

# THE INVERSE PROBLEM FOR BOOLEAN EQUATIONS

Ali Muhammad Ali Rushdi and Hussain Mobarak Albarakati

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

Received 2012-10-15, Revised 2012-12-29; Accepted 2012-12-29

## ABSTRACT

The Forward Problem (FB) of Boolean equations consists of finding solutions of a system of Boolean equations, or equivalently, a single Boolean equation of the form  $f(X) = 0$  where  $f(X): B^n \rightarrow B$  and  $B$  is an arbitrary Boolean algebra. By contrast, the Inverse Problem (IB) of Boolean equations aims to reconstruct the equation  $f(X) = 0$  given the set of solutions and hence to verify the correctness of this set. This study derives methods that handle this inverse problem for the main types of solutions of Boolean equations. These include: (a) Subsumptive general solutions, in which each of the variables is expressed as an interval by deriving successive conjunctive or disjunctive eliminants of the original function, (b) Parametric general solutions, in which each of the variables is expressed via arbitrary parameters which are freely chosen elements of the underlying Boolean algebra and (c) Particular solutions, each of which is an assignment from the underlying Boolean algebra to every pertinent variable that makes the Boolean equation an identity. The reconstructed function  $f(X)$  in every case is set in a canonical form, such as the complete-sum form, to facilitate proving its equivalence to the original function. The methods presented herein are demonstrated with carefully-chosen illustrative examples over big Boolean algebras of various sizes. Among the methods utilized in handling the inverse problem for Boolean equations, the ones utilizing the variable-entered Karnaugh map offered pictorial insight and exhibited an efficient divide-and-conquer strategy.

**Keywords:** Inverse Problem, Boolean Equations, Subsumptive General Solutions, Parametric General Solutions, Particular Solutions

## 1. INTRODUCTION

Boolean-equation solving permeates many areas of modern science such as logical design, biology, grammars, chemistry, law, medicine, spectroscopy and graph theory (Brown, 2003). Many important problems in operations research can be reduced to the problem of solving a system of Boolean equations. The solutions of Boolean equations serve also as an important tool in the treatment of pseudo-Boolean equations and inequalities and their associated problems in integer linear programming (Hammer and Rudeanu, 1968). Boolean-equation solving is also an indispensable tool in the cryptanalysis and breaking of ciphers (Chai *et al.*, 2008), Boolean Satisfiability (SAT) problem solving

(He and Zhang, 1999), the synthesis, simulation and testing of digital networks and VLSI systems (Abdel-Gawad *et al.*, 2010; Woods and Casinovi, 2001), output encoding and state assignments of finite state machines (Devadas and Newton, 1990) and automatic test-pattern generation (Larabee, 1992).

The Forward Problem (FB) of Boolean equations consists of finding solutions of a system of Boolean equations, or equivalently, a single Boolean equation of the form  $f(X) = 0$  where  $f(X): B^n \rightarrow B$  and  $B$  is an arbitrary Boolean algebra. By contrast, the Inverse Problem (IV) of Boolean equations aims at reconstructing the equation  $f(X) = 0$  given the set of solutions and hence verifying the correctness of this set. Naturally, the Forward Problem of Boolean

**Corresponding Author:** Ali Muhammad Ali Rushdi, Department of Electrical and Computer Engineering,  
Faculty of Engineering, King Abdulaziz University, P.O. Box 80204, Jeddah 21589, Saudi Arabia

equations has been extensively treated in the literature (see, for example, (Brown, 2003; Rudeanu, 1974; 2001; 2003; 2010; Tucker and Tapia, 1992; 1995; Trabado *et al.*, 1993; Unger, 1994; Jung, 1995; Woods and Casinovi, 1996; Brusentsov and Vladimirova, 1998; Levchenkov, 2000a; 2000b; Rushdi, 2001a; 2004; Baneres *et al.*, 2009; Rushdi and Amashah, 2011), while the inverse problem seems to have received no or little attention.

## 2. MATERIALS AND METHODS

This study presents methods that handle the inverse problem for the main types of solutions of Boolean equations. These include: (a) *Subsumptive general solutions*, in which each of the variables is expressed as an interval by deriving successive conjunctive or disjunctive eliminants of the original function, (b) *Parametric general solutions*, in which each of the variables is expressed via arbitrary parameters which are freely chosen elements of the underlying Boolean algebra and (c) *Particular solutions*, each of which is an assignment from the underlying Boolean algebra to every pertinent variable that makes the Boolean equation an identity (Brown, 2003). The reconstructed function  $f(X)$  in every case is set in a canonical form, such as the complete-sum form (the Blake Canonical form) (Brown, 2003; Rudeanu, 1974; 2001; Blake, 1938; Tison, 1967; Reusch, 1975; Cutler *et al.*, 1979; Muroga, 1979; Gregg, 1998; Rushdi and Al-Yahya, 2001; Rushdi, 2001b), to facilitate proving its equivalence to the original function. The methods presented herein are a mixture of purely-algebraic methods and map methods that utilize the variable-entered Karnaugh map (Rushdi, 1983; 1985; 1986; 1987; 1997; 2001a; 2004; Rushdi and Amashah, 2011; Rushdi and Al-Yahya, 2000a; 2000b; 2001). These methods are demonstrated with carefully-chosen illustrative examples over big Boolean algebras of various sizes. Both methods and examples demonstrate and utilize the basic concepts of Boolean reasoning as introduced and exposed in the seminal text (Brown, 2003).

