§14 The Boole/Stone algebra of sets

14.1. Lattices and Boolean algebras.

Given a set A , the subsets of A admit the following simple and familiar operations on them: $\cap$ (*intersection*), $\cup$ (*union*) and $-$ (*complementation*). If $X, Y \subset A$, then $X \cap Y$, $X \cup Y$ are also subsets of A . With A fixed (and suppressed in the notation), we write $-X = A - X$ for any $X \subset A$; of course, $-X \subset A$ again. Intersection and union are binary operations on $\mathcal{P}(A)$, $-$ is a unary operation on $\mathcal{P}(A)$:

$$\cap : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A) ,$$

$$\cup : \mathcal{P}(A) \times \mathcal{P}(A) \longrightarrow \mathcal{P}(A) ,$$

$$- : \mathcal{P}(A) \longrightarrow \mathcal{P}(A) .$$

Of course, intersection and union are defined for any number of arguments; using the binary versions repeatedly, we can reproduce finite intersections and union, *except* the empty intersection and the empty union. For the empty intersection, we take the set A itself; for the empty union, the empty set.

What is the justification? For any family $\mathcal{F} \subset \mathcal{P}(A)$ of subsets of A , we have

$$\bigcap \mathcal{F} = \{x \in A : \text{for all } X \in \mathcal{F} , x \in X\}$$

and

$$\bigcup \mathcal{F} = \{x \in A : \text{for some } X \in \mathcal{F} , \ x \in X\} .$$

Note that the expression for $\bigcap \mathcal{F}$ is the same as that in Section 3, page 35 except for the clause " $\in A$ " ; the expression for $\bigcup \mathcal{F}$ has a similar difference to the earlier expression on p. 30.

For the union, there is no actual difference in meaning; the old and the new expressions give the same set. For the intersection, the same is true except for the empty family $\mathcal{F}$; the old expression gives $\mathbf{V}$, a non-set; the new expression gives A itself. Of course, the union of the empty family, according to the general formula, is the empty set. It goes without saying that $X\cap Y = \bigcap \{X, Y\}$, $X\cup Y = \bigcup \{X, Y\}$.

The composite object

$$(\mathcal{P}(A); \cap, \cup, -, A, 0) \tag{1}$$

is an example of what we call an *algebra*: a set (in this case $\mathcal{P}(A)$), called the *underlying set of* the algebra, with certain particular *operations* on it (in this case, the binary operations $\cap$, $\cup$, the unary operation $-$, and the 0-*ary operations* A , 0 : 0-ary operations are distinguished elements of the underlying set). *Any* object of the form

$$(B ; \wedge , \vee , \neg , 1 , 0)$$

with B a set, $\wedge$, $\vee$ both $B\times B\longrightarrow B$, $\neg : B\longrightarrow B$, and $1, 0 \in B$, is an algebra *similar* to (1). Speaking in very general terms, we will seek, and at least partly find, properties of algebras of the form (1) that distinguish them among all the algebras similar to them; the result will be the notion of *Boolean algebra*.

For future reference, let's say that when we denote an algebra by a single letter, say B , $|B|$ denotes the underlying set of B . This, of course, conflicts with the notation for "cardinality"; it is advisable to use $\#A$ for the cardinality of the set A when the underlying set of an algebra is also to be used.

Let us first look at the basic operations from another point of view, namely the context of the *poset* $(\mathcal{P}(A), \subset)$. We have, for any $\mathcal{F} \subset \mathcal{P}(A)$, that

$\bigcap \mathcal{F}$ is the *largest* subset Y of A for which $Y \subset X$ for all $X \in \mathcal{F}$:

$\bigcap \mathcal{F} \subset X$ for all $X \in \mathcal{F}$, and

if $Y \subset X$ for all $X \in \mathcal{F}$, then $Y \subset \bigcap \mathcal{F}$;

and similarly,

$\bigcup \mathcal{F}$ is the *least* subset Y of A for which $X \subset Y$ for all $X \in \mathcal{F}$:

$X \subset \bigcup \mathcal{F}$ for all $X \in \mathcal{F}$, and

if $X \subset Y$ for all $X \in \mathcal{F}$, then $\bigcup \mathcal{F} \subset Y$.

