1-Resilient Boolean Function with Optimal Algebraic Immunity

Qingfang Jin Zhuojun Liu Baofeng Wu
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS
Beijing 100190, China
qfjin@amss.ac.cn zliu@mmrc.iss.ac.cn.

Abstract In this paper, We propose a class of $2k$-variable Boolean functions, which have optimal algebraic degree, high nonlinearity, and are 1-resilient. These functions have optimal algebraic immunity when $k > 2$ and $u = -2^l, 0 \leq l < k$. Based on a general combinatorial conjecture, algebraic immunity of these functions is optimal when $k > 2$ and $u = 2^l, 0 \leq l < k$. If the general combinatorial conjecture and a new assumption are both true, algebraic immunity of our functions is also optimal when $k > 2, u \neq \pm 2^l, 0 \leq l < k$.

Keywords Boolean function · Algebraic immunity · 1-Resilient · Balancedness · Nonlinearity · Algebraic degree

1 Introduction

To resist known attacks, Boolean functions used in the combiner and filter models of stream ciphers are generally required to be balanced, have high algebraic degree as well as high nonlinearity [2]. Correlation immunity, with respect to correlation attack, was proposed by Siegenthaler[22] in 1985. Xiao and Massey[25] gave a simple spectral characterization of correlation immune Boolean functions. Algebraic attack [1, 7, 8] was introduced by Meier et al.[7, 14]. It is more proper to speak that algebraic attack was improved by them, since the idea of algebraic attacks comes from Shannon. Consequently, a high algebraic immunity[14] for Boolean functions is needed due to the standard algebraic attacks.

The interaction of these properties is so complex that some are contrary to others to some extend. So it is very difficult to find functions achieving all the necessary criteria. There are several constructions of Boolean functions with optimum algebraic immunity, see [3, 4, 5, 11, 16, 17]. A class of 1-resilient Boolean functions with optimal algebraic immunity was obtained in [4]. However, The nonlinearity of most of the constructed Boolean functions are often not exceeding $2^{n-1} - \left(\begin{array}{c} n-1 \\ \lfloor \frac{n}{2} \rfloor \end{array} \right)$, which is insufficient. There are other that are not satisfied for Boolean functions satisfying some properties. In 2008, Carlet and Feng proposed in [6] an infinite excellent class of balanced functions with optimum algebraic immunity as well as very high nonlinearity. It is the first that the constructed Boolean functions have optimal nonlinearity among all known constructions of Boolean functions with optimal algebraic immunity and meet most of the cryptographic necessities. Very recently, Tu and Deng proposed in [23] two classes of algebraic immunity optimal functions of even variables based on a combinatoric conjecture. The nonlinearity of these functions is even better than functions in [6]. Some constructions in [19, 20] is on 1-resilient Boolean functions with optimal algebraic immunity. Balanced Boolean functions, which have maximum algebraic degree, high nonlinearity and are 1-resilient, were proposed by Tu and Deng in [24] through a modification to Boolean functions in [23]. Based on the combinatoric conjecture in [23], their functions are at least of suboptimal algebraic immunity. Tang D., Carlet C. and Tang X. proposed in [21] a class of Boolean functions, which have high nonlinearity and optimal algebraic immunity under a new combinatorial conjecture similar to the combinatoric conjecture in [23]. The authors generalized Boolean functions in [21, 23] and put forward two classes of more general Boolean functions with optimal algebraic immunity in [13] under the assumption that a general combinatorial conjecture[9, 21] is true.

In the present paper, we will modify Boolean functions in [13] to a new class of $2k$-variable Boolean functions. In fact, this class of functions are the generalization of functions in [24] and have optimal algebraic degree, high nonlinearity, and are 1-resilient. These functions have optimal algebraic immunity when $k > 2$ and $u = -2^l, 0 \leq l < k$. Based on the general combinatorial conjecture, algebraic immunity of these functions is optimal when $k > 2$ and $u = 2^l$, $0 \le l < k$. If the general combinatorial conjecture and a new assumption are true, algebraic immunity of our functions is also optimal when $k > 2, u \neq \pm 2^l$, $0 \le l < k$.

The rest of the paper is organized as follows. In Section 2, we recall the necessary background knowledge of Boolean functions. In Section 3, we propose our construction of a new class of Boolean functions. In Section 4, we discuss the 1-resilience, the algebraic degree and the nonlinearity of the constructed Boolean functions. In Section 5, we see the algebraic immunity of these Boolean functions. In Section 6, we give a similar construction of Boolean functions whose properties are the same as Boolean function defined in Section 3.

2 Preliminaries

Let $n \ge 2$ be a positive integer. A Boolean function on n variables

$$f = f(x) = f(x_1, \cdots, x_n) : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$$

where $\mathbb{F}_2$ denotes the finite field with two elements. We denote $\mathcal{B}_n$ the set of all n-variable Boolean functions. Any Boolean function has a unique representation as a multivariate polynomial over $\mathbb{F}_2$, called the *algebraic normal form*(ANF), of the special form

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

The *algebraic degree* of $f \neq 0$, $deg(f)$, is defined as

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

A Boolean function is affine if it has degree at most 1. The set of all affine functions is denoted by A_n. The *Hamming weight* of f, $wt(f)$, is the size of the support $supp(f) = \{\, x \in \mathbb{F}_2^n \,|\, f(x) = 1\,\}$. A Boolean function $f \in \mathcal{B}_n$ is called balanced if $|zero(f)| = |supp(f)| = 2^{n-1}$, where $zero(f) = \{\, x \in \mathbb{F}_2^n \,|\, f(x) = 0\,\}$.

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

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

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

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. $d_H(f, g) = |\{\, x \in \mathbb{F}_2^n \,|\, f(x) + g(x) = 1 \,\}|$. 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 $\mathbf{x} = (x_1, x_2, \cdots, x_n)$ and $\mathbf{a} = (a_1, a_2, \cdots, a_n)$ both belong to $\mathbb{F}_2^n$ and $\mathbf{a} \cdot \mathbf{x} = a_1x_1 + a_2x_2 + \cdots + a_nx_n$.

