A Conjecture on Binary String and Its Applications on Constructing Boolean Functions of Optimal Algebraic Immunity

Ziran Tu * and Yingpu deng †

Abstract

In this paper, we propose a combinatoric conjecture on binary string, on the premise that our conjecture is correct we mainly obtain two classes of functions which are both algebraic immunity optimal: the first class of functions are also bent, moreover, from this fact we conclude that the algebraic immunity of bent functions can take all possible values except one. The second class are balanced functions, which have optimal algebraic degree and the best nonlinearity up to now.

Keywords: boolean function, algebraic immunity, bent function, balanced, nonlinearity, algebraic degree [1]

1 Introduction

Boolean functions play very important roles in stream ciphers, of which there are two usual models: the combiner model and the filter model. They have been proved to be theoretically equivalent, but the attacks do not work quite similarly on each model. What they have in common is that both the combining function and the filtering function should be balanced, have high algebraic degree, high nonlinearity and high correlation immunity etc., however these properties are only necessities for cryptosystems in the last century.

In the year 2003, the so called standard algebraic attack [1, 3, 4] upon stream cipher proposed by N.T Courtois, brings us a completely new criterion for the design of secure stream cipher systems, known as the algebraic immunity criterion. As a cryptosystem, we naturally wish it be able to resist all kinds of known attacks, unfortunately, to do this is usually not an easy task. Although there have been several constructions that have the optimal algebraic immunity so far, many of which are unable to be candidates for real applications, because their other properties such as algebraic degrees, nonlinearities are not very good. As far as recently, [14] proposed an infinite excellent class of balanced functions which are algebraic immunity optimal and also have very high nonlinearity, it is very notable that their functions are nonlinearity optimal among all known constructions at that time. So it is interesting to study the relationships between algebraic immunity and other cryptographic criteria of boolean functions. The first such results about algebraic immunity and nonlinearity of Boolean functions appeared in [5]. In [2, 7], the people studied the lower bound of nonlinearity or of higher order nonlinearity of Boolean functions with prescribed algebraic immunity. In [7], the tight lower bound of nonlinearity of Boolean functions has been found, if the algebraic immunity of Boolean function is given.

We are interested in the tight upper bound of nonlinearity of boolean functions with given algebraic immunity. It is well-known that when the number n of input variables is even, the

*Henan University of Science and Technology, Luoyang 471003, PR China.Email:naturetu@gmail.com

†Academy of Mathematics and Systems Science, CAS, Beijing 100080, PR China. Email:ypdeng@amss.ac.cn

[1]This paper is supported by the NNSF of China (6532100) and 973 Project (2004CB318000)

nonlinearity of Bent functions reaches the maximum value i.e. $2^{n-1}-2^{\frac{n}{2}-1}$, but no one knows the case that the algebraic immunity is given. In [15] we have investigated some properties of functions of algebraic immunity one, and obtained that these functions can not be bent.

In this paper, we propose a combinatoric conjecture on binary string, and based which we construct two classes of Boolean functions: one class are bent, the other are balanced, both classes have the optimal algebraic immunity on the premise that our conjecture is correct. Moreover, we conclude that the algebraic immunity of bent functions can take all possible values except one, and these balanced functions we construct have optimal algebraic degree and the best nonlinearity up to now.

This paper is organized as follows. In section 2, we give some preliminaries of boolean functions, in section 3 we propose our combinatoric conjecture, based on which we give our main results in section 4, including two constructions of functions that are algebraically optimal. We conclude in section 5.

2 Preliminaries

Let n be a positive integer. A boolean function on n variables is a mapping from $\mathbb{F}_2^n$ into $\mathbb{F}_2$, which is the finite field with two elements. We denote B_n the set of all n-variable boolean functions.

Any boolean function f in B_n has a unique representation as multivariate polynomials over $\mathbb{F}_2$, which is called the algebraic normal form (ANF)

$$f(x_1, x_2, ..., x_n) = \sum_{I \subseteq \{1,...,n\}} a_I \prod_{i \in I} x_i$$

where the a_I's are in $\mathbb{F}_2$. The algebraic degree $\deg(f)$ of f equals the maximum degree of those monomials with nonzero coefficients in its algebraic normal form. A boolean function f is called affine, if $\deg(f) \leqslant 1$. We denote A_n the set of all affine functions in B_n. The support of f is defined as $\mathrm{Supp}(f) = \{x \in \mathbb{F}_2^n : f(x) = 1\}$, and the $\mathrm{wt}(f)$ is the number of vectors which lies in $\mathrm{Supp}(f)$. For two functions f and g in B_n, the Hamming distance $d(f, g)$ between f and g is defined as $\mathrm{wt}(f + g)$. The nonlinearity $nl(f)$ of a boolean function f is defined as the minimum Hamming distance between f and all affine functions, i.e. $\mathrm{nl}(f) = \mathrm{Min}_{g \in A_n} d(f, g)$.