(**verify** this statement).

In general, in any poset $(B, \leq)$, and for any family $\mathcal{F} \subset B$ of elements of B, a *lower bound of* $\mathcal{F}$ is any $y \in B$ such that $y \leq x$ for all $x \in \mathcal{F}$; the *greatest lower bound* (g.l.b), or *infimum* (inf) of $\mathcal{F}$ (if it exists!) is the *maximum* element of the set L of all lower bounds of $\mathcal{F}$: $y_0 \in L$ such that $y \leq y_0$ for all $y \in L$. (Note that the requirement is more than to say that y_0 be a *maximal* element of L !). The g.l.b. of $\mathcal{F}$ is denoted by $\bigwedge \mathcal{F}$; $\bigwedge \mathcal{F}$ does not necessarily exist (in an arbitrary poset $(B, \leq)$), but if it does, it is uniquely determined by the definition. The notions of *upper bound, least upper bound (l.u.b., supremum, sup*), with the notation $\bigvee \mathcal{F}$, are defined similarly ("dually"). [In the context of ordinals and well-orderings, we have already used lub's extensively.]

Now, notice that what we said above about intersections and unions amounts to this that in the poset $(\mathcal{P}(A), \subset)$, $\bigwedge \mathcal{F}$, $\bigvee \mathcal{F}$ exist for all $\mathcal{F} \subset \mathcal{P}(A)$, and in fact $\bigvee \mathcal{F} = \bigcap \mathcal{F}$, $\bigwedge \mathcal{F} = \bigcup \mathcal{F}$.

It is worth remarking that the definitions of inf (sup) can be put in the following form:

$$y \leq \bigwedge \mathcal{F} \iff y \leq x \text{ for all } x \in \mathcal{F};$$

$$\bigvee \mathcal{F} \leq y \iff x \leq y \text{ for all } x \in \mathcal{F};$$

y ranges over all the elements of the poset.

Note also that $\bigwedge \varnothing$ is the maximum element of the poset (if such exists); $\bigvee \varnothing$ is the minimum element (if exists). We write 1 for the maximum element, 0 for the minimum element (if they exist).

A poset $(B, \leq)$ is called a *lattice* if $\bigwedge \mathcal{F}$, $\bigvee \mathcal{F}$ exist for all *finite* sets $\mathcal{F} \subset B$. Thus, in a lattice $(B, \leq)$, there always are a maximum element 1, a minimum element 0; moreover, for any $x, y \in B$, $x \wedge y \underset{\text{def}}{=} \bigwedge \{x, y\}$, $x \vee y \underset{\text{def}}{=} \bigvee \{x, y\}$ always exist. The poset $(\mathcal{P}(A), \subset)$ is a lattice; in fact, it is what is called a *complete lattice*, meaning that $\bigwedge \mathcal{F}$, $\bigvee \mathcal{F}$ exist for all $\mathcal{F} \subset B = \mathcal{P}(A)$.

Note the following laws that always hold in any lattice:

$$x \wedge y = y \wedge x \ , \quad x \vee y = y \vee x \quad \text{(commutative laws)}$$

$$(x \wedge y) \wedge z = x \wedge (y \wedge z) \ , \quad (x \vee y) \vee z = x \vee (y \vee z)$$
(associative laws)

$$x \wedge x = x \ , \quad x \vee x = x \quad \text{(idempotent laws)}$$

$$x \wedge (x \vee y) = x \ , \quad x \vee (x \wedge y) = x \quad \text{(absorption laws)}$$

$$x \wedge 1 = x \, , \quad x \vee 1 = 1 \, , \quad x \wedge 0 = 0 \, , \quad x \vee 0 = x \, .$$

Exercises. (i) Verify that the above hold in any lattice.

(ii) Assume an algebra $(B, \wedge, \vee, 1, 0)$ satisfying the above laws. Show that there is a unique partial ordering $\leq$ on B that makes $(B, \leq)$ a lattice in such a way that the given $\wedge$, $\vee$, 1, 0 become the lattice operations.

