1

First, we'll define Boolean algebras, first as a ring where $x^2 = x$, then as a lattice with certain properties. We'll show that both define the same objects. Both approaches will be useful later on.

Let B be a ring where $x = x^2$ for all x. Some immediate consequences are:

Every element is its own additive inverse:

$$x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$$
$$0 = x + x$$

Multiplication is commutative:

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$$
$$0 = xy + yx$$
$$xy = -yx = yx$$

Where the last identity follows from our previous result.

Now, define the following binary relation: $x \leq y$ iff $xy = x$. We get:

$$xx = x, \text{ so } x \leq x$$

If $x \leq y$, $y \leq z$,

$$xy = x, yz = y$$
$$xz = x(yz) = (xy)z = yz = x, \text{ so } x \leq z$$

And, if $x \leq y$, $y \leq x$,

$$x = xy = yx = y$$

So, this is a reflexive partial order. Furthermore,

$$0x = 0, x1 = x$$

So, $0 \leq x$, $x \leq 1$.

We also have least upper bounds and greatest upper bounds:

We'll claim that for every $c \leq x, y$, $c \leq xy \leq x, y$.

If $c \leq x, c \leq y$, then $cx = x$, $cy = y$. Then,

$$cxy = cy = c$$

So $c \leq xy$.

$$x(xy) = xy$$

So $xy \leq x$.

$$y(xy) = (xy)y = xy$$

And then $xy \leq y$.

Similarly, we'll claim that if $x, y \leq c$, $x, y \leq x + y + xy \leq c$. If $x \leq c, y \leq c$,

$$(x + y + xy)c = xc + yc + xyc = x + y + xy$$

So $x + y + xy \leq c$.

$$(x + y + xy)x = x + yx + yx = x$$

So $x \leq x + y + xy$.

$$(x + y + xy)y = xy + y + xy = y$$

So, finally, $y \leq x + y + xy$.

Denoting the operations $x \frown y = xy, x \smile y = x + y + xy$, these operations form a lattice – a partial order with least upper bounds and greatest lower bounds.

This object is called a boolean algebra. We will now proceed to define Boolean algebras by starting from a lattice and defining a ring structure. One advantage of that approach is that in order to verify a map between boolean algebras is a homomorphism, it will suffice to check that it respects the order relation ($x \leq y$ iff $f(x) \leq f(y)$). We will also need the definition based on rings to discuss ideals later.

2

Let A be a lattice, where, for every x there's a x' with

$$x \smile x' = 1$$
$$x \frown x' = 0$$

Such a complement is unique – let x', x'' be complements of x. Then,

$$x' \smile x'' = (x' \smile x'') \frown 1$$
$$= (x' \smile x'') \frown (x \smile x'')$$
$$= (x' \frown x) \smile x''$$
$$= 0 \smile x'' = x''$$

So, $x' \leq x''$, by applying the definition in reverse we get $x'' \leq x'$ so $x' = x''$. In particular, this shows that the complement of the complement of x is x.

We can also use this to prove de Morgan's laws:

$$\begin{aligned}(x' \smile y') \frown (x \frown y) &= (x' \frown (x \frown y)) \smile (y' \frown (x \frown y)) \\ &= (0 \frown y) \smile (0 \frown x) = 0\end{aligned}$$

$$\begin{aligned}(x' \smile y') \smile (x \frown y) &= ((x' \smile y') \smile x) \frown (x' \smile y') \smile y) \\ &= (1 \smile y') \frown (1 \smile x') = 1\end{aligned}$$

So, $x' \smile y'$ is the complement of $x \frown y$:

$$(x' \smile y') = (x \frown y)'$$

Replacing x and y' by their respective complements, and taking the complement of both sides,

$$(x'' \smile y'')' = (x' \frown y')''$$

$$(x \smile y)' = x' \frown y'$$

To make this a ring, the multiplication is defined as $\frown$, and the addition is defined as:

$$x + y = (x \frown y') \smile (x' \frown y)$$

I'll omit the details, but this does form a ring, with $x^2 = x \frown x = x$, so a boolean algebra. The complement of x corresponds to taking $1 + x$.

