FACTA UNIVERSITATIS
Series: **Electronics and Energetics** Vol. 28, No 1, March 2015, pp. 51 - 76
DOI: 10.2298/FUEE1501051S

BOOLEAN DIFFERENTIAL EQUATIONS - A COMMON MODEL FOR CLASSES, LATTICES, AND ARBITRARY SETS OF BOOLEAN FUNCTIONS

Bernd Steinbach[1] **and Christian Posthoff**[2]
[1]Institute of Computer Science, Freiberg University of
Mining and Technology, Bernhard-von-Cotta-Str. 2,
D-09596 Freiberg, Germany
[2]Department of Computing and Information Technology,
The University of the West Indies, Trinidad & Tobago

Abstract: The *Boolean Differential Calculus* (BDC) significantly extends the Boolean Algebra because not only Boolean values 0 and 1, but also changes of Boolean values or Boolean functions can be described. A *Boolean Differential Equation* (BDE) is a Boolean equation that includes derivative operations of the Boolean Differential Calculus. This paper aims at the classification of BDEs, the characterization of the respective solutions, algorithms to calculate the solution of a BDE, and selected applications. We will show that not only classes and arbitrary sets of Boolean functions but also lattices of Boolean functions can be expressed by Boolean Differential Equations.

In order to reach this aim, we give a short introduction into the BDC, emphasize the general difference between the solutions of a Boolean equation and a BDE, explain the core algorithms to solve a BDE that is restricted to all vectorial derivatives of $f(\mathbf{x})$ and optionally contains Boolean variables. We explain formulas for transforming other derivative operations to vectorial derivatives in order to solve more general BDEs. New fields of applications for BDEs are simple and generalized lattices of Boolean functions. We describe the construction, simplification and solution.

Received November 17, 2014
*An earlier version of this paper was presented as Invited Paper at the the 13th Serbian Mathematical Congress (SMC 2014), May 22-25, 2014, in Vrnjačka Banja, Serbia.
Corresponding author: Bernd Steinbach
Institute of Computer Science, Freiberg University of Mining and Technology, Bernhard-von-Cotta-Str. 2, D-09596 Freiberg, Germany
(e-mail: steinb@informatik)

The basic operations of XBOOLE are sufficient to solve BDEs. We demonstrate how a XBOOLE-problem program (PRP) of the freely available XBOOLE-Monitor quickly solves some BDEs.

Keywords: Boolean Differential Calculus, Boolean Differential Equation (BDE), classes of Boolean functions, lattices of Boolean functions, arbitrary sets of Boolean functions, Lattice-BDE, XBOOLE.

1 Introduction

Boolean variables are the simplest variables. A Boolean variable carries only one element of the set $\mathbb{B} = \{0, 1\}$. These two values can be easily distinguished from each other in technical systems. Therefore we get more and more digital systems.

Boolean functions, the operations of the Boolean Algebra, and Boolean equations [1] are well known to solve many tasks for digital systems. The solution of a Boolean equation is a set of Boolean vectors which describes, e.g., the behavior of a circuit. However, this theory is restricted to fixed values for a given point in time.

The *Boolean Differential Calculus* (BDC) [1–3] allows us to study the change of the values of Boolean variables and Boolean functions. The substitution of the derivative operations of the BDC into a Boolean equation leads to a *Boolean Differential Equation* (BDE) [4, 5].

A BDE has a more general solution and consequently opens a wider field of applications. We show in this paper how lattices of Boolean functions can be expressed by BDEs. We will show that additionally to the well known lattices of incompletely specified functions also more general lattices of Boolean functions can be described in an easy way using the new special *Lattice-BDE*. The generalized lattices of Boolean functions open a new field of applications.

The rest of this paper is organized as follows. Section 2 defines the derivative operations of the BDC and briefly explains their meaning. Section 3 summarizes the known theory of Boolean Differential Equations, introduces algorithms that calculates either sets of classes of Boolean functions or arbitrary sets of Boolean functions as the solution of a BDE, explains a method to map a more general BDE into the form needed for one of these algorithms, and shows how a XBOOLE-problem programs (PRP) can solve a BDE in the XBOOLE-Monitor.

Lattices of Boolean functions are discussed in Section 4 as a new field of applications of BDEs. Both the well known lattices that describe incompletely specified functions (ISF) and a more general type of lattices of Boolean functions are uniquely described using *Lattice-BDEs*. Several examples show that the known algorithm can be used to solve different types of *Lattice-BDEs*. Finally, Section 5 concludes this paper.

2 Derivative Operations of the Boolean Differential Calculus

The BDC defines the *Boolean Differential* dx which is also a Boolean variable that is equal to 1 in the case that x changes its value. Additionally, the BDC defines several differential operations of Boolean functions which describe certain general properties depending on possible directions of change. We confine ourselves to derivatives of the BDC where the direction of change is fixed.

For simple derivative operations the direction of change is restricted to a single variable x_i. The (simple) *derivative*

$$\frac{\partial f(x_i, \mathbf{x}_1)}{\partial x_i} = f(x_i = 0, \mathbf{x}_1) \oplus f(x_i = 1, \mathbf{x}_1) \tag{1}$$

is equal to 1 if the function $f(x_i, \mathbf{x}_1)$ changes its value when the value of x_i changes. The (simple) *minimum*

$$\min_{x_i} f(x_i, \mathbf{x}_1) = f(x_i = 0, \mathbf{x}_1) \wedge f(x_i = 1, \mathbf{x}_1) \tag{2}$$

is equal to 1 when the value of the function $f(x_i, \mathbf{x}_1)$ remains unchanged equal to 1 while the value of x_i changes. The (simple) *maximum*

$$\max_{x_i} f(x_i, \mathbf{x}_1) = f(x_i = 0, \mathbf{x}_1) \vee f(x_i = 1, \mathbf{x}_1) \tag{3}$$

is equal to 0 when the value of the function $f(x_i, \mathbf{x}_1)$ remains unchanged equal to 0 while the value of x_i changes.

Vectorial derivative operations similarly describe cases where all variables of the vector $\mathbf{x}_0$ change their values at the same point in time. The following formulas define the *vectorial derivative*, the *vectorial minimum*, and the *vectorial maximum*:

$$\begin{aligned}
\frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} &= f(\mathbf{x}_0, \mathbf{x}_1) \oplus f(\overline{\mathbf{x}}_0, \mathbf{x}_1) \ , && (4)\\
\min_{\mathbf{x}_0} f(\mathbf{x}_0, \mathbf{x}_1) &= f(\mathbf{x}_0, \mathbf{x}_1) \wedge f(\overline{\mathbf{x}}_0, \mathbf{x}_1) \ , && (5)\\
\max_{\mathbf{x}_0} f(\mathbf{x}_0, \mathbf{x}_1) &= f(\mathbf{x}_0, \mathbf{x}_1) \vee f(\overline{\mathbf{x}}_0, \mathbf{x}_1) \ . && (6)
\end{aligned}$$

The simple derivative operations can sequentially be executed with regard to different variables of a subset $\mathbf{x}_0$. Such m-fold derivative operations describe a special property for subspaces $\mathbf{x}_1 = const$. The following formulas define the *m-fold derivative*, the *m-fold minimum*, the *m-fold maximum*, and the Δ-*operation*:

$$\begin{aligned}
\frac{\partial^m f(\mathbf{x}_0,\mathbf{x}_1)}{\partial x_1 \partial x_2 \ldots \partial x_m} &= \frac{\partial}{\partial x_m}\left(\ldots\left(\frac{\partial}{\partial x_2}\left(\frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial x_1}\right)\right)\ldots\right) , && (7)\\
\min_{\mathbf{x}_0}{}^m f(\mathbf{x}_0,\mathbf{x}_1) &= \min_{x_m}\left(\ldots\left(\min_{x_2}\left(\min_{x_1} f(\mathbf{x}_0,\mathbf{x}_1)\right)\right)\ldots\right) , && (8)\\
\max_{\mathbf{x}_0}{}^m f(\mathbf{x}_0,\mathbf{x}_1) &= \max_{x_m}\left(\ldots\left(\max_{x_2}\left(\max_{x_1} f(\mathbf{x}_0,\mathbf{x}_1)\right)\right)\ldots\right) , && (9)\\
\Delta_{\mathbf{x}_0} f(\mathbf{x}_0,\mathbf{x}_1) &= \min_{\mathbf{x}_0}{}^m f(\mathbf{x}_0,\mathbf{x}_1) \oplus \max_{\mathbf{x}_0}{}^m f(\mathbf{x}_0,\mathbf{x}_1) . && (10)
\end{aligned}$$

Because of the limited space, we skip all theorems about relations between certain derivative operations and refer to [3,6].

