International Journal of Mathematical, Engineering and Management Sciences
Vol. 7, No. 5, 670-680, 2022
https://doi.org/10.33889/IJMEMS.2022.7.5.044

Atomic Formulation of the Boolean Curve Fitting Problem

Ahmed S. Balamesh
Department of Electrical and Computer Engineering,
King Abdulaziz University, Jeddah, Saudi Arabia.
Corresponding author: abalamesh@kau.edu.sa

Ali M. Rushdi
Department of Electrical and Computer Engineering,
King Abdulaziz University, Jeddah, Saudi Arabia.
E-mail: arushdi@kau.edu.sa

(Received on February 26, 2022; Accepted on July 10, 2022)

Abstract
Boolean curve fitting is the process of finding a Boolean function that takes given values at certain points in its Boolean domain. The problem boils down to solving a set of 'big' Boolean equations that may or may not be consistent. The usual formulation of the Boolean curve fitting problem is quite complicated, indeed. In this paper, we formulate the Boolean curve fitting problem using the technique of atomic decomposition of Boolean equations. This converts the problem into a set of independent switching equations. We present the solution of these switching equations and express the solution in very simple and compact forms. We also present the consistency and uniqueness conditions for this problem again in very compact forms. A few illustrative examples are given. These examples clearly pinpoint the simplicity gained by the Boolean-equation solving step within the overall Boolean-fitting procedure. The method presented here can be applied to the design of Boolean functions for cryptographic systems.

Keywords- Boolean curve fitting; Boolean equations; Atomic decomposition; Cryptography.

1. Introduction

The solution of Boolean equations has received wide and continuous attention in the open literature. The classical work of Rudeanu (1974) is one of the most complete and influencing treatments of Boolean equations and functions. Brown (1990) explores the theory of Boolean equation solving and a wide range of related methods. Many recent methods of solving Boolean equations have been reported in the literature, e.g., (Balamesh & Rushdi, 2019; Barotov & Barotov, 2022; Rudeanu, 2010; Rushdi, 2001; Rushdi & Albarakati, 2014; Rushdi & Amashah, 2011; Tapia & Tucker, 1980). Applications of Boolean equation solving include circuit analysis (Rudeanu, 1959), digital circuit design (Rushdi & Ba-Rukab, 2003; Rushdi & Zagzoog, 2019; Rushdi & Ahmad, 2018), cryptography (Ahmad & Rushdi, 2018; Chai et al., 2008; Fedotova-Piven et al., 2019; Kochemazov et al., 2020), and many other diverse applications, e.g., (de Mesquita et al., 2022; Ishchukova et al., 2020; Kalkan et al., 2022; Marovac, 2018; Pakhomchik et al., 2022; Steinbach & Posthoff, 2015).

The problem of Boolean curve fitting (BCF), also known as Boolean interpolation, was handled as a pure mathematical curiosity during the past century. Contributions to solutions of the BCF problem culminated in a unified solution presented in the classical treatise on Boolean functions and equations by Rudeanu (1974). This unified solution is derived by solving a system of Boolean equations over a finite (atomic) Boolean algebra other than the two-valued one, referred to herein as a 'big' Boolean algebra. As a result, the existence of a solution (or solutions) of the BCF problem might require the satisfaction of a certain condition, called 'the consistency condition.' Boolean curve fitting has witnessed a recent revival, as it

finally found a particularly useful engineering application in the area of cryptography (Ahmad & Rushdi, 2018).

The present paper is a part of an ongoing effort to transfer the BCF problem from the domain of pure mathematics to that of engineering and problem solving. Our purpose is to convert the solution approach for the BCF problem from one of declarative specifications (a mathematical approach) to one of constructive procedures (an engineering approach). To achieve this, we utilize a novel method for Boolean-equation solving via the atomic decomposition of the underlying Boolean equation into several independent switching (two-valued Boolean) equations (Balamesh & Rushdi, 2019).

The organization of the remainder of this paper is as follows. Section 2 reviews the concepts of atomic decomposition of Boolean variables and functions. Section 3 presents a brief mathematical introduction to the BCF problem, while Section 4 introduces an atomic representation for it. Section 5 supports and clarifies the exposition of Section 4 via a few demonstrative examples. Section 6 concludes the paper.

2. Atomic Decomposition of Boolean Variables and Functions

In this paper, we consider a finite (atomic) Boolean algebra **B** with M atoms $\{q_0, q_1, \dots, q_{M-1}\}$. The number of elements in **B** is $|\mathbf{B}| = 2^M$. In the following, we will use '$\vee$' for the 'OR' operator and either '$\wedge$', '.', or juxtaposition for the 'AND' operator, and an overabar for the 'NOT' operator.

Balamesh and Rushdi (2019) have shown that any element in a finite (atomic) Boolean algebra **B** has a unique decomposition in terms of the atoms of the Boolean algebra. In particular, an element $p \in \mathbf{B}$ has a unique decomposition of the form

$$p = \bigvee_{m=0}^{M-1} p_m q_m. \tag{1}$$

where $p_m \in \{0,1\}, m = 0,1, \dots, M-1$. We call p_m the mth atomic component of p and we loosely call the vector $\mathbf{p} = (p_0, p_1, \dots, p_{M-1}) \in \{0,1\}^M$ the atomic decomposition of p, and we will write $\mathcal{A}(p) = \mathbf{p}$ and $\mathcal{A}_{|m}(p) = p_m$. It can be easily seen that $\mathcal{A}(0) = (0, \dots, 0)$ and $\mathcal{A}(1) = (1, \dots, 1)$.