The organization of the rest of this study is as follows. We start by outlining our methodology. Then we present the derivation of the original Boolean equation  $f(X) = 0$  (with  $f(X)$  cast in the CS-form  $F(X)$ ) from the set of its particular solutions. Subsequently, we discuss the derivation of  $F(X) = 0$  from the subsumptive and parametric general solutions, respectively. Finally, we discuss our results and conclude the study.

## 3. RESULTS

### 3.1. Derivation of the Boolean Equation from its Subsumptive Solution

Let the Boolean equation  $f(X) = 0$ , where  $X = [X_1 X_2 \dots X_n]^T$  and  $f(X): B^n \rightarrow B$ , have a consistency condition in Equation 1:

$$s_0 = 0 \quad (1)$$

And the subsumptive solution in Equation 2a:

$$\begin{aligned} s_n(X_1, X_2, \dots, X_{n-1}) &\leq X_n \leq t_n(X_1, X_2, \dots, X_{n-1}), \\ s_n(X_1, X_2, \dots, X_{n-2}) &\leq X_{n-1} \leq t_{n-1}(X_1, X_2, \dots, X_{n-2}) \\ s_2(X_1) &\leq X_2 \leq t_2(X_1) \\ s_1 &\leq X_1 \leq t_1 \end{aligned} \quad (2a)$$

Or equivalently in Equation 2b:

$$s_i \leq X_i \leq t_i, \quad 1 \leq i \leq n \quad (2b)$$

The relations (1b) are equivalent to Equation 3:

$$s_i \bar{X}_i = 0, \quad X_i \bar{t}_i = 0, 1 \leq i \leq n \quad (3)$$

Which can be ORed together and then ORed with (1) to reconstruct the original equation as Equation 4:

$$f(X) = s_0 \bigvee_{i=1}^n (s_i \bar{X}_i \vee \bar{t}_i X_i) \quad (4)$$

Note that in (4) if  $s_i = 0$  then  $(s_i \bar{X}_i = 0)$  reduces to the identity  $(0 \bar{X}_i = 0)$  and should be discarded. Similarly, if  $t_i = 1$ , the requirement  $(X_i \bar{t}_i = 0)$  becomes an identity  $(X_i (\bar{1}) = 0)$  and is also discarded.

**Example 1:** A Boolean equation of the form  $f(X_1, X_2, X_3) = 0$ , where  $f: B_{16}^3 \rightarrow B_{16}$ , where  $B_{16} = FB(a, b)$  has the subsumptive solutions of Equation 5a-d:

$$ab = 0 \quad (5a)$$

$$b \leq X_3 \leq \bar{a} \quad (5b)$$

$$0 \leq X_2 \leq (a \vee b) \quad (5c)$$

$$0 \leq X_1 \leq 0 \quad (5d)$$

The original function  $f(X_1, X_2, X_3)$  can be reconstructed via (4) as Equation 6:

$$f(X_1, X_2, X_3) = ab \vee b\bar{X}_3 \vee aX_3 \vee \bar{a}bX_2 \vee X_1 = 0 \quad (6)$$

The expression (6) for  $f(X_1, X_2, X_3)$  is in complete-sum form since it is a syllogistic absorptive formula (a sum-of products formula with no term that can be absorbed in other terms) and the consensus w.r.t. to the sole biform variable  $X_3$  is  $ab$  which is already in the disjunction (6) (Brown, 2003; Rushdi and Al-Yahya, 2000b).

