - 6K_{\frac{n}{2}-2}(n-2,n-2) - 8K_{\frac{n}{2}-3}(n-3,n-3)| \\ & = & |2(-1)^{\frac{n}{2}-1}\binom{n-1}{\frac{n}{2}-1}/(n-1) - 6(-1)^{\frac{n}{2}-2}\binom{n-2}{\frac{n}{2}-2} - 8(-1)^{\frac{n}{2}-3}\binom{n-3}{\frac{n}{2}-3}| \\ & = & (n+4)\binom{n-1}{\frac{n}{2}-1}/(n-1) \leq (2n-4)\binom{n-1}{\frac{n}{2}-1}/(n-1) = |W(1,1,2)|. \end{array}$$

Therefore, when $k=2$, it can be concluded

$$\max_{3\leq t\leq n-1} |W_f(\lambda)| = |W(1,1,k)|. \tag{29}$$

When $k \geq 3$, the value of $\max\limits_{3\leq t\leq n-1} |W_f(\lambda)|$ is similarly considered in the following.

If $\lambda_{k+1}=0$, Equalities (27) and (15) imply

$$\max_{3\leq t\leq n-1} |W_f(\lambda)| = \max_{3\leq t\leq n-1} |W(t,s,k)| = 2\binom{n-1}{\frac{n}{2}-1}/(n-1) + 6\binom{n-k}{\frac{n}{2}-k},$$

and if $\lambda_{k+1} = 1$, one has $1 \leq s \leq \min\{t, n-k\}$. By Equalities (27) and (12), for odd s,

$$\begin{aligned}
|W_f(\lambda)| &\leq 2|K_{\frac{n}{2}-1}(t-1, n-1)| + 2|K_{\frac{n}{2}-k}(s, n-k)| + 8|K_{\frac{n}{2}-k-1}(s-1, n-k-1)| \\
&\leq 2|K_{\frac{n}{2}-1}(2, n-1)| + 2|K_{\frac{n}{2}-k}(0, n-k)| + 8|K_{\frac{n}{2}-k-1}(0, n-k-1)| \\
&= 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 2\tbinom{n-k}{\frac{n}{2}-k} + 8\tbinom{n-k-1}{\frac{n}{2}-k-1} \\
&= 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 2\tbinom{n-k}{\frac{n}{2}-k} + 4(n-2k)\tbinom{n-k}{\frac{n}{2}-k}/(n-k) \\
&< 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 6\tbinom{n-k}{\frac{n}{2}-k}.
\end{aligned}$$

For even s, when $2 \leq s < n-k$,

$$\begin{aligned}
|W_f(\lambda)| &\leq 2|K_{\frac{n}{2}-1}(t-1, n-1)| + 6|K_{\frac{n}{2}-k}(s, n-k)| + 8|K_{\frac{n}{2}-k-1}(s-1, n-k-1)| \\
&\leq 2|K_{\frac{n}{2}-1}(2, n-1)| + 6|K_{\frac{n}{2}-k}(1, n-k)| + 8|K_{\frac{n}{2}-k-1}(0, n-k-1)| \\
&= 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 6k\tbinom{n-k}{\frac{n}{2}-k}/(n-k) + 4(n-2k)\tbinom{n-k}{\frac{n}{2}-k}/(n-k) \\
&= 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + (4n-2k)\tbinom{n-k}{\frac{n}{2}-k}/(n-k) \\
&< 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 6\tbinom{n-k}{\frac{n}{2}-k},
\end{aligned}$$

and when $s = n-k$ for even k,

$$\begin{aligned}
|W_f(\lambda)| &= |2K_{\frac{n}{2}-1}(t-1, n-1) - 6K_{\frac{n}{2}-k}(n-k, n-k) - 8K_{\frac{n}{2}-k-1}(n-k-1, n-k-1)| \\
&\leq 2|K_{\frac{n}{2}-1}(t-1, n-1)| + |6K_{\frac{n}{2}-k}(n-k, n-k) + 8K_{\frac{n}{2}-k-1}(n-k-1, n-k-1)| \\
&\leq 2|K_{\frac{n}{2}-1}(2, n-1)| + |6\tbinom{n-k}{\frac{n}{2}-k} - (4n-2k)\tbinom{n-k}{\frac{n}{2}-k}/(n-k)| \\
&< 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 6\tbinom{n-k}{\frac{n}{2}-k}.
\end{aligned}$$

From the above discussion, one has

$$\max_{3 \leq t \leq n-1} |W_f(\lambda)| = 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 6\tbinom{n-k}{\frac{n}{2}-k} < |W(1,1,k)| \tag{30}$$

when $k \geq 3$.

Therefore, for $k \geq 2$, by Equalities (28) and (29), by (30), one has

$$\max_{\text{odd wt}(\lambda)} |W_f(\lambda)| = |W(1,1,k)| = 2\tbinom{n-1}{\frac{n}{2}-1} - 2k\tbinom{n-k}{\frac{n}{2}-k}/(n-k).$$

On the other hand, Equality (8) implies

$$\max_{\text{even wt}(\lambda)} |W_f(\lambda)| \leq 2|A \backslash U| = 2\tbinom{n-1}{\frac{n}{2}-1} - 2\tbinom{n-k}{\frac{n}{2}-k} < |W(1,1,k)|.$$

Thus, one has

$$nl(f) = 2^{n-1} - |W(1,1,k)|/2 = 2^{n-1} - \tbinom{n-1}{\frac{n}{2}-1} + k\tbinom{n-k}{\frac{n}{2}-k}/(n-k),$$

which finishes the proof. □

By slightly modifying f, a highly nonlinear balanced function f_1 can be obtained.

Define $f_1 \in B_n$ as

$$f_1(x) = \begin{cases} 0, & x \in W^{<\frac{n}{2}} \cup \overline{T}_1 \cup U_1 \setminus T_1, \\ a_x, & x \in W^{\frac{n}{2}} \setminus U_1 \cup \overline{U}_1, \\ 1, & x \in W^{>\frac{n}{2}} \cup T_1 \cup \overline{U}_1 \setminus \overline{T}_1, \end{cases} \tag{31}$$

where $a_x = a_{\overline{x}} \in \{0, 1\}$, and the sets T_1 and U_1 are defined by

$$T_1 = \begin{cases} T, & \text{for even } \Theta_k, \\ T\backslash\{x_1\}, & \text{otherwise} \end{cases} \quad \text{and} \quad U_1 = \begin{cases} U, & \text{for even } \Theta_k, \\ U \setminus \{x_1 \oplus v_1\}, & \text{otherwise} \end{cases}$$

where x_1 is any one element of T^1. Similar to the analysis after Equality (24), the pairwise disjoint sets T_1 and U_1 satisfy the conditions in Equality (5), hence $AI(f_1) = n/2$.

With the same method used in the proof for Theorem 3.4, the nonlinearity of f_1 can be measured in the following.

Theorem 3.6. *For $2 \le k \le n/2-2$, if a_x is balanced on the set $W^{\frac{n}{2}} \backslash U_1 \cup \overline{U}_1$, then the function $f_1(x)$ defined in Equality (31) is balanced and its nonlinearity satisfies*

$$nl(f_1) = \begin{cases} 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k), & \text{for even } \Theta_k, \\ 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k) - 1, & \text{otherwise.} \end{cases}$$

Remark 3: Above results show T_1 can consist of elements with different weights, and as described in Remark 1, by taking $k = 2$, the balanced function f_1 can obtain nonlinearity $2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + 2\binom{n-2}{\frac{n}{2}-2}/(n-2)$ since $\Theta_2 = \binom{n-1}{\frac{n}{2}-1} - \binom{n-2}{\frac{n}{2}-2} = \binom{n-2}{\frac{n}{2}-1}$ is always even.

Case 2: $S = V = \emptyset$ or $T = U = \emptyset$.

We only consider the case of $S = V = \emptyset$. The similar conclusions can also be obtained for the case of $T = U = \emptyset$.

In this case, with restriction $a_x = 0$ for $x \in \overline{U}$, the function defined by (4) can be rewritten as

$$f(x) = \begin{cases} 0, & x \in W^{<\frac{n}{2}} \cup U \cup \overline{U} \setminus T, \\ a_x, & x \in W^{\frac{n}{2}} \setminus U \cup \overline{U}, \\ 1, & x \in W^{>\frac{n}{2}} \cup T, \end{cases} \tag{32}$$

where $a_x = a_{\overline{x}}$. Then, by Equality (6), one has

$$\begin{aligned} W_f(\lambda) &= \sum_{x\in W^{<\frac{n}{2}}} (-1)^{\lambda\cdot x} + 2\sum_{x\in T} (-1)^{\lambda\cdot x+1} + \sum_{x\in U} (-1)^{\lambda\cdot x} + \sum_{x\in \overline{U}} (-1)^{\lambda\cdot x} \\ &\quad + \sum_{x\in W^{\frac{n}{2}}\backslash U\cup\overline{U}} (-1)^{a_x+\lambda\cdot x} + \sum_{x\in W^{>\frac{n}{2}}} (-1)^{\lambda\cdot x+1} \\ &= \sum_{x\in W^{<\frac{n}{2}}} [(-1)^{\lambda\cdot x} + (-1)^{\lambda\cdot(x\oplus\underline{1})+1}] + \sum_{x\in U} [(-1)^{\lambda\cdot x} + (-1)^{\lambda\cdot(x\oplus\underline{1})}] \\ &\quad +2\sum_{x\in T} (-1)^{\lambda\cdot x+1} + \sum_{x\in A\backslash U} [(-1)^{a_x+\lambda\cdot x} + (-1)^{a_x+\lambda\cdot(x\oplus\underline{1})}] \end{aligned} \tag{33}$$

where A is a subset of $W^{\frac{n}{2}}$ defined by (9).

For $u \in W^{<\frac{n}{2}}$ with $3 \le \mathrm{wt}(u) = k \le \lfloor\frac{n}{4}\rfloor$, let T and U be defined as in Equality (10).