Moreover, in (Balamesh & Rushdi, 2019), it is shown that any Boolean function or expression has a unique atomic decomposition. The mth atomic component of a Boolean function or expression can be obtained by replacing each variable and constant in the function or expression by its mth atomic component.

We will use $p_{|m}$ to denote the mth atomic component of the variable or constant p and $x_{n|m}$ to denote the mth atomic component of x_n. The latter will be used for any number or any type of transcripts. In addition, for a vector $\mathbf{x} = (x_1, x_2, \dots, x_L)$, we will use $\mathbf{x}_{|m}$ to denote the vector composed of the mth atomic components of the elements of the vector, i.e.

$$\mathbf{x}_{|m} = \left(x_{1|m}, x_{2|m}, \dots, x_{L|m}\right). \tag{2}$$

In a similar fashion, for any entity **A**, we will use $\mathbf{A}_{|m}$ to denote an entity obtained by replacing the elements of **A** with their mth atomic components.

3. On Boolean Curve Fitting

In this section, we summarize from (Rudeanu, 1974) the main results known on Boolean curve fitting or Boolean interpolation. The problem at hand requires the determination of a Boolean curve whose graph passes through K given points $(z_1, \mathbf{x}_1), (z_2, \mathbf{x}_2), \dots, (z_K, \mathbf{x}_K)$ of the Boolean space $\mathbf{B}^{N+1}$,

where $\mathbf{x}_k = (x_{k,1}, x_{k,2}, \dots, x_{k,N}) \in \mathbf{B}^N, k = 1,2, \dots, K$ and $z_k \in \mathbf{B}, k = 1,2, \dots, K$. This means finding a Boolean function $f: \mathbf{B}^N \to \mathbf{B}$ such that

$$f(\mathbf{x}_k) = z_k, \ k = 1,2, \dots, K. \tag{3}$$

It is reasonable to assume that the $\mathbf{x}_k$'s are distinct. This is clear since if we assume that $\mathbf{x}_r = \mathbf{x}_s$, then we have two possibilities: either $z_r = z_s$ or $z_r \neq z_s$. The former will lead to two identical conditions, i.e., the conditions in (3) are redundant. In this case, we can remove the redundancy and readjust M. The latter will lead to a contradiction, i.e., the same $\mathbf{x}_k$ is mapped to two distinct z_k's. Of course, this, as we will see later, will be caught by the consistency condition required for solving the required Boolean equation. Actually, this consistency condition will enforce itself at the atomic level.

In this paper, we assume that **B** is finite and, therefore, atomic. If the problem is consistent (i.e., has a solution), the solution is (Balamesh & Rushdi, 2019; Rudeanu, 1974; Rushdi & Balamesh, 2017)

$$f(\mathbf{X}) = \bigvee_{\mathbf{u} \in \{0,1\}^N} f(\mathbf{u}) \mathbf{X}^{\mathbf{u}}, \tag{4}$$

where,

$$f(\mathbf{u}) = \left(\bigvee_{k=1}^{K} z_k \mathbf{x}_k^{\mathbf{u}}\right) \vee p_{\mathbf{u}} \bigwedge_{k=1}^{K} \overline{\mathbf{x}_k^{\mathbf{u}}}, \tag{5}$$

$$\mathbf{X} = (X_1, X_2, \dots, X_N) \in \mathbf{B}^N, u = (u_1, u_2, \dots, u_N) \in \{0,1\}^N,$$

$$\mathbf{X}^{\mathbf{u}} = \bigwedge_{n=1}^{N} X_n^{u_n} = X_1^{u_1} X_2^{u_2} \cdots X_N^{u_N} = \bigwedge_{n=1}^{N} (X_n \odot u_n), \tag{6}$$

and

$$\mathbf{x}_k^{\mathbf{u}} = \bigwedge_{n=1}^{N} x_{k,n}^{u_n} = x_{k,1}^{u_1} x_{k,2}^{u_2} \cdots x_{k,N}^{u_N} = \bigwedge_{n=1}^{N} (x_{k,n} \odot u_n). \tag{7}$$

In Equations (6) and (7), x^u is defined as

$$x^u = \begin{cases} x, & \text{if } u = 1 \\ \bar{x}, & \text{if } u = 0 \end{cases} = x \odot u, \tag{8}$$

where, '$\odot$' is the 'XNOR' operator. Complementing (8), we have

$$\overline{x^u} = \overline{x \odot u} = x \oplus u = x^{\bar{u}} = \bar{x}^u, \tag{9}$$

where '$\oplus$' is the 'XOR' operator. Note that for $\mathbf{x}, \mathbf{u} \in \{0,1\}^N, \mathbf{x}^{\mathbf{u}} = 1$ if and only if $\mathbf{x} = \mathbf{u}$.

The parameter $p_{\mathbf{u}}$ in (5) belongs to the underlying Boolean algebra **B**, and it can be chosen independently for each **u**. It should be noted here that different values of $p_{\mathbf{u}}$ do not necessarily produce distinct solutions of (3). In other words, although there are $|\mathbf{B}|$ possible values for $p_{\mathbf{u}}$ and 2^N possible values for **u**, we are not sure if there are $2^N|\mathbf{B}|$ distinct Boolean functions satisfying (3). It is not easy to find the number of distinct solutions from (4) and (5). In Section 4, we will give a simple method to find the number of distinct solutions.