### 3.2. Derivation of the Boolean Equation from its Parametric Solution

Let the Boolean equation  $f(X) = 0$ , where  $X = [X_1 X_2 \dots X_n]^T$  and  $f(X): B^n \rightarrow B$ , have a consistency condition (1) and the parametric solution of Equation 7:

$$X_i = f_i(P), 1 \leq i \leq n \quad (7)$$

Now, reduce (1) and (7) to the single equivalent Equation 8:

$$G(X;P) = s_0 \bigvee_{i=1}^n (X_i \oplus f_i(P)) \quad (8)$$

Then, we use Conjunctive Elimination (CE) (Brown, 2003) to eliminate  $P$  from (8) and obtain the following resultant which represents  $f(X)$  in Equation 9:

$$CE(G)(X,P,P) = \bigwedge_{C \in \{0,1\}^n} G(X,C) \quad (9)$$

The expression in (9) is called the conjunctive eliminant of  $G$  with respect to  $P$  (Brown, 2003) or the meet derivative of  $G$  with respect to  $P$  (Thayse, 1978). We reexpress (9) as a Complete Sum in Equation 10:

$$CS(G(X)) = CS(CE(G(X,P),P)) \quad (10)$$

We use a VEKM as a divide-and-conquer strategy for handling the above steps and to allow the two steps of conjunctive elimination and complete-sum derivation to run concurrently. Specifically, we note that in equation (10), one can commute (interchange) the operation of deriving the Complete Sum (CS) and Conjunctive Elimination (CE) (Rushdi and Al-Shehri, 2004), to obtain Equation 11:

$$CS(G(X)) = CE(CS(G(X,P),P)) \quad (11)$$

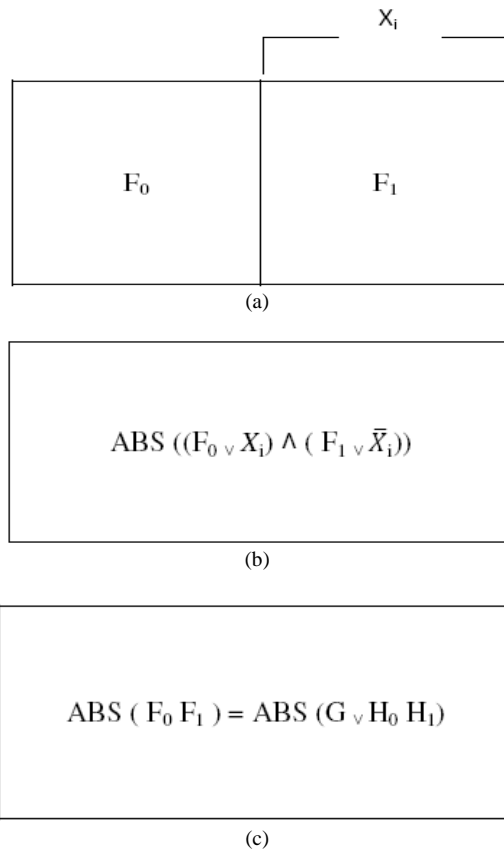
However with conventional algebraic or computer manipulation, (11) is more tedious than (10). With VEKM representation, the CE and CS operations can be made to go hand in hand, thereby making (11) more advantageous than (10).

Our procedure utilizes an adaptation of a VEKM folding technique for complete-sum derivation (Rushdi and Al-Yahya, 2000b). Let a VEKM be used to represent the pertinent function. Entries of the VEKM are converted into complete-sum entries via algebraic methods employing consensus generation and absorption. **Figure 1a** and **1b** demonstrate the basic step in VEKM folding which converts a map variable  $X_i$  into an entered variable, while retaining CS entries in the new VEKM representation of the pertinent function. In **Fig. 1b**, we use  $ABS(F)$  to denote an equivalent absorptive formula of  $F$ , i.e., a formula obtained from  $F$  by successive deletion of terms absorbed in other terms of  $F$ . The formula in **Fig. 1b** uses ANDing (multiplication) of CS formulas as an alternative for consensus generation. This multiplication is implemented via a multiplication matrix which allows an easy tracking of absorptions because of the fact that if a term is to be ever absorbed, then one of its absorbing terms will belong to either its row or to its column (Rushdi and Al-Yahya, 2000b). The current procedure adapts VEKM folding to produce the conjunctive eliminant of the pertinent function rather than the function itself, as shown in **Fig. 1c**. If the subfunctions  $F_0$  and  $F_1$  have some terms in common, i.e., if they can be written as  $F_0 = G \vee H_0$  and  $F_1 = G \vee H_1$ , where  $G$  is a disjunction of common terms, then "intelligent multiplication" (Brown, 2003; Rushdi and Al-Yahya, 2000b) replaces  $ABS(F_0 F_1)$  in **Fig. 1c** by  $ABS(G \vee H_0 H_1)$ . Note that  $CE(G(X,P),P)$  can be obtained by ANDing the VEKM cells of  $G(X,P)$  all at once, but we choose to implement this gradually by eliminating one map variable at a time. This allows the use of multiplication matrices at each step and hence simplifies the search for potentially absorbed terms. The VEKM procedure can now be stated as follows.