Let x_2 be any element of T. Take

$$T_2 = \begin{cases} T, & \text{for even } \Theta_k, \\ T\backslash\{x_2\}, & \text{otherwise} \end{cases} \quad \text{and } U_2 = \begin{cases} U, & \text{for even } \Theta_k, \\ U\backslash\{x_2 \oplus u\}, & \text{otherwise} \end{cases} \tag{34}$$

where Θ_k is given in Equality (20). Define a function $f_2 \in B_n$ by

$$f_2(x) = \begin{cases} 0, & x \in W^{<\frac{n}{2}} \cup U_2 \cup \overline{U}_2 \setminus T_2, \\ a_x, & x \in W^{\frac{n}{2}} \setminus U_2 \cup \overline{U}_2, \\ 1, & x \in W^{>\frac{n}{2}} \cup T_2, \end{cases} \tag{35}$$

where $a_x = a_{\overline{x}} \in \{0, 1\}$. By Proposition 3.1, one has $AI(f_2) = n/2$. The nonlinearity and balancedness of $f_2(x)$ are analyzed in the following theorem.

Theorem 3.7. *Let $n \ge 12$ and $u \in W^{<\frac{n}{2}}$ with $3 \le \mathrm{wt}(u) = k \le \lfloor\frac{n}{4}\rfloor$. If a_x is balanced on the set $W^{\frac{n}{2}} \backslash U_2 \cup \overline{U}_2$ and $f_2(x_2 \oplus u) = 0$, then $f_2(x)$ is balanced and its nonlinearity satisfies*

$$nl(f_2) = \begin{cases} 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k), & \text{for even } \Theta_k, \\ 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k) - 1, & \text{otherwise} \end{cases}$$

when k is even or $k = 3$.

Proof: By Equality (35), the Hamming weight of $f_2(x)$ is equal to

$$|W^{>\frac{n}{2}}| + |T_2| + \frac{1}{2}|W^{\frac{n}{2}} \backslash U_2 \cup \overline{U}_2| = 2^{n-1},$$

which shows the function $f_2(x)$ is balanced.

Equality (33) implies

$$W_{f_2}(\lambda) = \begin{cases} 2 \sum\limits_{x \in W^{<\frac{n}{2}}} (-1)^{\lambda \cdot x} - 2 \sum\limits_{x \in T_2} (-1)^{\lambda \cdot x}, & \text{for odd } \mathrm{wt}(\lambda), \\ \\ 2 \sum\limits_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x} - 2 \sum\limits_{x \in T_2} (-1)^{\lambda \cdot x} + 2 \sum\limits_{x \in U_2} (-1)^{\lambda \cdot x}, & \text{otherwise.} \end{cases} \tag{36}$$

When Θ_k is even, similarly to the proof of Theorem 3.3, one has

$$W_{f_2}(\lambda) = \begin{cases} 2K_{\frac{n}{2}-1}(t-1, n-1) - 2K_{\frac{n}{2}-k}(s, n-k), & \text{for odd } t \text{ and } 0 \le s \le t, \\ 2\sum_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x} - 4K_{\frac{n}{2}-k}(s, n-k), & \text{for even } t \text{ and odd } s \le t-1, \\ 2\sum_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x}, & \text{for even } t \text{ and even } s \le t, \end{cases} \tag{37}$$

where $\mathrm{wt}(\lambda) = t$ and $t - k \le s \le \min\{t, n-k\}$.

For odd t with $3 \le t \le n-1$, by Lemma 2.4, one has

$$\begin{aligned} \max |W_{f_2}(\lambda)| &\le 2|K_{\frac{n}{2}-1}(t-1, n-1)| + 2|K_{\frac{n}{2}-k}(s, n-k)| \\ &\le 2|K_{\frac{n}{2}-1}(2, n-1)| + 2K_{\frac{n}{2}-k}(0, n-k) \\ &= 2\tbinom{n-1}{\frac{n}{2}-1}/(n-1) + 2\tbinom{n-k}{\frac{n}{2}-k}. \end{aligned}$$

When $t = 1$, the maximal value of $|W_{f_2}(\lambda)|$ is equal to $2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k)$.

Thus, one has

$$\max_{\text{odd } wt(\lambda)} |W_{f_2}(\lambda)| = 2\tbinom{n-1}{\frac{n}{2}-1} - 2k\tbinom{n-k}{\frac{n}{2}-k}/(n-k). \tag{38}$$

For even $\mathrm{wt}(\lambda) = t$, the maximal value of $|W_{f_2}(\lambda)|$ is determined below.

Similarly to the analysis after (22), a_x is balanced on $A \backslash U_2$ since a_x is balanced on $W^{\frac{n}{2}} \backslash U_2 \cup \overline{U}_2$ with $a_x = a_{\overline{x}}$. Then, by Lemma 2.7, one has

$$\begin{aligned} & 2|\textstyle\sum_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x}| \\ \le\ & 2|A \backslash U_2| - 2|\textstyle\sum_{x \in A \backslash U_2} (-1)^{\lambda \cdot x}| \\ =\ & 2[\tbinom{n-1}{\frac{n}{2}-1} - \tbinom{n-k}{\frac{n}{2}-k}] - 2|\textstyle\sum_{x \in A} (-1)^{\lambda \cdot x} - \sum_{x \in U_2} (-1)^{\lambda \cdot x}| \\ =\ & 2[\tbinom{n-1}{\frac{n}{2}-1} - \tbinom{n-k}{\frac{n}{2}-k}] - |\textstyle\sum_{x \in W^{\frac{n}{2}}} (-1)^{\lambda \cdot x} - 2\sum_{x \in U_2} (-1)^{\lambda \cdot x}| \\ =\ & 2[\tbinom{n-1}{\frac{n}{2}-1} - \tbinom{n-k}{\frac{n}{2}-k}] - |K_{\frac{n}{2}}(t, n) - 2(-1)^{t-s} K_{\frac{n}{2}-k}(s, n-k)|. \end{aligned}$$

For odd $s \le \min\{t-1, n-k\}$, by Equality (37), one has

$$\begin{aligned} |W_{f_2}(\lambda)| &= |2\textstyle\sum_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x} - 4K_{\frac{n}{2}-k}(s, n-k)| \\ &\le 2|\textstyle\sum_{x \in A \backslash U_2} (-1)^{a_x + \lambda \cdot x}| + 4|K_{\frac{n}{2}-k}(s, n-k)| \\ &\le 2[\tbinom{n-1}{\frac{n}{2}-1} - \tbinom{n-k}{\frac{n}{2}-k}] - |K_{\frac{n}{2}}(t, n) + 2K_{\frac{n}{2}-k}(s, n-k)| + 4|K_{\frac{n}{2}-k}(s, n-k)|. \end{aligned} \tag{39}$$

When k is even, by Lemma 2.5, one has

$$\max_{1 \le s \le n-k-1} |K_{\frac{n}{2}-k}(s, n-k)| = K_{\frac{n}{2}-k}(1, n-k) = k\tbinom{n-k}{\frac{n}{2}-k}/(n-k). \tag{40}$$

Then, by (39) and Equality (40), one has

$$\begin{array}{rcl} |W_{f_2}(\lambda)| & \leq & 2[\binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}] + 4 \max\limits_{1\leq s\leq n-k-1} |K_{\frac{n}{2}-k}(s, n-k)| \\ & = & 2[\binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}] + 4k\binom{n-k}{\frac{n}{2}-k}/(n-k) \\ & = & 2\binom{n-1}{\frac{n}{2}-1} - (2n-6k)\binom{n-k}{\frac{n}{2}-k}/(n-k) \\ & \leq & 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k) \end{array} \tag{41}$$

for even $k \leq \lfloor \frac{n}{4} \rfloor$.

When $k = 3$, by Lemma 2.5, one has

$$\max_{1\leq s\leq n-5} |K_{\frac{n}{2}-3}(s, n-3)| = K_{\frac{n}{2}-3}(1, n-3) = 3\binom{n-3}{\frac{n}{2}-3}/(n-3),$$

then

$$\begin{array}{l} 4|K_{\frac{n}{2}-3}(s, n-3)| - |K_{\frac{n}{2}}(t, n) + 2K_{\frac{n}{2}-3}(s, n-3)| \\ \leq 4|K_{\frac{n}{2}-3}(s, n-3)| \leq 12\binom{n-3}{\frac{n}{2}-3}/(n-3) \leq (2n-12)\binom{n-3}{\frac{n}{2}-3}/(n-3) \end{array} \tag{42}$$

for $1 \leq s \leq n-5$. In the case of $s = n-3$, one has $t = n-2$ or n. Moreover, by Proposition 2.2 and Proposition 5 in [13], one has

$$\begin{array}{l} 4|K_{\frac{n}{2}-3}(n-3, n-3)| - |K_{\frac{n}{2}}(n-2, n) + 2K_{\frac{n}{2}-3}(n-3, n-3)| \\ = 4\binom{n-3}{\frac{n}{2}-3} - |(-1)^{n/2-1}\binom{n}{\frac{n}{2}}/(n-1) + 2(-1)^{n/2-3}\binom{n-3}{\frac{n}{2}-3}| \\ = 2\binom{n-3}{\frac{n}{2}-3} - \binom{n}{\frac{n}{2}}/(n-1) \\ = 2\binom{n-3}{\frac{n}{2}-3} - 8\binom{n-3}{\frac{n}{2}-3}/(n-4) \\ = (2n-16)\binom{n-3}{\frac{n}{2}-3}/(n-4) \\ < (2n-12)\binom{n-3}{\frac{n}{2}-3}/(n-3) \end{array}$$

and

$$\begin{array}{l} 4|K_{\frac{n}{2}-3}(n-3, n-3)| - |K_{\frac{n}{2}}(n, n) + 2K_{\frac{n}{2}-3}(n-3, n-3)| \\ = 4\binom{n-3}{\frac{n}{2}-3} - |(-1)^{n/2}\binom{n}{\frac{n}{2}} + 2(-1)^{n/2-3}\binom{n-3}{\frac{n}{2}-3}| \\ = 4\binom{n-3}{\frac{n}{2}-3} - [\binom{n}{\frac{n}{2}} - 2\binom{n-3}{\frac{n}{2}-3}] \\ = 6\binom{n-3}{\frac{n}{2}-3} - 8(n-1)\binom{n-3}{\frac{n}{2}-3}/(n-4) \\ < (2n-12)\binom{n-3}{\frac{n}{2}-3}/(n-3). \end{array}$$

Thus,

$$4|K_{\frac{n}{2}-3}(s, n-3)| - |K_{\frac{n}{2}}(t, n) + 2K_{\frac{n}{2}-3}(s, n-3)| \leq (2n-12)\binom{n-3}{\frac{n}{2}-3}/(n-3) \tag{43}$$

for $s = n-3$. By (42) and (43), one has

$$4|K_{\frac{n}{2}-3}(s, n-3)| - |K_{\frac{n}{2}}(t, n) + 2K_{\frac{n}{2}-3}(s, n-3)| \leq (2n-12)\binom{n-3}{\frac{n}{2}-3}/(n-3).$$

Furthermore, by (39), it can be proven that

$$\begin{array}{rcl} |W_{f_2}(\lambda)| & \leq & 2[\binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}] - |K_{\frac{n}{2}}(t, n) + 2K_{\frac{n}{2}-k}(s, n-k)| + 4|K_{\frac{n}{2}-k}(s, n-k)| \\ & \leq & 2[\binom{n-1}{\frac{n}{2}-1} - \binom{n-k}{\frac{n}{2}-k}] + (2n-4k)\binom{n-k}{\frac{n}{2}-k}/(n-k) \\ & = & 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k) \end{array} \tag{44}$$

for $k = 3$.

