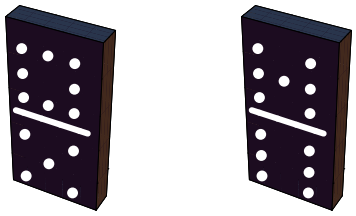
Chapter 13



BOOLEAN ALGEBRA

George Boole, 1815 - 1864

George Boole

George Boole wasn't idle a lot.
He churned out ideas on the spot,
Making marvellous use of
Inclusive/exclusive
Expressions like AND, OR, and NOT

- limerick by Andrew Robinson from the Omnificent English Dictionary In Limerick Form

GOALS

In this chapater we will develop an algebra that is particularly important to computer scientists, as it is the mathematical foundation of computer design, or switching theory. The similarities of Boolean algebra and the algebra of sets and logic will be discussed, and we will discover special properties of finite Boolean algebras.

In order to achieve these goals, we will recall the basic ideas of posets introduced in Chapter 6 and develop the concept of a lattice, which has applications in finite-state machines. The reader should view the development of the topics of this chapter as another example of an algebraic system. Hence, we expect to define first the elements in the system, next the operations on the elements, and then the common properties of the operations in the system.

13.1 Posets Revisited

From Chapter 6, Section 3, we recall the following definition:

***Definition**: Poset. A set L on which a partial ordering relation (reflexive, antisymmetric, and transitive) r is defined is called a partially ordered set, or poset, for short.*

We recall a few examples of posets:

(1) $L = \mathbb{R}$ and r is the relation $\leq$.

(2) $L = \mathcal{P}(A)$ where $A = \{a, b\}$ and r is the relation $\subseteq$.

(3) $L = \{1, 2, 3, 6\}$ and r is the relation $|$ (divides). We remind the reader that the pair (a, b) as an element of the relation r can be expressed as $(a, b) \in r$, or $a\ r\ b$, depending on convenience and readability.

The posets we will concentrate on in this chapter will be those which have maxima and minima. These partial orderings resemble that of $\leq$ on $\mathbb{R}$, so the symbol $\leq$ is used to replace the symbol r in the definition of a partially ordered set. Hence, the definition of a poset becomes:

***Definition**: Poset. A set on which a partial ordering, $\leq$, is defined is called a partially ordered set, or, in brief, a poset. Here, $\leq$ is a partial ordering on L if and only if for all $a, b, c \in L$:*

(1) $a \leq a$(*reflexivity*),

(2) $a \leq b$ *and* $b \leq a \Rightarrow a = b$ (*antisymmetry*), *and*

We now proceed to introduce maximum and minimum concepts. To do this, we will first define these concepts for two elements of the poset L, and then define the concepts over the whole poset L.

***Definition**: Lower Bound, Upper Bound. Let $a, b \in L$, a poset. Then $c \in L$ is a lower bound of a and b if $c \leq a$ and $c \leq b$. $d \in L$ is an upper bound of a and b if $a \leq d$ and $b \leq d$.*

***Definition**: **Greatest Lower Bound.** Let L be a poset and $\leq$ be the partial ordering on L. Let $a, b \in L$, then $g \in L$ is a greatest lower bound of a and b, denoted glb(a, b), if and only if*

- $g \leq a$,
- $g \leq b$, *and*
- *if* $g' \in L$ *such that if* $g' \leq a$ *and* $g' \leq b$, *then* $g' \leq g$.

The last condition says, in other words, that if g' is also a lower bound, then g is "greater" than g', so g is a greatest lower bound.

The definition of a least upper bound is a mirror image of a greatest lower bound:

***Definition: Least Upper Bound.** Let L be a poset and $\leq$ be the partial ordering on L. Let $a, b \in L$, then $\ell \in L$ is a least upper bound of a and b, denoted lub(a, b), if and only if*

- $a \leq \ell$,
- $b \leq \ell$, *and*
- *if* $\ell' \in L$ *such that if* $a \leq \ell'$ *and* $b \leq \ell'$, *then* $\ell \leq \ell'$.

Notice that the two definitions above refer to "...a greatest lower bound" and "a least upper bound." Any time you define an object like these you need to have an open mind as to whether more than one such object can exist. In fact, we now can prove that there can't be two greatest lower bounds or two least upper bounds.

***Theorem 13.1.1.** Let L be a poset and $\leq$ be the partial ordering on L, and $a, b \in L$. If a greatest lower bound of a and b exists, then it is unique. The same is true of a least upper bound, if it exists.*

Proof: Let g and g' be greatest lower bounds of a and b. We will prove that $g = g'$.

