J Syst Sci Complex (2015) 28: 725–742

# A Combinatorial Condition and Boolean Functions with Optimal Algebraic Immunity*

**JIN Qingfang · LIU Zhuojun · WU Baofeng · ZHANG Xiaoming**

DOI: 10.1007/s11424-014-2133-x
Received: 26 June 2012 / Revised: 25 March 2013


**Abstract** This paper first proposes an infinite class of $2k$-variable Boolean functions with high nonlinearity and high algebraic degree. Then an infinite class of balanced Boolean functions are proposed by modifying the above Boolean functions. This class of balanced Boolean functions have optimal algebraic degree and high nonlinearity. Both classes have optimal algebraic immunity based on a general combinatorial conjecture.

**Keywords** Algebraic degree, algebraic immunity, balancedness, Bent function, Boolean function, nonlinearity.

## 1 Introduction

Boolean functions are usually used for the combiner and filter functions in stream ciphers and for S-box designing in block ciphers. To resist known attacks, Boolean functions are generally required to have balancedness, high algebraic degree, high nonlinearity, high correlation immunity and high algebraic immunity, and so on[1]. Among them, Algebraic immunity was proposed by Meier, et al.[2, 3] as a response to algebraic attack[2, 4, 5].

It is a challenge to find Boolean functions achieving all the necessary cryptographic criteria. There are several constructions of Boolean functions with optimum algebraic immunity, see [6–10]. However, the nonlinearity of most of Boolean functions proposed are not sufficient for cryptographic applications. An infinite excellent class of balanced Boolean functions, which

JIN Qingfang
*Key Laboratory of System and Control, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190, *China.* Email: qfjin@amss.ac.cn.
LIU Zhuojun · ZHANG Xiaoming
*Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing* 100190, *China.* Email: zliu@mmrc.iss.ac.cn; xmzhang@amss.ac.cn.
WU Baofeng
*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China.* Email: wubaofeng@amss.ac.cn.
*This research is supported by the National Basic Research Program of China under Grant No. 2011CB302400.
◇ *This paper was recommended for publication by Editor LI Ziming.*

were first presented in [11], further studied by Carlet and Feng[12]. It was proved this class of Boolean functions have optimum algebraic immunity, optimal nonlinearity among all known constructions of Boolean functions with optimal algebraic immunity. In 2009, Tu and Deng[13] proposed two classes of Boolean functions of even variables, which have optimal algebraic immunity under the assumption that a combinatorial conjecture is correct. The nonlinearity of these functions is even better than that of the functions in [12]. But Tu-Deng functions are vulnerable to fast algebraic attacks[14]. Boolean functions, which have 1-resiliency, optimal algebraic degree and high nonlinearity, were proposed in [15, 16] through a modification of Boolean functions in [13]. Based on the combinatorial conjecture Tu and Deng[13] introduced, these functions are at least algebraic immunity suboptimal. Tang, et al.[17] proposed two classes of highly nonlinear Boolean functions with optimal algebraic immunity based on a new combinatorial conjecture which had been proved by Cohen and Flori[18] in 2011. These functions also have a good immunity to fast algebraic attacks.

In this paper, the constructions of Boolean functions in [13, 17] are extended to the more general case. We first propose an infinite class of $2k$-variable Boolean functions, which have high nonlinearity and high algebraic degree. Based on a general combinatorial conjecture[17, 18], this infinite class of $2k$-variable Boolean functions have optimal algebraic immunity. By a modification of the above Boolean functions, we also propose an infinite class of balanced Boolean functions with optimal algebraic degree and high nonlinearity. And this class of balanced Boolean functions have the same algebraic immunity as the above class. The proof techniques for the properties of Boolean functions are analogous to those of [12] and [13] in this presentation.

The remainder of the paper is organized as follows. In Section 2, we recall the necessary background of Boolean functions. In Section 3, we introduce the general combinatorial conjecture, with the aid of which we discuss the algebraic immunity of the proposed Boolean functions. In Section 4 and Section 5, we give two constructions and discuss their algebraic degree, nonlinearity and algebraic immunity. Section 6 concludes the paper.

## 2 Preliminaries

Let $n$ be a positive integer. A Boolean function of $n$ variables is a mapping from $\mathcal{F}_2^n$ to $\mathcal{F}_2$, where $\mathcal{F}_2$ denotes the finite field with two elements. Denote $\mathcal{B}_n$ the set of all $n$-variable Boolean functions. The basic representation of an $n$-variable Boolean function $f$ is by the output column of its truth table, i.e., a binary string of length $2^n$,

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

The Hamming weight of $f$, $\mathrm{w}t(f)$, is the size of the support $\mathrm{supp}(f) = \{\, x \in \mathcal{F}_2^n \mid f(x) = 1 \,\}$. We say that a Boolean function $f$ is balanced if the number of 1s equals the number of 0s in its truth table, that is, if its Hamming weight equals $2^{n-1}$.

Any Boolean function has a unique representation as a multivariate polynomial over $\mathcal{F}_2$,

which is called the algebraic normal form (ANF):

$$f(x_1, x_2, \cdots, x_n) = \sum_{I \subseteq \{1,2,\cdots,n\}} a_I \prod_{i \in I} x_i, \quad a_I \in \mathcal{F}_2.$$

The algebraic degree, $\deg(f)$, is defined to be

$$\deg(f) = \max_{I \subseteq \{1,2,\cdots,n\}} \{|I| \,|\, a_I \neq 0\}.$$

A Boolean function is affine if it has algebraic degree at most 1. The set of all affine functions is denoted by $A_n$.

We identify the field $\mathcal{F}_{2^n}$ with the vector space $\mathcal{F}_2^n$. An $n$-variable Boolean functions can also be uniquely expressed by a univariate polynomial over $\mathcal{F}_{2^n}$

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_0$, $a_{2^n-1} \in \mathcal{F}_2$, $a_i \in \mathcal{F}_{2^n}$ for $1 \leq i < 2^n - 1$ such that $a_i^2 = a_{2i(\mathrm{mod}\, 2^n-1)}$. The binary expansion of $i$ is $i = i_0 + i_1 2 + \cdots + i_{n-1}2^{n-1}$, and we denote $\overline{i} = (i_0, i_1, \cdots, i_{n-1}) \in \mathcal{F}_2^n$. The algebraic degree of $f$ equals $\max\{\, \mathrm{wt}(i) \,|\, a_i \neq 0,\, 0 \leq i < 2^n\}$, where $\mathrm{wt}(i) = i_0 + i_1 + \cdots + i_{n-1} \in \mathcal{Z}$.

The Hamming distance $d_H(f, g)$ between two Boolean functions $f$ and $g$ is the Hamming weight of their difference $f + g$, i.e., $d_H(f, g) = |\{\, x \in \mathcal{F}_2^n \,|\, f(x) + g(x) = 1 \,\}|$. The nonlinearity $N_f$ of a Boolean function $f \in \mathcal{B}_n$ is defined as

$$N_f = \min_{g \in A_n} (d_H(f, g)).$$

Let $x = (x_1, x_2, \cdots, x_n)$ and $a = (a_1, a_2, \cdots, a_n)$ both belong to $\mathcal{F}_2^n$ and $a \cdot x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$.

