International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Boolean Curve Fitting with the Aid of Variable-Entered Karnaugh Maps

Ali Muhammad Ali Rushdi
Department of Electrical and Computer Engineering,
King Abdulaziz University,
P. O. Box 80204, Jeddah 21589, Saudi Arabia
**Corresponding author*: arushdi@kau.edu.sa

Ahmed Said Balamesh
Department of Electrical and Computer Engineering,
King Abdulaziz University,
P. O. Box 80204, Jeddah 21589, Saudi Arabia

(Received May 21, 2019; Accepted July 26, 2019)

Abstract
The Variable-Entered Karnaugh Map is utilized to grant a simpler view and a visual perspective to Boolean curve fitting (Boolean interpolation); a topic whose inherent complexity hinders its potential applications. We derive the function(s) through m points in the Boolean space B^{n+1} together with consistency and uniqueness conditions, where B is a general 'big' Boolean algebra of $\ell \geq 1$ generators, $\mathcal{L}$ atoms ($2^{\ell-1} < \mathcal{L} \leq 2^{\ell}$) and $2^{\mathcal{L}}$ elements. We highlight prominent cases in which the consistency condition reduces to the identity $(0 = 0)$ with a unique solution or with multiple solutions. We conjecture that consistent (albeit not necessarily unique) curve fitting is possible if, and only if, $m = 2^n$. This conjecture is a generalization of the fact that a Boolean function of n variables is fully and uniquely determined by its values in the $\{0,1\}^n$ subdomain of its B^n domain. A few illustrative examples are used to clarify the pertinent concepts and techniques.

Keywords– Boolean curve fitting, Boolean interpolation, variable-entered Karnaugh map, Consistency condition, uniqueness.

1. Introduction

Cryptography is the science of encrypting and decrypting data so as to allow secure transfer of information over space (transmission over a communication channel) or over time (storage within a computer memory). The 'inverse' of encryption is cryptanalysis, which is the science of analyzing and breaking encrypted messages. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Conventionally, cryptography was largely of interest to the military and to diplomats. Nowadays, it permeates many aspects of life, including Internet banking, e-commerce, e-mail, and automatic teller machines. It has tremendous impact on the economic, sociological, and political aspects of the contemporary society. A cryptographic scheme, or a system used to accomplish the goals of cryptography is called a cryptosystem (Adler and Gailly, 1999; Menezes et al., 1996; Piper and Murphy, 2002; Tanenbaum and Wetherall, 2011; Rushdi and Alsheikhy, 2017; Ahmad and Rushdi, 2018).

This paper serves as a first step towards a novel cryptosystem that is based on the utilization of a 'big' Boolean algebra, *i.e.*, a finite (atomic) Boolean algebra other than the conventional two-valued one (Hammer and Rudeanu, 1968; Brown, 1990; Rudeanu, 1974, 2001; Crama and Hammer, 2011; Rushdi and Amashah, 2011). The basic idea is to dramatically extend the search space needed in satisfiability-based (SAT-based) cryptography (Ahmad and Rushdi, 2018). The adversary will not

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

only be obliged to traverse a search space (that can be arbitrarily huge), but will definitely end up with an arbitrarily large number of candidate answers, all of which are wrong except the one corresponding to the encrypted message.

In the envisioned cryptosystem, the alphabet of symbols used is a certain subset of the $2^{\mathcal{L}}$ elements of a general 'big' Boolean algebra B of $\ell \geq 1$ generators, $\mathcal{L}$ atoms ($2^{\ell-1} < \mathcal{L} \leq 2^{\ell}$). The sent message now consists of a sequence of functions $f_{ij}(\boldsymbol{X})$ over B encrypting the intended symbols s_i, where every symbol s_i is encrypted by an arbitrarily large number J of functions ($1 \leq j \leq J$). A single common particular vector $\boldsymbol{X}_c$ is selected such that $f_{ij}(\boldsymbol{X}_c) = s_i$ for all possible values of i and j. This common vector $\boldsymbol{X}_c$ is entrusted securely to the intended receiver. The job of the receiver is to trivially substitute this $\boldsymbol{X}_c$ into the sequence of functions received, thereby converting it into the original sequence of sent symbols. However, it is a totally different story for the adversary, whose potential approaches for cryptanalysis will be discussed in a forthcoming paper. The present paper will be devoted entirely to the job required of the sender (or system designer), which is to construct a pool of functions $f_{ij}(\boldsymbol{X})$ such that $f_{ij}(\boldsymbol{X}_c) = s_i$ for all possible values of i and j. It is also desirable that these functions should be as 'different' as possible and that none of them should equate to s_i at an input $\boldsymbol{X}$ other than $\boldsymbol{X}_c$. These requirements can be achieved *via* Boolean curve fitting (Boolean interpolation), which allows the algebraic derivation of a function passing through m points in the Boolean space B^{n+1}. As it is the case of all problems concerning Boolean equations, certain consistency conditions might be needed and uniqueness is not always guaranteed, (Hammer and Rudeanu, 1968; Brown, 1990; Rudeanu, 1974, 2001; Crama and Hammer, 2011; Rushdi and Amashah, 2011).

The problem of Boolean curve fitting (Boolean interpolation) was handled as a pure mathematical curiosity with no view of practical applications during the past century. Most prominent among the early contributions to this problem are those due to Stamm (1925), McKinsey (1936a, 1936b), Ellis (1953, 1956), and Scognamiglio (1961). Such contributions culminated in the (now) classical treatise by Rudeanu (1974). A sequel paper by Melter and Rudeanu (1984) specialized the results for Boolean functions that are linear in the sense of Löwenheim (Löwenheim, 1918). We have searched many scientific databases vehemently and repeatedly for any contribution to (or application of) Boolean interpolation beyond 1984, but could not find any. However, we should note that there are many papers containing the words 'Boolean interpolation' in text (and even in title), but these apparently refer to the utilization of Boolean methods in real interpolation (see, *e.g.* (Delvos and Posdorf, 1979; Neumann, 1982a, 1982b; Delvos, 1982, 1990; Rudeanu and Simovici, 2004). The work of Rushdi and Albarakati (2012) is related to Boolean interpolation as a special case since it deals with the inverse problem of Boolean equations, in which a Boolean function $f(\boldsymbol{X})$ is required to have the same value of 0 (or 1) at (and only at) several distinct points $\boldsymbol{X}$**.** However, the techniques used in (Rushdi and Albarakati, 2012) are not derived from or based on concepts of Boolean interpolation (Rushdi and Balamesh, 2018). It seems that the topic of Boolean interpolation (as understood herein) matured in a pure mathematical sense several decades ago. Subsequently, it went into a temporary state of hibernation in wait for a practical application. We hope that the appropriate time has arrived for such an application, and that the suggested application is a serious and important one, indeed.