(1) g a greatest lower bound of a and $b \Rightarrow g$ is a lower bound of a and b.

(2) g' a greatest lower bound of a and b and g a lower bound of a and $b \Rightarrow g \leq g'$ by the definition of greatest lower bound.

(3) g' a greatest lower bound of a and $b \Rightarrow g'$ is a lower bound of a and b.

(4) g a greatest lower bound of a and b and g' a lower bound of a and $b \Rightarrow g' \leq g$ by the definition of greatest lower bound.

(5) $g \leq g'$ and $g' \leq g \Rightarrow g = g'$ by the antisymmetry property of a partial ordering.

The proof of the second statement in the theorem is almost identical to the first and is left to the reader. ■

***Definition: Greatest Element, Least Element.** Let L be a poset. $M \in L$ is called the greatest (maximum) element of L if, for all $a \in L$, $a \leq M$. In addition, $m \in L$ is called the least (minimum) element of L if for all $a \in L$, $m \leq a$.*

Note: The greatest and least elements, when they exist, are frequently denoted by 1 and 0 respectively.

Example 13.1.1. Let $L = \{1, 3, 5, 7, 15, 21, 35, 105\}$ and let $\leq$ be the relation | (divides) on L. Then L is a poset. To determine the *lub* of 3 and 7, we look for all $\ell \in L$, such that $3 \mid \ell$ and $7 \mid \ell$. Certainly, both $\ell = 21$ and $\ell = 105$ satisfy these conditions and no other element of L does. Next, since $21 \mid 105$, then $21 = \text{lub}(3, 7)$. Similarly, the $lub(3, 5) = 15$. The greatest element of L is 105 since $a \mid 105$ for all $a \in L$. To find the *glb* of 15 and 35, we first consider all elements g of L such that $g \mid 15$ and $g \mid 35$. Certainly, both $g = 5$ and $g = 1$ satisfy these conditions. But since $1 \mid 5$, then $glb\,(15, 35) = 5$. The least element of L is 1 since $1 \mid a$ for all $a \in L$.

Henceforth, for any positive integer n, D_n will denote the set of all positive integers which are divisors of n. For example, the set L of Example 13.1.1 is D_{105}.

Example 13.1.2. Consider the poset $\mathcal{P}(A)$, where $A = \{a, b, c\}$, with the relation $\subseteq$ on $\mathcal{P}(A)$. The *glb* of the $\{a, b\}$ and $\{a, c\}$ is $g = \{a\}$. For any other element g' of M which is a subset of $\{a, b\}$ and $\{a, c\}$ (there is only one; what is it?), $g' \subseteq g$. The least element of $\mathcal{P}(A)$ is $\emptyset$ and the greatest element of $\mathcal{P}$(A) is $A = \{a, b, c\}$. The Hasse diagram of $\mathcal{P}$(A) is shown in Figure 13.1.1.

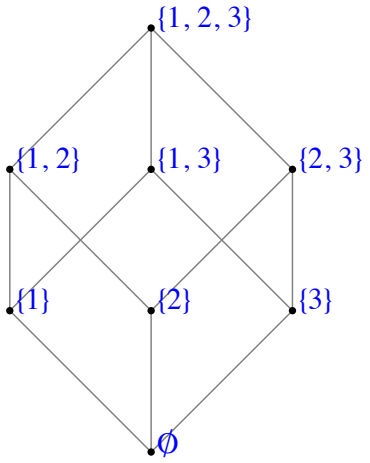


Figure 13.1.1
Example 13.1.2

With a little practice, it is quite easy to find the least upper bounds and greatest lower bounds of all possible pairs in $\mathcal{P}(A)$ directly from the graph of the poset.

The previous examples and definitions indicate that the *lub* and *glb* are defined in terms of the partial ordering of the given poset. It is not yet clear whether all posets have the property such every pair of elements has both a *lub* and a *glb*. Indeed, this is not the case (see Exercise 3).

EXERCISES FOR SECTION 13.1

A Exercises

1. Let $D_{30} = \{1, 2, 3, 5, 6, 10, 15, 30\}$ and let the relation | be a partial ordering on D_{30}.

   (a) Find all lower bounds of 10 and 15.

   (b) Find the *glb* of 10 and 15.

   (c) Find all upper bounds of 10 and 15.

   (d) Determine the *lub* of 10 and 15.

