Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2018) 42: 57 – 68
© TÜBİTAK
doi:10.3906/mat-1607-22

Boolean differential operators

Luis HERNÁNDEZ ENCINAS[1], **Ángel MARTIN DEL REY**[2,*]
[1]Institute of Physical and Information Technologies, CSIC Madrid, Spain
[2]Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics,
Universidad de Salamanca Salamanca, Spain

Received: 11.07.2016 • **Accepted/Published Online:** 11.03.2017 • **Final Version:** 22.01.2018

Abstract: In this work the notion of boolean differential operator is revisited and some new properties are stated. The theoretical results are illustrated with several examples.

Key words: Boolean functions, boolean differential operators, boolean derivative

1. Introduction

The main goal of this work is to revise the notion of boolean differential operator introducing some new important properties. This concept is based on the notion of boolean derivative and boolean differential equations ([12, 13]) that have several applications in different scientific branches.

Although the notion of boolean differential operator has been tackled from algebraic ([3]) and logical ([16]) points of view, its interpretation in terms of multivariate boolean calculus has not been completely considered. This is precisely the mail goal of this work. Specifically, the main contributions of this work are the following: the notion of boolean differential operator on the set of boolean functions is introduced, its expression in terms of partial boolean derivatives is explicitly shown, and an upper bound for the degree of a boolean differential operator is given. Moreover, the notion of boolean differential operator associated with the directional derivative is presented and some properties are shown. Finally, the concept of vectorial boolean operator is defined and the basic properties are stated.

The rest of the paper is organized as follows: in section 2 the mathematical background on boolean functions is introduced; the derivative of boolean functions and the main properties are presented in section 3; finally, in section 4 the notion of boolean differential operator is introduced based both on boolean derivative and directional derivative, and some new properties are shown. Moreover, some examples as boolean gradient and boolean curl are explicitly shown.

2. Mathematical background

In what follows, the basic theory of boolean functions is introduced. For a more detailed discussion about this topic, we refer the reader to [6].

Let $\mathbb{F}_2^n$ be the nth dimensional vector space over the Galois field $\mathbb{F}_2 = \{0, 1\}$, and set $\{e_1, \ldots, e_n\}$ its

[*]Correspondence: delrey@usal.es

2010 *AMS Mathematics Subject Classification:* Primary 06E99; Secondary 94C10 standard basis, that is:

$$e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1). \tag{1}$$

For any two vectors $x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n$ and $y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$, we recall the following three basic operations:

- XOR addition: $x \oplus y = (x_1 \oplus y_1, \ldots, x_n \oplus y_n) \in \mathbb{F}_2^n$.
- Scalar product: $x \cdot y = x_1 y_1 \oplus \ldots \oplus x_n y_n \in \mathbb{F}_2$.
- Hadamard product: $x \star y = (x_1 y_1, \ldots, x_n y_n) \in \mathbb{F}_2^n$.

An n-variable boolean function is a map of the form $f \colon \mathbb{F}_2^n \to \mathbb{F}_2$. The set of all n-variable boolean functions is denoted by $\mathcal{BF}_n$ and its cardinality is $|\mathcal{BF}_n| = 2^{2^n}$. The vector

$$t_f = (f(v_0), f(v_1), \ldots, f(v_{2^n-1})) \in \mathbb{F}_2^{2^n}, \tag{2}$$

where $v_0 = (0, \ldots, 0), v_1 = (0, \ldots, 0, 1), \ldots, v_{2^n-1} = (1, \ldots, 1)$, is called the truth table of f. Note that, for $1 \le i \le 2^n - 1$, v_i is the binary representation of i, written as a vector of length n.

The Hamming weight of a vector $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$ is denoted by $wt(x)$ and it is defined as the number of its nonzero coordinates. Moreover, the Hamming weight of an n-variable boolean function f is defined as

$$wt(f) = |\{x \in \mathbb{F}_2^n \text{ such that } f(x) \neq 0\}|, \tag{3}$$

that is, it is the cardinality of its support. An n-variable boolean function f is said to be balanced if $wt(f) = 2^{n-1}$, i.e if the number of 1's are equal to the number of 0's of its truth table.

The Hamming distance between two boolean functions $f, g \in \mathcal{BF}_n$ is $d(f, g) = wt(f \oplus g)$, where $(f \oplus g)(x) = f(x) \oplus g(x)$.