It is well known that for any $a \in \mathbb{F}_2^n$, the value

$$\mathrm{W}_f(a) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+<x,a>}$$

is called the Walsh spectrum of f at a, where $< x, a >$ denotes the inner product between x and a i.e.$< x, a >= x_1a_1 + \ldots + x_na_n$. The nonlinearity of boolean function f can be expressed via its Walsh spectra by the next formula

$$\mathrm{nl}(f) = 2^{n-1} - \frac{1}{2}\mathrm{Max}_{a \in \mathbb{F}_2^n} |\mathrm{W}_f(a)|.$$

And it holds the following inequality

$$\mathrm{nl}(f) \leqslant 2^{n-1} - 2^{\frac{n}{2}-1}.$$

When n is even, the above upper bound can be attained, and such boolean functions are called bent [10]. Bent functions have several equivalent definitions. For instance, it is equivalent to $|\mathrm{W}_f(a)| = 2^{n/2}$, for every $a \in \mathbb{F}_2^n$. It is also equivalent to that $\mathrm{Supp}(f)$ is a $(2^n, 2^{n-1} \pm 2^{\frac{n}{2}-1}, 2^{n-2} \pm 2^{\frac{n}{2}-1})$-difference set in the additive group of $\mathbb{F}_2^n$.

Definition 2.1. *[8] The algebraic immunity $AI_n(f)$ of an n-variable boolean function f is defined to be the lowest degree of nonzero functions g such that $fg = 0$ or $(f + 1)g = 0$.*

3 Our combinatoric conjecture

Conjecture: Assume $k \in \mathbb{Z}$, $k > 1$, for every $x \in \mathbb{Z}$, we expand x as a binary string of length k, and denote the number of one's in the string by $w(x)$, for any $t \in \mathbb{Z}$, $0 < t < 2^k - 1$, let

$$S_t = \{(a, b) | a, b \in \mathbb{Z}_{2^k-1}, a + b = t \ mod \ 2^k - 1, w(a) + w(b) \leqslant k - 1\}$$

then $|S_t| \leqslant 2^{k-1}$.

Remark 3.1. *We believe that the above conjecture is correct, although we are unable to prove it mathematically up to now. However, we successfully design a tranfer-matrix algorithm, through which we validate our conjecture when $k \leqslant 29$.*

4 Bent function with optimal algebraic immunity

Based on our conjecture, we construct a subclass of the so-called *Partial Spread* function, first we recall Dillon's construction:
Dillon's construction:[11] Let $n = 2k$, $\mathbb{F}_{2^n} \approx \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \longrightarrow \mathbb{F}_2$ is balanced, $f(x, y) : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$ is defined by

$$f(x, y) = g(\frac{x}{y})$$

if $y = 0$, we define $\frac{x}{y}$ to be 0 or 1, then f is bent

In fact, this is the so-called PS^- function, the idea of the construction is that: the space $\mathbb{F}_{2^n}$, viewed as a 2-dimensional $\mathbb{F}_{2^k}-$vectorspace, is a set of $2^k + 1$ lines through the origin, Dillon choose randomly 2^{k-1} lines, except the origin, to form the support of his function, the idea of ours is choosing these lines following some rules:
Construction 1. Let $n = 2k$, α is a primitive element of $\mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$, g is defined as

$$supp(g) = \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^{k-1}-1}\}$$

in whicn $0 \leqslant s < 2^k - 1$, $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, define

$$f(x, y) = \begin{cases} g(\frac{x}{y}), & \text{if} x \cdot y \neq 0 \\ 0, & \text{otherwise} \end{cases}$$

Before proving our result we introduce the famous BCH bound and the definition of BCH code in coding theory[13].