3 Boolean Differential Equations

3.1 An Introductory Example

If we know the function $f(\mathbf{x})$ and need the result of any derivative operation then we simply apply the definition and get as result an uniquely specified Boolean function.

Example 1. *We take the Boolean function:*

$$f(\mathbf{x}) = f(x_1,x_2,x_3) = x_1 \vee x_2 x_3 \tag{11}$$

and use Definition (4) to calculate the vectorial derivative of $f(\mathbf{x})$ with regard to (x_1,x_3):

$$\begin{aligned}
\frac{\partial f(x_1,x_2,x_3)}{\partial(x_1,x_3)} &= f(x_1,x_2,x_3) \oplus f(\overline{x}_1,x_2,\overline{x}_3)\\
&= (x_1 \vee x_2 x_3) \oplus (\overline{x}_1 \vee x_2 \overline{x}_3)\\
&= x_1 \oplus x_2 x_3 \oplus x_1 x_2 x_3 \oplus \overline{x}_1 \oplus x_2 \overline{x}_3 \oplus \overline{x}_1 x_2 \overline{x}_3\\
&= (x_1 \oplus \overline{x}_1) \oplus x_2 (x_3 \oplus \overline{x}_3) \oplus x_2 (x_1 x_3 \oplus \overline{x}_1 \overline{x}_3)\\
&= \overline{x}_2 \oplus x_2 (\overline{x}_1 \oplus x_3)\\
&= \overline{x}_2 \vee (\overline{x}_1 \oplus x_3) ,
\end{aligned}$$

and get as result the unique Boolean function:

$$g(x_1,x_2,x_3) = \overline{x}_2 \vee (\overline{x}_1 \oplus x_3) . \tag{12}$$

Arrows in Figure 1 illustrate the pairs of function values which determine the result of this vectorial derivative. Different function values in these pairs lead to function values 1 in the calculated vectorial derivative.

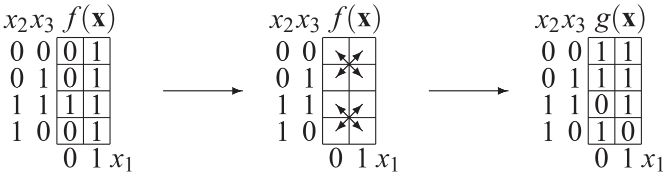


Fig. 1. Related function values of the vectorial derivative of Example 1

Tab. 1. Pairs of functions values and their result of: $\frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} = g(\mathbf{x}_0,\mathbf{x}_1)$

$f(\mathbf{x}_0,\mathbf{x}_1 = const.)$	$f(\overline{\mathbf{x}}_0,\mathbf{x}_1 = const.)$	$g(\mathbf{x}_0,\mathbf{x}_1 = const.)$	$g(\overline{\mathbf{x}}_0,\mathbf{x}_1 = const.)$
0	0	0	0
1	1	0	0
0	1	1	1
1	0	1	1

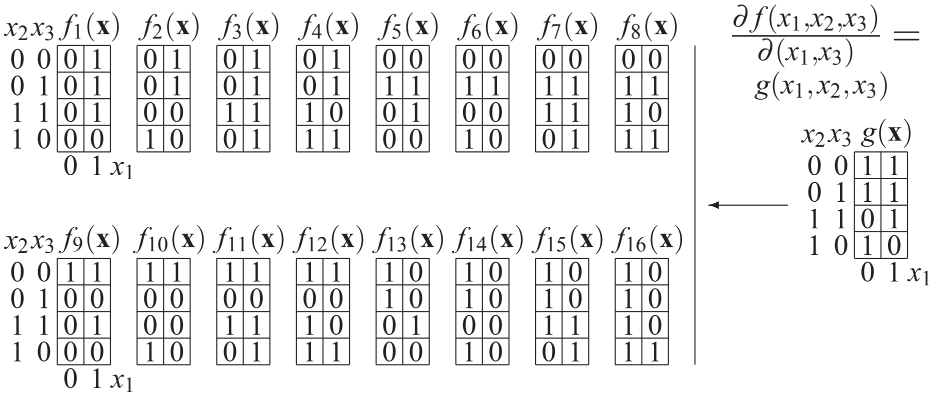
Now we consider the reverse situation that we know $g(\mathbf{x})$ and want to find the function $f(\mathbf{x})$ such that $g(\mathbf{x})$ is the result of a derivative operation of the unknown function $f(\mathbf{x})$. From Figure 1, we can conclude that the vectorial derivative of several functions $f(\mathbf{x})$ with regard to (x_1,x_3) result in the same function $g(\mathbf{x})$ (12). Table 1 shows that two different patterns of function values of $f(\mathbf{x})$ result for a vectorial derivative in the same pair of patterns of function values of $g(\mathbf{x})$. In the special case of Example 1 (see also Figure 1), the two possible patterns of pairs of function values for each of the four pairs lead to $4^2 = 16$ different function $f(\mathbf{x})$ with the same function $g(x_1,x_2,x_3)$ (12) as result of the vectorial derivative with regard to (x_1,x_3). Figure 2 shows the Karnaugh-maps of these 16 functions using the same encoding of the leftmost Karnaugh-maps for all of them. The original function $f(x_1,x_2,x_3)$ belongs to this set of functions and is labeled as $f_3(x_1,x_2,x_3)$ in Figure 2.

Another interesting question: is there for each given function $g(\mathbf{x}_0,\mathbf{x}_1)$ at least one solution function $f(\mathbf{x}_0,\mathbf{x}_1)$ of the simple BDE

$$\frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} = g(\mathbf{x}_0,\mathbf{x}_1)\ ? \tag{13}$$

Due to the commutativity of the $\oplus$-operations we have

$$g(\mathbf{x}_0,\mathbf{x}_1) = \frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} = f(\mathbf{x}_0,\mathbf{x}_1) \oplus f(\overline{\mathbf{x}}_0,\mathbf{x}_1) = \frac{\partial f(\overline{\mathbf{x}}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} = g(\overline{\mathbf{x}}_0,\mathbf{x}_1)\ . \tag{14}$$



x_2x_3	$f_1(\mathbf{x})$	$f_2(\mathbf{x})$	$f_3(\mathbf{x})$	$f_4(\mathbf{x})$	$f_5(\mathbf{x})$	$f_6(\mathbf{x})$	$f_7(\mathbf{x})$	$f_8(\mathbf{x})$
0 0	0 1	0 1	0 1	0 1	0 0	0 0	0 0	0 0
0 1	0 1	0 1	0 1	0 1	1 1	1 1	1 1	1 1
1 1	0 1	0 0	1 1	1 0	0 1	0 0	1 1	1 0
1 0	0 0	1 0	0 1	1 1	0 0	1 0	0 1	1 1
	0 1 x_1							

x_2x_3	$f_9(\mathbf{x})$	$f_{10}(\mathbf{x})$	$f_{11}(\mathbf{x})$	$f_{12}(\mathbf{x})$	$f_{13}(\mathbf{x})$	$f_{14}(\mathbf{x})$	$f_{15}(\mathbf{x})$	$f_{16}(\mathbf{x})$
0 0	1 1	1 1	1 1	1 1	1 0	1 0	1 0	1 0
0 1	0 0	0 0	0 0	0 0	1 0	1 0	1 0	1 0
1 1	0 1	0 0	1 1	1 0	0 1	0 0	1 1	1 0
1 0	0 0	1 0	0 1	1 1	0 0	1 0	0 1	1 1
	0 1 x_1							

$$\frac{\partial f(x_1,x_2,x_3)}{\partial(x_1,x_3)} = g(x_1,x_2,x_3)$$

x_2x_3	$g(\mathbf{x})$
0 0	1 1
0 1	1 1
1 1	0 1
1 0	1 0
	0 1 x_1

Fig. 2. Sixteen functions with the same vectorial derivative $g(x_1,x_2,x_3)$ (12).