The consistency and uniqueness conditions for the solution of Equation (4) are (Rudeanu, 1974):

C0. Consistency Condition: For any $k, h \in \{1,2, \dots, K\}$,

$$(z_k \oplus z_h) \bigwedge_{n=1}^{N} (x_{k,n} \odot x_{h,n}) = 0. \tag{10}$$

U0. Uniqueness Condition: For any $\mathbf{u} \in \{0,1\}^N$,
$\bigwedge_{k=1}^{K} \overline{\mathbf{x}_k^{\mathbf{u}}} = 0.$ (11)

Note that Equation (5) provides independent solutions (over the choice of $\mathbf{u} \in \{0,1\}^N$) for $f(\mathbf{u})$. Therefore, if the uniqueness condition (11) is satisfied for a given $\mathbf{u}$, then $f(\mathbf{u})$ has a unique solution. Otherwise, $f(\mathbf{u})$ has up to $|\mathbf{B}|$ distinct solutions.

4. Atomic Representation of the Curve Fitting Problem

Let $(X_{n|0}, X_{n|1}, \dots, X_{n|M-1})$, $(x_{k,n|0}, x_{k,n|1}, \dots, x_{k,n|M-1})$, $(z_{k|0}, z_{k|1}, \dots, z_{k|M-1})$, and $(p_{\mathbf{u}|0}, p_{\mathbf{u}|1}, \dots, p_{\mathbf{u}|M-1})$ be, respectively, the atomic decompositions of X_n, $x_{k,n}$, z_k and $p_{\mathbf{u}}$. Note that, since $\mathbf{u}$ has binary components, then $\mathbf{u}_{|m} = \mathbf{u}$.

Now, we will derive the mth atomic component of the solution in (4) and (5). Replacing each entry in (4) and (5) with its mth atomic component, we get
$f_{|m}(\mathbf{X}_{|m}) = \bigvee_{\mathbf{u}\in\{0,1\}^N} f_{|m}(\mathbf{u})\mathbf{X}_{|m}^{\mathbf{u}},$ (12)

where,
$f_{|m}(\mathbf{u}) = \left(\bigvee_{\substack{k=1 \\ z_k=1}}^{K} \mathbf{x}_{k|m}^{\mathbf{u}} \right) \vee p_{(\mathbf{u};m)} \bigwedge_{k=1}^{K} \overline{\mathbf{x}_{k|m}^{\mathbf{u}}}.$ (13)

We remind the reader here that all entities in (12) and (13) are binary. Moreover, since $p_{\mathbf{u}|m} \in \{0,1\}$, we have replaced it with $p_{(\mathbf{u};m)} \in \{0,1\}$ to indicate an arbitrarily binary parameter that can be chosen independently for each pair $(\mathbf{u}; m)$. Equation (13) gives independent solutions for $f_{|m}(\mathbf{u})$ for each pair $(\mathbf{u}; m)$.

The mth atomic component of Equation (10) is
$(z_{k|m} \oplus z_{h|m}) \bigwedge_{n=1}^{N} (x_{k,n|m} \odot x_{h,n|m}) = 0.$ (14)

Since all variables in (14) are binary, the equation is equivalent to
$z_{k|m} \oplus z_{h|m} = 0$ or $\bigwedge_{n=1}^{N} (x_{k,n|m} \odot x_{h,n|m}) = 0.$ (15)

Equation (15) is equivalent to the following statement:
C1. Consistency Condition: For any $m \in \{0,1,\dots,M-1\}$ and $k, h \in \{1,2,\dots,K\}$, at least one of the following is true:
(a) $z_{k|m} = z_{h|m}$,
and
(b) $\mathbf{x}_{k|m} \neq \mathbf{x}_{h|m}$,

where, $\mathbf{x}_{k|m} = (x_{k,1|m}, x_{k,2|m}, \dots, x_{k,n|m})$.

The consistency condition means that no two vectors $\mathbf{x}_k$ and $\mathbf{x}_h$ which are identical in some atomic component(s) are mapped to two z's which are different in that (those) same atomic component(s). This means that 'at the atomic level,' two identical vectors cannot map to two different z's. Although this might look trivial, it is really not. It is a remarkable consequence of the atomic decomposition.

Similarly, the mth atomic component of (11) is

$$\Lambda_{k=1}^{K} \overline{\mathbf{x}_{k|m}^{\mathbf{u}}} = 0. \tag{16}$$

Since all entries in (16) are binary, it is equivalent to the following statement:
U1. Uniqueness Condition: For any $m \in \{0,1,\dots,M-1\}$ and any $u \in \{0,1\}^N$, there exists $k \in \{1,2,\dots,K\}$ such that $\mathbf{x}_{k|m} = \mathbf{u}$.

Note that if the uniqueness condition is satisfied for a pair $(\mathbf{u}; m)$, then there is a unique solution for $f_{|m}(\mathbf{u})$. Otherwise, $f_{|m}(\mathbf{u})$ will have at most two distinct solutions, one for each choice of $p_{(\mathbf{u};m)} \in \{0,1\}$. We will show later that, in the latter case, $f_{|m}(\mathbf{u})$ will have exactly two distinct solutions.