   (e) Draw the Hasse diagram for D_{30} with |. Compare this Hasse diagram with that of Example 13.1.2. Note that the two diagrams are structurally the same.

2. List the elements of the sets D_8, D_{50}, and D_{1001}. For each set, draw the Hasse diagram for "divides."

3. Figure 13.1.2 contains Hasse diagrams of posets.

   (a) Determine the *lub* and *glb* of all pairs of elements when they exist. Indicate those pairs that do not have a *lub* (or a *glb*).

   (b) Find the least and greatest elements when they exist.

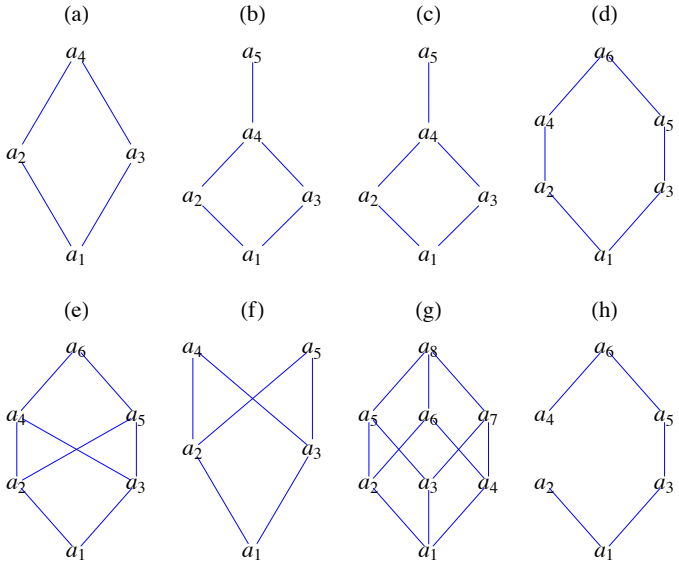


Figure 13.1.2
Exercise 3

4. For the poset $(\mathbb{N}, \leq)$, what are $glb(a, b)$ and $lub(a, b)$? Are there least and/or greatest elements?

5. (a) Prove the second part of Theorem 13.1.1, the least upper bound of two elements in a poset is unique, it one exists.

(b) Prove that if a poset L has a least element, then that element is unique.

6. We naturally order the numbers in $A_m = \{1, 2, \ldots, m\}$ with "less than or equal to," which is a partial ordering. We may order the elements of $A_m \times A_n$ by $(a, b) \leq (a', b') \Leftrightarrow a \leq a'$ and $b \leq b'$.

(a) Prove that this defines a partial ordering of $A_m \times A_n$.

(b) Draw the ordering diagrams for $\leq$ on $A_2 \times A_2$, $A_2 \times A_3$, and $A_3 \times A_3$.

(c) What are $glb((a, b), (a', b'))$ and $lub((a, b), (a', b'))$?

(d)Are there least and/or greatest elements in $A_m \times A_n$?

13.2 Lattices

In this section, we restrict our discussion to *lattices*, those posets where every pair of elements has a *lub* and a *glb*. We first introduce some notation.

Definitions: Join, Meet. *Let L be a poset under an ordering* $\leq$. *Let* $a, b \in L$. *We define:*

$a \bigvee b$ *(read "a join b") as the least upper bound of a and b, and*

$a \bigwedge b$ *(read "a meet b") as greatest lower bound of a and b.*

Since the join and meet operations produce a unique result in all cases where they exist, by Theorem 13.1.1, we can consider them as binary operations on a set if they aways exist. Thus the following definition:

Definition: Lattice. *A lattice is a poset L (under* $\leq$ *) in which every pair of elements has a lub and a glb. Since a lattice L is an algebraic system with binary operations* $\vee$ *and* $\wedge$ *, it is denoted by* $[L; \bigvee, \bigwedge]$.

In Example 13.1.2, the operation table for the *lub* operation is easy, although admittedly tedious, to do. We can observe that every pair of elements in this poset has a least upper bound. In fact, $A \bigvee B = A \bigcup B$.

The reader is encouraged to write out the operation table for the *glb* operation and to note that every pair of elements in this poset also has a *glb*, so that $\mathcal{P}(A)$ together with these two operations is a lattice. We further observe that:

(1) $[\mathcal{P}(A); \bigvee, \bigwedge]$ is a lattice (under $\subseteq$) for any set A, and

(2) the join operation is the set operation of union and the meet operation is the operation intersection; that is, $\bigvee = \bigcup$ and $\bigwedge = \bigcap$.