Therefore a function $f(\mathbf{x}_0,\mathbf{x}_1)$ exists only in the case

$$\begin{aligned} g(\mathbf{x}_0,\mathbf{x}_1) &= g(\overline{\mathbf{x}}_0,\mathbf{x}_1) \\ g(\mathbf{x}_0,\mathbf{x}_1)\oplus g(\overline{\mathbf{x}}_0,\mathbf{x}_1) &= g(\overline{\mathbf{x}}_0,\mathbf{x}_1)\oplus g(\overline{\mathbf{x}}_0,\mathbf{x}_1) \\ g(\mathbf{x}_0,\mathbf{x}_1)\oplus g(\overline{\mathbf{x}}_0,\mathbf{x}_1) &= 0 \\ \frac{\partial g(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} &= 0\,. \end{aligned} \tag{15}$$

We call (15) the integrability condition and can conclude: the functions $f(\mathbf{x}_0,\mathbf{x}_1)$ of the BDE (13) exist if and only if $g(\mathbf{x}_0,\mathbf{x}_1)$ satisfies the integrability condition (15). All solution functions of the BDE (13) are given by

$$f_i(\mathbf{x}_0,\mathbf{x}_1) = x_i \wedge g(\mathbf{x}_0,\mathbf{x}_1)\oplus h_j(\mathbf{x}_0,\mathbf{x}_1) \tag{16}$$

with $\mathbf{x}_0 = (x_1,\ldots,x_i,\ldots,x_k)$, $\mathbf{x}_1 = (x_{k+1},\ldots,x_n)$, and

$$\frac{\partial h_j(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} = 0\,. \tag{17}$$

We learn from this example:

1. A Boolean Differential Equation $\frac{\partial f(x_1,x_2,x_3)}{\partial(x_1,x_3)} = g(x_1,x_2,x_3)$ includes the unknown function $f(x_1,x_2,x_3)$.

2. There are solutions of a BDE only if the right-hand function $g(x_1,x_2,x_3)$ satisfies a special integrability condition.

3. The general solution of an inhomogeneous BDE is built using a single special solution of the inhomogeneous BDE and the set of all solutions of the associated homogeneous BDE. The associated homogeneous BDE is built by replacing the right-hand side of an inhomogeneous BDE by 0.

4. *Generally, the solution of a Boolean Differential Equation is a set of Boolean functions*. This is a significant difference to Boolean equations. The solution of a Boolean equation is a set of Boolean vectors.

3.2 BDEs of Simple and Vectorial Derivatives - Separation of Classes

Generally, a Boolean Differential Equation (BDE) is an equation in which derivative operations of an unknown function $f(\mathbf{x})$ occur. In order to find a convenient solution method, we restrict in this subsection BDEs such that only the function $f(\mathbf{x})$ and all its simple and vectorial derivatives are allowed in expressions on both sides of an equation:

$$\begin{aligned} D_l & \left(f(\mathbf{x}), \frac{\partial f(\mathbf{x})}{\partial x_1}, \frac{\partial f(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0}, \ldots, \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}} \right) \\ & = D_r \left(f(\mathbf{x}), \frac{\partial f(\mathbf{x})}{\partial x_1}, \frac{\partial f(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0}, \ldots, \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}} \right) . \end{aligned} \tag{18}$$

Using the $\oplus$-operation, each BDE(18) can be transformed into a homogeneous restrictive BDE:

$$D \left(f(\mathbf{x}), \frac{\partial f(\mathbf{x})}{\partial x_1}, \frac{\partial f(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0}, \ldots, \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}} \right) = 0 . \tag{19}$$

The following definition supports the description of the solution procedure.

Definition 1. *Let $g(\mathbf{x})$ be a solution function of (19). Then*

1.

$$\left[g(\mathbf{x}), \frac{\partial g(\mathbf{x})}{\partial x_1}, \frac{\partial g(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial g(\mathbf{x})}{\partial \mathbf{x}} \right]_{\mathbf{x}=\mathbf{c}} \tag{20}$$

is a local solution for $\mathbf{x} = \mathbf{c}$,

2.

$$\mathrm{D}(u_0, u_1, \ldots, u_{2^n-1}) = 0 \tag{21}$$

is the Boolean equation, associated to the Boolean Differential Equation (19), and has the set of local solutions SLS.

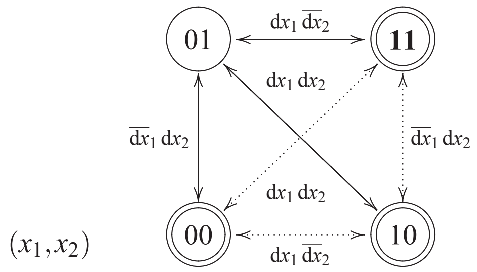

01
11
00
10
(x_1,x_2)
$\mathrm{d}x_1\,\overline{\mathrm{d}x_2}$
$\mathrm{d}x_1\,\mathrm{d}x_2$
$\overline{\mathrm{d}x_1}\,\mathrm{d}x_2$
$\overline{\mathrm{d}x_1}\,\mathrm{d}x_2$
$\mathrm{d}x_1\,\mathrm{d}x_2$
$\mathrm{d}x_1\,\overline{\mathrm{d}x_2}$

Fig. 3. Values of the function $g(x_1,x_2) = x_1 \vee \overline{x}_2$ and their simple and vectorial derivatives for $(x_1,x_2) = (1,1)$.

3.

$$\nabla g(\mathbf{x}) = \left(g(\mathbf{x}), \frac{\partial g(\mathbf{x})}{\partial x_1}, \frac{\partial g(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial g(\mathbf{x})}{\partial \mathbf{x}} \right) \tag{22}$$

The local solutions (20) are the key to solve a BDE. The values of the simple and vectorial derivatives in a single selected point of the Boolean space specify the function values in all other points of this space. Figure 3 shows the function $g(x_1,x_2) = x_1 \vee \overline{x}_2$ where function values 1 are indicated by double circles, values 1 of derivatives are indicated by solid arrows, and values 0 of derivatives are indicated by dotted arrows.

Example 2. *Assume, we know the local solution for* $(x_1,x_2) = (1,1)$ *as depicted in Figure 3. Then we can conclude:*

- *due to the known point:* $g(\mathbf{x})|_{(x_1,x_2)=(11)} = 1 \rightarrow g(1,1) = 1$,
- *due to the direction of change* $\mathrm{d}x_1\,\overline{\mathrm{d}x_2}$*:* $\left.\frac{\partial g(\mathbf{x})}{\partial x_1}\right|_{(x_1,x_2)=(11)} = 1 \rightarrow g(0,1) = 0$,
- *due to the direction of change* $\overline{\mathrm{d}x_1}\,\mathrm{d}x_2$*:* $\left.\frac{\partial g(\mathbf{x})}{\partial x_2}\right|_{(x_1,x_2)=(11)} = 0 \rightarrow g(1,0) = 1$, *and*
- *due to the direction of change* $\mathrm{d}x_1\,\mathrm{d}x_2$*:* $\left.\frac{\partial g(\mathbf{x})}{\partial (x_1,x_2)}\right|_{(x_1,x_2)=(11)} = 0 \rightarrow g(0,0) = 1$.

Hence, a possible solution function $g(\mathbf{x}) = x_1 \vee \overline{x}_2$ *could be reconstructed based on the knowledge of the local solution in a single point of the Boolean space.*

The BDE (19) contains all elements of $\nabla f(\mathbf{x})$ either in non-negated or negated form. Hence, all these elements can be encoded by Boolean variables u_i as shown in Table 2.

Tab. 2. Mapping of the BDE into the associated Boolean equation

index	binary code	u_i	associated element
0	$(0\dots00)$	u_0	$f(\mathbf{x})$
1	$(0\dots01)$	u_1	$\frac{\partial f(\mathbf{x})}{\partial x_1}$
2	$(0\dots10)$	u_2	$\frac{\partial f(\mathbf{x})}{\partial x_2}$
3	$(0\dots11)$	u_3	$\frac{\partial f(\mathbf{x})}{\partial (x_1,x_2)}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
2^n-1	$(1\dots11)$	u_{2^n-1}	$\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}$

The result of this substitution is an *associated Boolean equation* $D(\mathbf{u}) = 0$. The solution of this Boolean equation is the set of all local solutions $SLS(\mathbf{u})$. There are local solutions for which no global solution functions of the BDE (19) exist. The sufficient condition for a global solution function of the BDE (19) is that a local solution exists for each point of the Boolean space B^n:

$$\forall \mathbf{c} \in B^n \quad \nabla f(\mathbf{x}) \left.\right|_{\mathbf{x}=\mathbf{c}} \in SLS(\mathbf{u}) \ . \tag{23}$$

An important consequence of (23) is that the solutions of the BDE (19) consist of classes of Boolean functions as characterized by Theorem 1; the proof is given in [4,5].

Theorem 1. *If the Boolean function $f(\mathbf{x})$ is a solution function of the Boolean Differential Equation (19), then all Boolean functions*

$$f(x_1,x_2,...,x_n) = f(x_1 \oplus c_1, x_2 \oplus c_2, ..., x_n \oplus c_n) \tag{24}$$

for $\mathbf{c} = (c_1,\dots,c_n) \in B^n$ are also solution functions of (19).