From (7), we can get the mth atomic component $\mathbf{x}_{k|m}^{\mathbf{u}}$ of $\mathbf{x}_{k}^{\mathbf{u}}$ as

$$\mathbf{x}_{k|m}^{\mathbf{u}} = \Lambda_{n=1}^{N} x_{k,n|m}^{u_n} = \Lambda_{n=1}^{N}\left(x_{k,n|m} \odot u_n\right) = \begin{cases} 0, & \mathbf{x}_{k|m} \neq \mathbf{u} \\ 1, & \mathbf{x}_{k|m} = \mathbf{u} \end{cases}. \tag{17}$$

Complementing (17), we get

$$\overline{\mathbf{x}_{k|m}^{\mathbf{u}}} = \overline{\left(\Lambda_{n=1}^{N}\left(x_{k,n|m} \odot u_n\right)\right)} = \mathrm{V}_{n=1}^{N}\left(x_{k,n|m} \oplus u_n\right) = \begin{cases} 1, & \mathbf{x}_{k|m} \neq \mathbf{u} \\ 0, & \mathbf{x}_{k|m} = \mathbf{u} \end{cases}. \tag{18}$$

To represent our results in a more concise form, for each $m \in \{0,1,\dots,M-1\}$, we define

$$\mathcal{C}_{|m} = \left\{\mathbf{x}_{k|m} : k = 1,2,\dots,K\right\}, \tag{19}$$

$$\mathcal{C}_{0|m} = \left\{\mathbf{x}_{k|m} : z_{k|m} = 0, k = 1,2,\dots,K\right\}, \tag{20}$$

and

$$\mathcal{C}_{1|m} = \left\{\mathbf{x}_{k|m} : z_{k|m} = 1, k = 1,2,\dots,K\right\}. \tag{21}$$

Using the new notation, we can see that

$$\mathrm{V}_{\substack{k=1 \\ z_k=1}}^{K} \mathbf{x}_{k|m}^{\mathbf{u}} = \begin{cases} 1, & \mathbf{u} \in \mathcal{C}_{1|m} \\ 0, & \text{otherwise} \end{cases}, \tag{22}$$

and

$$\Lambda_{k=1}^{K} \overline{\mathbf{x}_{k|m}^{\mathbf{u}}} = \overline{\mathrm{V}_{k=1}^{K} \mathbf{x}_{k|m}^{\mathbf{u}}} = \begin{cases} 0, & \mathbf{u} \in \mathcal{C}_{|m} \\ 1, & \text{otherwise} \end{cases}. \tag{23}$$

Additionally, we note that

$$\mathrm{V}_{\substack{k=1 \\ z_k=1}}^{K} \mathbf{x}_{k|m}^{\mathbf{u}} \leq \mathrm{V}_{k=1}^{K} \mathbf{x}_{k|m}^{\mathbf{u}} = \overline{\Lambda_{k=1}^{K} \overline{\mathbf{x}_{k|m}^{\mathbf{u}}}}. \tag{24}$$

This means that

$$\Lambda_{k=1}^{K} \overline{\mathbf{x}_{k|m}^{\mathbf{u}}} = 1 \Rightarrow \mathrm{V}_{\substack{k=1 \\ z_k=1}}^{K} \mathbf{x}_{k|m}^{\mathbf{u}} = 0. \tag{25}$$

Using the definitions (19)-(21), the consistency condition becomes:
C2. Consistency Condition: For any $m \in \{0,1,\dots,M-1\}$, $\mathcal{C}_{0|m} \cap \mathcal{C}_{1|m} = \emptyset$.

On the other hand, the uniqueness condition becomes:
U2a. Uniqueness Condition: For any $m \in \{0,1,\dots,M-1\}$ and any $\mathbf{u} \in \{0,1\}^N$, $\mathbf{u} \in \mathcal{C}_{|m}$.

If the uniqueness condition is satisfied for all $(\mathbf{u};m)$, then it is equivalent to:
U2b. Uniqueness Conditions: For any $m \in \{0,1,\dots,M-1\}$, $\mathcal{C}_{|m} = \{0,1\}^N$.

Using (22)-(25) and assuming that the consistency condition holds for a given $(\mathbf{u};m)$, (i.e. $\mathcal{C}_{0|m} \cap \mathcal{C}_{1|m} = \emptyset$), we recast Equation (13) in the form

$$f_{|m}(\mathbf{u}) = \begin{cases} 1, & \mathbf{u} \in \mathcal{C}_{1|m} \\ 0, & \mathbf{u} \in \mathcal{C}_{0|m} \\ p_{(\mathbf{u};m)}, & \mathbf{u} \notin \mathcal{C}_{|m} \end{cases}. \tag{26}$$

From (26), we can see that the number of distinct solutions for the Boolean curve fitting problem is

$$2^{|\{(\mathbf{u};m):\mathbf{u}\notin\mathcal{C}_{|m}\}|} = 2^{\sum_m (2^N - |\mathcal{C}_{|m}|)} = 2^{M2^N - \sum_m |\mathcal{C}_{|m}|}. \tag{27}$$

where $|\{\cdot\}|$ denotes the cardinality of, or the number of elements in, the set $\{\cdot\}$.

Finally, using (12) and (26), and the atomic composition, we get

$$f(\mathbf{X}) = \bigvee_{m=0}^{M-1} q_m \bigvee_{\mathbf{u}\in\{0,1\}^N} f_{|m}(\mathbf{u})\mathbf{X}^{\mathbf{u}} = \bigvee_{\mathbf{u}\in\{0,1\}^N} \left[\bigvee_{\substack{m=0 \\ \mathbf{u}\in\mathcal{C}_{1|m}}}^{M-1} q_m \vee \bigvee_{\substack{m=0 \\ \mathbf{u}\notin\mathcal{C}_{|m}}}^{M-1} p_{(\mathbf{u};m)} q_m \right] \mathbf{X}^{\mathbf{u}}. \tag{28}$$

5. Illustrative Examples

The following three examples have previously been solved in (Rushdi & Balamesh, 2019) using the methods of (Rudeanu, 1974) with the aid of variable-entered Karnaugh maps. Here, we solve the same examples using the atomic formulation presented in this paper.