To set the stage for our intended application in cryptography, we studied the available results on Boolean interpolation, and produced a tutorial exposition of them in Section 2. In Section 3, we considered important special cases in which the consistency condition needed for Boolean

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

interpolation reduces to the trivial identity (0 = 0). In Section 4, we gave our exposition an insightful, visual and procedural interpretation with the aid of the Variable-Entered Karnaugh Map (VEKM) (Rushdi, 1987, 2004, 2018a, 2018b; Rushdi and Ahmad, 2017, 2018; Rushdi and Al-Yahya, 2000, 2001; Rushdi and Albarakati, 2012, 2014; Rushdi and Ba-Rukab, 2017; Rushdi and Rushdi, 2018), which is the natural map for functions on big Boolean algebras (Rushdi and Amashah, 2011). We supplemented this interpretation with three demonstrative examples. Section 5 uses elementary solution techniques to further illustrate and independently verify the results of the demonstrative examples in Section 4. Section 6 concludes the paper.

To make the paper self-contained, it is supplemented with two appendices. Appendix A is a general discussion of the solution of a Boolean equation in a single variable. Appendix B details the solution of the Boolean equation in one of the illustrative examples.

2. Boolean Curve Fitting

In this section, we reproduce from (Rudeanu, 1974) the main results known on Boolean curve fitting or Boolean interpolation. We replace the mathematical theorem-proof style in (Rudeanu, 1974) by an engineering problem-solving procedure. We take care to have a rather self-contained exposition and fill-in any missing details in (Rudeanu, 1974). We realize that some of the details might be said to be 'obvious' (to particularly talented mathematicians). The problem at hand requires the determination of a Boolean curve whose graph passes through m given points $(\mathbf{X}_1, z_1), (\mathbf{X}_2, z_2), \dots, (\mathbf{X}_m, z_m)$ of the Boolean space B^{n+1}, where $\mathbf{X}_k = [X_{k,1}, X_{k,2}, \dots, X_{k,n}]^T \in B^n,\ k = 1, 2, \dots, m$ and $z_k \in B,\ k = 1, 2, \dots, m$. This is equivalent to finding a Boolean function $f: B^n \to B$ such that

$$f(\mathbf{X}_k) = z_k,\ k = 1,2, \dots, m \tag{1}$$

The function $f(\mathbf{X})$ and its complement $\bar{f}(\mathbf{X})$ can, respectively, be represented by their minterm expansions (Hammer and Rudeanu, 1968; Rudeanu, 1974, 2001; Brown, 1990; Crama and Hammer, 2011)

$$f(\mathbf{X}) = \bigvee_{\mathbf{A} \in \{0,1\}^n} f(\mathbf{A}) \mathbf{X}^{\mathbf{A}} \tag{2}$$

and

$$\bar{f}(\mathbf{X}) = \bigvee_{\mathbf{A} \in \{0,1\}^n} \bar{f}(\mathbf{A}) \mathbf{X}^{\mathbf{A}} \tag{3}$$

where $\mathbf{A} = [a_1, a_2, \dots, a_n]^T \in \{0,1\}^n$, $f(\mathbf{A})$ and $\bar{f}(\mathbf{A})$ are discriminants of $f(\mathbf{X})$ and $\bar{f}(\mathbf{X})$, respectively, and $\mathbf{X}^{\mathbf{A}}$ is the primitive product (minterm) given by

$$\mathbf{X}^{\mathbf{A}} = X_1^{a_1} X_2^{a_2} \dots X_2^{a_n} \tag{4}$$

and

$$X_i^{a_i} = X_i \odot a_i = \begin{cases} X_i, & \text{if } a_i = 1 \\ \bar{X}_i, & \text{if } a_i = 0 \end{cases} \tag{5}$$

The set of m equations (1) can be rewritten in the equivalent form

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

$$f(\mathbf{X}_k) \oplus z_k = 0, \qquad k = 1,2,\dots,m \tag{6}$$

which are characterized with a 0 in the right-hand side. These are further combined into a single equivalent equation:

$$\bigvee_{k=1}^{m} (f(\mathbf{X}_k) \oplus z_k) = 0 \tag{7}$$

Replacing the XOR function with its equivalent sum-of-products expression, we get

$$\bigvee_{k=1}^{m} \left(z_k \bar{f}(\mathbf{X}_k) \vee \bar{z}_k f(\mathbf{X}_k) \right) = 0 \tag{8}$$

Substituting the minterm expansions (2) and (3) for $f(\mathbf{X}_k)$ and $\bar{f}(\mathbf{X}_k)$, we obtain

$$\bigvee_{k=1}^{m} \bigvee_{\mathbf{A}\in\{0,1\}^n} \left(z_k \bar{f}(\mathbf{A}) \vee \bar{z}_k f(\mathbf{A}) \right) \mathbf{X}_k^{\mathbf{A}} = 0 \tag{9}$$

Interchanging the OR operators over k and **A,** we obtain

$$\bigvee_{\mathbf{A}\in\{0,1\}^n} \left[\left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}} \right) \bar{f}(\mathbf{A}) \vee \left(\bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}} \right) f(\mathbf{A}) \right] = 0 \tag{10}$$

Equation (10) is equivalent to a set of 2^n equations valid for each $\mathbf{A} \in \{0,1\}^n$:

$$F\big(f(\mathbf{A})\big) = \left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}} \right) \bar{f}(\mathbf{A}) \vee \left(\bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}} \right) f(\mathbf{A}) = 0 \tag{11}$$

Each of these equations is a Boolean equation in a single variable $f(\mathbf{A})$. The function in the left-hand side of (11) can be represented by the Variable-Entered Karnaugh Map (VEKM) (Rushdi, 1987, 2004; Rushdi and Al-Yahya, 2000, 2001; Rushdi and Albarakati, 2012, 2014; Rushdi and Ahmad, 2017) of a single map variable $f(\mathbf{A})$ shown in Figure 1.

	$f(\mathbf{A})$
$\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}$	$\bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}}$

$F\big(f(\mathbf{A})\big)$

Figure 1. VKEM representation of the left-hand side of equation (11)

We use the results in Appendix A to solve the Boolean equation (11). The consistency condition for this equation is

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

$$\left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}\right)\left(\bigvee_{h=1}^{m} \bar{z}_h \mathbf{X}_h^{\mathbf{A}}\right) = 0 \tag{12}$$

The condition in (12) is valid for each $\mathbf{A} \in \{0,1\}^n$. This means that we have 2^n consistency conditions that can be combined into a single consistency condition by ORing (12) over all possible values of **A**.

$$\bigvee_{\mathbf{A}\in\{0,1\}^n} \bigvee_{k=1}^{m} \bigvee_{h=1}^{m} z_k \bar{z}_h \mathbf{X}_k^{\mathbf{A}} \mathbf{X}_h^{\mathbf{A}} = 0 \tag{13}$$

If we interchange k and h in (13), we obtain

$$\bigvee_{\mathbf{A}\in\{0,1\}^n} \bigvee_{k=1}^{m} \bigvee_{h=1}^{m} \bar{z}_k z_h \mathbf{X}_k^{\mathbf{A}} \mathbf{X}_h^{\mathbf{A}} = 0 \tag{14}$$

