RESEARCH ON PROPERTIES OF E-PARTIAL DERIVATIVE OF LOGIC FUNCTIONS

[1]WANG FANG

[1]Dept. of Computer and Information Technology, Zhejiang Changzheng Vocational and Technical College, Hangzhou 310023; 2.Dept. of Information and Electronics Engineering, Zhejiang University, Hangzhou 310028

E-mail: [1]595297508@qq.com

ABSTRACT

E-derivative [1] has accessed a wide range of applications in these areas and caused academia concerned [1-4], such as detecting faults in combinational circuits, discussing on cryptographic properties of H-Boolean function and revealing the internal structure of Boolean function together with Boolean derivative, thus more effectively analyzing the property of Boolean functions. Referring to the discussion on Boolean derivative and Boolean partial derivative, the concept of e-partial derivative is presented. The definitions and properties of e-partial derivative and high order e-partial derivative are given. We also give their proofs for some properties. The work made in this paper is the complement and improvement of the research on the e-derivative of logic functions.

Key words: *Logic Function; e-Derivative; e-Partial Derivative; Special Operation Of Logic Function*

1. INTRODUCTIONS

Logic function e- derivative is a new special operation. Since the document [1] puts forward e-derivative, due to the unique characteristics of e-derivative, it has accessed a wide range of applications in these areas and caused academia concerned [1-4], such as detecting faults in combinational circuits, discussing on cryptographic properties of H-Boolean function and revealing the internal structure of Boolean function together with Boolean derivative, thus more effectively analyzing the property of Boolean functions. However, the document [1-4] simply discusses definition, properties and application of the first order e-derivative of logic function, the high order e-derivative and e-partial derivative is a lack of research. Referring to the discussion of Boolean derivative and Boolean partial derivative of logic function, this article will study the logic function e-partial derivative and its properties, and proof of some properties are given out, thus makes further complement and perfection of e-derivative study, in order to promote research on special operations.

2. DEFINITION AND RELEVANT PROPERTY OF e- PARTIAL DERIVATIVE

Document [1] introduces definitions and properties of e-derivative, and this article just takes some relevant properties for example.

Definition1 set $f\left(x_1{\sim}x_n\right)$ as variable n fully defined logic functions, definition of e-derivative to the variables x_i is:

$$\frac{ef\left(x_1{\sim}x_n\right)}{ex_i} \qquad (1.1)$$

$$\equiv f\left(x_1\cdots x_i\cdots x_n\right)\cdot f\left(x_1\cdots \overline{x_i}\cdots x_n\right)$$

Property 1.1

$$\frac{ef}{ex_i} \qquad (1.2)$$

$$= f\left(x_1\cdots 1\cdots x_n\right)\cdot f\left(x_1\cdots 0\cdots x_n\right)$$

Property1 $\frac{ef}{e\overline{x_i}} = \frac{ef}{ex_i}$ （1.3 ）

Property 1.3 $\frac{e\left(f\cdot g\right)}{ex_i} = \frac{ef}{ex_i}\cdot\frac{eg}{ex_i}$ （1.4）

Property 1.4 $\frac{ef}{ex_i}\cdot\frac{df}{dx_i}=0$ （1.5）

Formula $\frac{df}{dx_i}$ is the Boolean Difference, first order e-partial derivative.

Property 1.5 $\frac{e(f\cdot g)}{ex_i}\cdot\frac{e(f\oplus g)}{ex_i}=0$ （1.6）

Formula “ $\oplus$ ” means XOR(exclusive OR)

Property 1.6 $\frac{ef}{ex_i}\cdot\frac{d(f\oplus g)}{dx_i}=\frac{ef}{ex_i}\cdot\frac{dg}{dx_i}$ （1.7）

Property 1.7 IF f has no relationship with x_i, THEN $\frac{ef}{ex_i}=f$ （1.8） Property1.8 IF variable x_i is the linear variable of f ,THEN $\frac{ef}{ex_i}=0$ （1.9）

Property 1.9 IF $\frac{df}{dx_i}=1$，

THEN $\frac{ef}{ex_i}=0$ （1.10）

Property 1.10 IF $\frac{ef}{ex_i}=1$，

THEN $\frac{df}{dx_i}=0$ （1.11）

3. DEFINITION AND RELEVANT PROPERTY OF e-PARTIAL DERIVATIVE

Definition2 set $f\left(x_1{\sim}x_n\right)$ as variable n fully defined logic functions, first order e -partial derivative f to the variables x_i is e-derivative.