5.1 Example 1

In this example, we need to find $f(\mathbf{X}) = f(X_1, X_2): \mathbf{B}_4^2 \to \mathbf{B}_4$, where $\mathbf{B}_4 = \mathrm{FB}(a) = \{0,1,a,\bar{a}\}$ is the free Boolean algebra with one generator (Brown, 1990). The function $f(\mathbf{X})$ has the following values:

k	1	2	3	4	5	6	7	8
$\mathbf{x}_k = (x_{k,1}, x_{k,2})$	$(0,0)$	$(0,a)$	$(\bar{a},0)$	$(\bar{a},a)$	$(a,\bar{a})$	$(a,1)$	$(1,\bar{a})$	$(1,1)$
z_k	0	0	0	0	1	1	1	1

The atoms of $\mathbf{B}_4$ are $q_0 = a$ and $q_1 = \bar{a}$. The atomic representations of the elements of $\mathbf{B}_4$ are $\mathcal{A}(0) = (0,0), \mathcal{A}(1) = (1,1), \mathcal{A}(a) = (1,0), \mathcal{A}(\bar{a}) = (0,1)$.

The sets $\mathcal{C}_{0|m}$, $\mathcal{C}_{1|m}$, and $\mathcal{C}_{|m}$ are:

$$\mathcal{C}_{|0} = \{(0,0),(0,1),(1,0),(1,1)\}, \tag{29}$$

$$\mathcal{C}_{0|0} = \{(0,0),(0,1)\}, \tag{30}$$

$$\mathcal{C}_{1|0} = \{(1,0),(1,1)\}, \tag{31}$$

$$\mathcal{C}_{|1} = \{(0,0),(0,1),(1,0),(1,1)\}, \tag{32}$$

$$\mathcal{C}_{0|1} = \{(0,0),(1,0)\}, \tag{33}$$

and

$$\mathcal{C}_{1|1} = \{(0,1),(1,1)\}. \tag{34}$$

Note that $\mathcal{C}_{0|0} \cap \mathcal{C}_{1|0} = \emptyset$, $\mathcal{C}_{0|1} \cap \mathcal{C}_{1|1} = \emptyset$, and $\mathcal{C}_{|0} = \mathcal{C}_{|1} = \{0,1\}^2$. This means that both consistency and uniqueness conditions are satisfied. Table 1 details the computation of $f_{|m}(\mathbf{u})$ using Equation (26). From Table 1 and Equation (28), we get

$$\begin{aligned} f(X_1,X_2) &= q_1\bar{X}_1X_2 \vee q_0X_1\bar{X}_2 \vee (q_0 \vee q_1)X_1X_2 \\ &= \bar{a}\bar{X}_1X_2 \vee aX_1\bar{X}_2 \vee (a \vee \bar{a})X_1X_2 \\ &= \bar{a}\bar{X}_1X_2 \vee aX_1\bar{X}_2 \vee X_1X_2 = aX_1 \vee \bar{a}X_2. \end{aligned} \tag{35}$$

This is identical to the result obtained in (Rushdi & Balamesh, 2019).

Table 1. Computation of $f(\mathbf{u})$ for Example 1.

$\mathbf{u}$	m	Atom, q_m	$\mathbf{u} \in \mathcal{C}_{1\|m}$?	$f_{\|m}(\mathbf{u})$	$f(\mathbf{u})$	$\mathbf{X}^{\mathbf{u}}$
(0,0)	0	a	no	0	0	$\bar{X}_1\bar{X}_2$
	1	$\bar{a}$	no	0		
(0,1)	0	a	no	0	$\bar{a}$	$\bar{X}_1X_2$
	1	$\bar{a}$	yes	1		
(1,0)	0	a	yes	1	a	$X_1\bar{X}_2$
	1	$\bar{a}$	no	0		
(1,1)	0	a	yes	1	$a \vee \bar{a} = 1$	X_1X_2
	1	$\bar{a}$	yes	1		

5.2 Example 2

In this example, we consider $f: \mathbf{B}_4^2 \to \mathbf{B}_4$ satisfying:

k	1	2
$\mathbf{x}_k = (x_{k,1}, x_{k,2})$	(0,0)	(1,1)
z_k	0	1

The sets $\mathcal{C}_{0|m}$, $\mathcal{C}_{1|m}$, and $\mathcal{C}_{|m}$ are:

$$\mathcal{C}_{|0} = \{(0,0),(1,1)\}, \tag{36}$$

$$\mathcal{C}_{0|0} = \{(0,0)\}, \tag{37}$$

$$\mathcal{C}_{1|0} = \{(1,1)\}, \tag{38}$$

$$\mathcal{C}_{|1} = \{(0,0),(1,1)\}, \tag{39}$$

$$\mathcal{C}_{0|1} = \{(0,0)\}, \tag{40}$$

and

$$\mathcal{C}_{1|1} = \{(1,1)\}. \tag{41}$$

Note that $\mathcal{C}_{0|0} \cap \mathcal{C}_{1|0} = \emptyset$, $\mathcal{C}_{0|1} \cap \mathcal{C}_{1|1} = \emptyset$. This means that the problem is consistent. However, the solution is not unique since $\mathcal{C}_{|0} \neq \{0,1\}^2$ and $\mathcal{C}_{|1} \neq \{0,1\}^2$. Using (27), we find that there are $2^{2^2\times 2-(2+2)} = 2^4 = 16$ distinct solutions to this problem.