ORing (13) and (14), we obtain

$$\bigvee_{\mathbf{A}\in\{0,1\}^n} \bigvee_{k=1}^{m} \bigvee_{h=1}^{m} (z_k \bar{z}_h \vee \bar{z}_k z_h) \mathbf{X}_k^{\mathbf{A}} \mathbf{X}_h^{\mathbf{A}} = 0 \tag{15}$$

We now replace $z_k \bar{z}_h \vee \bar{z}_k z_h$ by $z_k \oplus z_h$ and interchange the order of the ORing to obtain

$$\bigvee_{k=1}^{m} \bigvee_{h=1}^{m} (z_k \oplus z_h) \bigvee_{\mathbf{A}\in\{0,1\}^n} \mathbf{X}_k^{\mathbf{A}} \mathbf{X}_h^{\mathbf{A}} = 0 \tag{16}$$

Now, using Lemma 13.3 in Rudeanu (1974) (due to McKinsey (1936a))

$$\bigvee_{\mathbf{A}\in\{0,1\}^n} \mathbf{X}_k^{\mathbf{A}} \mathbf{X}_h^{\mathbf{A}} = \bigwedge_{i=1}^{n} \left(X_{k,i} \odot X_{h,i}\right), \qquad k, h = 1,2, \dots, m \tag{17}$$

We simplify the overall consistency condition into

$$\bigvee_{k=1}^{m} \bigvee_{h=1}^{m} (z_k \oplus z_h) \bigwedge_{i=1}^{n} \left(X_{k,i} \odot X_{h,i}\right) = 0 \tag{18}$$

Using Appendix A, we write the parametric solution of (11) as

$$f(\mathbf{A}) = \left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}\right) \vee p_{\mathbf{A}} \overline{\left(\bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}}\right)} \tag{19}$$

where $p_{\mathbf{A}}$ is a parameter that belongs to the underlying Boolean algebra B. The last term in (19) can be simplified by De Morgan's law and, then, by the reflection law to

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

$$\overline{\left(\bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}}\right)} = \bigwedge_{k=1}^{m} \left(z_k \vee \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)}\right) = \bigwedge_{k=1}^{m} \left(z_k \mathbf{X}_k^{\mathbf{A}} \vee \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)}\right) \tag{20}$$

The right-hand side of (20) is equal to $\bigwedge_{k=1}^{m} \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)}$ ORed with products containing at least one $z_k \mathbf{X}_k^{\mathbf{A}}$ term. Each of these products subsumes (and hence is absorbed in) some of the terms in $\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}$ when inserted in (19). Therefore, (19) will ultimately take the form

$$f(\mathbf{A}) = \left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}\right) \vee \; p_{\mathbf{A}} \bigwedge_{k=1}^{m} \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)} \tag{21}$$

This solution for $f(\mathbf{A})$ is then substituted in the minterm expansion (2) to obtain the desired interpolating function:

$$f(\mathbf{X}) = \bigvee_{\mathbf{A} \in \{0,1\}^n} \left[\left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}\right) \vee \; p_{\mathbf{A}} \bigwedge_{k=1}^{m} \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)}\right] \mathbf{X}^{\mathbf{A}} \tag{22}$$

The solution in (22) is unique if, and only if, the term containing $p_{\mathbf{A}}$ vanishes for each $\mathbf{A} \in \{0,1\}^n$. This will occur if, and only if (McKinsey, 1936a; Rudeanu, 1974)

$$\bigvee_{\mathbf{A} \in \{0,1\}^n} \bigwedge_{k=1}^{m} \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)} = 0 \tag{23}$$

and, in this case, the unique solution is

$$f(\mathbf{X}) = \bigvee_{\mathbf{A} \in \{0,1\}^n} \left(\bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}\right) \mathbf{X}^{\mathbf{A}} \tag{24}$$

Note that the uniqueness condition (23) depends only on the $\mathbf{X}_k$'s and is independent of the z_k's. Incidentally, a Boolean curve through a single point (i.e., $m = 1$) cannot be unique, since $\bigvee_{\mathbf{A} \in \{0,1\}^n} \bigwedge_{k=1}^{1} \overline{\left(\mathbf{X}_k^{\mathbf{A}}\right)}$ becomes identically 1 and cannot be equated to 0.

3. Cases of Unconditional Consistency

There are two prominent cases in which the consistency condition (18) reduces to the identity $0 = 0$, and hence consistency is achieved unconditionally:

1) The case when the z_k's are the same, i.e. $z_k = z_0$ for $1 \leq k \leq m$. This includes the case of $m = 1$ and, more importantly, the case of the inverse problem of consistent Boolean equations (Rushdi and Albarakati, 2012).
2) The case when the $\mathbf{X}_k$'s ($1 \leq k \leq m$) cover exactly all the K-map cells $\mathbf{A} \in \{0,1\}^n$, i.e. $\{\mathbf{X}_1, \mathbf{X}_2, \dots, \mathbf{X}_m\} = \{0,1\}^n$ with $m = 2^n$. For $k \neq h$, $\mathbf{X}_k$ and $\mathbf{X}_h \in \{0,1\}^n$, there must be at least a single $X_{k,i} \neq X_{h,i}$ such that $X_{k,i} \odot X_{h,i} = 0$, and for $k = h$, $z_k \oplus z_h = 0$.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

In case (2) above, the uniqueness condition (23) is also satisfied since

$$\mathbf{X}_k^{\mathbf{A}} = \begin{cases} 1, & \mathbf{X}_k = \mathbf{A} \\ 0, & \mathbf{X}_k \neq \mathbf{A} \end{cases} \tag{25}$$

$$\overline{\mathbf{X}_k^{\mathbf{A}}} = \begin{cases} 0, & \mathbf{X}_k = \mathbf{A} \\ 1, & \mathbf{X}_k \neq \mathbf{A} \end{cases} \tag{26}$$

$$\forall \mathbf{A} \in \{0,1\}^n : \bigwedge_{k=1}^{m} \overline{\mathbf{X}_k^{\mathbf{A}}} = \bigwedge_{\mathbf{X}_k \in \{0,1\}^n} \overline{\mathbf{X}_k^{\mathbf{A}}} = 0 \tag{27}$$

The observation above corresponds to the fact that a Boolean function $f: B^n \to B$ is unconditionally and uniquely defined by its Karnaugh map $f: \{0,1\}^n \to B$ (Brown, 1990; Rushdi and Amashah, 2011).