Use a VEKM of map variables  $P$  and entered variables  $X$  to represent  $G(X,P)$ . Make use of the fact:

$$X_i \oplus f_i(P) = \begin{cases} X_i & \text{when } f_i(P) = 0 \\ \bar{X}_i & \text{when } f_i(P) = 1 \end{cases} \quad (12)$$

Equation (12) means that the term  $(X_i \oplus f_i(P))$  is replaced by  $X_i$  itself in all map cells in which  $f_i(P)$  is not asserted and by the complement of  $X_i$  in all map cells in which  $f_i(P)$  is asserted:



**Fig. 1.** The typical step of VEKM folding modified to obtain the conjunctive eliminant of the pertinent function (a)  $f(X)$  with CS subfunctions  $F_0$  and  $F_1$  (b)  $f(X)$  in CS form (c) CE  $\{f(X), X_i\}$

Make sure that VEKM entries in the VEKM for  $G(X, P)$  are represented by CS formulas. If they are not, use a simple algebraic technique, such as the Improved Tison Method (Rushdi and Al-Yahya, 2000b) to cast them in CS form. Now conjunctively eliminate the map variables of the VEKM, one by one, till a VEKM of 0 map variables and a single cell is obtained. This is a purely-algebraic formula for CE (CS  $(G(X, P), P)$  or CS  $(CE(G(X, P), P))$ ). In each folding, use a multiplication matrix for the conjunction shown in **Fig. 1c** and restrict your application of the  $ABS(.)$  operator to comparing a potentially absorbable term to terms in its row and its column.

### Example 2

A Boolean equation of the form  $f(X_1, X_2, X_3) = 0$ , where  $f: B^3_{16} \rightarrow B_{16}$ ,  $B_{16} = FB(a, b)$  has the single-parameter parametric general solution Equation 13a-d:

$$ab = 0 \quad (13a)$$

$$X_3 = b\bar{P} \vee aP \quad (13b)$$

$$X_2 = b\bar{P} \vee aP \quad (13c)$$

$$X_1 = 0 \quad (13d)$$

Construct the equivalent single Equation 14:

$$G(X_1, X_2, X_3; P) = (ab) \vee (X_3 \oplus (\bar{a}P \vee b\bar{P})) \vee (X_2 \oplus aP \vee b\bar{P}) \vee (X_1 \oplus 0) = 0 \quad (14)$$

**Figure 2** is a VEKM representation of the function  $G(X_1, X_2, X_3; P)$  with map variable  $P$  and entered variables  $X_1, X_2$  and  $X_3$ . The entries of this VEKM are rewritten in CS form with the aid the Improved Tison Method (Rushdi and Al-Yahya, 2000b).

**Figure 3** shows an ANDing table (Multiplication table) for the two VEKM entries in **Fig. 2** to produce CE  $(G(X, P), P)$  in CS form. Absorbed terms are deleted by circling them, while retained terms are highlighted by writing them in bold. In the spirit of **Fig. 1c**, common terms of these entries are kept aside and noncommon terms are multiplied. As seen in **Fig. 3** absorptions take place within individual rows or within individual columns. The final result is Equation 15:

$$CS(CE)(G(X, P), P) = ab \vee X_1 \vee aX_3 \vee b\bar{X}_3 \vee a\bar{X}_3 \vee \bar{a}X_2\bar{X}_3 \vee \bar{a}bX_2 \vee \bar{b}X_2X_3 \quad (15)$$

### 3.3. Derivation of the Boolean Equation from its Particular Solutions

Let the Boolean equation  $f(X) = 0$ , where  $X = [X_1 X_2, \dots, X_n]^T$  and  $f(X): B^n \rightarrow B$ , (where  $B$  is a big Boolean algebra) has a consistency condition (1) and a set of  $m$  particular solutions. The  $j$ th such solution  $u_j = [u_{1j} u_{2j} \dots u_{nj}]^T$  ( $1 \leq j \leq m$ ) is given by Equation 16:

$$X_{ij} = u_{ij}, \quad 1 \leq i \leq n \quad (16)$$

where,  $u_{ij}$  are elements of the underlying Boolean algebra  $B$  (collapsed to a smaller algebra if  $s_0 \neq 0$ ). The conditions (16) for a particular solution  $j$  are equivalent to Equation 17:

$$x_{ij} \oplus u_{ij} = 0, \quad 1 \leq i \leq n \quad (17)$$

where,  $\oplus$  stands for the exclusive-OR (XOR) operation or modulo-2 addition. Conditions (17) and (1) can be disjuncted (ORed) together to form a single equation (Equation 18) whose unique solution is solution  $u_j$  (Rudeanu, 2001):

$$V_{i=1}^n (X_{ij} \oplus u_{ij}) \vee s_0 = 0 \quad (18)$$

There are  $m$  conditions of the form (18) since  $1 \leq j \leq m$ . The conjunction (ANDing) of equations (18) produces an equation which has  $m$  solutions  $u_j$  ( $1 \leq j \leq n$ ) (Rudeanu, 2001). Hence, the function  $f(X)$  can be reconstructed by the formula of Equation 19:

$$f(X) = (\Lambda_{j=1}^m [V_{i=1}^n (X_{ij} \oplus u_{ij})] \vee s_0) \quad (19)$$