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

is called the Walsh spectrum of $f$ at $a$. For $f : \mathcal{F}_{2^n} \longrightarrow \mathcal{F}_2$, the Walsh spectrum of $f$ at $a \in \mathcal{F}_{2^n}$ is defined by

$$W_f(a) = \sum_{x \in \mathcal{F}_{2^n}} (-1)^{f(x)+\mathrm{tr}(ax)},$$

where tr is the trace function from $\mathcal{F}_{2^n}$ to $\mathcal{F}_2$. For $f : \mathcal{F}_{2^k} \times \mathcal{F}_{2^k} \longrightarrow \mathcal{F}_2$, the Walsh spectrum of $f$ at $(a, b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}$ is defined by

$$W_f(a, b) = \sum_{(x,y) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}} (-1)^{f(x,y)+\mathrm{tr}(ax+by)}.$$

A Boolean function $f$ is balanced if and only if $W_f(0) = 0$. The nonlinearity of $f$ can also be expressed via its Walsh spectra as

$$N_f = 2^{n-1} - \frac{1}{2} \max_{a \in \mathcal{F}_{2^n}} |W_f(a)|.$$

It is well-known that the nonlinearity satisfies the following inequality

$$N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

The upper bound can be attained when $n$ is even, and such Boolean functions are called Bent functions.

**Definition 2.1** (see [3]) The algebraic immunity $AI(f)$ of an $n$-variable Boolean function $f \in \mathcal{B}_n$ is defined to be the lowest degree of nonzero Boolean functions $g$ such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.

Courtois and Meier[2] proved that $AI(f) \leq \lceil \frac{n}{2} \rceil$. The algebraic immunity, as well as the nonlinearity and algebraic degree, is affine invariant.

We can refer to [19] for BCH code and [20] for finite fields used in this paper.

## 3 Some Combinatorial Conditions

In this section, we will introduce some combinatorial conjectures for discussing the algebraic immunity of some Boolean functions. Denote $\mathcal{Z}^*_{2^k-1} = \{u \in \mathcal{Z}_{2^k-1} | \gcd(u, 2^k - 1) = 1\}$ throughout this paper.

Tu and Deng in [13] presented two classes of Boolean functions as follows.

**Construction 3.1** Let $n = 2k \geq 4$ be an integer and $\alpha$ be a primitive element of the finite field $\mathcal{F}_{2^k}$. Set $\Delta = \{1 = \alpha^0, \alpha^1, \cdots, \alpha^{2^{k-1}-1}\}$. Define $f, F \in \mathcal{B}_n$ as

$$f(x,y) = g(xy^{2^k-2}), \quad F(x,y) = \begin{cases} g(xy^{2^k-2}), & x \neq 0, \\ g(y), & x = 0, \end{cases}$$

where $g$ is a Boolean function defined over $\mathcal{F}_{2^k}$ with $\mathrm{supp}(g) = \Delta$.

In order to discuss the algebraic immunity of Boolean functions above, they presented the following combinatorial conjecture on binary strings.

**Conjecture 3.2** (see [13]) Let $k \geq 2$ be an integer. For any $0 < t < 2^k - 1$, define

$$S_{k,t,+} = \{ (a,b) \,|\, 0 \leq a, b < 2^k - 1, a + b \equiv t (\mathrm{mod}\, 2^k - 1), \mathrm{wt}(a) + \mathrm{wt}(b) \leq k - 1 \}.$$

Then $|S_{k,t,+}| \leq 2^{k-1}$.

Tu and Deng[13] pointed out that the correctness of Conjecture 3.2 implies the optimal algebraic immunity of Boolean functions in Construction 3.1. And they could validate this conjecture when $k \leq 29$[13]. In [21, 22], the authors proved it is true for many cases of $t$.

Tang, et al.[17] presented another combinatorial conjecture similar to Conjecture 3.2 to investigate the algebraic immunity of Boolean functions they introduced.

**Conjecture 3.3** (see [17]) Let $k \geq 2$ be an integer. For any $0 \leq t < 2^k - 1$, define

$$S_{k,t,-} = \{ (a,b) \,|\, 0 \leq a, b < 2^k - 1, a - b \equiv t (\mathrm{mod}\, 2^k - 1), \mathrm{wt}(a) + \mathrm{wt}(b) \leq k - 1 \}.$$

Then $|S_{k,t,-}| \leq 2^{k-1}$.

Fortunately, Conjecture 3.3 has been proved[18], so Boolean functions Tang, et al.[17] proposed have optimal algebraic immunity. The authors also referred to a general conjecture in [17] as follows.

**Conjecture 3.4** Let $k \geq 2$ be an integer, and $u \in \mathcal{Z}^*_{2^k-1}$. For any $0 \leq t < 2^k - 1$, define

$$S_{k,t,u} = \{\, (a,b) \,|\, 0 \leq a, b < 2^k - 1, ua + b \equiv t (\mathrm{mod}\, 2^k - 1), \mathrm{w}t(a) + \mathrm{w}t(b) \leq k - 1\}.$$

Then $|S_{k,t,u}| \leq 2^{k-1}$.

For $2 \leq k \leq 15$, this general conjecture was checked in [17]. This general conjecture includes Conjecture 3.2 and Conjecture 3.3 as special cases. A more general conjecture is as follows.

**Conjecture 3.5** Let $k \geq 2$ be an integer, and $u, v \in \mathcal{Z}^*_{2^k-1}$. For any $0 \leq t < 2^k - 1$, define

$$S_{k,t,u,v} = \{\, (a,b) \,|\, 0 \leq a, b < 2^k - 1, ua + vb \equiv t (\mathrm{mod}\, 2^k - 1), \mathrm{w}t(a) + \mathrm{w}t(b) \leq k - 1\}.$$

Then $|S_{k,t,u,v}| \leq 2^{k-1}$.

**Lemma 3.6** *Conjecture* 3.5 *is equivalent to Conjecture* 3.4.

*Proof* It's obvious Conjecture 3.5 implies Conjecture 3.4.

If Conjecture 3.4 is true, i.e., for any $u \in \mathcal{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{k,t,u}| \leq 2^{k-1}$. For any $v \in \mathcal{Z}^*_{2^k-1}$,

$$(a,b) \in S_{k,t,u} \text{ if and only if } (a,b) \in S_{k,vt,uv,v},$$

so $|S_{k,vt,uv,v}| = |S_{k,t,u}| \leq 2^{k-1}$.

For any $u, v \in \mathcal{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{k,vt,uv,v}| \leq 2^{k-1}$ if and only if for any $u, v \in \mathcal{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{k,t,u,v}| \leq 2^{k-1}$. Therefore, Conjecture 3.5 is true. ∎

The properties of set $S_{k,t,u}$ were also investigated in [18].

**Lemma 3.7** (see [18]) *Let $S_{k,t,u}$ be defined as above. Then it satisfies the following properties:*

i) $|S_{k,t,u}| = |\{\, a \in \mathcal{Z}_{2^k-1} \,|\, \mathrm{w}t(a) + \mathrm{w}t(t - ua) \leq k - 1\}|$.

ii) $|S_{k,t,u}| = |S_{k,2t,u}|$.

iii) $|S_{k,t,u}| = |S_{k,t,2u}|$.

iv) $|S_{k,t,u}| = |S_{k,u^{-1}t,u^{-1}}|$.

As Lemma 3.7 and the proved Conjecture 3.3, Conjecture 3.4 is correct for $u = -2^l$, $0 \leq l < k$.

## 4 Boolean Functions with Optimal Algebraic Immunity

In this section, we present an infinite class of $2k$-variable Boolean functions and discuss its algebraic immunity, algebraic degree and nonlinearity.

**Construction 4.1** Let $n = 2k \geq 4$, $u \in \mathcal{Z}^*_{2^k-1}$. Let $\alpha$ be a primitive element of the finite field $\mathcal{F}_{2^k}$. Set $\Delta_s = \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k - 1$ is an integer. Then we

define a Boolean function $f \in \mathcal{B}_n$ as follows:

$$f(x,y) = g(xy^{2^k-1-u}),$$

where $g$ is a Boolean function defined over $\mathcal{F}_{2^k}$ with $\mathrm{supp}(g) = \Delta_s$.