4. VEKM Representation

The algebraic solution procedure in Section 2 will now be implemented by constructing a sequence of five Variable-Entered Karnaugh Maps (VEKMs) of map variables **X**, that we characterize in Table 1. Use of the map allows us to work either at the level of a single cell $\mathbf{A} \in \{0,1\}^n$ or the level of the entire map. The entries of the cell **A** for the first two VEKMs are, respectively, the two subfunctions $F(0)$ and $F(1)$ of the function $F(f(\mathbf{A}))$ in Figure 1. The entry in cell **A** of the third VEKM is obtained by ANDing the corresponding entries in the first two VEKMs. All VKEM entries are expressed solely in terms of the input data of the problem, with the only exception of the fifth VEKM which needs an arbitrarily selected parameter $p_{\mathbf{A}} \in B$. Out of the five VKEM functions in Table 1, the third and fourth functions are important for stating the consistency and uniqueness conditions. In fact, each of these two conditions results by equating to 0 the disjunctive eliminant (Brown, 1990) or join derivative (Thayse, 1978) of the corresponding function, i.e., ORing all VEKM entries of the corresponding map. The fifth VEKM function is the general desired solution subject to the consistency condition. If further the uniqueness condition is involved, the fifth VEKM is replaced by the first VEKM which stands for a unique solution. Only the second function, called an auxiliary function, is merely an intermediate product and not a final one. In the following sections, we demonstrate the solution of the Boolean curve fitting problem by constructing the aforementioned VEKMs.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Table 1. Five VEKMs of map variables **X** for achieving a (unique) consistent solution of the problem of curve fitting

Map Number	**Entry in Cell A** $\in \{\mathbf{0},\mathbf{1}\}^{n}$	**Map Function**	**Pertinent Equation**
1	$E_1(\mathbf{A}) = \bigvee_{k=1}^{m} z_k \mathbf{X}_k^{\mathbf{A}}$	$f(X) = \bigvee_{\mathbf{A}\in\{0,1\}^n} E_1(\mathbf{A})\mathbf{X}^{\mathbf{A}}$ Unique solution (subject to consistency and uniqueness conditions)	(24)
2	$E_2(\mathbf{A}) = \bigvee_{k=1}^{m} \bar{z}_k \mathbf{X}_k^{\mathbf{A}}$	Auxiliary function	
3	$E_3(\mathbf{A}) = E_1(\mathbf{A}) \wedge E_2(\mathbf{A})$	Consistency function: $\bigvee_{\mathbf{A}\in\{0,1\}^n} E_3(\mathbf{A})\mathbf{X}^{\mathbf{A}}$ The consistency condition is obtained by equating to 0 the disjunctive eliminant of this function: $\vee_{\mathbf{A}\in\{0,1\}^n} E_3(\mathbf{A}) = 0$	(12)
4	$E_4(A) = \bigwedge_{k=1}^{m} \overline{(\mathbf{X}_k^{\mathbf{A}})}$	Uniqueness function: $\bigvee_{\mathbf{A}\in\{0,1\}^n} E_4(\mathbf{A})\mathbf{X}^{\mathbf{A}}$ The uniqueness condition is obtained by equating to 0 the disjunctive eliminant of this function: $\vee_{\mathbf{A}\in\{0,1\}^n} E_4(\mathbf{A}) = 0$	(23)
5	$E_5(\mathbf{A}) = E_1(\mathbf{A}) \vee p_{\mathbf{A}} E_4(\mathbf{A})$	$f(X) = \bigvee_{\mathbf{A}\in\{0,1\}^n} E_5(\mathbf{A})\mathbf{X}^{\mathbf{A}}$ General solution (subject to consistency condition)	(22)

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

		X_1
	$(1)(\bar{a})(a)\vee(1)(\bar{a})(0)\vee(1)(0)(a)\vee(1)(0)(0)$	$(1)(a)(a)\vee(1)(a)(0)\vee(1)(1)(a)\vee(1)(1)(0)$
X_2	$(1)(\bar{a})(\bar{a})\vee(1)(\bar{a})(1)\vee(1)(0)(\bar{a})\vee(1)(0)(1)$	$(1)(a)(\bar{a})\vee(1)(a)(1)\vee(1)(1)(\bar{a})\vee(1)(1)(1)$

a) Initial map 1

		X_1
	0	a
X_2	$\bar{a}$	1

b) Final map 1

		X_1
	$(1)(1)(1)\vee(1)(1)(\bar{a})\vee(1)(a)(1)\vee(1)(a)(\bar{a})$	$(1)(0)(1)\vee(1)(0)(\bar{a})\vee(1)(\bar{a})(1)\vee(1)(\bar{a})(\bar{a})$
X_2	$(1)(0)(1)\vee(1)(0)(\bar{a})\vee(1)(\bar{a})(1)\vee(1)(\bar{a})(\bar{a})$	$(1)(0)(0)\vee(1)(0)(a)\vee(1)(\bar{a})(0)\vee(1)(\bar{a})(a)$

c) Initial map 2

		X_1
	1	$\bar{a}$
X_2	a	0

d) Final map 2

		a_1
	0	0
a_2	0	0

e) Map 3

		a_1
	$(0\vee0)(0\vee a)(\bar{a}\vee0)(\bar{a}\vee a)$ $(a\vee\bar{a})(a\vee1)(1\vee\bar{a})(1\vee1)$	$(1\vee0)(1\vee a)(a\vee0)(a\vee a)$ $(\bar{a}\vee\bar{a})(\bar{a}\vee1)(0\vee\bar{a})(0\vee1)$
a_2	$(0\vee1)(0\vee\bar{a})(\bar{a}\vee1)(\bar{a}\vee\bar{a})$ $(a\vee a)(a\vee0)(1\vee a)(1\vee0)$	$(1\vee1)(1\vee\bar{a})(a\vee1)(a\vee\bar{a})$ $(\bar{a}\vee a)(\bar{a}\vee0)(0\vee a)(0\vee0)$

f) Initial map 4

		a_1
	0	0
a_2	0	0

g) Final map 4

Figure 2. VEKMs for example 1

Example 1.
We use the aforementioned VEKM procedure for Boolean curve fitting to obtain $f(\mathbf{X}) = f(X_1, X_2)$: $B_4^2 \to B_4$ where $B_4 = \{0,1,a,\bar{a}\}$ and $f(\mathbf{X})$ satisfies:

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

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Figure 2 shows the development of the first four maps mentioned in Table 1 for this example. Map 3 indicates that the consistency condition is the identity $(0 = 0)$. Likewise, Map 4 indicates that the uniqueness condition is identically satisfied. Therefore, there is no need for Map 5. Thus, the final unique solution can be read from Map 1 as (Rushdi, 1987; Rushdi and Al-Yahya, 2000, 2001)

$$f(\mathbf{X}) = f(X_1, X_2) = aX_1\bar{X}_2 \vee \bar{a}\bar{X}_1X_2 \vee X_1X_2 = aX_1 \vee \bar{a}X_2 \tag{28}$$

Example 2.
In this example, we find the function $f(X_1, X_2)$: $B_4^2 \to B_4$ where $B_4 = \{0,1,a,\bar{a}\}$ that satisfies:

k	1	2
$\mathbf{X}_k = (X_{k,1}, X_{k,2})$	(0,0)	(1,1)
z_k	0	1

The five maps mentioned in Table 1 that correspond to this problem are shown in final form in Figure 3. Map 3 indicates that the consistency condition is the identity $(0 = 0)$. However, Map 4 indicates that the uniqueness condition is not satisfied. Therefore, the desired function $f(X_1, X_2)$ is not unique and is obtained from Map 5 as

$$f(\mathbf{X}) = f(X_1, X_2) = p_1X_1\bar{X}_2 \vee p_2\bar{X}_1X_2 \vee X_1X_2 = p_1X_1 \vee p_2X_2 \vee X_1X_2 \tag{29}$$

where p_1 and p_2 are arbitrary parameters that independently belong to B_4. So, there are 16 different solutions to this problem. Figure 4 displays all the solutions.