The usual representation of a boolean function f is by means of its algebraic normal form (ANF for short) which is the n-variable polynomial representation over $\mathbb{F}_2$, that is

$$f(x_1, \ldots, x_n) = a_0 \oplus \bigoplus_{\substack{1 \le k \le n \\ 1 \le i_1 < i_2 < \ldots < i_k \le n}} a_{i_1 i_2 \ldots i_k} x_{i_1} x_{i_2} \ldots x_{i_k}, \tag{4}$$

where $a_0, a_{i_1 \ldots i_k} \in \mathbb{F}_2$. Let $\deg(f)$ be the degree of the ANF, which is the algebraic degree of the function. The simplest boolean functions considering their ANF are the affine boolean functions: $f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus a_2 x_2 \oplus \ldots \oplus a_n x_n$, where $a_0, a_1, \ldots, a_n \in \mathbb{F}_2$. If $a_0 = 0$, we have the linear boolean functions and each of them is denoted by $l_a(x)$ with $a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$.

A vectorial boolean function, or (n, m)-boolean function, is a mapping from the vector space $\mathbb{F}_2^n$ to the vector space $\mathbb{F}_2^m$:

$$\begin{array}{rcl} F \colon \mathbb{F}_2^n & \to & \mathbb{F}_2^m \\ x & \mapsto & F(x) = (f_1(x), f_2(x), \ldots, f_m(x)) \end{array} \tag{5}$$

The n-variable boolean functions $f_1, \ldots, f_m$ are called the coordinate functions of F. When the numbers m and n are not given, the (n, m)-boolean functions are also called multioutput boolean functions or S-boxes. The set of all (n, m)-boolean functions is denoted by $\mathcal{BF}_{n,m}$ and its cardinality is $|\mathcal{BF}_{n,m}| = \left(2^{2^n}\right)^m$. Note that an n-variable boolean function is a particular case of a (n,m)-boolean function when $m=1$, that is, $\mathcal{BF}_{n,1}=\mathcal{BF}_n$.

Set $F,G\in\mathcal{BF}_{n,m}$ such that $F=(f_1,f_2,\ldots,f_m)$ and $G=(g_1,g_2,\ldots,g_m)$. Then we can define the (n,m)-boolean function $F\oplus G$ as follows: $F\oplus G=(f_1\oplus g_1,f_2\oplus g_2,\ldots,f_m\oplus g_m)$. Moreover, the Hadamard product of F and G is another vectorial boolean function $F\star G\in\mathcal{BF}_{n,m}$ such that $F\star G=(f_1\cdot g_1,f_2\cdot g_2,\ldots,f_m\cdot g_m)$, where $(f\cdot g)(x)=f(x)\cdot g(x)$.

3. The derivative of a boolean function

3.1. Definition and some interesting results

The notion of boolean derivative was introduced by Reed (see [12]) as a tool for constructing a decoding method for a class of error-correcting codes. Furthermore, this concept has also been used for example in the design of properties that boolean functions must satisfy for cryptographic applications (see [6]), for stack filters and image processing (see [1, 7]), to develop a new order parameter for the random boolean network phase transition (see [8]), or for simulations of cellular automata (see [2]). It is defined as follows (see, for example, [14]):

Definition 1 *The partial derivative of an n-variable boolean function f with respect to the i-th variable x_i is another n-variable boolean function defined as follows:*

$$\begin{array}{rcl} D_i f\colon \mathbb{F}_2^n & \to & \mathbb{F}_2 \\ x & \mapsto & D_i f(x)=f(x)\oplus f(x\oplus e_i) \end{array} \tag{6}$$

that is,

$$D_i f(x)=f(x_1,\ldots,x_i,\ldots,x_n)\oplus f(x_1,\ldots,x_i\oplus 1,\ldots,x_n). \tag{7}$$

This definition allows one to state a derivation rule similar to the derivation rule for multivariate polynomials over real numbers (see [11]):

Lemma 2 *Let f be an n-variable boolean function whose ANF expression is given in (4). Then for each variable x_i it is*

$$f(x)=g_i(x\oplus x_ie_i)\oplus x_ih_i(x\oplus x_ie_i), \tag{8}$$

where h_i and g_i are $(n-1)$-variable boolean functions that do not depend on the variable x_i. Moreover, if f does not depend on the variable x_i then $h_i=0$.

Note that for the sake of simplicity we set $x\oplus x_ie_i=(x_1,\ldots,\widehat{x_i},\ldots,x_n)$.