**Remark 4.2** If we replace $xy^{2^k-1-u}$ with $x^v y^{2^k-1-u}$, $u, v \in \mathcal{Z}^*_{2^k-1}$ in Construction 4.1, the conclusions in this section can be applied to the corresponding Boolean functions. More precisely, if Boolean functions $f(x,y) = g(x^v y^{2^k-1-u})$ with the function $g$ as above. Then $\mathrm{supp}(f) = \{(x, y) \mid x^v y^{2^k-1-u} \in \Delta_s, x, y \in \mathcal{F}^*_{2^k-1}\}$, i.e., $\mathrm{supp}(f) = \{(x, y) \mid xy^{2^k-1-v^{-1}u} \in \Delta'_s, x, y \in \mathcal{F}^*_{2^k-1}\}$, where $\Delta'_s = \{(\alpha^{v^{-1}})^s, (\alpha^{v^{-1}})^{s+1}, \cdots, (\alpha^{v^{-1}})^{2^{k-1}+s-1}\}$. For example, $\mathrm{supp}(f) = \{(x, y) \mid xy^{2^k-2} \in \{(\alpha^{-1})^s, (\alpha^{-1})^{s+1}, \cdots, (\alpha^{-1})^{2^{k-1}+s-1}\}, x, y \in \mathcal{F}^*_{2^k-1}\}$ for $u = v = -1$. That is to say, the function $f$ is Boolean functions defined in Construction 4.1 when $\alpha^{v^{-1}}$ is a primitive element of the finite field $\mathcal{F}_{2^k}$.

It is obtained immediately that $\mathrm{wt}(f) = 2^{k-1}(2^k-1) = 2^{2k-1} - 2^{k-1}$. The properties of Boolean functions in Construction 4.1 will be investigated in the following subsections.

### 4.1 Algebraic Immunity

**Theorem 4.3** *Let $f$ be the $n$-variable Boolean function defined in Construction* 4.1. *If Conjecture* 3.4 *is correct, then $f$ has optimal algebraic immunity, i.e., $AI(f) = k$.*

*Proof* It is sufficient to prove that both $f$ and $f+1$ have no annihilators with algebraic degrees less than $k$. Let $f$ admit a nonzero annihilator $h : \mathcal{F}_{2^k} \times \mathcal{F}_{2^k} \longrightarrow \mathcal{F}_2$ with $\deg(h) < k$. Boolean function $h$ can be written as a bivariate polynomial on $\mathcal{F}_{2^k}$

$$h(x,y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j, \quad h_{i,j} \in \mathcal{F}_{2^k}.$$

It follows that $h_{i,j} = 0$ if $\mathrm{wt}(i) + \mathrm{wt}(j) \geq k$, which implies $h_{2^k-1,i} = h_{j,2^k-1} = 0$ for all $0 \leq i, j \leq 2^k - 1$. Since $f \cdot h = 0$ and $\mathrm{supp}(f) = \{(\gamma y^u, y) | y \in \mathcal{F}^*_{2^k}, \gamma \in \Delta_s\}$, then $h(x,y) = 0$ for all $(x,y) \in \mathrm{supp}(f)$, i.e., $h(\gamma y^u, y) = 0$ for all $y \in \mathcal{F}^*_{2^k}$, $\gamma \in \Delta_s$.

$$h(\gamma y^u, y) = \sum_{i=0}^{2^k-2} \sum_{j=0}^{2^k-2} h_{i,j} (\gamma y^u)^i y^j = \sum_{i=0}^{2^k-2} \sum_{j=0}^{2^k-2} h_{i,j} \gamma^i y^{j+ui}$$

can be written as

$$h(\gamma y^u, y) = \sum_{t=0}^{2^k-2} h_t(\gamma) y^t,$$

where

$$\begin{aligned} h_t(\gamma) &= \sum_{0 \leq i,j \leq 2^k-2, ui+j \equiv t (\mathrm{mod}\, 2^k-1)} h_{i,j} \gamma^i \\ &= h_{0,t} + h_{1,t-u(\mathrm{mod}\, 2^k-1)} \gamma + h_{2,t-2u(\mathrm{mod}\, 2^k-1)} \gamma^2 \\ &\quad + \cdots + h_{2^k-2,t-(2^k-2)u(\mathrm{mod}\, 2^k-1)} \gamma^{2^k-2}. \end{aligned}$$

Note that $\{t - ui(\mathrm{mod}\, 2^k - 1) | 0 \le i < 2^k - 1\} = \mathcal{Z}_{2^k-1}$ due to $(u, 2^k - 1) = 1$.

For any $\gamma \in \Delta_s$, $h(\gamma y^u, y) = 0$ for all $y \in \mathcal{F}_{2^k}^*$, so it follows that

$$h_t(\gamma) = 0,\ 0 \le t \le 2^k - 2,\ \text{for all } \gamma \in \Delta_s.$$

From the definition of BCH code, we know that the vector

$$(h_{0,t}, h_{1,t-u(\mathrm{mod}\, 2^k-1)}, h_{2,t-2u(\mathrm{mod}\, 2^k-1)}, \cdots, h_{2^k-2,t-(2^k-2)u(\mathrm{mod}\, 2^k-1)})$$

is a codeword in some BCH code of length $2^k - 1$ over $\mathcal{F}_{2^k}$, having the elements in $\Delta_s$ as zeros and the designed distance $2^{k-1} + 1$. If this codeword is nonzero, its Hamming weight should be greater than or equal to $2^{k-1} + 1$. But this contradicts the fact that the Hamming weight of this codeword should be less than or equal to $2^{k-1}$ from Conjecture 3.4. Hence, this codeword must be zero, that is,

$$h_{0,t} = h_{1,t-u(\mathrm{mod}\, 2^k-1)} = h_{2,t-2u(\mathrm{mod}\, 2^k-1)} = \cdots = h_{2^k-2,t-(2^k-2)u(\mathrm{mod}\, 2^k-1)} = 0$$

for any $0 \le t \le 2^k - 2$. This proves $h = 0$.

Next, we prove a similar result for $f + 1$. Let $h(x, y) \in \mathcal{B}_{2k}$ such that $\deg(h) < k$ and $(f + 1) \cdot h = 0$, then

$$\mathrm{supp}(f + 1) = \{\, (x, y) \,|\, xy^{2^k-1-u} \in \mathcal{F}_{2^k} \setminus \Delta_s, x, y \in \mathcal{F}_{2^k} \}.$$

Similarly, for all $0 \le t \le 2^k - 2$, we have

$$h_t(\gamma) = 0,\ \text{for any } \gamma \in \mathcal{F}_{2^k}^* \setminus \Delta_s.$$

Then the vector

$$(h_{0,t}, h_{1,t-u(\mathrm{mod}\, 2^k-1)}, h_{2,t-2u(\mathrm{mod}\, 2^k-1)}, \cdots, h_{2^k-2,t-(2^k-2)u(\mathrm{mod}\, 2^k-1)})$$

is also a codeword in some BCH code of length $2^k - 1$ over $\mathcal{F}_{2^k}$, having the elements in $\mathcal{F}_{2^k}^* \setminus \Delta_s$ as zeros and designed distance $2^{k-1}$. If the codeword is nonzero, its Hamming weight is at least $2^{k-1}$.

At the same time, $h(0, \beta) = \sum_{j=0}^{2^k-2} h_{0,j}\beta^j$ for any $\beta \in \mathcal{F}_{2^k}$, hence $h_{0,j} = 0$ for $0 \le j \le 2^k - 2$. According to Conjecture 3.4 and $h_{0,i} = 0, 0 \le i \le 2^k - 2$, the Hamming weight of vector $h_t$ is less than $2^{k-1}$. A contraction follows. Thus it's obtained that $h = 0$.