The set of local solutions $SLS(\mathbf{u})$ expresses by u_0 the function value in one point of B^n and by u_i, $0 < i < 2^n$, the values of changes with regard to all the other points of B^n. The separation of function classes becomes easier when the function value in all points of B^n are uniquely given. The function d2v (*derivative to value*) uses (25) to transform the set $SLS(\mathbf{u})$ into the set $SLS'(\mathbf{v})$.

$$\begin{aligned} v_0 &= u_0 \ , \\ v_i &= u_0 \oplus u_i \ , \quad \text{with} \quad i = 1,2,...,2^n-1 \ . \end{aligned} \tag{25}$$

Due to (24), the exchange of x_i and $\overline{x}_i$ does not change the set of solution functions. The function `epv` (*exchange of pairs of values*) realizes this exchange:

$$SLST(\mathbf{v}) = \texttt{epv}(SLS'(\mathbf{v}), i) \ . \tag{26}$$

Applied to variables v_i this exchange is described by:

$$\begin{aligned} v_{(m+2k\cdot 2^{i-1})} &\iff v_{(m+(2k+1)\cdot 2^{i-1})} \ , \\ \text{with} \quad i &= 1, 2, ..., n \ , \\ m &= 0, 1, ..., 2^{i-1} - 1 \ , \\ k &= 0, 1, ..., 2^{n-i} - 1 \ . \end{aligned} \tag{27}$$

Table 3 enumerates the index pairs which are used in the function `epv` for Boolean spaces up to $\mathbb{B}^4$.

Tab. 3. Index pairs defined by (27) for the exchange of function values

$i = 1$	$i = 2$	$i = 3$	$i = 4$
$0 \Leftrightarrow 1$	$0 \Leftrightarrow 2$	$0 \Leftrightarrow 4$	$0 \Leftrightarrow 8$
$2 \Leftrightarrow 3$	$1 \Leftrightarrow 3$	$1 \Leftrightarrow 5$	$1 \Leftrightarrow 9$
$4 \Leftrightarrow 5$	$4 \Leftrightarrow 6$	$2 \Leftrightarrow 6$	$2 \Leftrightarrow 10$
$6 \Leftrightarrow 7$	$5 \Leftrightarrow 7$	$3 \Leftrightarrow 7$	$3 \Leftrightarrow 11$
$8 \Leftrightarrow 9$	$8 \Leftrightarrow 10$	$8 \Leftrightarrow 12$	$4 \Leftrightarrow 12$
$10 \Leftrightarrow 11$	$9 \Leftrightarrow 11$	$9 \Leftrightarrow 13$	$5 \Leftrightarrow 13$
$12 \Leftrightarrow 13$	$12 \Leftrightarrow 14$	$10 \Leftrightarrow 14$	$6 \Leftrightarrow 14$
$14 \Leftrightarrow 15$	$13 \Leftrightarrow 15$	$11 \Leftrightarrow 15$	$7 \Leftrightarrow 15$

The intersection of the given set $SLS'(\mathbf{v})$ with the exchanged set $SLST(\mathbf{v})$ for all variables x_i separates the set of global solution functions from the local solutions which are not sufficient. Algorithm 1 describes the procedure to solve the BDE (19) in detail. The solution vectors $\mathbf{v}$ of Algorithm 1 specify, substituted into (28), all solution functions of the BDE (19).

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) = {} & \overline{x}_1 \overline{x}_2 \ldots \overline{x}_n \wedge v_0 \vee x_1 \overline{x}_2 \ldots \overline{x}_n \wedge v_1 \vee \ldots \vee \\ & x_1 x_2 \ldots x_n \wedge v_{2^n - 1} \end{aligned} \tag{28}$$

3.3 BDEs of Simple and Vectorial Derivatives as well as Variables - Separation of Arbitrary Function Sets

The solution of a Boolean Differential Equation of the type (18) is a set of function classes characterized by (24). Additional Boolean variables $\mathbf{x}$ in a Boolean Differential Equation of the type (29) restrict the derivatives to certain points of the

Algorithm 1 Separation of function classes

```
Require: BDE (19) with function $f(\mathbf{x})$ containing $n$ variables
Ensure: set of Boolean vectors $\mathbf{v} = (v_0, v_1, \ldots, v_{2^n-1})$ that describe, substituted in
    (28), the set of all solution functions of the BDE (19)
$SLS(\mathbf{u}) \leftarrow$ solution of BE (21) associated with BDE (19)
$SLS'(\mathbf{v}) \leftarrow \texttt{d2v}(SLS(\mathbf{u}))$
for $i \leftarrow 1$ to $n$ do
    $SLST(\mathbf{v}) \leftarrow \texttt{epv}(SLS'(\mathbf{v}), i)$
    $SLS'(\mathbf{v}) \leftarrow SLS'(\mathbf{v}) \cap SLST(\mathbf{v})$
end for
```

Boolean space. Therefore, selected functions of the function classes can belong to the set of solution functions. Hence, a BDE (29) has an arbitrary set of Boolean functions as solution.

$$\begin{aligned} D_l &\left(f(\mathbf{x}), \frac{\partial f(\mathbf{x})}{\partial x_1}, \frac{\partial f(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} \ldots, \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}, \mathbf{x} \right) \\ &= D_r \left(f(\mathbf{x}), \frac{\partial f(\mathbf{x})}{\partial x_1}, \frac{\partial f(\mathbf{x})}{\partial x_2}, \ldots, \frac{\partial f(\mathbf{x}_0, \mathbf{x}_1)}{\partial \mathbf{x}_0} \ldots, \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}}, \mathbf{x} \right) . \end{aligned} \tag{29}$$

A BDE (29) can be solved using a slightly modified algorithm. The variables $\mathbf{x}$ remain in the associated Boolean equation (30) associated to (29):

$$\begin{aligned} &\mathrm{D}_l(u_0, u_1, \ldots, u_{2^n-1}, x_1, x_2, \ldots, x_n) \\ &\qquad = \mathrm{D}_r(u_0, u_1, \ldots, u_{2^n-1}, x_1, x_2, \ldots, x_n) . \end{aligned} \tag{30}$$

A detailed analysis in [4] reveals that the local solutions must be split into the cofactors S_0 for $x_i = 0$ and S_1 for $x_i = 1$ and the exchange of function pairs must be restricted to S_1. Algorithm 2 describes the detailed steps to solve a BDE (29).

3.4 More General Boolean Differential Equations

In addition to the simple and vectorial derivatives all other derivative operations can be used within a BDE. We do not need special solution algorithms for such more general Boolean Differential Equations because the theorems of the BDC allow us the transformation of all types of derivative operations into the elements of $\nabla f(\mathbf{x})$

Algorithm 2 Separation of functions

Require: BDE (29) in which the function $f(\mathbf{x})$ depends on n variables

Ensure: set S of Boolean vectors $\mathbf{v} = (v_0, v_1, \ldots, v_{2^n-1})$ that describe, substituted in (28), the set of all solution functions of the BDE (29)

```
$SLS(\mathbf{u},\mathbf{x}) \leftarrow$ solution of the BE (30) associated with BDE (29)
$S(\mathbf{v},\mathbf{x}) \leftarrow \mathtt{d2v}(SLS(\mathbf{u},\mathbf{x}))$
for $i \leftarrow 1$ to $n$ do
    $S_0(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)) \leftarrow \max_{x_i} [\overline{x}_i \wedge S(\mathbf{v},x_i,\ldots,x_n)]$
    $S_1(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)) \leftarrow \max_{x_i} [x_i \wedge S(\mathbf{v},x_i,\ldots,x_n)]$
    $ST_1(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)) \leftarrow \mathtt{epv}(S_1(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)),i)$
    $S(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)) \leftarrow S_0(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i)) \cap ST_1(\mathbf{v},\mathbf{x} \setminus (x_1,\ldots,x_i))$
end for
```

(22).