Definition 3 set $f\left(x_1{\sim}x_n\right)$ as variable n fully defined logic functions, definition of second order e- partial derivative f to the variables x_i 、 x_j is:

$$\frac{e^2 f}{ex_i ex_j}\equiv\frac{e}{ex_i}\left(\frac{ef}{ex_j}\right) \qquad （2.1）$$

Definition 4 set $f\left(x_1{\sim}x_n\right)$ as variable n fully defined logic functions, definition of K order e-partial derivative f to the variables $x_{i_1}{\sim}x_{i_K}$ is:

$$\frac{e^K f}{ex_{i_1}\sim ex_{i_K}}\equiv\frac{e}{ex_{i_1}}\left(\frac{e}{ex_{i2}}\cdots\left(\frac{ef}{ex_{i_K}}\right)\cdots\right) \qquad （2.2）$$

Many properties of the e-partial derivatives can be directly deduced according to the definition of e-partial derivatives and related properties in § 1, here only gives proof of some properties.

Property 2.1 $\frac{e^2 f}{ex_i ex_j}=\frac{e^2 f}{ex_j ex_i}$ （2.3）

Deduction2.1 $\frac{e^K f}{ex_{i_1}{\sim}ex_{i_K}}=\frac{e^K f}{ex_{i_2}ex_{i_1}{\sim}ex_{i_K}}$ （2.4）

$$=\cdots=\frac{e^K f}{ex_{i_K}{\sim}ex_{i_1}}$$

Property 2.2 $\frac{e^2 f}{ex_i ex_i}=\frac{ef}{ex_i}$ （2.5）

Deduction 2.2 $\frac{e^K f}{\underbrace{ex_i{\sim}ex_i}_{K}}=\frac{ef}{ex_i}$ （2.6）

Property 2.3 $\frac{e^2 f}{ex_i ex_j}$ （2.7）

$$=f(00)\,f(01)\,f(10)\,f(11)$$

Proof

$$\frac{e^2 f}{ex_i ex_j}=\frac{e}{ex_i}\left(f(x_i 0)f(x_i 1)\right)=f(00)f(01)f(10)f(11)$$

Deduction2.3

$$\frac{e^K f}{ex_{i_1}{\sim}ex_{i_K}} \qquad （2.8）$$

$$=f(0\cdots00)\,f(0\cdots01)\cdots f(1\cdots10)\,f(1\cdots11)$$

Property 2.4 $\frac{e^2 f}{ex_i ex_j}=\frac{e^2 f}{e\left(x_i,x_j\right)}\frac{ef}{ex_i}\frac{ef}{ex_j}$ （2.9）

Formula $\frac{e^2 f}{e\left(x_i,x_j\right)}$ is the second order e -derivative

$$\frac{e^2 f}{e\left(x_i, x_j\right)}\frac{ef}{ex_i}\frac{ef}{ex_j}$$

Proof $= f\left(x_i x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right) f\left(x_i x_j\right) f\left(\overline{x_i} x_j\right) f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right)$

$$= f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right) = \frac{e^2 f}{ex_i ex_j}$$

Deduction 2.4

$$\frac{e^K f}{ex_{i_1} \sim ex_{i_k}} \qquad (2.10)$$

$$= \frac{e^K f}{e\left(x_{i_1} \sim x_{i_K}\right)} \frac{e^{K-1} f}{e\left(x_{i_1} \sim x_{i_{K-1}}\right)}$$

$$\cdots \frac{e^{K-1} f}{e\left(x_{i_2} \sim x_{i_K}\right)} \frac{e^{K-2} f}{e\left(x_{i_1} \sim x_{i_{K-2}}\right)} \cdots \frac{ef}{ex_{i_1}} \cdots \frac{ef}{ex_{i_K}}$$

Property 2.5 $\frac{e^2 f}{ex_i ex_j}\frac{\partial^2 f}{\partial x_i \partial x_j} = 0$ (2.11)

Formula $\frac{\partial^2 f}{\partial x_i \partial x_j}$ is the Boolean second order e-Partial derivative