3 Homomorphisms and Isomorphisms

A homomorphism of boolean algebras as rings is a homomorphism of rings that happen to be boolean albegras – maps h so that

$$h(x + y) = h(x) + h(y)$$

$$h(xy) = h(x)h(y)$$

$$h(1) = 1$$

The condition $h(0) = 0$ can be derived from:

$$h(0) = h(0 + 0) = h(0) + h(0) = 0$$

From this definition, we can easily prove

$$h(x \frown y) = h(xy) = h(x)h(y) = h(x) \frown h(y)$$

$$h(x') = h(x + 1) = h(x) + h(1) = h(x) + 1 = h(x)'$$

$$h(x \smile y) = h(x + y + xy) = h(x) + h(y) + h(x)h(y) = h(x) \smile h(y)$$

$$x \leq y \to xy = x \to h(xy) = h(x) \to h(x) \leq h(y)$$

It also suffices to specify

$$h(x \frown y) = h(x) \frown h(y)$$

$$h(x') = h(x)'$$

Since

$$x + y = (x \frown y') \smile (x' \frown y) = (x \frown y')' \frown (x' \frown y)'$$

An isomorphism of Boolean algebras is a bijective homomorphism. For a surjective h, the following condition is necessary and sufficient to define an isomorphism:

$$x \leq y \text{ if and only if } h(x) \leq h(y)$$

In an isomorphism, this holds, since

$$xy = x \text{ if and only if } h(x)h(y) = h(x)$$

Conversely, if this holds, h is injective – if $h(x) = h(y)$,

$$h(x) \leq h(y) \to x \leq y$$

$$h(y) \leq h(x) \to y \leq x$$

$$x = y$$

We can prove that $x \frown y = h(x \frown y)$ using the greatest lower bound property:

Let z be the number such that $h(z) = h(x) \frown h(y)$. Then,

$$h(z) \leq h(x) \to z \leq x$$

$$h(z) \leq h(y) \to z \leq y$$

So, $z \leq x \frown y$.

$$x \frown y \leq x \to h(x \frown y) \leq h(x)$$

$$x \frown y \leq y \to h(x \frown y) \leq h(y)$$

$$h(x \frown y) \leq h(x) \frown h(y) = h(y)$$

$$x \frown y \leq z$$

We can prove that $h(x \smile y) = h(x) \smile h(y)$ using a similar argument.

$h(1)$ is greater than or equal to every element, so $h(1) = 1$, and similarly $h(0)$ is 0.

Finally,

$$h(x') \smile h(x) = h(x' \smile x) = h(1) = 1$$
$$h(x') \frown h(x) = h(x' \frown x) = h(0) = 0$$

So $h(x') = h(x)'$

Then, h is a bijective homomorphism as claimed.

This also shows that the inverse of an isomorphism is still an isomorphism, since the condition $x \leq y$ iff $h(x) \leq h(y)$ implies the same thing for the inverse.

4 Ideals

In the following, 'ideal' means a proper ideal of a ring, so an ideal which is not the whole ring. For a subset I of a Boolean algebra A to be an ideal, the following are necessary and sufficient:

$$0 \in I, 1 \notin I$$
$$\text{for all } x, y \in I, x \smile y \in I$$
$$\text{for all } x \in I, y \in A, y \leq x \text{ implies } y \in I$$

Proof:

Let I be an ideal. 0 is in I, since it's an additive subgroup. 1 isn't, since then, for every $a \in A$, $a * 1 = a$ is in I, then I would have to be the entire ring.

If x and y are in I, by definition, xy is too. Then, since I is an additive subgroup, $x \smile y = x + y + xy$ is as well.

Finally, if x is in I, $xy \in I$. $y \leq x$, by definition means $xy = y \in I$.

Conversely, let these conditions be satisfied.

If $x, y \in I$, $x \smile y \in I$.

$$(x+y)(x \smile y) = (x+y)((x+y)+xy) = x+y+(x+y)xy = x+y+xy+xy = x+y$$

So, $x + y \leq x \smile y$, and $x + y \in I$ by the third condition. Since $-x = x$ in a boolean algebra, we conclude that I is an additive subgroup.

For $x \in I$, $xy = x \frown y \leq x$, so $xy \in I$. So, I is an ideal. It's proper, since it doesn't include the element 1.

The equivalent conditions define what's called an ideal in the context of partially ordered sets. We've proven that they're equivalent to ideals for rings in Boolean algebras.