P	
$ab \vee (b \oplus X_3) \vee$ $(b \oplus X_2) \vee X_1$ $= ab \vee X_1 \vee \bar{b}X_3 \vee b\bar{X}_3$ $\vee \bar{b}X_2 \vee b\bar{X}_2 \vee aX_3 \vee$ $aX_2 \vee \bar{X}_2X_3 \vee X_2\bar{X}_3$	$ab \vee (\bar{a} \oplus X_3) \vee$ $(a \oplus X_2) \vee X_1$ $= ab \vee X_1 \vee aX_3 \vee \bar{a}\bar{X}_3$ $\vee \bar{a}X_2 \vee a\bar{X}_2 \vee b\bar{X}_3 \vee$ $bX_2 \vee X_2X_3 \vee \bar{X}_2\bar{X}_3$

$G(X_1, X_2, X_3; P)$  in CS entries

**Fig. 2.** A VEKM representation of the function  $G(X_1, X_2, X_3; P)$  with map variable  $P$  and CS entries

$ab \vee X_1 \vee aX_3 \vee b\bar{X}_3$					
$\bar{b}X_3$	$\bar{b}X_2$	$b\bar{X}_2$	$aX_2$	$\bar{X}_2X_3$	$X_2\bar{X}_3$
$\bar{a}\bar{X}_3$	$\bar{a}\bar{b}X_2\bar{X}_3$	$\bar{a}b\bar{X}_2\bar{X}_3$			$\bar{a}X_2\bar{X}_3$
$\bar{a}X_2$	$\bar{a}\bar{b}X_2X_3$	$\bar{a}bX_2$			$\bar{a}X_2\bar{X}_3$
$a\bar{X}_2$	$a\bar{b}\bar{X}_2X_3$	$ab\bar{X}_2$		$a\bar{X}_2X_3$	
$bX_2$			$abX_2$		$bX_2\bar{X}_3$
$X_2X_3$	$\bar{b}X_2X_3$	$\bar{b}X_2\bar{X}_3$	$aX_2X_3$		
$\bar{X}_2\bar{X}_3$		$b\bar{X}_2\bar{X}_3$			

**Fig. 3.** The conjunctive eliminant of the function in Fig. 2 obtained in CS form

Which reduces by intelligent multiplication (Brown, 2003; Rushdi and Al-Yahya, 2000b) to Equation 20:

$$f(X) = (\Lambda_{j=1}^m (V_{i=1}^n (X_{ij} \oplus u_{ij}))) \vee s_0 \quad (20)$$

Use of purely-algebraic manipulations to (a) construct  $f(X)$  via (6) and (b) convert it into a canonical form, can be somewhat cumbersome. Instead we construct the natural map or VEKM for  $f(X)$ . We obtain the map entries which are the discriminants of  $f(X)$  and cast them in complete-sum form. Then we apply the conventional procedure of VEKM folding that retains complete-sum entries in the cells of the folded VEKM as in Fig. 1a and b (Rushdi and Al-Yahya, 2001). Finally, we end with a VEKM of 0 map variables, i.e., a purely algebraic expression, that represents the complete sum  $F(X) = CS(f(X))$ .

### Example 3

Consider the equation  $f(X, Y) = 0$  over  $B_{16} = FB(a, b)$ , whose solution in (Rudeanu, 1974) indicated that it has a consistency condition  $0 = 0$  and a set  $S$  of particular solutions  $(X, Y)$  given by Equation 21:

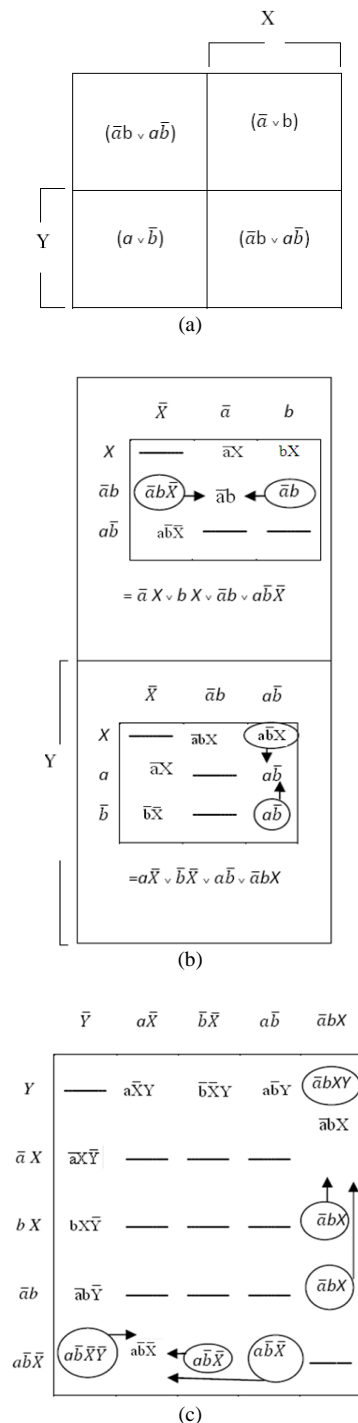
$$S = \{(ab, \bar{a}b), (a, b), (\bar{b}, \bar{a}), (a \vee \bar{b}), (\bar{a} \vee b)\} \quad (21)$$