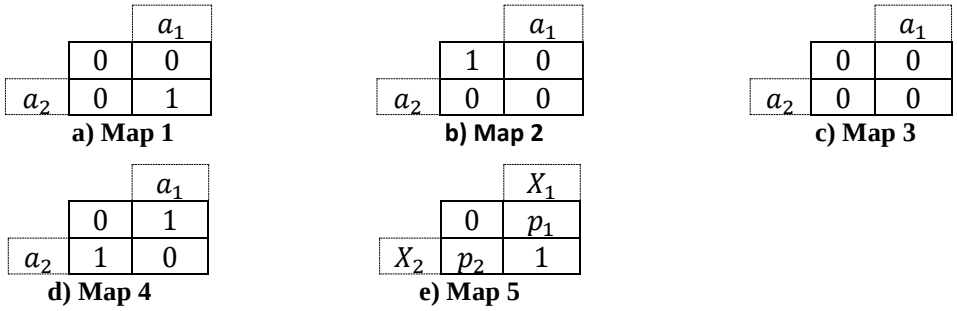

Figure 3. VEKMs for example 2

p_2 \ p_1	0	1	a	$\bar{a}$
0	X_1X_2	X_1	$X_1X_2 \vee aX_1$	$X_1X_2 \vee \bar{a}X_1$
1	X_2	$X_1 \vee X_2$	$aX_1 \vee X_2$	$\bar{a}X_1 \vee X_2$
a	$X_1X_2 \vee aX_2$	$X_1 \vee aX_2$	$X_1X_2 \vee a(X_1 \vee X_2)$	$\bar{a}X_1 \vee aX_2$
$\bar{a}$	$X_1X_2 \vee \bar{a}X_2$	$X_1 \vee \bar{a}X_2$	$aX_1 \vee \bar{a}X_2$	$X_1X_2 \vee \bar{a}(X_1 \vee X_2)$

Figure 4. All possible solutions of example 2

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Example 3.
In this example, we consider $f: B_4^2 \to B_4$ 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

Figure 5 displays the five VEKMs for this function. Map 3 shows that the problem is consistent and Map 4 indicates that the solution is not unique. For $i \in \{0,3\}$, $p_i \in B_4$ and, hence, $p_i a \in \{0, a\}$. Therefore, the number of particular solutions in Map 5 is $2 \times 2 = 4$, namely,

$$f_0(X_1, X_2) = aX_1\bar{X}_2 \vee \bar{a}\bar{X}_1X_2 \vee \bar{a}X_1X_2 = aX_1\bar{X}_2 \vee \bar{a}X_2, \tag{30}$$

$$f_1(X_1, X_2) = a\bar{X}_1\bar{X}_2 \vee aX_1\bar{X}_2 \vee \bar{a}\bar{X}_1X_2 \vee \bar{a}X_1X_2 = a\bar{X}_2 \vee \bar{a}X_2, \tag{31}$$

$$f_2(X_1, X_2) = aX_1\bar{X}_2 \vee \bar{a}\bar{X}_1X_2 \vee X_1X_2 = aX_1 \vee \bar{a}X_2, \tag{32}$$

and

$$f_3(X_1, X_2) = a\bar{X}_1\bar{X}_2 \vee aX_1\bar{X}_2 \vee \bar{a}\bar{X}_1X_2 \vee X_1X_2 = a\bar{X}_2 \vee \bar{a}X_2 \vee X_1X_2, \tag{33}$$

		a_1
	0	a
a_2	$\bar{a}$	$\bar{a}$

a) Map 1

		a_1
	$\bar{a}$	$\bar{a}$
a_2	a	0

b) Map 2

		a_1
	0	0
a_2	0	0

c) Map 3

		a_1
	a	0
a_2	0	a

d) Map 4

		X_1
	$p_0 a$	a
X_2	$\bar{a}$	$\bar{a} \vee p_3 a$

e) Map 5

Figure 5. VEKMs for example 3

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

5. Elementary Solution Techniques

In this section, we revisit the three examples in Section 4 solving them by elementary methods. We verify that, in each case, we recover the same solutions obtained via the formal interpolation procedure.

Example 1 – Revisited

Here, we solve example 1 from first principles and without using the theory presented in Sections 2 and 4. Figure 6 shows the function table ($B_4^2 \to B_4$) for $f(X_1, X_2)$. Note that the section marked with the thick line is the Karnaugh map ($\{0,1\}^2 \to B_4$) for this function. The function $f(X_1, X_2)$ is uniquely determined by its Karnaugh map. Two entries in the Karnaugh are required by the problem statements to be $f(0,0) = 0$ and $f(1,1) = 1$. So, to complete the entries of the map, we assume that $f(0,1) = \beta$ and $f(1,0) = \gamma$, as shown in Figure 6. Then the map produces

$$f(X_1, X_2) = \beta X_1 \bar{X}_2 \vee \gamma \bar{X}_1 X_2 \vee X_1 X_2 = X_1 X_2 \vee \beta X_1 \vee \gamma X_2 \tag{34}$$

Now, we find the conditions on $\beta, \gamma \in B_4$ from the remaining known elements in the function table. We obtain the following set of simple Boolean equations with their corresponding solutions:

$$f(0, a) = 0 = \gamma a \;\Rightarrow\; \gamma \in \{0, \bar{a}\} \tag{35}$$

$$f(\bar{a}, 0) = 0 = \beta \bar{a} \;\Rightarrow\; \beta \in \{0, a\} \tag{36}$$

$$f(\bar{a}, a) = 0 = \beta \bar{a} \vee \gamma a \;\Rightarrow\; \gamma \in \{0, \bar{a}\}, \beta \in \{0, a\} \tag{37}$$

$$f(a, 1) = 1 = a \vee \beta a \vee \gamma = a \vee \gamma \;\Rightarrow\; \gamma \in \{1, \bar{a}\} \tag{38}$$

$$f(1, \bar{a}) = 1 = \bar{a} \vee \beta \vee \bar{a}\bar{a} = \bar{a} \vee \beta \;\Rightarrow\; \beta \in \{1, a\} \tag{39}$$

Conditions in (35)-(39) are consistent and they produce the solution $\gamma = \bar{a}$ and $\beta = a$. These values are also consistent with the given value for $f(a, \bar{a})$, since

$$f(a, \bar{a}) = 0 \vee \beta a \vee \gamma \bar{a} = 0 \vee aa \vee \bar{a}\bar{a} = 1 \tag{40}$$

as required. Substituting for β and γ into (34), we obtain

$$f(X_1, X_2) = X_1 X_2 \vee \beta X_1 \vee \gamma X_2 = X_1 X_2 \vee a X_1 \vee \bar{a} X_2 = a X_1 \vee \bar{a} X_2 \tag{41}$$

which is identical to the solution obtained before in (28).