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

is called the Walsh spectrum of f at $\mathbf{a}$. If $W_f(\mathbf{a}) = 0$ for all $\mathbf{a}$ with $1 \leq wt(\mathbf{a}) \leq m$, f is called m-th order correlation immune. This is the famous Xiao-Massey[25] characterization of correlation immune functions. Moreover, if f is also balanced, we call f m-th order resilient.

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

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

where tr is the trace function from $\mathbb{F}_{2^n}$ onto $\mathbb{F}_2$, which is defined as

$$tr(\alpha) = \sum_{i=0}^{n-1} \alpha^{2^i}, \ \alpha \in \mathbb{F}_{2^n}.$$

For $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \longrightarrow \mathbb{F}_2$, the Walsh spectrum of f at $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ is defined by

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

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

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

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

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

When n is even, the upper bound can be attained, and these Boolean functions are called bent.

Definition 2.1 *[14] The algebraic immunity $AI_n(f)$ of an n-variable Boolean function $f \in \mathcal{B}_n$ is defined to be the lowest degree of nonzero functions g such that $f \cdot g = 0$ or $(f+1) \cdot g = 0$.*

The algebraic immunity, as well as the nonlinearity and degree, is affine invariant. Courtois and Meier[7] showed $AI(f) \leq \lceil \frac{n}{2} \rceil$. In this paper, we refer to the knowledge of BCH code in [15] and finite field in [18].

3 Boolean functions with good cryptographic properties

In this section, we give our construction. In the subsequent sections, we will consider these functions' resiliency, algebraic degree, nonlinearity and algebraic immunity.

Construction 3.1 *Let $n = 2k \geq 4$, $u \in \mathbb{Z}^*_{2^k-1}$. Let α be a primitive element of the finite field $\mathbb{F}_{2^k}$. 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. We define a function $f \in \mathcal{B}_n$, whose support supp(f) consistes of the following four disjoint parts:*

- $\{\ (x,y) \mid xy^{2^k-1-u} \in \Delta_s \setminus \{\alpha^s\}\}$
- $\{\ (x,y) \mid xy^{2^k-1-u} = \alpha^s,\ y \in \mathbb{F}^*_{2^k} \setminus \Delta_s\}$
- $\{\ (\alpha^s x^u, 0) \mid x \in \Delta_s\}$
- $\{\ (0,y) \mid y \in \Delta_s\}$

4 1-resiliency, algebraic degree and nonlinearity of the constructed function

Theorem 4.1 *Let Boolean function f be defined as in Construction 3.1. Then f is 1-resilient.*

Proof: f is balanced since $wt(f)=(2^{k-1}-1)(2^k-1)+(2^{k-1}-1)+2^{k-1}+2^{k-1}=2^{2k-1}$, which implies $W_f(0,0)=0$.

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

$$\begin{aligned}
W_f(a,b) &= \sum_{(x,y)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} (-1)^{f(x,y)+tr(ax+by)}\\
&= \sum_{(x,y)\in zero(f)} (-1)^{tr(ax+by)} - \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)}\\
&= -2\sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)}\\
&= -2\sum_{i=s+1}^{2^{k-1}+s-1}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr(a\alpha^i y^u+by)} - 2\sum_{y\in\mathbb{F}_{2^k}^*\setminus\Delta_s}(-1)^{tr(a\alpha^s y^u+by)}\\
&\quad -2\sum_{x\in\Delta_s}(-1)^{tr(a\alpha^s x^u)} - 2\sum_{y\in\Delta_s}(-1)^{tr(by)}.
\end{aligned}$$

Case 1. $a\neq 0$, $b=0$, then

$$\begin{aligned}
W_f(a,0) &= -2\sum_{i=s+1}^{2^{k-1}+s-1}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr(a\alpha^i y^u)} - 2\sum_{y\in\mathbb{F}_{2^k}^*\setminus\Delta_s}(-1)^{tr(a\alpha^s y^u)}\\
&\quad -2\sum_{x\in\Delta_s}(-1)^{tr(a\alpha^s x^u)} - 2\sum_{y\in\Delta_s}(-1)^{tr(0)}\\
&= -2\sum_{i=s+1}^{2^{k-1}+s-1}\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr(a\alpha^i y^u)} - 2\sum_{y\in\mathbb{F}_{2^k}^*}(-1)^{tr(a\alpha^s y^u)} - 2^k\\
&= -2(2^{k-1}-1)(-1)+2-2^k=0.
\end{aligned}$$

Case 2. $b \neq 0$, $a = 0$, then

$$\begin{aligned} W_f(0,b) = -2 \sum_{i=s+1}^{2^{k-1}+s-1} \sum_{y \in \mathbb{F}^*_{2^k}} (-1)^{tr(by)} - 2 \sum_{y \in \mathbb{F}^*_{2^k} \setminus \Delta_s} (-1)^{tr(by)} \\ -2 \sum_{x \in \Delta_s} (-1)^{tr(0)} - 2 \sum_{y \in \Delta_s} (-1)^{tr(by)} \\ = -2 \sum_{i=s+1}^{2^{k-1}+s-1} \sum_{y \in \mathbb{F}^*_{2^k}} (-1)^{tr(by)} - 2 \sum_{y \in \mathbb{F}^*_{2^k}} (-1)^{tr(by)} - 2^k \\ = -2(2^{k-1}-1)(-1) + 2 - 2^k = 0. \end{aligned}$$

From the above discussion, $W_f(a,b) = 0$ for $ab = 0$ and $(a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. Therefore f is 1-resilient.