For even $0 \leq s \leq t$, by Equality (37), one has

$$|W_{f_2}(\lambda)| \leq 2\binom{n-1}{\frac{n}{2}-1} - 2\binom{n-k}{\frac{n}{2}-k} < 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k). \tag{45}$$

Thus, by (41), (44) and (45), one has

$$\max_{\text{even wt}(\lambda)} |W_{f_2}(\lambda)| \le 2\binom{n-1}{\frac{n}{2}-1} - 2k\binom{n-k}{\frac{n}{2}-k}/(n-k) \tag{46}$$

when k is even or $k = 3$.

By Equality (38) and by (46), one has

$$nl(f_2) = 2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + k\binom{n-k}{\frac{n}{2}-k}/(n-k).$$

When Θ_k is odd, the conclusion can be proven similarly to the method used in Theorem 3.4. □

To end this subsection, the nonlinearities of the constructed functions are compared with those of some known functions with optimal algebraic immunity.

Let $n = 2m$. Both symmetric functions $F(x)$ from Construction 3 in [13] and (unbalanced) $\phi_{2m}(x)$ from Construction 2 in [6] have optimal algebraic immunity. Moreover, they have the same nonlinearity $2^{n-1} - \binom{n-1}{\frac{n}{2}-1}$. By changing the initializations, the function ϕ_{2m} can be balanced [6]. However, the nonlinearity will be reduced. In this paper, the functions f_0, f_1 and f_2 are balanced, and their nonlinearities are higher than $nl(F)$ and $nl(\phi_{2m})$. Take $\text{wt}(u) = 3$ in Theorems 3.4 and 3.7, and take $\text{wt}(v_1) = 2$ in Theorem 3.6. For even n, $8 \le n \le 20$, the nonlinearities of these functions are compared as in Table 1.

Table 1 Comparison of nonlinearities

n	8	10	12	14	16	18	20
$nl(f_0)$, $nl(f_2)$	96	394	1614	6566	26630	107762	435342
$nl(f_1)$	98	400	1628	6608	26762	108192	436772
$nl(F)$, $nl(\phi_{2m})$	93	386	1586	6476	26333	106762	431910

The nonlinearity of f_2 is determined for $\text{wt}(u) \le \lfloor \frac{n}{4} \rfloor$ in Theorem 3.6. Then, when $\text{wt}(u) = 3$, one has $n \ge 12$. However, by randomly choosing a_x such that it is balanced on $W^{\frac{n}{2}} \backslash U_2 \cup \overline{U}_2$, balanced functions f_2 with nonlinearity 96, 394 respectively for $n = 8$, 10 can be obtained.

3.2. **Algebraic degree of the constructed functions.**

In this subsection, the algebraic degree of balanced functions f_0, f_1 and f_2 is studied.

Theorem 3.8. *Let the function f_0, f_1 be given in Section 3.1.*

(1) When Θ_k is odd, $\deg(f_0) = \deg(f_1) = n - 1$*;*

(2) When Θ_k is even, if either $(\binom{n-1}{\frac{n}{2}} + \binom{n-k}{\frac{n}{2}})/2$ or $\binom{n-k-1}{\frac{n}{2}-k}$ is odd, $\deg(f_0) = \deg(f_1) = n-1$.

Proof: With the same method, the results about the algebraic degree of f_0 and f_1 can be obtained. We only give the proof for $\deg(f_0)$ in the following.

Since f_0 is balanced, one has $\deg(f_0) \le n - 1$. By Equality (21), the support set $\text{supp}(f_0)$ can be expressed as

$$\text{supp}(f_0) = (\{x \in W^{\frac{n}{2}} \mid a_x = 1\} \setminus U_0 \cup \overline{U}_0) \cup W^{>\frac{n}{2}} \cup T_0 \cup \overline{U}_0 \setminus \overline{T}_0.$$

Let $f_0(x) = \sum_{\nu \in \mathbb{F}_2^n} \widetilde{f}_\nu x^\nu$ be the algebraic normal form (ANF) of f_0. Since $\widetilde{f}_\nu = \sum_{x \preceq \nu} f_0(x)$ for each $\nu \in \mathbb{F}_2^n$, $\widetilde{f}_\nu = 1$ if and only if

$$\begin{aligned} |C_\nu \cap \text{supp}(f_0)| = |C_\nu \cap (\{x \in W^{\frac{n}{2}} \mid a_x = 1\} \setminus U_0 \cup \overline{U}_0)| + \\ |C_\nu \cap W^{>\frac{n}{2}}| + |C_\nu \cap T_0| + |C_\nu \cap \overline{U}_0| - |C_\nu \cap \overline{T}_0| \end{aligned} \tag{47}$$

is odd.

For any $\alpha \in W^{n-1}$, either $x \preceq \alpha$ or $\overline{x} \preceq \alpha$ holds for each $x \in \mathbb{F}_2^n$. Then one has

$$|C_\alpha \cap (\{x \in W^{\frac{n}{2}} \mid a_x = 1\} \setminus U_0 \cup \overline{U}_0)| = (|W^{\frac{n}{2}}| - |U_0| - |\overline{U}_0|)/4 = (\tbinom{n-1}{\frac{n}{2}} - |T_0|)/2$$

since $a_x = a_{\overline{x}}$ is balanced on $W^{\frac{n}{2}} \setminus U_0 \cup \overline{U}_0$ and

$$|C_\alpha \cap W^{>\frac{n}{2}}| = \tbinom{n-1}{\frac{n}{2}+1} + \cdots + \tbinom{n-1}{n-1} = 2^{n-2} - \tbinom{n-1}{\frac{n}{2}}.$$

Thus,

$$|C_\alpha \cap (\{x \in W^{\frac{n}{2}} \mid a_x = 1\} \setminus U_0 \cup \overline{U}_0)| + |C_\alpha \cap W^{>\frac{n}{2}}| = 2^{n-2} - (\tbinom{n-1}{\frac{n}{2}} + |T_0|)/2. \tag{48}$$

When Θ_k is odd, $T_0 = T \backslash \{x_0\}$, $\overline{T}_0 = \overline{T} \backslash \{\overline{x}_0\}$ and $\overline{U}_0 = \overline{U} \backslash \{\overline{x}_0 \oplus u\}$. Then, there exist two elements $\alpha_1,\ \alpha_2 \in W^{n-1}$ such that

$$u \preceq \alpha_1,\ x_0 \preceq \alpha_1,\ u \preceq \alpha_2, \text{ and } x_0 \npreceq \alpha_2,$$

by which one has

$$\begin{cases} |C_{\alpha_1} \cap T_0| = \tbinom{n-k-1}{\frac{n}{2}-k} - 1, \\ |C_{\alpha_1} \cap \overline{U}_0| = |C_{\alpha_1} \cap \overline{T}_0|, \end{cases} \begin{cases} |C_{\alpha_2} \cap T_0| = \tbinom{n-k-1}{\frac{n}{2}-k}, \\ |C_{\alpha_2} \cap \overline{U}_0| = |C_{\alpha_2} \cap \overline{T}_0|. \end{cases}$$

Therefore, by Equality (47) and Equality (48), either $|C_{\alpha_1} \cap \mathrm{supp}(f_0)|$ or $|C_{\alpha_2} \cap \mathrm{supp}(f_0)|$ is odd, i.e., either $\widetilde{f}_{\alpha_1} = 1$ or $\widetilde{f}_{\alpha_2} = 1$. This implies $\deg(f_0) = n-1$.

When Θ_k is even, $T_0 = T$. Take α_1 in W^{n-1} with $u \preceq \alpha_1$, then

$$|C_{\alpha_1} \cap T_0| = \tbinom{n-k-1}{\frac{n}{2}-k},\ |C_{\alpha_1} \cap \overline{U}_0| = |C_{\alpha_1} \cap \overline{T}_0|.$$

By Equality (47) and Equality (48), one has

$$|C_{\alpha_1} \cap \mathrm{supp}(f_0)| = 2^{n-2} - (\tbinom{n-1}{\frac{n}{2}} + \tbinom{n-k}{\frac{n}{2}})/2 + \tbinom{n-k-1}{\frac{n}{2}-k}. \tag{49}$$

Take α_2 in W^{n-1} with $u \npreceq \alpha_2$, then

$$|C_{\alpha_2} \cap T_0| = \tbinom{n-k}{\frac{n}{2}-k},\ |C_{\alpha_2} \cap \overline{U}_0| = \tbinom{n-k}{\frac{n}{2}},\ |C_{\alpha_2} \cap \overline{T}_0| = 0.$$

By Equality (47) and by (48), one has

$$|C_{\alpha_2} \cap \mathrm{supp}(f_0)| = 2^{n-2} - (\tbinom{n-1}{\frac{n}{2}} + \tbinom{n-k}{\frac{n}{2}})/2 + 2\tbinom{n-k}{\frac{n}{2}}. \tag{50}$$

Thus, by Equality (49) and Equality (50), if $(\tbinom{n-1}{\frac{n}{2}} + \tbinom{n-k}{\frac{n}{2}})/2$ is odd, then $\widetilde{f}_{\alpha_2} = 1$. Otherwise, if $\tbinom{n-k-1}{\frac{n}{2}-k}$ is odd, then $\widetilde{f}_{\alpha_1} = 1$. Thus, $\deg(f_0) = n-1$. □

The following results can be obtained by the same method as for Theorem 3.8.

