The Nonlinearity of Sum and Product for Boolean Functions

Huang Jinglian[a], and Wang Zhuo

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, 730030, China

Abstract. In this paper, we study the relationship between the nonlinearity of Boolean function and the nonlinearity of the sum and product of Boolean function, while derivative and e-derivative are used to study the problem further . We obtain that the sum of two functions' nonlinearity is not less than the nonlinearity of the sum of two functions. The relationship between the nonlinearity of function and the nonlinearity of the sum and product of two functions are also obtained. Furthermore, we also get the relationship between the nonlinearity of the product of functions, and the derivative and e-derivative of function. Moreover, we also deduced some important applications on the basis of the above work.

1 Introduction

The cipher security is the core of the cryptosystem, and only a cryptosystem with good security has an existing significance. Boolean functions with a variety of secure cipher properties are the key factors to design the cryptosystem with the ability to resist multiple cipher attacks and good safety performance. It is of great importance for a security cryptosystem to study some properties of Boolean functions, which make the cryptosystem resist various attacks, such as high algebraic degree, high nonlinearity, the strict avalanche criterion and propagation, higher-order correlation immunity and higher-order algebraic immunity. Therefore, there are some important research problems, such as the existence, the feature, the design, the construction and the count of Boolean functions with some kind of secure cryptographic property [1~7].

The nonlinearity of Boolean functions is a measure of the ability to resist the affine approximation attack. The higher the nonlinearity of Boolean functions, the stronger the ability to resist the affine approximation attacks. It is an important task to study the nonlinearity of Boolean functions [8~9].

With the sum or product of two Boolean functions, the Boolean functions with good cryptographic properties can be obtained. As the sum of a 2 time homogeneous H Boolean function and a $n/2$ monomial can be a Bent function. Therefore, it is also necessary to study the cryptographic properties of the sum of the function or the product function of two Boolean functions, such as nonlinearity.

In this paper, we will discuss whether there is a triangle inequality between the nonlinearity of Boolean functions and the sum of two functions. At the same time, the derivative and e-derivative of the Boolean function are used to reveal the relationship between the nonlinearity of Boolean function and the sum or the product of the two functions.

2 Preliminaries

To study cryptographic properties of H Boolean functions, we proposed the concept of the e-derivative [10~12]. The e-derivative and derivative are defined here as Definition 1&2.

Definition 1: The e-derivative (e-partial derivative) of n-dimensional Boolean functions $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&ef(x)/e(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)\cdot\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}. \quad (1)$$

If $r=1$, (1) turns into the e-derivative of $f(x)=f(x_1,x_2,\cdots,x_n)$ for a single variable, which is denoted by $ef(x)/ex_i$ $(i=1,2,\cdots,n)$. As a result, the simplified form below can be easily derived.

$$\begin{aligned}&ef(x)/ex_i\\&=f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n)\cdot\\&f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n)\end{aligned}\ (i=1,2,\cdots,n).$$

Definition 2: The derivative (partial derivative) of n-dimensional Boolean functions $f(x)=f(x_1,x_2,\cdots,x_n)\in GF(2)^{GF(2)^n}$ for r variables $x_{i1},x_{i2},\cdots,x_{ir}$ is defined as

$$\begin{aligned}&\partial f(x)/\partial(x_{i1},x_{i2},\cdots,x_{ir})\\&=f(x_1,x_2,\cdots,x_{i1},x_{i2},\cdots,x_{ir},\cdots,x_n)+\\&f(x_1,x_2,\cdots,1+x_{i1},1+x_{i2},\cdots,1+x_{ir},\cdots,x_n)\\&(1\le i\le n,1\le i_1\le i_2\le\cdots\le i_r\le n,1\le r\le n)\end{aligned}. \quad (2)$$

If $r=1$, (2) turns into the derivative of $f(x)=f(x_1,x_2,\cdots,x_n)$ for a single variable, which is

[a] Huang Jinglian: huangjlstudy@163.com

denoted by $df(x)/dx_i$ $(i=1,2,\cdots,n)$. As a result, the simplified form below can be easily derived.