Theorem 4.2 *Let Boolean function f be defined as in Construction 3.1. Then $deg(f) = n-2$.*

Proof: Let $g, h \in \mathcal{B}_n$ be two n-variable Boolean functions defined by $supp(g) = \{\,(x,y)\,|\, xy^{2^k-i-u} \in \Delta_s, y \in \mathbb{F}^*_{2^k}\,\}$ and $supp(h) = \{(x,y)|xy^{2^k-1-u} = \alpha^s, y \in \Delta_s\} \cup \{(\alpha^s x^u, 0)|x \in \Delta_s\} \cup \{(0,y)|y \in \Delta_s\}$. For $(x,y) \in \{(x,y)|\mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \setminus \{(x,y)|xy^{2^k-1-u} = \alpha^s, y \in \mathbb{F}^*_{2^k}\}\}$, it is obvious that $f = g+h$. When $(x,y) \in \{(x,y)|xy^{2^k-1-u} = \alpha^s, y \in \mathbb{F}^*_{2^k}\}$, $g(x,y) + h(x,y) = 1+1 = 0 = f(x,y)$ for $xy^{2^k-1-u} = \alpha^s, y \in \Delta_s$ and $g(x,y)+h(x,y) = 1+0 = 1 = f(x,y)$ for $xy^{2^k-1-u} = \alpha^s, y \in \mathbb{F}^*_{2^k} \setminus \Delta_s$. Thus $f = g+h$ for any $(x,y) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$. By Lagrange's interpolation formula, we have

$$h(x,y) = \sum_{i=s}^{2^{k-1}-1+s} ((x+\alpha^s\alpha^{iu})^{2^k-1}+1)((y+\alpha^i)^{2^k-1}+1)$$

$$+ \sum_{i=s}^{2^{k-1}-1+s} ((x+\alpha^s\alpha^{iu})^{2^k-1}+1)(y^{2^k-1}+1) + \sum_{i=s}^{2^{k-1}-1+s} (x^{2^k-1}+1)((y+\alpha^i)^{2^k-1}+1)$$

The coefficient of $x^{2^k-1}y^{2^k-1}$ vanishes.

The coefficient of $x^{2^k-1}y^{2^k-2}$ is

$$\sum_{i=s}^{2^{k-1}+s-1} \alpha^i + \sum_{i=s}^{2^{k-1}+s-1} \alpha^i = 0.$$

The coefficient of $x^{2^k-2}y^{2^k-1}$ is

$$\sum_{i=s}^{2^{k-1}+s-1} \alpha^s\alpha^{iu} + \sum_{i=s}^{2^{k-1}+s-1} \alpha^s\alpha^{iu} = 0.$$

The coefficient of $x^{2^k-2}y^{2^k-2}$ is

$$\sum_{i=s}^{2^{k-1}+s-1} \alpha^s\alpha^{iu}\alpha^i = \sum_{i=s}^{2^{k-1}+s-1} \alpha^s\alpha^{i(u+1)}.$$

Since g has the following representation

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

when the exponent of x is 2^k-2 in g, the exponent of y is 2^k-2 if and only if $u = 2^k-2$. So for $u = 2^k-2$ the coefficient of $x^{2^k-2}y^{2^k-2}$ in g is $\alpha^s(1+\alpha)^{2^{k-1}-1}$, which is not zero. As in this case the coefficient of $x^{2^k-2}y^{2^k-2}$ in h vanishes, the coefficient of $x^{2^k-2}y^{2^k-2}$ in f is not zero.

For $u \neq 2^k-2$, g does not contain $x^{2^k-2}y^{2^k-2}$. The coefficient of $x^{2^k-2}y^{2^k-2}$ in h is

$$\sum_{i=s}^{2^{k-1}+s-1} \alpha^s\alpha^{i(u+1)} = \alpha^{s(u+2)}(1+\alpha^{u+1})^{2^{k-1}-1} \neq 0.$$

Thus the coefficient of $x^{2^k-2}y^{2^k-2}$ in f is not zero.

From the above discussion, $deg(f) = n-2$. □

We know that for 1-resilient Boolean function g, it should be satisfied that $deg(g) \leq n-2$ form Siegenthaler's inequality[22]. So Boolean functions in Construction 3.1 have optimal algebraic degree. Subsequently, we discuss the nonlinearity of the constructed functions.

Lemma 4.3 *[13] Let $k \geq 2$ be a positive integer and α be a primitive element of $\mathbb{F}_{2^k}$. Let $\Delta_s = \{\alpha^s, \cdots, \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k-1$ is an integer. Define*

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

where $(u, 2^k - 1) = 1$. *Then*

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

Lemma 4.4 *[6, 13] Let* $\alpha \in \mathbb{F}_{2^k}^*$ *be a primitive element and* $\lambda \in \mathbb{F}_{2^k}$, *and denote*

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

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

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

Theorem 4.5 *Let* f *be the* n*-variable Boolean function defined by Construction 3.1. Then*

$$\begin{aligned} N_f &\geq 2^{n-1} - \frac{2^{k+1}}{\pi} \ln \frac{4(2^k - 1)}{\pi} - 2^{k-1} - 2\frac{2^{\frac{k}{2}+1}}{\pi} \ln \frac{4(2^k - 1)}{\pi} - 3 \\ &\approx 2^{n-1} - \frac{2 \ln 2}{\pi}(k + \frac{1}{2})2^k - \frac{4 \ln 2}{\pi} k 2^{\frac{k}{2}}. \end{aligned}$$

Proof: By Theorem 4.1, for $ab = 0$, $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $W_f(a, b) = 0$.

For $ab \neq 0,\ a, b \in \mathbb{F}_{2^k}$,

$$\begin{aligned}
-\frac{1}{2}W_f(a,b) &= \sum_{(x,y)\in supp(f)} (-1)^{tr(ax+by)} \\
&= \sum_{i=s+1}^{2^{k-1}-1+s} \sum_{y\in\mathbb{F}^*_{2^k}} (-1)^{tr(a\alpha^i y^u+by)} + \sum_{y\in\mathbb{F}^*_{2^k}\setminus\Delta_s} (-1)^{tr(a\alpha^s y^u+by)} \\
&\quad + \sum_{x\in\Delta_s} (-1)^{tr(a\alpha^s x^u)} + \sum_{y\in\Delta_s} (-1)^{tr(by)} \\
&= \sum_{i=s}^{2^{k-1}-1+s} \sum_{y\in\mathbb{F}^*_{2^k}} (-1)^{tr(a\alpha^i y^u+by)} - \sum_{y\in\Delta_s} (-1)^{tr(a\alpha^s y^u+by)} \\
&\quad + \sum_{x\in\Delta_s} (-1)^{tr(a\alpha^s x^u)} + \sum_{y\in\Delta_s} (-1)^{tr(by)} \\
&= \sum_{i=s'}^{2^{k-1}-1+s'} \sum_{y\in\mathbb{F}^*_{2^k}} (-1)^{tr(\alpha^i y^u+y)} - \sum_{y\in\Delta_s} (-1)^{tr(a\alpha^s y^u+by)} \\
&\quad + \sum_{x\in\Delta_s} (-1)^{tr(a\alpha^s x^u)} + \sum_{y\in\Delta_s} (-1)^{tr(by)} \\
&= \Gamma_{s'} - \sum_{y\in\Delta_s} (-1)^{tr(a\alpha^s y^u+by)} + S_{\alpha^u}(a\alpha^s) + S_\alpha(b)
\end{aligned}$$