According to (21), an expression for the function  $f(X, Y)$  is Equation 22:

$$f(X, Y) = 0 \vee [((X \oplus \bar{a}b) \vee (Y \oplus \bar{a}b))((X \oplus a) \vee (Y \oplus b))((X \oplus \bar{b}) \vee (Y \oplus \bar{a}))((X \oplus (a \vee \bar{b})) \vee (Y \oplus (\bar{a} \vee b)))] \quad (22)$$

X	
$(\bar{a}\bar{b} \vee \bar{a}b) \wedge (a \vee b) \wedge$ $(\bar{b} \vee \bar{a}) \wedge (a \vee \bar{b} \vee \bar{a} \vee b)$	$(\bar{a} \vee b \vee \bar{a}b) \wedge (\bar{a} \vee b) \wedge$ $(b \vee \bar{a}) \wedge (\bar{a}b \vee \bar{a} \vee b)$
$((\bar{a}\bar{b} \vee a \vee \bar{b}) \wedge a \vee \bar{b}) \wedge$ $(\bar{b} \vee a) \wedge (a \vee \bar{b} \vee a\bar{b})$	$(\bar{a} \vee b \vee a \vee \bar{b}) \wedge (\bar{a} \vee \bar{b}) \wedge$ $(b \vee a) \wedge (\bar{a}b \vee a\bar{b})$

**Fig. 4.** A VEKM representation of the function whose particular solutions are given by the set  $S$  in (21), subject to consistency condition  $0 = 0$



**Fig. 5.** The VEKM in Fig. 4: (a) with each of its entries reduced to simplified form which is also complete-sum (CS) form, (b) folded w.r.t X with entries still in CS form and (c) further folded w.r.t Y with entry in CS form

A simpler expression for the function  $f(X, Y)$  can be obtained by representing this function via the VEKM in Fig. 4, which has map variables  $X$  and  $Y$ . Each of the entries of this VEKM is a product-of-sums (pos) expression that can be multiplied out into a simplified sum-of-products (sop) expression as shown in Fig. 5a. The VEKM in Fig. 5 can be used to yield the following expression for  $f(X, Y)$  in Equation 23:

$$f(X, Y) = \bar{a}\bar{b}(\bar{X} \vee Y) \vee \bar{a}b(X \vee \bar{Y}) \vee (a \vee \bar{b})\bar{X}Y \vee (\bar{a} \vee b)X\bar{Y} \quad (23)$$

The VEKM can also be folded twice with the CS nature of entries retained Fig. 5b and c to yield the following expression for the complete sum  $F(X)$  of the function  $f(X)$  in Equation 24:

$$F(X) = CS(f(X)) = \bar{a}\bar{X}Y \vee \bar{a}b\bar{X}Y \vee \bar{a}bX \vee \bar{a}X\bar{Y} \vee bX\bar{Y} \vee \bar{a}b\bar{Y} \vee \bar{a}b\bar{X} \quad (24)$$

The minimal sum formula for  $f(X)$  in (23) is the same as its complete-sum formula in (24). The VEKM representations for  $f(X)$  in Fig. 5 and its formula (24) can be shown to be equivalent to the corresponding ones for the original function in (Rudeanu, 1974).

## 4. DISCUSSION

In all cases, the VEKM proved very useful as a natural map for the pertinent function and as an efficient implementation of the required procedures. Not only did the VEKM offer pictorial insight for clarifying the pertinent concepts, but it also acted as a divide-and-conquer strategy for implementing the required procedures. The VEKM proved to be highly suitable for implementing the tasks constituting the required procedures. In particular, the VEKM allowed the combination of the two major tasks of conjunctive elimination and complete-sum derivation. In addition, use of the VEKM resulted in a considerable reduction of the complexity of complete-sum derivation. Consensus generation was restricted to the initial entries of the VEKM and subsequently avoided through the use of multiplication (ANDing) during VEKM folding. Tracking of absorbable terms was considerably simplified by restricting elimination to one variable at a time, or equivalently by implementing multiplication via a two-dimensional matrix form.