Proof $\frac{e^2 f}{ex_i ex_j}\frac{\partial^2 f}{\partial x_i \partial x_j}$

$$= f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right)$$

$$\left[f\left(x_i x_j\right) \oplus f\left(x_i \overline{x_j}\right) \oplus f\left(\overline{x_i} x_j\right) \oplus f\left(\overline{x_i}\,\overline{x_j}\right) \right]$$

$$= f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right)$$

$$\oplus f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right)$$

$$\oplus f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right) \oplus$$

$$f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right) = 0 \oplus 0 = 0$$

Deduction 2.5 $\frac{e^K f}{ex_{i_1} \sim ex_{i_k}}\frac{\partial^K f}{\partial x_{i_1} \sim \partial x_{i_K}} = 0$ (2.12)

Property 2.6 $\frac{e^2 f}{\overline{ex_i} \cdot \overline{ex_j}} = \frac{e^2 f}{ex_i ex_j}$ (2.13)

Deduction 2.6 $\frac{e^K f}{\overline{ex_{i_1}} \sim \overline{ex_{i_K}}} = \frac{e^K f}{ex_{i_1} \sim ex_{i_K}}$ (2.14)

Property 2.7 IF $f = a$ （ constant ）, THEN $\frac{e^2 f}{ex_i ex_j} = a$ (2.15)

Deduction 2.7 IF $f = a$ （ constant ）, THEN $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = a$ (2.16)

Property 2.8 IF $\frac{ef}{ex_i} = \frac{ef}{ex_j} = f$,

THEN $\frac{e^2 f}{ex_i ex_j} = f$ (2.17)

Deduction2.8 $\frac{ef}{ex_{i_1}} = \frac{ef}{ex_{i_2}} = \cdots = \frac{ef}{ex_{i_K}} = f$, THEN $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = f$ (2.18)

Property 2.9 $\frac{e^2 \left(f \cdot g\right)}{ex_i ex_j} = \frac{e^2 f}{ex_i ex_j}\frac{e^2 g}{ex_i ex_j}$ (2.19)

Deduction 2.9 $\frac{e^K \left(f \cdot g\right)}{ex_{i_1} \sim ex_{i_K}} = \frac{e^K f}{ex_{i_1} \sim ex_{i_K}}\frac{e^K g}{ex_{i_1} \sim ex_{i_K}}$ (2.20)

Property 2.10 $\frac{e^2 f}{ex_i ex_j}\frac{\partial^2 \left(f \oplus g\right)}{\partial x_i \partial x_j} = \frac{e^2 f}{ex_i ex_j}\frac{\partial^2 g}{\partial x_i \partial x_j}$ (2.21)

Proof

$$\frac{e^2 f}{ex_i ex_j}\frac{\partial^2 \left(f \oplus g\right)}{\partial x_i \partial x_j}$$

$$= f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right)$$

$$[f\left(x_i x_j\right) \oplus g\left(x_i x_j\right) \oplus f\left(x_i \overline{x_j}\right) \oplus g\left(x_i \overline{x_j}\right) \oplus$$

$$f\left(\overline{x_i} x_j\right) \oplus g\left(\overline{x_i} x_j\right) \oplus f\left(\overline{x_i}\,\overline{x_j}\right) \oplus g\left(\overline{x_i}\,\overline{x_j}\right)]$$

$$= f\left(x_i x_j\right) f\left(x_i \overline{x_j}\right) f\left(\overline{x_i} x_j\right) f\left(\overline{x_i}\,\overline{x_j}\right)$$

$$[g\left(x_i x_j\right) \oplus g\left(x_i \overline{x_j}\right) \oplus$$

$$g\left(\overline{x_i} x_j\right) \oplus g\left(\overline{x_i}\,\overline{x_j}\right)] = \frac{e^2 f}{ex_i ex_j}\frac{\partial^2 g}{\partial x_i \partial x_j}$$

Deduction 2.10 $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}}\frac{\partial^K \left(f \oplus g\right)}{\partial x_{i_1} \sim \partial x_{i_K}}$ (2.22)

$$= \frac{e^K f}{ex_{i_1} \sim ex_{i_K}}\frac{\partial^K g}{\partial x_{i_1} \sim \partial x_{i_K}}$$

Property 2.11 $\frac{e^2 f}{ex_i ex_j}\frac{\partial^2 \left(f + g\right)}{\partial x_i \partial x_j} = 0$ (2.23)