where $\sum_{x\in\Delta_s}(-1)^{tr(a\alpha^s x^u)} = \sum_{y\in{\Delta_s}'}(-1)^{tr(a\alpha^s y)} = S_{\alpha^u}(a\alpha^s)$ since α^u also is primitive. So we have

$$|-\frac{1}{2}W_f(a,b)| = \frac{1}{2}|W_f(a,b)| \leq |\Gamma_{s'}| + |\sum_{y\in\Delta_s}(-1)^{tr(a\alpha^s y^u+by)}| + |S_{a\alpha^s}| + |S_b|.$$

By Lemma 4.3 and Lemma 4.4

$$\frac{1}{2}|W_f(a,b)| \leq 1 + \frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi} + 2^{k-1} + 2(1 + \frac{2^{\frac{k}{2}+1}}{\pi}\ln\frac{4(2^k-1)}{\pi}).$$

So the nonlinearity of f is

$$\begin{aligned}
N_f &= 2^{n-1} - \max_{(a,b)\in\mathbb{F}_{2^k}\times\mathbb{F}_{2^k}} \frac{1}{2}|W_f(a,b)| \\
&\geq 2^{n-1} - \frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi} - 2^{k-1} - 2\frac{2^{\frac{k}{2}+1}}{\pi}\ln\frac{4(2^k-1)}{\pi} - 3 \\
&\approx 2^{n-1} - \frac{2\ln 2}{\pi}k2^k - 2^{k-1} - \frac{4\ln 2}{\pi}k2^{\frac{k}{2}} \\
&= 2^{n-1} - \frac{2\ln 2}{\pi}(k+\frac{1}{2})2^k - \frac{4\ln 2}{\pi}k2^{\frac{k}{2}}.
\end{aligned}$$

□

5 Algebraic immunity of the constructed Boolean function

In this section, we consider the algebraic immunity of the constructed functions. The binary expansion of the integer x is $x = x_0 + x_1 2 + \cdots + x_{n-1}2^{n-1}$, $\overline{x} = (x_0, x_1, \cdots, x_{n-1})$, $wt(x) := wt(\overline{x})$, where $wt(\overline{x}) = x_0 + x_1 + \cdots + x_{n-1}$.

Definition 5.1 *For* $0 \leq a \leq 2^k - 2$, $-a := 2^k - 1 - a$, *and* $wt(-a) := wt(2^k - 1 - a) = k - wt(a)$.

Conjecture 5.2 *[23] Let* $k \leq 2$ *be an integer. For any* $0 \leq t < 2^k - 1$. *Define*

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

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

Tu and Deng [23] could validate this conjecture when $k \leq 29$. In [10, 12], the authors proved it is true for many cases of t. Tang et al. in [21] presented a new combinatorial conjecture similar to Conjecture 5.2 as follows

Conjecture 5.3 *[21] Let* $k \leq 2$ *be an integer. For any* $0 \leq t < 2^k - 1$, *define*

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

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

This conjecture has been proved in [9]. The authors also referred to the following conjecture in [21].

Conjecture 5.4 *Let $k \leq 2$ be a integer and $u \in \mathbb{Z}^*_{2^k-1}$. For any $0 \leq t < 2^k - 1$, define*

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

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

For $2 \leq k \leq 15$, this general conjecture was checked in [21]. This general conjecture is Conjecture 5.2 when $u = 1$ and Conjecture 5.3 when $u = -1$.

Lemma 5.5 *[9] Let $S_{k,t,u}$ be defined as above. Then it satisfies the following properties*

i) $|S_{k,t,u}| = |\{\, a \,|\, 0 \leq a \leq 2^k - 2, wt(a) + wt(t - ua) \leq k - 1\}|$
ii) $|S_{k,t,u}| = |S_{k,2t,u}|$
iii) $|S_{k,t,u}| = |S_{k,t,2u}|$
iv) $|S_{k,t,u}| = |S_{k,u^{-1}t,u^{-1}}|$

Lemma 5.6 *Let $k \leq 2$ be a integer and $u \in \mathbb{Z}^*_{2^k-1}$. Set $\Delta_{k,t,u} = \{\, (a,b) \,|\, 0 \leq a, b < 2^k - 1, ua+b \equiv t(\bmod 2^k-1), wt(a)+wt(b) = k\}$ satisfies the following properties*

i) $|\Delta_{k,t,u}| = |\{\, a \,|\, 0 \leq a \leq 2^k - 2, wt(a) + wt(t - ua) = k\}|$
ii) $|\Delta_{k,t,u}| = |\Delta_{k,2t,u}|$
iii) $|\Delta_{k,t,u}| = |\Delta_{k,t,2u}|$
iv) $|\Delta_{k,t,u}| = |\Delta_{k,u^{-1}t,u^{-1}}|$
v) $|\Delta_{k,t,u}| = |\Delta_{k,-t,u}|$

Proof: Similar to the proof of Lemma 5.5 in [9], $i), ii), iii)$ and $iv)$ can be deduced. $(a,b) \in \Delta_{k,t,u}$, i.e. $0 \leq a, b < 2^k - 1, ua + b = t, wt(a) + wt(b) = k$ if and only if $0 \leq a, b < 2^k - 1, u(-a) + (-b) = -t, wt(-a) + wt(-b) = k - wt(a) + k - wt(b) = 2k - k = k$ if and only if $(a,b) \in \Delta_{k,-t,u}$. Hence we have $|\Delta_{k,t,u}| = |\Delta_{k,-t,u}|$. □

Lemma 5.7 *With the above notation, $S_{k,t,u}$ and $S_{k,-t,u}$ satisfy*

$$|S_{k,t,u}| + |S_{k,-t,u}| = 2^k + 1 - |\Delta_{k,t,u}|.$$

Proof: It is obvious that $|S_{k,t,u}| = |\{\, a \in \mathbb{Z}_{2^k-1} \,|\, wt(a) + wt(t-ua) \leq k-1\}|$. Since $wt(0)+wt(t) \leq k-1$ and $wt(u^{-1}t)+wt(0) \leq k-1$, we have $\{0, u^{-1}t\} \subset \{\, a \,|\, 0 \leq a \leq 2^k-2, wt(a)+wt(a-t) \leq k-1\}$.