From the above discussion, we have $AI(f) = k$. That is to say, the constructed Boolean functions have optimal algebraic immunity. ∎

Conjecture 3.4 is correct for $u = -2^l$, $0 \le l < k$, therefore Boolean function $f$ defined by Construction 4.1 has the optimal algebraic immunity, i.e., $AI(f) = k$ in this case.

### 4.2 Polynomial Representation and Algebraic Degree

**Theorem 4.4** *Let $f$ be the $n$-variable Boolean function defined in Construction* 4.1. *Then its bivariate representation is*

$$f(x, y) = \sum_{i=1}^{2^k-2} \alpha^{-is}(1 + \alpha^{-i})^{2^{k-1}-1}(xy^{2^k-1-u})^i.$$

*Furthermore, the algebraic degree of $f$ is* $\max_{1\le i\le 2^k-2}\{\mathrm{wt}(i)+\mathrm{wt}((2^k-1-u)i)\}$ *and* $k\le \deg(f)\le 2(k-1)$.

*Proof* Let $g(x)=\sum_{i=0}^{2^k-1} g_i x^i$ be the univariate representation of $g$ over $\mathcal{F}_{2^k}$. It's obvious $g_0=g(0)=0$, $g_{2^k-1}=0$ (since $g$ has even Hamming weight). For every $i\in\{1,2,\cdots,2^k-2\}$,

$$g_i=\sum_{j=0}^{2^k-2} g(\alpha^j)\alpha^{-ij}=\sum_{j=s}^{2^{k-1}-1+s}\alpha^{-ij}=\alpha^{-is}\frac{1+\alpha^{-i2^{k-1}}}{1+\alpha^{-i}}=\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}.$$

Then $g(y)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}y^i$ and $\deg(g)=k-1$. By the definition of $f(x,y)$, we obtain

$$f(x,y)=g(xy^{2^k-1-u})=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}(xy^{2^k-1-u})^i$$

and $\deg(f)=\max_{1\le i\le 2^k-2}\{\mathrm{wt}(i)+\mathrm{wt}((2^k-1-u)i)\}$. It is obvious $k\le\deg(f)\le 2(k-1)$. ∎

**Remark 4.5** 1) If $u=1$, $f$ has algebraic degree $k$, since $\mathrm{wt}(i)+\mathrm{wt}(-i)=k$ for any $1\le i\le 2^k-2$; If $u=2^l$, $1\le l<k$, $\deg(f)=\max_{1\le i\le 2^k-2}(\mathrm{wt}(i)+\mathrm{wt}(-2^l i))=\max_{1\le i\le 2^k-2}\big(\mathrm{wt}(i)+\mathrm{wt}(-i)\big)=k$.

2) If $u=2^k-2$, $\deg(f)=\max_{1\le i\le 2^k-2}\{2\mathrm{wt}(i)\}=2(k-1)=n-2$; If $u=2^k-1-2^l$, $0\le l<k$, $\deg(f)=\max_{1\le i\le 2^k-2}\big(\mathrm{wt}(i)+\mathrm{wt}(2^l i)\big)=\max_{1\le i\le 2^k-2}\big(\mathrm{wt}(i)+\mathrm{wt}(i)\big)=2(k-1)=n-2$.

In Table 1, we give the exact algebraic degree of Boolean functions in Construction 4.1 for some cases.

**Table 1** The algebraic degree of functions in Construction 4.1

| $n$ | The algebraic degree of functions in Construction 4.1 | | | | | | |
|---|---|---|---|---|---|---|---|
| 10 | $u$ | 1 | 3 | 5 | 7 | 11 | 15 | 30 |
| | deg | 5 | 7 | 7 | 7 | 7 | 8 | 8 |
| 12 | $u$ | 1 | 5 | 11 | 13 | 23 | 31 | 62 |
| | deg | 6 | 8 | 9 | 8 | 9 | 10 | 10 |
| 14 | $u$ | 1 | 9 | 19 | 21 | 27 | 55 | 126 |
| | deg | 7 | 10 | 11 | 11 | 10 | 11 | 12 |
| 16 | $u$ | 1 | 7 | 19 | 59 | 61 | 182 | 254 |
| | deg | 8 | 12 | 12 | 12 | 12 | 12 | 14 |
| 18 | $u$ | 1 | 3 | 37 | 57 | 59 | 239 | 510 |
| | deg | 9 | 13 | 14 | 12 | 15 | 15 | 16 |

### 4.3 Nonlinearity

**Lemma 4.6** *Let $k \geq 2$ be a positive integer and $\alpha$ be a primitive element of $\mathcal{F}_{2^k}$. Let $\Delta_s = \{\alpha^s, \cdots, \alpha^{2^{k-1}+s-1}\}$, where $0 \leq s < 2^k - 1$ is an integer. Define*

$$\Gamma_s = \sum_{\gamma \in \Delta_s} \sum_{x \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(\gamma x^u + x)},$$

*where $u \in \mathcal{Z}_{2^k-1}^*$. Then*

$$|\Gamma_s| \leq 1 + \frac{2^{k+1}}{\pi} \ln \frac{4(2^k-1)}{\pi}.$$

*Proof* Let $\zeta = \mathrm{e}^{\frac{2\pi\sqrt{-1}}{2^k-1}}$ be a primitive $(2^k-1)$-th root of unity in the complex field $\mathcal{C}$, and $\chi$ be the multiplicative character of $\mathcal{F}_{2^k}^*$ defined by $\chi(\alpha^j) = \zeta^j$ $(0 \leq j \leq 2^k-2)$. We define the Gauss sum

$$G(\chi^\mu) = \sum_{x \in \mathcal{F}_{2^k}^*} \chi^\mu(x)(-1)^{tr(x)}, \quad 0 \leq \mu \leq 2^k - 2.$$

It is well-known that $G(\chi^0) = -1$ and $|G(\chi^\mu)| = 2^{\frac{k}{2}}$ for $1 \leq \mu \leq 2^k - 2$. By Fourier inverse transform,

$$(-1)^{tr(\alpha^j)} = \frac{1}{2^k-1} \sum_{\mu=0}^{2^k-2} G(\chi^\mu)\overline{\chi}^\mu(\alpha^j), \quad 0 \leq j \leq 2^k - 2.$$

Let $q = 2^k$,

$$\begin{aligned}
\Gamma_s &= \sum_{\gamma \in \Delta_s} \sum_{x \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(\gamma x^u + x)} \\
&= \sum_{i=s}^{\frac{q}{2}+s-1} \sum_{j=0}^{q-2} (-1)^{\mathrm{tr}(\alpha^{i+uj})} (-1)^{\mathrm{tr}(\alpha^j)} \\
&= \frac{1}{(q-1)^2} \sum_{i=s}^{\frac{q}{2}+s-1} \sum_{j=0}^{q-2} \left( \sum_{\mu=0}^{q-2} G(\chi^\mu)\overline{\chi}^\mu(\alpha^{i+ju}) \right) \left( \sum_{\nu=0}^{q-2} G(\chi^\nu)\overline{\chi}^\nu(\alpha^j) \right) \\
&= \frac{1}{(q-1)^2} \sum_{\mu=0}^{q-2} \sum_{\nu=0}^{q-2} \sum_{i=s}^{\frac{q}{2}+s-1} \sum_{j=0}^{q-2} G(\chi^\mu) G(\chi^\nu) \zeta^{-\mu(i+ju)-\nu j} \\
&= \frac{1}{(q-1)^2} \sum_{\mu=0}^{q-2} \sum_{\nu=0}^{q-2} G(\chi^\mu) G(\chi^\nu) \left( \sum_{i=s}^{\frac{q}{2}+s-1} \zeta^{-\mu i} \right) \left( \sum_{j=0}^{q-2} \zeta^{(-\mu u-\nu)j} \right).
\end{aligned}$$