$X_2 \setminus X_1$	0	1	a	$\bar{a}$
0	0	β		0
1	γ	1	1	
a	0			0
$\bar{a}$		1	1	

$f(X_1, X_2)$

Figure 6. Function table for the function of example 1 with its Karnaugh map part highlighted

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Example 2 – Revisited.
Figure 7 shows the function table for the function in example 2, where we have assumed that $f(1,0) = \beta$ and $f(0,1) = \gamma$ where $\beta, \gamma \in B_4$. So, we can write the function based on its Karnaugh map as

$$f(X_1, X_2) = \beta X_1 \bar{X}_2 \vee \gamma \bar{X}_1 X_2 \vee X_1 X_2 = \beta X_1 \vee \gamma X_2 \vee X_1 X_2 \tag{42}$$

Note that, in this case, we have no further constraints on f. So, there are no more conditions on β and γ other than the fact that each of them belongs to B_4. This solution (42) is exactly the same as the earlier solution (29) with β identified as p_1 and γ identified as p_2.

$X_2 \setminus X_1$	0	1	a	$\bar{a}$
0	0	β		
1	γ	1		
a				
$\bar{a}$				

$f(X_1, X_2)$

Figure 7. Function table for the function of example 2

Example 3 – Revisited
Figure 8 shows the function table for the function in example 3. We can write the function as

$$f(X_1, X_2) = \alpha \bar{X}_1 \bar{X}_2 \vee \beta X_1 \bar{X}_2 \vee \gamma \bar{X}_1 X_2 \vee \delta X_1 X_2 \tag{43}$$

We apply the constraints dictated by the function table to get equations on the unknowns $\alpha, \beta, \gamma,$ and δ. Table 2 shows the resulting equations and their individual solutions (which could be obtained either by inspection or formally as shown in Appendix B). The overall solution set is the intersection of the solutions of the individual equations which is not empty (indicating that the system of equations is consistent). This overall solution set is

$$\alpha \in \{0, a\}, \beta = a, \gamma = \bar{a}, \delta \in \{\bar{a}, 1\} \tag{44}$$

Substituting the four possible solutions obtained in (43), we obtain the four functional expressions in (30)-(33).

$X_2 \setminus X_1$	0	1	a	$\bar{a}$
0	α	β		
1	γ	δ		
a	0			0
$\bar{a}$		1	1	

$f(X_1, X_2)$

Figure 8. Function table for the function of example 3

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

Table 2. Equations resulting from constraints of example 3

Equation	Solution
$\bar{a}\alpha \vee a\gamma = 0$	$\alpha \in \{0, a\}, \gamma \in \{0, \bar{a}\}$
$\bar{a}\beta \vee a\gamma = 0$	$\beta \in \{0, a\}, \gamma \in \{0, \bar{a}\}$
$a\beta \vee \bar{a}\gamma = 1$	$\beta \in \{a, 1\}, \gamma = \{\bar{a}, 1\}$
$a\beta \vee \bar{a}\delta = 1$	$\beta = \{a, 1\}, \delta \in \{\bar{a}, 1\}$

6. Conclusions

This paper revisited the classical problem of Boolean curve fitting, and offered a detailed exposition of its algebraic formulation and solution together with conditions for consistency and uniqueness. This is followed by a map procedure implementing these algebraic results via a sequence of five Variable-Entered Karnaugh Maps (VEKMs). Three illustrative examples are then solved twice, first via the curve-fitting procedure and then based on elementary principles of Boolean algebra. The solutions based on elementary principles are insightful, but they demand much care or effort in solving the elementary Boolean equations required. The earlier solutions based on the curve-fitting procedure are almost mechanical in nature, since the solution of Boolean equations is already taken care of.

The main aim of this paper is to set the stage for constructing a cryptosystem based on Boolean curve fitting. As an offshoot, it is an invitation for further exploration of Boolean curves drawn in arbitrary Boolean spaces. It is well known that if the m interpolation points exactly cover the 2^n Karnaugh map points $\{0,1\}^n$, then it is possible to draw a Boolean curve through them consistently and uniquely. One of our examples (Example 3) shows that when 2^n interpolation points other than the Karnaugh-map points are used, consistency is achieved but uniqueness is not. So far, we have been unable to prove a conjecture that 2^n interpolation points will lead to consistent curve fitting, but in the meanwhile we could not find a counterexample against this conjecture.

Appendix A: Solution of a Boolean Equation in a Single Variable

We consider the Boolean equation

$$F(X) = 0 \tag{A1}$$

for a single variable X where $F: B \to B$ and B is an arbitrary Boolean algebra.

The function $F(X)$ can be represented via the Boole-Shannon expression (Brown, 1990; Crama and Hammer, 2011; Hammer and Rudeanu, 1968; Rudeanu, 1974, 2001; A. M. Rushdi and Amashah, 2011)

$$F(X) = F(0)\bar{X} \vee F(1)X \tag{A2}$$

Each of the subfunctions $F(0)$ and $F(1)$ in (A2) is a disjunction of certain atoms of the underlying Boolean algebra B. The two terms in the right-hand side of (A2) can be augmented by their consensus with respect to X, leading to a replacement of (A2) by

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

$$F(X) = F(0)\bar{X} \vee F(1)X \vee F(0)F(1) = 0 \quad \text{(A3)}$$

The single equation (A3) is equivalent to the following three individual equations taken collectively

$$F(0)\bar{X} = 0 \quad \text{(A4)}$$

$$F(1)X = 0 \quad \text{(A5)}$$

$$F(0)F(1) = 0 \quad \text{(A6)}$$

Equations (A4) and (A5) are, respectively, equivalent to the inequalities

$$F(0) \leq X \quad \text{(A7)}$$

$$X \leq \bar{F}(1) \quad \text{(A8)}$$

which can be combined into the general subsumptive solution of (A1), namely

$$F(0) \leq X \leq \bar{F}(1) \quad \text{(A9)}$$

subject to the consistency condition (A6), which is implicit in (A9), since if X is eliminated, one obtains the inequality

$$F(0) \leq \bar{F}(1) \quad \text{(A10)}$$

which is equivalent to (A6). Another prominent solution of (A1) is its general parametric solution

$$X = F(0) \vee p\bar{F}(1) \quad \text{(A11)}$$

where $p \in B$ is an arbitrary parameter.

The consistency condition (A6) is interpreted to mean that any atom of B belonging to $F(0)F(1)$ must be nullified or annihilated, thereby leading to collapse of the algebra B to a subalgebra lacking the nullified atoms (Rushdi, 2004; Crama and Hammer, 2011; Rushdi and Albarakati, 2014; Rushdi and Ahmad, 2017;). The solution (A11) indicates that X is a disjunction of certain atoms of B. This disjunction includes at least all the atoms constituting $F(0)$ and possibly some of the atoms which imply $\bar{F}(1)$. To disjoint the two terms in (A11), we apply the Reflection Law to obtain

$$X = F(0) \vee p\bar{F}(0)\bar{F}(1) \quad \text{(A12)}$$

Since the parameter p is any element of B, it is a disjunction of any possible subset of the set of atoms of B. Its multiplication by $\bar{F}(0)\bar{F}(1)$ can select or omit any atoms appearing in $\bar{F}(0)\bar{F}(1)$ independently of the other atoms.