Proposition 3 *[11] Let f be an n-variable boolean function. Then*

$$D_i f(x)=h_i(x\oplus x_ie_i). \tag{9}$$

Proof By definition, $D_i f(x)=f(x)\oplus f(x\oplus e_i)$, and taking into account the last lemma, it yields

$$\begin{aligned} D_i f(x) &= g_i(x\oplus x_ie_i)\oplus x_ih_i(x\oplus x_ie_i)\oplus g_i(x\oplus x_ie_i) \\ &\quad \oplus(x_i\oplus 1)h_i(x\oplus x_ie_i)=h_i(x\oplus x_ie_i), \end{aligned} \tag{10}$$

thus finishing. □

Corollary 4 *As a consequence, the partial derivative (with respect to one variable) reduces the algebraic degree of the boolean function by* 1*.*

Example 5 *Set* $x = (x_1, x_2, x_3, x_4, x_5)$ *and let us consider the* 5*-variable boolean function whose ANF is*

$$f(x) = 1 \oplus x_2 \oplus x_3 \oplus x_4x_5 \oplus x_1x_3x_4x_5; \tag{11}$$

then, as simple computations show,

$$\begin{aligned} D_1f(x) &= x_3x_4x_5, && (12)\\ D_2f(x) &= 1, && (13)\\ D_3f(x) &= 1 \oplus x_1x_4x_5, && (14)\\ D_4f(x) &= x_5 \oplus x_1x_3x_5, && (15)\\ D_5f(x) &= x_4 \oplus x_1x_3x_4. && (16) \end{aligned}$$

The composition of partial derivatives with respect to the ith and jth variables is defined as follows:

$$\begin{aligned} (D_i \circ D_j) f(x) &= D_i(D_jf)(x) = D_jf(x) \oplus D_jf(x \oplus e_i) && (17)\\ &= f(x) \oplus f(x \oplus e_j) \oplus f(x \oplus e_i) \oplus f(x \oplus e_i \oplus e_j). \end{aligned}$$

In this sense, it is easy to check that this composition commutes:

$$(D_i \circ D_j) f(x) = (D_j \circ D_i) f(x). \tag{18}$$

Definition 6 *[15] The boolean jacobian matrix of an* (n, m)*-boolean function* $F = (f_1, f_2, \ldots, f_m)$ *is the following boolean matrix:*

$$J_F = \begin{pmatrix} D_1(f_1) & D_2(f_1) & \cdots & D_n(f_1)\\ D_1(f_2) & D_2(f_2) & \cdots & D_n(f_2)\\ \vdots & \vdots & \ddots & \vdots\\ D_1(f_m) & D_2(f_m) & \cdots & D_n(f_m) \end{pmatrix}. \tag{19}$$

Definition 7 *[15] The hessian jacobian matrix of an* n*-variable boolean function* f *is the following boolean matrix:*

$$H_f = \begin{pmatrix} (D_1 \circ D_1)(f) & (D_1 \circ D_2)(f) & \cdots & (D_1 \circ D_n)(f)\\ (D_2 \circ D_1)(f) & (D_2 \circ D_2)(f) & \cdots & (D_2 \circ D_n)(f)\\ \vdots & \vdots & \ddots & \vdots\\ (D_n \circ D_1)(f) & (D_n \circ D_2)(f) & \cdots & (D_n \circ D_n)(f) \end{pmatrix}. \tag{20}$$

It is easy to check that the hessian matrix of any boolean function is the null matrix.

We can extend the notion of partial derivative to directional derivative as follows (see [4]):

Definition 8 *The directional derivative of the* n*-variable boolean function* f *with respect to* $b \in \mathbb{F}_2^n$ *is another* n*-variable boolean function defined as follows:*

$$\begin{aligned} D_bf : \mathbb{F}_2^n &\to \mathbb{F}_2 && (21)\\ x &\mapsto D_bf(x) = f(x) \oplus f(x \oplus b) \end{aligned}$$

Note that if $wt(b) = k$ then $b \in \mathbb{F}_2^n$ has k nonzero coefficients placed at positions $1 \leq i_1 < \ldots < i_k \leq n$; thus $b = e_{i_1} \oplus \ldots \oplus e_{i_k} \in \mathbb{F}_2^n$. As a consequence and for the sake of simplicity we take

$$D_b f(x) = D_{e_{i_1} \oplus \ldots \oplus e_{i_k}} f(x) = D_{i_1,\ldots,i_k} f(x). \tag{22}$$

In the following proposition, the relation between partial derivatives and directional derivatives is stated (see [11]):

Proposition 9 *Let f be an n-variable boolean function and set*

$$1 \leq i_1 < i_2 < \ldots < i_k \leq n \tag{23}$$

with $k \leq n$, then

$$(D_{i_1} \circ \ldots \circ D_{i_k}) f(x) = \bigoplus_{\substack{1 \leq l \leq k \\ j_1 < \ldots < j_l \\ j_1,\ldots,j_l \in \{i_1,\ldots,i_k\}}} D_{j_1,\ldots,j_l} f(x). \tag{24}$$

Note that (24) yields

$$D_{i_1,\ldots,i_k} f(x) = (D_{i_1} \circ \ldots \circ D_{i_k}) f(x) \oplus \bigoplus_{\substack{1 \leq l \leq k-1 \\ j_1 < \ldots < j_l \\ j_1,\ldots,j_l \in \{i_1,\ldots,i_k\}}} D_{j_1,\ldots,j_l} f(x). \tag{25}$$