$$\begin{aligned} &df(x)/dx_i \\ &= f(x_1,x_2,\cdots,x_{i-1},1,x_{i+1},\cdots,x_n) \\ &+f(x_1,x_2,\cdots,x_{i-1},0,x_{i+1},\cdots,x_n) \end{aligned} \quad (i=1,2,\cdots,n).$$

Definition 3: The cascade function $f(x)$ $(x=x_0x_1x_2\cdots x_n \in GF(2)^{n+1})$ cascade with two n-dimensional Boolean functions $f_1(x')$ and $f_2(x')$ $(x'=x_1x_2\cdots x_n \in GF(2)^n)$ is defined as

$$\begin{aligned} &f(x)=(1+x_0)f_1(x')+x_0f_2(x') \\ &=f_1(x')+x_0(f_1(x')+f_2(x')) \end{aligned},$$

$f(x)$ is denoted by $f(x)=f_1(x)\|f_2(x)$.

According to Definition 1~3, we can get Lemmas 1 easily.

Lemma 1: For any arbitrary Boolean function $f(x)$, the following equations are true:

$$\begin{aligned} &f(x) \\ &=f(x)df(x)/dx_i+ef(x)/ex_i \end{aligned} \quad (i=1,2,\cdots,n),$$

and

$$\begin{aligned} &w_t(f(x)) \\ &=w_t(f(x)df(x)/dx_i)+w_t(ef(x)/ex_i) \\ &=2^{-1}w_t(df(x)/dx_i)+w_t(ef(x)/ex_i) \\ &(i=1,2,\cdots,n) \end{aligned}.$$

3 The triangle inequality for the nonlinearity of the sum of two Boolean functions

We are always wondering if there exists a relationship among the nonlinearity of two Boolean functions and the sum function ,which can be represented by a triangle inequality. Theorem 1 just reveals the triangle inequality.

Theorem 1: Suppose Boolean functions $f_1(x),f_2(x)\in GF(2)^{GF(2)^n}$. The nonlinearity of $f_1(x)$ and $f_2(x)$ are N_{f_1} and N_{f_2}, the nonlinearity of the sum function $f_1(x)+f_2(x)$ of $f_1(x)$ and $f_2(x)$ are $N_{f_1+f_2}$. So N_{f_1}, N_{f_2} and $N_{f_1+f_2}$ are contacted with the following triangle inequality :

$$N_{f_1}+N_{f_2}\geq N_{f_1+f_2}.$$

Proof: Suppose there exists $l_1(x),l_2(x)\in L_n[x]$ which makes

$$N_{f_1}=\min_{l(x)\in L_n[x]} w_t(f_1(x)+l(x))=w_t(f_1(x)+l_1(x)),$$

and

$$N_{f_2}=\min_{l(x)\in L_n[x]} w_t(f_2(x)+l(x))=w_t(f_2(x)+l_2(x)).$$

And there exists $l_0(x)\in L_n[x]$ which makes

$$\begin{aligned} &N_{f_1+f_2} \\ &=\min_{l(x)\in L_n[x]} w_t(f_1(x)+f_2(x)+l(x)). \\ &=w_t(f_1(x)+f_2(x)+l_0(x)) \end{aligned}$$

So

$$\begin{aligned} &w_t(f_1(x)+f_2(x)+l_1(x)+l_2(x)) \\ &\geq w_t(f_1(x)+f_2(x)+l_0(x)) \end{aligned}.$$

There are

$$\begin{aligned} &w_t(f_1(x)+f_2(x)+l_1(x)+l_2(x)) \\ &=w_t(f_1(x)+l_1(x)+f_2(x)+l_2(x)) \\ &=w_t(f_1(x)+l_1(x))+w_t(f_2(x)+l_2(x)). \\ &-2w_t(f_1(x)f_2(x)+l_1(x)f_2(x) \\ &+l_2(x)f_1(x)+l_1(x)l_2(x)) \end{aligned}$$

Therefore

$$\begin{aligned} &w_t(f_1(x)+l_1(x))+w_t(f_2(x)+l_2(x))-2w_t(f_1(x)\cdot \\ &f_2(x)+l_1(x)f_2(x)+l_2(x)f_1(x)+l_1(x)l_2(x)) \\ &\geq w_t(f_1(x)+f_2(x)+l_0(x)) \end{aligned}.$$

which is

$$\begin{aligned} &N_{f_1}+N_{f_2}-2w_t(f_1(x)f_2(x)+ \\ &l_1(x)f_2(x)+l_2(x)f_1(x)+l_1(x)l_2(x)). \\ &\geq N_{f_1+f_2} \end{aligned}$$