Theorem 3.9. *Let the balanced function f_2 be given in Theorem 3.7.*

(1) When Θ_k is odd, $\deg(f_2) = n-1$*;*

(2) When Θ_k is even, if either $\tbinom{n-k-1}{\frac{n}{2}-k} - (\tbinom{n-1}{\frac{n}{2}} + \tbinom{n-k}{\frac{n}{2}})/2$ or $\tbinom{n-k-1}{\frac{n}{2}}$ is odd, $\deg(f_2) = n-1$.

4. The nonlinearity of a class of Boolean functions with optimum algebraic immunity, in odd number of variables

This section determines the nonlinearity of a class of Boolean functions, included in Carlet's construction [4], in odd number of variables.

Construction 2: [4] Let n be odd, and let $a_1, a_2, \cdots, a_{\binom{n}{\frac{n+1}{2}}}$ be the list of $W^{\frac{n+1}{2}}$, define $g \in B_n$ as

$$g(x) = \begin{cases} 0, & x \in W^{\leq \frac{n+1}{2}} \setminus T, \\ 1, & x \in W^{\geq \frac{n+3}{2}} \cup T \end{cases} \tag{51}$$

where $T = \{b_1, b_2, \cdots, b_{\binom{n}{\frac{n+1}{2}}}\}$ is a subset of $W^{\leq \frac{n+1}{2}}$ such that

$$\forall\ 1 \leq j \leq \binom{n}{\frac{n+1}{2}},\ \mathrm{supp}(b_j) \subseteq \mathrm{supp}(a_j);\ \text{ and } \forall\ 1 \leq l < j \leq \binom{n}{\frac{n+1}{2}},\ \mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l). \tag{52}$$

Since the function g in Equality (51) is balanced, it has optimal algebraic immunity $(n+1)/2$ if and only if $AN(f)$ does not contain any nonzero function of degree strictly less than $(n+1)/2$ [3]. Note that g can be regarded as a Boolean function provided by the algorithm after Corollary 1 in [4], thus, g has algebraic immunity $(n+1)/2$. By choosing suitable set T, the nonlinearity of g can be measured.

Let g_0 be the majority function with support $W^{\geq \frac{n+1}{2}}$. Denote $U_3 = W^{\frac{n+1}{2}} \setminus T$ and $T_3 = T \setminus W^{\frac{n+1}{2}}$, then g can be rewritten as

$$g(x) = \begin{cases} g_0 + 1, & x \in U_3 \cup T_3, \\ g_0, & \text{otherwise.} \end{cases}$$

Thus, the Walsh spectrum of g can be calculated as follows.

$$\begin{aligned} W_g(\lambda) &= \sum_{x \notin U_3 \cup T_3} (-1)^{g_0(x) + \lambda \cdot x} + \sum_{x \in U_3 \cup T_3} (-1)^{g_0(x) + 1 + \lambda \cdot x} \\ &= \sum_{x \in \mathbb{F}_2^n} (-1)^{g_0(x) + \lambda \cdot x} - 2 \sum_{x \in U_3 \cup T_3} (-1)^{g_0(x) + \lambda \cdot x} \\ &= W_{g_0}(\lambda) - 2[\sum_{x \in T_3} (-1)^{\lambda \cdot x} - \sum_{x \in U_3} (-1)^{\lambda \cdot x}]. \end{aligned}$$

By Lemma 2.6 (1), (2) in [13] and Lemma 2.3, the Walsh transform of g_0 can be characterized as

$$W_{g_0}(\lambda) = \begin{cases} 2K_{\frac{n-1}{2}}(\mathrm{wt}(\lambda) - 1, n - 1), & \text{for odd } \mathrm{wt}(\lambda), \\ 0, & \text{otherwise.} \end{cases}$$

Therefore, for $\mathrm{wt}(\lambda) = t$, one has

$$W_g(\lambda) = \begin{cases} 2K_{\frac{n-1}{2}}(t-1, n-1) - 2[\sum_{x \in T_3} (-1)^{\lambda \cdot x} - \sum_{x \in U_3} (-1)^{\lambda \cdot x}], & \text{for odd } t, \\ -2[\sum_{x \in T_3} (-1)^{\lambda \cdot x} - \sum_{x \in U_3} (-1)^{\lambda \cdot x}], & \text{for even } t. \end{cases} \tag{53}$$

Equality (53) shows that the nonlinearity of g is determined by the sets T_3 and U_3, which can be defined based on a series of vectors provided by the following algorithm.

Algorithm 1:

```
Input: three positive integers $r$, $u$ and $N$ with $r+u-1 \le N$.
Output: $m = \sum_{s=0}^{r-1}\binom{N}{u+s}$ vectors $x_1, x_2, \cdots, x_m$ in $\mathbb{F}_2^r$ such that
    $$\min_{1\le j\le r} |\{x_i = (x_{i1}, \cdots, x_{ir}) \,|\, x_{ij} = 1,\ i = 1, 2, \cdots, m\}| = \lfloor \sum_{s=0}^{r-1}\binom{N}{u+s}\frac{r-s}{r} \rfloor.$$
1. Denote $M = \sum_{s=0}^{r-1}\binom{N}{u+s}(r-s)$ and take a sequence $l = (l_1, l_2, \cdots, l_M)$ where
    $$l_i = \begin{cases} r & \text{if } r \,|\, i \\ i \pmod{r} & \text{otherwise} \end{cases} \quad \text{for } i = 1, 2, \cdots, M.$$
2. Initialization: $s \leftarrow 0$, $k \leftarrow 0$, $t \leftarrow 1$.
3. While $s \le r-1$ do the following:
    3.1 for $j$ from 1 to $\binom{N}{u+s}$ do:
        3.1.1 take $x_t$ with $\mathrm{supp}(x_t) = \{l_{k+1}, l_{k+2}, \cdots, l_{k+r-s}\}$.
        3.1.2 $t \leftarrow t+1$, $k = k+r-s$.
    3.2 $s \leftarrow s+1$.
4. Return the vectors $x_1, x_2, \cdots, x_m$.
```

The validity of Algorithm 1 is explained as follows.

From the algorithm, on one hand, for any $1 \le j \le r$, the number of j's in the sequence $(l_1, l_2, \cdots, l_M)$ is no less than $\lfloor \frac{M}{r} \rfloor$; on the other hand, according to $\mathrm{supp}(x_t)$ $(t = 1, 2, \cdots, m)$ described in step 3.1.1, it can be concluded that the value of $|\{x_i \,|\, x_{ij} = 1,\ i = 1, 2, \cdots, m\}|$ is exactly the number of j's in the sequence $(l_1, l_2, \cdots, l_M)$ for $1 \le j \le r$. Thus,

$$\min_{1\le j\le r} |\{x_i \,|\, x_{ij} = 1,\ i = 1, 2, \cdots, m\}| = \lfloor \tfrac{M}{r} \rfloor = \lfloor \sum_{s=0}^{r-1}\binom{N}{u+s}\frac{r-s}{r} \rfloor.$$

Define a multiset Q (in the sense that the vector x_i can be the same as x_j for $1 \le i \ne j \le m$ in Q) as

$$Q = \{x_1, x_2, \cdots, x_m\} \tag{54}$$

where the vectors $x_1, x_2, \cdots, x_m$ are obtained from Algorithm 1. According to Algorithm above, the number of vectors in Q with weight s is $\binom{N}{u+r-s}$ for $1 \le s \le r$.

Running Algorithm 1, some examples can be given as follows.

Example 1: (1) For $r = 4$, $u = 1$ and $N = 4$, the vectors $x_1, \cdots, x_{15}$ are listed as follows.

$$\begin{array}{rrrrr} x_1 = (1,1,1,1), & x_2 = (1,1,1,1), & x_3 = (1,1,1,1), & x_4 = (1,1,1,1), & x_5 = (1,1,1,0), \\ x_6 = (1,1,0,1), & x_7 = (1,0,1,1), & x_8 = (0,1,1,1), & x_9 = (1,1,1,0), & x_{10} = (1,1,0,1), \\ x_{11} = (0,0,1,1), & x_{12} = (1,1,0,0), & x_{13} = (0,0,1,1), & x_{14} = (1,1,0,0), & x_{15} = (0,0,1,0). \end{array}$$

The value $\min_{1\le j\le 4} |\{x_i \,|\, x_{ij} = 1,\ 1 \le i \le 15\}| = |\{x_i \,|\, x_{i4} = 1,\ 1 \le i \le 15\}| = 10$.

(2) For $r = 3$, $u = 3$ and $N = 5$, the vectors $x_1, \cdots, x_{16}$ are listed as follows.

$$\begin{array}{rrrr} x_1 = (1,1,1), & x_2 = (1,1,1), & x_3 = (1,1,1), & x_4 = (1,1,1), \\ x_5 = (1,1,1), & x_6 = (1,1,1), & x_7 = (1,1,1), & x_8 = (1,1,1), \\ x_9 = (1,1,1), & x_{10} = (1,1,1), & x_{11} = (1,1,0), & x_{12} = (1,0,1), \\ x_{13} = (0,1,1), & x_{14} = (1,1,0), & x_{15} = (1,0,1), & x_{16} = (0,1,0). \end{array}$$

The value $\min_{1\le j\le 3} |\{x_i \,|\, x_{ij} = 1,\ 1 \le i \le 16\}| = |\{x_i \,|\, x_{i3} = 1,\ 1 \le i \le 16\}| = 13$.

An integer n larger than 4 can be written as a sum of four positive integers r_i $(1 \le i \le 4)$, i.e., $n = r_1 + r_2 + r_3 + r_4$. For convenience, denote

$$\begin{array}{l} m_1 = \sum\limits_{i=0}^{r_1-1} \binom{n-r_1-2}{\frac{n+1}{2}-(r_1-i)} \frac{r_1-i}{r_1},\ m_2 = \sum\limits_{i=0}^{r_2-1} \binom{n-r_2-2}{\frac{n-1}{2}-(r_2-i)} \frac{r_2-i}{r_2}, \\ m_3 = \sum\limits_{i=0}^{r_3-1} \binom{n-r_3-3}{\frac{n-3}{2}-(r_3-i)} \frac{r_3-i}{r_3},\ m_4 = \sum\limits_{i=0}^{r_4-1} \binom{n-r_4-3}{\frac{n-5}{2}-(r_4-i)} \frac{r_4-i}{r_4}. \end{array} \tag{55}$$

and divide the set $\{1, 2, \cdots, n\}$ into four subsets as follows:

$$\begin{array}{ll} \Lambda_1 = \{1, 2, \cdots, r_1\}, & \Lambda_2 = \{r_1+1, r_1+2, \cdots, r_1+r_2\}, \\ \Lambda_3 = \{r_1+r_2+1, \cdots, r_1+r_2+r_3\}, & \Lambda_4 = \{r_1+r_2+r_3+1, \cdots, n\}. \end{array} \tag{56}$$

In the following, a method of choosing the sets T_3 and U_3 is presented. This method will generate an infinite class of Boolean functions with optimal algebraic immunity and high nonlinearity.