Table 2 details the computation of $f_{|m}(\mathbf{u})$ using Equation (26). From Table 2 and Equation (28), we get

$$\begin{aligned} f(X_1, X_2) &= \left(p_{((0,1);0)}a \vee p_{((0,1);1)}\bar{a}\right)\bar{X}_1 X_2 \\ &\quad \vee \left(p_{((1,0);0)}a \vee p_{((1,0);1)}\bar{a}\right)X_1\bar{X}_2 \vee X_1 X_2, \end{aligned} \tag{42}$$

where the parameters $p_{((\cdot,\cdot);\cdot)} \in \{0,1\}$. Relabeling the parameters, we get

$$\begin{aligned} f(X_1, X_2) &= (p_1 a \vee p_2\bar{a})\bar{X}_1 X_2 \vee (p_3 a \vee p_4\bar{a})X_1\bar{X}_2 \vee X_1 X_2 \\ &= (p_3 a \vee p_4\bar{a})X_1 \vee (p_1 a \vee p_2\bar{a})X_2 \vee X_1 X_2. \end{aligned} \tag{43}$$

Since there are four arbitrary parameters, there are $2^4 = 16$ distinct solutions. Table 3 shows the 16 solutions. This result is identical to the result obtained in (Rushdi & Balamesh, 2019).

Table 2. Computation of $f(\mathbf{u})$ for Example 2.

$\mathbf{u}$	m	Atom, q_m	$\mathbf{u} \notin \mathcal{C}_{\|m}$?	$\mathbf{u} \in \mathcal{C}_{1\|m}$?	$f_{\|m}(\mathbf{u})$	$f(\mathbf{u})$	$\mathbf{X}^{\mathbf{u}}$
(0,0)	0	a	no	no	0	0	$\bar{X}_1\bar{X}_2$
	1	$\bar{a}$	no	no	0		
(0,1)	0	a	yes	no	$p_{((0,1);0)}$	$p_{((0,1);0)}a \vee p_{((0,1);1)}\bar{a}$	$\bar{X}_1 X_2$
	1	$\bar{a}$	yes	no	$p_{((0,1);1)}$		
(1,0)	0	a	yes	no	$p_{((1,0);0)}$	$p_{((1,0);0)}a \vee p_{((1,0);1)}\bar{a}$	$X_1\bar{X}_2$
	1	$\bar{a}$	yes	no	$p_{((1,0);1)}$		
(1,1)	0	a	no	yes	1	$a \vee \bar{a} = 1$	$X_1 X_2$
	1	$\bar{a}$	no	yes	1		

Table 3. All solutions of Example 2.

p_1p_2 \ p_3p_4	00	01	10	11
00	X_1X_2	$\bar{a}X_1 \vee X_1X_2$	$aX_1 \vee X_1X_2$	$X_1 \vee X_1X_2 = X_1$
01	$\bar{a}X_2 \vee X_1X_2$	$\bar{a}X_1 \vee \bar{a}X_2 \vee X_1X_2$	$aX_1 \vee \bar{a}X_2 \vee X_1X_2$ $= aX_1 \vee \bar{a}X_2$	$X_1 \vee \bar{a}X_2 \vee X_1X_2$ $= X_1 \vee \bar{a}X_2$
10	$aX_2 \vee X_1X_2$	$\bar{a}X_1 \vee aX_2 \vee X_1X_2$ $= \bar{a}X_1 \vee aX_2$	$aX_1 \vee aX_2 \vee X_1X_2$	$X_1 \vee aX_2 \vee X_1X_2$ $= X_1 \vee aX_2$
11	$X_2 \vee X_1X_2 = X_2$	$\bar{a}X_1 \vee X_2 \vee X_1X_2$ $= \bar{a}X_1 \vee X_2$	$aX_1 \vee X_2 \vee X_1X_2$ $= aX_1 \vee X_2$	$X_1 \vee X_2 \vee X_1X_2$ $= X_1 \vee X_2$

5.3 Example 3

In this example, we consider $f: \mathbf{B}_4^2 \to \mathbf{B}_4$ satisfying:

k	1	2	3	4
$\mathbf{x}_k = (x_{k,1}, x_{k,2})$	$(0, a)$	$(\bar{a}, a)$	$(a, \bar{a})$	$(1, \bar{a})$
z_k	0	0	1	1