It can be shown (see the exercises) that the commutative laws, associative laws, idempotent laws, and absorption laws are all true for any lattice. An example of this is clearly $[\mathcal{P}(A); \bigcup, \bigcap]$, since these laws hold in the algebra of sets. This lattice is also distributive in that join is distributive over meet and meet is distributive over join. This is not always the case for lattices in general however.

Definition: Distributive Lattice. *Let* $[L; \vee, \wedge]$ *be a lattice (under* $\leq$*).* $[L; \vee, \wedge]$ *is called a distributive lattice if and only if the distributive laws hold; that is, for all* $a, b, c \in L$*, we have:*

$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ and

$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$.

Example 13.2.1. If A is any set, the lattice $[\mathcal{P}(A); \bigcup, \bigcap]$ is distributive.

Example 13.2.2. We now give an example of a lattice where the distributive laws do not hold. Let $L = \{1, 2, 3, 5, 30\}$. Then L is a poset under the relation divides. The operation tables for $\vee$ and $\wedge$ on L are:

$\vee$	1	2	3	5	30
1	1	2	3	5	30
2	2	2	30	30	30
3	3	30	3	30	30
5	5	30	30	5	30
30	30	30	30	30	30

$\wedge$	1	2	3	5	30
1	1	1	1	1	1
2	1	2	1	1	2
3	1	1	3	1	3
5	1	1	1	5	5
30	1	2	3	5	30

Since every pair of elements in L has both a join and a meet, $[L; \vee, \wedge]$ is a lattice (under divides). Is this lattice distributive? We note that:

$2 \vee (5 \wedge 3) = 2 \vee 1 = 2$ and

$(2 \vee 5) \wedge (2 \vee 3) = 30 \wedge 30 = 30$,

so that $a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c)$ for some values of $a, b, c \in L$. Hence L is not a distributive lattice.

It can be shown that a lattice is nondistributive if and only if it contains a sublattice isomorphic to one of the lattices in Figure 13.2.1.

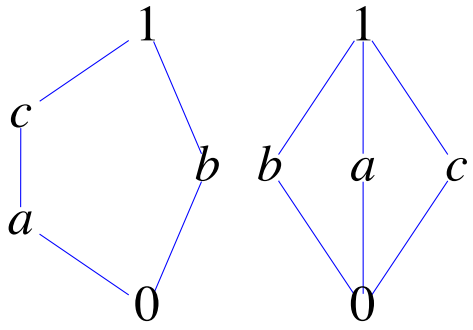


Figure 13.2.1
Nondistributive lattices

It is interesting to note that for the relation "divides" on $\mathbb{P}$, if $a, b \in \mathbb{P}$ we have:

$a \vee b = lcm(a, b)$, the least common multiple of a and b; that is, the smallest integer (in $\mathbb{P}$) that is divisible by both a and b;

$a \wedge b = gcd(a, b)$, the greatest common divisor of a and b; that is, the largest integer that divides both a and b.

EXERCISES FOR SECTION 13.2

A Exercises

1. Let L be the set of all propositions generated by p and q. What are the meet and join operations in this lattice. What are the maximum and minimum elements?

2. Which of the posets in Exercise 3 of Section 13.1 are lattices? Which of the lattices are distributive?

B Exercises

3. (a) State the commutative laws, associative laws, idempotent laws, and absorption laws for lattices.

   (b) Prove these laws.

4. Let $[L; \bigvee, \bigwedge]$ be a lattice based on a partial ordering $\leq$. Prove that if $a, b, c \in L$,

   (a) $a \bigvee b \geq a$.

   (b) $a \bigwedge b \leq a$.

   (c) $a \geq b$ and $a \geq c \Rightarrow a \geq b \bigvee c$.

13.3 Boolean Algebras

In order to define a Boolean algebra, we need the additional concept of complementation.