(iii) Suppose that in a poset, $\bigwedge \mathcal{F}$ exists for all sets of elements of the poset. Show that then also $\bigvee \mathcal{F}$ always exists. Show that if, in this assertion, we restrict $\mathcal{F}$ to be a finite set in both occurrences, then the resulting statement is not always true any more.

Exercises (i) and (ii) say that the concept of lattice can be given a purely "operational" ("algebraic") formulation.

The set-theoretic complement $-X = A - X$ also can be given a "lattice" description. The set $Y = -X$ is distinguished among all the subsets of A by the following two properties:

$$Y \cup X = A \text{ and } Y \cap X = 0 \, ,$$

(**verify!**). In a lattice, y is *a complement* of x if $y \vee x = 1$ and $y \wedge x = 0$. In a general lattice, the complement of an element may not exist, and it is also possible that there are two different complements of the same element.

A particular property of $(\mathcal{P}(A), \subset)$ as a lattice is that it is *distributive*. A lattice $(B, \leq)$ is distributive if

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

for all $x, y, z \in B$.

Indeed, the distributive law is familiar for $(\mathcal{P}(A), \subset)$ (see Assignment 1).

Exercises. (iv) Show that in a distributive lattice, the dual of the distributive law, that is

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

holds too.

(v) Show that in a distributive lattice, every element has at most one complement.

(vi) Show that any linear ordering with a minimal and a maximal element is a distributive lattice.

A *Boolean algebra* is a distributive lattice in which every element has a complement. Of course, $(\mathcal{P}(A), \subset)$ is a Boolean algebra.

One particular Boolean algebra, $(\mathcal{P}(1), \subset)$, plays a central role in our theory. This one has two elements: 0 and 1 (right?) ; note that $\mathcal{P}(1) = 2$. The binary Boolean operations are tabulated as follows:

$\wedge$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

In addition, we have $\neg(1) = 0$, $\neg(0) = 1$. We call this algebra the *two-element Boolean algebra*, and denote it by 2 .

Let us point out that 2 is also considered to be the *algebra of truth values* **t**=**true** and

$\mathbf{f}=\mathbf{false}$; $\mathbf{t}$ is identified with 1 , $\mathbf{f}$ with 0 . Under this identification, the above operations $\wedge$, $\vee$ and $\neg$ become the logical operations of *conjunction* ("and"), *disjunction* ("or"), and *negation* ("not").

With any poset $B=(|B|,\leq)$, we have its *opposite*, B^{o} . The underlying set of B^{o} is the same, $|B|$, as of B ; the ordering in B^{o} is the *opposite* of that in B : $x\leq_{B^{\mathrm{o}}}y \underset{\mathrm{def}}{\iff} y\leq x$. It is clear that B^{o} so defined is a poset too. Moreover, it is also clear that the inf of a set $\mathcal{F}$ in the sense of B^{o} is the same as the sup of $\mathcal{F}$ in the sense of B , and *vice versa*. Thus, of B is a lattice, so is B^{o} . Moreover, as exercise (iv) above shows, if B is a distributive lattice, then B^{o} is distributive too. Also, the definition of complement shows that the notions of complement in B and B^{o} are the same. Briefly put, the notion of "lattice", "distributive lattice", and "Boolean algebra" are each self-dual concepts: if a poset falls in any of these categories, so does its opposite.

14.2. Some algebraic ideas.

Note that the notion of Boolean algebra is defined in terms of the operations $\wedge$, $\vee$, $\neg$, 1 and 0 by *identities* : the laws describing lattices, the distributive law, and the laws defining the complement. In general, an identity, for any kind of algebra, is an equality of two *terms* built up of the basic operations of the algebra, required to hold for all values of the variables involved. In the definition of Boolean algebra, we have found some *particular* identities that hold in the set-algebra $(\mathcal{P}(A),\wedge,\vee,\neg,1,0)$; *have we found them all*?