For $1 \le i \le 4$, denote $\varepsilon_i = \begin{cases} 2 \text{ for } i = 1, 2 \\ 3 \text{ for } i = 3, 4 \end{cases}$ and take

$$P_i = \{y \in F_2^{n-r_i-\varepsilon_i} \mid (n+3)/2 - i - r_i \le \mathrm{wt}(y) \le (n+1)/2 - i\}.$$

Let Q_i be the multiset defined by Equality (54) where $r = r_i$, $u = (n+3)/2 - i - r_i$ and $N = n - r_i - \varepsilon_i$. Since the number of vectors y in P_i with weight $(n+3)/2 - i - s$ and that of vectors in Q_i with weight s are both equal to $\binom{n-r_i-\varepsilon_i}{\frac{n+3}{2}-i-s}$ for $1 \le s \le r_i$, an one-to-one correspondence φ_i from P_i to Q_i can be induced such that $\mathrm{wt}(y) + \mathrm{wt}(\varphi_i(y)) = (n+3)/2 - i$ holds for any $y \in P_i$.

With the sets P_i and the correspondence φ_i $(i = 1, 2, 3, 4)$, eight sets T_3^i and U_3^i can be defined as Table 2.

Table 2 The definition of T_3^i and U_3^i for $i = 1, 2, 3, 4$

$T_3^1 = \{(0,\ 0,\ y_1, 0) \in \mathbb{F}_2^{r_1} \times \mathbb{F}_2 \times \mathbb{F}_2^{n-r_1-2} \times \mathbb{F}_2 \mid y_1 \in P_1\}$ $U_3^1 = \{(\varphi_1(y_1),\ 0,\ y_1, 0) \in \mathbb{F}_2^{r_1} \times \mathbb{F}_2 \times \mathbb{F}_2^{n-r_1-2} \times \mathbb{F}_2 \mid y_1 \in P_1\}$
$T_3^2 = \{(0, y_1,\ 0,\ y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2^{r_1-1} \times \mathbb{F}_2^{r_2} \times \mathbb{F}_2^{n-r_1-r_2-1} \times \mathbb{F}_2 \mid (y_1, y_2) \in P_2\}$ $U_3^2 = \{(0, y_1,\ \varphi_2(y),\ y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2^{r_1-1} \times \mathbb{F}_2^{r_2} \times \mathbb{F}_2^{n-r_1-r_2-1} \times \mathbb{F}_2 \mid y = (y_1, y_2) \in P_2\}$
$T_3^3 = \{(1, 0, y_1, 0, y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{r_1+r_2-2} \times \mathbb{F}_2^{r_3} \times \mathbb{F}_2^{r_4-1} \times \mathbb{F}_2 \mid (y_1, y_2) \in P_3\}$ $U_3^3 = \{(1, 0, y_1, \varphi_3(y), y_2, 1) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{r_1+r_2-2} \times \mathbb{F}_2^{r_3} \times \mathbb{F}_2^{r_4-1} \times \mathbb{F}_2 \mid y = (y_1, y_2) \in P_3\}$
$T_3^4 = \{(1, 1, y_1, 1, y_2, 0) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{r_1-2} \times \mathbb{F}_2 \times \mathbb{F}_2^{r_2+r_3-1} \times \mathbb{F}_2^{r_4} \mid (y_1, y_2) \in P_4\}$ $U_3^4 = \{(1, 1, y_1, 1, y_2, \varphi_4(y)) \in \mathbb{F}_2 \times \mathbb{F}_2 \times \mathbb{F}_2^{r_1-2} \times \mathbb{F}_2 \times \mathbb{F}_2^{r_2+r_3-1} \times \mathbb{F}_2^{r_4} \mid y = (y_1, y_2) \in P_4\}$

Then, by Algorithm 1, one has

$$\min_{j \in \Lambda_i} |\{x \in U_3^i \mid x_j = 1\}| = \lfloor m_i \rfloor.$$

for $i = 1, 2, 3, 4$.

Define two sets

$$T_3 = \bigcup_{i=1}^{4} T_3^i, \quad U_3 = \bigcup_{i=1}^{4} U_3^i. \tag{57}$$

Then,

$$|U_3| = |T_3| = \sum_{i=0}^{r_1-1} \binom{n-r_1-2}{\frac{n+1}{2}-(r_1-i)} + \sum_{i=0}^{r_2-1} \binom{n-r_2-2}{\frac{n-1}{2}-(r_2-i)} + \sum_{i=0}^{r_3-1} \binom{n-r_3-3}{\frac{n-3}{2}-(r_3-i)} + \sum_{i=0}^{r_4-1} \binom{n-r_4-3}{\frac{n-5}{2}-(r_4-i)}.$$

Let T_3 and U_3 be defined in Equality (57), define

$$g_1(x) = \begin{cases} g_0 + 1, & x \in U_3 \cup T_3, \\ g_0, & \text{otherwise}, \end{cases} \tag{58}$$

where g_0 is the majority function, whose support is $W^{\geq \frac{n+1}{2}}$.

In what follows, the algebraic immunity and nonlinearity of g_1 is considered.

Proposition 4.1. *The Boolean function g_1 defined in Equality (58) has algebraic immunity $(n+1)/2$.*

Proof: Take $U' = W^{\frac{n+1}{2}} \backslash U_3$ and $T = T_3 \cup U'$, then g_1 is exactly the function g defined in Equality (51). Thus, it is sufficient to prove the set T satisfies the condition in (52).

List the elements of $W^{\frac{n+1}{2}}$ and T as

$$W^{\frac{n+1}{2}}:\ a_1, \cdots, a_{|U_3|}, c_1, \cdots, c_{|U'|},\ T:\ b_1, \cdots, b_{|T_3|}, c_1, \cdots, c_{|U'|},$$

where $a_j \in U_3$, $b_j \in T_3$ $(1 \leq j \leq |T_3|)$ and $c_k \in U'$ $(1 \leq k \leq |U'|)$, then the sets $W^{\frac{n+1}{2}}$ and T satisfy the condition in (52) if and only if U_3 and T_3 satisfy it.

The elements $b_1, b_2, \cdots, b_{|T_3|}$ listed from left to right above obey the following rules:

1. For any $b_{j_1} \in T_3^{i_1}$, $b_{j_2} \in T_3^{i_2}$, if $i_1 < i_2$, then $j_1 < j_2$;

2. For any $b_{j_1}, b_{j_2} \in T_3^i$, $j_1 \leq j_2$ if and only if $\mathrm{wt}(b_{j_1}) \leq \mathrm{wt}(b_{j_2})$.

From Table 2, every element in U_3^i is uniquely determined by an element b_j in T_3^i and some correspondence φ_i. Thus, we denote this element by a_j.

According to the order of elements above, $b_1, b_2, \cdots, b_{|T_3|}$ and $a_1, a_2, \cdots, a_{|U_3|}$ will be proven to satisfy the condition

$$\forall\ 1 \leq j \leq |T_3|,\ \mathrm{supp}(b_j) \subseteq \mathrm{supp}(a_j);\ \text{and}\ \forall\ 1 \leq l < j \leq |T_3|,\ \mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l).$$

By Table 2 and the choice of a_j, one has $\mathrm{supp}(b_j) \subseteq \mathrm{supp}(a_j)$ for every $1 \leq j \leq |T_3|$.

For any $1 \leq l < j \leq |T_3|$, suppose that b_j belongs to some T_3^i. When $a_l \in U_3^i$, respectively, $b_l \in T_3^i$, since the elements of T_3^i are sorted by increasing weight, one has $\mathrm{wt}(b_j) \geq \mathrm{wt}(b_l)$, then $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(b_l)$. According to Table 2, one has $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$.

When $a_l \notin U_3^i$, one has $a_l \in U_3^{i_1}$ where $i_1 < i$. By Table 2, when $b_j \in T_3^4$, one has $1, 2, r_1 + 1 \in \mathrm{supp}(b_j)$; in addition, if $a_l \in U_3^3$, $2 \notin \mathrm{supp}(a_l)$, if $a_l \in U_3^2$, $1 \notin \mathrm{supp}(a_l)$ and if $a_l \in U_3^1$, $r_1 + 1 \notin \mathrm{supp}(a_l)$, then $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$; when $b_j \in T_3^3$, one has $1, n \in \mathrm{supp}(b_j)$, moreover, if $a_l \in U_3^2$, $1 \notin \mathrm{supp}(a_l)$ and if $a_l \in U_3^1$, $n \notin \mathrm{supp}(a_l)$, then $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$; when $b_j \in T_3^2$, $n \in \mathrm{supp}(b_j)$, since $n \notin \mathrm{supp}(a_l)$ for $a_l \in U_3^1$, one has $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$. Therefore, $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$ holds for $a_l \notin U_3^i$.

The above analysis implies that $\mathrm{supp}(b_j) \not\subseteq \mathrm{supp}(a_l)$ for any $l < j$, which finishes the proof. □

The following lemmas can be used to analyze the nonlinearity of g_1.

Lemma 4.2. *(1) For $n = 4k+1$, let $r_1 = r_2 = k+1$, $r_3 = k$ and $r_4 = k-1$, then m_i's $(i = 1, 2, 3, 4)$ given in (55) satisfy*

$$\min_{1 \leq i \leq 4} \{m_i\} = m_3 \text{ for } k \geq 3.$$

(2) For $n = 4k+3$, let $r_1 = k+2$, $r_2 = k+1$ and $r_3 = r_4 = k$, then m_i's $(i = 1, 2, 3, 4)$ given in (55) satisfy

$$\min_{1 \leq i \leq 4} \{m_i\} = \begin{cases} m_4 \text{ for } k = 3, 4 \\ m_1 \text{ for } k \geq 5. \end{cases}$$

Proof: We only give the proof for the result in (1), and the result in (2) can be similarly proven.