Due to

$$\begin{aligned} &w_t(f_1(x)f_2(x)+l_1(x)f_2(x)+l_2(x)f_1(x)+l_1(x)l_2(x)) \\ &\geq 0 \end{aligned},$$

it must be

$$N_{f_1}+N_{f_2}\geq N_{f_1+f_2}.$$

The proof ends.

$l_0(x)\in L_n[x]$ of the formula $N_{f_1+f_2}=w_t(f_1(x)+f_2(x)+l_0(x))$ in Theorem 1, can help us calculate the nonlinearity $N_{f_1f_2}$ of the product functions $f_1(x)f_2(x)$ of $f_1(x)$ and $f_2(x)$. So we can get Theorem 2.

Theorem 2: For n-variable Boolean function $f_1(x)$ and $f_2(x)$ ($f_1(x),f_2(x)\in GF(2)^{GF(2)^n}$), if there exists $l_0(x)\in L_n[x]$ which makes the nonlinearity $N_{f_1+f_2}$ of $f_1(x)+f_2(x)$ are

$$\begin{aligned} &N_{f_1+f_2} \\ &=\min_{l(x)\in L_n[x]} w_t(f_1(x)+f_2(x)+l(x)), \\ &=w_t(f_1(x)+f_2(x)+l_0(x)) \end{aligned}$$

then for $1+l_0(x)\in L_n[x]$, there must be

$$\begin{aligned} &N_{f_1f_2} \\ &=\min_{l(x)\in L_n[x]} w_t(f_1(x)f_2(x)+l(x)). \\ &=w_t(f_1(x)f_2(x)+1+l_0(x)) \end{aligned}$$

Proof: Known by the condition, there exists $l_0(x)\in L_n[x]$ which makes

$$N_{f_1+f_2} = \min_{l(x)\in L_n[x]} w_t(f_1(x)+f_2(x)+l(x))$$
$$= \min_{l(x)\in L_n[x]} (w_t(f_1(x)+f_2(x))+w_t(l(x))$$
$$-2w_t(l(x)(f_1(x)+f_2(x)))$$
$$= w_t(f_1(x)+f_2(x))+w_t(l(x))$$
$$-2\max_{l(x)\in L_n[x]} w_t(l(x)(f_1(x)+f_2(x)))$$
$$= w_t(f_1(x)+f_2(x))+w_t(l(x))$$
$$-2\max_{l(x)\in L_n[x]} w_t(l(x)(f_1(x)+f_1(x)f_2(x)))$$
$$-2\max_{l(x)\in L_n[x]} w_t(l(x)(f_2(x)+f_1(x)f_2(x)))$$
$$= w_t(f_1(x)+f_2(x))+w_t(l_0(x))$$
$$-2w_t(l_0(x)(f_1(x)+f_1(x)f_2(x)))$$
$$-2w_t(l_0(x)(f_2(x)+f_1(x)f_2(x)))$$
$$= w_t(f_1(x)+f_2(x)+l_0(x))$$

So

$$\begin{cases} w_t(l_0(x)(f_1(x)+f_1(x)f_2(x))) \\ = \max_{l(x)\in L_n[x]} w_t(l(x)(f_1(x)+f_1(x)f_2(x))) \\ w_t(l_0(x)(f_2(x)+f_1(x)f_2(x))) \\ = \max_{l(x)\in L_n[x]} w_t(l(x)(f_2(x)+f_1(x)f_2(x))) \end{cases}.$$

There are

$$\begin{cases} w_t(l_0(x)f_1(x)) - w_t(l_0(x)f_1(x)f_2(x))) \\ = \max_{l(x)\in L_n[x]} (w_t(l(x)f_1(x)) - w_t(l(x)f_1(x)f_2(x))) \\ w_t(l_0(x)f_2(x)) - w_t(l_0(x)f_1(x)f_2(x))) \\ = \max_{l(x)\in L_n[x]} (w_t(l(x)f_2(x)) - w_t(l(x)f_1(x)f_2(x))) \end{cases}.$$