As a consequence, the following results hold:

Corollary 10 *Taking into account Proposition 9 it is verified:*

1. *The directional derivative reduces the algebraic degree of the boolean function to be applied by, at least, one.*
2. *If $k = n$ then*
$$(D_1 \circ \ldots \circ D_n) f(x) = \bigoplus_{b \in \mathbb{F}_2^n} D_b f(x). \tag{26}$$
3. *If σ is a permutation of n elements, then*
$$(D_1 \circ \ldots \circ D_n) f(x) = \left(D_{\sigma(1)} \circ \ldots \circ D_{\sigma(n)}\right) f(x). \tag{27}$$
4. *The directional derivative can be given in terms of the composition of partial derivatives as follows:*
$$D_{i_1,\ldots,i_k} f(x) = \bigoplus_{\substack{1 \leq l \leq k \\ j_1 < \ldots < j_l \\ j_1,\ldots,j_l \in \{i_1,\ldots,i_k\}}} (D_{j_1} \circ \ldots \circ D_{j_l}) f(x). \tag{28}$$

4. Boolean differential operators

In this section the novel notion of differential boolean operator is introduced and its main properties are shown. Moreover, some examples are introduced and studied.

4.1. Boolean differential operators on $\mathcal{BF}_n$

4.1.1. Definitions and basic properties

Definition 11 *A boolean differential operator on* $\mathcal{BF}_n$ *is a map acting on* $\mathcal{BF}_n$

$$\begin{array}{rcl} D\colon \mathcal{BF}_n & \to & \mathcal{BF}_n \\ f & \mapsto & D(f) \end{array} \tag{29}$$

such that

$$Df(x) = \bigoplus_{b\in\mathbb{F}_2^n} p_b(x)\, D_b f(x), \tag{30}$$

where $x \in \mathbb{F}_2^n$ *and* $p_b \in \mathcal{BF}_n$. *The set of all boolean differential operators on* $\mathcal{BF}_n$ *is denoted by* $\mathcal{BD}_n$. *The number of boolean differential operators is* 2^{n+2^n}. *In the Table the first values are shown.*

Table. Cardinality of the set of boolean differential operators on $\mathcal{BF}_n$.

n	1	2	3	4	5	6	7	8
$\lvert\mathcal{BD}_n\rvert \approx$	8	64	2048	1.05×10^{6}	1.37×10^{11}	1.18×10^{21}	4.36×10^{40}	2.96×10^{59}

Example 12 *Let us consider the boolean differential operator on* $\mathcal{BF}_3$

$$D = (x_1 \oplus x_3)\, D_{b_1} \oplus x_2x_3 D_{b_2} \oplus x_1x_2x_3 D_{b_3}, \tag{31}$$

where $b_1 = (1,0,1), b_2 = (1,0,0), b_3 = (0,0,1)$ *and* $p_{b_1} = x_1 \oplus x_3, p_{b_2} = x_2x_3, p_{b_3} = x_1x_2x_3$, *and* $p_b = 0$ *for* $b \in \mathbb{F}_2^3$ *such that* $b \neq b_1, b_2, b_3$. *If we apply* D *to* $f(x_1,x_2,x_3) = x_1 \oplus x_2 \oplus x_3$, *it yields*

$$Df(x) = x_2x_3 \oplus x_1x_2x_3. \tag{32}$$

Taking into account item 4 of Corollary 10, the expression of a boolean differential operator can be given in terms of the partial boolean derivatives. Consequently, the boolean differential operator whose explicit expression is

$$Df(x) = \bigoplus_{b\in\mathbb{F}_2^n} p_b(x)\, D_b f(x), \tag{33}$$

can be written as follows:

$$\begin{aligned} Df(x) &= \bigoplus_{b\in\mathbb{F}_2^n} p_b(x)\, D_b f(x) \\ &= \bigoplus_{\substack{1\le k\le n \\ 1\le i_1<\ldots<i_k\le n}} p_{i_1,\ldots,i_k}(x)\, D_{i_1,\ldots,i_k} f(x) \\ &= \bigoplus_{\substack{1\le k\le n, 1\le l\le k \\ 1\le i_1<\ldots<i_k\le n \\ j_1<\ldots<j_l, j_1,\ldots,j_l\in\{i_1,\ldots,i_k\}}} p_{i_1,\ldots,i_k}(x)\, (D_{j_1}\circ\ldots\circ D_{j_l})\, f(x) \end{aligned} \tag{34}$$

Example 13 *Let us consider the boolean differential operator on* $\mathcal{BF}_3$

$$D=\left(x_1\oplus x_3\right)D_{13}\oplus x_1x_3D_{12}\oplus\left(1\oplus x_2\right)D_{123}. \tag{35}$$

