On Relevance of Nonlinearity, Derivative, and E-Derivative for Boolean Functions

Jing-Lian HUANG\textsuperscript{a,\textdagger}, Zhuo WANG\textsuperscript{b}

School of Electrical Engineering, Northwest University for Nationalities, Lanzhou, China
\textsuperscript{a}huangjwork@163.com, \textsuperscript{b}wzh0902@126.com

\textdagger Corresponding author

Keywords: Boolean functions, Derivative, E-derivative, Nonlinearity, Solution.

Abstract. In this paper, we discuss the impact of weight structure of the derivative and e-derivative on the nonlinearity of Boolean functions, and the relationship among the nonlinearity, derivative, and e-derivative of Boolean functions. And get six kinds of relations among nonlinearity, derivative, and e-derivative of Boolean functions. The methods to solve the nonlinearity are derived based on those relationships, thus solving the problem that it’s difficult to calculate the nonlinearity only in accordance with the definition.

Introduction 

The properties of Boolean functions, such as the nature linear complexity, the nonlinearity \cite{2}, the proliferation, correlation immunity, algebraic immunity and so on, are necessary properties to resist a variety of cryptography password attacks \cite{1-5}. Looking for Boolean functions with a variety of high index cryptographic properties of Boolean functions are cryptographic properties of the important research work task. The high nonlinearity of Boolean functions is important properties of affine cryptosystem resist attack. High nonlinearity of Boolean functions of existence and other issues are also important work \cite{6-8}.

The nonlinearity of Boolean function is a nonlinear index to measure the resistance of a password system to an affine approximation attack. The higher the nonlinearity of Boolean functions, the stronger the ability to resist the affine approximation attacks \cite{6-7}. The nonlinearity of Boolean functions \( N \) has always been defined by the definition \( N = \min_{l \in \mathcal{L}_x} \omega'(f(x) + l(x)) \), which requires us to find a linear function \( l^*(x) \) through the collection \( \mathcal{L}_x \) of \( 2^n \) linear functions, so \( N = \omega'(f(x) + l^*(x)) \) can be satisfied. But it is tough to find \( l^*(x) \) \cite{8}.

On the study of cryptography properties of Boolean functions, the main research methods \cite{1-8} we take are as follows, such as the methods of algebraic analysis, spectral analysis, matrix analysis, weighting analysis, linear subspace analysis and cascade analysis. Using these methods, we analyze the whole values of Boolean functions, but cannot differentiate values of Boolean functions’ two different properties. Therefore we cannot find the relation between values of Boolean functions’ two different properties and properties of Boolean functions.

The derivative of Boolean function, also known as difference, was proposed long ago. The derivative of Boolean function doesn’t play a significant role when it is used alone in studying the properties of Boolean functions. So we cannot find the trace of the derivative of Boolean function in studying the properties of Boolean functions. Using the derivative of Boolean function expresses the values of one property of Boolean functions, and the values of another property of Boolean functions can be reflected by the e-derivative which defined by ourselves. Using the derivative and the e-derivative as main research tools to study the cryptographic properties of Boolean functions, we can reveal the relation between values of Boolean functions’ two different properties and properties of
Boolean functions. So we will find more useful results through researching properties of Boolean functions from a broad and sufficient view.

The Boolean function is formed by its derivative and its e-derivative [9~10]. This paper reveals the impacts of the derivative and e-derivative on the nonlinearity of Boolean functions, through respectively discussing the relationship of the linear function, derivative and e-derivative of Boolean functions. At the same time, the method to calculate \(f_i(x)\) with the derivative and e-derivative is gotten, so \(N_j\) can also be solved. So the hard-solved calculation of the nonlinearity of Boolean functions has got its solution.

## Preliminaries

The Boolean functions of cryptographic are defined on Galois field \(GF(2)\), i.e. \(f(x) = f(x_1, x_2, \ldots, x_n) \in GF(2)^{GF(2)^n}\). In this paper, we discuss cryptographic properties of H Boolean functions on \(GF(2)\).