(1) It can be verified that $m_4 - m_3 = \left\{ \begin{array}{c} 0 \text{ for } k = 3 \\ 83 \text{ for } k = 4 \end{array} \right.$ and for $k \geq 5$,

$$\begin{aligned}
m_4 - m_3 &= \sum_{i=0}^{k-2} \binom{3k-1}{k+i-1} \frac{k-1-i}{k-1} - \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k} \\
&= \sum_{i=0}^{k-2} [\binom{3k-2}{k+i-1} + \binom{3k-2}{k+i-2}] \frac{k-1-i}{k-1} - \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k} \\
&= \sum_{i=0}^{k-2} \binom{3k-2}{k+i-1} (\frac{k-1-i}{k-1} - \frac{k-i}{k}) - \binom{3k-2}{2k-2} \frac{1}{k} + \sum_{i=0}^{k-2} \binom{3k-2}{k+i-2} \frac{k-1-i}{k-1} \\
&= \sum_{i=0}^{k-2} \binom{3k-2}{k+i-1} \frac{-i}{k(k-1)} - \binom{3k-2}{2k-2} \frac{1}{k} + \sum_{i=0}^{k-2} \binom{3k-2}{k+i-2} \frac{k-1-i}{k-1} \\
&= \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{-i}{k(k-1)} + \sum_{i=0}^{k-2} \binom{3k-2}{k+i-2} \frac{k-1-i}{k-1} \\
&= \sum_{i=1}^{k} \binom{3k-2}{k+i-2} \frac{-(i-1)}{k(k-1)} + \sum_{i=0}^{k-2} \binom{3k-2}{k+i-2} \frac{k-1-i}{k-1} \\
&= \sum_{i=1}^{k-2} \binom{3k-2}{k+i-2} \frac{k^2-k+1-(k+1)i}{k(k-1)} - \binom{3k-2}{2k-3} \frac{k-2}{k(k-1)} - \binom{3k-2}{2k-2} \frac{1}{k} + \binom{3k-2}{k-2} \\
&= \sum_{i=1}^{k-2} \binom{3k-2}{k+i-2} \frac{k^2-k+1-(k+1)i}{k(k-1)} - \binom{3k-2}{k} \frac{3(k-1)}{k(k+1)} + \binom{3k-2}{k-2} \\
&> \binom{3k-2}{k+2-2} \frac{k(k-1)+1-2(k+1)}{k(k-1)} - \binom{3k-2}{k} \frac{3(k-1)}{k(k+1)} \\
&= \binom{3k-2}{k} [\frac{k^2-3k-1}{k(k-1)} - \frac{3(k-1)}{k(k+1)}] \\
&> \binom{3k-2}{k} [\frac{k^2-4k+3}{k(k-1)} - \frac{3(k-1)}{k(k+1)}] \\
&= \binom{3k-2}{k} \frac{k-5}{k+1} \geq 0.
\end{aligned}$$

By (55), one has

$$\begin{aligned}
m_2 - m_3 &= \sum_{i=0}^{k} \binom{3k-2}{k+i-1} \frac{k+1-i}{k+1} - \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k} \\
&> \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} (\frac{k+1-i}{k+1} - \frac{k-i}{k}) \\
&= \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{i}{k(k+1)} > 0.
\end{aligned}$$

and

$$\begin{aligned}
m_1 - m_3 &= \sum_{i=0}^{k} \binom{3k-2}{k+i} \frac{k+1-i}{k+1} - \sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k} \\
&= \sum_{i=0}^{k} \binom{3k-2}{k+i} \frac{k+1-i}{k+1} - \sum_{i=0}^{k-2} \binom{3k-2}{k+i} \frac{k-i-1}{k} - \binom{3k-2}{k-1} \\
&= \sum_{i=0}^{k-2} \binom{3k-2}{k+i} (\frac{k+1-i}{k+1} - \frac{k-i-1}{k}) + \binom{3k-2}{2k-1} \frac{2}{k+1} + \binom{3k-2}{2k} \frac{1}{k+1} - \binom{3k-2}{k-1} \\
&= \sum_{i=0}^{k-2} \binom{3k-2}{k+i} \frac{k+i+1}{k(k+1)} + \binom{3k-2}{k-2} \frac{1}{k+1} - \binom{3k-2}{k-1} \frac{k-1}{k+1} \\
&> \sum_{i=0}^{k-2} \binom{3k-2}{k+i} \frac{1}{k+1} + \binom{3k-2}{k-2} \frac{1}{k+1} - \binom{3k-2}{k-1} \frac{k-1}{k+1} \\
&> \binom{3k-2}{k-1} \frac{k-1}{k+1} + \binom{3k-2}{k-2} \frac{1}{k+1} - \binom{3k-2}{k-1} \frac{k-1}{k+1} > 0.
\end{aligned}$$

Thus, $\min\limits_{1\leq i\leq 4}\{m_i\} = m_3$ for $k \geq 3$. This completes the proof. □

Lemma 4.3. *(1) Let* $|U_3| = \sum\limits_{i=0}^{k}\binom{3k-2}{k+i} + \sum\limits_{i=0}^{k}\binom{3k-2}{k+i-1} + \sum\limits_{i=0}^{k-1}\binom{3k-2}{k+i-1} + \sum\limits_{i=0}^{k-2}\binom{3k-1}{k+i-1}$ *and* $m_3 = \sum\limits_{i=0}^{k-1}\binom{3k-2}{k+i-1}\frac{k-i}{k}$*, then*

$$(4k-2)\tbinom{4k}{2k}/(4k-1) - 2|U_3| - 2m_3 > 0$$

for $k \geq 4$*.*

(2) Let $|U_3| = \sum\limits_{i=0}^{k+1}\binom{3k-1}{k+i} + \sum\limits_{i=0}^{k}\binom{3k}{k+i} + \sum\limits_{i=0}^{k-1}\binom{3k}{k+i} + \sum\limits_{i=0}^{k-1}\binom{3k}{k+i-1}$ *and* $m_1 = \sum\limits_{i=0}^{k+1}\binom{3k-1}{k+i}\frac{k+2-i}{k+2}$*, then*

$$4k\tbinom{4k+2}{2k+1}/(4k+1) - 2|U_3| - 2m_1 > 0$$

for $k \geq 3$*.*

Proof: The proofs of Lemma 4.3 (1) and (2) are similar, and we give only the proof of Lemma 4.3 (1).

(1) For $k \geq 4$, one has

$$\begin{aligned}
& |U_3| + m_3 \\
< \ & [\sum_{i=0}^{k}\tbinom{3k-2}{k+i} + \sum_{i=0}^{k}\tbinom{3k-2}{k+i-1} + \sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1} + \sum_{i=0}^{k-2}\tbinom{3k-1}{k+i-1}] + \sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1} \\
= \ & \sum_{i=0}^{k}\tbinom{3k-2}{k+i} + \sum_{i=0}^{k}\tbinom{3k-2}{k+i-1} + 2\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1} + (\sum_{i=0}^{k-2}\tbinom{3k-2}{k+i-1} + \sum_{i=0}^{k-2}\tbinom{3k-2}{k+i-2})) \\
= \ & \sum_{i=2}^{k+2}\tbinom{3k-2}{k+i-2} + \sum_{i=1}^{k+1}\tbinom{3k-2}{k+i-2} + 2\sum_{i=1}^{k}\tbinom{3k-2}{k+i-2} + \sum_{i=1}^{k-1}\tbinom{3k-2}{k+i-2} + \sum_{i=0}^{k-2}\tbinom{3k-2}{k+i-2} \\
= \ & \tbinom{3k-2}{k-2} + 5\tbinom{3k-2}{k-1} + 6\sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2} + 5\tbinom{3k-2}{2k-3} + 4\tbinom{3k-2}{2k-2} + 2\tbinom{3k-2}{2k-1} + \tbinom{3k-2}{2k} \\
= \ & 2\tbinom{3k-2}{k-2} + 7\tbinom{3k-2}{k-1} + 6\sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2} + 5\tbinom{3k-2}{2k-3} + 4\tbinom{3k-2}{2k-2}
\end{aligned}$$

and

$$\begin{aligned}
\tbinom{4k}{2k} \ = \ & 2\tbinom{4k-1}{2k-1} = 2\sum_{i=0}^{k+1}\tbinom{3k-2}{k+i-2}\tbinom{k+1}{k+1-i} \\
= \ & 2[\tbinom{3k-2}{k-2} + (k+1)\tbinom{3k-2}{k-1} + \sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2}\tbinom{k+1}{k+1-i} + \tbinom{k+1}{2}\tbinom{3k-2}{2k-3} + (k+1)\tbinom{3k-2}{2k-2} + \tbinom{3k-2}{2k-1}] \\
= \ & 2[\tbinom{3k-2}{k-2} + (k+2)\tbinom{3k-2}{k-1} + \sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2}\tbinom{k+1}{k+1-i} + \tbinom{k+1}{2}\tbinom{3k-2}{2k-3} + (k+1)\tbinom{3k-2}{2k-2}] \\
\geq \ & 2[\tbinom{3k-2}{k-2} + (k+2)\tbinom{3k-2}{k-1} + \tbinom{k+1}{2}\sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2} + \tbinom{k+1}{2}\tbinom{3k-2}{2k-3} + (k+1)\tbinom{3k-2}{2k-2}] \\
\geq \ & 2[\tbinom{3k-2}{k-2} + 6\tbinom{3k-2}{k-1} + 10\sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2} + 10\tbinom{3k-2}{2k-3} + 5\tbinom{3k-2}{2k-2}] \\
\geq \ & 2[3\tbinom{3k-2}{k-2} + 8\tbinom{3k-2}{k-1} + 8\sum_{i=2}^{k-2}\tbinom{3k-2}{k+i-2} + 8\tbinom{3k-2}{2k-3} + 5\tbinom{3k-2}{2k-2}],
\end{aligned}$$

thus,

$$\begin{array}{rl} & (4k-2)\binom{4k}{2k}/(4k-1)-2|U_3|-2m_3 \\ > & \frac{2(4k-2)}{4k-1}[3\binom{3k-2}{k-2}+8\binom{3k-2}{k-1}+8\sum\limits_{i=2}^{k-2}\binom{3k-2}{k+i-2}+8\binom{3k-2}{2k-3}+5\binom{3k-2}{2k-2}] \\ & -2[2\binom{3k-2}{k-2}+7\binom{3k-2}{k-1}+6\sum\limits_{i=2}^{k-2}\binom{3k-2}{k+i-2}+5\binom{3k-2}{2k-3}+4\binom{3k-2}{2k-2}] \\ > & 0 \end{array}$$

since $(4k-2)/(4k-1) \geq 14/15 > 7/8 > 4/5 > 6/8 > 2/3 > 5/8$ for $k \geq 4$. □

With the above preparation, the nonlinearity of g_1 can be determined.