## 5. CONCLUSION

This study presented methods that handle the inverse problem for the three main types of solutions of Boolean equations: (a) Subsumptive general solutions, (b) Parametric general solutions and (c) Particular solutions. The reconstructed function  $f(X)$  in every case was set in a canonical form, namely, the complete-sum form (the Blake Canonical form), to facilitate proving its equivalence to the original function. The methods presented herein are a mixture of purely-algebraic methods and map methods that utilize the variableentered Karnaugh map. These methods are demonstrated with carefully-chosen illustrative examples over big Boolean algebras of various sizes.

## ACKNOWLEDGEMENT

This article was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah. The authors, therefore, acknowledge with thanks DSR technical and financial support.

## 5. REFERENCES

- Abdel-Gawad, A.H., A.F. Atiya and N.M. Darwish, 2010. Solution of systems of Boolean equations via the integer domain. *J. Inform. Sci.*, 180: 288-300. DOI: 10.1016/j.ins.2009.09.010
- Baneres, D., J. Cortadella and M. Kishinevsky, 2009. A recursive paradigm to solve Boolean relations. *IEEE Trans. Comput.*, 58: 512-527. DOI: 10.1109/TC.2008.165
- Blake, A., 1938. *Canonical Expressions in Boolean Algebra*. 1st Edn., University of Chicago, Chicago, pp: 60.
- Brown, F.M., 2003. *Boolean Reasoning: The Logic of Boolean Equations*. 2nd Edn., Courier Dover Publications, Mineola, New York, ISBN-10: 0486427854, pp: 291.
- Brusentsov, N.P. and Y.S. Vladimirova, 1998. Solution of Boolean equations. *Comput. Math. Model.*, 9: 287-295. DOI: 10.1007/BF02409862
- Chai, F., X.S. Gao and C. Yuan, 2008. A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers. *J. Syst. Sci. Complexity*, 21: 191-208. DOI: 10.1007/s11424-008-9103-0
- Cutler, R.B., K. Kinoshita and S. Muroga, 1979. *Exposition of Tison's Method to Derive all Prime Implicants and all Irredundant Disjunctive Forms for a Given Switching Function*. 1st Edn., University of Illinois at Urbana-Champaign, Urbana, pp: 125.
- Devadas, S. and A.R. Newton, 1990. Exact algorithms for output encoding, state assignment and four-level Boolean minimization. *IEEE Trans. Comput. Aided Design*, 10: 13-27. DOI: 10.1109/HICSS.1990.205139
- Gregg, J., 1998. *Ones and Zeros: Understanding Boolean Algebra, Digital Circuits and the Logic of Sets*. 1st Edn., IEEE Press, New York, ISBN-10: 0780334264, pp: 281.
- Hammer, P.L. and S. Rudeanu, 1968. *Boolean methods in operations research and related areas*. *Econ. Operat. Res.* DOI: 10.1007/978-3-642-85823-9
- He, S. and B. Zhang, 1999. Solving SAT by algorithm transform of Wu's method. *J. Comput. Sci. Technol.*, 14: 468-480. DOI: 10.1007/BF02948788
- Jung, G., 1995. Comments on 'Some additions to solution of switching equations based on tabular algebra'. *IEEE Trans. Comput.*, 44: 1357-1358. DOI: 10.1109/12.475135
- Larabee, T., 1992. Test pattern generation using Boolean satisfiability. *IEEE Trans. Comput. Aided Design*, 11: 4-15. DOI: 10.1109/43.108614
- Levchenkov, V.S., 2000a. Solution of equations in Boolean algebra. *Comput. Math. Model.*, 11: 154-163. DOI: 10.1007/BF02359182
- Levchenkov, V.S., 2000b. Boolean equations with many unknowns. *Comput. Math. Model.*, 11: 143-53. DOI: 10.1007/BF02359181
- Muroga, S., 1979. *Logic Design and Switching Theory*. 1st Edn., Wiley, New York, ISBN-10: 0471044180, pp: 617.
- Reusch, B., 1975. Generation of prime implicants from subfunctions and a unifying approach to the covering problem. *IEEE Trans. Comput.*, C-24: 924-930. DOI: 10.1109/T-C.1975.224338
- Rudeanu, S., 1974. *Boolean Functions and Equations*. 1st Edn., North-Holland, Amsterdam, North-Holland, New York, ISBN-10: 0444105204, pp: 442.
- Rudeanu, S., 2001. Lattice functions and equations, *Discrete Math. Theoretical Comput. Sci.* DOI: 10.1007/978-1-4471-0241-0
- Rudeanu, S., 2003. Algebraic methods versus map methods of solving Boolean equations. *Int. J. Comput. Math.*, 80: 815-817. DOI: 10.1080/0020716031000087159