It is easy to deduce that

$$\sum_{i=s}^{\frac{q}{2}+s-1} \zeta^{-\mu i} = \zeta^{-\mu s} \sum_{i=0}^{\frac{q}{2}-1} \zeta^{-\mu i} = \begin{cases} \frac{q}{2}, & \mu = 0, \\ \zeta^{-\mu s} \frac{1 - \zeta^{-\mu \frac{q}{2}}}{1 - \zeta^{-\mu}}, & \mu \neq 0 \end{cases}$$

and

$$\sum_{j=0}^{q-2} \zeta^{(-\mu u-\nu)j} = \begin{cases} q-1, & \nu = \mu(q-1-u), \\ 0, & \nu \neq \mu(q-1-u). \end{cases}$$

Therefore,

$$\begin{aligned}\Gamma_s &= \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^{\mu})G(\chi^{\mu(q-1-u)})\left(\zeta^{-\mu s}\frac{1-\zeta^{-\mu\frac{q}{2}}}{1-\zeta^{-\mu}}\right)+\frac{q}{2(q-1)}\\ &= \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^{\mu})G(\chi^{\mu(q-1-u)})\frac{\zeta^{-\mu s+\frac{\mu}{2}-\frac{\mu q}{4}}(\zeta^{\frac{\mu q}{4}}-\zeta^{-\frac{\mu q}{4}})}{\zeta^{\frac{\mu}{2}}-\zeta^{-\frac{\mu}{2}}}+\frac{q}{2(q-1)}\\ &= \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^{\mu})G(\chi^{\mu(q-1-u)})\frac{\zeta^{-\mu s+\frac{\mu}{2}-\frac{\mu q}{4}}\sin\frac{\mu q\pi}{2(q-1)}}{\sin\frac{\mu\pi}{q-1}}+\frac{q}{2(q-1)}.\end{aligned}$$

We have

$$\begin{aligned}|\Gamma_s| &\le \frac{1}{q-1}\sum_{\mu=1}^{q-2}|G(\chi^{\mu})||G(\chi^{\mu(q-1-u)})|\frac{1}{|\sin\frac{\mu\pi}{q-1}|}+\frac{q}{2(q-1)}\\ &= \frac{q}{2(q-1)}+\frac{q}{q-1}\sum_{\mu=1}^{q-2}\frac{1}{\sin(\frac{\mu\pi}{q-1})}.\end{aligned}$$

From [12],

$$\sum_{\mu=1}^{q-2}\left(\sin\frac{\mu\pi}{q-1}\right)^{-1} \le -\frac{2(q-1)}{\pi}\ln\tan\left(\frac{\pi}{4(q-1)}\right),$$

we get

$$\begin{aligned}|\Gamma_s| &\le \frac{q}{2(q-1)}-\frac{2q}{\pi}\ln\tan\left(\frac{\pi}{4(q-1)}\right)\\ &\le 1-\frac{2q}{\pi}\ln\frac{\pi}{4(q-1)}\\ &\le 1+\frac{2q}{\pi}\ln\frac{4(q-1)}{\pi}.\end{aligned}$$

Therefore, it is obtained that $|\Gamma_s| \le 1+\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}$. ∎

**Theorem 4.7** *Let $n=2k$ and $f\in\mathcal{B}_n$ be the Boolean function given by Construction* 4.1. *Then*

$$N_f \ge 2^{n-1}-\frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}-1 \approx 2^{n-1}-\frac{2\ln 2}{\pi}k2^k.$$

*Proof* We only need to compute $W_f(a,b)$. Obviously $W_f(0,0)=2^{2k}-2\mathrm{wt}(f)=2^{2k}-2(2^k-1)2^{k-1}=2^k$.

For any $(a,b)\in\mathcal{F}_{2^k}\times\mathcal{F}_{2^k}\setminus\{(0,0)\}$,

$$\begin{aligned}W_f(a,b) &= \sum_{(x,y)\in\mathcal{F}_{2^k}\times\mathcal{F}_{2^k}}(-1)^{f(x,y)+\mathrm{tr}(ax+by)}\\ &= -2\sum_{(x,y)\in\mathrm{supp}(f)}(-1)^{\mathrm{tr}(ax+by)}\\ &= -2\sum_{\gamma\in\Delta_s}\sum_{y\in\mathcal{F}_{2^k}^*}(-1)^{\mathrm{tr}(a\gamma y^u+by)}.\end{aligned}$$

If $a = 0, b \in \mathcal{F}_{2^k}^*$, then

$$W_f(0,b) = -2 \sum_{\gamma \in \Delta_s} \sum_{y \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(by)} = 2^k.$$

Since $(u, 2^k - 1) = 1$, $h(y) = ay^u$ is a permutation polynomial on $\mathcal{F}_{2^k}$ s.t. $h(0) = 0$. So if $b = 0,\ a \in \mathcal{F}_{2^k}^*$, then

$$W_f(a,0) = -2 \sum_{\gamma \in \Delta_s} \sum_{y \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(ay^u)} = 2^k.$$

For any $(a,b) \in \mathcal{F}_{2^k}^* \times \mathcal{F}_{2^k}^*$,

$$W_f(a,b) = -2 \sum_{\gamma \in \Delta_s} \sum_{y \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(ab^{-u}\gamma y^u + y)}.$$

Take $ab^{-u}\alpha^s = \alpha^{s'}$,

$$W_f(a,b) = -2 \sum_{\gamma \in \Delta_{s'}} \sum_{y \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(\gamma y^u + y)}.$$

So we get

$$\max_{(a,b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}} |W_f(a,b)| = \max \left\{ 2 \max_{0 \le s < 2^k - 1} \left| \sum_{\gamma \in \Delta_s} \sum_{y \in \mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(\gamma y^u + y)} \right|,\ 2^k \right\}.$$

By Lemma 4.6, we have

$$\begin{aligned} N_f &= 2^{n-1} - \frac{1}{2} \max_{(a,b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}} |W_f(a,b)| \\ &\ge 2^{n-1} - \left( 1 + \frac{2^{k+1}}{\pi} \ln \frac{4(2^k - 1)}{\pi} \right) \\ &\approx 2^{n-1} - \frac{2 \ln 2}{\pi} k 2^k. \end{aligned}$$

The proof is finished. ∎

Theorem 4.7 gives a lower bound of the nonlinearity, which is constant for various $u \in \mathcal{Z}_{2^k-1}^*$. Theorem 4.7 also shows Boolean functions in Construction 4.1 indeed have high nonlinearity. In Table 2, we give the nonlinearity of Boolean functions in Construction 4.1 for even $n$. Let us denote by $N_f$ the nonlinearity of Boolean functions in Construction 4.1. It's found that the nonlinearity varies from $u \in \mathcal{Z}_{2^k-1}^*$. When $u = 1$ and $u = 2^k - 2$, the exact nonlinearity of Boolean functions in Construction 4.1 equals to the exact value in [13, 17].