Then, the following are equivalent:

$$\text{(1)I is a maximal ideal}$$
$$\text{(2)}A/I \text{ is isomorphic to } \{0, 1\}$$
$$\text{(3)I is the kernel of a homomorphism } A \to \{0, 1\}$$
$$\text{(4)For all } x, x \in I \text{ or } x + 1 \in I$$

$$(5)\text{For all } x, y, \text{ if } xy \in I, \text{ then } x \in I \text{ or } y \in I$$

$$(6)\text{For all } x_1 x_2 ... x_k \in I, x_1 \in I \text{ or } x_2 \in I \text{ or } ... x_k \in I$$

(1) $\to$ (2)

In fact, in any commutative ring, we can prove that A/I is a field if and only if I is maximal:

If I isn't maximal, let $I \subsetneq J$, and $a \in J - I$. a isn't in I, so $[a]$ isn't the zero element in A/I. If it was invertible, there would be a b with

$$[a][b] = 1$$

$$[ab - 1] = 0$$

$$ab - 1 \in I$$

$a \in I$, so $ab \in I$. Then,

$$ab - (ab - 1) = 1 \in I$$

This is a contradiction. We conclude that, A/I has an non-invertible elements, so it can't be a field.

Conversely, assume I is maximal. Let $[a] \neq 0 \in A/I$. Form

$$K = \{ay + z : y \in A, z \in I\}$$

Clearly, $0 = a*0+0 \in K$, if ay_1+z_1, $ay_2+z_2 \in K$, since the ring is commutative,

$$ay_1 + z_1 - (ay_2 + z_2) = a(y_1 - y_2) + (z_1 - z_2) \in K$$

And, if $ay + z \in K$,

$$(ay + z)t = a(yt) + (zt) \in K$$

So, K is an ideal. It includes any element $a*0+y$ of I, and it includes $a*1+0 = a$, which isn't in I. Since I is maximal, K must be the whole ring, and then, there must be y, z with

$$ay + z = 1$$

Then,

$$ay + z = [a][y] + [z] = [a][y] = 1$$

Note that $z \in I$. Then, any nonzero element of A/I does have an inverse, and this proof is complete.

Finally, note that $\{0, 1\}$ is the only Boolean algebra which is a field: For every x,

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

Which, if this is a field (or even a domain), implies that either $x = 0$ or $x = 1$.

(2) $\to$ (3) I is the kernel of the quotient map $A \to A/I = \{0, 1\}$.

(3) $\to$ (4) Let h be the homomorphism $A \to \{0, 1\}$ with kernel I. Then, for all x, $h(x) = 0$ or $h(x) = 1$. In the latter case, $h(1+x) = h(1)+h(x) = 1+1 = 0$. So, x or $1 + x$ is in the kernel, which is I.

(4) $\to$ (5) Let $x, y \notin I$. Then, $1+x, 1+y \in I$. Then,

$$(1+x) \smile (1+y) = 1 + (x \frown y) = 1 + xy \in I$$

So, $xy \in I$ implies $x \in I$ or $y \in I$.

(5) $\to$ (1) Suppose I isn't maximal. Then, let $I \subsetneq J$ be an ideal, $a \in J - I$. $a \in J$, so $1 + a \notin J$, because then

$$a \smile (1+a) = 1 \in J$$

But, $(1+a) \in I \subseteq J$, which is a contradiction.

(5) $\leftrightarrow$ (6) This is an obvious use of induction.

The fact that maximal ideals are the kernels of homomorphisms $A \to \{0,1\}$ will be important later on – the elements of the Stone space of a boolean algebra A are homomorphisms $A \to \{0,1\}$.

5 Filters

Filters in order theory are the dual notion of ideals:

A filter is a subset F of a Boolean algebra A such that:

$$0 \notin F, 1 \in F$$

$$x, y \in F \to x \frown y \in F$$

$$x \in F, y \geq x \to y \in F$$

In boolean algebras, we can equivalently define them as subsets F such that $\{x \in A : 1 + x \in F\}$ is an ideal.

Proof:

Let

$$I = \{x \in A : 1 + x \in F\}$$

Assume the first set of conditions hold.

The first condition implies $0 \in I, 1 \notin I$.