For $a \neq 0, u^{-1}t$, we have

$$\begin{aligned} wt(a)+wt(t-ua) &= wt(a)+wt(-(-t+ua)) \\ &= k - wt(-a) + k - wt(-t+ua) \\ &= 2k - (wt(-a)+wt(-t+ua)). \end{aligned}$$

The map $\varphi : \mathbb{Z}_{2^k-1} \longrightarrow \mathbb{Z}_{2^k-1}$, $\varphi(a) = -a$ is a permutation of $\mathbb{Z}_{2^k-1}$. Then

$$\begin{aligned} |S_{k,t,u}| &= 2 + |\{\, a \,|\, 0 < a \leq 2^k-2, a \neq u^{-1}t, wt(a)+wt(t-ua) \leq k-1\}| \\ &= 2 + |\{a|0 < a \leq 2^k-2, a \neq t, wt(-a)+wt(-t+ua) \geq k+1\}| \\ &= 2 + |\{a|0 \leq a \leq 2^k-2, wt(-a)+wt(-t+ua) \geq k+1\}| \\ &= 2 + |\{a|0 \leq a \leq 2^k-2, wt(a)+wt((-t-ua)) \geq k+1\}| \\ &= 2 + (2^k-1 - |\{a|0 \leq a \leq 2^k-2, wt(a)+wt(-t-ua) \leq k\}| \\ &= 2^k+1 - |\{a|0 \leq a \leq 2^k-2, wt(a)+wt((-t-ua)) \leq k-1\}| \\ &\quad -|\{a|0 \leq a \leq 2^k-2, wt(a)+wt(-t-ua) = k\}| \\ &= 2^k+1-|S_{k,-t,u}|-|\Delta_{k,-t,u}|. \end{aligned}$$

Hence, by Lemma 5.6 v), we have

$$|S_{k,t,u}| + |S_{k,-t,u}| = 2^k+1-|\Delta_{k,t,u}|.$$

□

Assumption 5.8 *With the notation of Conjecture 5.4. Set $T_{k,u} = \{\, t \,|\, 0 \leq t \leq 2^k-2, |S_{k,t,u}| = 2^{k-1}\}$. Then $|T_{k,u}| < 2^{k-1}$ for $k > 2$.*

Remark 5.9 *Assumption 5.8 is the generalization of the assumption in [24]. Subsequently, we will prove this assumption is valid for $u = -2^l, 0 \leq l < k$. Moreover, if Conjecture 5.4 is correct, we can show this assumption is true for $u = 2^l, 0 \leq l < k$ and check this assumption when $2 < k < 20$ besides $u = \pm 2^l, 0 \leq l < k$.*

Theorem 5.10 *Let $k > 2$ be an integer and $n = 2k$, $u \in \mathbb{Z}^*_{2^k-1}$. Assume Conjecture 5.4 and Assumption 5.8 are correct. Then the Boolean function f defined in Construction 3.1 has optimal algebraic immunity, i.e. $AI(f) = k$.*

Proof: We need to prove that both f and $f+1$ have no annihilators with algebraic degrees less than k.

Let a nonzero Boolean function $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \longrightarrow \mathbb{F}_2$ satisfy $deg(h) < k$ and $f \cdot h = 0$. We will prove $h = 0$. Boolean function h can be written as

$$h(x, y) = \sum_{i=0}^{2^k-1} \sum_{j=0}^{2^k-1} h_{i,j} x^i y^j,$$

where $h_{i,j} \in \mathbb{F}_{2^k}$. By $deg(h) < k$, we have $h_{i,j} = 0$ if $wt(i) + wt(j) \geq k$, which implies $h_{2^k-1,i} = h_{j,2^k-1} = 0$ for all $0 \leq i, j \leq 2^k - 1$. $\{(\gamma y^u, y) | y \in \mathbb{F}_{2^k}^*, \gamma \in \Delta_s \setminus \{\alpha^s\}\} \cup \{(0, y) | y \in \Delta_s\} \subset supp(f)$. By $f \cdot h = 0$, then $h(\gamma y^u, y) = 0$ for all $y \in \mathbb{F}_{2^k}^*$, $\gamma \in \Delta_s \setminus \{\alpha^s\}$.

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

can be written as

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

where

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

Note that $\{t - ui (\bmod 2^k-1) | 0 \leq i < 2^k-1\} = \mathbb{Z}_{2^k-1}$ due to $(u, 2^k-1) = 1$. For any $\gamma \in \Delta_s \setminus \{\alpha^s\}$, $h(\gamma y^u, y) = 0$ for $y \in \mathbb{F}_{2^k}^*$, it follows that

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

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

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

is a codeword in some BCH code of length 2^k-1 over $\mathbb{F}_{2^k}$, having the elements in $\Delta_s \setminus \{\alpha^s\}$ as zeros and the designed distance 2^{k-1}. If this codeword is nonzero, its Hamming weight should be greater than or equal to 2^{k-1}. Set $T_1 = \{t|0 \leq t \leq 2^k-2, |S_{k,t,u}| < 2^{k-1}\}$ and $T_2 = \{t|0 \leq t \leq 2^k-2, |S_{k,t,u}| = 2^{k-1}\}$. For $t \in T_1$, since $S_{k,t,u} < 2^{k-1}$, we have $h_t = 0$.