Since

$$\begin{aligned} D_{13} &= D_1\oplus D_3\oplus\left(D_1\circ D_3\right), & (36)\\ D_{12} &= D_1\oplus D_2\oplus\left(D_1\circ D_2\right), & (37)\\ D_{123} &= D_1\oplus D_2\oplus D_3\oplus\left(D_1\circ D_2\right)\oplus\left(D_1\circ D_3\right)\oplus\left(D_2\circ D_3\right) & (38)\\ &\quad\oplus\left(D_1\circ D_2\circ D_3\right), & (39)\end{aligned}$$

then

$$\begin{aligned} D &= \left(1\oplus x_1\oplus x_2\oplus x_3\oplus x_1x_3\right)D_1\oplus\left(1\oplus x_2\oplus x_1x_3\right)D_2\\ &\quad\oplus\left(1\oplus x_1\oplus x_2\oplus x_3\right)D_3\oplus\left(1\oplus x_2\oplus x_1x_3\right)\left(D_1\circ D_2\right)\\ &\quad\oplus\left(1\oplus x_1\oplus x_2\oplus x_3\right)\left(D_1\circ D_3\right)\oplus\left(1\oplus x_2\right)\left(D_2\circ D_3\right)\\ &\quad\oplus\left(1\oplus x_2\right)\left(D_1\circ D_2\circ D_3\right) \end{aligned} \tag{40}$$

A simple computation shows the following result:

Proposition 14 *Set* $f\in\mathcal{BF}_n$ *with* $\deg(f)=k\leq n$*, and* $D=\bigoplus_{b\in\mathbb{F}_2^n}p_bD_b\in\mathcal{BD}_n$*; then*

$$\deg\left(Df\right)\leq\max_{b\in\mathbb{F}_2^n}\{\deg\left(p_b\right)\}+k-1. \tag{41}$$

Proof By definition

$$Df\left(x\right)=\bigoplus_{b\in\mathbb{F}_2^n}p_b\left(x\right)D_bf\left(x\right). \tag{42}$$

Then, taking into account item 1 of Corollary 10, the algebraic degree of D_bf is as most $k-1$, and, consequently, the algebraic degree of the addend $p_b\left(x\right)D_bf\left(x\right)$ is at most $\deg\left(p_b\right)+k-1$. Then, the algebraic degree of Df is at most $\max_{b\in\mathbb{F}_2^n}\{\deg\left(p_b\right)\}+k-1$. □

Definition 15 *The partial derivative with respect to the* i*-th variable defines the following boolean differential operator:*

$$\begin{aligned} D_i\colon\mathcal{BF}_n &\to \mathcal{BF}_n\\ f &\mapsto D_if \end{aligned} \tag{43}$$

Moreover, the directional derivative with respect to $b\in\mathbb{F}_2^n$ *defines the following boolean differential operator:*

$$\begin{aligned} D_b\colon\mathcal{BF}_n &\to \mathcal{BF}_n\\ f &\mapsto D_bf \end{aligned} \tag{44}$$

Proposition 16 *Set* $b\in\mathbb{F}_2^n$*. The differential operator* D_b *satisfies the following properties:*

1. *If f and g are two n-variable boolean functions, then*

$$D_b(f \oplus g) = D_b(f) \oplus D_b(g). \tag{45}$$

2. *If f is an n-variable boolean function and $a \in \mathbb{F}_2$, then*

$$D_b(af) = aD_b(f). \tag{46}$$

3. *If f and g are two n-variable boolean functions, then*

$$D_b(f \cdot g) = D_b(f) \cdot D_b(g) \oplus f \cdot D_b(g) \oplus g \cdot D_b(f). \tag{47}$$

4. *Let $D_{i_1}, \ldots, D_{i_k}$ be the differential operators defined by the partial derivatives with respect to the variables $x_{i_1}, \ldots, x_{i_k}$ respectively; then*

$$(D_{i_1} \circ \ldots \circ D_{i_k}) = \bigoplus_{\substack{1 \le l \le k \\ j_1 < \ldots < j_l \\ j_1, \ldots, j_l \in \{i_1, \ldots, i_k\}}} D_{j_1, \ldots, j_l}. \tag{48}$$

Proof

1. Set $x \in \mathbb{F}_2^n$; then

$$\begin{aligned} D_b(f \oplus g)(x) &= (f \oplus g)(x) \oplus (f \oplus g)(x \oplus b) \\ &= f(x) \oplus g(x) \oplus f(x \oplus b) \oplus g(x \oplus b) \\ &= (f(x) \oplus f(x \oplus b)) \oplus (g(x) \oplus g(x \oplus b)) \\ &= D_b(f)(x) \oplus D_b(g)(x). \end{aligned} \tag{49}$$

