Chapter 4 Boolean algebras and Propositional Logic

Section 4.1 Boolean algebras

Let $(A, \leq)$ be a lattice, let $x, y \varepsilon A$. We say that y is a *complement of* x if

$$x \vee y = \top , \quad x \wedge y = \bot .$$

The concept comes from the algebra of sets. If $(A, \leq) = (\mathcal{P}(B), \subseteq)$, the lattice of subsets of B , then to say that Y is a complement of X in the lattice-theoretic sense just introduced is the same as to say that Y is the complement of X in the simple sense: $Y = B - X$ (see Chapter 1, Section 1.2, p. 12: "laws for complements").

If y is a complement of x , then x is a complement of y : the definition essentially symmetric in x and y , since $y \vee x = x \vee y$ and $y \wedge x = x \wedge y$.

The complement is not necessarily unique. E.g., in both displayed lattices on p. 90 of Chapter 3, both x and z are complements of y . However,

in a distributive lattice, the complement is unique: if y *and* z *are both complements of the same element* x *, then* $y = z$.

Indeed,

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$$

by the distributive law. But

$$x \vee y = \top \quad \text{and} \quad x \wedge z = \bot$$

by the assumption on y and z . Substituting, we get

$$\top \wedge z = \bot \vee (y \wedge z) ,$$

that is, by $\bot \vee u = u$ (see p. 85, Chapter 3),

$$z = y \wedge z ,$$

which means (see the laws on p. 85, Chapter 3)

$$z \leq y .$$

The roles of z and y are completely symmetric; hence, by interchanging them in the above argument, we get

$$y \leq z .$$

Of course, we can now conclude that $z = y$, as promised.

The complement does not necessarily exist in a lattice even if the lattice is distributive. E.g., any *total* ordering with a maximal and a minimal element is a distributive lattice (*exercise*; show that, in this case, $x \wedge y = \mathtt{min}(x, y)$, where $\mathtt{min}(x, y) = x$ when $x \leq y$, and $\mathtt{min}(x, y) = y$ when $y \leq x$; and $x \vee y = \mathtt{max}(x, y)$, with $\mathtt{max}(x, y)$ defined similarly to $\mathtt{min}(x, y)$). However, if x is an element in such a total order which is not the maximal, nor the minimal, element, then x cannot have a complement; if y is any element, then $x \vee y = \mathtt{max}(x, y) = \top$ implies that $y = \top$, and $x \wedge y = \mathtt{min}(x, y) = \bot$ implies that $y = \bot$, thus $x \vee y = \top$ and $x \wedge y = \bot$ cannot hold at the same time.

A *Boolean algebra* is a distributive lattice in which every element has a complement. Since in a Boolean algebra, the distributice law holds, by what we saw above, the complement of any given element is uniquely determined; the complement of x is denoted by $-x$, or also by $\bar{x}$, or even $\neg x$.

A *complete Boolean algebra* is a complete lattice which is distributive, and in which every element has a complement; that is, a complete lattice which is a Boolean algebra at the same time.

Let us note that in any distributive lattice, the **dual** version of the **distributive law** also holds:

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)\ ;$$

here, we reversed the roles of the operations $\wedge$ and $\vee$ with respect to the original version of the distributive law. For the proof, we start by the right-hand side, apply the (first form of the) distributive law to it twice, and use the absorption laws at two places, until we arrive at the left-hand side:

$$(x\vee y) \wedge (x\vee z) = \overbrace{((x\vee y)\wedge x)}^{=\,x} \vee ((x\vee y)\wedge z) = x \vee ((x\wedge z)\vee(y\wedge z)) =$$
$$= \overbrace{x \ \vee\ (x\wedge z)}^{=\,x} \vee (y\wedge z) = x \vee (y\wedge z)$$

Since lattices can be described by operations and identities, without mentioning the ordering relation (namely, by saying that the items $\top, \perp, \wedge, \vee$ satisfy the associative, commutative, absorption, idempotent and identity laws), we can alternatively describe Boolean algebras by the lattice operations $\top, \perp, \wedge, \vee$, together with the operation of complementation, $-$, and require that these satisfy the lattice identities just mentioned, the distributive law (ensuring that the lattice is distributive), and the two **laws of complements**:

$$x \vee (-x) = \top\ , \quad x \wedge (-x) = \perp .$$

It turns out that this latter definition is slightly redundant. Alternatively, we have:

Boolean algebras may equivalently be defined by the following laws:

the **associative laws**:

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$
$$x \vee (y \vee z) = (x \vee y) \vee z$$

the **commutative laws**:

$$x \wedge y = y \wedge x$$

$$x \vee y = y \vee x$$

both **distributive law**s

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$
$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

the **identity laws:**

$$x \wedge \top = x , \qquad x \vee \bot = x .$$

the laws of complements:

$$x \vee (-x) = \top , \quad x \wedge (-x) = \bot .$$

The original definition, which says that a Boolean algebra is an *ordered set with certain properties*, namely:

the top and bottom elements exist;
the meet and join of any two elements exist;
the complement of any element exists;
the *first* distributive law ($x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$) holds;

is preferable, however.

The powerset-lattice $\mathcal{P}(B)$ is a complete Boolean algebra. We pointed out before that it is a complete distributive lattice; and above, we pointed out that any $X \varepsilon \mathcal{P}(B)$ has a complement, namely $-Y = B - Y$. Following this example, in any Boolean algebra, we denote the unique complement of x by $-x$.

By what we said about the symmetry in the relation " y is a complement of x " translates into the statement that

$$--x = x ,$$

the law of double negation.

In the case of the powerset-algebra $\mathcal{P}(B)$, in Section 1.2 we talked about the difference $X - Y$ of two sets $X, Y \varepsilon \mathcal{P}(B)$. It is clear that $X - Y = X \cap (-Y)$. Generalizing this operation, we define, in any Boolean algebra,

$$x - y \underset{\text{def}}{=} x \wedge (-y) \,;$$

$x - y$ is called the *difference* of x and y. One can easily verify that

$$x - y = x - (x \wedge y) \,,$$

and

$$(x - y) \vee (x \wedge y) = x \,, \quad (x - y) \wedge (x \wedge y) = \perp .$$

(*exercise*).

Note that, in the case of a powerset algebra, the last two equalities mean that x is the disjoint union of $x - y$ and $x \cap y$, which is an obvious fact. Another useful fact about the difference is this:

$$x \leq y \iff x - y = \perp .$$

Indeed, if $x \leq y$, then $x - y = x \wedge (-y) \leq y \wedge (-y) = \perp$, that is, $x - y = \perp$. On the other hand, if $x - y = \perp$, then $x \wedge (-y) = \perp$, hence,

$$x = x \wedge \top = x \wedge (y \vee -y) = (x \wedge y) \vee (x \wedge (-y)) = (x \wedge y) \vee \perp = x \wedge y \,;$$

which means that $x \leq y$.

Let us verify **De Morgan's laws**

$$-(x \wedge y) = (-x) \vee (-y) \,, \qquad -(x \vee y) = (-x) \wedge (-y)$$

in any Boolean algebra; these laws were stated in Section 1.2 for sets. To prove the first law, we show that the element $(-x) \vee (-y) = -x \vee -y$ is the complement of $x \wedge y$; that is,

$$(x \wedge y) \vee (-x \vee -y) = \top \tag{1}$$

and

$$(x \wedge y) \wedge (-x \vee -y) = \bot . \qquad (2)$$

Using distributivity in its dual form, we have

$$(x \wedge y) \vee (-x \vee -y) =$$

$$= (x \vee (-x \vee -y)) \wedge (y \vee (-x \vee -y))$$

$$= ((x \vee -x) \vee -y) \wedge ((y \vee -y) \vee -x)$$

(by associativity and commutativity)

$$= (\top \vee -y) \wedge (\top \vee -x)$$

$$= \top \wedge \top \qquad \text{(since } \top \vee \text{anything} = \top \text{)}$$

$$= \top \quad \text{(idempotence)} .$$

The proof of (2) is, essentially, the "dual" of that of (1): "interchange $\vee$ and $\wedge$". In fact, (2) is a *consequence* of (1), the latter applied in the "dual algebra". Let us explain the use of duality in some generality first.