The second condition implies for $x, y \in I$, $(1+x), (1+y) \in F$, then

$$(1+x) \frown (1+y) \in F$$

$$1 + (x \smile y) \in F$$

$$x \smile y \in I$$

Finally, notice that $x \leq y$ imples $1 + y \leq 1 + x$:

$$xy = x$$

$$(1+x)(1+y) = 1 + x + y + xy = 1 + x + y + x = 1 + y$$

Then, if $x \in I$, $y \leq x$, $1 + x \in F$, $1 + y \geq 1 + x$, so by the third condition, $1 + y \in F$, and $y \in I$. So, I is an ideal as we have defined.

Conversely, if I is an ideal, the proof is entirely the same:
The first condition is given by $0 \in I, 1 \notin I$.
If $x, y \in F$, $1+x, 1+y \in I$, then

$$(1+x) \smile (1+y) \in I$$

$$1 + (x \frown y) \in F$$

$$x \frown y\ inF$$

And finally, if $x \in F$, $y \geq x$,

$$1 + x \in I, 1 + y \leq 1 + x \to 1 + y \in I$$

$$y \in F$$

We also have a similar characterization for maximal filters, which are called ultrafilters. The following are equivalent:

$$(1')F \text{ is an ultrafilter}$$

$$(3') \text{ there's a homomorphism } g : A \to \{0,1\} \text{ with } F = h^{-1}(\{1\})$$

$$(4') \text{ for all x}, x \in F \text{ or } 1 + x \in F$$

$$(5') \text{ if } x \smile \in F, \text{ then } x \in F \text{ or } y \in F$$

$$(6') \text{ if } x_1 \smile ... \smile x_n \in F, \text{ then } x_1 \in F \text{ or } ...x_n \in F$$

We'll prove this by proving that if and only if F has one of these properties, the dual filter I as defined above has the corresponding property.

$(1')$ Saying there's no filter $F' \supsetneq F$ is equivalent to saying there's no ideal $I' \supsetneq I$, since a set is a filter if and only if the set of its complements is an ideal and vice versa.

$(3')$ For a boolean algebra homomorphism, $h(x+1) = h(x) + 1$, so a homomorphism sending F to 1 is equivalent to a homomorphism sending I to 0.

$(4')$ This is obvious by the definition of $I - x \in I$ if and only if $x + 1 \in F$, etc.

$(5')$ If this condition is true, for $x \frown y \in I$, $1 + x \frown y = (1+x) \smile (1+y) =$ is in F, so $1+x$ or $1+y$ is in F, so x or y is in I.

Similarly, if the corresponding statement is true for I, let $x \smile y \in F$.

$$I \ni 1 + (x \smile y) = (1+x) \frown (1+y)$$

$$1 + x \in I \text{ or } 1 + y\ inI$$

And x or y is in F.

Finally, $(6')$ may be shown to be equivalent to $(5')$ by induction.

Continuing with the remark last section, the property 3 will be especially important, we'll be interested in homomorphisms $A \to \{0,1\}$. Property 3 says they correspond bijectively with ultrafilters – any ultrafilter is $h^{-1}(1)$ for such a homomorphism, and every such preimage of a homomorphism is an ultrafiler.

Remark.

For any $x \neq 0 \in A$, we can form a filter including x:

$$F = \{y \in A : y \geq x\}$$

It's easy to see that $0 \notin F$, $1 \in F$, $u, v \in F$ implies $u \frown v \in F$, and $u \in F, v \geq u$ implies $v \in F$, so it's indeed a filter.

Krull's theorem, which we'll prove later with the axiom of choice, states that every ideal in a commutative ring is included in some maximal ideal. This implies that every element in x is included in some ultrafilter.

Equivalently, for any $x \in A$, we can form a homomorphism $A \to \{0, 1\}$ with $h(x) = 1$.

6 Zero Dimensional Topological Spaces

A topological space is said to be zero dimensional if it has a basis consisting of closed sets. We won't get into a definition of dimension in general for topological spaces here.

We can equivalently say that the family of sets which are both open and closed ('clopen') form a basis for the topology. This clearly implies the previous condition, and if the previous statement is true, the basis consisting of closed sets is a subset of the set of clopen sets, so the latter forms a basis as well.