- Rudeanu, S., 2010. Boolean sets and most general solutions of Boolean equations. *J. Inform. Sci.*, 180: 2440-2447. DOI: 10.1016/j.ins.2010.01.029
- Rushdi, A.M., 1997. Karnaugh Map. In: *Encyclopaedia of Mathematics, Supplement I*, Hazewinkel, M. (Eds.). Springer, pp: 327-328.
- Rushdi, A.M. and A. Al-Shehri, 2004. Selective deduction with the aid of the variable-entered Karnaugh map. *J. King Abdulaziz Univ.: Eng. Sci.*, 15 (2): 21-29. DOI: 10.4197/Eng.15-2.2
- Rushdi, A.M. and H.A. Al-Yahya, 2000a. A Boolean minimization procedure using the variable-entered Karnaugh map and the generalized consensus concept. *Int. J. Elect.*, 87: 769-794. DOI: 10.1080/00207210050028724
- Rushdi, A.M. and H.A. Al-Yahya, 2000b. Derivation of the complete sum of a switching function with the aid of the variable entered karnaugh map. *King Saud Univ. J. Eng. Sci.*, 13: 239-269.
- Rushdi, A.M. and H.A. Al-Yahya, 2001. Further improved variable-entered Karnaugh map procedures for obtaining the irredundant forms of an incompletely-specified switching function. *J. King Abdulaziz University: Eng. Sci.*, 13: 111-152. DOI: 10.4197/Eng.13-1.6
- Rushdi, A.M. and M.H. Amashah, 2011. Using variable-entered Karnaugh maps to produce compact parametric general solutions of Boolean equations. *Int. J. Comput. Math.*, 88: 3136-3149. DOI: 10.1080/00207160.2011.594505
- Rushdi, A.M., 1983. Symbolic reliability analysis with the aid of variable-entered Karnaugh maps. *IEEE Trans. Reliabil.*, R-32: 134-139. DOI: 10.1109/TR.1983.5221510
- Rushdi, A.M., 1985. Map derivation of the minimal sum of a switching function from that of its complement. *Microelectronics Reliabil.*, 25: 1055-1065. DOI: 10.1016/0026-2714(85)90481-0
- Rushdi, A.M., 1986. Map differentiation of switching functions. *Microelectronics Reliabil.*, 26: 891-908. DOI: 10.1016/0026-2714(86)90233-7
- Rushdi, A.M., 1987. Improved variable-entered Karnaugh map procedures. *Comput. Elect. Eng.*, 13: 41-52. DOI: 10.1016/0045-7906(87)90021-8
- Rushdi, A.M., 2001a. Prime-implicant extraction with the aid of the variable-entered Karnaugh map. *Umm Al-Qura University J. Sci. Med. Eng.*, 13: 53-74.
- Rushdi, A.M., 2001b. Using variable-entered Karnaugh maps to solve Boolean equations. *Int. J. Comput. Math.*, 78: 23-38. DOI: 10.1080/00207160108805094
- Rushdi, A.M., 2004. Efficient solution of Boolean equations using variable-entered Karnaugh maps. *J. King Abdul-Aziz Univ.: Eng. Sci.*, 15 (1): 105-121. DOI: 10.4197/Eng.15-1.7
- Thayse, A., 1978. Meet and join derivatives and their use in switching theory. *IEEE Trans. Comput.*, C-27: 713- 720. DOI: 10.1109/TC.1978.1675178
- Tison, P., 1967. Generalization of consensus theory and application to the minimization of Boolean functions. *IEEE Trans. Elect. Comput.*, EC-16: 446-456. DOI: 10.1109/PGEC.1967.264648
- Trabado, P.P., A. Lloris-Ruiz and J. Ortega-Lopera, 1993. Solution of switching equations based on a tabular algebra. *IEEE Trans. Comput.*, 42: 591-596. DOI: 10.1109/12.223678
- Tucker, J.H. and M.A. Tapia, 1992. Using Karnaugh maps to solve Boolean equations by successive elimination. *Proc. IEEE Southeastcon*, 2: 589-592. DOI: 10.1109/SECON.1992.202260
- Tucker, J.H. and M.A. Tapia, 1995. Solution of a class of Boolean equations. *Proc. IEEE Southeastcon*, 1: 106-112. DOI: 10.1109/SECON.1995.513067
- Unger, S.H., 1994. Some additions to solution of switching equations based on a tabular algebra. *IEEE Trans. Comput.*, 43: 365-367. DOI: 10.1109/12.272437
- Woods, S. and G. Casinovi, 1996. Efficient solution of systems of Boolean equations. *Proceedings of the IEEE/ACM International Conference on Computer-Aided Design*, Nov. 10-14, ACM Press, San Jose, CA, USA., pp: 542-546.
- Woods, S. and G. Casinovi, 2001. Multiple-level logic simulation algorithm. *IEEE Proc. Comput. Digital Techniques*, 148: 129-137. DOI: 10.1049/ip-cdt:20010485