Theorem 4.1. (*The BCH bound*) *Let Φ be a cyclic code of length n and with generator polynomial $g(x)$ such that for some $b \geqslant 0$, $\delta \geqslant 1$*

$$g(\alpha^b) = g(\alpha^{b+1}) = \cdots = g(\alpha^{b+\delta-2}) = 0$$

i.e. the code has a string of $\delta - 1$ consecutive powers of α as zeros, α is a primitive $n-$th root, then the minimal distance of Φ is at least δ.

This induces the definition of the BCH codes:

Definition 4.2. *A cyclic code of length n over $\mathbb{F}_q$ is a BCH code of designed distance δ if for some integer $b \geqslant 0$,*

$$g(x) = lcm\{m^{(b)}(x), m^{(b+1)}(x), \cdots, m^{(b+\delta-2)}(x)\}$$

i.e. $g(x)$ is the lowest degree monic polynomial over $\mathbb{F}_q$ having $\alpha^b, \alpha^{b+1}, \cdots, \alpha^{b+\delta-2}$ as zeros.

The following is our main result:

Proposition 4.3. *Assume the conjecture is correct, then the $f(x, y)$ comes from construction 1 is bent, and $AI_n(f) = k = \frac{n}{2}$.*

Proof. Since $f(x, y)$ is included in the class of PS^-, it is obvious that f is *bent*. Our task is to prove that $f(x, y)$ has the optimal algebraic immunity, in other words, both f and $f + 1$ have no annihilators with algebraic degrees less than k.

Let $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, $deg(h) < k$ and satisfies $f \cdot h = 0$, we need to prove $h = 0$. h can be write as a polynomial of 2 variables on $\mathbb{F}_{2^k}$

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

Because $deg(h) < k$, so we have $h_{i,j} = 0$ if $w(i) + w(j) \geqslant k$. From $f \cdot h = 0$, then $h(x, y) = 0$ for all $(x, y) \in supp(f)$, $supp(f) = \{(y, \gamma y) : y \in \mathbb{F}_{2^k}^*, \gamma \in \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^{k-1}-1}\}\}$, we denote $\{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^{k-1}-1}\}$ by Δ, then $h(y, \gamma y) = 0$ for $\forall y \in \mathbb{F}_{2^k}^*, \gamma \in \Delta$.

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

We write $h(y, \gamma y)$ in another simplified form

$$h(y, \gamma y) = h_{00} + \sum_{t=1}^{2^k-1} h_t(\gamma) y^t$$

in which

$$h_t(\gamma) = \sum_{i=0}^{t} h_{i,t-i} \gamma^i + \sum_{i=t}^{2^k-1} h_{i,2^k-1+t-i} \gamma^i$$

For any $0 \leqslant i \leqslant 2^k - 1$, it satisfies $w(i) + w(2^k - 1 - i) = k$, then $h_{2^k-1}(\gamma) = 0$ and $h_{2^k-1,t} = h_{2^k-1}(\gamma) = 0$ for all t, so

$$h_t(\gamma) = \sum_{i=0}^{t} h_{i,t-i} \gamma^i + \sum_{i=t}^{2^k-2} h_{i,2^k-1+t-i} \gamma^i$$

We get

$$h(\gamma y, y) = h_{00} + \sum_{t=1}^{2^k-2} h_t(\gamma) y^t$$

For some fixed $\gamma \in \Delta$, since $h(\gamma y, y) = 0 \ \forall y \in \mathbb{F}_{2^k}^*$, it follows that

$$h_t(\gamma) = 0, 1 \leqslant t \leqslant 2^k - 2, \forall \gamma \in \Delta$$

From the definition of the BCH codes, we know that $(h_{0,t}, h_{1,t-1}, \cdots, h_{t,0}, h_{t+1,2^k-2}, \cdots, h_{2^k-2,t+1})$ is a codeword in some 2^k-ray BCH code of length $2^k - 1$, having the elements in Δ as zeros and

with designed distance $2^{k-1}+1$, if this codeword is nonzero, then its Hamming weight should be greater than $2^{k-1}+1$, but from our conjecture, the weight of this codeword should be less than or equal to 2^{k-1}, this contradicts, then this codeword must be 0, that is

$$h_{0,t} = h_{1,t-1} = \cdots = h_{t,0} = h_{t+1,2^k-2} = \cdots = h_{2^k-2,t+1} = 0$$

then $h_{i,j} = 0\ \forall 0 \leqslant i,j \leqslant 2^k-1$, this proves $h=0$, by other words, f has no annihilators with algebraic degrees less than k.

We need to prove a similar result on $f+1$.

