Lattices and Boolean Algebra from Boole to Huntington to Shannon and Lattice Theory

Hassan Farhat
Computer Science
University of Nebraska at Omaha, USA

Abstract - The study of computer design and architecture includes many topics on formal languages and discrete structures. Among these are state minimizations, Boolean algebra, and switching algebra. In minimization, three approaches are normally used that are based on equivalence relations. Partial order relations are used today in constructions of Boolean algebra.

In this paper we survey this important algebra from its beginnings as alternative symbolic algebra starting with George Boole and De Morgan, to Peirce, to Venn, to Huntington and to Shannon. We then look at definitions based on lattice theory. Lattices are special cases of partially ordered sets that have common properties with equivalence relations. The paper is educational in nature intended to aid the instructor on this topic from its beginnings and provide a condensed survey.

Keywords: Digital Design, Boolean Algebra, Switching Algebra, Symbolic Algebra, Lattices, State Minimization

1 Introduction

Fundamental to all aspects of computer design is the mathematics of Boolean algebra and formal languages used in the study of finite state machines. Topics on formal languages are found in [1-3].

Boolean algebra provides the mathematical tools needed in design, realization and verification. While the algebra was intended as a mathematical tool for formalizing logic [4], many years later it found applications in computer engineering where it was adapted by Shannon as two-valued algebra to be used in design of relays [5,6]. The algebra has matured since its introduction by its founder George Boole and other scholars such as De Morgan [7]. Boole introduction of the symbolic algebra emphasized similarities and differences to traditional numerical algebra. In expanding the possible similarities between both, Boole did consider a two-valued Boolean algebra as a solution to the idempotent property \((x \cdot x = x)\). The idempotent property holds true in traditional numerical algebra only for two cases, \(x = 0\) and \(x = 1\) [8]. Today, with few exceptions, many textbooks on computer and digital design assume a two-value Boolean algebra where the elements can be true or false, high or low, and 0 or 1 for example [9-15].

In this paper we survey the progress of this important algebra from its beginnings to today's definitions based on lattice theory. Since its introduction in 1847 the algebra has witnessed contributions by many scholar such as Pierce [16], Venn [17], Huntington [18], and Shannon [5]. We compare these contributions as we progress in the survey. After the initial idea of forming this survey, we found an expanded reference on the topic [19]. Part of our work is influenced by [19].

The paper is organized as follows. In section 2, we look at the history of the algebra from Boole to Peirce to Venn and to Huntington. Section 3 looks at the contributions by Shannon. In section 4 we look at Boolean algebra as a special type of a lattice. Section 5 discusses the common mathematical properties. The conclusion is given in section 6.

2 A Brief History of Boolean Algebra from Boole to Peirce, Venn, and Huntington

Boolean algebra derives its name in honor of George Boole [4]. During the mid-nineteenth century, several scholars were interested in formalizing alternative algebras on logic that is different from numerical algebra (algebra of numbers) [4,7]. These included Boole, De Morgan and Hamilton. De Morgan's influence on the formalization of Boolean algebra is evident in De Morgan's Formal Logic and examples of symbolic algebra [7]. In symbolic algebra, the algebra is defined by a set of symbols and a set of operations on the symbols. The different interpretations of the algebra are derived afterwards. This notion of the symbolic algebra has influenced Boole formalization of the algebra as discussed next.

In [8], Boole discussed his Algebra of Logic where he referred to the combinations of symbols and operations as signs and then continued to break the signs into literals (symbols) and "signs of operations" on the literals such as +, −, × and "sign of identity, =" (borrowed from numeric algebra
but with different interpretations). His interpretation of a literal such as \( x \) as "a class of individuals to which a particular name or description is applicable". He also referred to the class of "nothing" to mean "no being" and class of "universe" to mean "all beings". Today these represent the empty set and the universal set.

As to the operations on classes, Boole used the product \( xy \), where \( x \) and \( y \) represent two classes, to mean the class of things where the descriptions (or individuals) given to \( x \) and \( y \) are simultaneously true (applicable). "Let it further be agreed, that by the combination \( xy \) shall be represented that class of things to which the names or descriptions represented by \( x \) and \( y \) are simultaneously applicable. Thus, if \( x \) alone stands for "white things," and \( y \) for "sheep," let \( xy \) stand for "white sheep;"". With this definition, two important properties are deduced to hold true, as is the case in numeric algebra with respect to multiplication, mainly commutativity and associativity, hold true in Boole Algebra of Logic.