Theorem 4.4. *Let $g_1 \in B_n$ be defined in Equality (58). Then, for $n \geq 15$, its nonlinearity can achieve $2^{n-1}-\binom{n-1}{\frac{n-1}{2}}+\Delta(n)$, where the function $\Delta(n)$ satisfies*

$$\Delta(n)=\begin{cases} 2\lfloor\sum\limits_{i=0}^{k-1}\binom{3k-2}{k+i-1}\frac{k-i}{k}\rfloor & n=4k+1,\ k\geq 4 \\ 2\lfloor\sum\limits_{i=0}^{k+1}\binom{3k-1}{k+i}\frac{k+2-i}{k+2}\rfloor & n=4k+3,\ k\geq 5 \end{cases}$$

and $\Delta(15)=268$, $\Delta(19)=2436$.

Proof: By Equality (53), the Walsh transform of $W_{g_1}(\lambda)$ is determined by the value

$$\Gamma_\lambda=\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x} \text{ for } \lambda\in\mathbb{F}_2^n.$$

When $\mathrm{wt}(\lambda)=1$, let $\lambda_1,\lambda_2,\cdots,\lambda_n$ be n vectors with $\mathrm{supp}(\lambda_j)=\{j\}$ $(j=1,2,\cdots,n)$. According to the definition of sets T_3^i and U_3^i $(1\leq i\leq 4)$, when $j\notin\Lambda_i$,

$$\sum_{x\in T_3^i}(-1)^{\lambda_j\cdot x}-\sum_{x\in U_3^i}(-1)^{\lambda_j\cdot x}=0.$$

Thus, when $j\in\Lambda_1$, $x_j=0$ for all $x\in T_3^1$, it can be concluded that

$$\begin{array}{rcl}\Gamma_{\lambda_j} & = & \sum\limits_{x\in T_3}(-1)^{\lambda_j\cdot x}-\sum\limits_{x\in U_3}(-1)^{\lambda_j\cdot x} \\ & = & \sum\limits_{i=1}^{4}[\sum\limits_{x\in T_3^i}(-1)^{x_j}-\sum\limits_{x\in U_3^i}(-1)^{x_j}] \\ & = & \sum\limits_{x\in T_3^1}(-1)^{x_j}-\sum\limits_{x\in U_3^1}(-1)^{x_j} \\ & = & |T_3^1|-(|U_3^1|-2|\{x\in U_3^1\,|\,x_j=1\}|) \\ & = & 2|\{x\in U_3^1\,|\,x_j=1\}|,\end{array}$$

and

$$\min\{\Gamma_{\lambda_j}\,|\,j\in\Lambda_1\}=2\lfloor m_1\rfloor.$$

Applying the same method, one has $\min\{\Gamma_{\lambda_j}\,|\,j\in\Lambda_i\}=2\lfloor m_i\rfloor$ for $i=2,3,4$. Thus,

$$\min_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda=\min\{\Gamma_{\lambda_j}\,|\,j=1,2,\cdots,n\}=\min_{1\leq i\leq 4}\{2\lfloor m_i\rfloor\}.$$

In the following, the results will be proved for two cases: $n=4k+1$ and $n=4k+3$.

(1) When $n=4k+1$, we can take $r_1=r_2=k+1$, $r_3=k$ and $r_4=k-1$, then the value of Γ_λ for $\lambda\in\mathbb{F}_2^n$ is studied as follows. By substituting r_i into (55), one has

$$m_1=\sum_{i=0}^{k}\tbinom{3k-2}{k+i}\tfrac{k+1-i}{k+1},\, m_2=\sum_{i=0}^{k}\tbinom{3k-2}{k+i-1}\tfrac{k+1-i}{k+1},$$
$$m_3=\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}\tfrac{k-i}{k},\ m_4=\sum_{i=0}^{k-2}\tbinom{3k-1}{k+i-1}\tfrac{k-1-i}{k-1}.$$

By Lemma 4.2 (1), for $k\geq 4$, $\min\limits_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda=2\lfloor m_3\rfloor$. Thus, by Equality (53), one has

$$\begin{aligned}\max_{\mathrm{wt}(\lambda)=1}|W_{g_1}(\lambda)| &= \max_{\mathrm{wt}(\lambda)=1}|W_{g_0}(\lambda)-2[\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}]|\\ &= 2K_{\frac{n-1}{2}}(0,n-1)-2\min_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda \\ &= 2\tbinom{4k}{2k}-4\lfloor m_3\rfloor\end{aligned}\tag{59}$$

for $k\geq 4$.

For $\mathrm{wt}(\lambda)=n$,

$$\begin{aligned}W_{g_1}(\lambda) &= 2K_{\frac{n-1}{2}}(n-1,n-1)-2[\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}]\\ &= (-1)^{\frac{n-1}{2}}2\tbinom{n-1}{\frac{n-1}{2}}-2\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)}+(-1)^{\frac{n+1}{2}}2|U_3|\\ &= 2[\tbinom{4k}{2k}-\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)}-|U_3|\,].\end{aligned}$$

Since

$$\begin{aligned}&\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)}+|U_3|\\ =\ &\sum_{i=1}^{4}\sum_{x\in T_3^i}(-1)^{\mathrm{wt}(x)}+|T_3^1|+|T_3^2|+|T_3^3|+|T_3^4|\\ \geq\ &\sum_{x\in T_3^2}(-1)^{\mathrm{wt}(x)}+\sum_{x\in T_3^3}(-1)^{\mathrm{wt}(x)}+|T_3^2|+|T_3^3|\\ =\ &\sum_{i=0}^{k}(-1)^{k+i}\tbinom{3k-2}{k+i-1}+\sum_{i=0}^{k-1}(-1)^{k+i+1}\tbinom{3k-2}{k+i-1}+\sum_{i=0}^{k}\tbinom{3k-2}{k+i-1}+\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}\\ =\ &2\tbinom{3k-2}{2k-1}+2\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}\\ >\ &2\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1},\end{aligned}$$

one has

$$|W_{g_1}(\lambda)|<2[\tbinom{4k}{2k}-2\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}]<2\tbinom{4k}{2k}-4m_3\leq 2\tbinom{4k}{2k}-4\lfloor m_3\rfloor\tag{60}$$

for $\mathrm{wt}(\lambda)=n$.

By Equality (53) and Lemma 2.6, for odd $3\leq\mathrm{wt}(\lambda)=t\leq n-2$,

$$\begin{aligned}|W_{g_1}(\lambda)| &= |2K_{\frac{n-1}{2}}(t-1,n-1)-2[\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}]|\\ &\leq 2\tbinom{n-1}{\frac{n-1}{2}}/(n-2)+4|U_3|\\ &= 2\tbinom{4k}{2k}/(4k-1)+4|U_3|,\end{aligned}$$

and for even $\mathrm{wt}(\lambda)$,

$$|W_{g_1}(\lambda)|=2|\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}|\leq 4|U_3|.$$

Thus, for $2 \leq \mathrm{wt}(\lambda) \leq n-1$,

$$|W_{g_1}(\lambda)| \quad \leq \quad 2\binom{4k}{2k}/(4k-1)+4|U_3|. \tag{61}$$

By Lemma 4.3 (1), for $k \geq 4$,

$$\begin{aligned} & [2\tbinom{4k}{2k}-4\lfloor m_3\rfloor]-[2\tbinom{4k}{2k}/(4k-1)+4|U_3|] \\ = \;& 2[(4k-2)\tbinom{4k}{2k}/(4k-1)-2|U_3|-2\lfloor m_3\rfloor] \\ = \;& 2[(4k-2)\tbinom{4k}{2k}/(4k-1)-2|U_3|-2m_3] \\ > \;& 0. \end{aligned}$$

Thus, by Equality (59), by (60) and (61), one has

$$\max_{\lambda\in\mathbb{F}_2^n}|W_{g_1}(\lambda)| = 2\tbinom{4k}{2k}-4\lfloor m_3\rfloor = 2\tbinom{4k}{2k}-4\lfloor\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}\tfrac{k-i}{k}\rfloor$$

for $k \geq 4$. This implies

$$nl(g_1) = 2^{4k}-\tbinom{4k}{2k}+2\lfloor\sum_{i=0}^{k-1}\tbinom{3k-2}{k+i-1}\tfrac{k-i}{k}\rfloor.$$

(2) When $n=4k+3$, take $r_1=k+2$, $r_2=k+1$ and $r_3=r_4=k$. The value of Γ_λ for $\lambda\in\mathbb{F}_2^n$ is studied as follows. In this case, substitute r_i into (55), then

$$\begin{aligned} m_1 &= \sum_{i=0}^{k+1}\tbinom{3k-1}{k+i}\tfrac{k+2-i}{k+2}, & m_2 &= \sum_{i=0}^{k}\tbinom{3k}{k+i}\tfrac{k+1-i}{k+1}, \\ m_3 &= \sum_{i=0}^{k-1}\tbinom{3k}{k+i}\tfrac{k-i}{k}, & m_4 &= \sum_{i=0}^{k-1}\tbinom{3k}{k+i-1}\tfrac{k-i}{k}. \end{aligned}$$

By Lemma 4.2 (2), one has

$$\min_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda = \min_{1\leq i\leq 4}\{2\lfloor m_i\rfloor\} = \begin{cases} 2\lfloor m_4\rfloor & \text{for } k=3,4 \\ 2\lfloor m_1\rfloor & \text{for } k\geq 5. \end{cases}$$

Thus,

$$\begin{aligned} \max_{\mathrm{wt}(\lambda)=1}|W_{g_1}(\lambda)| &= \max_{\mathrm{wt}(\lambda)=1}|W_{g_0}(\lambda)-2[\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}]| \\ &= 2K_{\frac{n-1}{2}}(0,n-1)-2\min_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda \\ &= 2\tbinom{4k+2}{2k+1}-4\lfloor m_4\rfloor \end{aligned} \tag{62}$$

for $k=3,4$ and

$$\begin{aligned} \max_{\mathrm{wt}(\lambda)=1}|W_{g_1}(\lambda)| &= \max_{\mathrm{wt}(\lambda)=1}|W_{g_0}(\lambda)-2[\sum_{x\in T_3}(-1)^{\lambda\cdot x}-\sum_{x\in U_3}(-1)^{\lambda\cdot x}]| \\ &= 2K_{\frac{n-1}{2}}(0,n-1)-2\min_{\mathrm{wt}(\lambda)=1}\Gamma_\lambda \\ &= 2\tbinom{4k+2}{2k+1}-4\lfloor m_1\rfloor \end{aligned} \tag{63}$$

for $k \geq 5$.