Definition: Complemented Lattice. *Let $[L; \bigvee, \bigwedge]$ be a lattice that contains a least element, 0, and a greatest element, 1. $[L; \bigvee, \bigwedge]$ is called a complemented lattice if and only if for every element $a \in L$, there exists an element $\overline{a}$ in L such that $a \wedge \overline{a} = 0$ and $a \vee \overline{a} = 1$. Such an element $\overline{a}$ is called a complement of the element a.*

Example 13.3.1. Let $L = \mathcal{P}(A)$, where $A = \{a, b, c\}$. Then $[L; \bigcup, \bigcap]$ is a bounded lattice with $0 = \emptyset$ and $1 = A$. Then, to find if it exists, the complement, $\overline{B}$, of, say $B = \{a, b\} \in L$, we want $\overline{B}$ such that

$$\{a, b\} \bigcap \overline{B} = \emptyset \text{ and } \{a, b\} \bigcup \overline{B} = A\,.$$

Here, $\overline{B} = \{c\}$, and since it can be shown that each element of L has a complement (see Exercise 1), $[L; \bigcup, \bigcap]$ is a complemented lattice. Note that if A is any set and $L = \mathcal{P}(A)$, then $[L; \bigcup, \bigcap]$ is a complemented lattice where the complement of $B \in L$ is $\overline{B} = B^c = A - B$.

In Example 13.3.1, we observe that the complement of each element of L is unique. Is this always the case? The answer is no. Consider the following.

Example 13.3.2. Let $L = \{1, 2, 3, 5, 30\}$ and consider the lattice $[L; \bigvee, \bigwedge]$ (under "divides"). The least element of L is 1 and the greatest element is 30. Let us compute the complement of the element $a = 2$. We want to determine $\overline{a}$ such that $2 \bigwedge \overline{a} = 1$ and $2 \bigvee \overline{a} = 30$. Certainly, $\overline{a} = 3$ works, but so does $\overline{a} = 5$, so the complement of $a = 2$ in this lattice is not unique. However, $[L; \bigvee, \bigwedge]$ is still a complemented lattice since each element does have at least one complement.

The following theorem gives us an insight into when uniqueness of complements occurs.

Theorem 13.3.1. *If $[L; \bigvee, \bigwedge]$ is a complemented and distributive lattice, then the complement $\overline{a}$ of any element $a \in L$ is unique.*

Proof: Let $a \in L$ and assume to the contrary that a has two complements, namely a_1 and a_2. Then by definition of complement,

$$a \wedge a_1 = 0 \text{ and } a \vee a_1 = 1,$$

Also,

$$a \wedge a_2 = 0 \text{ and } a \vee a_2 = 1.$$

So that

$$\begin{aligned} a_1 &= a_1 \bigwedge 1 = a_1 \wedge (a \vee a_2) \\ &= (a_1 \wedge a) \vee (a_1 \wedge a_2) \\ &= 0 \bigvee (a_1 \wedge a_2) \\ &= a_1 \wedge a_2. \end{aligned}$$

On the other hand,

$$\begin{aligned} a_2 &= a_2 \bigwedge 1 = a_2 \wedge (a \vee a_1) \\ &= (a_2 \wedge a) \vee (a_2 \wedge a_1) \\ &= 0 \bigvee (a_2 \wedge a_1) \\ &= a_2 \wedge a_1. \end{aligned}$$

Hence $a_1 = a_2$, which contradicts the assumption that a has two different complements, a_1 and a_2. ■

Definition: Boolean Algebra. *A Boolean algebra is a lattice that contains a least element and a greatest element and that is both complemented and distributive.*

Since the complement of each element in a Boolean algebra is unique (by Theorem 13.3.1), complementation is a valid unary operation over the set under discussion, and we will list it together with the other two operations to emphasize that we are discussing a set together with three operations. Also, to help emphasize the distinction between lattices and lattices that are Boolean algebras, we will use the letter B as the generic symbol for the set of a Boolean algebra; that is, $[B; -, \bigvee, \bigwedge]$ will stand for a general Boolean algebra.

Example 13.3.3. Let A be any set, and let $B = \mathcal{P}(A)$. Then $[B; c, \bigcup, \bigcap]$ is a Boolean algebra. Here, c stands for the complement of an element of B with respect to A, $A - B$.

This is a key example for us since all finite Boolean algebras and many infinite Boolean algebras look like this example for some A. In fact, a glance at the basic Boolean algebra laws in Table 13.3.1, in comparison with the set laws of Chapter 4 and the basic laws of logic of Chapter 3, indicates that all three systems behave the same; that is, they are isomorphic.

The "pairing" of the above laws reminds us of the principle of duality, which we state for a Boolean algebra.