Since $h(0,y) = 0$ for $y \in \Delta_s$, i.e.

$$h(0,y) = \sum_{j=0}^{2^k-2} h_{0,j}y^j = 0, \text{for } y \in \Delta_s$$

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

$$(h_{0,0}, h_{0,1}, h_{0,2}, \cdots, h_{0,2^k-2})$$

is a codeword in some BCH code of length 2^k-1 over $\mathbb{F}_{2^k}$, having the elements in Δ_s as zeros and the designed distance $2^{k-1}+1$. Since $t \in T_1$, $h_t = 0$, $h_{0,t} = 0$. By Corollary 5.12, $|T_2| < 2^{k-1}$, so $|T_1| \geq 2^{k-1}$, i.e. the number of nonzero in $(h_{0,0}, h_{0,1}, h_{0,2}, \cdots, h_{0,2^k-2})$ is at most $2^{k-1}-1$. This contradicts, So $h_{0,0} = h_{0,1} = h_{0,2} = \cdots = h_{0,2^k-2} = 0$.

For $t \in T_2$, the Hamming weight of the vector h_t at least 2^k. However, by Conjecture 5.4 and $h_{0,t} = 0$, this vector' Hamming weight at most $2^{k-1}-1$. This contradicts, hence $h_t = 0$

Finally, we have $h_t = 0$ for all $0 \leq t \leq 2^k-2$.

Since

$$\{(\gamma y^u, y)|y \in \mathbb{F}_{2^k}^*, \gamma \in \mathbb{F}_{2^k}^* \setminus \Delta_s\} \cup \{(0,y)|y \in \mathbb{F}_{2^k}^* \setminus \Delta_s\} \subset supp(f+1),$$

a similar argument is applicable to $f+1$, it can be proved that $f+1$ has no annihilator of degree less than k.

Therefore, we have $AI(f) = k$. □

5.1 When $u = 2^l$

Lemma 5.11 *Let $k > 2$ be an integer. Assume that Conjecture 5.2 is true. Set $T_{k,+} = \{t|0 \leq t \leq 2^k-2, |S_{k,t,+}| = 2^{k-1}\}$. Then $|T_{k,+}| < 2^{k-1}$.*

Proof: It is obvious that $|\Delta_{k,t,+}| = |\Delta_{k,2t,+}|$ since $(a,b) \in \Delta_{k,t,+}$ if and only if $(2a,2b) \in \Delta_{k,2t,+}$. Since $|\Delta_{k,t,+}| = |\Delta_{k,2t,+}|$, without loss of generality we suppose that t has the following form

$$t = \underbrace{11\cdots1}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{11\cdots1}_{n_3}\underbrace{00\cdots0}_{n_4}\cdots\underbrace{11\cdots1}_{n_{2r-1}}\underbrace{00\cdots0}_{n_{2r}}$$

We construct A as follows:

$$A = \underbrace{0\cdots01}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{0\cdots01}_{n_3}\underbrace{00\cdots0}_{n_4}\cdots\underbrace{0\cdots01}_{n_{2r-1}}\underbrace{00\cdots0}_{n_{2r}}$$

It is obtained:

$$t + A = \underbrace{00\cdots0}_{n_1}\underbrace{0\cdots01}_{n_2}\underbrace{00\cdots0}_{n_3}\underbrace{0\cdots01}_{n_4}\cdots\underbrace{00\cdots0}_{n_{2r-1}}\underbrace{0\cdots01}_{n_{2r}}$$

Consequently, $wt(A) = wt(t + A)$. By $wt(A) + wt(2^k - 1 - A) = k$, we have

$$(t + A) + (2^k - 1 - A) \equiv t(\mathrm{mod}2^k - 1)\,\mathrm{and}\,wt(t + A) + wt(2^k - 1 - A) = k$$

That is $(t + A, 2^k - 1 - A) \in \Delta_{k,t,+}$. If $t + A \neq 2^k - 1 - A$, then it also is true that $(2^k - 1 - A, t + A) \in \Delta_{k,t,+}$.

If $t + A = 2^k - 1 - A$, i.e. $t \equiv -2A$, then $(2t + 2A, 2(2^k - 1) - 2A) \equiv (t, t) \in \Delta_{k,2t,+}$, which implies $(\frac{t}{2}, \frac{t}{2}) \in \Delta_{k,t,+}$. In this case, t has the following form:

$$t = 101010\cdots1010$$

We construct (a, b) as

$$a = \underbrace{0101\cdots01}_{k-6}000111$$

$$b = \underbrace{0101\cdots01}_{k-6}100011$$

Obviously, $a + b \equiv t, wt(a) + wt(b) = k$, so $(a, b) \neq (\frac{t}{2}, \frac{t}{2})$, $(a, b) \in \Delta_{k,t,+}$

Therefore $|\Delta_{k,t,+}| \geq 2$ for $1 \leq t \leq 2^k - 2, k > 2, k \neq 4$

By Lemma 5.7 $S_{k,t,+}$ and $S_{k,-t,+}$ satisfies the following equation

$$|S_{k,t,+}| + |S_{k,-t,+}| = 2^k + 1 - |\Delta_{k,t,+}|,$$

So we have, for $1 \leq t \leq 2^k - 2, k > 2, k \neq 4$

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

If Conjecture 5.2 is correct, then either $|S_{k,t,+}| < 2^{k-1}$ or $|S_{k,-t,+}| < 2^{k-1}$ is true. It is trivial that $|S_{k,0,+}| < 2^{k-1}$. So $|T_{k,+}| = |\{t|0 \leq t \leq 2^k-2,\ |S_{k,t,+}| = 2^{k-1}\}| \leq 2^{k-1} - 1 < 2^{k-1}$ for $k > 2,\ k \neq 4$.

When $k = 4$, through our computation, it is true $|\{\,t\,|\,0 \leq t \leq 2^k - 2, |S_{k,t,+}| = 2^{k-1}\}| < 2^{k-1}$.

At last, $|T_{k,+}| < 2^{k-1}$ for any $k > 2$ if Conjecture 5.2 is true.