In his writings, it was a common theme for Boole to relate his form of algebra to traditional numeric algebra and point to similarities as well as to differences. Among the differences between the two algebras he discussed were the cancellation property, which holds true in regular algebra but not in his symbolic algebra, and the idempotent property, which holds true in symbolic algebra but not in regular algebra. The cancellation property is

\[
xy = xz \quad \text{and} \quad x \neq 0 \quad \text{then} \quad y = z \tag{1}
\]

The idempotent property is

\[
x^2 = x \tag{2}
\]

In continuing with comparisons of common properties of the two algebras, Boole introduced a two-value Boolean algebra as an algebra where the idempotent property does hold true as follows. If the composition is understood as a multiplication in traditional numeric algebra then the solution to equation (2) in regular algebra is \( x = 0 \) and \( x = 1 \). Hence an algebra with two classes only "nothing" (0 in traditional algebra) and "universe" (1 in traditional algebra) will work in both algebras with the operators interpreted accordingly.

Today's Boolean algebra includes two additional operations, OR (+) and NOT (¯). Boole considered these operations in [8] where he defined the binary operator + to have a meaning over classes (operands) that have nothing in common, mutually exclusive. \( x + y \) refers to aggregate class (set) composed of \( x \) and \( y \). This was done in analogy to regular algebra, the number of elements in the aggregate set is the sum of the elements in each class. This definition has changed since then and is replaced by the inclusive OR as suggested by Peirce and Venn [16,17]. As to the NOT operator, Boole used the notation \( 1 - x \) to mean \( \overline{x} \) or \( x' \). The use of the over bar, instead of \( 1 - x \), was suggested by Venn to remove the ambiguity resulted from \( 1 - x \). Later, Shannon [5] used the prime symbol as alternative to the over bar and to \( 1 - x \). Boole represented \( 1 - x \) as "contrary or supplementary class of objects".

Today's Boolean algebra is such that the idempotent property holds true under + as well based on Peirce and Venn modifications [16,17]. While under Boole the term \( x + x \) will have no meaning due to the constraint that the classes must be mutually exclusive (not possible when both terms (\( x \)) are the same), starting with Peirce and following with Venn the idempotent property holds true due to relaxing the constraint of mutual exclusion.

Boole restriction of the use of + with mutual exclusive to preserve the aggregate sum as in arithmetic sum was relaxed by Peirce where + represents a logical relation (logical operation). To emphasize this, Peirce changed the + operation to '⊔,' and defined '⊔,' as "\( a \, ⊔, \, b \) denote all the individuals contained under \( a \) and \( b \) together". That is, what is common to \( a \) and \( b \) is taken into account once. This is similar to counting number of elements in the resulting set of the union operation.

Similar arguments were presented by Venn to the meaning of logical add, \( a \, ⊔, \, b \), where he considered several interpretations [17]. Venn's contribution to symbolic logic includes Venn diagrams where he represented classes (sets) using circles and represented composition (set intersection), addition (set union) and \( 1 - x \) (set complement) using these diagrams.

In further developing the symbolic algebra introduced by Boole, Huntington [18] has considered an alternative important approach to further the study; it is that of axiomatic algebra based on a set of symbols, and a set of postulates including composition postulates. This was emphasized in Huntington paper [18], "... show how the whole algebra, in its abstract form, may be developed from a selected set of fundamental propositions, or postulates, which shall be independent of each other, and from which all the other propositions of the algebra can be deduced by purely formal processes."

The algebra considered does not depend on the meaning or interpretation of the symbols as intended by Boole but rather on the set of postulates placed on the compositions of the symbols. To distinguish the compositions symbols found in the postulates from the traditional symbols found in numeric algebra, Huntington used the symbols ★, ⊕, V, and \( \Lambda \) to represent combination operators and special element symbols. In the application to Boolean algebra, the symbols represent, respectively, the logical sum, logical product, the constant 1, and constant 0.

