Introduction to Foundation of Boolean Algebra

Prawat Nagvajara, ECE Drexel University

This note introduces the foundation of Boolean algebra starting from the power set definition of the structure. Backgrounds are introduced as needed in the derivations of the concepts. The note concludes with the derivation of switching (logic) functions.

1. Power set: The power set of a set A of n elements, P(A) is the set of all subsets of B. Its cardinality is 2^n.

Example 1: S = {p, q, r}, n = 3, P(S) = { ø, {r}, {q}, {p), {q, r}, {p,r}, {p,q}, {p, q, r} } (ø denotes the empty set). Elements of P(S) can be coded with 3-bit vectors as P(S) = {000, 001, 010, 100, 011, 101, 110, 111} where 0 and 1 indicate the presence of the objects the subset, i.e., the empty set is coded as ø ↔ 000, {r} ↔ 001, {q} ↔ 010, {p} ↔ 100, {q, r} ↔ 011, {p, r} ↔ 101, {p, q} ↔ 110, {p, q, r} ↔ 111. A structure that describes the relations between P(A) together with properties and operations on the elements is known as Boolean algebra.

2. Boolean cubes: A Boolean cube B_n is an algebraic structure comprises vertices and edges which represent the elements of P(A) and their relation, respectively. The structure is enumerated in terms of ≤ the number of elements in the subsets (i.e., the number of ones in the vectors of the vector representation). This type of structure is called "partly ordered set." The bottom level of the structure consists of one vertex, the empty set. It is the universal lower bound of the structure. The next level in the enumeration comprises all the subsets containing one element (vectors containing single one). The next level comprises all the subsets containing two elements. The levels continue on until reach the top level comprises one vertex, the universal upper bound, which is the subset containing n elements or the set A itself. The edges are connecting vertices between immediate levels. This brings up the notion of (immediate) successors different from the arithmetic of natural numbers (totally ordered set).

To gain more insight, compare the partly ordered set to the number arithmetic. Giuseppe Peano in 1899 proposed axioms for arithmetic. 1) Zero is a number, 2) The immediate successor of a number is a number, 3) Zero is not an immediate successor of a number (universal lower bound), 4) No two numbers have the same immediate successor (arithmetic is a totally ordered set), 5) The Principle of Mathematical Induction: properties that hold true for zero and the immediate successor of a number, hold true for all numbers.

3. Successors: For v belongs in the level immediately above u, there is an edge connecting v and u if u is a subset of v. Figure 1 shows the Boolean cube of 3 elements - the power set of S, S = {p, q, r} and subset relations between the elements. Note that the successors of the 000 (the empty set) are 001, 010, 100, the subsets with 1 element which is enumerated at the first level. The second level comprises all the subsets with two elements and the third level {p, q, r} the set S itself. The universal lower bound is the empty set or the vector of all 0's, and the universal upper bound is the set itself or the vector of all 1's. The structure is said to be bounded when the universal upper bound has finite number of elements.