Corollary 5.12 *Let $k > 2$ be an integer and $u = 2^l, 0 \leq l < k$, Set $T_{k,u} = \{t|0 \leq t \leq 2^k - 2, |S_{k,t,u}| = 2^{k-1}\}$. Then $|T_{k,u}| < 2^{k-1}$.*

Proof: Since $u = 2^l, 0 \leq l < k$, $(a,b) \in S_{k,t,+}$ if and only if $(u^{-1}a, b) \in S_{k,t,u}$. We have $|S_{k,t,+}| = |S_{k,t,u}|$. Hence $|T_{k,u}| = |\{t|0 \leq t \leq 2^k - 2, |S_{k,t,u}| = 2^{k-1}\}| = |\{t|0 \leq t \leq 2^k - 2, |S_{k,t,+}| = 2^{k-1}| = |T_{k,+}| < 2^{k-1}$. □

Theorem 5.13 *Let $k > 2$ be an integer and $n = 2k$, $u = 2^l, 0 \leq l < k$. Assume Conjecture 5.4 is correct. Then the Boolean function f defined in Construction 3.1 has optimal algebraic immunity, i.e. $AI(f) = k$.*

Proof: If Conjecture 5.4 is correct, by Theorem 5.10 and Corollary 5.12, it can be obtained immediately. □

5.2 When $u = -2^l$

Lemma 5.14 *For $k > 2, 0 < t \leq 2^k - 2$, let $\Delta_{k,t,-} = \{(a,b)|0 \leq a,b \leq 2^k - 2, a - b \equiv t(\text{mod}2^k - 1), wt(a) + wt(b) = k\}$. Then $|\Delta_{k,t,-}| \geq 2$*

Proof: Since $(a,b) \in \Delta_{k,t,-}$ if and only if $(2a, 2b) \in \Delta_{k,2t,-}$, $|\Delta_{k,t,-}| = |\Delta_{k,2t,-}|$. If $t \neq 0$, without loss of generality we suppose that t has the following form:

$$t = \underbrace{11\cdots1}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{11\cdots1}_{n_3}\underbrace{00\cdots0}_{n_4}\cdots\underbrace{11\cdots1}_{n_{2r-1}}\underbrace{00\cdots0}_{n_{2r}}$$

It is obvious that $(t, -t) \in \Delta_{k,2t,-}$, $-t$ have the following form respectively

$$-t = \underbrace{00\cdots0}_{n_1}\underbrace{11\cdots1}_{n_2}\underbrace{00\cdots0}_{n_3}\underbrace{11\cdots1}_{n_4}\cdots\underbrace{00\cdots0}_{n_{2r-1}}\underbrace{11\cdots1}_{n_{2r}}$$

If $n_i \geq 2$ for some $1 \leq i \leq 2r$, without loss of generality we suppose $n_1 \geq 2$, take

$$a = \underbrace{010\cdots0}_{n_1}\underbrace{00\cdots0}_{n_2}\underbrace{00\cdots0}_{n_3}\underbrace{00\cdots0}_{n_4}\cdots\underbrace{00\cdots0}_{n_{2r-1}}\underbrace{00\cdots0}_{n_{2r}}$$

then

$$\begin{aligned} t + a &= \overbrace{001\cdots1}^{n_1}\overbrace{10\cdots0}^{n_2}\overbrace{11\cdots1}^{n_3}\overbrace{00\cdots0}^{n_4}\cdots\overbrace{11\cdots1}^{n_{2r-1}}\overbrace{00\cdots01}^{n_{2r}} \\ -t + a &= \underbrace{010\cdots0}_{n_1}\underbrace{11\cdots1}_{n_2}\underbrace{00\cdots0}_{n_3}\underbrace{11\cdots1}_{n_4}\cdots\underbrace{00\cdots0}_{n_{2r-1}}\underbrace{11\cdots11}_{n_{2r}} \end{aligned}$$

So we have $(t+a)-(-t+a)=2t, wt(t+a)+wt(-t+a)=k$, that is to say $(t+a,-t+a)\in\Delta_{k,2t,-}$.

If $n_i=1$ for all $1\le i\le 2r$,

$$\begin{aligned} t &= 1010\,\overbrace{1010\cdots10}^{k-4} \\ -t &= 0101\,\underbrace{0101\cdots01}_{k-4} \end{aligned}$$

We take

$$a = 0011\,\underbrace{00\cdots0}_{k-4}$$

then

$$\begin{aligned} t+a &= 1101\,\overbrace{1010\cdots10}^{k-4} \\ -t+a &= 1000\,\underbrace{0101\cdots01}_{k-4} \end{aligned}$$

It is attained that $(t+a,-t+a)\ne(t,-t)$, $(t+a,-t+a)\in\Delta_{k,t,-}$.

Therefore $|\Delta_{k,t,-}|\ge 2$ for $k>2, 0<t\le 2^k-2$. □

Proposition 5.15 *Let $k>2$ be an integer. For any $0<t\le 2^k-2$, define*

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

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

Proof: By Lemma 5.7, $S_{k,t,-}$ and $S_{k,-t,-}$ satisfy

$$|S_{k,t,-}|+|S_{k,-t,-}|=2^k+1-|\Delta_{k,t,-}|.$$

$|S_{k,t,-}|=|S_{k,-t,-}|$ since Lemma 5.5 *iv*), we have

$$2|S_{k,t,-}|=2^k+1-|\Delta_{k,t,-}|.$$

Since $|\Delta_{k,t,-}|\ge 2,$ for $k>2, 0<t\le 2^k-2$ by Lemma 5.14, we can get

$$|S_{k,t,-}|<2^{k-1}, \quad \text{for } k>2, 0<t\le 2^k-2$$

□

Corollary 5.16 *Let $u = -2^l, 0 \leq l < k$. Then $|S_{k,t,u}| < 2^{k-1}$ for $k > 2, 0 < t \leq 2^k - 2$.*

Proof: By Lemma 5.5 *iii*), we can get $|S_{k,t,-}| = |S_{k,t,-2^l}|$, $0 \leq l < k$. Since Proposition 5.15, the conclusion can be obtained immediately.

Theorem 5.17 *Let $k > 2$ be an integer, $n = 2k$, $u = -2^l, 0 \leq l < k$. Then the Boolean function f defined in Construction 3.1 has optimal algebraic immunity, i.e. $AI(f) = k$.*

Proof: By Corollary 5.16, it is obvious that $T_{k,u} < 2^{k-1}$. It can be obtained by Theorem 5.10 and Corollary 5.12. □

6 Conclusion

In this paper, a class of $2k$-variable Boolean functions are constructed, and this class of functions have optimal algebraic degree, high nonlinearity, and are 1-resilient. Algebraic immunity of our functions is optimal when $k > 2$ and $u = -2^l, 0 \leq l < k$. Based on Conjecture 5.4[9, 21], algebraic immunity of our functions is optimal when $k > 2$ and $u = 2^l, 0 \leq l < k$. What's more, if Conjecture 5.4[9, 21] and Assumption 5.8 are true, algebraic immunity of our functions is also optimal when $k > 2, u \neq \pm 2^l, 0 \leq l < k$.