In his paper, Huntington presented three sets of equivalent postulates. We list the first set taken from [18]. "... we take as the fundamental concepts a class, \( K \), with two rules of combination, ★ and ⊕; and as the fundamental propositions, the following ten postulates:

\begin{itemize}
  \item [a.] \( a \, ⊕ \, b \) is in the class whenever \( a \) and \( b \) are in the class.
  \item [b.] \( a \, ⊕ \, b \) is in the class whenever \( a \) and \( b \) are in the class.
\end{itemize}
IIa. There is an element $\Lambda$ such that $a \oplus \Lambda = a$ for every element $a$.

IIb. There is an element $V$ such that $a \ominus V = a$ for every element $a$.

IIia. $a \oplus b = b \ominus a$ whenever $a, b, a \oplus b, b \ominus a$ are in the class.

IIib. $a \ominus b = b \ominus a$ whenever $a, b, a \ominus b, b \ominus a$ are in the class.

IVa. If $(b \ominus c) = (a \ominus b) \ominus (a \ominus c)$ whenever $a, b, c, a \ominus b, a \ominus c, b \ominus c, a \ominus (b \ominus c)$, and $(a \ominus b) \ominus (a \ominus c)$ are in the class.

IVb. $(b \ominus c) = (a \ominus b) \ominus (a \ominus c)$ whenever $a, b, c, a \ominus b, a \ominus c, b \ominus c, a \ominus (b \ominus c)$, and $(a \ominus b) \ominus (a \ominus c)$ are in the class.

V. If the elements $\Lambda$ and $V$ in postulates IIa and IIb exist and are unique, then for every element $a$ there is an element $\bar{a}$ such that $a \ominus \bar{a} = V$ and $a \ominus \bar{a} = \Lambda$.

VI. There are at least two elements, $x$ and $y$, in the class such that $x \neq y$.

Huntington used proof by deduction to derive the different Boolean algebra properties found in today's textbooks. He also gave an example of $\oplus$ and $\ominus$ tables similar to truth tables of the logic OR and AND when the class of elements, $K$, contains 0 and 1 only (two-valued Boolean algebra).

3 Shannon's Contribution to Digital Design

While the algebra and its definitions as an abstract algebra was founded and studied as an abstract mathematical algebraic structure, Shannon [5] related the algebra to relays design in electrical engineering. With that, the algebra found footing in digital and computer design. We look at Shannon's contribution in this section.

Shannon represented the composition operations in Boolean algebra as switches in parallel and in series. He also used the switch structure to simplify Boolean expressions. In addition, he introduced the method of proof by perfect induction, used to show equality of Boolean functions. Other contributions included Shannon's expansion, adapted from Boole expansion with regard to his special two-value algebra. The following excerpts are taken from Boole [8].

"Suppose that we are considering any class of things with reference to this question, viz., the relation in which its members stand as to the possession or want of a certain property $x$. As every individual in the proposed class either possesses or does not possess the property in question, we may divide the class into two portions, the former consisting of those individuals which possess, the latter of those which do not possess, the property. ... Suppose then, ..., that the members of that portion which possess the property $x$, possess also a certain property $u$, and that these conditions united are a sufficient definitions for them. We may then represent that portion of the original class by the expression $ux$. Hence the class in its totality will be represented by $ux + v(1-x)$; which may be considered as a general developed form for the expression of any class of objects considered with reference to the possession or want of a given property $x$.

Note that based Boole definition of $+$, the $+$ applies to mutually exclusive classes which is certainly the case for a two-valued algebra (the universe is $x$ and $(1-x)$). He later states "treat $x$ as a quantitative symbol, susceptible only of the values 0 and 1" and assigns the above equation to $f(x)$. Then he solves the equation for $x = 0$ and $x = 1$ to result in

$$f(x) = f(1)x + f(0)(1-x)$$

Shannon used $X$ instead of $(1-x)$ and has expanded the above equation to several variables as

$$f(X_1, X_2, ..., X_n) = X_1.f(1, X_2, ..., X_n) + X_1'.f(0, X_2, ..., X_n)$$

He then proved the equality by perfect induction on $X_1 (X_1 = 0$ and $X_1 = 1)$. He then repeated the above on all variables, always expanding the right-hand side, to obtain the canonical-sum equation

$$f(X_1, X_2, ..., X_n) = f(0,0, ..., 0)X_n'X_{n-1}'...X_1' + f(0,0, ..., 1)X_nX_{n-1}'...X_1' + \cdots + f(1,1, ..., 1)X_nX_{n-1}...X_1$$

Shannon's proofs by perfect induction were possible because of the two-valued Boolean algebra chosen with known domain.