So

$$w_t(l_0(x)f_1(x)f_2(x)) = \min_{l(x)\in L_n[x]} w_t(l(x)f_1(x)f_2(x)).$$

So there have

$$C_{f_1f_2} = \max_{l(x)\in L_n[x]} w_t(f_1(x)f_2(x)+l(x))$$
$$= \max_{l(x)\in L_n[x]} (w_t(f_1(x)f_2(x))+w_t(l(x))$$
$$-2w_t(l(x)f_1(x)f_2(x)))$$
$$= w_t(f_1(x)f_2(x))+w_t(l(x))$$
$$-2\min_{l(x)\in L_n[x]} w_t(l(x)f_1(x)f_2(x))$$
$$= w_t(f_1(x)f_2(x))+w_t(l_0(x))$$
$$-2w_t(l_0(x)f_1(x)f_2(x))$$
$$= w_t(f_1(x)f_2(x)+l_0(x))$$

Therefore

$$w_t(f_1(x)f_2(x)+1+l_0(x))$$
$$= 2^n - w_t(f_1(x)f_2(x)+l_0(x))$$
$$= 2^n - C_{f_1f_2}$$
$$= N_{f_1f_2}$$

That is

$$N_{f_1f_2} = \min_{l(x)\in L_n[x]} w_t(f_1(x)f_2(x)+l(x))$$
$$= w_t(f_1(x)f_2(x)+1+l_0(x))$$

The proof ends.

Theorem 1&2 reveal that the nonlinearity of the sum of the two Boolean functions is not more than the sum of nonlinearity of two functions, and nonlinearity of the sum of the two functions and the nonlinearity of product of two functions. For the nonlinearity of the sum of two functions with two functions of the relationship between the nonlinearity of a single function, need to use e-derivative and derivative to discuss, back to do the work.

4 The nonlinearity of Boolean functions with the derivative and e-derivative

In Theorem 3, we will discuss the relationship between the nonlinearity of the sum of two Boolean functions, and the nonlinearity of a single function.

Theorem 3: Suppose Boolean functions $f_1(x), f_2(x) \in GF(2)^{GF(2)^n}$. There are $w_t(f_1(x)) > 2^{n-1}$, $w_t(f_2(x)) > 2^{n-1}$, and

$$\deg e(f_1(x)f_2(x))/ex_n = \deg ef_1(x)/ex_n$$
$$= \deg ef_2(x)/ex_n = 1.$$

1) If

$$w_t(f_1(x)df_1(x)/dx_n + f_2(x)df_2(x)/dx_n) < 2^{n-2},$$

then $\begin{cases} N_{f_1+f_2} > N_{f_1} \\ N_{f_1+f_2} > N_{f_2} \end{cases}$.

2) If

$$w_t(f_1(x)df_1(x)/dx_n) + w_t(f_1(x)df_1(x)/dx_n + f_2(x)df_2(x)/dx_n) \geq 2^{n-1},$$

and $2^{n-2} \geq w_t(f_2(x)df_2(x)/dx_n) \geq w_t(f_1(x)df_1(x)/dx_n)$, then $N_{f_1+f_2} \leq N_{f_1} \leq N_{f_2}$ and

$$w_t(f_1(x)df_1(x)/dx_n + f_2(x)df_2(x)/dx_n) \geq 2^{n-2}.$$

3) There are

$$N_{f_1f_2} = w_t(f_1(x)df_1(x)/dx_n \cdot f_2(x)df_2(x)/dx_n).$$

4) There are $N_{f_1+f_2} = 2^n - N_{f_1} - N_{f_2} + 2N_{f_1f_2}$.

Proof: Because

$$\deg e(f_1(x)f_2(x))/ex_n = \deg ef_1(x)/ex_n$$
$$= \deg ef_2(x)/ex_n = 1,$$

so

$$e(f_1(x)f_2(x))/ex_n = ef_1(x)/ex_n \cdot ef_2(x)/ex_n$$
$$= ef_1(x)/ex_n = ef_2(x)/ex_n,$$

and $e(f_1(x)f_2(x))/ex_n \in L_n[x]$.