Note that

if $(A, \leq)$ *is a Boolean algebra, then so its converse* $(A, \geq)$.

(the *converse* was mentioned in section 2.3; of course, $x \geq y$ means the same as $x \leq y$.) In fact, if $(A, \leq)$ is a lattice, then $(A, \geq)$ is also a lattice, in which the join operation is the same as the meet operation in $(A, \leq)$, the meet in $(A, \geq)$ is the join in $(A, \leq)$. Since $(A, \leq)$ is distributive, the dual distributive law holds in $(A, \leq)$, which means that the original law of distributivity holds in $(A, \geq)$ (and of course, as a consequence, also the dual law holds in $(A, \geq)$). In other words, $(A, \geq)$ is a distributive lattice. Finally, note that the top element of $(A, \geq)$ is the bottom element of $(A, \leq)$, and the bottom of $(A, \geq)$ is the top of $(A, \leq)$; therefore, if we take x and its complement $-x$ in $(A, \leq)$, the two equations defining complements *when read them in* $(A, \geq)$ become

$$x \wedge -x = \bot \ , \quad x \vee -x = \top$$

that is, $-x$ is again the complement of x in $(A, \geq)$.

We have shown that if $(A, \leq)$ is a Boolean algebra, then so is its converse $(A, \geq)$, and in fact, the top, bottom, meet, join and complement in the converse are the same as, respectively, the bottom, top, join, meet and complement in the original algebra. Thus, if we have shown some identity involving these operations to hold in any Boolean algebra, then the *dual identity*, obtained by changing top, bottom, meet, join to bottom, top, join and meet, respectively, and leaving complements alone, is again true in any Boolean algebra: the meaning of an equality in a Boolean algebra is the same as the meaning of its dual in the converse algebra.

Now, the dual of the identity (1) is

$$(x \vee y) \ \wedge \ (-x \wedge -y) \ = \ \top \ .$$

This is not quite the same as (2). However, since it is true for all values of the variables, we may replace x with $-x$, y with $-y$, and still have a true identity:

$$(-x \vee -y) \ \wedge \ (--x \wedge --y) \ = \ \top \ .$$

Since $--x = x$, $--y = y$, we get

$$(-x \vee -y) \ \wedge \ (x \wedge y) \ = \ \top \ ,$$

which is, up to commutativity, the same as (2).

We have shown the first De Morgan identity. The second one is the dual of the first one; therefore the second one holds as well.

Recall the notion of *isomorphism* from Chapter 2, Section 2.1. Recall that two isomorphic relations are "essentially the same" as far as "mathematically interesting" properties are concerned. For instance, it is easy to see that for two isomorphic relations, if one of them is a lattice, so is the other; if one of them is a Boolean algebra, so is the other.

We are going to show that

Theorem

every finite Boolean algebra is isomorphic to a powerset algebra $(\mathcal{P}(B), \subseteq)$;

Paraphrasing, we may say that, up to isomorphism, all *finite* Boolean algebras are represented as powerset algebras.

In yet other words, we may say that the notion of Boolean algebra completely captures the notion of subset and the operations of union and intersection on subsets, at least as far as *finite* sets are concerned.

It should be noted, however, that there are many *infinite* Boolean algebras, even complete ones, that are very different from powerset algebras.

Towards proving the theorem, let us define an *atom* in any Boolean algebra, or in any order for that matter, to be any element on the *second level* in the order. This means, in the case of a Boolean algebra, that an atom a is not the bottom element, but there is no x such that $\perp<x<a$. In other words, a is an atom iff $x\neq\perp$, and from $x\leq a$ it follows that either $x=\perp$, or $x=a$. An atom is "indivisible" (which is the original meaning of the word "atom"): it does not have any "proper part".

Recall the notion of *height* of an element introduced in Section 3.1 in any *finite* order. Assume that our Boolean algebra is finite. Then an atom is an element whose height is exactly 2 ; the unique element of height 1 is $\perp$.