To study cryptographic properties of H Boolean functions, we proposed the concept of the e-derivative. The e-derivative [9~10] and derivative [11] are defined here as Definition 1&2.

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

\[
ef(x) / ex_i = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) (1 \leq r \leq n)
\]

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

\[
ef(x) / ex_i = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) (i = 1, 2, \ldots, n).
\]

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

\[
df(x) / \partial x_i = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) + f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) (1 \leq r \leq n)
\]

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

\[
df(x) / dx_i = f(x_1, x_2, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) + f(x_1, x_2, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) (i = 1, 2, \ldots, n).
\]

**Remark:** Obviously, From Definition 1&2, there are \(df(x) / dx_i \cdot ef(x) / ex_i = 0 (i = 1, 2, \ldots, n)\) for Boolean functions \(f(x) = f(x_1, x_2, \ldots, x_n) \in GF(2)^{GF(2)^n}\). So, e-derivative and derivative represent the values of two properties of Boolean functions: on one hand, there is \(ef(x) / ex_i = 0\) at \(x\) which satisfies \(df(x) / dx_i = 1\); on another hand, there is \(df(x) / dx_i = 0\) at \(x\) which satisfies \(ef(x) / ex_i = 1\).

According to Definition 1&2, we can get Lemmas easily.

**Lemma 1:**

1) A Boolean function is a function with propagation of degree \(r\) iff \(w_i(df(x) / \partial x_i) = 2^{-r} (1 \leq i \leq n, 1 \leq r \leq n, 1 \leq i_i \leq i_i \leq \cdots \leq i_i \leq n)\).

2) A Boolean function \(f(x)\) is an H Boolean function iff the following equations hold for all \(x_i (i = 1, 2, \ldots, n)\):

\[
w_i(df(x) / dx_i) = 2^{-r} (i = 1, 2, \ldots, n).
\]
Lemma 2: For any arbitrary Boolean function \( f(x) \), the following equations are true:

\[
f(x) = f(x)df(x)/dx_i + ef(x)/ex_i \quad (i = 1, 2, \cdots, n),
\]

and

\[
w_i(f(x)) = w_i(f(x)df(x)/dx_i) + w_i(ef(x)/ex_i) \quad (i = 1, 2, \cdots, n).
\]

Calling \( f(x)df(x)/dx_i \) is derivative part of \( f(x) \), and \( ef(x)/ex_i \) is e-derivative of \( f(x) \).

The Linear Function and Weight of Derivative, and E-Derivative

Since nonlinearity of Boolean functions and linear function \( l(x) \) are closely related, and the weight of \( l(x) \) is \( w_i(l(x)) = 2^{n-1} \), we first discuss the relationship between quantity \( 2^{n-1} \) and the weight of derivative and e-derivative, which can provide us with reference to discuss the nonlinearity of Boolean functions.

In Theorem 1, we firstly discuss the features of \( R(y) \) and \( S(x) \) when \( f(x) \) are H Boolean functions.

Note the collection of all \( n \)-variable Boolean function as \( f[x] \).

**Theorem 1:** For any \( f(x) \in f[x] \), there must be \( \max_{f(x)\in f[x]} w_i(f(x)df(x)/dx_i) = 2^{n-1} \).

**Proof:** Because \( \max_{f(x)\in f[x]} w_i(f(x)) = w_i(1) = 2^n \), but the function 1 does not contain the value 0, so the function 1 can only be represented by \( df(x)/dx_n \) or \( ef(x)/ex_n \).

Known by Lemma, there are \( w_i(f(x)) = w_i(f(x)df(x)/dx_n) + w_i(ef(x)/ex_n) \). Take \( ef(x)/ex_n = 0 \), i.e., when \( w_i(ef(x)/ex_n) = 0 \) and only \( w_i(df(x)/dx_n) = 2^n \), \( w_i(f(x)df(x)/dx_n) \) are maximum value. Therefore

\[
\max_{f(x)\in f[x]} w_i(f(x)df(x)/dx_n) = 2^{n-1} \quad \max_{f(x)\in f[x]} w_i(df(x)/dx_n) = 2^n.
\]

The proof ends.