Known by Lemma and conditions $w_t(f_1(x)) > 2^{n-1}$ and $w_t(f_2(x)) > 2^{n-1}$,

$$\begin{cases} w_t(f_1(x)df_1(x)/dx_n) \leq 2^{n-2} \\ w_t(f_2(x)df_2(x)/dx_n) \leq 2^{n-2} \end{cases},$$

and

$$df_1(x)/dx_n ef_2(x)/ex_n = df_2(x)/dx_n ef_1(x)/ex_n$$
$$= df_1(x)/dx_n ef_1(x)/ex_n = df_2(x)/dx_n ef_2(x)/ex_n = 0.$$

So

$$
\begin{aligned}
&f_1(x)+f_2(x)\\
&=(f_1(x)df_1(x)/dx_n+ef_1(x)/ex_n)\\
&+(f_2(x)df_2(x)/dx_n+ef_2(x)/ex_n)\\
&=f_1(x)df_1(x)/dx_n+f_2(x)df_2(x)/dx_n
\end{aligned}
,
$$

and

$$
\begin{aligned}
&f_1(x)f_2(x)\\
&=f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n\\
&+f_2(x)df_2(x)/dx_nef_1(x)/ex_n+\\
&f_1(x)df_1(x)/dx_nef_2(x)/ex_n\\
&+ef_1(x)/ex_nef_2(x)/ex_n\\
&=f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n\\
&+ef_1(x)f_2(x)/ex_n
\end{aligned}
.
$$

Take $l_0(x)=ef_1(x)f_2(x)/ex_n\in L_n[x]$, there are

$$
\begin{aligned}
&N_{f_1+f_2}\\
&=\min_{l(x)\in L_n[x]}w_t(f_1(x)df_1(x)/dx_n\\
&+f_2(x)df_2(x)/dx_n+l(x))\\
&=w_t(f_1(x)df_1(x)/dx_n+f_2(x)df_2(x)/dx_n, \qquad (3)\\
&+1+l_0(x))\\
&=2^n-w_t(f_1(x)df_1(x)/dx_n\\
&+f_2(x)df_2(x)/dx_n)
\end{aligned}
$$

$$
\begin{aligned}
&N_{f_1}=\min_{l(x)\in L_n[x]}w_t(f_1(x)+l(x))\\
&=w_t(f_1(x)+l_0(x))=w_t(f_1(x)df_1(x)/dx_n)
\end{aligned}
, \qquad (4)
$$

$$
\begin{aligned}
&N_{f_2}=\min_{l(x)\in L_n[x]}w_t(f_2(x)+l(x))\\
&=w_t(f_2(x)+l_0(x))=w_t(f_2(x)df_2(x)/dx_n)
\end{aligned}
, \qquad (5)
$$

and

$$
\begin{aligned}
&N_{f_1f_2}\\
&=\min_{l(x)\in L_n[x]}w_t(f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n\\
&+ef_1(x)f_2(x)/ex_n+l(x))\\
&=w_t(f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n\\
&+ef_1(x)f_2(x)/ex_n+l_0(x))\\
&=w_t(f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n)
\end{aligned}
. \qquad (6)
$$

1) When

$w_t(f_1(x)df_1(x)/dx_n+f_2(x)df_2(x)/dx_n)<2^{n-2}$,

due to obtained permits $w_t(f_1(x)df_1(x)/dx_n)\le 2^{n-2}$, and $w_t(f_2(x)df_2(x)/dx_n)\le 2^{n-2}$, then known by (3), (4) and (5), there are

$$
\begin{cases}
N_{f_1+f_2}>N_{f_1}\\
N_{f_1+f_2}>N_{f_2}
\end{cases}
.
$$

2) From the conditions, (3), (4) and (5), at a glance there are

$$N_{f_1+f_2}\le N_{f_1}\le N_{f_2}$$

and

$$w_t(f_1(x)df_1(x)/dx_n+f_2(x)df_2(x)/dx_n)\ge 2^{n-2}.$$

3) (6) already shows the results.