The parametric solution (A11) or (A12) can be directly obtained by viewing the VEKM in Figure A1 that represents $\bar{F}(X)$ and seeking solutions of the equation

$$\bar{F}(X) = 1 \quad \text{(A13)}$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

by using the method in (Brown, 1990; A. M. Rushdi and Amashah, 2011). According to this method, we can divide the atoms in the map into four categories, namely:

1) Atoms that do not appear in any map cell, i.e., atoms whose disjunction constitutes $F(0)F(1)$. These atoms should be nullified as a consistency condition.
2) Atoms that appear in both map cells, i.e. atoms whose disjunction constitutes $\bar{F}(0)\bar{F}(1)$. Each of these atoms should be tagged in the X-cell by an independent parameter of its own and tagged in the $\bar{X}$-cell by the complement of this parameter. Each of these parameters belongs to $B_2 = \{0,1\}$ (and not necessarily to the underlying B, which might be a bigger algebra). The disjunction of these atoms tagged by the respective parameters constitutes a part of the sum-of-products expression for X.
3) Atoms that appear in the X-cell but not in the $\bar{X}$-cell, i.e. atoms whose disjunction constitutes $F(0)\bar{F}(1)$. Each of these atoms is tagged by a 1 (i.e., remains intact) and is added to the sum-of-products expression of X.
4) Atoms that appear in the $\bar{X}$-cell but not in the X-cell, i.e., atoms whose disjunction constitutes $\bar{F}(0)F(1)$. Each of these atoms is tagged by 1 and is not added to the sum-of-products expression of X.

	X
$\bar{F}(0)$	$\bar{F}(1)$
$\bar{F}(X)$	

Figure A1. VEKM representation of $\bar{\boldsymbol{F}}(\boldsymbol{X})$ used in the equation $\bar{\boldsymbol{F}}(\boldsymbol{X}) = \mathbf{1}$

The final expression of X, using don't-care notation (rather than the equivalent parametric one) is

$$\begin{aligned} X &= F(0)\bar{F}(1) \vee d\big(\bar{F}(0)\bar{F}(1)\big) && \text{(a)} \\ &= F(0) \vee d\big(\bar{F}(0)\bar{F}(1)\big) && \text{(b)} \end{aligned} \qquad \text{(A14)}$$

Note that, thanks to the consistency condition (A6), there is no difference between the two versions of (A14). Equation (A14) is an admittedly unusual way of expressing (A11) or (A12). However, the don't-care notation of (A14) is rigorously defined in (Reusch, 1975; A. M. Rushdi, 1987; A. M. Rushdi and Albarakati, 2014) and is a very convenient way of abbreviating the fact that atoms appearing in $\bar{F}(0)\bar{F}(1)$ are added independently of one another. Therefore, if $\bar{F}(0)\bar{F}(1)$ is a disjunction of ℓ atoms, the solution (a) of disjoint terms clearly expresses 2^{ℓ} possibilities or particular solutions.

Appendix B: Solution of the Boolean Equations in Example 3 (Revisited)

In this Appendix, we use the methods in (Brown, 1990; Rudeanu, 2003; A. M. Rushdi, 2001, 2012; A. M. Rushdi and Amashah, 2011, 2012) to develop parametric (and then particular) solutions of the four equations in Example 3 (revisited). Each of the equations is a consistent equation of two variables that can be written (directly or via complementation) in the form $g_i(X_1, X_2) = 1$, where $g_i: B_4^2 \to B_4, 1 \leq i \leq 4$. The Boolean algebra B_4 has two atoms, a and $\bar{a}$, either of which appears twice in the natural map of g_i $(1 \leq i \leq 4)$ as shown in Table B1. This means that the consistency condition is the identity $\{0 = 0\}$ and the number of particular solutions is $2 \times 2 = 4$. We need a single parameter $p \in B_4$ to produce the orthonormal set of tags $\{p, \bar{p}\}$ and use these two elements

International Journal of Mathematical, Engineering and Management Sciences
Vol. 4, No. 6, 1287–1306, 2019
https://dx.doi.org/10.33889/IJMEMS.2019.4.6-102

of the set to tag the two appearances of each of the atoms a and $\bar{a}$, thereby producing the auxiliary functions G_i $(1 \leq i \leq 4)$ in Table B1. The final columns of Table B1 list the parametric solutions and then the particular solutions of each equation.

Table B1. Illustration of the solution of the Boolean equations in example 3 (revisited)

Equation	**Natural Map of g_i**	**Auxiliary Function G_i**	**Parametric Solution**	**Particular Solutions**
$\bar{a}\alpha \vee a\gamma = 0$ $(\bar{a}\bar{\alpha} \vee a\bar{\gamma} = 1)$	α | $a \vee \bar{a}$ | a γ | $\bar{a}$ |	α | $\bar{p}a \vee \bar{p}\bar{a}$ | pa γ | $p\bar{a}$ |	$\alpha = pa$ $\gamma = p\bar{a}$	p 0 1 a $\bar{a}$ α 0 a a 0 γ 0 $\bar{a}$ 0 $\bar{a}$
$\bar{a}\beta \vee a\gamma = 0$ $(\bar{a}\bar{\beta} \vee a\bar{\gamma} = 1)$	β | $a \vee \bar{a}$ | a γ | $\bar{a}$ |	β | $\bar{p}a \vee \bar{p}\bar{a}$ | pa γ | $p\bar{a}$ |	$\beta = pa$ $\gamma = p\bar{a}$	p 0 1 a $\bar{a}$ β 0 a a 0 γ 0 $\bar{a}$ 0 $\bar{a}$
$a\beta \vee \bar{a}\gamma = 1$	β | | a γ | $\bar{a}$ | $a \vee \bar{a}$	β | $\bar{p}a$ γ | $\bar{p}\bar{a}$ | $pa \vee p\bar{a}$	$\beta = a \vee p\bar{a}$ $\gamma = \bar{a} \vee pa$	p 0 1 a $\bar{a}$ β a 1 a 1 γ $\bar{a}$ 1 1 $\bar{a}$
$a\beta \vee \bar{a}\delta = 1$	β | | a δ | $\bar{a}$ | $a \vee \bar{a}$	β | $\bar{p}a$ δ | $\bar{p}\bar{a}$ | $pa \vee p\bar{a}$	$\beta = a \vee p\bar{a}$ $\delta = \bar{a} \vee pa$	p 0 1 a $\bar{a}$ α a 1 a 1 δ $\bar{a}$ 1 1 $\bar{a}$

Conflict of Interest
The authors confirm that this article contents have no conflict of interest.

Acknowledgement
The authors would like to acknowledge the financial support of the Deanship of Scientific Research (DSR), King Abdulaziz University (KAU), Jeddah, Saudi Arabia.