A compact zero dimensional topological space is called a Boolean topological space.

Given an indexed family of topological spaces $(X_i)_{i \in I}$, we can define a topology on their product $\Pi_{i \in I} X_i$ – elements $\Pi_{i \in I} O_i$, where all the O_i are open in X_i and all but finitely many ones are equal to X_i. Tychonoff's Theorem, which is equivalent to the axoim of choice, states that if all the X_i are compact, this product space is too.

Take the discrete topology on two points $\{0, 1\}$, and form the product space $\{0, 1\}^I$ for some indexing set I. A basic open set Ω is either empty (in case when one of the open sets is the empty set), or has a finite number of indices which are either $\{0\}$ or $\{1\}$. Where the element of the product space are written as functions $I \to \{0, 1\}$, it's the set of functions whose values at a finite number of points is determined:

$$\{f : I \to \{0, 1\} : f(i_1) = \epsilon_1, ...f(i_n) = \epsilon_n\}$$

Where n is some natural number and each ϵ_i is either 0 or 1. By De Morgan's Law, the complement of this set is

$$\bigcup_{1 \leq j \leq n} \{f : f(i_j) = 1 - \epsilon_j\}$$

This is a finite union of open sets in the basis, so it's open. Then, Ω is closed as well. Since every set in the basis is clopen, this is a zero dimensional topological set. $\{0,1\}$ is clearly compact. By Tychonoff's Theorem, this space is compact as well, and therefore a Boolean topological space.

6.a The Stone space of a Boolean algebra

For a Boolean algebra A, the subset of $\{0,1\}^A$ which consists of homomorphisms $A \to \{0,1\}$ is denoted $S(A)$ and called the Stone space of A.

We've seen that $\{0,1\}^A$ is zero dimensional, so we can find a basis by clopen sets. With $S(A)$ under the subspace topology, the same basis forms a basis of clopen sets, so $S(A)$ is zero dimensional as well.

Proposition: The sets in the basis of $S(A)$ are exactly the sets defined as

$$\{h \in S(A) : h(a) = 1\}$$

for some $a \in A$. This element a is unique.

Note that the basis of $\{0,1\}^A$ are the functions which take a finite set of points to either 0 or 1.

Clearly, every set defined this way is a set in the basis – $S(A) \cap \{f : A \to \{0,1\} : f(a) = 1\}$.

Every set in the basis can be defined this way:

Let Δ be an arbitrary element in the basis, given by

$$\Delta = \{h \in S(A) : h(a_1) = \epsilon_1, ...h(a_n) = \epsilon_n\}$$

Where $a_i \in A$, and ϵ_i are either zero or one. Define:

$$b_k = a_k \text{ if } \epsilon_k = 1, 1 + a_k \text{ otherwise}$$

Since the elements of $S(A)$ are homomorphisms, if $\epsilon_k = 1$,

$$h(b_k) = h(a_k)$$

and, if $\epsilon_k = 0$,

$$h(b_k) = h(1 + a_k) = 1 + h(a_k)$$

In other words, $h(b_k) = 1$ if and only if $h(a_k) = \epsilon_k$. Then, $h(a_1) = \epsilon_1, h(a_2) = \epsilon_2, ...h(a_n) = \epsilon_n$ if and only if

$$h(b_1) \frown h(b_2) \frown ... \frown h(b_n) = 1$$

Since h also preserves intersections, this happens if and only if

$$h(b_1 \frown b_2 \frown ... \frown b_n) = 1$$

So we've shown that every open set has the form $h : h(a) = 1$ for some $a \in A$.

Maybe as a special case, notice that the empty set and $S(A)$ are given by $\{h \in S(A) : h(0) = 1\}$ and $\{h \in S(A) : h(1) = 1\}$ respectively.

Now, we'll show that the element a is unique. Let $a \neq b$. Then, $a + b \neq 0$.

Then, as we've shown using Krull's theorem, there's an ultrafilter that includes $a + b$, so a homomorphism with

$$\phi(a + b) = 1 = \phi(a) + \phi(b)$$

Since the right hand side is in $\{0, 1\}$, this implies $\phi(a) = 1$ and $\phi(b) = 0$, or vice versa. Without loss of generality, assume $\phi(a) = 1$. Then,

$$\phi \in \{h \in S(A) : h(a) = 1\}$$
$$\phi \notin \{h \in S(A) : h(b) = 1\}$$

So the sets aren't equal.