The sets $\mathcal{C}_{0|m}, \mathcal{C}_{1|m}$ and $\mathcal{C}_{|m}$ are:

$$\mathcal{C}_{|0} = \{(0,1),(1,0)\}, \tag{44}$$

$$\mathcal{C}_{0|0} = \{(0,1)\}, \tag{45}$$

$$\mathcal{C}_{1|0} = \{(1,0)\}, \tag{46}$$

$$\mathcal{C}_{|1} = \{(0,0),(0,1),(1,0),(1.1)\}, \tag{47}$$

$$\mathcal{C}_{0|1} = \{(0,0),(1,0)\}, \tag{48}$$

and

$$\mathcal{C}_{1|1} = \{(0,1),(1,1)\}. \tag{49}$$

Note that $\mathcal{C}_{0|0} \cap \mathcal{C}_{1|0} = \emptyset$ and $\mathcal{C}_{0|1} \cap \mathcal{C}_{1|1} = \emptyset$. This means that the problem is consistent. However, the solution is not unique since $\mathcal{C}_{|0} \neq \{0,1\}^2$. Using (27), we find that there are $2^{2^2 \times 2 - (2+4)} = 2^2 = 4$ distinct solutions to this problem. From Table 4, the solutions are given by

$$f(X_1, X_2) = p_{((0,0);0)} a \bar{X}_1 \bar{X}_2 \vee \bar{a} \bar{X}_1 X_2 \vee a X_1 \bar{X}_2 \vee \left(p_{((1,1);0)} a \vee \bar{a}\right) X_1 X_2. \tag{50}$$

Substituting all possible values for the arbitrary parameters, we get the four distinct solutions:

$$f_0(X_1, X_2) = \bar{a} \bar{X}_1 X_2 \vee a X_1 \bar{X}_2 \vee \bar{a} X_1 X_2 = a X_1 \bar{X}_2 \vee \bar{a} X_2, \tag{51}$$

$$f_1(X_1, X_2) = \bar{a} \bar{X}_1 X_2 \vee a X_1 \bar{X}_2 \vee X_1 X_2 = \bar{a} X_2 \vee a X_1, \tag{52}$$

$$f_2(X_1, X_2) = a \bar{X}_1 \bar{X}_2 \vee \bar{a} \bar{X}_1 X_2 \vee a X_1 \bar{X}_2 \vee \bar{a} X_1 X_2 = a \bar{X}_2 \vee \bar{a} X_2, \tag{53}$$

and

$$f_3(X_1, X_2) = a \bar{X}_1 \bar{X}_2 \vee \bar{a} \bar{X}_1 X_2 \vee a X_1 \bar{X}_2 \vee X_1 X_2 = a \bar{X}_2 \vee \bar{a} X_2 \vee X_1 X_2. \tag{54}$$

This result is identical to the result obtained in (Rushdi & Balamesh, 2019).

Table 4. Computation of $f(\mathbf{u})$ for Example 3.

$\mathbf{u}$	m	Atom, q_m	$\mathbf{u} \notin \mathcal{C}_{\|m}$?	$\mathbf{u} \in \mathcal{C}_{1\|m}$?	$f_{\|m}(\mathbf{u})$	$f(\mathbf{u})$	$\mathbf{X}^{\mathbf{u}}$
(0,0)	0	a	yes	no	$p_{((0,0);0)}$	$p_{((0,0);0)} a$	$\bar{X}_1 \bar{X}_2$
	1	$\bar{a}$	no	no	0		
(0,1)	0	a	no	no	0	$\bar{a}$	$\bar{X}_1 X_2$
	1	$\bar{a}$	no	yes	1		
(1,0)	0	a	no	yes	1	a	$X_1 \bar{X}_2$
	1	$\bar{a}$	no	no	0		
(1,1)	0	a	yes	no	$p_{((1,1);0)}$	$p_{((1,1);0)} a \vee \bar{a}$	$X_1 X_2$
	1	$\bar{a}$	no	yes	1		

6. Conclusion

The main goal of this work is to set the stage for constructing a cryptosystem based on Boolean curve fitting. The paper revisits the now classical problem of Boolean curve fitting and offers a brief exposition of its algebraic formulation. Subsequently, it presents a novel method for its solution via atomic decomposition into several independent switching equations, where due care is paid to the conditions for consistency and uniqueness. Several illustrative examples are used to expose the details of the method.

These examples demonstrate that the method efficiently constructs an exhaustive nonredundant list of all particular solutions, without having to derive a general solution first.

In future work, we will explore potential applications of Boolean curve fitting and use the proposed method to improve on existing methods. In particular, the application of atomic Boolean curve fitting to the design of Boolean functions for cryptographic systems is of special interest (Cusick & Stanica, 2017; Wu & Feng, 2016). The ultimate goal is building cryptographic systems based on Boolean equations as proposed in (Ahmad & Rushdi, 2018).

Conflict of Interest

The authors confirm that there is no conflict of interest to declare for this publication.

Acknowledgments

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The authors would like to thank the editor and anonymous reviewers for their comments that help improve the quality of this work.

References

Ahmad, W., & Rushdi, A.M.A. (2018). A new cryptographic scheme utilizing the difficulty of big Boolean satisfiability. *International Journal of Mathematical, Engineering and Management Sciences*, *3*(1), 47-61. https://doi.org/10.33889/IJMEMS.2018.3.1-005.

Balamesh, A.S., & Rushdi, A.M. (2019). Solution of Boolean equations via atomic decomposition into independent switching equations. *International Journal of Computer Mathematics: Computer Systems Theory*, *4*(3-4), 185-203. https://doi.org/10.1080/23799927.2019.1700396.

Barotov, D.N., & Barotov, R.N. (2022). Polylinear transformation method for solving systems of logical equations. *Mathematics*, *10*(6), 918. https://doi.org/10.3390/math10060918.

Brown, F.M. (1990). *Boolean Reasoning: The Logic of Boolean Equations*. Kluwer Academic.

Chai, F., Gao, X.-S., & Yuan, C. (2008). A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers. *Journal of Systems Science and Complexity*, *21*(2), 191-208. https://doi.org/10.1007/s11424-008-9103-0.