References

Adler, M., & Gailly, L.J. (1999). *An Introduction to cryptography.* Network Associates.

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.

Brown, F.M. (1990). *Boolean reasoning: the logic of Boolean equations*. Boston: Kluwer Academic Publishers.

Crama, Y., & Hammer, P.L. (2011). *Boolean functions: theory, algorithms, and applications*. Cambridge University Press, Cambridge, New York. ISBN: 9780521847513.

Delvos, F.J. (1982). d-variate Boolean interpolation. *Journal of Approximation Theory, 34*(2), 99–114.

Delvos, F.J. (1990). Boolean methods for double integration. *Mathematics of Computation, 55*(192), 683–692.

Delvos, F.J., & Posdorf, H. (1979). Boolesche zweidimensionale lagrange-interpolation (Boolean two-dimensional Lagrange interpolation). *Computing, 22*(4), 311–323.

Ellis, D. (1953). Remarks on Boolean functions. *Journal of the Mathematical Society of Japan, 5*(3-4), 345–350.

Ellis, D. (1956). Remarks on Boolean functions II. *Journal of the Mathematical Society of Japan, 8*(4), 363–368.

Hammer, P.L., & Rudeanu, S. (1968). *Boolean methods in operations research and related areas*. Springer, Berlin, Heidelberg.

Löwenheim, L. (1918). Gebietsdeterminanten (Domain determinants). *Mathematische Annalen, 79*(3), 223–236.

McKinsey, J.C.C. (1936a). Boolean functions and points. *Duke Mathematical Journal, 2*(3), 465–471.

McKinsey, J.C.C. (1936b). On Boolean functions of many variables. *Transactions of the American Mathematical Society, 40*(3), 343–362.

Melter, R.A., & Rudeanu, S. (1984). Linear equations and interpolation in Boolean algebra. *Linear Algebra and Its Applications, 57*, 31–40.

Menezes, A.J., van Oorschot, P.C., & Vanstone, S.A. (1996). *Handbook of applied cryptography*. CRC Press, Inc.

Neumann, G. (1982a). Boolean constructed cubature formulas of interpolatory type. In G. Hämmerlin (Ed.). *Numerical Integration*, (pp. 177–186). Basel: Birkhäuser.

Neumann, G. (1982b). Boolesche interpolatorische kubatur (Boolean interpolatory cubature). *Results in Mathematics, 6*(1-2), 116-117.

Piper, F.C., & Murphy, S. (2002). *Cryptography: a very short introduction*. Oxford: Oxford University Press.

Reusch, B. (1975). Generation of prime implicants from sub-functions and a unifying approach to covering problem. *IEEE Transactions on Computers, C-24*(9), 924-930.

Rudeanu, S. (1974). *Boolean functions and equations*. Amsterdam, the Netherlands, North-Holland Publishing Company & American Elsevier.

Rudeanu, S. (2001). *Lattice functions and equations*. London, UK: Springer Verlag.

Rudeanu, S. (2003). Algebraic methods versus map methods of solving Boolean equations. *International Journal of Computer Mathematics, 80*(7), 815-817.

Rudeanu, S., & Simovici, D.A. (2004, May). A graph-theoretical approach to Boolean interpolation of non-Boolean functions. In *Proceedings. 34th International Symposium on Multiple-Valued Logic*, (pp. 245-250). IEEE.

Rushdi, A.M., & Al-Yahya, A.H. (2000). A Boolean minimization procedure using the variable entered Karnaugh map and the generalized consensus concept. *International Journal of Electronics, 87*(7), 769–794.

Rushdi, A.M., & Al-Yahya, A.H. (2001). Further improved variable-entered Karnaugh map procedures for obtaining the irredundant forms of an incompletely-specified switching function. *Journal of King Abdulaziz University: Engineering Sciences, 13*(1), 111–152.

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.

Rushdi, A.M., & Amashah, M.H. (2012). Purely-algebraic versus VEKM methods for solving big Boolean equations. *Journal of King Abdulaziz University: Engineering Sciences, 23*(2), 75-85.

Rushdi, A.M., & Balamesh, A.S. (2018). 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.

Rushdi, A.M., & Ba-Rukab, O.M. (2017). Map calculation of the shapley-shubik voting powers: An example of the European Economic Community. *International Journal of Mathematical, Engineering and Management Sciences, 2*(1), 17-29.

Rushdi, A.M.A. (1987). Improved variable-entered Karnaugh map procedures. *Computers and Electrical Engineering, 13*(1), 41–52.

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

Rushdi, A.M.A. (2004). Efficient solution of Boolean equations using variable-entered Karnaugh maps. *Journal of King Abdulaziz University: Engineering Sciences, 15*(1), 105–121.

Rushdi, A.M.A. (2012). A comparison of algebraic and map methods for solving general Boolean equations. *Journal of Qassim University: Engineering and Computer Sciences, 5*(2), 147-173.

Rushdi, A.M.A. (2018a). Handling generalized type-2 problems of digital circuit design via the variable-entered Karnaugh map. *International Journal of Mathematical, Engineering and Management Sciences, 3*(4), 392-403.

Rushdi, A.M.A. (2018b). Utilization of Karnaugh maps in multi-value qualitative comparative analysis. *International Journal of Mathematical, Engineering and Management Sciences, 3*(1), 28-46.

Rushdi, A.M.A., & Ahmad, W. (2017). Satisfiability in 'big' Boolean algebras via Boolean-equation solving. *Journal of King Abdulaziz University: Engineering Sciences, 28*(1), 3-18.

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.

Rushdi, A.M.A., & Albarakati, H.M. (2012). The inverse problem for Boolean equations. *Journal of Computer Science, 8*(12), 2098–2105.

Rushdi, A.M.A., & Albarakati, H.M. (2014). Prominent classes of the most general subsumptive solutions of Boolean equations. *Information Sciences, 281*, 53–65.

Rushdi, A.M.A., & Alsheikhy, A. (2017). A pedagogical multi-key multi-stage package to secure communication channels. *Journal of Qassim University: Engineering and Computer Sciences, 10*(2), 105-124.

Rushdi, R.A., & Rushdi, A.M. (2018). Karnaugh-map utility in medical studies: The case of fetal malnutrition. *International Journal of Mathematical, Engineering and Management Sciences, 3*(3), 220-244.

Scognamiglio, G. (1961). Interpolazione per le funzioni algebriche Booleane (Interpolation for Boolean algebraic functions). *Giron. Mat. Battaglini, 89*, 14–41.

Stamm, E. (1925). Geometrische theorie logischer funktionen: Beitrag zur algebra der logik (Geometrical theory of logical functions: Contribution to the algebra of logic). *Prace Matematyczno-Fizyczne*, *34*(1), 119–158.

Tanenbaum, A.S., & Wetherall, D.J. (2011). *Computer Networks* (5th ed.). Boston, MA, USA: Pearson Education.

Thayse, A. (1978). Meet and join derivatives and their use in switching theory. *IEEE Transactions on Computers*, *C-27*(8), 713-720.