Note that the atoms in $(\mathcal{P}(B), \subseteq)$ are exactly the singletons $\{u\}$, with $u\varepsilon B$. In other words, the elements of the set B are, in a sense, represented in the set-algebra $(\mathcal{P}(B), \subseteq)$, namely by the atoms of the algebra. We claim that *in any finite Boolean algebra* $(A, \leq)$, *every element is the join of the atoms below it*:

$$x = \bigvee \{a \varepsilon A \mid a \leq x \;\&\; a \text{ is an atom}\} . \tag{3}$$

Certainly, since A is a finite set, the join is the join of a finite set, therefore, it exists. To prove the equality, let us denote the join on the right-hand side by y . Since y is the join of some elements each of which is $\leq x$, we have that $y \leq x$. Now, consider the element

$$z = x - y .$$

What we want is that $z = \bot$; indeed, if $z = x - y = \bot$, then $x \leq y$; and since $y \leq x$ is true, the desired equality $x=y$ follows.

Now, assume that $z \neq \bot$, to derive a contradiction. In that case, the height, in the sense of Section 3.1, of z is at least 2 . But then, as we noted in Section 3.1, there is at least one element b of height exactly 2 which is under z ; in other words, there is an atom b such that $b \leq z$. Before proceeding, let us mark down this last, frequently used, conclusion:

In a finite Boolean algebra, every non-bottom element has at least one atom below it.

Now, since $b \leq z$, we have that

$$b \wedge y \leq z \wedge y = \bot ,$$

that is,

$$b \wedge y = \bot .$$

If n is the number of atoms that are $\leq x$, and a_i for $i < n$ are all the distinct atoms $\leq x$, then

$$y = a_0 \vee a_1 \vee \ldots \vee a_{n-1} ,$$

and so

$$\bot = b \wedge y = b \wedge (a_0 \vee a_1 \vee \ldots \vee a_{n-1}) =$$

$$= (b \wedge a_0) \vee (b \wedge a_1) \vee \ldots (b \wedge a_{n-1}) ;$$

thus, $b \wedge a_i \leq \perp$, and $b \wedge a_i = \perp$ for all $i<n$. But this means that

the atom b is different from each of the atoms a_i ;

if we had $b=a_i$, then $b \wedge a_i = b \neq \perp$. On the other hand, since $z \leq x$ and $b \leq z$, we have that $b \leq x$ and b is an atom; by the definition of the a_i's as all the atoms below x says that

the atom b is equal to a_i for some $i<n$.

The last two displayed sentences contradict each other. We have shown that $z \neq \perp$ leads to a contradiction; therefore, we have $z = \perp$, and thus $y=x$ as desired.

Let us point out another fact concerning atoms. In any Boolean algebra,

any two distinct atoms are disjoint, and any two disjoint atom are distinct:
if a, b *are atoms, then*

$$a \neq b \iff a \wedge b = \perp . ;$$

This is almost obvious. Suppose first that $a \neq b$. Since a is an atom, and $a \wedge b \leq a$, the only possibilities for $a \wedge b$ are $a \wedge b = \perp$ and $a \wedge b = a$. But the latter means that $a \leq b$; since $a \neq \perp$, and b is an atom, this means $a = b$, which we assumed was not the case. So, $a \wedge b = \perp$ must be the case. Conversely, assume $a \wedge b = \perp$. Since $a \neq \perp$, $a=b$ would mean $a \wedge b = a \neq \perp$. Thus, $a \neq b$.

Note that, in the case of the complete powerset-algebra $(\mathcal{P}(B), \subseteq)$, the atom $\{u\}$ is $\leq$ the set $X \in \mathcal{P}(B)$ just in case $u \varepsilon X$; thus, the atoms that are $\leq X$ correspond exactly to the elements of X. The equality (3) says, in this case, that any set X is the union of all singletons $\{u\}$ with $u \varepsilon X$, an obvious fact.

Let now $(A, \leq)$ be any finite Boolean algebra, let B the set of all atoms of $(A, \leq)$. We define two mappings

$$A \underset{g}{\overset{f}{\rightleftarrows}} \mathcal{P}(B)$$

as follows:

$$x \overset{f}{\longmapsto} \{a\varepsilon A \mid a\leq x \ \& \ a \text{ is an atom}\}$$

and

$$\bigvee X \underset{g}{\longleftarrow\!\!\!\shortmid} X \quad .$$

In words: with any element x of the given Boolean algebra, f associates the set of atoms below x; with any set X of atoms, g associates the join of X.

