A general conjecture similar to T-D conjecture and its applications in constructing Boolean functions with optimal algebraic immunity

Qingfang Jin Zhuojun Liu Baofeng Wu
Xiaoming Zhang
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 two classes of $2k$-variable Boolean functions, which have optimal algebraic immunity under the assumption that a general combinatorial conjecture is correct. These functions also have high algebraic degree and high nonlinearity. One class contain more bent functions, and the other class are balanced.

Keywords Boolean function · Algebraic immunity · Bent function · Balancedness · Nonlinearity · Algebraic degree

1 Introduction

Boolean functions, which are used in the combiner and filter models of stream ciphers and for S-box designing in block ciphers, play an critical role in symmetric cryptographic systems. To resist known attacks, Boolean functions are generally required to be balanced and have high algebraic degree, high nonlinearity, high correlation immunity and high algebraic immunity[2]. Algebraic immunity, as a response to algebraic attack [1, 8, 9], was proposed by Meier et al.[8, 15].

It is a difficult challenge to find functions achieving all the necessary criteria. There are several constructions of Boolean functions with optimum algebraic immunity, for example, see[3, 4, 5, 12, 17, 18]. However, most of the constructed Boolean functions are improper for cryptographic applications because of less of other good properties such as low algebraic degree or low nonlinearity. 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 are of optimal nonlinearity among all known constructions and meet most of the cryptographic necessities. Very recently, Tu and Deng proposed in [21] a class of algebraic immunity optimal functions of even variables under the assumption of a combinatoric conjecture. The nonlinearity of these functions is even better than functions in [6]. Carlet [7] proved that these functions are well immune to fast algebraic attacks after small modifications. In [22], balanced Boolean functions which have optimal algebraic degree, high nonlinearity, and are 1-resilient, were proposed by Tu and Deng through a modification to Boolean functions in [21]. Based on T-D conjecture [21], their functions are at least algebraic immunity suboptimal. Tang D., Carlet C. and Tang X. proposed in [20] a class of highly nonlinear Boolean functions with optimal algebraic immunity under a new combinatorial conjecture similar to T-D conjecture[21]. These functions also have a good immunity to fast algebraic attacks.

In this paper, T-D functions[21] and functions in [20] are extended to the more general case. Based on a general combinatorial conjecture[10, 20], two classes of $2k$-variable Boolean functions are constructed, both of which have optimal algebraic immunity. The first class contain more bent functions and the second class are balanced. Both classes of Boolean functions have high nonlinearity as well as high algebraic degree.

2 Preliminaries

Let n be a positive integer. A Boolean function of n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$, where $\mathbb{F}_2$ denotes the finite field with two elements. We denote $\mathcal{B}_n$ the set of all n-variable Boolean functions. 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, $wt(f)$, is the size of the support $supp(f) = \{x \in \mathbb{F}_2^n | f(x) = 1\}$. We say that a Boolean function f is balanced if the number of 1's equals 0's 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 $\mathbb{F}_2$, called the *algebraic normal form* (ANF):

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

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 degree at most 1. The set of all affine functions is denoted by A_n.

We identify the field $\mathbb{F}_{2^n}$ with the vector space $\mathbb{F}_2^n$. 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 $a_i^2 = a_{2i(mod 2^n-1)}$. The algebraic degree of f equals $\max\{wt(\bar{i}) | a_i \neq 0, 0 \leq i < 2^n - 1\}$, where $\bar{i}$ is the binary expansion of i.

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

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

is called the Walsh spectrum of f at a. 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 trace map from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$. 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 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 such Boolean functions are called bent.

Definition 2.1 *[15] 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 algebraic degree, is affine invariant. Courtois and Meier [8] showed $AI(f) \leq \lceil \frac{n}{2} \rceil$.

We refer to [16] and [19] for the knowledge of BCH code and finite fields used in this paper.

3 Combinatorial Conjecture

Recall that $\overline{x}$ is the binary expansion of the integer x.

Conjecture 3.1 *[21] Let $k > 1$ be an integer. For any $0 \leq t < 2^k - 1$, define*

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

Then $|S_t| \leq 2^{k-1}$.

Tu and Deng [21] could validate this conjecture when $k \leq 29$. In [11, 14], the authors proved it is true for many cases of t. Tang et al.in [20] presented a new combinatorial conjecture similar to Conjecture 3.1 as follows:

Conjecture 3.2 *[20] Let $k > 1$be an integer. For any $0 \leq t < 2^k - 1$, define*

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

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

This conjecture has been proved in [10]. The authors also referred to the following conjecture in [20].