As a corollary of this characterization of basis elements, the complements of the sets in the basis are still in the basis:

$$\{h \in S(A) : h(a) = 1\}^c = \{h \in S(A) : h(1 + a) = 1\}$$

So the sets in the basis are clopen. If we can also show that the topological space is closed, we'll show that it's a Boolean topological space. Since the product space $\{0, 1\}^A$ is compact by Tychonoff's theorem, we only need to show that it's closed, since a closed subset of a compact space is compact.

We've proved that a function in $\{0, 1\}^A$ is a homomorphism of Boolean algebras if and only if it preserves intersections and complements.

Let

$$\Omega(a, b) = \{f : A \to \{0, 1\} : f(ab) = f(a)f(b), f(1 + a) = 1 + f(a)\}$$

Then, the set of homomorphisms $S(A)$ is exactly:

$$S(A) = \bigcap_{a \in A, b \in A} \Omega(a, b)$$

We can each write $\Omega(a, b)$ as the following finite union of closed sets:

$$\begin{aligned}
\Omega(a, b) = \{f : f(a) = 0, f(b) = 0, f(ab) = 0), f(1 + a) = 1\} \\
\cup\{f : f(a) = 0, f(b) = 1, f(ab) = 0), f(1 + a) = 1\} \\
\cup\{f : f(a) = 1, f(b) = 1, f(ab) = 0), f(1 + a) = 0\} \\
\cup\{f : f(a) = 1, f(b) = 1, f(ab) = 1), f(1 + a) = 0\}
\end{aligned}$$

Then, each $\Omega(a, b)$ is closed as a finite union of closed sets, and $S(A)$ itself is closed, since it's some arbitrary intersection of closed sets. As a closed subset of a compact space, it's compact. Then, since it's also zero-dimensional, it's a Boolean topological space.

We already know that the sets in the basis are clopen, but we'll later need the fact that the clopen sets are exactly the sets in this basis.

Given an open and closed set Γ,

Since it's open, it's covered by sets in the basis $\{\Gamma_i\}_{i \in I}$ Since Γ is a closed subset of a compact space, it's compact. Then, find a finite subcover $\Gamma_1, ...\Gamma_n$. Each has form:

$$\Gamma_i = \{h : h(x_i) = 1\}$$

Then,

$$\Gamma = \{h : h(x_1 \smile x_2 \smile ... \smile x_n) = 1\}$$

and so it is in the basis.

7 Characterization of Boolean Algebras

Given a topological space S, the set of its clopen subsets form a Boolean algebra under the regular set operations union, intersection, complement – clearly, the intersection or complement of clopen sets is clopen. This will be denoted as $B(S)$. Given a connected space, this Boolean algebra does become $\{0, 1\}$.

We'll now prove that every Boolean algebra is isomorphic to the Boolean algebra of clopen sets of its Stone space. In particular, this does show that any Boolean algebra is equivalent to the Boolean algebra of certain subsets of some set, under the set operations intersection, complement, etc.

Let H be the map $A \to \mathcal{P}(S(A))$

$$H(a) = \{h \in S(A) : h(a) = 1\}$$

We've done a lot of the work in the previous sections: We know that $H(a)$ is a clopen subset of $S(A)$ for any a, so the codomain is actually $B(S(A))$.

We know that any basis element, so any clopen subset, has this form, so the map is surjective. We also know that given any clopen set, a in the expression is unique, so the map is injective.

To show that it's an isomorphism of Boolean algebras, we'll show that $H(a) \le H(b)$ if and only if $a \le b$.

If $x \le y$, and h is any homomorphism with $h(x) = 1$, $h(x) \le h(y)$ implies that $h(y) = 1$. Then, $H(x) \subseteq H(y)$.

Now, assume x is not less than or equal to y. Then, $xy \ne x$, $x(1 + y) \ne 0$. As we've remarked, for any element, we can find an ultrafilter that includes it, so a homomorphism h with

$$h(x(1 + y)) = 1$$

Then,

$$h(x)(1 + h(y)) = 1$$

$$h(x) = 1, h(y) = 0$$

And then, $h \in H(x)$, $h \notin H(y)$, and $H(x) \nsubseteq H(y)$.