$$\min_{x_i} f(\mathbf{x}) = f(\mathbf{x}) \wedge \overline{\frac{\partial f(\mathbf{x})}{\partial x_i}} \tag{31}$$

$$\max_{x_i} f(\mathbf{x}) = f(\mathbf{x}) \vee \frac{\partial f(\mathbf{x})}{\partial x_i} \tag{32}$$

$$\min_{\mathbf{x}_0} f(\mathbf{x}_0,\mathbf{x}_1) = f(\mathbf{x}_0,\mathbf{x}_1) \wedge \overline{\frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0}} \tag{33}$$

$$\max_{\mathbf{x}_0} f(\mathbf{x}_0,\mathbf{x}_1) = f(\mathbf{x}_0,\mathbf{x}_1) \vee \frac{\partial f(\mathbf{x}_0,\mathbf{x}_1)}{\partial \mathbf{x}_0} \tag{34}$$

$$\min_{(x_1,x_2)}{}^2 f(\mathbf{x}) = f(\mathbf{x}) \wedge \overline{\frac{\partial f(\mathbf{x})}{\partial x_1}} \wedge \overline{\frac{\partial f(\mathbf{x})}{\partial x_2}} \wedge \overline{\frac{\partial f(\mathbf{x})}{\partial (x_1,x_2)}} \tag{35}$$

$$\max_{(x_1,x_2)}{}^2 f(\mathbf{x}) = f(\mathbf{x}) \vee \frac{\partial f(\mathbf{x})}{\partial x_1} \vee \frac{\partial f(\mathbf{x})}{\partial x_2} \vee \frac{\partial f(\mathbf{x})}{\partial (x_1,x_2)} \tag{36}$$

$$\frac{\partial^2 f(\mathbf{x})}{\partial x_1 \partial x_2} = \frac{\partial f(\mathbf{x})}{\partial x_1} \oplus \frac{\partial f(\mathbf{x})}{\partial x_2} \oplus \frac{\partial f(\mathbf{x})}{\partial (x_1,x_2)} \tag{37}$$

$$\Delta_{(x_1,x_2)} f(\mathbf{x}) = \frac{\partial f(\mathbf{x})}{\partial x_1} \vee \frac{\partial f(\mathbf{x})}{\partial x_2} \vee \frac{\partial f(\mathbf{x})}{\partial (x_1,x_2)} \tag{38}$$

General formulas to express the simple or vectorial minimum or maximum by the function $f(\mathbf{x})$ and simple or vectorial derivatives are given in (31),..., (34). The equations (35),..., (38) describe how all 2-fold derivative operations can be transformed into expressions that contain only the function $f(\mathbf{x})$ and simple or vectorial derivatives. These formulas can be generalized for any $m \leq n$ of functions in $\mathbb{B}^n$ [6].

Using these transformations each more general BDE results either in the BDE

(18) for which the solution classes can be calculated using Algorithm 1, or it results in the BDE (29) so that the arbitrary solution set is found using Algorithm 2.

3.5 Solving a Boolean Differential Equations Using a XBOOLE PRP

The XBOOLE-Monitor can be downloaded (for free) from:

```
http://www.informatik.tu-freiberg.de/xboole/
```

and provides many operations which can be applied to sets of Boolean functions. All XBOOLE-operations are explained in the help-system of the XBOOLE-Monitor.

We summarize here some XBOOLE-operations needed to solve a BDE. All XBOOLE-objects are indicated by numbers. The XBOOLE-operations can be executed in the XBOOLE-Monitor by means of

1. a selected and parametrized menu item,
2. a tool-bar button followed by the same dialog to specify the parameters,
3. a XBOOLE-command that specifies both the operation and the objects, and
4. a XBOOLE-problem program (PRP) that contains a sequence of commands.

The main data structure is the *ternary vector list* (TVL). All XBOOLE-operations are executed in a Boolean space. The user must specify the number of Boolean variables which can be used in a Boolean space using the XBOOLE-command:

```
space vmax sno
```

where `vmax` is the number of variables and `sno` is the number of the space.

Variables in a wanted order can be attached to an XBOOLE-space using:

```
avar sni
```

where on the next lines the names of the variables separated by a space and finished by a point (.) are declared. A Boolean equation or a system of Boolean equations is solved using:

```
sbe sni tno
```

where `tno` is the object number of the result TVL and the Boolean equation is given on the following lines finished by a point (.) using the operation signs ‘`/`’ for the negation, ‘`&`’ for the conjunction $\wedge$, ‘`+`’ for the disjunction $\vee$, ‘`#`’ for the antivalence $\oplus$, ‘`=`’ for the equivalence $\odot$ as well as for separating both sides of the equation, and ‘`,`’ to separate the equations within a system of Boolean equations. Logic operations for the input TVL (`tni`, `tni1`, `tni2`) and the calculation of the output TVL (`tno`) are given by:

- negation $f_o = \overline{f}$ (complement):

```
cpl tni tno
```

- conjunction $f_o = f_1 \wedge f_2$ (intersection):

  ```
  isc tni1 tni2 tno
  ```

- disjunction $f_o = f_1 \vee f_2$ (union):

  ```
  uni tni1 tni2 tno
  ```

- antivalence $f_o = f_1 \oplus f_2$ (symmetric difference):

  ```
  syd tni1 tni2 tno
  ```

- equivalence $f_o = f_1 \odot f_2$ (complement of the symmetric difference):

  ```
  csd tni1 tni2 tno
  ```

An ordered set of variables can be defined as a XBOOLE-object called *variables tuple* (VT) using:

```
vtin sni vtno
```

followed by the variable in the needed order as in the case of the command `avar`. Two such VTs define ordered pairs of variables which can be changed using:

```
cco tni vtni1 vtni2 tno
```

where the exchange of columns of `tni` is realized for all defined pair of variables. Alternatively the VTs can be directly specified within a special XBOOLE-command:

```
_cco tni <x1 x2> <x8 x9> tno
```

which exchanges, e.g., column x_1 with column x_8 and column x_2 with column x_9. A single VT is used to specify the variables for a vectorial or *m*-fold derivative operation; e.g.:

```
maxk tni vtni tno
```

calculates the *k*-fold maximum with regard to all variables specified in VT `vtni` and

```
_maxk tni <xi x2> tno
```

calculates the 2-fold maximum with regard to (x_1, x_2).

Example 3. *Bent functions [7–9] are the most non-linear functions which are needed in cryptography. The simplest bent functions are specified by the BDE:*

$$\frac{\partial^2 f(x_1,x_2)}{\partial x_1 \partial x_2} = 1 \; . \tag{39}$$

Using (37) we get the equivalent BDE:

$$\frac{\partial f(x_1,x_2)}{\partial x_1} \oplus \frac{\partial f(x_1,x_2)}{\partial x_2} \oplus \frac{\partial f(x_1,x_2)}{\partial (x_1,x_2)} = 1 \; . \tag{40}$$

This BDE contains two simple and and one vectorial derivative. Hence, it can be solved using Algorithm 1. The associated Boolean equation of (40) is

$$u_1 \oplus u_2 \oplus u_3 = 1 \ . \tag{41}$$

```
1  space 32 1
2  avar 1
3  u0 u1 u2 u3 v0 v1 v2 v3.
4  sbe 1 1
5  u1#u2#u3=1.
6  sbe 1 2
7  v0=u0,
8  v1=u0#u1,
9  v2=u0#u2,
10 v3=u0#u3.
11 isc 1 2 3
12 vtin 1 4
13 u0 u1 u2 u3.
14 maxk 3 4 5
15 vtin 1 6
16 v0 v2.
17 vtin 1 7
18 v1 v3.
19 cco 5 6 7 8
20 isc 5 8 9
21 vtin 1 10
22 v0 v1.
23 vtin 1 11
24 v2 v3.
25 cco 9 10 11 12
26 isc 9 12 13
```

Fig. 4. Listing of the PRP to solve the BDE (40).

Figure 4 show the PRP that can be used by the XBOOLE-Monitor to solve BDE (40). The solution of (41) is stored as XBOOLE-object 1. The lines 6 to 14 in Figure 4 realize the `d2v`*-transformation of line 2 of Algorithm 1 so that the XBOOLE-object 5 stores* $SLS'(\mathbf{v})$. *The first sweep of the loop in lines 3 to 6 of Algorithm 1 is executed in lines 15 to 20 and the second sweep of this loop leads to the XBOOLE-object 13 as final result in lines 21 to 26 of Figure 4.*

Table 4 shows in the left part the solution TVL of BDE (40). The eight **v**-*vectors describe two classes of Boolean functions. The expressions of these functions are built by the substitution of the* **v**-*vectors of the solution into (28). Table 4 shows these functions in the right part associated to the classes 1 and 2.*

4 Boolean Differential Equations for Lattices of Boolean Functions

4.1 Lattices of Incompletely Specified Boolean Functions

A lattice of Boolean function is a special set of functions that has the following properties:

- if both $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ belong to the lattice then $f(\mathbf{x}) = f_1(\mathbf{x}) \wedge f_2(\mathbf{x})$ belongs also to this lattice of Boolean functions, and

Tab. 4. Solution functions of BDE (40)

v_0	v_1	v_2	v_3	class 1	class 2
0	1	1	1	$x_1 \vee x_2$	
1	0	0	0		$\overline{x}_1 \wedge \overline{x}_2$
1	0	1	1	$\overline{x}_1 \vee x_2$	
0	1	0	0		$x_1 \wedge \overline{x}_2$
0	0	0	1		$x_1 \wedge x_2$
1	1	1	0	$\overline{x}_1 \vee \overline{x}_2$	
1	1	0	1	$x_1 \vee \overline{x}_2$	
0	0	1	0		$\overline{x}_1 \wedge x_2$

- if both $f_1(\mathbf{x})$ and $f_2(\mathbf{x})$ belong to the lattice then $f(\mathbf{x}) = f_1(\mathbf{x}) \vee f_2(\mathbf{x})$ belongs also to this lattice of Boolean functions.