4 Boolean Algebra as a Lattice

Today the definition of Boolean algebra has extended to lattice theory. A good source for lattice theory and Boolean algebra is found in [20]. The section looks at this topic. Boole restricted his discussion to: composition, the aggregate operator $+$ and the contrary operator $(1-x)$. Lattice theory is an extension of the concepts of partial orders defined over a set of elements and a relation, $R$, over the set. The contribution of this section is in presenting a condensed compiling of the concepts.

A relation, $R$, from a set $L$ to itself is a subset of the Cartesian product $L \times L$ and called a relation on $L$ (or relation over $L$). Elements of $R$ can be written as $(a, b)$ or a $R b$.

Let $R$ be a relation on a set $L$. We say

a) $R$ is reflexive if and only if $(a, a) \in R, \forall a \in L$

b) $R$ is symmetric if and only if $(a, b) \in R$ then $(b, a) \in R$
c) \( R \) is transitive if and only if \((a, b) \in R \) and \((b, c) \in R \) then \((a, c) \in R \).

d) \( R \) is antisymmetric if and only if \((a, b) \in R \) and \((b, a) \in R \) then \(a = b \).

A relation that is reflexive, symmetric and transitive is called an equivalence relation. In digital design equivalence relations are used in state minimizations as an example. A relation that is reflexive, antisymmetric and transitive is said to be a partial ordering relation. The set with the partial ordering relation is called a partially ordered set and abbreviated as poset. A partially ordered set, \( L \), is normally represented as 2-tuple \((S, \leq)\) where \( \leq \) represents the partially ordered relation \( R \) on \( L \). This is in analogy with the less than or equal to operator \((\leq)\) as a partial ordered relation on the set of integers. Lattices are special types of partially ordered set on set \( L \) where for each \( a \in L \) and \( b \in L \), the 2-tuple \((a, b)\) has a unique greatest lower bound (glb) and unique least lower bound (lub) discussed next.

Let \((L, \leq)\) be partially ordered with \(a, b, x, y \in L\). (a) \( x \) is said to be a lower bound of \( a \) and \( b \) if \( x \leq a \) and \( x \leq b \). (b) Similarly, \( y \) is said to be upper bound of \( a \) and \( b \) if \( a \leq y \) and \( b \leq y \). (c) \( x \) is also said to be a greatest lower bound (glb) of \( a \) and \( b \) if and only if for any other element \( x' \) in \( L \), where \( x' \) is a lower bound of \( a \) and \( b \) we have \( x' \leq x \). (d) \( y \) is also said to be a least upper bound (lub) of \( a \) and \( b \) if and only if for any other element \( y' \) in \( L \) where \( y' \) is an upper bound of \( a \) and \( b \) we have \( y \leq y' \). An element, \( g \), in \( L \) is said to be a greatest element if and only if for every \( a \in L \), \( a \leq g \). Similarly, and element \( l \) in \( L \) is said to be least element if and only if for every \( a \in L \), \( l \leq a \).

The greatest upper bound, least upper bound, greatest element and least element are unique. For completeness we include the proof of two sample cases.

Case 1: for any two elements \( a, b \in L \) their glb is unique. Assume there are two glb's \( x_1 \) and \( x_2 \). Since \( x_1 \) and \( x_2 \) are both lower bounds of \( a \) and \( b \) we have \( x_1 \leq x_2 \) since \( x_2 \) is the greatest lower bound of \( a \) and \( b \). Similarly, we have \( x_2 \leq x_1 \) since \( x_1 \) is the greatest lower bound of \( a \) and \( b \). By the antisymmetric property \( x_1 = x_2 \).