We claim that the mappings f is an *isomorphism* of orderings, with g its inverse (which then becomes an isomorphism itself):

$$(A,\leq) \underset{g}{\overset{f}{\rightleftarrows}} (\mathcal{P}(B),\subseteq) \ ;$$

$$g\circ f = 1_A \ , \quad f\circ g = 1_B \ . \tag{4?}$$

Recall what we have to show, besides (4), for our claim; see (1) on page 37 in Section 2.1. We have to have

$$x \leq y \quad \Longleftrightarrow \quad f(x) \subseteq f(y) \tag{4'?}$$

The most difficult part is (4?); we will grant this for the moment, and prove the rest; in this we will use (4); finally, we will prove (4).

First, we show

$$x \le y \implies f(x) \subseteq f(y) \tag{4.1?}$$

and

$$X \subseteq Y \implies g(X) \le g(Y) \tag{4.2?}$$

for all $x, y \in A$ and $X, Y \in \mathcal{P}(B)$.

If $x \le y$, and $a \le x$, then clearly, $a \le y$. This implies directly that the implication (4.1) holds. (4.2) is the same as to say that

$$X \subseteq Y \implies \bigvee X \le \bigvee Y$$

which is clear (why?). To see (4'), the left-to-right implication in (4') is (4.1); for the other implication:

$$f(x) \subseteq f(y) \underset{\substack{\uparrow \\ (4.2)}}{\implies} g(f(x)) \le g(f(y)) \underset{\substack{\uparrow \\ (4)}}{\implies} x \le y \, .$$

Now, for (4). The first equality under (4) is exactly the assertion under (3) (why?). Finally, let us show that $f \circ g = 1_B$. This means that for any set X of atoms, if $x = \bigvee X$, then

$$\{a \varepsilon A \mid a \le x \ \& \ a \text{ is an atom}\} = X \, .$$

Now, clearly, the right-hand side is contained in the left-hand side (why?). Conversely, to show that the left-hand side is contained in the right-hand side, let a be an atom such that $a \le x$, to show that $a \varepsilon X$. Since $x = \bigvee X$, we have $a \le \bigvee X$, that is $a \wedge \bigvee X = a$. Let $X = \{b_i \mid i < n\}$. We have

$$a = a \wedge (b_0 \vee b_1 \vee \ldots \vee b_{n-1}) = (a \wedge b_0) \vee (a \wedge b_1) \vee \ldots \vee (a \wedge b_{n-1}) \, . \tag{5}$$

In particular, each $a \wedge b_i \le a$. Since a is an atom, either $a \wedge b_i = \bot$ or $a \wedge b_i = a$. It cannot be that for all i , $a \wedge b_i = \bot$, since then the union on the right-hand side of (5) would be $\bot$, and $a \ne \bot$. Therefore, for at least one i , $a \wedge b_i = a$. But then $a \le b_i$, and thus, since b_i is an atom, and $a \ne \bot$, we must have $a = b_i$. This means that a is an element of X , which was our goal to show.

This completes the proof of the **Theorem**.

One consequence of the theorem is that a finite Boolean algebra $(A, \leq)$ must have a cardinality which is a power of 2 ;

$$|A| = 2^n \text{ for some } n \in \mathbb{N} ;$$

in fact,

if the cardinality of the set of atoms of a Boolean algebra A is n , *then* $|A| = 2^n$.

This is clear, since two isomorphic algebras have underlying sets of the same cardinality, and $|\mathcal{P}(B)| = 2^{|B|}$.

Thus, we have Boolean algebras of cardinalities $1 = 2^0$ (the degenerate Boolean algebra, the power-set of the empty set; $\mathcal{P}(\emptyset) = \{\emptyset\}$), $2 = 2^1$, $4 = 2^2$, $8 = 2^3$, $16 = 2^4$, ..., but none of powers in between.