Proof $\frac{e^2 f}{ex_i ex_j}\frac{\partial^2(f+g)}{\partial x_i \partial x_j}$

$$= f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$\frac{\partial^2(f \oplus g \oplus fg)}{\partial x_i \partial x_j}$$

$$= f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$\frac{\partial}{\partial x_i}[f(x_i x_j) \oplus g(x_i x_j) \oplus f(x_i x_j) g(x_i x_j)$$

$$\oplus f(x_i \overline{x_j}) \oplus g(x_i \overline{x_j}) \oplus f(x_i \overline{x_j}) g(x_i \overline{x_j})]$$

$$= f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$[f(x_i x_j) \oplus g(x_i x_j) \oplus f(x_i x_j) g(x_i x_j)$$

$$\oplus f(x_i \overline{x_j}) \oplus g(x_i \overline{x_j}) \oplus f(x_i \overline{x_j}) g(x_i \overline{x_j})$$

$$f(\overline{x_i} x_j) \oplus g(\overline{x_i} x_j) \oplus f(\overline{x_i} x_j) g(\overline{x_i} x_j)$$

$$\oplus f(\overline{x_i}\,\overline{x_j}) \oplus g(\overline{x_i}\,\overline{x_j}) \oplus f(\overline{x_i}\,\overline{x_j}) g(\overline{x_i}\,\overline{x_j})]$$

$$= 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 \oplus 0 = 0$$

Deduction2.1 $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}}\frac{\partial^K(f+g)}{\partial x_{i_1} \sim \partial x_{i_K}} = 0$ （2.24）

Property2.12 IF $f(x_1 \sim x_n)$ has no relationship with x_i、x_j，

THEN $\frac{e^2 f}{ex_i ex_j} = f$ （2.25）

Deduction2.12 IF $f(x_1 \sim x_n)$ has no relationship with $x_{i_1} \sim x_{i_K}$，

THEN $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = f$ （2.26）

Property 2.13 IF one of $x_{i_1} \sim x_{i_K}$ is the linear variable, THEN $\frac{e^2 f}{ex_i ex_j} = 0$ （2.27）

Proof Set x_i as linear variable ，$f(x_i x_j) = \overline{f(\overline{x_i} x_j)}$

$$\frac{e^2 f}{ex_i ex_j} = f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$= \overline{f(\overline{x_i} x_j)} f(\overline{x_i} x_j) f(x_i \overline{x_j}) f(\overline{x_i}\,\overline{x_j}) = 0$$

Deduction 2.13 IF one of $x_{i_1} \sim x_{i_K}$ is the linear variable, THEN $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = 0$ （2.28）

Property 2.14 IF $\frac{e^2 f}{ex_i ex_j} = f$，

THEN $\frac{\partial^K f}{\partial x_i \partial x_j} = 0$ （2.29）

Proof

$$\because \frac{e^2 f}{ex_i ex_j} = f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j}) = f(x_i x_j)$$

$$\therefore f(x_i x_j) = f(x_i \overline{x_j}) = f(\overline{x_i} x_j) = f(\overline{x_i}\,\overline{x_j})$$

So

$$\frac{\partial^K f}{\partial x_i \partial x_j} = f(x_i x_j) \oplus f(x_i \overline{x_j}) \oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j}) = 0 \oplus 0 = 0$$

Deduction 2.14 IF $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = f$ ，

THEN $\frac{\partial^K f}{\partial x_{i_1} \sim \partial x_{i_K}} = 0$ （2.30）

Property 2.15 IF $\frac{\partial^2 f}{\partial x_i \partial x_j} = 1$，

THEN $\frac{e^2 f}{ex_i ex_j} = 0$ （2.31）

Proof

$$\because 1 = \frac{\partial^2 f}{\partial x_i \partial x_j} = f(x_i x_j) \oplus f(x_i \overline{x_j}) \oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j})$$

$$\therefore f(x_i x_j)$$

$$= \overline{f(x_i \overline{x_j}) \oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j})}$$

$$= \overline{f(x_i \overline{x_j})} \oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j})$$

$$\frac{e^2 f}{ex_i ex_j} = f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$= \left(\overline{f(x_i \overline{x_j})} \oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j})\right)$$

$$f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j})$$

$$= f(\overline{x_i} x_j) f(x_i \overline{x_j}) f(\overline{x_i}\,\overline{x_j})$$

$$\oplus f(\overline{x_i} x_j) f(x_i \overline{x_j}) f(\overline{x_i}\,\overline{x_j}) = 0$$