Definition: Principle of Duality for Boolean Algebras. *Let* $[B; -, \vee, \wedge]$ *be a Boolean algebra (under* $\leq$*), and let S be a true statement for* $[B; -, \vee, \wedge]$. *If* S^* *is obtained from S by replacing* $\leq$ *by* $\geq$ *(this is equivalent to turning the graph upside down),* $\vee$ *by* $\wedge$, $\wedge$ *by* $\vee$, 0 *by* 1, *and* 1 *by* 0, *then* S^* *is also a true statement.*

TABLE 13.3.1

Basic Boolean Algebra Laws

Commutative Laws	
1. $a \vee b = b \vee a$	1.' $a \wedge b = b \wedge a$
Associative Laws	
2. $a \vee (b \vee c) = (a \vee b) \vee c$	2.' $a \wedge (b \wedge c) = (a \wedge b) \wedge c$
Distributive Laws	
3. $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$	3.' $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$
Identity Laws	
4. $a \vee 0 = 0 \vee a = a$	4.' $a \wedge 1 = 1 \wedge a = a$
Complement Laws	
5. $a \vee \overline{a} = 1$	5.' $a \wedge \overline{a} = 0$
Idempotent Laws	
6. $a \vee a = a$	6.' $a \wedge a = a$
Null Laws	
7. $a \vee 1 = 1$	7.' $a \wedge 0 = 0$
Absorption Laws	
8. $a \vee (a \wedge b) = a$	8.' $a \wedge (a \vee b) = a$
DeMorgan's Laws	
9. $\overline{a \vee b} = \overline{a} \wedge \overline{b}$	9.' $\overline{a \wedge b} = \overline{a} \vee \overline{b}$
Involution Law	
10. $\overline{\overline{a}} = a$	

Example 13.3.4. The laws 1' through 9' are the duals of the Laws 1 through 9 respectively. Law 10 is its own dual.

We close this section with some comments on notation. The notation for operations in a Boolean algebra is derived from the algebra of logic. However, other notations are used. These are summarized in the following chart;

Notation used in this text (Mathematics notation)	Set Notation	Logic Design (CS/EE notation)	Read as
$\vee$	$\cup$	$\oplus$	join
$\wedge$	$\cap$	$\otimes$	meet
$-$	c	$-$	complement
$\leq$	$\subseteq$	$\leq$	underlying partial ordering

Mathematicians most frequently use the notation of the text, and, on occasion, use set notation for Boolean algebras. Thinking in terms of sets may be easier for some people. Computer designers traditionally use the arithmetic and notation. In this latter notation, DeMorgan's Laws become:

$$(9)\quad \overline{a \oplus b} = \overline{a} \otimes \overline{b}$$

and

$$(9')\quad \overline{a \otimes b} = \overline{a} \oplus \overline{b}.$$

EXERCISES FOR SECTION 13.3

A Exercises

1. Determine the complement of each element $B \in L$ in Example 13.3.1. Is this lattice a Boolean algebra? Why?
2. (a) Determine the complement of each element of D_6 in $[D_6; \vee, \wedge]$.
   (b) Repeat part a using the lattice in Example 13.2.2.
   (c) Repeat part a using the lattice in Exercise 1 of Section 13.1.
   (d) Are the lattices in parts a, b, and c Boolean algebras? Why?
3. Determine which of the lattices of Exercise 3 of Section 13.1 are Boolean algebras.
4. Let $A = \{a, b\}$ and $B = \mathcal{P}(A)$.
   (a) Prove that $[B; c, \cup, \cap]$ is a Boolean algebra.
   (b) Write out the operation tables for the Boolean algebra.
5. It can be shown that the following statement, S, holds for any Boolean algebra $[B; -, \vee, \wedge]$: $(a \wedge b) = a$ if $a \leq b$.
   (a) Write the dual, S^*, of the statement S.
   (b) Write the statement S and its dual, S^*, in the language of sets.
   (c) Are the statements in part b true for all sets?
   (d) Write the statement S and its dual, S^*, in the language of logic.
   (e) Are the statements in part d true for all propositions?
6. State the dual of:
   (a) $a \vee (b \wedge a) = a$.
   (b) $a \vee (\overline{(\overline{b} \vee a)} \wedge b) = 1$.
   (c) $\overline{(a \wedge \overline{b})} \wedge b = a \vee b$.

   B Exercises
7. Formulate a definition for isomorphic Boolean algebras.

13.4 Atoms of a Boolean Algebra

In this section we will look more closely at previous claims that every finite Boolean algebra is isomorphic to an algebra of sets. We will show that every finite Boolean algebra has 2^n elements for some n with precisely n generators, called *atoms*.