Case 2: The least element is unique. Similar logic is applied. \( 11 \leq 12 \) since \( 11 \) is the least element \((12 \in L \) hence \( 11 \leq 12 \)). Similarly \( 12 \leq 11 \). By the antisymmetric property we have \( 11 = 12 \).

The uniqueness of the glb, lub, least element and greatest element is used in the definition of Boolean algebra as follows. First, for any two elements \( a \) and \( b \) in \( L \), since lub and glb are unique they can be thought of as binary operations called join or sum represented by \( V \) or \( + \) for the lub, and meet or product represented as \( \Lambda \) or \( \cdot \). Since the least element and greatest elements are unique, they are represented as \( 0 \) and \( 1 \). In terms of algebraic representation, we can represent the previous as a 5-tuple \((L, V, \Lambda, 0, 1)\) where \( L \) is a set of elements, \( V \) and \( \Lambda \) are binary operations, and with \( 0 \) and \( 1 \) representing the least and greatest elements of \( L \).

With two additional properties on elements of a lattice the definition of a Boolean algebra is established: a Boolean algebra is \((L, V, \Lambda)\) where \( L \) is a distributive and complemented lattice. With \( 0 \) and \( 1 \), a complemented lattice is a lattice where for each element \( a \in L \) there exists an element, \( \overline{a} \), called complement of \( a \), where \( a \lor \overline{a} = 1 \) and \( a \land \overline{a} = 0 \). A distributive lattice satisfies the properties: \( a \lor (b \land c) = (a \lor b) \land (a \lor c) \) and \( a \land (b \lor c) = (a \land b) \lor (a \land c) \lor a \lor b \lor c \in L \).

With the above definition, we can show Huntington proposition as given in the previous section hold true. This is done in the next section.

5. Boolean algebra as Lattices, Huntington postulates, and Shannon's two-valued Boolean algebra

In this section we look at showing the algebra defined using lattice theory satisfies the Huntington proposition. In the verification, note that \( \Phi \) is the join (sum) \( V \) and \( \Theta \) the meet (product) \( \Lambda \). Note as well \( V \) is the greatest element \( 1 \) and \( \Lambda \) is the least element \( 0 \).

Verification of Ia and Ib follows since by definition the glb and lub of any two elements in \( L \) is such that both glb and lub are in \( L \) as well. This is set closure under \( \Lambda \) (\( \Theta \)) and \( V \) (\( \Phi \)). Proposition IIa and IIb follow as well since for each element \( a \in L \) we have \( a \lor 0 = a \) and \( a \land 1 = a \). IIa and IIb for commutativity also holds true since the glb of \((a,b)\) is the same as the glb of \((b,a)\) and the lub of \((a,b)\) is the same as the lub of \((b,a)\). The distributive properties holds by definition of the Boolean algebra above (distributive lattice). For postulates VI there at least two elements in the class; we assume the minimum number of elements in \( L \) is two corresponding to the least element \((0)\) and greatest element \((1)\).

It is remaining to show the existence of the complements and the uniqueness of the complements. The existence of complements follows from complemented lattices. The uniqueness of complements follows.

Assume given an element \( a \in L \) with two complements \( x \) and \( y \). Since each is a complement of \( a \), we have

\[
\begin{align*}
x &= x \land 1 = x \land (a \lor y) \\
&= (x \land a) \lor (x \land y) \\
&= 0 \lor (x \land y) \\
&= x \land y = y \land x
\end{align*}
\]

Now starting with \( y \) we have

\[
\begin{align*}
y &= y \land 1 = y \land (a \lor x) \\
&= (y \land a) \lor (y \land x) \\
&= 0 \lor (y \land x) \\
&= y \land x
\end{align*}
\]

Hence \( x = y \) and the complement is unique.
6 Conclusion

In this paper we surveyed the algebra, Boolean algebra, from its beginning by George Boole and De Morgan's where it did not attract initial interest to attracting much interest many years later by several scholars such as Peirce, Venn, Huntington and Shannon. We then looked at lattice theory and at Boolean algebra as a special type of a lattice, a complemented and distributive lattice. We concluded with showing that Huntington postulates can be derived from Boolean algebra as a complemented and distributive lattice. Our contribution is to provide a condensed survey of the progress of the important algebra from its beginnings starting with Boole and De Morgan's.

References