Conjecture 3.3 *Let $k > 1$ be an integer, and any $u \in \mathbb{Z}^*_{2^k-1}$. For any $0 \leq t < 2^k - 1$, define*

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

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

For $2 \leq k \leq 15$, this general conjecture is checked in [20]. This general conjecture includes Conjecture 3.1 and Conjecture 3.3 as special cases. The most general conjecture is as follows:

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

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

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

Lemma 3.5 *Conjecture 3.4 is equivalent to Conjecture 3.3.*

Proof: It's obvious Conjecture 3.4 implies Conjecture 3.3.

If Conjecture 3.3 is true, i.e. for any $u \in \mathbb{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{t,u}| \leq 2^{k-1}$. For any $v \in \mathbb{Z}^*_{2^k-1}$,

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

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

For any $u, v \in \mathbb{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{vt,uv,v}| \leq 2^{k-1}$ if and only if for any $u, v \in \mathbb{Z}^*_{2^k-1}$, $0 \leq t < 2^k - 1$, $|S_{t,u,v}| \leq 2^{k-1}$. Therefore Conjecture 3.4 is true. □

4 Boolean functions with optimal algebraic immunity

In this section, we present a class of $2k$-variable Boolean functions with optimal algebraic immunity under the assumption that the general conjecture is true. Its algebraic degree and nonlinearity will also be discussed. This construction is a generalization of Dillon's construction[13].

Construction 4.1 *Let $n = 2k \geq 4$, $(u, 2^k - 1) = 1$. 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 $f \in \mathcal{B}_n$ as follows*

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

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

4.1 Algebraic immunity

Theorem 4.2 *Let f be the n-variable boolean function defined by Construction 4.1. If the general conjecture is correct, then f has the 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 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 a bivariate polynomial on $\mathbb{F}_{2^k}$

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

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

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

can be written as

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

where

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

Note that $\{t-ui(\mathrm{mod}\, 2^k-1) | 0 \le i < 2^k-1\} = \mathbb{Z}_{2^k-1}$ due to $(u, 2^k-1) = 1$. For any $\gamma \in \Delta_s$, $h(\gamma y^u, y) = 0$ for all $y \in \mathbb{F}_{2^k}^*$, 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 $\mathbb{F}_{2^k}$, having the elements in Δ_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 $2^{k-1}+1$. However, from Conjecture 3.3, the weight of this codeword should be less than or equal to 2^{k-1}. This leads to a contradiction. Hence this codeword must be zero, that is

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

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 $(f+1) \cdot h = 0$, we will prove $h = 0$.

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

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

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

At the same time, $h(0,\beta)=\sum_{j=0}^{2^k-2}h_{0,j}\beta^j$ for any $\beta\in\mathbb{F}_{2^k}$, hence $h_{0,j}=0$ for $0\le j\le 2^k-2$. 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 $\mathbb{F}_{2^k}$, having the elements in $\mathbb{F}_{2^k}^*\setminus\Delta_s$ as zeros and designed distance 2^{k-1}. By the BCH bound, if the codeword is nonzero, then it has Hamming weight at least 2^{k-1}. But according to Conjecture 3.3 and $h_{0,i}=0, 0\le i\le 2^k-2$, its Hamming weight is less than 2^{k-1}. A contraction follows. So we obtain $h=0$.

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

4.2 Polynomial representation and algebraic degree

Theorem 4.3 *Let f be the n-variable boolean function defined in Construction 4.1. Then its bivariate representation is*

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

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

Proof: Let $g(x)=\sum_{i=0}^{2^k-1}g_ix^i$ be the univariate representation of g. We have $g_0=g(0)=0$, $g_{2^k-1}=0$ (since g have even Hamming weight). For every $i\in\{1,\cdots,2^k-2\}$,

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

Then we have $g(y)=\sum_{i=1}^{2^k-2}\alpha^{-is}(1+\alpha^{-i})^{2^{k-1}-1}y^i$ 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 $deg(f)=\max_{1\le i\le 2^k-2}\{wt(\bar{i})+wt(\overline{(2^k-1-u)i})\}$. It is obvious $k\le deg(f)\le 2(k-1)$. □

Remark 4.4 *(1) If $u = 1$, f has algebraic degree k, since $wt(\bar{i})+wt(\overline{-i}) = k$ for any $0 \le i \le 2^k - 2$; If $u = 2^l$, $0 \le l < k$, $deg(f) = \max_{1\le i\le 2^k-2}(wt(\bar{i}) + wt(\overline{-2^l i})) = \max_{1\le i\le 2^k-2}(wt(\bar{i}) + wt(\overline{-i})) = k$.*