2. Set $x \in \mathbb{F}_2^n$; then

$$\begin{aligned} D_b(af)(x) &= af(x) \oplus af(x \oplus b) = a(f(x) \oplus f(x \oplus b)) \\ &= aD_b(f). \end{aligned} \tag{50}$$

3. Set $x \in \mathbb{F}_2^n$; then

$$\begin{aligned} D_b(f \cdot g)(x) &= (f \cdot g)(x) \oplus (f \cdot g)(x \oplus b) \\ &= f(x) \cdot g(x) \oplus f(x \oplus b) \cdot g(x \oplus b) \\ &= f(x) \cdot g(x) \oplus (D_b f(x) \oplus f(x)) \cdot (D_b g(x) \oplus g(x)) \\ &= D_b f(x) \cdot D_b g(x) \oplus f(x) \cdot D_b g(x) \oplus g(x) \cdot D_b f(x). \end{aligned} \tag{51}$$

4. It follows from Proposition 9.

□

As a consequence and taking into account the last result and equation (30), the following statements hold:

Corollary 17 *Let D be a boolean differential operator; then*

1. *If f and g are two n-variable boolean functions, then*

$$D\left(f\oplus g\right)=D\left(f\right)\oplus D\left(g\right). \tag{52}$$

2. *If f is an n-variable boolean function and $a\in\mathbb{F}_2$, then*

$$D\left(af\right)=aD\left(f\right). \tag{53}$$

3. *If f and g are two n-variable boolean functions, then*

$$\begin{aligned} D\left(f\cdot g\right) &= D\left(f\right)\cdot D\left(g\right) \\ &\quad \oplus f\cdot D\left(g\right)\oplus g\cdot D\left(f\right) \\ &\quad \oplus \bigoplus_{\substack{b,c\in\mathbb{F}_2^n\\ b\neq c}} p_b p_c D_b\left(f\right)D_c\left(g\right). \end{aligned} \tag{54}$$

4.1.2. Some examples of boolean differential operators

Definition 18 *The homogeneity boolean differential operator denoted by Θ is defined as follows:*

$$\begin{aligned} \Theta\colon \mathcal{BF}_n &\to \mathcal{BF}_n \\ f &\mapsto \Theta\left(f\right)=\bigoplus_{1\le i\le n} x_i D_i f \end{aligned} \tag{55}$$

Definition 19 *The boolean divergence is the boolean differential operator denoted by div and defined in the following way:*

$$\begin{aligned} div\colon \mathcal{BF}_n &\to \mathcal{BF}_n \\ f &\mapsto div\left(f\right)=\bigoplus_{1\le i\le n} D_i f \end{aligned} \tag{56}$$

Note that boolean divergence operator is a particular case of the homogeneity boolean differential operator when the coefficients of the partial derivatives are the nonzero constant boolean function. As is well known, elementary cellular automata (ECA for short) are a particular type of finite state machine where the evolution of states of the cells is governed by means of a 3-variable boolean function (see [17]). The boolean derivative of ECA has been extensively studied (see, for example, [2, 15]) and also the cryptographic significance of its boolean divergence has been analyzed (see [9]).

Definition 20 *The boolean Laplacian is the boolean differential operator denoted by ∇^2 and defined as follows:*

$$\begin{aligned} \nabla^2\colon \mathcal{BF}_n &\to \mathcal{BF}_n \\ f &\mapsto \nabla^2\left(f\right)=\bigoplus_{1\le i\le n} \left(D_i\circ D_i\right)f \end{aligned} \tag{57}$$

As a simple calculus shows, $\nabla^2\left(f\right)=0$ for every n-variable boolean function f.

Example 21 *Let f be the following 5-variable boolean function:*

$$f\left(x\right)=1\oplus x_2\oplus x_3\oplus x_4x_5\oplus x_1x_3x_4x_5; \tag{58}$$

then its divergence is

$$\begin{aligned} div\left(f\right) &= \bigoplus_{1\leq i\leq 5} D_i f \\ &= x_4\oplus x_5\oplus x_1x_3x_4\oplus x_1x_3x_5\oplus x_1x_4x_5\oplus x_3x_4x_5. \end{aligned} \tag{59}$$

4.2. Vectorial boolean differential operators

Definition 22 *A vectorial boolean differential operator is a map from $\mathcal{BF}_{n,m}$ to $\mathcal{BF}_{p,q}$*

$$\begin{aligned} D\colon \mathcal{BF}_{n,m} &\to \mathcal{BF}_{p,q} \\ F &\mapsto D\left(F\right) \end{aligned} \tag{60}$$

Note that when $m=q=1$ and $n=p$ we obtain the boolean differential operators on $\mathcal{BF}_n$. Usually $p=n$ and, consequently, this work deals with boolean differential operators from $\mathcal{BF}_{n,m}$ to $\mathcal{BF}_{n,q}$.