A lattice of Boolean function is very often used for the design of a digital circuit. Based on another point of view, such a lattice is sometimes called *incompletely specified function* (ISF).

One method to describe the lattice of functions of an ISF uses two mark functions called:

1. ON-set $q(\mathbf{x})$: all functions of the lattice must be equal to one for $q(\mathbf{x}) = 1$, and
2. OFF-set $r(\mathbf{x})$: all functions of the lattice must be equal to zero for $r(\mathbf{x}) = 1$.

Using these known mark functions each function $f(\mathbf{x})$ of the set of functions $\{f_i(\mathbf{x})\}$ must hold the inequalities:

$$f(\mathbf{x}) \geq q(\mathbf{x}) \,, \tag{42}$$

$$f(\mathbf{x}) \leq \overline{r(\mathbf{x})} \,, \tag{43}$$

which can be transformed into the equivalent restrictions:

$$\overline{f(\mathbf{x})} \wedge q(\mathbf{x}) = 0 \,, \tag{44}$$

$$f(\mathbf{x}) \wedge r(\mathbf{x}) = 0 \,. \tag{45}$$

The system of equations (44) and (45) can be merged into a single Boolean equation:

$$\overline{f(\mathbf{x})} \wedge q(\mathbf{x}) \vee f(\mathbf{x}) \wedge r(\mathbf{x}) = 0 \,. \tag{46}$$

The functions $q(\mathbf{x})$ and $r(\mathbf{x})$ in (46) are known and can be represent by expressions of Boolean variables connected by Boolean operations. The term $f(\mathbf{x})$ in (46) describes the unknown functions of the lattice. Hence, the equation (46) fits to the type of Boolean Differential Equations (29), where only $f(\mathbf{x})$ and variables x_i but no simple or vectorial derivatives occur. All functions of a lattice which is specified by the BDE (46) can be calculated using Algorithm 2.

Example 4. *Let $q(\mathbf{x}) = x_1 x_3 \vee \overline{x}_2 \overline{x}_3$ and $r(\mathbf{x}) = \overline{x}_1 x_2$ be the given mark functions of a lattice of Boolean functions $f(\mathbf{x})$. Using (46), we get the BDE of this lattice:*

$$\overline{f(\mathbf{x})} \wedge (x_1 x_3 \vee \overline{x}_2 \overline{x}_3) \vee f(\mathbf{x}) \wedge \overline{x}_1 x_2 = 0 \tag{47}$$

and the associated Boolean equation:

$$\overline{u}_0 \wedge (x_1 x_3 \vee \overline{x}_2 \overline{x}_3) \vee u_0 \wedge \overline{x}_1 x_2 = 0 \; . \tag{48}$$

Figure 5 shows the PRP that is used in the XBOOLE-Monitor to solve the BDE (47). After the definition of the Boolean space $\mathbb{B}^{32}$ in line 1; the used variables are defined in lines 2 to 5, and the associated Boolean equation is solved in lines 6 to 8. The BDE (47) contains only $f(\mathbf{x})$ out of the vector $\nabla f(\mathbf{x})$ so that the transformation `d2v` *can be restricted to the mapping of u_0 to v_0 in lines 9 to 14.*

Due to the existing variables x_i Algorithm 2 must be used to separate the set of solution functions. All steps of the loop of lines 3 to 8 of Algorithm 2 are realized in lines 15 to 53 of the PRP in Figure 5. The lines 15 to 27 of the PRP describe the first sweep of this loop for x_1. The indices of the variables v_i are taken from the first four rows of column $i = 1$ of Table 3 where the VT 11 uses the left values and the VT 12 the right values. The intermediate solution of this sweep is stored into the same XBOOLE-object 5 that represent the function S of Algorithm 2. Hence, the fragment of lines 15 to 27 of the first sweep of the loop can be reused in lines 28 to 40 for the second sweep with x_2 and the VTs specified by column $i = 2$ of Table 3 and in lines 41 to 53 for the third sweep with x_3 and the VTs specified by column $i = 3$ of Table 3, respectively.

Tab. 5. Solution functions of BDE (47)

v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	solution functions
1	1	0	1	1	1	0	1	$f_1(\mathbf{x}) = x_1 \vee \overline{x}_2$
1	1	0	1	0	1	0	1	$f_2(\mathbf{x}) = x_1 \vee \overline{x}_2 \overline{x}_3$
1	1	0	0	1	1	0	1	$f_3(\mathbf{x}) = x_1 x_3 \vee \overline{x}_2$
1	1	0	0	0	1	0	1	$f_4(\mathbf{x}) = x_1 x_3 \vee \overline{x}_2 \overline{x}_3$

```
space 32 1
avar 1
u0
v0 v1 v2 v3 v4 v5 v6 v7
x1 x2 x3.
sbe 1 1
/u0&(x1&x3+/x2&/x3)+
u0&(/x1&x2)=0.
sbe 1 2
v0=u0.
isc 1 2 3
vtin 1 4
u0.
maxk 3 4 5
sbe 1 6
x1=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v2 v4 v6.
vtin 1 12
v1 v3 v5 v7.
cco 10 11 12 13
isc 8 13 5
sbe 1 6
x2=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v1 v4 v5.
vtin 1 12
v2 v3 v6 v7.
cco 10 11 12 13
isc 8 13 5
sbe 1 6
x3=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v1 v2 v3.
vtin 1 12
v4 v5 v6 v7.
cco 10 11 12 13
isc 8 13 5
```

Fig. 5. Listing of the PRP to solve the BDE (47).

Table 5 enumerates the four solution functions of the BDE (47) calculated by the XBOOLE-Monitor using the PRP of Figure 5. The columns v_3 and v_4 show that this lattice contains all functions which are smaller or equal to the supremum function $f_1(\mathbf{x})$ and greater or equal to the infimum function $f_4(\mathbf{x})$.

4.2 Generalized Lattices of Boolean Functions

Each derivative operation transforms a given lattice of Boolean functions into another lattice of Boolean functions. The resulting lattices are more general because the function values 0 and 1 cannot only be chosen for a single **x**-pattern, but also for pairs of $\mathbf{x}$-patterns. The proof that all derivative operations of any lattice result in such a generalized lattice is given for the first time in [10]. The generalized lattices are described in [10] by the mark function $q(\mathbf{x})$ and $r(\mathbf{x})$ as well as an *independence matrix* (IDM) that have the shape of an echelon and elements below the main diagonal are equal to 0. The IDM describes all independent directions of change where no function of the lattice changes its values. Associated to the independence matrix *IDM* an *independence function* $f^{id}(\mathbf{x})$ is defined in [10]. Knowing the mark functions $q(\mathbf{x})$ and $r(\mathbf{x})$ and the independence function $f^{id}(\mathbf{x})$, a Boolean equation given in [10] allows us to check for each function $f(\mathbf{x})$ whether it belongs to the generalized lattice or not.

Instead of the two mark functions and the independence matrix we suggest here a *single Boolean Differential Equation* to describe a generalized lattice of Boolean functions. The directions, in which no function of the lattice changes its values, are described in a restrictive BDE by simple and vectorial derivatives which are connected by disjunctions ($\vee$):

$$\bigvee_{i=1}^{n} \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}_{0i}} = 0 \;, \tag{49}$$

where

- i is the row index of the IDM,
- values 1 in the row of IDM specify the variables of $\mathbf{x}_{0i}$, and
- $\frac{\partial f(\mathbf{x})}{\partial \mathbf{x}_{0i}} = 0$ if all elements of the i-th row in IDM(f) are equal to 0.

A BDE (50) can be solved by Algorithm 1, and the special structure of the BDE ensures that the set of classes of solution function describes a lattice of Boolean functions.