Again we let $h : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, $deg(h) < k$ and it satifies $(f+1)\cdot h = 0$, we will prove $h=0$. First we have

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

Since $h(x,0)=0$ for $\forall x \in \mathbb{F}_{2^k}$, then $h_{i,0}=0$ for $\forall 0 \leqslant i \leqslant 2^k-1$, similarly, for all $1 \leqslant t \leqslant 2^k-2$, $h_t(\gamma)=0$ when $\gamma \in \mathbb{F}_{2^k} \setminus \Delta$. We can see that $(h_{0,t}, h_{1,t-1}, \cdots, h_{t,0}, h_{t+1,2^k-2}, \cdots, h_{2^k-2,t+1})$ is a codeword in some 2^k-ray BCH code of length 2^k-1, having the elements in $\mathbb{F}_{2^k} \setminus \Delta$ as zeros and with designed distance 2^{k-1}(without loss of generality we suppose $s=0$, then $\mathbb{F}_{2^k} \setminus \Delta = \{\alpha^{2^{k-1}}, \alpha^{2^{k-1}+1}, \cdots, \alpha^{2^k-2}\}$). If this codeword is nonzero then its weight should be greater than $\geqslant 2^{k-1}(BCH$ bound), from our conjecture and $h_{i,0}=0$, the weight should be less than 2^{k-1}. This proves $h=0$

Now we can conclude that $AI_n(f) = k = \frac{n}{2}$, that is, there exists bent functions with optimal algebraic immunity.

All the elements of PS^- have algebraic degree $\frac{n}{2}$ exactly[16], this is an interesting property, combine with our construction 1, we are able to get some significant corollaries:

Corollary 4.4. *Let $n=2k$, $k \geqslant 2$, then the algebraic immunity of bent can take $2,3,\cdots,k$, except 1.*

Proof. Let $2 \leqslant t \leqslant k$, we will construct *bent* function $f \in B_n$ such that $AI_n(f) = t$. At first we can get $g(x_1, x_2, \cdots, x_{2t}) \in B_{2t}$ which is *bent* and $AI_{2t}(g) = deg(g) = t$, then we construct $g' \in B_{2t+2}$

$$g'(x_1, x_2, \cdots, x_{2t}, x_{2t+1}, x_{2t+2}) = g(x_1, x_2, \cdots, x_{2t}) + x_{2t+1}x_{2t+2}$$

It's not difficult to know that g' is *bent* in B_{2t+2} and $deg(g') = t$, because for any $(\alpha, a_{2t+1}, a_{2t+2})$, in which $\alpha \in \mathbb{F}_2^{2t}$, we have

$$W_{g'}(\alpha, a_{2t+1}, a_{2t+2}) = \pm 2 W_g(\alpha)$$

From the bentness of g, it is easy to know that g' is *bent*. Next we should prove

$$AI_{2t+2}(g') = t$$

First it is obvious that

$$AI_{2t+2}(g') \leqslant min\{deg(g'), AI_{2t}(g)+1\} = t$$

Let $h \in B_{2t+2}$, $deg(h) < t$ s.t. $g' \cdot h = 0$, h can be write as

$$h = h_0 + h_1 x_{2t+1} + h_2 x_{2t+2} + h_3 x_{2t+1} x_{2t+2}$$

Through direct computations we can see that g' has no non-zero annihilators with algebraic degree $< t$, by a similar proof for $g'+1$, then we have

$$t \leqslant AI_{2t+2}(g')$$

Repeating this progress again and again until we finally obtain a $f \in B_n$ which is *bent* and $AI_n(f) = t$.

Boolean functions are required to have high algebraic degrees, which is an important design criterion as well. As another corollary of construction 1, we discuss the relations between algebraic immunity and algebraic degrees:

Consider the following inequality: suppose $f \in B_n$, then

$$AI_n(f) \leqslant min\{\lceil \frac{n}{2} \rceil, deg(f)\} \tag{4.1}$$

The (4.1)is obviously right because of the results in [3]:

Theorem 4.5. *Let $f \in B_n$, then there exists $g \in B_n$, $deg(g) \leqslant \lceil \frac{n}{2} \rceil$, satisfies $deg(f \cdot g) \leqslant \lceil \frac{n}{2} \rceil$.*