If $F=\left(f_1,f_2,\ldots,f_m\right)$, then $DF=\left(\tilde{f}_1,\tilde{f}_2,\ldots,\tilde{f}_m\right)$, where $\tilde{f}_i$ is obtained when some differential operators (on $\mathcal{BF}_n$) are applied to some of the functions $f_1,f_2,\ldots,f_m$. That is, for $1\leq i\leq m$, it is

$$\tilde{f}_i=D^{(i,1)}f_1\oplus D^{(i,2)}f_2\oplus\ldots\oplus D^{(i,m)}f_m, \tag{61}$$

where $D^{(i,k)}$ are boolean differential operators (on $\mathcal{BF}_m$) with $1\leq i,k\leq m$. Now suppose that

$$D^{(i,k)}=\bigoplus_{b\in\mathbb{F}_2^n} p_b^{i,k}D_b, \tag{62}$$

where $p_b^{i,k}\in\mathcal{BF}_n$. Then

$$\tilde{f}_i=\bigoplus_{\substack{1\leq k\leq m\\ b\in\mathbb{F}_2^n}} p_b^{i,k}D_bf_k. \tag{63}$$

Example 23 *Let D be the vectorial boolean differential operator from $\mathcal{BF}_{3,2}$ to $\mathcal{BF}_{3,2}$ defined as follows: If $F=\left(f_1,f_2\right)\in\mathcal{BF}_{3,2}$ then*

$$D\left(F\right)=\left(\tilde{f}_1,\tilde{f}_2\right), \tag{64}$$

where

$$\tilde{f}_1 = D_1f_1\oplus D_2f_2, \tag{65}$$

$$\tilde{f}_2 = D_{12}f\oplus 1. \tag{66}$$

If, for example, $F=\left(x_1\oplus x_2\oplus x_3,x_1\oplus x_3\right)$, then

$$D\left(F\right)=\left(1,x_1\oplus x_3\right). \tag{67}$$

Straightforward computations yield the following results:

Proposition 24 *Let D be a vectorial boolean differential operator from $\mathcal{BF}_{n,m}$ to $\mathcal{BF}_{n,q}$; then*

1. *If $F, G \in \mathcal{BF}_{n,m}$ then $D(F \oplus G) = D(F) \oplus D(G)$.*
2. *If $F \in \mathcal{BF}_{n,m}$ and $a \in \mathbb{F}_2$, then $D(aF) = aD(F)$.*
3. *If $F, G \in \mathcal{BF}_{n,m}$ then $D(F \star G) = D(F) \star D(G) \oplus H$, where $H = (h_1, h_2, \ldots, h_m)$, with*

$$\begin{aligned} h_i &= \bigoplus_{\substack{1\le k\le m \\ b\in\mathbb{F}_2^n}} p_b^{i,k}\left(f_k \cdot D_b g_k \oplus g_k \cdot D_b f_k\right) \\ &\oplus \bigoplus_{\substack{1\le k<j\le m \\ c,b\in\mathbb{F}_2^n, b\neq c}} p_b^{i,k} \cdot p_c^{i,j} \cdot D_b f_k \cdot D_b g_j. \end{aligned} \tag{68}$$

4.2.1. Some examples of boolean differential operators on $\mathcal{BF}_{n,m}$

Definition 25 *Let f be an n-variable boolean function. The boolean gradient of f is a vectorial boolean differential operator denoted by $\nabla(f)$ and defined as follows:*

$$\begin{aligned} \nabla\colon \mathcal{BF}_n &\to \mathcal{BF}_{n,n} \\ f &\mapsto \nabla(f) = \left(D_1(f), D_2(f), \ldots, D_n(f)\right) \end{aligned} \tag{69}$$

In [5] the dynamics of cellular automata is studied in terms of the boolean gradient and the jacobian matrix of its local transition function.