Example 5. *The generalized lattice of the Boolean function $f(x_1,x_2,x_3)$ in which all functions do not change their function values if either x_1 and x_3 or x_2 and x_3 are commonly changed at the same point in time can be described by the BDE:*

$$\frac{\partial f(\mathbf{x})}{\partial (x_1,x_3)} \vee \frac{\partial f(\mathbf{x})}{\partial (x_2,x_3)} = 0 \tag{50}$$

and the associated Boolean equation:

$$u_5 \vee u_6 = 0 \;. \tag{51}$$

Figure 6 shows the PRP that is used in the XBOOLE-Monitor to solve the BDE (50). After the definition of the Boolean space $\mathbb{B}^{32}$ in line 1; the used variables are

```
1  space 32 1
2  avar 1
3  u0 u5 u6
4  v0 v1 v2 v3 v4 v5 v6 v7.
5  sbe 1 1
6  u5+u6=0.
7  sbe 1 2
8  v0=u0,
9  v5=u0#u5,
10 v6=u0#u6.
11 isc 1 2 3
12 vtin 1 4
13 u0 u5 u6.
14 maxk 3 4 5
15 vtin 1 6
16 v0 v2 v4 v6.
17 vtin 1 7
18 v1 v3 v5 v7.
19 cco 5 6 7 8
20 isc 5 8 5
21 vtin 1 6
22 v0 v1 v4 v5.
23 vtin 1 7
24 v2 v3 v6 v7.
25 cco 5 6 7 8
26 isc 5 8 5
27 vtin 1 6
28 v0 v1 v2 v3.
29 vtin 1 7
30 v4 v5 v6 v7.
31 cco 5 6 7 8
32 isc 5 8 5
```

Fig. 6. Listing of the PRP to solve the BDE (50).

Tab. 6. Solution functions of BDE (50)

v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	class 1	class 2	class 3
1	1	1	1	1	1	1	1	$f_1(\mathbf{x}) = 1$		
1	0	0	1	0	1	1	0		$f_2(\mathbf{x}) = \overline{x}_1 \oplus x_2 \oplus x_3$	
0	1	1	0	1	0	0	1		$f_3(\mathbf{x}) = x_1 \oplus x_2 \oplus x_3$	
0	0	0	0	0	0	0	0			$f_4(\mathbf{x}) = 0$

defined in lines 2 to 4, and the associated Boolean equation is solved in lines 5 to 6. The BDE (50) contains only two vectorial derivatives out of the vector $\nabla f(\mathbf{x})$ so that the transformation `d2v` *can be restricted to the mapping of u_5 to v_5 and u_6 to v_6 in lines 7 to 14, where u_0 is needed as counterpart to v_0.*

Due to missing variables x_i Algorithm 1 can be used to separate the classes of solution functions. All steps of the loop of lines 3 to 6 of Algorithm 1 are realized in lines 15 to 32 of the PRP in Figure 6. The lines 15 to 20 of the PRP describe the first sweep of this loop for the exchange of x_1. The indices of the variables v_i are taken from the first four rows of column $i = 1$ of Table 3 where the VT 6 uses the left values and the VT 7 the right values. The intermediate solution of this sweep is stored into the same XBOOLE-object 5 that represents the function SLS′ of Algorithm 1. Hence, the fragment of lines 15 to 20 of the first sweep of the loop can be reused in lines 21 to 26 for the second sweep with regard to x_2 and the VTs specified by column $i = 2$ of Table 3 and in lines 27 to 32 for the third sweep with regard to x_3 and the VTs specified by column $i = 3$ of Table 3, respectively.

Table 6 enumerates the four solution functions of the BDE (50) calculated by the XBOOLE-Monitor using the PRP of Figure 6. The solution of the BDE (50) consists of three classes of Boolean functions. The class 1 only contains the function $f_1(\mathbf{x}) = 1$ *that is the supremum* $\overline{r(\mathbf{x})}$ *of the lattice. Due to (24) a solution class in* $\mathbb{B}^3$ *generally contains* $2^3 = 8$ *functions. Two times four of these functions are identical in case of class 2:*

$$\begin{aligned} f_2(\mathbf{x}) &= \bar{x}_1 \oplus x_2 \oplus x_3 = x_1 \oplus \bar{x}_2 \oplus x_3 = x_1 \oplus x_2 \oplus \bar{x}_3 = \bar{x}_1 \oplus \bar{x}_2 \oplus \bar{x}_3 \ , \\ f_3(\mathbf{x}) &= x_1 \oplus x_2 \oplus x_3 = \bar{x}_1 \oplus \bar{x}_2 \oplus x_3 = \bar{x}_1 \oplus x_2 \oplus \bar{x}_3 = x_1 \oplus \bar{x}_2 \oplus \bar{x}_3 \ . \end{aligned}$$

The class 3 only contains the function $f_4(\mathbf{x}) = 0$ *that is the infimum* $q(\mathbf{x})$ *of the lattice. The solution lattice contains only two of* $2^8 - 2 = 254$ *functions of* $\mathbb{B}^3$ *which are greater than* $q(\mathbf{x}) = 0$ *and smaller than* $\overline{r(\mathbf{x})} = 1$. *Nevertheless, the four function of Table 6 constitute a lattice—both the conjunction and the disjunction of any pair of these function result in one of these functions.*

It should be mentioned that there are four different BDE having the same lattice of solutions shown in Table 6. The most extended BDE with this solution lattice is:

$$\frac{\partial f(\mathbf{x})}{\partial(x_1,x_2)} \vee \frac{\partial f(\mathbf{x})}{\partial(x_1,x_3)} \vee \frac{\partial f(\mathbf{x})}{\partial(x_2,x_3)} = 0 \ . \tag{52}$$

The equivalent other three BDE with the same solution are built by omitting one of the three vectorial derivatives:

$$\frac{\partial f(\mathbf{x})}{\partial(x_1,x_3)} \vee \frac{\partial f(\mathbf{x})}{\partial(x_2,x_3)} = 0 \ , \tag{53}$$

$$\frac{\partial f(\mathbf{x})}{\partial(x_1,x_2)} \vee \frac{\partial f(\mathbf{x})}{\partial(x_2,x_3)} = 0 \ , \tag{54}$$

$$\frac{\partial f(\mathbf{x})}{\partial(x_1,x_2)} \vee \frac{\partial f(\mathbf{x})}{\partial(x_1,x_3)} = 0 \ , \tag{55}$$

where (53) is identical with (50) and used in Example 5. The reason for these alternative BDE with the same solution lattice is that only two of the three directions of change in (52) of the vectorial derivatives are linearly independent. Two algorithms in [10] describe how the *unique independent directions of change* can be found. The BDE (53) is the unique representative BDE for the solution lattice of Table 6.

Example 5 explores a generalized lattice with the special mark functions $q(\mathbf{x}) = 0$ and $r(\mathbf{x}) = 0$, in order to emphasize that only a special subset of functions between these two mark function belong to the lattice. However, this restriction is not necessary. The BDE (46) can be combined with the BDE (49) to the BDE of a most general lattice:

$$\overline{f(\mathbf{x})} \wedge q(\mathbf{x}) \vee f(\mathbf{x}) \wedge r(\mathbf{x}) \vee \bigvee_{i=1}^{n} \frac{\partial f(\mathbf{x})}{\partial \mathbf{x}_{0i}} = 0 \; . \tag{56}$$

Example 6. *We assume that a generalized lattice of the Boolean function $f(\mathbf{x})$ is described by the BDE:*

$$\begin{aligned} \overline{f(\mathbf{x})} \wedge (\overline{(x_1 \oplus x_3)} \wedge (x_2 \oplus x_4)) \vee f(\mathbf{x}) \wedge ((x_1 \oplus x_3) \wedge (x_2 \oplus x_4)) \vee \\ \frac{\partial f(\mathbf{x})}{\partial (x_1, x_3)} \vee \frac{\partial f(\mathbf{x})}{\partial (x_2, x_4)} &= 0 \end{aligned} \tag{57}$$

which has the associated Boolean equation:

$$\overline{f(\mathbf{x})} \wedge (\overline{(x_1 \oplus x_3)} \wedge (x_2 \oplus x_4)) \vee f(\mathbf{x}) \wedge ((x_1 \oplus x_3) \wedge (x_2 \oplus x_4)) \vee u_5 \vee u_{10} = 0 \; . \tag{58}$$

Figure 7 shows the PRP that is used to solve the BDE (57) *of a most general lattice of Boolean functions. After the definition of the Boolean space $\mathbb{B}^{32}$ in line 1; the used variables are defined in lines 2 to 8, and the associated Boolean equation is solved in lines 9 to 12. The BDE* (57) *contains only $f(\mathbf{x})$ and two vectorial derivatives out of the vector $\nabla f(\mathbf{x})$ so that the transformation* `d2v` *can be restricted to the mapping of $u0$ to $v0$, $u5$ to $v5$, and $u10$ to $v10$, in lines 13 to 20.*

Due to the existing variables x_i Algorithm 2 must be used to separate the set of solution functions which have the structure of a lattice due to the structure of the BDE to be solved. All steps of the loop of lines 3 to 8 of Algorithm 2 are realized in lines 21 to 80 of the PRP in Figure 7. The lines 21 to 35 of the PRP describe the first sweep of this loop for x_1. The indices of the variables v_i are taken from the column $i = 1$ of Table 3 where the VT 11 uses the left values and the VT 12 the right values. The intermediate solution of this sweep is stored to the same XBOOLE-object 5 that represent the function S of Algorithm 2. Hence, the fragment of lines 21 to 35 of the first sweep of the loop can be reused in lines 36 to 50 for the second sweep with x_2 and the VTs specified by column $i = 2$ of Table 3, in lines 51 to 65 for the third sweep with x_3 and the VTs specified by column $i = 3$, and finally in lines 66 to 80 for the fourth sweep with x_4 and the VTs specified by column $i = 4$ of Table 3, respectively.