For $\mathrm{wt}(\lambda)=n$, similarly to the case $n=4k+1$, one has

$$\begin{aligned} |W_{g_1}(\lambda)| &= |(-1)^{\frac{n-1}{2}}2\tbinom{n-1}{\frac{n-1}{2}}-2\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)}+(-1)^{\frac{n+1}{2}}2|U_3|| \\ &= 2|\tbinom{4k+2}{2k+1}+\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)}-|U_3|| \\ &= 2|\tbinom{4k+2}{2k+1}-(|U_3|-\sum_{x\in T_3}(-1)^{\mathrm{wt}(x)})|. \end{aligned}$$

Similarly to the comparison made in Theorem 4.4 (1), we have

$$|U_3| - \sum_{x\in T_3} (-1)^{\mathrm{wt}(x)} > 2\sum_{i=0}^{k-1} \binom{3k}{k+i}.$$

Thus, by Equality (62) and Equality (63), for $\mathrm{wt}(\lambda) = n$, one has

$$|W_{g_1}(\lambda)| < 2[\binom{4k+2}{2k+1} - 2\sum_{i=0}^{k-1}\binom{3k}{k+i}] < 2\binom{4k+2}{2k+1} - 4m_3 < \max_{\mathrm{wt}(\lambda)=1} |W_{g_1}(\lambda)| \tag{64}$$

for $k \geq 3$.

Similarly to the analysis for the case $n = 4k + 1$, one has

$$|W_{g_1}(\lambda)| \quad \leq \quad 2\binom{4k+2}{2k+1}/(4k+1) + 4|U_3| \text{ for } 2 \leq \mathrm{wt}(\lambda) \leq n-1. \tag{65}$$

For $k = 3$, 4, by Lemma 4.3 (2) and Lemma 4.2 (2), one has

$$\begin{aligned} & [2\tbinom{4k+2}{2k+1} - 4\lfloor m_4\rfloor] - [2\tbinom{4k+2}{2k+1}/(4k+1) + 4|U_3|] \\ = \ & 2[4k\tbinom{4k+2}{2k+1}/(4k+1) - 2|U_3| - 2\lfloor m_4\rfloor] \\ \geq \ & 2[4k\tbinom{4k+2}{2k+1}/(4k+1) - 2|U_3| - 2m_1] \\ > \ & 0. \end{aligned}$$

Thus, by Equality (62), by (64) and (65), for $k = 3$, 4, one has

$$\max_{\lambda\in\mathbb{F}_2^n} |W_{g_1}(\lambda)| = 2\binom{4k+2}{2k+1} - 4\lfloor m_4\rfloor = 2\binom{4k+2}{2k+1} - 4\lfloor\sum_{i=0}^{k-1}\binom{3k}{k+i-1}\frac{k-i}{k}\rfloor,$$

which implies

$$nl(g_1) = 2^{4k+2} - \binom{4k+2}{2k+1} + 2\lfloor\sum_{i=0}^{k-1}\binom{3k}{k+i-1}\frac{k-i}{k}\rfloor,$$

i.e., $\Delta(15) = 268$ and $\Delta(19) = 2436$.

For $k \geq 5$, by Lemma 4.3 (2),

$$\begin{aligned} & [2\tbinom{4k+2}{2k+1} - 4\lfloor m_1\rfloor] - [2\tbinom{4k+2}{2k+1}/(4k+1) + 4|U_3|] \\ = \ & 2[4k\tbinom{4k+2}{2k+1}/(4k+1) - 2|U_3| - 2\lfloor m_1\rfloor] \\ \geq \ & 2[4k\tbinom{4k+2}{2k+1}/(4k+1) - 2|U_3| - 2m_1] \\ > \ & 0. \end{aligned}$$

Thus, by Equality (63), by (64) and (65), one has

$$\max_{\lambda\in\mathbb{F}_2^n} |W_{g_1}(\lambda)| = 2\binom{4k+2}{2k+1} - 4\lfloor m_1\rfloor = 2\binom{4k+2}{2k+1} - 4\lfloor\sum_{i=0}^{k+1}\binom{3k-1}{k+i}\frac{k+2-i}{k+2}\rfloor.$$

This shows

$$nl(g_1) = 2^{4k+2} - \binom{4k+2}{2k+1} + 2\lfloor\sum_{i=0}^{k+1}\binom{3k-1}{k+i}\frac{k+2-i}{k+2}\rfloor.$$

The proof is completed. □

Table 3 Comparison of nonlinearities for odd n variables

n	9	11	13	15	17	19
$2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$	186	772	3172	12952	52666	213524
$nl(g_1)$	196	798	3284	13220	53578	215960

The nonlinearity of g_1 is determined for $n \geq 15$ in Theorem 4.4. For the cases $n = 9$, 11 and 13, its nonlinearity is determined as in Table 3 by a direct calculation.

5. Conclusion

This paper studied several classes of Boolean functions included in Carlet's Construction, and the nonlinearities of these functions were determined. Their values are not yet sufficient for proposing these functions for pseudo-random generators in stream ciphers. But they significantly improve upon the best previously known nonlinearities of functions with optimal algebraic immunity.

References

[1] F. Armknecht, "Improving fast algebraic attacks," In FSE 2004, number 3017 in Lecture Notes in Computer Science, pp. 65-82. Springer Verlag, 2004.

[2] A. Braeken and B. Preneel, "On the algebraic immunity of symmetric Boolean functions," In *Indocrypt 2005*, number 3797 in Lecture Notes in Computer Science, pp. 35-48. Springer Verlag, 2005.

[3] A. Canteaut, "Open problems related to algebraic attacks on stream ciphers," In *Workshop on Coding and Cryptography 2005*, number 3969 in Lecture Notes in Computer Science, pp. 120-134. Springer Verlag, 2006.

[4] C. Carlet, "A method of construction of balanced functions with optimum algebraic immunity," Available online, http://eprint.iacr.org/2006/149. To appear in the proceedings of the Wuyi Workshop on Coding and Cryptology, published by World Scientific Publishing Co. in its series of Coding and Cryptology.

[5] C. Carlet,"On the higher order nonlinearities of algebraic immune functions," In *CRYPTO 2006*, number 4117 in Lecture Notes in Computer Science, pp. 584-601, Springer, 2006.

[6] C. Carlet, D. K. Dalai, K. C. Gupta, and S. Maitra, "Algebraic immunity for cryptographically significant Boolean functions: analysis and construction," *IEEE Transactions on Information Theory,* vol. 52, no. 7, pp. 3105-3121, 2006.

[7] J. Y. Cho and J. Pieprzyk, "Algebraic attacks on SOBER-t32 and SOBER-128," In FSE 2004, number 3017 in Lecture Notes in Computer Science, pp. 49-64. Springer Verlag, 2004.

[8] N. Courtois," Fast algebraic attacks on stream ciphers with linear feedback," In Advances in Cryptology - CRYPTO 2003, number 2729 in Lecture Notes in Computer Science, pp. 176-194. Springer Verlag, 2003.

[9] N. Courtois and W. Meier, "Algebraic attacks on stream ciphers with linear feedback," In *Eurocrypt 2003*, number 2656 in Lecture Notes in Computer Science, pp. 345-359. Springer Verlag, 2003.

[10] N. Courtois and J. Pieprzyk, "Cryptanalysis of block ciphers with overdefined systems of equations," In Advances in Cryptology- ASIACRYPT 2002, number 2501 in Lecture Notes in Computer Science, pp. 267-287. Springer Verlag, 2002.

[11] A. Canteaut and M. Trabbia, "Improved fast correlation attacks using parity-check equations of weight 4 and 5," In *Eurocrypt 2000*, number 1807 in Lecture Notes in Computer Science, pp. 573-588. Springer Verlag, 2000.

[12] D. K. Dalai, K. C. Gupta and S. Maitra, "Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity," In *Workshop on Fast Software Encryption*, FSE 2005, number 3557 in Lecture Notes in Computer Science, pp. 98-111, Springer-Verlag, 2005.

[13] D. K. Dalai, S. Maitra, and S. Sarkar, "Basic theory in construction of Boolean functions with maximum possible annihilator immunity," *Des. Codes Cryptography,* vol. 40, no. 1, pp. 41-58, 2006.

[14] C. Ding, G. Xiao, and W. Shan. The Stability Theory of Stream Ciphers. Number 561 in Lecture Notes in Computer Science. Springer-Verlag, 1991.

[15] D. H. Lee, J. Kim, J. Hong, J. W. Han and D. Moon, "Algebraic attacks on summation generators," In FSE 2004, number 3017 in Lecture Notes in Computer Science, pp. 34-48. Springer Verlag, 2004.

[16] N. Li and W. F. Qi, "Construction and analysis of Boolean functions of $2t + 1$ variables with maximum algebraic immunity," In ASIACRYPT 2006, number 4284 in Lecture Notes in Computer Science, 84-98, 2006.

[17] F. J. MacWilliams and N. J. Sloane, The Theory of Error-Correcting Codes. Amsterdam, The Netherlands: North-Holland, 1977.

[18] W. Meier, E. Pasalic and C. Carlet, "Algebraic attacks and decomposition of Boolean functions," In *Eurocrypt 2004*, number 3027 in Lecture Notes in Computer Science, pp. 474-491. Springer Verlag, 2004.

[19] S. Rønjom and T. Helleseth. A new attack on the filter generator. To appear in *IEEE Transactions on Information theory*, 2007.