For the correctness of the other half, $f + 1$ is a annihilator of f. [12] investigate the so-called *majority function*

$$f(x_1, x_2, \cdots, x_n) = \begin{cases} 0, & \text{if} wt(x) \leqslant \lfloor \frac{n}{2} \rfloor \\ 1, & \text{otherwise} \end{cases}$$

It is discovered in [12]that:

Theorem 4.6. *Let $n \in \mathbb{Z}_+$, $f \in B_n$, f is the majority function defined as above, then $AI_n(f) = \lceil \frac{n}{2} \rceil$ and $deg(f) = 2^{\lfloor log_2 n \rfloor}$.*

Consider 4.6, if we choose $n = 2^k - 1$, then

$$deg(f) = 2^{\lfloor log_2 n \rfloor} = 2^{k-1} = \frac{n+1}{2} = \lceil \frac{n}{2} \rceil = AI_n(f)$$

In other words, for infinitely many n of this form, (4.1) are sharp.

Corollary 4.7. *Let $n \in \mathbb{Z}_+$, if $n = 2m$, then for any $1 \leqslant k \leqslant m$, there exists $f \in B_n$ satisfies $AI_n(f) = deg(f) = k$; if $n = 2m + 1$, then for any $1 \leqslant k \leqslant m$, there exists $f \in B_n$ satisfies $AI_n(f) = deg(f) = k$.*

Proof. It should be noted that our corollary does not cover that when $n = 2m+1$ and $k = m+1$. First we prove a simple result: assume $h(x_1, x_2, \cdots, x_n) \in B_n$, if we let

$$h'(x_1, x_2, \cdots, x_n, x_{n+1}) = h(x_1, x_2, \cdots, x_n) \in B_{n+1}$$

then

$$AI_n(h) = AI_{n+1}(h')$$

Because if there is a $g(x_1, x_2, \cdots, x_n) \in B_n$ satisfies

$$g(x_1, x_2, \cdots, x_n) \cdot h(x_1, x_2, \cdots, x_n) = 0$$

Obviously

$$g(x_1, x_2, \cdots, x_n) \cdot h'(x_1, x_2, \cdots, x_n) = 0$$

then $AI_n(h') \leqslant AI_{n+1}(h)$.

For another direction, let $g(x_1, x_2, \cdots, x_n, x_{n+1}) \in B_{n+1}$ satisfy

$$g(x_1, x_2, \cdots, x_n, x_{n+1}) h'(x_1, x_2, \cdots, x_n, x_{n+1}) = 0$$

and $deg(g) = AI_{n+1}(h')$, since g can be write as

$$g(x_1, x_2, \cdots, x_n, x_{n+1}) = g_1(x_1, x_2, \cdots, x_n) + x_{n+1} g_2(x_1, x_2, \cdots, x_n)$$

From $gh = gh' = 0$, then

$$\begin{aligned} h(x_1, x_2, \cdots, x_n)g_1(x_1, x_2, \cdots, x_n) &= 0 \\ h(x_1, x_2, \cdots, x_n)g_2(x_1, x_2, \cdots, x_n) &= 0 \end{aligned}$$

If $g_2(x_1, x_2, \cdots, x_n) = 0$, then $AI_n(h) \leqslant deg(g_1) = AI_{n+1}(h')$; if $g_2(x_1, x_2, \cdots, x_n) \neq 0$, then $AI_n(h) \leqslant AI_{n+1}(h') - 1 < AI_{n+1}(h')$. We can deduce that

$$AI_n(h') = AI_{n+1}(h)$$

Back to our proofs: if $n = 2m$, the corollary is obviously correct when $k = 1$. When $2 \leqslant k \leqslant m$, first we could construct a bent function in B_{2k}, whose algebraic immunity and algebraic degree are both k, viewed as a function in B_n, its algebraic immunity is k also; if $n = 2m + 1$, for all $\forall 1 \leqslant k \leqslant m$, the procedures are completely the same.

From this corollary we may conjecture that (4.1)is very possibly sharp when n is odd.