Example 26 *Let us consider the 5-variable boolean function*

$$f(x) = 1 \oplus x_2 \oplus x_3 \oplus x_4x_5 \oplus x_1x_3x_4x_5; \tag{70}$$

then its gradient is the following $(5,5)$-boolean function:

$$\begin{aligned} \nabla\colon \mathcal{BF}_5 &\to \mathcal{BF}_{5,5} \\ f &\mapsto \nabla(f) = \left(x_3x_4x_5, 1, 1 \oplus x_1x_4x_5, x_5 \oplus x_1x_3x_5, x_4 \oplus x_1x_3x_4\right) \end{aligned} \tag{71}$$

Definition 27 *Let F be a $(3,3)$-boolean function such that $F = (F_1, F_2, F_3)$. Then the boolean curl of F is the boolean differential operator on $\mathcal{BF}_{3,3}$ denoted by $\operatorname{curl}(F)$ and defined as follows:*

$$\begin{aligned} \operatorname{curl}\colon \mathcal{BF}_{3,3} &\to \mathcal{BF}_{3,3} \\ F &\mapsto \operatorname{curl}(F) = (R_1, R_2, R_3) \end{aligned} \tag{72}$$

where

$$R_1(x) = D_2F_3(x) \oplus D_3F_2(x), \tag{73}$$

$$R_2(x) = D_3F_1(x) \oplus D_1F_3(x), \tag{74}$$

$$R_3(x) = D_1F_2(x) \oplus D_2F_1(x). \tag{75}$$

We can generalize this notion to (n,n)-vectorial boolean functions with $n \geq 3$ as follows:

Definition 28 *Let $F \in \mathcal{BF}_{n,n}$ with $n \geq 3$. Its curl, $\operatorname{curl}(F)$, is the (n,n)-boolean function $\operatorname{curl}(F): \mathbb{F}_2^n \to \mathbb{F}_2^n$, such that*

$$\operatorname{curl}(F)(x) = (R_1(x), \ldots, R_i(x), \ldots, R_n(x)), \tag{76}$$

where

$$R_i(x) = \bigoplus_{1 \leq j \leq n,\, j \neq i} D_{1 \oplus e_i \oplus e_j} F_j(x) \tag{77}$$

The curl of elementary cellular automata has been introduced in [10].

Acknowledgments

We would like to thank the anonymous referee for his/her valuable suggestions and comments to improve the original manuscript.

This work has been supported by Ministry of Economy and Competitiveness (Spain) and European FEDER Fund under projects TIN2014-55325-C2-1-R, TIN2014-55325-C2-2-R, and MTM2015-69138-REDT.

References

[1] Agaian SS, Panetta KA, Nercessian SC, Danahy EE. Boolean derivatives with applications to edge detection for image system. IEEE T Syst Man Cybern 2010; 40: 371-382.

[2] Bagnoli F. Boolean derivatives and computation of cellular automata. Int J Mod Phys C 1992; 3: 307-320.

[3] Catumba J, Díaz R. Boolean differential operators. Comment Math Univ Carolin 2014; 55: 141-158.

[4] Chen H, Sun J. A new calculation for Boolean derivative using Cheng product. J Appl Math 2012; Article ID 748343 (11 pages). Doi number: 10.1155/2012/748343.

[5] Choudhury PP, Sahoo S, Chakraborty M, Bhandari SK, Pal A. Investigation of the global dynamics of cellular automata using Boolean derivatives. Comput Math Appl 2009; 57: 1337-1351.

[6] Cusick TW, Stanica P. Cryptographic Boolean Functions and Applications. Oxford, UK: Academic Press, 2009.

[7] Egiazarian K, Kousmanen P, Astola J. Boolean derivatives, weighted chow parameters, and selection probabilities of stack filters. IEEE T Signal Process 1996; 44: 1634-1641.

[8] Kahn J, Kalai G, Linial N. The influence of variables on boolean functions. In: Proceedings of the IEEE 29th Annual Symposium on Foundations of Computer Science, 24–26 October 1998; White Plains, New York. Washington DC, IEEE Computer Society, 1998, pp. 68-80.

[9] Martín del Rey A, Queiruga Dios A., Rodríguez Sánchez G. Propagation characteristics of the divergence of elementary cellular automata. Int J Mod Phys C 2010; 21: 1263-1276.

[10] Martín del Rey A, Rodríguez Sánchez G. The curl of elementary cellular automata. Int J Mod Phys C 2012; 23: 1250011.

[11] Martín del Rey A, Rodríguez Sánchez G, de la Villa Cuenca A. On the boolean partial derivatives and their composition. Appl Math Lett 2012; 25: 739-744.

[12] Reed JS. A class of multiple error-correcting codes and the decoding scheme. Trans IRE Prof Group Inf Theory 1954; 4: 38-49.

[13] Serfati M. Boolean differential equations. Discrete Math 1995; 146: 235-246.

[14] Tucker JH, Tapia MA, Bennet AW. Boolean integral calculus for digital systems. IEEE T Comput 1985; c-34: 78-81.

[15] Vichniac GY. Boolean derivatives on cellular automata. Physica D 1990; 45: 63-74.

[16] Vigo R. Categorical invariance and structural complexity in human concept learning. J Math Psychology 2009; 53: 203-221.

[17] Wolfram, W. A New Kind of Science. Champaign, IL, USA: Wolfram Media Inc., 2002.