8 Characterization of Boolean Topological Spaces

We can also now prove that every Boolean topological space X is homeomorphic to the Stone space of the Boolean algebra of clopen subsets of X: $X = S(B(X))$.

We've seen that the Boolean algebra of clopen sets of X is a basis for the topology on any Boolean topological space. For all $x \in X$, define

$$f_x : B(X) \to \{0,1\} = \Omega \mapsto \{1 \text{if} x \in \Omega, 0 \text{otherwise}\}$$

First, we'll show that f_x is really a homomorphism of Boolean algebras, so in $S(B(X))$.

For clopen subsets Ω, Δ,

$$f_x(\Omega \cap \Delta) = 1 \text{ iff } x \in \Omega \cap \Delta$$

$$= 1 \iff f_x(\Omega) = 1 \text{ and } f_x(\Delta) = 1$$
$$= f_x(\Omega) f_x(\Delta)$$

$$f_x(\Omega^c) = 1 \text{ iff } x \in \Omega^c$$
$$= 0 \text{ iff } x \in \Omega$$
$$= f_x(\Omega)^c$$

So, f_x is a Boolean algebra homomorphism from $B(X)$ onto $\{0,1\}$, so is in $S(B(X))$.

Now, we'll show that it's injective.

If $x \neq y$, because X is Hausdorff, we can find an open set O with $x \in O$, $y \notin O$. O is a union of basic open sets, so there's a clopen set $\Omega \in B(X)$ with $x \in \Omega$, $y \notin \Omega$. Then,

$$f_x(\Omega) = 1 \neq f_y(\Omega) = 0$$

So, $f_x \neq f_y$, and f is injective.

Now, we'll show that it's surjective.

Let h be an arbitrary element of $S(B(X))$, so a homomorphism $B(X) \to \{0,1\}$. The filter associated with h is

$$U = \{\Omega \in B(X) : h(\Omega) = 1\}$$

Since U is a filter, it has the property that if $x_1, ...x_n \in U$, their intersection $x_1 \frown x_2 \frown ... \frown x_n$ is in U, so it's nonzero – in this case, it's not the empty set.

The usual definition of compactness states that every open cover has a finite subcover. By taking complements of every set in the cover, this equivalently states that every infinite set of closed sets whose intersection is empty has a finite subset of closed sets whose intersection is still empty.

Now, since X is compact, and the elements of U are closed, and every finite intersection of elements of U are nonempty, we can conclude that the intersection of every element of U is still nonempty.

Let x be an element of this intersection.

For every clopen subset Ω of $B(X)$,

Ω might be an element of U. In this case, since c is in every element of U, it's in Ω, and

$$f_x(\Omega) = 1$$

If Ω isn't an element of U, $1+\Omega$ is, since U is an ultrafilter. Then, x is in $1+\Omega$, and

$$f_x(1+\Omega) = 1$$

Then, since f_x is a homomorphism,

$$f_x(\Omega) = 0$$

Then,

$$f_x(\Omega) = 1 \text{ iff } \Omega \in U$$

And, by definition, $U = \{\Omega \in B(X) : h(\Omega) = 1\}$. So,

$$f_x = h$$

Then, $H : f \mapsto f_x$ is surjective onto $S(B(X))$. Since we know that f is injective, this also tells us the x, the intersection of all the elements of U, is unique – $h = f_x = f_y$ implies $x = y$.

Finally, we can prove that f is continuous:

Let G be an element in the basis of $S(B(X))$, so a clopen set. We've seen that i Stone spaces, this means it has the form

$$G = \{h \in S(B(X)) : h(\Omega) = 1\}$$

For some $\Omega \in B(X)$.

$$\begin{aligned} f^{-1}(G) &= \{x \in X : f_x \in G\} \\ &= \{x \in X : f_x(\Omega) = 1\} \\ &= \{x \in X : x \in \Omega\} = \Omega \end{aligned}$$

Where $\Omega \in B(X)$, so it's open. Since the inverse image of elements in the basis are open, f is continuous.

f^{-1} is continuous:

Let $\Omega \in X$ be an open set in the basis of X.

$$(f^{-1})^{-1}(\Omega) = f(\Omega) = \{f_x \in S(B(X)) : x \in \Omega\}$$

We've seen that f is surjective, so every $h \in S(B(X))$ has form f_x for some x. Then, $h(\Omega) = 1$ if and only if x such that $h = f_x$ is in Ω – by definition of f, $f_x(\Omega) = 1$ if and only if x is in Ω. This means:

$$\{f_x \in S(B(X)) : x \in \Omega\} = \{h \in S(B(X)) : h(\Omega) = 1\}$$

The latter is a basis element in the Stone space of $B(X)$, so we conclude that f^{-1} is continuous as well.