It is well known that *bent* functions are not balanced, so they are improper to be used in crypto-systems directly, using the idea in construction 1, we construct another class of functions which are balanced:

construction 2: Let $n = 2k$, $k \geqslant 1$, α is primitive in $\mathbb{F}_{2^k}$, $g : \mathbb{F}_{2^k} \to \mathbb{F}_2$, let

$$supp(g) = \{\alpha^s, \alpha^{s+1}, \cdots, \alpha^{s+2^{k-1}-1}\}$$

in which $0 \leqslant s < 2^k - 1$, $f : \mathbb{F}_{2^k} \times \mathbb{F}_{2^k} \to \mathbb{F}_2$, define

$$f(x, y) = \begin{cases} g(\frac{x}{y}), & \text{if} x \cdot y \neq 0 \\ 1, & \text{if} x = 0, y \in \Delta \\ 0, & \text{other.} \end{cases}$$

in which $\Delta = \{\alpha^i : i = 2^{k-1} - 1, 2^{k-1}, \cdots, 2^k - 2\}$.

Proposition 4.8. *If our conjecture is true, functions come from construction 2 are balanced and have optimal algebraic immunity.*

Proof. It is obvious that these functions are balanced, because bent functions have $2^{n-1} - 2^{k-1}$ elements in their supports, taking into the 2^{k-1} points on the $y-$axis, then the balancedness can be seen. To imitate the proof in 4.3 we can get these functions are also algebraic immunity optimal.

K.Feng gives a very nice construction of boolean functions in [14], which are algebraic immunity optimal:

Theorem 4.9. *Let n be any integer such that $n \geqslant 2$ and β a primitive element of the finite field $\mathbb{F}_{2^n}$. Let f be the boolean function on $\mathbb{F}_{2^n}$ whose support is $\{0, 1, \beta, \cdots, \beta^{2^{n-1}-2}\}$. Then f has optimal algebraic immunity.*

[14] has the following inequality when considering the nonlinearity of functions

Proposition 4.10. *Let $\omega \in \mathbb{F}_{2^n}^*$ is a primitive element and $\lambda \in \mathbb{F}_{2^n}^*$, denote*

$$S_\lambda = \sum_{i=2^{n-1}-1}^{2^n-2} (-1)^{tr(\lambda\omega^i)}$$

then

$$|S_\lambda| \leqslant 2^{\frac{n}{2}} n \cdot ln2 + 1$$

From this inequality we can easily estimate a lower bound about the nonlinearity of our functions in construction 2:

Corollary 4.11. *Let $f \in B_n$ be defined as in construction 2, then the nonlinearity of f satisfies*

$$nl(f) \geqslant 2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\frac{k}{2}} k \cdot ln2 - 1$$

Proof. The proof is a direct computation of the walsh spectrum of f. Let $0 \neq (a,b) \in \mathbb{F}_{2^k} \times \mathbb{F}_{2^k}$, then

$$W_f(a,b) = W_h(a,b) - 2 \sum_{x,y \in B} (-1)^{tr(ax+by)}$$

in which h comes from construction 1 and $B = \{(0,\alpha^i) : i = 2^{k-1}-1, 2^{k-1}, \cdots, 2^k - 2\}$, α is primitive in $\mathbb{F}_{2^k}$.

$$\sum_{x,y \in B} (-1)^{tr(ax+by)} = \sum_{i=2^{k-1}-1}^{2^k-2} (-1)^{tr(b\alpha^i)} = S_b$$

$$|W_f(a,b)| \leqslant |W_h(a,b)| + 2|S_b|$$

From the fact that h is *bent* and the estimation of $|S_b|$, the corollary is obvious.

When n is even, we give the following table, comparing the nonlinearity of functions of [14] with ours:

n	$2^{n-1} - 2^{\frac{n}{2}-1}$	$nl(f)$in construction 2	bound in 4.11	$nl(f)$in [14]
2	1	0	0	0
4	6	4	3	4
6	28	26	21	24*
8	120	116	107	112*
10	496	490	476	478*
12	2016	2008	1982	1970
14	8128	8118	8073	8036
16	32640	32624	32551	32530
18	130812	130792	130674	

From this table we can see that the nonlinearity of our functions are very near to the bound of bent functions, it is even better than functions in [14], which are thought to have the optimal nonlinearity in all known functions that are algebraic immunity optimal at that time. We note that in the last column these numbers followed by asterisks come from [14], the others come from our own computations under the choose of default primitive element.