4) expanding (3), binding (4) and (5), there are

$$
\begin{aligned}
&N_{f_1+f_2}\\
&=2^n-w_t(f_1(x)df_1(x)/dx_n)-w_t(f_2(x)df_2(x)/dx_n)\\
&+2w_t(f_1(x)df_1(x)/dx_nf_2(x)df_2(x)/dx_n)\\
&=2^n-N_{f_1}-N_{f_2}+2N_{f_1f_2}
\end{aligned}
.
$$

The proof ends.

Known from Theorem 3, when comparing the nonlinearity of the sum of two Boolean functions with each of the two functions under different conditions, it comes to different results . Under certain conditions, the nonlinearity of the sum and the product of two Boolean functions can establish contact.

In the following Theorem 4, using the derivative and e-derivative, we will discuss the nonlinearity of a class of separable variables Boolean function.

Theorem 4: If n is even, $\{y\}=\left\{x_1,x_2,\cdots,x_{\frac{n}{2}}\right\}$, $\{z\}=\left\{x_{\frac{n}{2}+1},x_{\frac{n}{2}+2},\cdots,x_n\right\}$, $\{x\}=\{x_1,x_2,\cdots,x_n\}$. There are $f(x)=R(y)S(z)$, $\deg dR(y)/dx_{\frac{n}{2}}=1$, $\deg dS(z)/dx_n=1$, $w_t(eS(z)/ex_n)<2^{n-2}$, and $w_t(eR(y)/ex_{\frac{n}{2}})<2^{n-2}$. Then there are

$$
\begin{aligned}
&N_f=w_t((1+S(z))R(y)dS(z)/dx_n)\\
&+w_t(R(y)eS(z)/ex_n)\\
&=w_t((1+R(y))S(z)dR(y)/dx_{\frac{n}{2}})\\
&+w_t(S(z)eR(y)/ex_{\frac{n}{2}})
\end{aligned}
,
$$

and

$$
\begin{cases}
2^{n-2}<N_{S(z)}<2^{n-1}\\
2^{n-2}<N_{R(y)}<2^{n-1}
\end{cases}
.
$$

Proof: Known by the condition $\deg dS(z)/dx_n=1$, there are

$$
\begin{aligned}
&w_t(S(z)dS(z)/dx_n)=w_t((1+S(z))dS(z)/dx_n)\\
&=2^{-1}w_t(dS(z)/dx_n)=2^{n-2}
\end{aligned}
.
$$

Also, because $w_t(eS(z)/ex_n)<2^{n-2}$, known by Lemma, there are $2^{n-2}<w_t(S(z))<2^{n-1}$.

Because the value of the structure of $eS(z)/ex_n$ and $S(z)dS(z)/dx_n$ is different, i.e. at x in $eS(z)/ex_n=1$, $dS(z)/dx_n=0$. And each linear function has only a single the value of the structure. Therefore,

$$
\begin{aligned}
&N_{S(z)}=\min_{l(x)\in L_n[x]}w_t(S(z)+l(x))\\
&=w_t(S(z)+dS(z)/dx_n)\\
&=w_t(S(z))+w_t(dS(z)/dx_n)-2w_t(S(z)dS(z)/dx_n)\\
&=w_t(S(z))
\end{aligned}
.
$$

So $2^{n-2}<N_{S(z)}<2^{n-1}$, and

$$\max_{l(x)\in L_n[x]}w_t(l(x)S(z))=w_t(S(z)dS(z)/dx_n).$$

So

$$\max_{l(x)\in L_n[x]} w_t(R(y)S(z)l(x)) = w_t(R(y)S(z)dS(z)/dx_n).$$

Therefore

$$\begin{aligned} N_f &= \min_{l(x)\in L_n[x]} w_t(R(y)S(z)+l(x)) \\ &= w_t(R(y)S(z)+dS(z)/dx_n) \\ &= w_t((1+S(z))R(y)dS(z)/dx_n) \\ &+w_t(R(y)eS(z)/ex_n) \end{aligned}.$$

Since $R(y)$ has the same conditions with $S(z)$ correspondingly, through the same deduction, we can get

$$2^{n-2} < N_{R(y)} < 2^{n-1}.$$

Also

$$\begin{aligned} &N_f \\ &= w_t((1+R(y))S(z)dR(y)/dx_{\frac{n}{2}}). \\ &+w_t(eR(y)/ex_{\frac{n}{2}}S(z)) \end{aligned}$$

The proof ends.