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

4.3 Nonlinearity

Lemma 4.5 *Let $k \ge 2$ be a positive integer and α a primitive element of $\mathbb{F}_{2^k}$. Let $\Delta_s = \{\alpha^s, \cdots, \alpha^{2^{k-1}+s-1}\}$ where $0 \le s < 2^k - 1$ 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

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

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

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

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

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

Let $q = 2^k$,

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

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

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

We have

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

From [6], $\sum_{\mu=1}^{q-2}(\sin\frac{\mu\pi}{q-1}) \le -\frac{2(q-1)}{\pi}\ln\tan(\frac{\pi}{4(q-1)})$, so we get

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

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

Theorem 4.6 *Let $n = 2k$ and $f \in \mathcal{B}_n$ be the Boolean function given by Construction 4.1. Then we have*

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

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

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

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

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

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

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

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

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

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

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

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

So we get

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

By Lemma 4.5, we have

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

□

4.4 A class of bent function with optimal algebraic immunity

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

Theorem 4.7 *Let f be the n-variable boolean function defined in Construction 4.1. Take $u = 2^l$, $0 \le l < k$. If Conjecture 3.3 is true, then f is bent with optimal algebraic immunity, and has algebraic degree k.*

Proof: As is proved in 4.2 that $AI(f) = \frac{n}{2} = k$.

From Theorem 4.6, when $(a, b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$ and $ab = 0$, $W_f(a, b) = 2^k$.

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

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

Since $(u, 2^k - 1) = 1$, there exists a unique $\beta_\gamma \in \mathbb{F}_{2^k}^*$ s.t. $\beta_\gamma^u = a\gamma$. So for $u = 2^l$, $tr(a\gamma y^u) = tr(\beta_\gamma y)$. We have

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

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

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

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

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

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

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

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

By Remark 4.4 $deg(f) = k$. □

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 4.8 *In fact, this class of bent function with optimal algebraic degree is Dillon's $\mathcal{PS}$ functions[13], since $E_\gamma = \{(\gamma y^{2^l}, y) | y \in \mathbb{F}_{2^k}\}, \gamma \in \Delta_s$ are 2^{k-1} linear subspaces of $\mathbb{F}_{2^{2k}}$ of dimension k and $E_{\gamma_1} \cap E_{\gamma_2} = \emptyset$ for $\gamma_1 \neq \gamma_2, \gamma_1, \gamma_2 \in \Delta_s$.*

This class of Boolean functions defined by Construction 4.1 are Tu-Deng functions[21] when $u = 1$, and are Boolean functions proposed by Tang el et.[20] when $u = 2^k - 2$.

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 3.3, 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, $k \geq 2$. Let α be a primitive element of the finite field $\mathbb{F}_{2^k}$. Set $\Delta_s = \{\alpha^s, \cdots, \alpha^{2^{k-1}+s-1}\}$ where $0 \leq s < 2^k - 1$ is an integer. We define the Boolean $F \in \mathcal{B}_n$ 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 $\mathbb{F}_{2^k}$ with $supp(g) = \Delta_s$.

Theorem 5.2 *Let F be the n-variable Boolean function defined by Construction 5.1. Then F is balanced and $deg(F) = n - 1$.*

Proof: It is obvious that F is balanced since $wt(F) = wt(g) + wt(f) = 2^{k-1} + 2^{k-1}(2^k - 1) = 2^{n-1}$.

It's easy to see that $F(x,y) = f(x,y) + (1 + x^{2^k-1})g(y)$, where $f \in \mathcal{B}_{2k}$ is the Boolean function defined in Construction 4.1. Since $deg((1 + x^{2^k-1})g(y)) = 2k - 1 > deg(f)$, we get $deg(F) = 2k - 1 = n - 1$. □

Theorem 5.3 *Let F be the n-variable Boolean function defined by Construction 5.1. If Conjecture 3.3 is true, then $AI(F) = \frac{n}{2} = k$.*

Proof: From Construction 5.1, we have $\{(\gamma y^u, y)|y \in \mathbb{F}_{2^k}^*, \gamma \in \Delta_s\} \subseteq supp(F)$ and $\{(\gamma y^u, y)|y \in \mathbb{F}_{2^k}^*, \gamma \in \mathbb{F}_{2^k}^* \setminus \Delta_s\} \cup \{(x, 0)|x \in \mathbb{F}_{2^k}\} \subseteq supp(F+1)$. By a similar proof to that of Theorem 4.2, we can see both F and $F+1$ have no nonzero annihilators with algebraic degree less than k. So the function F also has optimal algebraic immunity. □