**Theorem 2:** For any \( f(x) \in f[x] \), if \( w_i(ef(x)/ex_n) = 2^{n-1} \), then \( \max_{f(x)\in f[x]} w_i(f(x)df(x)/dx_n) = 2^{n-2} \).

**Proof:** Due to \( w_i(ef(x)/ex_n) = 2^{n-1} \), and \( \max_{f(x)\in f[x]} w_i(f(x)) = 2^n \), therefore

\[
\max_{f(x)\in f[x]} w_i(df(x)/dx_n) = 2^n - 2^{n-1} = 2^{n-1}.
\]

So

\[
\max_{f(x)\in f[x]} w_i(f(x)df(x)/dx_n) = 2^{n-1} \quad \max_{f(x)\in f[x]} w_i(df(x)/dx_n) = 2^{n-2}.
\]

The proof ends.

Theorems 1&2 are founded, so when discussing the nonlinearity of Boolean functions, we only need to concern the situation when \( w_i(ef(x)/ex_n) \leq 2^{n-1} \). In most cases, we can only discuss this situation when \( w_i(ef(x)/ex_n) \leq 2^{n-1} \) and \( w_i(f(x)df(x)/dx_n) \leq 2^{n-2} \).

The relationship of nonlinearity, derivative, and e-derivative of Boolean functions

In this section, we discuss the relationship among the nonlinearity, the algebraic immunity, derivative, and e-derivative of Boolean functions.

**Theorem 3:** For \( f(x) \in GF(2)^{GF(2)^r} \),

1) If \( w_i(f(x)df(x)/dx_n) = 0 \), and \( w_i(ef(x)/ex_n) = 2^{n-1} \), \( AI(f(x)) = 1 \), then \( N_f = 0 \);  

2) If \( w_i(ef(x)/ex_n) = 0 \), and \( w_i(f(x)df(x)/dx_n) = 2^{n-1} \), \( AI(f(x)) = 1 \), then \( N_f = 0 \).

Theorem 3 is clearly established. Since \( AI(f(x)) = 1 \) and \( w_i(ef(x)/ex_n) = 2^{n-1} \), \( f(x) \) is a linear function; or since \( w_i(ef(x)/ex_n) = 0 \) and \( w_i(f(x)df(x)/dx_n) = 2^{n-1} \), \( f(x) \) is also a linear function. So, we always have \( N_f = 0 \). And we don't have to prove in detail.

**Theorem 4:** For \( f(x) \in GF(2)^{GF(2)^r} \), if \( w_i(ef(x)/ex_n) = 2^{n-1} \) and \( AI(f(x)) = 1 \), then
\[ N_f = \min_{t \in [s]} w_t(f(x)/dx_n) = 2^{n-2}. \]

**Proof:** Known by the conditions \( w_t(ef(x)/ex_n) = 2^{n-1} \), there must be
\[ w_t(f(x)/dx_n) \leq 2^{n-2}. \]
And known by \( AI(f(x)) = 1 \), \( ef(x)/ex_n \) must be linear functions. Because of \( ef(x)/ex_n \cdot df(x)/dx_n = 0 \), there are
\[ ef(x)/ex_n(1+f(x)) = ef(x)/ex_n + ef(x)/ex_n f(x) = ef(x)/ex_n + ef(x)/ex_n = 0. \]
That is \( ef(x)/ex_n \) are annihilators of the lowest algebraic degree of \( 1+f(x) \).
Selection \( l_\theta(x) = ef(x)/ex_n \), there are
\[ N_f = \min_{t \in [s]} w_t(f(x) + l(\theta)) = w_t(f(x) + l_\theta(x)) = w_t(f(x)df(x)/dx_n) \leq 2^{n-2}. \]
The proof ends.