**Table 2** The nonlinearity of functions in Construction 4.1

| $n$ | | The nonlinearity of functions in Construction 4.1 | | | | | Bound in TH 3 | $2^{n-1}-2^{\frac{n}{2}-1}$ |
|---|---|---|---|---|---|---|---|---|
| 4 | $u$ | 1 | 2 | - | - | - | 5 | 6 |
| | $N_f$ | 6 | 6 | - | - | - | | |
| 6 | $u$ | 1 | 2 | 3 | 5 | 6 | 22 | 28 |
| | $N_f$ | 28 | 28 | 24 | 24 | 24 | | |
| 8 | $u$ | 1 | 7 | 11 | 13 | 14 | 100 | 120 |
| | $N_f$ | 120 | 112 | 112 | 112 | 112 | | |
| 10 | $u$ | 1 | 5 | 7 | 11 | 30 | 442 | 496 |
| | $N_f$ | 496 | 488 | 480 | 480 | 480 | | |
| 12 | $u$ | 1 | 5 | 11 | 23 | 62 | 1879 | 2016 |
| | $N_f$ | 2016 | 1984 | 1992 | 1984 | 1988 | | |
| 14 | $u$ | 1 | 9 | 21 | 112 | 126 | 7797 | 8128 |
| | $N_f$ | 8128 | 8048 | 8064 | 8080 | 8036 | | |
| 16 | $u$ | 1 | 7 | 19 | 134 | 254 | 31865 | 32640 |
| | $N_f$ | 32640 | 32512 | 32480 | 32528 | 32520 | | |
| 18 | $u$ | 1 | 72 | 376 | 457 | 510 | 129039 | 130816 |
| | $N_f$ | 130816 | 130432 | 130624 | 130576 | 130520 | | |
| 20 | $u$ | 1 | 7 | 36 | 587 | 1022 | 519770 | 523776 |
| | $N_f$ | 523776 | 523104 | 523168 | 523200 | 523164 | | |
| 22 | $u$ | 1 | 19 | 257 | 1726 | 2046 | 2087212 | 2096128 |
| | $N_f$ | 2096128 | 2095008 | 2094720 | 2095440 | 2095012 | | |

### 4.4 A Class of Bent Function with Optimal Algebraic Immunity

The infinite class of Boolean functions defined in Construction 4.1 have different nonlinearity for various $u$. We note that this class are Bent functions when $u = 2^l$.

**Theorem 4.8** *Let $f$ be the $n$-variable Boolean function defined in Construction* 4.1. *Take $u = 2^l$, $0 \le l < k$. If Conjecture* 3.4 *is true, then $f$ is Bent with optimal algebraic immunity, and has algebraic degree $k$.*

*Proof* As is proved in Theorem 4.3 that $AI(f) = \frac{n}{2} = k$.

From Theorem 4.7, when $(a, b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}$ and $ab = 0$, $W_f(a, b) = 2^k$.

For any $(a,b) \in \mathcal{F}_{2^k}^* \times \mathcal{F}_{2^k}^*$,

$$\begin{aligned} W_f(a,b) &= \sum_{(x,y)\in \mathcal{F}_{2^k}\times\mathcal{F}_{2^k}} (-1)^{f(x,y)+\mathrm{tr}(ax+by)} \\ &= -2 \sum_{(x,y)\in \mathrm{supp}(f)} (-1)^{\mathrm{tr}(ax+by)} \\ &= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(a\gamma y^u+by)} \\ &= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(a\gamma y^u)+\mathrm{tr}(by)}. \end{aligned}$$

There exists a unique $\beta_\gamma \in \mathcal{F}_{2^k}^*$ s.t. $\beta_\gamma^u = a\gamma$. So $\mathrm{tr}(a\gamma y^u) = \mathrm{tr}(\beta_\gamma y)$ and

$$\begin{aligned} W_f(a,b) &= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}(\beta_\gamma y)+\mathrm{tr}(by)} \\ &= -2 \sum_{\gamma\in\Delta_s} \sum_{y\in\mathcal{F}_{2^k}^*} (-1)^{\mathrm{tr}((\beta_\gamma+b)y)}. \end{aligned}$$

Case 1: $\beta_\gamma + b \neq 0$, i.e., $a\gamma \neq b^u$ for any $\gamma \in \Delta_s$,

$$W_f(a,b) = -2 \sum_{\gamma\in\Delta_s} \left( \sum_{x\in\mathcal{F}_{2^k}} (-1)^{\mathrm{tr}(x)} - (-1)^{\mathrm{tr}(0)} \right) = 2^k$$

(since $\sum_{x\in\mathcal{F}_{2^k}} (-1)^{\mathrm{tr}(x)} = 0$).

Case 2: $\beta_\gamma + b = 0$, i.e., $a\gamma_1 = b^u$ for some $\gamma_1 \in \Delta_s$,

$$\begin{aligned} W_f(a,b) &= -2 \sum_{\gamma\in\Delta_s\setminus\{\gamma_1\}} \left( \sum_{x\in\mathcal{F}_{2^k}} (-1)^{\mathrm{tr}(x)} - (-1)^{\mathrm{tr}(0)} \right) - 2 \sum_{y\in\mathcal{F}_{2^k}^*} (-1)^0 \\ &= -2(2^{k-1}-1)(-1) - 2(2^k-1) = -2^k. \end{aligned}$$

Note that there exists at most one element $\gamma \in \Delta_s$ satisfying $a\gamma = b^u$ for any $(a,b) \in \mathcal{F}_{2^k}^* \times \mathcal{F}_{2^k}^*$.

From the above discussion, for any $(a,b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}$, $W_f(a,b) = 2^k$ or $W_f(a,b) = -2^k$, so $f$ is Bent.

By Remark 4.5, $\deg(f) = k$. ∎

Recall that the algebraic degree of $2k$-variable Bent functions is at most $k$, so this class of Bent functions that we construct is algebraic degree optimal.

**Remark 4.9** In fact, this class of Bent functions is Dillon's $\mathcal{PS}$ functions[23], since $E_\gamma = \{(\gamma y^{2^l}, y) | y \in \mathcal{F}_{2^k}\}, \gamma \in \Delta_s$ are $2^{k-1}$ linear subspaces of $\mathcal{F}_{2^{2k}}$ of dimension $k$ and $E_{\gamma_1} \cap E_{\gamma_2} = \emptyset$ for $\gamma_1 \neq \gamma_2, \gamma_1, \gamma_2 \in \Delta_s$. Besides, this class of Boolean functions are affine equivalent to Bent functions Tu and Deng proposed.

## 5 Balanced Function with Optimal Algebraic Immunity

In this section, we will give a class of $2k$-variable balanced Boolean functions by a slight modification of Construction 4.1. Based on Conjecture 3.4, we will show this class of functions have optimal algebraic immunity. These functions also have high nonlinearity and high algebraic degree.

**Construction 5.1** Let $n = 2k$ be an even integer, $k \geq 2$ and $u \in \mathcal{Z}^*_{2^k-1}$. Let $\alpha$ be a primitive element of the finite field $\mathcal{F}_{2^k}$. Set $\Delta_s = \{\alpha^s, \cdots, \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k - 1$ is an integer. Define the Boolean function $F \in \mathcal{B}_n$ as follows:

$$F(x,y) = \begin{cases} g(xy^{2^k-1-u}), & x \neq 0, \\ g(y), & x = 0, \end{cases}$$

where $g$ is a Boolean function defined on $\mathcal{F}_{2^k}$ with $\mathrm{supp}(g) = \Delta_s$.

**Remark 5.2** Similar to Remark 4.2, one can get Boolean functions by replacing $xy^{2^k-1-u}$ with $x^v y^{2^k-1-u}$, $u, v \in \mathcal{Z}^*_{2^k-1}$, to which the conclusions in this section are also applied.

**Theorem 5.3** *Let $F$ be the $n$-variable Boolean function defined in Construction* 5.1. *Then $F$ is balanced and* $\deg(F) = n - 1$.

*Proof* Let $n$-variable Boolean function $f$ be defined in Construction 4.1. It is obvious that $F$ is balanced since $\mathrm{wt}(F) = \mathrm{wt}(g) + \mathrm{wt}(f) = 2^{k-1} + 2^{k-1}(2^k - 1) = 2^{n-1}$.