Lemma 5.4 *Let $\alpha \in \mathbb{F}_{2^k}^*$ be a primitive element and $\lambda \in \mathbb{F}_{2^k}$. Denote*

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

If $\lambda \neq 0$, then

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

Proof: Similar to Lemma 4.5, we have

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

Denote $q = 2^k$,

$$\begin{aligned} S_\lambda &= \sum_{i=s}^{2^{k-1}+s-1} (-1)^{tr(\lambda\alpha^i)} \\ &= \frac{1}{q-1} \sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=s}^{2^{k-1}+s-1} \overline{\chi}^\mu(\lambda\alpha^i) \end{aligned}$$

Take $\lambda = \alpha^l$,

$$\begin{aligned}
S_\lambda &= \frac{1}{q-1}\sum_{\mu=0}^{q-2} G(\chi^\mu) \sum_{i=s}^{2^{k-1}+s-1} \zeta^{-(l+i)\mu} \\
&= -\frac{q}{2(q-1)} + \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^\mu)\frac{\zeta^{-(l+s)\mu}(1-\zeta^{\frac{-\mu q}{2}})}{1-\zeta^{-\mu}} \\
&= -\frac{q}{2(q-1)} + \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^\mu)\frac{\zeta^{-(l+s)\mu+\frac{\mu}{2}-\frac{\mu q}{4}}(\zeta^{\frac{\mu q}{4}}-\zeta^{-\frac{\mu q}{4}})}{\zeta^{\frac{\mu}{2}}-\zeta^{-\frac{\mu}{2}}} \\
&= -\frac{q}{2(q-1)} + \frac{1}{q-1}\sum_{\mu=1}^{q-2} G(\chi^\mu)\frac{\zeta^{-(l+s)\mu+\frac{\mu}{2}-\frac{\mu q}{4}}\sin\frac{\pi\mu q}{2(q-1)}}{\sin\frac{\pi\mu}{q-1}}
\end{aligned}$$

Therefore

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

By the inequality $\sum_{\mu=1}^{q-2}(\sin\frac{\mu\pi}{q-1}) \le -\frac{2(q-1)}{\pi}\ln\tan(\frac{\pi}{4(q-1)})$, we get

$$|S_\lambda| \le 1 + \frac{2\sqrt{q}}{\pi}\ln\frac{4(q-1)}{\pi}$$

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

Theorem 5.5 *Let F be the n-variable Boolean function defined by Construction 5.1. Then*

$$\begin{aligned}
N_F &\ge 2^{n-1} - \frac{2^{k+1}}{\pi}\ln\frac{4(2^k-1)}{\pi} - \frac{2^{\frac{k}{2}+1}}{\pi}\ln\frac{4(2^k-1)}{\pi} - 2 \\
&\approx 2^{n-1} - \frac{2\ln 2}{\pi}k2^k - \frac{2\ln 2}{\pi}k2^{\frac{k}{2}}.
\end{aligned}$$

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

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

Consequently,

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

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

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

By Lemma 4.5 and Lemma 5.4

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

□

This class of Boolean functions defined by Construction 5.1 is Tu-Deng balanced functions[21] when $u = 1$, and is balanced Boolean functions proposed by Tang el et.[20] when $u = 2^k - 2$.

6 Conclusion

We generalize T-D functions[21] and functions proposed Tang et al.[20] and put forward two infinite classes of $2k$-variable Boolean functions, one of which is balanced. Both classes have high nonlinearity and high algebraic degree. Based on Conjecture 3.3, both class have optimal algebraic immunity. If we replace xy^{2^k-1-u} by $x^{2^k-1-u}y$ or $x^{2^k-1-v}y^{2^k-1-u}$, $(v, 2^k-1) = 1$, the corresponding Boolean functions have the same properties as Boolean functions in this paper.

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. Inf. 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] Carlet C.: On a weakness of the Tu-Deng function and its repair, Cryptology ePrint Archive, Report 2009/606. http://eprint.iacr.org/2009/606.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.

[13] Dillon J. F.: Elementary Hadamard Difference Sets, PhD thesis, University of Maryland, 1974.

[14] 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.

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

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

[17] 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.

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

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

[20] 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.

[21] 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.

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