Remark 4.12. *We discover that the nonlinearity is related to chose which primitive element in $\mathbb{F}_{2^k}$, this suggests that when choosing different primitive elements the functions we get are not affine equivalent.*

Considering the algebraic degrees of functions in construction 2, we find it is also satisfying:

Proposition 4.13. *Let $f \in B_n$ be defined as in construction 2, then $deg(f) = n - 1$.*

Proof. f can be write as a $2-$variable polynomial on $\mathbb{F}_{2^k}$

$$f(x,y) = h(x,y) + \sum_{(a,b) \in B} (1 + (x+a)^{2^k-1})(1 + (y+b)^{2^k-1})$$

in which $B = \{(\alpha^i, 0) : i = 2^{k-1} - 1, 2^{k-1}, \cdots, 2^k - 2\}$, $supp(h) = \bigcup_{i=s}^{2^{k-1}+s-1}\{(\alpha^i, \alpha^i w) : w \in \mathbb{F}_{2^k}^*\}$. We know that the degree of h is k, so we only need to consider the second summand.

$$\sum_{(a,b)\in B}(1+(x+a)^{2^k-1})(1+(y+b)^{2^k-1})$$

$$= \sum_{i=2^{k-1}-1}^{2^k-2}(x+\alpha^i)^{2^k-1} + \sum_{i=2^{k-1}-1}^{2^k-2}\sum_{j=0}^{2^k-2}\alpha^{ij}x^{2^k-1-j}y^{2^k-1}$$

Compute the coefficients of the monomials $x^{2^k-1-j}y^{2^k-1}$,

$$\sum_{i=2^{k-1}-1}^{2^k-2}\alpha^{ij} = \frac{1+\alpha^{j\cdot(2^{k-1}-1)}}{1+\alpha^j} \tag{4.2}$$

We can see that (4.2) is nonzero when $j = 1$, then $deg(f) = n - 1$.

5 Conclusion

Before Courtois's attack, people believe that it is enough for a stream cipher to choose boolean functions about 12 variables, then in order to resist algebraic attacks, [4] suggested that choosing functions about 32 variables. We have validated our conjecture until $k \leqslant 29$, in other words, we have constructed a class of functions when the number of variables is even and $\leqslant 58$, which are optimal in terms of balancedness, degree, nonlinearity and algebraic immunity, and they are good for real applications.

References

[1] F. Armknecht, *Improving fast algebraic attacks*, FSE 2004, LNCS 3017, pp. 65–82, Springer.

[2] C. Carlet, *On the higher order nonlinearities of algebraic immune functions*, Crypto 2006, LNCS 4117, pp.584–601, Springer.

[3] N. T. Courtois, *Fast algebraic attacks on stream ciphers with linear feedback*, Crypto 2003, LNCS 2729, pp. 176–194, Springer.

[4] N. T. Courtois, W. Meier, *Algebraic attacks on stream ciphers with linear feedback*, Eurocrypt 2003, LNCS 2656, pp. 345–359, Springer.

[5] D. K. Dalai, K. C. Gupta, S. Maitra, *Results on algebraic immunity for cryptographically significant Boolean functions*, Indocrypt 2004, LNCS 3348, pp. 92–106 Springer.

[6] N.Li and W.Qi. *Construction and analysis of boolean functions of 2t+1 variables with maximum algebraic immunity.* ASIACRYPT 2006, LNCS 4284: pages 84–98, Springer, 2006.

[7] M. Lobanov, *Exact relation between nonlinearity and algebraic immunity*, Discrete Mathematics and Applications, 16(2006),453-460.

[8] W. Meier, E. Psalic, C. Carlet, *Algebraic attacks and decomposition of Boolean functions*, Eurocrypt 2004, LNCS 3027 pp. 474–491, Springer.

[9] L. Qu, G. Feng, C. Li, *On the Boolean functions with maximum possible algebraic immunity: construction and a lower bound of the count*, Available: http://eprint.iacr.org/2005/449

[10] O. S. Rothaus, *On bent functions*, Journal of Combinatorial Theory, Series A, 20(1976), 300–305.

[11] J.F.Dillon. *Elementary Hadamard Difference Sets.* Ph.D thesis, University of Maryland, 1974.

[12] D.K.Dalai, S.Maitra and S.Sarkar. *Basic theory in construction of boolean functions with maximum possible annihilator immunity.* DCC, Volume 40, , Number 1, (2006):41–58.

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

[14] C.Carlet and K.Feng. *An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity.* ASIACRYPT 2008, LNCS 5350: pages 425–440, Springer.

[15] Tu, Z. and Deng, Y. *Algebraic Immunity Hierarchy of Boolean Functions* ChinaCrypt2007

[16] O.S.Rothaus. *On bent functions.* Journal of Combinatorial Theory, Ser. A, Volume 20, (1976):300–305.