Cusick, T.W., & Stanica, P. (2017). *Cryptographic Boolean Functions and Applications*. Academic Press.

de Mesquita, V.A., Cortez, P.C., Ribeiro, A.B., & de Albuquerque, V.H.C. (2022). A novel method for lung nodule detection in computed tomography scans based on Boolean equations and vector of filters techniques. *Computers and Electrical Engineering*, *100*, 107911. https://doi.org/10.1016/j.compeleceng.2022.107911.

Fedotova-Piven, I.M., Rudnytskyi, V.M., Piven, O.B., & Myroniuk, T.V. (2019). The inversion method of four-bit boolean sac cryptotransforms. *Radio Electronics, Computer Science, Control*(4), 199-210. https://doi.org/10.15588/1607-3274-2019-4-19.

Ishchukova, E., Maro, E., & Pristalov, P. (2020). Algebraic analysis of a simplified encryption algorithm GOST R 34.12-2015. *Computation*, *8*(2), 51. https://doi.org/10.3390/computation8020051.

Kalkan, T., Nichita, F.F., Oner, T., Senturk, I., & Terziler, M. (2022). Mathematics and poetry: Yang-Baxter equations, Boolean algebras, and BCK-algebras. *Science*, *4*(2), 16. https://doi.org/10.3390/sci4020016.

Kochemazov, S., Zaikin, O., Gribanova, I., Otpuschennikov, I., & Semenov, A. (2020). Translation of algorithmic descriptions of discrete functions to SAT with applications to cryptanalysis problems. *Logical Methods in Computer Science*, *16*. https://doi.org/10.23638/LMCS-16(1:29)2020.

Marovac, U. (2018). Applications of Boolean equations in n-gram analysis. *Proceedings of the 8th International Conference on Information Systems and Technologies, Istanbul, Turkey*. https://doi.org/10.1145/3200842.3200859.

Pakhomchik, A.I., Voloshinov, V.V., Vinokur, V.M., & Lesovik, G.B. (2022). Converting of Boolean expression to linear equations, iequalities and QUBO pnalties for cyptanalysis. *Algorithms*, *15*(2), 33. https://doi.org/10.3390/a15020033.

Rudeanu, S. (1959). Boolean equations and their applications to the study of bridge-circuits I. *Bulletin mathématique de la Société des Sciences Mathématiques et Physiques de la République Populaire Roumaine*, *3*(4), 445-473.

Rudeanu, S. (1974). *Boolean Functions and Equations*. North-Holland.

Rudeanu, S. (2010). Boolean sets and most general solutions of Boolean equations. *Information Sciences*, *180*(12), 2440-2447. https://doi.org/10.1016/j.ins.2010.01.029.

Rushdi, A., & Ba-Rukab, O.M. (2003). Low-cost design of multiple-output switching circuits using map solutions of Boolean equations. *Umm Al-Qura University Journal of Science–Medicine–Engineering*, *15*(2), 59-79.

Rushdi, A.M. (2001). Using variable-entered Karnaugh maps to solve Boolean equations. *International Journal of Computer Mathematics*, *78*(1), 23-38. https://doi.org/10.1080/00207160108805094.

Rushdi, A.M., & Albarakati, H.M. (2014). Prominent classes of the most general subsumptive solutions of Boolean equations. *Information Sciences*, *281*, 53-65. https://doi.org/10.1016/j.ins.2014.04.057.

Rushdi, A.M., & Amashah, M.H. (2011). Using variable-entered Karnaugh maps to produce compact parametric general solutions of Boolean equations. *International Journal of Computer Mathematics*, *88*(15), 3136-3149. https://doi.org/10.1080/00207160.2011.594505.

Rushdi, A.M., & Balamesh, A.S. (2017). On the relation between Boolean curve fitting and the inverse problem of Boolean equations. *Journal of King Abdulaziz University: Engineering Sciences*, *28*(2), 3-9. https://doi.org/10.4197/Eng.28-2.1.

Rushdi, A.M., & Zagzoog, S.S. (2019). On 'big' boolean-equation solving and its utility in combinatorial digital design. In P. Elangovan (Ed.), *Advances in Applied Science and Technology* (Vol. 2, pp. 25-48). B P International. https://doi.org/10.9734/bpi/aast/v2.

Rushdi, A.M.A., & Ahmad, W. (2018). Digital circuit design utilizing equation solving over 'big'Boolean algebras. *International Journal of Mathematical, Engineering and Management Sciences*, *3*(4), 404-428. https://doi.org/10.33889/IJMEMS.2018.3.4-029.

Rushdi, A.M.A., & Balamesh, A.S. (2019). Boolean curve fitting with the aid of variable-entered Karnaugh maps. *International Journal of Mathematical, Engineering and Management Sciences*, *4*(6), 1287-1306. https://doi.org/10.33889/IJMEMS.2019.4.6-102.

Steinbach, B., & Posthoff, C. (2015). The solution of combinatorial problems using Boolean equations: New challenges for teaching. *Open Mathematical Education Notes*, *5*(1), 1-30. https://oaji.net/articles/2015/484-1423741165.pdf

Tapia, M.A., & Tucker, J.H. (1980). Complete solution of Boolean equations. *IEEE Transactions on Computers*, *29*(07), 662-665. https://doi.org/10.1109/TC.1980.1675639.

Wu, C.-K., & Feng, D. (2016). *Boolean Functions and their Applications in Cryptography*. Springer.