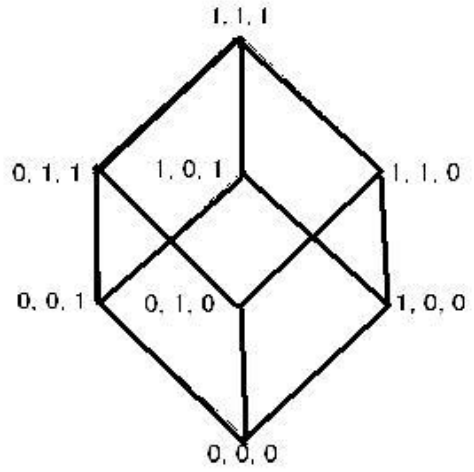

Fig. 1 Boolean Cube B_3 for Power Set of 3 Elements

4. Recursive construction of Boolean cubes: The power set of one element set has 2 elements, the empty set and the set itself, in vector representation B_1 is the set {0, 1}. Consider B_n, to construct B_{n+1} take two copies of B_n and extend the vector to n+1 bits – one copy with 0 appended on the left and the other with 1. Raise the copy with the 1 prefix (appended) by one level, since it has one more element or 1, and connect lines between the same vertices of the two copies. In Fig 1, B_1 subcube {000, 001} is the ground structure. When the 00 prefix removed the set {0, 1} is a line. The ground B_2 is the subcube {000, 001, 010, 011}, that is, when the 0 prefix is removed the set {00, 01, 10, 11} can be constructed from two copies of B_1 with 0 appended to one copy and 1 appended to the other copy. The 1 prefix copy is raised by one level and edges are connected between the same vertices of the two copies. Similarly, the ground B_2 in Fig. 1 is {000, 001, 010, 011} and the prefix 1 copy is the subcube {100, 101, 110, 111}. Try constructing B_4 and B_5.

5. Least Upper Bound or Union or '+' and Greatest Lower Bound or Intersection or '$\cdot$' - Binary Operations on the Vertices of Boolean Cube: Any two vertices in the Boolean cubes has unique least upper bound or the union (sum), that is, the union of any two elements of the power set can only result in one other subset. More precisely, take any u, v the sum, $u + v = t$ implies $u \leq t$, $v \leq t$, there is no another subset x such that $u \leq x \leq t$ and $v \leq x \leq t$. Similarly, the same can be said about the greatest lower bound or the intersection (product). Partly ordered set [S, ≤] with unique sum and product of any two elements are known as a "lattice."

6. Duality Principle: A partial ordering relation on a set: ≤ or ≥ is reflexive, anti-symmetric (ordering is a one-way relation) and transitive. The inverse relation of a partial ordering is a partial ordering. This means that an upside-down Boolean cube is a Boolean cube. The dual expressions are derived by exchanging the universal upper bound and the universal lower bound, and, the least upper bound and greatest lower bound operations are exchanged. Boolean algebra properties are listed in two versions – the properties and their dual statements.

6. Properties of lattices

Idempotent	$a + a = a$	$a \cdot a = a$
Commutative	$a + b = b + a$	$a \cdot b = b \cdot a$
Associative	$a+(b+c) = (a+b)+c$	$a \cdot (a \cdot c) = (a \cdot b) \cdot c$
Absorption	$a + a \cdot b = a$	$a \cdot (a+b) = a$

7. Complementary of a subset: Consider the power set P(A) of a set A , v' denotes the set theoretic complement. For v is a subset of A and v' is the subset of A whose elements are elements of A which are not in v. Refer to Example 1, the complement of {p, r} ↔ 101 is {q}↔ 010. The complement of the universal upper bound is the universal lower bound, {p, q, r}' = ø. In fact, v + v' = A (A is the universal upper bound), and the dual, v·v' = ø, (ø is the universal lower bound). The complementary is a unary operation, a function F: P(A) → P(A). Readily, (v')' = v, this property is called the involution.

8. Distributive property: Any t, u, v in B_n $t(u + v) = t \cdot u + t \cdot v$ and $t + u \cdot v = (t + u)(t + u)$.

9. Boolean Cube is a Lattice: Partly ordered set with the universal lower bound (the empty set), universal upper bound (the set itself), least upper bound (union, +), greatest lower bound (intersection, ·), the complementary of set (interchanging 0 and 1 in the vector representation), and the distributive property, makes Boolean cube an algebraic structure known as bounded, distributive, complementary lattice. There are lattices that are distributive but not complementary and vice versa.

7. Canonical representation: Vertices in distributive lattices have a canonical representation in terms of the sum of the vertices which are the successors of the universal lower bounds. For Boolean cubes these are the vertices containing one element. This concept is similar to the basis vectors in linear algebra, that is, any vertex can be expressed uniquely in terms of the union of these basis vertices. The distributivity is necessary for the one-to-one correspondence between the elements of the lattice and its canonical sum of the products.

8. Calculus of Boolean Expressions of n Variables: An expression $E(x_{n-1}, \ldots, x_0)$ is defined as an induction; Axiom: The literals $\{x_{n-1}, \ldots, x_0\}$ and the universal lower bound are expressions. Rule of inference: Any +, · and complementation of expressions are expressions.