It's easy to see that $F(x,y) = f(x,y) + (1 + x^{2^k-1})g(y)$. Since $\deg((1 + x^{2^k-1})g(y)) = 2k - 1 > \deg(f)$, $\deg(F) = 2k - 1 = n - 1$. ∎

**Theorem 5.4** *Let $F$ be the $n$-variable Boolean function defined in Construction* 5.1. *If Conjecture* 3.4 *is true, then $F$ has the optimal algebraic immunity, i.e., $AI(F) = \frac{n}{2} = k$.*

*Proof* From Construction 5.1, we have $\{(\gamma y^u, y) | y \in \mathcal{F}^*_{2^k}, \gamma \in \Delta_s\} \subseteq \mathrm{supp}(F)$ and $\{(\gamma y^u, y) | y \in \mathcal{F}^*_{2^k}, \gamma \in \mathcal{F}^*_{2^k} \setminus \Delta_s\} \cup \{(x,0) | x \in \mathcal{F}_{2^k}\} \subseteq \mathrm{supp}(F+1)$. By a similar proof to that of Theorem 4.3, we can see both $F$ and $F+1$ have no nonzero annihilators with algebraic degree less than $k$. So Boolean function $F$ also has optimal algebraic immunity. ∎

For $u = -2^l$, $0 \leq l < k$, Boolean function $F$ defined by Construction 5.1 has the optimal algebraic immunity, i.e., $AI(F) = k$.

**Lemma 5.5** (see [12]) *Let $\alpha \in \mathcal{F}^*_{2^k}$ be a primitive element and $\lambda \in \mathcal{F}_{2^k}$. Denote*

$$S_\lambda = \sum_{i=s}^{2^{k-1}+s-1} (-1)^{\mathrm{tr}(\lambda \alpha^i)}.$$

*If $\lambda \neq 0$, then*

$$|S_\lambda| \leq 1 + \frac{2^{\frac{k}{2}+1}}{\pi} \ln \frac{4(2^k-1)}{\pi}.$$

**Theorem 5.6** *Let $F$ be the $n$-variable Boolean function defined by Construction* 5.1. *Then*

$$\begin{aligned} N_F &\geq 2^{n-1} - \frac{2^{k+1}}{\pi} \ln \frac{4(2^k-1)}{\pi} - \frac{2^{\frac{k}{2}+1}}{\pi} \ln \frac{4(2^k-1)}{\pi} - 2 \\ &\approx 2^{n-1} - \frac{2\ln 2}{\pi} k 2^k - \frac{2\ln 2}{\pi} k 2^{\frac{k}{2}}. \end{aligned}$$

*Proof* For any $(a,b) \in \mathcal{F}_{2^k} \times \mathcal{F}_{2^k}$,

$$\begin{aligned} W_F(a,b) &= \sum_{(x,y)\in \mathcal{F}_{2^k}\times\mathcal{F}_{2^k}} (-1)^{F(x,y)+\mathrm{tr}(ax+by)} \\ &= \sum_{y\in\mathcal{F}_{2^k}} (-1)^{g(y)+\mathrm{tr}(by)} + \sum_{(x,y)\in \mathcal{F}_{2^k}^*\times\mathcal{F}_{2^k}} (-1)^{f(x,y)+\mathrm{tr}(ax+by)} \\ &= \sum_{y\in\mathcal{F}_{2^k}} (-1)^{g(y)+\mathrm{tr}(by)} + \sum_{(x,y)\in \mathcal{F}_{2^k}\times\mathcal{F}_{2^k}} (-1)^{f(x,y)+\mathrm{tr}(ax+by)} \\ &\quad - \sum_{y\in\mathcal{F}_{2^k}} (-1)^{\mathrm{tr}(by)} \\ &= \begin{cases} 0, & \text{if } \ b=0, \\ W_g(b)+W_f(a,b), & \text{else.} \end{cases} \end{aligned}$$

Consequently,

$$\max_{(a,b)\in\mathcal{F}_{2^k}\times\mathcal{F}_{2^k}} |W_F(a,b)| \le \max_{(a,b)\in\mathcal{F}_{2^k}\times\mathcal{F}_{2^k}^*} |W_f(a,b)| + \max_{b\in\mathcal{F}_{2^k}^*} |W_g(b)|.$$

For $b \in \mathcal{F}_{2^k}^*$,

$$W_g(b) = \sum_{x\in\mathcal{F}_{2^k}} (-1)^{g(x)+\mathrm{tr}(bx)} = -2 \sum_{i=s}^{2^{k-1}+s-1} (-1)^{\mathrm{tr}(b\alpha^i)}.$$

By Lemmas 4.6 and 5.5,

$$\begin{aligned} N_F &\ge 2^{n-1} - \frac{2^{k+1}}{\pi} \ln \frac{4(2^k-1)}{\pi} - \frac{2^{\frac{k}{2}+1}}{\pi} \ln \frac{4(2^k-1)}{\pi} - 2 \\ &\approx 2^{n-1} - \frac{2\ln 2}{\pi} k 2^k - \frac{2\ln 2}{\pi} k 2^{\frac{k}{2}}. \end{aligned}$$

The proof is finished. ∎

Theorem 5.6 shows Boolean functions in Construction 5.1 indeed have high nonlinearity. This lower bound is constant for various $u \in \mathcal{Z}_{2^k-1}^*$. In Table 3, we give the nonlinearity of Boolean functions in Construction 5.1 for even $n$ compared with that of the Carlet-Feng functions in [12]. $N_f$, $N_{CF}$ and $N_{TCT}$ denote the nonlinearity of Boolean functions in Construction 5.1, that of the Carlet-Feng functions and that of balanced Boolean functions in [17] respectively. It can be found that there are Boolean functions in Construction 5.1 with higher nonlinearity than that of the Carlet-Feng functions and that of balanced Boolean functions in [17]. Indeed, Boolean functions in Construction 5.1 for $u = -1$ is different from balanced Boolean functions in [17] only when $x = 0$. We can also see the nonlinearity is various for different $u \in \mathcal{Z}_{2^k-1}^*$.

**Table 3** The nonlinearity of functions in Construction 5.1

| $n$ | The nonlinearity of functions in Construction 5.1 | | | | | | $N_{CF}$ | $N_{TCT}$ | $Bound_{TH7}$ | $2^{n-1}-2^{\frac{n}{2}-1}$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 4 | $u$ | 1 | - | - | - | 2 | 4 | 4 | 3 | 6 |
| | $N_f$ | 4 | - | - | - | 4 | | | | |
| 6 | $u$ | 1 | 2 | 3 | 5 | 6 | 24 | 22 | 18 | 28 |
| | $N_f$ | 26 | 26 | 22 | 22 | 22 | | | | |
| 8 | $u$ | 1 | 7 | 11 | 13 | 14 | 112 | 108 | 93 | 120 |
| | $N_f$ | 116 | 110 | 110 | 110 | 110 | | | | |
| 10 | $u$ | 1 | 5 | 11 | 19 | 30 | 478 | 476 | 429 | 496 |
| | $N_f$ | 490 | 482 | 476 | 474 | 474 | | | | |
| 12 | $u$ | 1 | 5 | 11 | 23 | 62 | 1970 | 1982 | 1858 | 2016 |
| | $N_f$ | 2008 | 1976 | 1984 | 1976 | 1982 | | | | |
| 14 | $u$ | 1 | 9 | 21 | 112 | 126 | 8036 | 8028 | 7762 | 8128 |
| | $N_f$ | 8118 | 8038 | 8054 | 8070 | 8026 | | | | |
| 16 | $u$ | 1 | 7 | 19 | 134 | 254 | 32530 | 32508 | 31808 | 32640 |
| | $N_f$ | 32624 | 32496 | 32464 | 32514 | 32504 | | | | |
| 18 | $u$ | 1 | 72 | 376 | 457 | 510 | 130442 | 130504 | 128949 | 130816 |
| | $N_f$ | 130792 | 130408 | 130600 | 130552 | 130496 | | | | |

In the following, we consider the behavior of Boolean functions defined by Construction 5.1 against fast algebraic attacks. For a positive integer pair $(e, d)$ with $e$ small and $d$ not too large, if there is a nonzero Boolean function $g$ with degree at most $e$ such that the product $gf$ has degree at most $d$, the Boolean function is considered to be weak against fast algebraic attacks.