As it is, this question is not very intelligent since, e.g., $1\wedge x=x$ is an identity not listed above that obviously holds in the set-algebra, and in fact, in all lattices, as a consequence of two of the axioms (why?). However, we may ask:

(*) is it the case that all identities that hold in the set-algebras are *consequences* of the Boolean axioms, that is, are true in *all* Boolean algebras?

Put this way, the question amounts to asking whether we have found, in the Boolean axioms, a sufficient basis to deduce all identities formulated in terms $\cap$, $\cup$, $-$, 1, 0 that are true for sets; if the answer is "no", then there is another, still undiscovered, *essentially new* identity concerning these set-operations.

We will give an affirmative answer to the question just asked, by deducing it from a more abstract theorem to be stated soon.

Example. The so-called De-Morgan law: $\neg(x\wedge y) = (\neg x)\vee(\neg y)$ holds in set-algebras; in fact, it holds, in all Boolean algebras (**exercise** (vii)).

A *homomorphism* of lattices L and M, in notation $f:L\longrightarrow M$, is a mapping $f:|L|\longrightarrow|M|$ between the underlying sets that *preserves* the lattice operations:

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

$$f(x\vee y) = f(x)\vee f(y) ,$$

$$f(1) = 1 ,$$

$$f(0) = 0 .$$

These equalities are required to hold for all $x, y\in |L|$; of course, on the left sides, $\wedge$, $\vee$, 1, 0 refer to the lattice operations of L, on the right to those of M.

An *embedding* of lattices is a 1-1 homomorphism; an *isomorphism* is a bijective homomorphism.

Exercises. (viii) A lattice homomorphism f between Boolean algebras is a *Boolean homomorphism* in the sense that it also preserves complements: $f(\neg x) = \neg f(x)$.

(ix) Find a Boolean *embedding* of $(\mathcal{P}(2), \leq)$ into $(\mathcal{P}(3), \leq)$.

(x) Any lattice homomorphism preserves the partial ordering relation: $x \le y \;\Rightarrow\; fx \le fy$. If L, M are lattices, and f is a poset isomorphism $f:(|L|, \le) \longrightarrow (|M|, \le)$ (i.e., f is a bijection $f: |L| \xrightarrow{\cong} |M|$, and $x \le y \iff fx \le fy$ $(x, y \in |L|)$), then f is a lattice isomorphism as well. However, a poset-homomorphism between lattices (map preserving the order) is not necessarily a lattice homomorphism.

There are the following points to be made about homomorphisms and embeddings:

(1) given a (Boolean) homomorphism $f:B \longrightarrow C$, and a Boolean term $t(\vec{x})$ built up of variables and the symbols for the Boolean operations, then for any values $\vec{b}$ from B for the variables $\vec{x}$ we have

$$f(t^B(\vec{b})) = t^C(f\vec{b}) \;;$$

that is, if we first evaluate t at $\vec{b}$ in B, then apply f, we obtain the same value as when we first apply f to each of the values in $\vec{b}$, and then evaluate t in C at those arguments;

and

(2) if an *identity* $s(\vec{x}) = t(\vec{x})$ holds in C (for all values in $|C|$), and $f:B \longrightarrow C$ is an *embedding*, then the same identity also holds in B.

(1) is a consequence of the definition of "homomorphism"; note that the "homomorphism" is defined in such a way that the assertion hold in case t is a simple term (has just one operation mentioned in it); the general statement is proved by "induction". (2) is a consequence of (1) as follows. Suppose $s(\vec{x}) = t(\vec{x})$ holds in C, and $f:B \longrightarrow C$ is an embedding. To show that the same identity holds in B, let $\vec{b}$ be arbitrary elements to evaluate the variables $\vec{x}$. Then

$$f(s^B(\vec{b})) = s^C(f\vec{b})$$

and

$$f(t^B(\vec{b})) = t^C(f\vec{b}) .$$

Since we have $s^C(f\vec{b}) = t^C(f\vec{b})$ by the assumption that the identity holds in C, we get that $f(s^B(\vec{b})) = f(t^B(\vec{b}))$. Since f is 1-1, it follows that $s^B(\vec{b}) = t^B(\vec{b})$ as desired.