Consider the Boolean algebra $[B; -, \vee, \wedge]$, whose graph is:

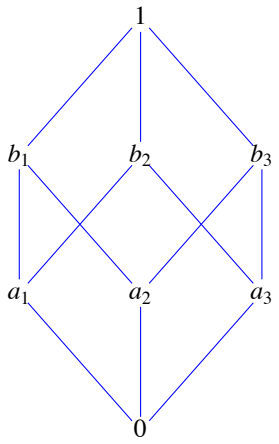


Figure 13.4.1
Illustration of the atom concept

We note that $1 = a_1 \vee a_2 \vee a_3$, $b_1 = a_1 \vee a_2$, $b_2 = a_1 \vee a_3$, and $b_3 = a_2 \vee a_3$; that is, each of the elements above level one can be described completely and uniquely in terms of the elements on level one. The a_i s have uniquely generated the nonzero elements of B much like a basis in linear algebra generates the elements in a vector space. We also note that the a_i s are the immediate successors of the minimum element, 0. In any Boolean algebra, the immediate successors of the minimum element are called *atoms*. Let A be any nonempty set. In the Boolean algebra $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$ (over $\subseteq$), the singleton sets are the generators, or atoms, of the algebraic structure since each element $\mathcal{P}(A)$ can be described completely and uniquely as the join or union of singleton sets.

Definition: Atom. *A nonzero element a in a Boolean algebra $[B;\ -,\ \vee,\ \wedge]$ is called an atom if for every $x \in B$, $x \wedge a = a$ or $x \wedge a = 0$.*

The condition that $x \wedge a = a$ tells us that x is a successor of a; that is, $a \leq x$, as depicted in Figure 13.4.2a.

The condition $x \wedge a = 0$ is true only when x and a are "not connected." This occurs when x is another atom or if x is a successor of atoms different from a, as depicted in Figure 13.4.2b.

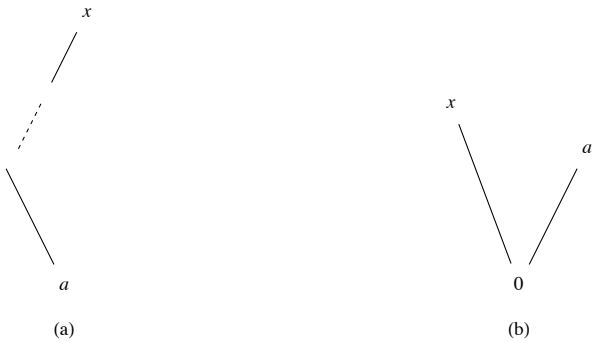


Figure 13.4.2

Example 13.4.1. The set of atoms of the Boolean algebra $[D_{30};\ -,\ \bigvee,\ \bigwedge]$ is $M = \{2,\ 3,\ 5\}$. To see that $a = 2$ is an atom, let x be any nonzero element of D_{30} and note that one of the two conditions $x \bigwedge 2 = 2$ or $x \bigwedge 2 = 1$ holds. Of course, to apply the definition to this Boolean algebra, we must remind ourselves that in this case the 0-element is 1, the operation $\wedge$ is *gcd*, and the poset relation $\leq$ is "divides." So if $x = 10$, we have $10 \bigwedge 2 = 2$ (or $2 \mid 10$), so Condition 1 holds. If $x = 15$, the first condition is not true. (Why?) However, Condition 2, $15 \bigwedge 2 = 1$, is true. The reader is encouraged to show that each of the elements 2, 3, and 5 satisfy the definition (see Exercise 13.4.1). Next, if we compute the join (*lcm* in this case) of all possible combinations of the atoms 2, 3, and 5, we will generate all nonzero elements of D_{30}. For example, $2 \bigvee 3 \bigvee 5 = 30$ and $2 \bigvee 5 = 10$. We state this concept formally in the following theorem, which we give without proof.

Theorem 13.4.1. *Let $[B;\ -,\ \vee,\ \wedge]$ be any finite Boolean algebra. Let $A = \{a_1,\ a_2,\ \ldots,\ a_n\}$ be the set of all n atoms of $[B;\ -,\ \vee,\ \wedge]$. Then every nonzero element in B can be expressed uniquely as the join of a subset of A.*

We now ask ourselves if we can be more definitive about the structure of different Boolean algebras of a given order. Certainly, the Boolean algebras $[D_{30};\ -,\ \bigvee,\ \bigwedge]$ and $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$ have the same graph (that of Figure 13.4.1), the same number of atoms, and, in all respects, look the same except for the names of the elements and the operations. In fact, when we apply corresponding operations to corresponding elements, we obtain corresponding results. We know from Chapter 11 that this means that the two structures are isomorphic as Boolean algebras. Furthermore, the graphs of these examples are exactly the same as that of Figure 13.4.1, which is an arbitrary Boolean algebra of

order $8 = 2^3$.