Similar to Construction 3.1, we propose

Construction 6.1 *Let $n = 2k \geq 4$, $u \in \mathbb{Z}^*_{2^k-1}$. Let α be a primitive element of the finite field $\mathbb{F}_{2^k}$. 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 function $f \in \mathcal{B}_n$, whose support supp(f) consistes of the following four disjoint parts:*

- $\{\ (x, y) \mid xy^{2^k-1-u} \in \Delta_s \setminus \{\alpha^{2^{k-1}-1+s}\}\}$
- $\{\ (x, y) \mid xy^{2^k-1-u} = \alpha^{2^{k-1}-1+s},\ y \in \mathbb{F}^*_{2^k} \setminus \Delta_s\}$
- $\{\ (\alpha^{2^{k-1}-1+s}x^u, 0) \mid x \in \Delta_s\}$
- $\{\ (0, y) \mid y \in \Delta_s\}$

All conclusions in this paper are true for Boolean functions defined by Construction 6.1.

References

[1] Armkneckt F.: Improving fast algebraic attacks, 11th International Workshop on Fast Software Encryption, FSE 2004. Lecture Notes in Computer Science, vol.3017, pp. 65-82(2004).

[2] Carlet C.: The momography Boolean Methods and Models, In *Boolean functions for Cryptography and Error Correcting Codes*. Y. Crama and P. Hammer, Eds, Cambridge University Press, Cambridge.

[3] Carlet C.: A method of construction of balanced functions with optimum algebraic immunity, Cryptology ePrint Archive, http://eprint.iacr.org/2006/149.

[4] Carlet C., Dalai D. K., Gupta K. C., Maitra S.: Algebraic immunity for cryptographically significant Boolean functions: analysis and construction, IEEE Trans. Inform. Theory, vol. 52, pp. 3105-3121(2006).

[5] Carlet C., Zeng X., Li C., Hu L.: Further properties of several classes of Boolean functions with optimum algebraic immunity, Des. Codes Cryptogr., vol. 52, pp. 303-338(2009).

[6] Carlet C., Feng K.: An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonliearity, Advances in Cryptology, Asiacrypt 2008, Lecture Notes in Computer Science, vol. 5350, pp. 425-440(2008).

[7] Courtois N., Meier W.: Algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology-EUROCRYPT 2003, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, vol. 2656, pp. 345-359(2003).

[8] Courtois N.T.: Fast algebraic attacks on stream ciphers with linear feedback, Advances in Cryptology, Crypto 2003. Lecture Notes in Computer Science, vol. 2729, pp. 176-194(2003).

[9] Cohen G., Flori J. P.: On a generalized combinatorial conjecture involving addition mod $2^k - 1$, Cryptology ePrint Archive, http://eprint.iacr.org/2011/400.

[10] Cusick T. W., Li Y., Stanica P.: On a conbinatoric conjecture, Cryptology ePrint Archive, Report 2009/554, 209, http://eprint.iacr.org/2009/554.

[11] Dalai D.K., Maitra S., Sarkar S.: Basic theory in construction of Boolean functions with maximum possible annihilator immunity, Des. Codes Crytogr., vol. 40, pp. 41-58(2006).

[12] Flori J. P., Randriambololona H., Cohen G., Mesnager S.: On a conjecture about binary strings distribution, Cryptology ePrint Archive, Report 2010/170, 2010, http://eprint.iacr.org/2010/170.

[13] Jin Q., Liu Z., Wu B, Zhang X.: A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity, Cryptology ePrint Archive, http://eprint.iacr.org/2011/515.

[14] Meier W., Pasalic E., Carlet C.: Algebraic attacks and decomposition of Boolean functions, Advances inCryptology-EUROCRYPT 2004, ser. Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, vol. 3027, pp. 474-491(2004).

[15] MacWilliams F. J., Sloane N. J. A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam(1977).

[16] Li N., Qi W.: Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity, in Advances in Cryptology-ASIACRYPT 2006, ser. Lecture Notes in computer Science. Berlin, Germany: Springer-Verlag, vol.4284, pp. 84-98(2006).

[17] Li N., Qu L., Qi W., Feng G., Li C., Xie D.: On the construction of Boolean functions with optimal algebraic immunity, IEEE Trans. Inform. Theory, vol. 54, pp. 1330-1334(2008).

[18] Lidl R., Niederreiter H.: Finite Fields, Cambridge University Press, Second edition(1997).

[19] Pan S., Fu X., Zhang W.: Construction of 1-Resilient Boolean Functions with Optimal Algebraic Immunity and Good Nonlinearity, Journal of Computer Science and Technology, vol. 26(2), pp. 269-275(2011).

[20] Su W., Zeng X., Hu L.: Construction of 1-resilient Boolean functions with optimum algebraic immunity, International Journal of Computer Mathematics, vol. 88(2), pp. 222-238(2011).

[21] Tang D., Carlet C., Tang X.: highly nonlinear boolean functions with optimum algebraic immunity and good behavior against fast algebraic attacks, Cryptology ePrint Archive, http://eprint.iacr.org/2011/366.

[22] Siegenthaler T.: Correlation-immunity of nonlinear combining functions for cryptographic applications. IEEE Trans. Inform. Theory, vol. 30, pp. 776-780(1984).

[23] Tu Z., Deng Y.: A conjecture about binary strings and its applications on constructing Boolean functions with optimal algebraic immunity. Des. Codes Cryptogr., vol.60, pp.1-14(2011).

[24] Tu Z., Deng Y.: Boolean functions with all main cryptographic properties, Cryptology ePrint Archive, http://eprint.iacr.org/2010/518.

[25] Xiao G., Massey J.: A spectral characterization of correlation immune combining functions. IEEE Trans. Inform. Theory, vol. 34, pp. 569-571(1988).