Put briefly, (2) says that *any identity that holds in an algebra holds in any other that can be embedded into the given one*.

Exercise. (xi) Suppose the lattice L can be embedded into a distributive lattice. Then L itself is distributive.

Given a family $\langle L_i \rangle_{i \in I}$ of posets, their *Cartesian product*, $\prod_{i \in I} L_i$, is the poset L whose underlying set is $|L| = \times_{i \in I} |L_i|$, and for which

$$f \leq g \iff f(i) \leq g(i) \text{ for all } i \in I .$$

Here, f and g are arbitrary elements of $\times_{i \in I} |L_i|$ (remember that the latter is the set of certain functions with domain I); on the left side, $\leq$ is the ordering of $\prod_{i \in I} L_i$ to be defined; on the right, $\leq$ refers to the ordering given in (each) L_i.

Exercise. (xii) Verify that $\prod_{i \in I} L_i$ is indeed a poset; if each L_i is a lattice, then so is $\prod_{i \in I} L_i$; if each L_i is a distributive lattice, or a Boolean algebra, then so is $\prod_{i \in I} L_i$. In fact, the lattice (Boolean) operations on $\prod_{i \in I} L_i$ are defined *pointwise*: e.g., $(f \wedge g)(i) = f(i) \wedge g(i)$.

(xiii) The *projection mapping*

$$\pi_j \ : \ \prod_{i\in I} L_i \longrightarrow L_j$$
$$f \longmapsto f(j)$$

one for each $j \in I$, is a lattice homomorphism.

(xiv) Turning to Cartesian products of sets, let us note the following "mapping property" of Cartesian products: for any sets A_i for $i \in I$, and any further set B:

the maps $f:B \longrightarrow \times_{i\in I} A_i$ are in a one-to-one correspondence with families of the form $\langle f_i:B \longrightarrow A_i \rangle_{i\in I}$. Indeed, the correspondence, in one direction, associates with f the family where $f_i = \pi_i \circ f$ (with π_i defined as in (xiii)).

(xv) Now, if the A_i and B are lattices (say), then the correspondence of (iii) gives a one-to-one correspondence between homomorphisms $f:B \longrightarrow \prod_{i\in I} A_i$ and families of homomorphisms of the form $\langle f_i:B \longrightarrow A_i \rangle_{i\in I}$. Put in another way, to give a homomorphism $f:B \longrightarrow \prod_{i\in I} A_i$ is the same as to give a family of homomorphisms $\langle f_i:B \longrightarrow A_i \rangle_{i\in I}$.

When in the product $\prod_{i\in I} A_i$ all the algebras A_i are the same, say A, we write A^I for the product $\prod_{i\in I} A$; A^I is a *power* (the I^{th} *power*) of A. Note that the underlying set of the algebra A^I, $|A^I|$, is the same as ${}^I|A|$, where in the latter the notation of Section 3, p.36 is used.

The reason why we talk about products of algebras is because the power-set algebras $(\mathcal{P}(A), \subset)$ are all, essentially, powers of 2, the two-element algebra, and this turns out to be a useful way of looking at power-set algebras. Recall the bijection

$$\begin{array}{ccc} \mathcal{P}(A) & \xrightarrow{\cong} & {}^{A}2 \\ X & \longmapsto & \mathrm{char}\, X . \end{array} \qquad (1)$$

Now, $\mathcal{P}(A)$ and ${}^{A}2$ are the respective underlying sets of the algebras $(\mathcal{P}(A), \subset)$ and 2^{A}. We have that

the mapping in (1) is an isomorphism $(\mathcal{P}(A), \subset) \xrightarrow{\cong} 2^{A}$.

Exercise (xvi): verify this important fact.

Combining the last fact with what we learned above about mappings into a product-algebra, we obtain

for any lattice L, and any set A, the lattice homomorphisms $f: L \longrightarrow (\mathcal{P}(A), \subset)$ are in a one-to-one correspondence with families of homomorphisms of the form $\langle f_a : L \longrightarrow 2 \rangle_{a \in A}$.