In these examples of a Boolean algebra of order 8, we note that each had 3 atoms and $2^3 = 8$ number of elements, and all were isomorphic to $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$, where $A = \{a,\ b,\ c\}$. This leads us to the following questions:

(1) Are there any other different (nonisomorphic) Boolean algebras of order 8?

(2) What is the relationship, if any, between finite Boolean algebras and their atoms?

(3) How many different (nonisomorphic) Boolean algebras are there of order 2? Order 3? Order 4? And so on.

The answers to these questions are given in the following theorem and corollaries. We include the proofs of the corollaries since they are instructive.

Theorem 13.4.2. *Let* $[B;\ -,\ \vee,\ \wedge]$ *be any finite Boolean algebra, and let A be the set of all atoms in this Boolean algebra. Then* $[B;\ -,\ \vee,\ \wedge]$ *is isomorphic to* $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$.

Corollary 13.4.1. *Every finite Boolean algebra* $[B;\ -,\ \vee,\ \wedge]$ *has* 2^n *elements for some positive integer n.*

Proof: Let A be the set of all atoms of B and let $|A| = n$. Then there are exactly 2^n elements (subsets) in $\mathcal{P}(A)$, and by Theorem 13.4.2, $[B;\ -,\ \bigvee,\ \bigwedge]$ is isomorphic to $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$. ■

Corollary 13.4.2. All Boolean algebras of order 2^n are isomorphic to each other. (The graph of the Boolean algebra of order 2^n is the n-cube).

Proof: By Theorem 13.4.2, every Boolean algebra of order 2^n is isomorphic to $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$ when $|A| = n$. Hence, they are all isomorphic to one another. ■

The above theorem and corollaries tell us that we can only have finite Boolean algebras of orders $2^1,\ 2^2,\ 2^3,\ \ldots,\ 2^n$, and that all finite Boolean algebras of any given order are isomorphic. These are powerful tools in determining the structure of finite Boolean algebras. In the next section, we will try to find the easiest way of describing a Boolean algebra of any given order.

EXERCISES FOR SECTION 13.4

A Exercises

1. (a) Show that $a = 2$ is an atom of the Boolean algebra $[D_{30};\ -,\ \bigvee,\ \bigwedge]$.

   (b) Repeat part a for the elements 3 and 5 of D_{30}.

   (c) Verify Theorem 13.4.1 for the Boolean algebra $[D_{30};\ -,\ \bigvee,\ \bigwedge]$.

2. Let $A = \{a,\ b,\ c\}$.

   (a) Rewrite the definition of atom for $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$. What does $a \leq x$ mean in this example?

   (b) Find all atoms of $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$.

   (c) Verify Theorem 13.4.1 for $[\mathcal{P}(A);\ c,\ \bigcup,\ \bigcap]$.

3. Verify Theorem 13.4.2 and its corollaries for the Boolean algebras in Exercises 1 and 2 of this section.

4. Give a description of all Boolean algebras of order 16. (*Hint*: Use Theorem 13.4.2.) Note that the graph of this Boolean algebra is given in Figure 9.4.5.

5. Corollary 13.4.1 states that there do not exist Boolean algebras of orders 3, 5, 6, 7, 9, etc. (orders different from 2^n). Prove that we cannot have a Boolean algebra of order 3. (*Hint*: Assume that $[B;\ -,\ \bigvee,\ \bigwedge]$ is a Boolean algebra of order 3 where $B = \{0,\ x,\ 1\}$ and show that this cannot happen by investigating the possibilities for its operation tables.)

6. (a) There are many different, yet isomorphic, Boolean algebras with two elements. Describe one such Boolean algebra that is derived from a power set, $\mathcal{P}(A)$, under $\subseteq$. Describe a second that is described from D_n, for some $n \in P$, under "divides."

   (b) Since the elements of a two-element Boolean algebra must be the greatest and least elements, 1 and 0, the tables for the operations on $\{0, 1\}$ are determined by the Boolean algebra laws. Write out the operation tables for $[\{0,\ 1\};\ -,\ \bigvee,\ \bigwedge]$.

B Exercises

7. Find a Boolean algebra with a countably infinite number of elements.

8. Prove that the direct product of two Boolean algebras is a Boolean algebra. (*Hint*: "Copy" the corresponding proof for groups in Section 11.6.)