Balanced Boolean function in [13], i.e., Boolean functions in Construction 5.1 for $u = 1$, were pointed out to be weak against fast algebraic attacks in [14]. But it is showed there are Boolean functions in Construction 5.1 for some $u \in \mathcal{Z}^*_{2^k-1}$ with good immunity against fast algebraic attacks by some experiments. Some examples are given as follows. We list pairs $(e, d)$ such that there is no nonzero Boolean function $g$ with degree at most $e$ such that the product $gf$ has degree at most $d$ for the following $n$, $u$.

$n = 10$, $u = 5$: $(1, 6), (2, 6), (3, 5), (4, 4)$;
$u = 7$: $(1, 6), (2, 6), (3, 5), (4, 4)$;
$u = 11$: $(1, 6), (2, 6), (3, 5), (4, 4)$;
$u = 30$: $(1, 7), (2, 6), (3, 5), (4, 4)$.
$n = 12$, $u = 5$: $(1, 7), (2, 7), (3, 7), (4, 6), (5, 5)$;
$u = 11$: $(1, 8), (2, 7), (3, 7), (4, 6), (5, 5)$;
$u = 23$: $(1, 8), (2, 7), (3, 7), (4, 6), (5, 5)$;

$u = 62$: $(1,9),(2,7),(3,7),(4,6),(5,5)$.

$n = 14$, $u = 9$: $(1,9),(2,9),(3,9),(4,8),(5,7),(6,6)$;

$u = 21$: $(1,10),(2,10),(3,9),(4,8),(5,7),(6,6)$;

$u = 112$: $(1,10),(2,9),(3,9),(4,8),(5,7),(6,6)$;

$u = 126$: $(1,11),(2,10),(3,9),(4,7),(5,7),(6,6)$.

$n = 16$, $u = 7$: $(1,11),(2,11),(3,10),(4,10),(5,9),(6,8),(7,7)$;

$u = 19$: $(1,11),(2,11),(3,11),(4,10),(5,9),(6,8),(7,7)$;

$u = 134$: $(1,11),(2,11),(3,11),(4,10),(5,9),(6,8),(7,7)$;

$u = 254$: $(1,13),(2,11),(3,11),(4,9),(5,9),(6,7),(7,7)$.

$n = 18$, $u = 72$: $(1,11),(2,11),(3,11),(4,11),(5,11),(6,10),(7,9),(8,8)$;

$u = 376$: $(1,12),(2,12),(3,12),(4,12),(5,11),(6,10),(7,9),(8,8)$;

$u = 457$: $(1,13),(2,13),(3,13),(4,12),(5,11),(6,10),(7,9),(8,8)$;

$u = 510$: $(1,15),(2,14),(3,13),(4,12),(5,11),(6,10),(7,9),(8,8)$.

How do Boolean functions in Construction 5.1 for any $u \in \mathcal{Z}^*_{2^k-1}$ behave against fast algebraic attacks is a further research work of the authors.

## 6 Conclusions

We generalize Tu-Deng functions[13] and the functions proposed by Tang, et al.[17] and put forward two infinite classes of $2k$-variable Boolean functions. Based on Conjecture 3.4, both classes have optimal algebraic immunity. These classes have high nonlinearity and high algebraic degree, even there are Boolean functions in Construction 5.1 with higher nonlinearity than that of the Carlet-Feng functions and that of balanced Boolean functions in [17]. Some experiments show there are Boolean functions in Construction 5.1 with good immunity against fast algebraic attacks.

**Acknowledgements** Thanks LIU Meicheng for his algorithm in computing the immunities of Boolean function against fast algebraic attacks.

### References

[1] Carlet C, Boolean functions for cryptography and error correcting codes, in *The Momography Boolean Methods and Models in Mathematics, Computer Science, and Engineering* (ed. by Crama Y and Hammer P), Cambridge University Press, 2010, 257–397.

[2] Courtois N and Meier W, Algebraic attacks on stream ciphers with linear feedback, Eurocrypt 2003, *Lecture Notes in Computer Science*, 2003, **2656**: 345–359.

[3] Meier W, Pasalic E, and Carlet C, Algebraic attacks and decomposition of Boolean functions, Eurocrypt 2004, *Lecture Notes in Computer Science*, 2004, **3027**: 474–491.

[4] Armkneckt F, Improving fast algebraic attacks, FSE 2004, *Lecture Notes in Computer Science*, 2004, **3017**: 65–82.

[5] Courtois N T, Fast algebraic attacks on stream ciphers with linear feedback, Crypto 2003, *Lecture Notes in Computer Science*, 2003, **2729**: 176–194.

[6] Carlet C, A method of construction of balanced functions with optimum algebraic immunity, Cryptology ePrint Archive, 2006, Report 2006/149.

[7] Carlet C, Dalai D K, Gupta K C, and Maitra S, Algebraic immunity for cryptographically significant Boolean functions: Analysis and construction, *IEEE Transaction on Information Theory*, 2006, **52**(7): 3105–3121.

[8] Carlet C, Zeng X, Li C, and Hu L, Further properties of several classes of Boolean functions with optimum algebraic immunity, *Designs, Codes, Cryptography*, 2009, **52**(3): 303–338.

[9] Dalai D K, Maitra S, and Sarkar S, Basic theory in construction of Boolean functions with maximum possible annihilator immunity, *Designs, Codes, Cryptography*, 2006, **40**(1): 41–58.

[10] Li N and Qi W, Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, Asiacrypt 2006, *Lecture Notes in Computer Science*, 2006, **4284**: 84–98.

[11] Feng K, Liao Q, and Yang J, Maximal values of generalized algebraic immunity, *Designs, Codes, Cryptography*, 2009, **50**(2): 243–252.

[12] Carlet C and Feng K, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonliearity, Asiacrypt 2008, *Lecture Notes in Computer Science*, 2008, **5350**: 425–440.

[13] Tu Z and Deng Y, A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity, *Designs, Codes, Cryptography*, 2011, **60**(1): 1–14.

[14] Carlet C, On a weakness of the Tu-Deng function and its repair, Cryptology ePrint Archive, 2009, Report 2009/606.

[15] Tang X, Tang D, Zeng X, and Hu L, Balanced boolean functions with (almost) optimal algebraic immunity and very high nonlinearity, Cryptology ePrint Archive, 2010, Report 2010/443.

[16] Tu Z and Deng Y, Boolean functions optimizing most of the cryptographic criteria, *Discrete Applied Mathematics*, 2012, **160**(4–5): 427–435.

[17] Tang D, Carlet C, and Tang X, Highly nonlinear Boolean functions with optimum algebraic immunity and good behavior against fast algebraic attacks, *IEEE Transaction on Information Theory*, 2013, **59**(1): 653–664.

[18] Cohen G and Flori J P, On a generalized combinatorial conjecture involving addition mod $2^k-1$, Cryptology ePrint Archive, 2011, Report 2011/400.

[19] MacWilliams F J and Sloane N J A, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[20] Lidl R and Niederreiter H, *Finite Fields*, 2nd Edition, Cambridge University Press, 1997.

[21] Cusick T W, Li Y, and Stanica P, On a combinatorial conjecture, Cryptology ePrint Archive, 2009, Report 2009/554.

[22] Flori J P, Randriambololona H, Cohen G, and Mesnager S, On a conjecture about binary strings distribution, Cryptology ePrint Archive, 2010, Report 2010/170.

[23] Dillon J F, Elementary hadamard difference sets, PhD thesis, University of Maryland, 1974.