Table 7 enumerates the four solution functions of the BDE (57) calculated by the XBOOLE-Monitor using the PRP of Figure 7. The function values in the columns $v_0, \ldots, v_{15}$ confirm that the calculated four functions form a lattice. It can also be seen in these columns that not all functions which are smaller than the supremum f_1 and larger than the infimum f_4 belong to this generalized lattice of Boolean functions.

```
space 32 1
avar 1
u0 u5 u10
v0 v1 v2 v3
v4 v5 v6 v7
v8 v9 v10 v11
v12 v13 v14 v15
x1 x2 x3 x4.
sbe 1 1
/u0&(/(x1#x3)&(x2#x4))+
u0&((x1#x3)&(x2#x4))+
u5+u10=0.
sbe 1 2
v0=u0,
v5=u0#u5,
v10=u0#u10.
isc 1 2 3
vtin 1 4
u0 u5 u10.
maxk 3 4 5
sbe 1 6
x1=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v2 v4 v6
v8 v10 v12 v14.
vtin 1 12
v1 v3 v5 v7
v9 v11 v13 v15.
cco 10 11 12 13
isc 8 13 5
sbe 1 6
x2=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v1 v4 v5
v8 v9 v12 v13.
vtin 1 12
v2 v3 v6 v7
v10 v11 v14 v15.
cco 10 11 12 13
isc 8 13 5
sbe 1 6
x3=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v1 v2 v3
v8 v9 v10 v11.
vtin 1 12
v4 v5 v6 v7
v12 v13 v14 v15.
cco 10 11 12 13
isc 8 13 5
sbe 1 6
x4=0.
isc 5 6 7
maxk 7 6 8
cpl 6 6
isc 5 6 9
maxk 9 6 10
vtin 1 11
v0 v1 v2 v3
v4 v5 v6 v7.
vtin 1 12
v8 v9 v10 v11
v12 v13 v14 v15.
cco 10 11 12 13
isc 8 13 5
```

Fig. 7. Listing of the PRP to solve the BDE (57).

Tab. 7. Solution functions of BDE (57)

v_0	v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}	v_{15}	solution functions
1	1	1	0	1	1	0	1	1	0	1	1	0	1	1	1	$f_1(\mathbf{x}) = (\bar{x}_1 \oplus x_3) \vee (\bar{x}_2 \oplus x_4)$
1	0	1	0	0	1	0	1	1	0	1	0	0	1	0	1	$f_2(\mathbf{x}) = \bar{x}_1 \oplus x_3$
0	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	$f_3(\mathbf{x}) = x_1 \oplus x_2 \oplus x_3 \oplus x_4$
0	0	1	0	0	0	0	1	1	0	0	0	0	1	0	0	$f_4(\mathbf{x}) = (\bar{x}_1 \oplus x_3) \wedge (x_2 \oplus x_4)$

5 Conclusions

The Boolean Differential Calculus extends the field of application of the Boolean Algebra significantly. Simple and vectorial derivative operations evaluate pairs of function values in the selected direction of change. The values of m-fold derivative operations depend on values of the given function in whole subspaces.

An unknown function $f(\mathbf{x})$ and derivative operations of this function appear in Boolean expressions on both sides of a Boolean Differential Equation (BDE). The solution of each BDE is a set of Boolean functions. This is an important extension to a Boolean equation which has a set of binary vectors as solution.

The explored algorithms allow us to solve BDEs which describe either sets of classes of Boolean functions or arbitrary sets of Boolean functions. We demonstrated that these algorithms can easily be implemented using the XBOOLE-Monitor. The used problem programs (PRP) show all details of the introduced algorithms to solve a BDE. Using the XBOOLE-Library all these steps can be wrapped by special programs such that the set of solution functions of a BDE is automatically created.

The algorithms known from [4,5] are able to separate (depending on the type of the BDE) either classes of solution functions or arbitrary sets of solution functions. We presented in this paper special types of BDEs which either combine certain classes to a lattice of Boolean functions or restrict the arbitrary sets of solutions to a lattice of Boolean functions.

There is a wide field of applications of BDEs. Many examples are explained in [4]. Here, we introduced three new types of BDEs. All of them describe lattices of Boolean functions.

1. A BDE of the type (46) describes a well known and widely used lattice of Boolean functions that can alternatively be expressed by an incompletely specified function. Such a BDE can be solved using Algorithm 2.

2. A BDE of the type (49) describes a lattice with the infimum function $q(\mathbf{x}) = 0$ and the supremum function $\overline{r(\mathbf{x})} = 1$ and can be solved using Algorithm

1. Such a lattice contains not all functions which are greater than $q(\mathbf{x})$ and smaller than $\overline{r(\mathbf{x})}$.

3. A BDE of the more general type (56) merges the BDEs of the cases 1 and 2. Such a BDE must be solved using Algorithm 2 because the mark functions $q(\mathbf{x})$ and $r(\mathbf{x})$ are not limited to the case 2.

It can be very difficult to find a BDE for a needed set of Boolean functions. However, it is an advantage that BDEs for lattices can be built in a straight manner based on the mentioned types. Therefore, we call BDEs of the types (46), (49), and (56) *Lattice-BDEs*.

The result of a Lattice-BDE (49) or (56) is a generalized lattice of Boolean functions that cannot be expressed by an incompletely specified function. In this way these Lattice-BDEs opens many new fields of applications, e.g., in circuit design. Vice versa, the Lattice-BDE (46) is a sub-type of the most general Lattice-BDE (56) so that the so far widely used lattices of Boolean functions fitting to an incompletely specified Boolean function are integrated in the new theory in a natural manner. It is a challenge for the future to utilize Lattice-BDEs for specific applications.

References

[1] C. Posthoff and B. Steinbach, *Logic Functions and Equations - Binary Models for Computer Science*. Dordrecht: Springer, 2004.

[2] B. Steinbach and C. Posthoff, “Boolean Differential Calculus,” in *Progress in Applications of Boolean Functions*. Morgan & Claypool Publishers, San Rafael, CA - USA, 2010, pp. 55–78.

[3] ——, “Boolean Differential Calculus - theory and applications,” *Journal of Computational and Theoretical Nanoscience*, vol. 7, no. 6, pp. 933–981, 2010.

[4] ——, *Boolean Differential Equations*. Morgan & Claypool Publishers, 2013.

[5] B. Steinbach, “Lösung binärer Differentialgleichungen und ihre Anwendung auf binäre Systeme,” Ph.D. dissertation, TH Karl-Marx-Stadt (Germany), 1981.

[6] D. Bochmann and C. Posthoff, *Binre dynamische Systeme*. Munich, Vienna: Oldenbourg, 1981.

[7] O. S. Rothaus, “On ”bent” functions,” *J. Combinatorial Theory*, vol. 20, pp. 300–305, 1976.

[8] B. Steinbach and C. Posthoff, “Classification and generation of bent functions,” in *Proceedings Reed-Muller 2011 Workshop*, Gustavelund Conference Centre, Tuusula, Finnland, 2011, pp. 81–91.

[9] ——, “Classes of bent functions identified by specific normal forms and generated using boolean differential equations,” *FACTA UNIVERSITATIS (NIŠ)*, vol. 24, no. 3, pp. 357–383, 2011.

[10] B. Steinbach, “Generalized lattices of boolean functions utilized for derivative operations,” in *Materiały konferencyjne KNWS’13*, Łagów, Poland, 2013, pp. 1–17.