Moreover, in this correspondence,

f is an embedding (1-1) if and only if, for every pair (x, y) of distinct elements $x \neq y$ of L, there is $a \in A$ such that $f_a(x) \neq f_a(y)$.

Exercise (xvii)**.** Verify the last two displayed assertions.

Stone representation theorem for distributive lattices (and Boolean algebras).

Any distributive lattice (hence, any Boolean algebra) has an embedding into a power-set algebra.

Equivalently, if L a distributive lattice, and $x \neq y$ are arbitrary elements of L, then there is a 2-valued homomorphism $f: L \longrightarrow 2$ such that $f(x) \neq f(y)$.

The proof of the Stone representation theorem is the subject of the next subsection.

Exercise (xviii)**.** Verify that the two version of the theorem are indeed equivalent. Note that the distributivity condition on the lattice is *necessary*. Note that the question asked under (*) (at the beginning of the present subsection 14.2) has, as a consequence of the Stone representation theorem, an affirmative answer.

14.3. Prime filters and ultrafilters

We now set out to prove the Stone representation theorem. First, we investigate the notion of a 2-valued lattice homomorphism $f:L\longrightarrow 2$. Any such f is given by the set $F=\{x\in L : f(x)=1\}$; namely, f is then the characteristic function of X , $f=\mathrm{char}\,F : |L|\longrightarrow 2$. The question is what properties F must have in order for $\mathrm{char}\,F$ to be a lattice homomorphism. We introduce some standard terminology.

Let L be a lattice. $F\subset |L|$ is a *filter on* L if (i)$_{\mathrm{F}}$ $1_L\in F$, (ii)$_{\mathrm{F}}$ F is closed upward: $x\in F$, $x\le y \Rightarrow y\in F$ $(x, y\in |L|)$ [as a consequence, in (i)$_{\mathrm{F}}$, it would have been enough to require that F be non-empty], and (iii)$_{\mathrm{F}}$ if x and y both belong to F , then so does $x\wedge y$ $(x, y\in |L|)$.

Exercise (xix)**.** Verify that $F\subset |L|$ is a filter iff $\mathrm{char}\,F$ is an order-preserving map $L\longrightarrow 2$, and it also preserves $\wedge$ and 1 [for this, we say that f is a *meet-semilattice homomorphism*].

A filter F on L is *prime* if (iv)$_{\mathrm{PF}}$ $0_L\notin F$ [equivalently, $F\ne |L|$; we say that F is a *proper* filter] and (v)$_{\mathrm{PF}}$ whenever $x\vee y\in F$, then either $x\in F$, or $y\in F$ $(x, y\in |L|)$.

Exercises. (xx) The prime filters on a lattice L are in a one-to-one correspondence with the homomorphisms $L\longrightarrow 2$.

(xxi) Let F be a filter on the Boolean algebra B . Then F is a prime filter on B iff for any $x\in |B|$, exactly one of x , $\neg x$ belongs to F .

In the case of a Boolean algebra, we may say "*ultrafilter*" to mean "prime filter".

In view of the reformulation of the notion of *2*-valued homomorphism as prime filter, and in view of second form of the Stone representation theorem (at the end of the second section), we now see that the Stone representation theorem is equivalent to the following statement:

For any distributive lattice L *, and any pair of distinct elements* $x\neq y$ *of* $|L|$ *, there is a prime filter* P *of* L *for which one of* x, y *belongs to* P *, and the other of* x, y *does not belong to* P *.*

We are going to show a stronger statement, which is also more specific concerning which of the two given elements can be made to belong, and which not to belong, to the prime filter. The stronger version can then be used to obtain other interesting consequences. The main feature of the stronger version is a certain symmetry with respect to "dualizing", that is, taking the opposite of the lattice in question.

Consider a lattice L . An *ideal* of L is, by definition, the same thing as a filter in L^{o} . Unraveling this, we obtain that an ideal is a subset I of $|L|$ such that (i)$_I$ $0_L\in I$, (ii)$_I$ I is closed downward: $x\in I$, $y\leq x \implies y\in I$ $(x, y\in |L|)$, and (iii)$_I$ if both x and y belong to I , then so does $x\vee y$ $(x, y\in |L|)$. A *prime ideal* of L is a prime filter of L^{o} , that is, an ideal I for which (iv)$_{PI}$ $1_L\notin I$, and (v)$_{PI}$ whenever $x\wedge y\in I$, then either $x\in I$ or $y\in I$.