Deduction 2.15 IF $\frac{\partial^K f}{\partial x_{i_1} \sim \partial x_{i_K}} = 1$,

THEN $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = 0$ （2.32）

Property 2.16 IF $\frac{e^2 f}{ex_i ex_j} = 1$，

THEN $\frac{\partial^2 f}{\partial x_i \partial x_j} = 0$ （2.33）

Proof

$$\because \frac{e^2 f}{ex_i ex_j} = f(x_i x_j) f(x_i \overline{x_j}) f(\overline{x_i} x_j) f(\overline{x_i}\,\overline{x_j}) = 1$$

$$\therefore f(x_i x_j) = f(x_i \overline{x_j}) = f(\overline{x_i} x_j) = f(\overline{x_i}\,\overline{x_j}) = 1$$

$$\frac{\partial^2 f}{\partial x_i \partial x_j} = f(x_i x_j) \oplus f(x_i \overline{x_j})$$

$$\oplus f(\overline{x_i} x_j) \oplus f(\overline{x_i}\,\overline{x_j}) = 1 \oplus 1 \oplus 1 \oplus 1 = 0$$

Deduction2.16 IF $\frac{e^K f}{ex_{i_1} \sim ex_{i_K}} = 1$,

THEN $\frac{\partial^K f}{\partial x_{i_1} \sim \partial x_{i_K}} = 0$ （2.34）

4. CONCLUSIONS

（1）This article has studied the logic function e-partial derivative and its properties, and proof of some properties are given out, thus makes further complement and perfection of e-derivative study, and promoted research on special operations. Obviously, e-derivative defined in document [1] is the special case of e-partial derivative when K=1. Properties of e-partial derivative in this paper are all suitable to e-derivative. However, some of the properties of e-derivative are not applicable to the high order e-partial derivative. For example：

$$\frac{ef}{ex_i} + \frac{e\overline{f}}{ex_i} = \frac{\overline{df}}{dx_i} = \frac{\overline{\partial f}}{\partial x_i}$$

$$\frac{e^2 f}{ex_i ex_j} + \frac{e^2 \overline{f}}{ex_i ex_j} \neq \frac{\overline{\partial^2 f}}{\partial x_i \partial x_j}$$

(2) Property 2.4 explains relationship between high order e -partial derivative and high order derivative, and Properties 2.5, 2.10, 2.11, 2.14, 2.15 and 2.16 explains relationship between higher order e-partial derivative and Boolean partial derivative.

(3) Introduction of e-partial derivative improves research on the derivative, helps to reveal the property of Boolean functions. Application domains like e-derivative, high order e-derivative and e-partial derivative need to be further widened.

REFERENCES

[1] LI W W, WANG z. The derivative of Boolean functions and its application in the fault detection and cryptographic system [J]. Kybernetes, 2008,37(2):49-65.

[2] LI W W, WANG z.,ZHANG z J. The application of derivative and e-derivative on H-Boolean functions [J]. CHINA SCI-TEC, 2008,(01):267-271.

[3] DING Y J,WANG z, YE J H. Initial-value problem of the Boolean function’s primary function and its application in cryptographic system [J]. Kybernetes, 2010,39(6):900-906.

[4] HE Liang, WANG zhuo, LI Wei-wei. Algorithm of reducing the balanced H-Boolean function correlation-measure and research on correlative issue[J]. Journal of communications, 2010,31(2):93-99.

[5] OU Hai-wen,ZHANG Yu-juan. On algebraic immunity of a class of special Boolean functions[J].Application Research of Computers,2012.

[6]LIU Nan-nan,ZHAO Feng.The relationship between the algebraic immunity and nonlinearity of Boolean functions[J].Huaibei coal industry teachers College (Natural Science),2010.

[7] LIU Guan-sheng, LIAN Yi-qun, CHEN Xie-xiong. Tabular method of calculating Boolean partial derivative and difference of the OC type logic function[J]. Journal of zhe jiang University: Science Edition, 2007,34(2):176-180.