9. The fundamental products (minterms): The product of all distinct n literals, are irreducible. In other words, the minterms cannot be expressed as a sum of other products. For example, consider Boolean expression with three variables x, y and z, an expression $m_5 = x'yz'$ is a product of distinct literals. It is a minterm. m_5 cannot be further reduced to a sum of other products.

10. Free Boolean Algebra with n Generators $x_{n-1}, \ldots, x_0$: The 2^n fundamental products of n literals are the bases of the canonical representation of $B_{2\wedge n}$ – Boolean algebra of $2^{2\wedge n}$ elements. For example, n=3 there are 8 minterms which form the bases for Boolean algebra of 64 elements. Try to construct a free Boolean algebra with 2 generators x_1, x_0. It is called free algebra because with n variables expressions can be constructed freely, but the expressions can be transformed to one of the $2^{2\wedge n}$ elements. The rules of the calculus stated in (8) are in fact the rules of the free Boolean algebra with n generators. The

universal lower bound – the empty set is denoted by 0. The universal upper bound, i.e., the least upper bound (sum) of all the bases, is denoted with 1.

For example, let $E(x_{n-1}, \dots , x_0)$ be an expression, we have,

$E(x_{n-1}, \dots , x_0) + 0 = E(x_{n-1}, \dots , x_0)$ $\quad\quad$ $E(x_{n-1}, \dots , x_0)\cdot 1 = E(x_{n-1}, \dots , x_0)$

$E(x_{n-1}, \dots , x_0) + 1 = 1$ $\quad\quad$ $E(x_{n-1}, \dots , x_0)\cdot 0 = 0$

where 0 denotes the universal lower bound and 1 denotes the universal upper bound of $B_{2\text{^}n}$.

11. Evaluation of Expression: The variables in expressions can be evaluated (substituted) with the elements of a Boolean algebra (called the ground algebra). For example, expression of 5 variables is evaluated over Boolean algebra of 16 elements, B_4. For a fixed assignment of the variables to elements in B_4 the result of the evaluation is an element in B_4. The evaluation is done according to rules in B_4.

12. Boolean Function F(u): $\{B_m\}^n \rightarrow B_m$, u is an n dimensional vector $[u_{n-1}\ u_{n-2} \dots u_0]$ over B_m belongs in the domain. F is an expression with n variables x_{n-1}, x_{n-2} ... and x_0. In general when m>1 not every mapping has an expression to describe it. In other words, a function exists if there is an expression for it.

13. Switching (Logic) Function: An interesting case is when m=1, $F(u): \{0, 1\}^n \rightarrow \{0, 1\}$, u is an n-bit vector $[u_{n-1}\ u_{n-2} \dots u_0]$ belongs in the domain. There is a one-to-one correspondence between an expression $E_F(x_{n-1}, x_{n-2} \dots , x_0)$ and a function F. In fact consider E_F represented by the canonical form. A minterm, $a = a_{n-1}a_{n-2} \dots a_0$ in E_F is given by a vector u where $F(u) = 1$ and $a_i = x_i$ if $u_i = 1$ and $a_i = x_i'$ if $u_i = 0$. For example u = [1 0 1] correspond to the minterm $x_2x_1'x_0$. This assertion on the isomorphism between F and E_F can be proved by induction, starting with n = 1, there are 4 mappings (truth tables) which map $\{0, 1\} \rightarrow \{0, 1\}$, the corresponding expressions are 0, x, x', x+x'. Assume that (13) is true for n-1 case, show that it is true for the n case. The proof uses the fact that $E_F(x_{n-1}, x_{n-2} \dots , x_0) = x_{n-1}'\ E_{F0}(x_{n-2} \dots , x_0) + x_{n-1}\ E_{F1}(x_{n-2} \dots , x_0)$.

14. Karnaugh map: A tabular representation of the canonical expression of a switching function of n variables. It is based on B_n where the nodes are the 2^n minterms. The map aids the visualization of the subcubes (implicants) containing in an expression. It is instrumental in understanding approaches in minimizing the number of products in an expression.