Prime Filter Existence Theorem (PFET)**.** Given any filter F_0 and any ideal I_0 on the distributive lattice L such that F_0 and I_0 are disjoint: $F_0\cap I_0=\emptyset$, there is at least one prime filter P on L which contains F_0 as a subset and which is disjoint from I_0 :

$$F_0\subset P\ ,\ \ I_0\cap P=\emptyset\ .$$

Before we turn to the proof of the PFET, let us see how the latest formulation of the Stone representation theorem follows from it. Suppose $x, y\in |L|$, and $x\neq y$. Then either $x\not\leq y$, or $y\not\leq x$ (or both). Say, we have $x\not\leq y$. Now, consider the sets $F_0=\uparrow x \overset{=}{\text{def}} \{u\in |L| : u\geq x\}$, and $I_0=\downarrow y \overset{=}{\text{def}} \{v\in |L| : v\leq y\}$. We immediately see that $\uparrow x$ is a filter, and $\downarrow y$ is an ideal (**exercise**). Also, they are disjoint: if we had $u \in \uparrow x \cap \downarrow y$, then $x \le u$ and $u \le y$, and thus $x \le y$ would be the case. The PFET gives a prime filter P with $\uparrow x \subset P$ and $\downarrow y \cap P = \emptyset$. Then, since $x \in \uparrow x$ and $y \in \downarrow y$, we have that $x \in P$ and $y \notin P$ as desired.

The proof of the PFET is an application of Zorn's lemma. To emphasize the character of this proof, we isolate a part of it as a separate statement.

Criterion for a prime filter. Let F_0 be a filter, I_0 an ideal on the distributive lattice L. Then any filter on L which is *maximal* among those filters that contain F_0 and disjoint from I_0 is prime.

Proof of the PFET from the Criterion. Assuming the truth of the Criterion, we proceed as expected. Consider the set $\mathcal{F}$ of all filters on L that contain F_0 as a subset and are disjoint from I_0, partially ordered by inclusion, $\subset$. We apply Zorn's lemma to the poset $(\mathcal{F}, \subset)$. We **claim** that if $\mathcal{C}$ is any *non-empty* chain in $\mathcal{F}$, then $\bigcup \mathcal{C} \in \mathcal{F}$. Indeed, it is clear that condition $(i)_F$ for filters holds, because $\mathcal{C}$ is non-empty; $(ii)_F$ is also clear. To see $(iii)_F$, if $x, y \in \bigcup \mathcal{C}$, then there are $F, F' \in \mathcal{C}$ with $x \in F$, $y \in F'$; since $\mathcal{C}$ is a chain, either $F \subset F'$, or $F' \subset F$; we conclude that both x and y belong either to F or to F', hence, so does $x \wedge y$ (since F, F' are filters!); but F, F' are both subsets of $\bigcup \mathcal{C}$, thus $x \wedge y$ belongs to $\bigcup \mathcal{C}$ as was to be shown. As to $I_0 \cap \bigcup \mathcal{C}$, if $a \in I_0$ belonged to $\bigcup \mathcal{C}$, then it would belong to an $F \in \mathcal{C}$, contradicting $F \in \mathcal{F}$ and the definition of $\mathcal{F}$. The **claim** is verified.

The condition of Zorn's lemma, namely that each chain have an upper bound is *almost* verified: for each non-empty chain $\mathcal{F}$, $\bigcup \mathcal{F}$ is such an upper bound. For the empty chain, take $F_0 \in \mathcal{F}$ as an upper bound.

By Zorn's lemma, there is a maximal element P of $(\mathcal{F}, \subset)$. By the Criterion, any such maximal element, that is, any filter maximal among those filters that contain F_0 and disjoint from I_0 is prime. This completes the proof.