Known from the proof of Theorem 4 , if $R(y)$ is changed while $S(z)$ remains the same , $2^{n-2} < N_{S(z)} = w_t(S(z)) < 2^{n-1}$ and $N_f = w_t((1+S(z))R(y)dS(z)/dx_n) + w_t(R(y)eS(z)/ex_n)$ still hold. So, if taking $R(y) = x_1x_2\cdots x_{\frac{n}{2}}$, we can get

$$\begin{aligned} N_f &= w_t(dS(z)/dx_n) + w_t(R(y)S(z)) \\ &-2w_t(R(y)S(z)dS(z)/dx_n) \\ &= 2^{n-1} + 2^{-1}\cdot 2^{\frac{n}{2}} - 2\cdot 2^{\frac{n}{2}-1} \\ &= 2^{n-1} - 2^{\frac{n}{2}-1} \end{aligned}.$$

Then there are following Corollary.

Corollary: In Theorem 4, if taken $R(y) = x_1x_2\cdots x_{\frac{n}{2}}$, $S(z)$ unchanged, then for $f(x) = R(y)S(z)$, there have

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

It found that there exists functions with high nonlinearity in the function $f(x) = R(y)S(z)$ which variables can be separable .

5 Conclusions

The nonlinearity of the sum of Boolean functions can be roughly estimated by the triangle inequality , so the triangle inequality has its practical significance. The relationship among triangle inequality, and the nonlinearity of the sum and the product of two Boolean functions in Theorem 2, plays a role on constructing Boolean functions with higher nonlinearity.

To estimate the lower bound of the nonlinearity of the sum of two Boolean functions,we can use derivatives and e-derivative to analysis as Theorem 3 . It shows that using the derivative and e- derivative to study nonlinearity of Boolean function is very useful.

Acknowledgment

This work is supported by National Natural Science Foundation of China (Grant No. 61262085).

References

1. Courtois, N., and Meier, W. Algebraic attacks on stream ciphers with linear feedback. Advances in Cryptology-EUROCRYPT 2003, Warsaw, Poland, 2003, LNCS, 2656:345-359.
2. Carlet C and Zeng X Y. Further properties of several classes of Boolean functions with optimum algebraic immunity.Designs, Codes and Cryptography, 2009, 52(3): 303-338.
3. Carlet C. A method of construction of balanced functions with optimum algebraic immunity. Proceedings of the First International Workshop on Coding and Cryptography, Fujian, 2007: 25-43.
4. Li Y, Yang M, and Kan H B. Constructing and counting Boolean functions on even variables with maximum algebraic immunity. IEICE Transactions on Fundamentals, 93-A(3): 640-643(2010).
5. Rizomiliotis P. On the resistance of Boolean functions against algebraic attacks using univariate polynomial representation[J]. IEEE Transactions on Information Theory, 56(8):4014-4024(2010).
6. Tu Z R and Deng Y P. A class of 1-resilient function with high nonlinearity and algebraic immunity. Ryptography ePrint Archive, Report 2010, 2010/179.
7. Wang Q, Peng J, Kan H, et al.. Constructions of cryptographically significant Boolean functions using primitive polynomials. IEEE Transactions on Information Theory, 56(6): 3048-3053(2010).
8. Li, C.,Zhang, H.,Zeng, X, et al. The lower bound on the second-order nonlinearity for a class of Bent functions. Chinese Journal of Computers, 35(8):1588-1593(2012).
9. Su S H, Tang X H. Construction of rotation symmetric Boolean functions with optimal algebraic immunity and high nonlinearity. Designs, Codes and Cryptography, 71(2): 183–199(2014).
10. J. Huang, Z. Wang. The relationship between correlation immune and weight of H Boolean functions. Journal on Communications, Vol.33(2):110-118(2012). (In Chinese)
11. W. Li, Z. Wang, J. Huang. The e-derivative of boolean functions and its application in the fault detection and cryptographic system. Kybernetes, Vol.40(5-6):905-911(2011).
12. Zhao, M.. Method of detecting special logic function based on Boolean e-derivative. Journal of Zhejiang University (Science Edition), 41(4):424-426(2014).