**Theorem 5:** For \( f(x) \in GF(2) \), if \( ef(x)/ex_n = 0 \), \( w_t(e(1+f(x))/ex_n) = 2^{n-1} \) and \( AI(f(x)) = 1 \), then
\[ 2^{n-1} > N_f = 2^n - w_t(f(x)df(x)/dx_n) \geq 2^{n-2}. \]

**Proof:** Because \( w_t(e(1+f(x))/ex_n) = 2^{n-1} \), so
\[ w_t((1+f(x))d(1+f(x))/dx_n) \leq 2^{n-2}. \]
Which is
\[ w_t(df(x)/dx_n) - w_t(f(x)df(x)/dx_n) \leq 2^{n-2}, \]
and
\[ \max w_t(d(1+f(x))/dx_n) = \max w_t(df(x)/dx_n) = 2^{n-1}. \]
So, \( w_t(f(x)df(x)/dx_n) \leq 2^{n-2}. \)
And known from \( ef(x)/ex_n = 0 \), \( w_t(e(1+f(x))/ex_n) = 2^{n-1} \) and \( AI(f(x)) = 1 \), \( e(1+f(x))/ex_n \) are linear functions. Take \( l_\theta(x) = 1+e(1+f(x))/ex_n \), there are
\[ 2^{n-1} > N_f = \min_{t \in [s]} w_t(f(x) + l(\theta)) = w_t(f(x) + l_\theta(x)) = 2^{n-1} - w_t(f(x)df(x)/dx_n) \geq 2^{n-2}. \]
The proof ends.

**Theorem 6:** For \( f(x) \in GF(2) \), if \( w_t(f(x)df(x)/dx_n) = 2^{n-2} \), and \( AI(f(x)) = 1 \),
\[ 2^{n-2} \leq w_t(ef(x)/ex_n) < 2^{n-1} \], then
\[ N_f = 2^{n-2} + w_t(ef(x)/ex_n). \]

**Proof:** Because \( d(f(x)df(x)/dx_n)/dx_n = df(x)/dx_n, \) and \( w_t(f(x)df(x)/dx_n) = 2^{n-2}, \) so
\[ w_t(df(x)/dx_n) = 2^{n-1}. \]
Since \( AI(f(x)) = 1 \) and \( 2^{n-2} \leq w_t(ef(x)/ex_n) < 2^{n-1} \), \( df(x)/dx_n \) is a linear function, and \( f(x)df(x)/dx_n \) cannot form a linear function with part of \( ef(x)/ex_n \) together.
So take \( l_\theta(x) = df(x)/dx_n \), there are
\[ N_f = \min_{t \in [s]} w_t(f(x) + l(\theta)) = w_t(f(x) + l_\theta(x)) = w_t((1+f(x))df(x)/dx_n) + w_t(ef(x)/ex_n) \]
\[ = 2^{n-2} + w_t(ef(x)/ex_n). \]
The proof ends.
By Theorem 6, we can obtain the following important corollary.

**Corollary:** For Boolean function \( f(x) \) in Theorem 6, if \( w_t(ef(x)/ex_n) = 2^{n-2} - 2^{n-1} \), then
\[ N_f = 2^{n-2} - 2^{n-1}. \]
Corollary 1 is clearly established, so we won’t prove it in detail.
Following, we verify the above Theorem via Example.

**Example:** Suppose a Boolean function \( f(x) = x_1x_2 + x_2x_3 + x_3x_7 + x_4x_8 + x_5x_2x_3 + x_1x_2x_3x_4 \), there are
\[ f(x)df(x)/dx_n = x_1x_2x_3 + x_1x_2x_3 + x_1x_2 + x_1x_3 + x_1x_2x_3 + x_1x_2x_3. \]
Conclusions

The results of this paper show that, the nonlinearity of Boolean functions is decided by the structure of Boolean functions’ derivative and e-derivative. As long as we find the relationship among derivative, e-derivative and linear functions of Boolean functions, it is easy to calculate the nonlinearity of Boolean function.

Although the weight of the derivative and the e-derivative took special value, it also offers the standard on the value of the weight by a certain measure. Referring to these standards, it is easy to find relationship among the derivative, e-derivative and the linear functions of any Boolean functions, thus obtaining the arbitrary nonlinearity of any Boolean functions. In the future, we can also discuss the relationship among the derivative, e-derivative and nonlinearity of any Boolean functions.

Acknowledgement

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

References