Proof of the Criterion. Let P be any filter maximal among those filters that contain F_0 and disjoint from I_0. We verify the conditions $(iv)_{PF}$ and $(v)_{PF}$ for P. Since I_0 is an ideal, $0_L \in I_0$. Since $I_0 \cap P = \emptyset$, it follows that $0_L \notin P$; this is (iv)$_{PF}$.

To see (v)$_{PF}$, assume $x \vee y \in P$, and assume, contrary to what we want, that $x \notin P$ and $y \notin P$. We now construct a filter $P[x]$ containing $P \cup \{x\}$ as a subset; we put

$$P[x] = \{u \in |L| : u \geq s \wedge x \text{ for some } s \in P\} .$$

Indeed, $P[x]$ is a filter: conditions (i)$_F$ and (ii)$_F$ are clear; and if u , v both belong to $P[x]$, then there are s , $t \in P$ with

$$u \geq s \wedge x \quad \text{and} \quad v \geq t \wedge x ;$$

it follows that, for $r = s \wedge t$, we have

$$u \geq r \wedge x \quad \text{and} \quad v \geq r \wedge x ,$$

and hence, $u \wedge v \geq r \wedge x$ (why?); this shows that $u \wedge v \in P[x]$.

Since $x \notin P$, we have $P \underset{\neq}{\subset} P[x]$. By the maximality of P among those filters that contain F_0 and are disjoint from I_0 , and since clearly $F_0 \subset P[x]$ (because $F_0 \subset P$), it must be that $P[x]$ is not disjoint from I_0 ; there is $a \in I_0 \cap P[x]$. The definition of $P[x]$ gives that there is $s \in P$ such that

$$s \wedge x \leq a .$$

Doing the same with y as with x , we get $b \in I_0$ and $t \in P$ such that

$$t \wedge y \leq b .$$

Let $c = a \vee b$ and $r = s \wedge t$. Then, of course,

$$r \wedge x \leq c \quad \text{and} \quad r \wedge y \leq c ,$$

(why?); also, $c \in I_0$ and $r \in P$, since I_0 is an ideal and P is a filter. Now [and this is the one point where we use that L is distributive!],

$$r \wedge (x \vee y) = (r \wedge x) \vee (r \wedge y) \leq c$$
$$\uparrow \qquad\qquad\qquad \uparrow$$
distributive law $\quad\quad \vee$ means "sup"

Since we assumed that $x \vee y \in P$, and P is a filter, it follows that $c \in P$, in contradiction to the fact that $P \cap I_0 = \emptyset$. This contradiction shows that, indeed, $x \vee y \in P$ implies that either $x \in P$, $y \in P$, showing that P is a prime filter.

This completes the proof of the PFET.

Exercise. (xxii) A *principal* filter is one of the form $\uparrow x$ (for the latter notation, see above). Show that the principal ultrafilters of $(\mathbf{P}(A), \subset)$ are in a one-to-one correspondence with the elements of the set A.

(xxiii) The set $I_{\mathrm{rat}} = \{q : 0 \leq q \leq 1$ and q is rational$\}$, with the standard ordering of the rational (real) numbers is a distributive lattice. Give a description in familiar terms of the non-principal filters of $(I_{\mathrm{rat}}, \leq)$.

(xxiv) What can we say about prime filters of a total ordering with 0 and 1 as a distributive lattice?

(xxv) If U and V are prime filters (ultrafilters) in a Boolean algebra, then $U \subset V$ implies $U = V$.

(xxvi)* Conversely, if in a distributive lattice L, we have that $P \subset Q$ implies that $P = Q$ whenever P, Q are prime filters, then L is a Boolean algebra.

(xxvii) Apply the PFET to show the following. Let A be any non-empty set, and assume that $\mathcal{F}$ is a family of subsets of A with the property that the intersection of any finitely many sets in $\mathcal{F}$ is non-empty. Show that there is an ultrafilter of $(\mathcal{P}(A), \subset)$ which contains $\mathcal{F}$.

(xxviii) The set A is finite if and only if all ultrafilters of $(\mathcal{P}(A), \subset)$ are principal.