Name the isomorphism $A \to B(S(A))$ H_A.

9 Categorical equivalence

We will now construct a bijection between homomorphisms between Boolean algebras A to A' and continuous functions $S(A')$ to $S(A)$.

Since elements of $S(A)$ can be regarded as functions $A \to \{0,1\}$, we can define this mapping similarly to dual spaces in vector spaces:

$$\Phi(\phi) = (h : A' \to \{0,1\}) \mapsto (h \circ \phi : A \to \{0,1\})$$

We'll first show that this map is actually continuous.

Let Ω be an element in the basis of $S(A)$. It has form $\{h \in S(A) : h(a) = 1\}$ for some $a \in A$.

$$\begin{aligned}
(\Phi(\phi))^{-1}(\Omega) &= \{h' \in S(A') : \Phi(\phi)(h') \in \{h \in S(A) : h(a) = 1\}\} \\
&= \{h' \in S(A') : (\Phi(\phi)(h'))(a) = 1\} \\
&= \{h' \in S(A') : (h' \circ \phi)(a) = 1\} \\
&= \{h' \in S(A') : h'(\phi(a)) = 1\}
\end{aligned}$$

This is an open set in $S(A')$, so this map is continuous.

We'll show that this is a bijection by defining an inverse. If α is a continuous function $S(A')$ to $S(A)$, let α^{-1} be the function $\mathcal{P}(S(A)) \to \mathcal{P}(S(A'))$. Since α is continuous, α^{-1} takes clopen sets to clopen sets, and so it's a map $B(S(A')) \to B(S(A))$. Then, the following defines a function $A \to B(S(A)) \to B(S(A')) \to A'$:

$$\Psi(\alpha) = H_{A'}^{-1} \circ \alpha^{-1} \circ H_A$$

$$\begin{aligned}
(\Psi \circ \Phi)(\phi) &= \Psi(\Phi(\phi)) \\
&= H_{A'}^{-1} \circ (\Phi(\phi))^{-1} \circ H_A \\
&= a \mapsto (H_{A'}^{-1} \circ (\Phi(\phi))^{-1})\,(\{h \in S(A) : h(a) = 1\}) \\
&= a \mapsto H_{A'}^{-1}\,(\{g \in S(A') : \Phi(\phi)(g) \in \{h \in S(A) : h(a) = 1\}\}) \\
&= a \mapsto H_{A'}^{-1}(\{g \in S(A') : ((\Phi(\phi))(g))(a) = 1\}) \\
&= a \mapsto H_{A'}^{-1}(\{g \in S(A') : ((g \circ \phi)(a) = 1\})) \\
&= a \mapsto H_{A'}^{-1}(\{g \in S(A') : g(\phi(a)) = 1\}) \\
&= a \mapsto H_{A'}^{-1}(H_{A'}(\phi(a))) \\
&= a \mapsto \phi(a) \\
&= \phi
\end{aligned}$$

$$(\Phi \circ \Psi)(\alpha) = \Phi(H_{A'}^{-1} \circ \alpha^{-1} \circ H_A)$$

$$= h \mapsto h \circ H_{A'}^{-1} \circ \alpha^{-1} \circ H_A$$
$$= h \mapsto (a \mapsto (h \circ H_{A'}^{-1} \circ \alpha^{-1} \circ H_A)(a))$$

Let U be the argument of $h \circ H_{A'}^{-1}$ in the expression, so

$$U \in B(S(A)) = \alpha^{-1}(H_A(a))$$
$$= \alpha^{-1}\{h \in S(A) : h(a) = 1\}$$
$$= \{h' \in S(A') : \alpha(h') \in \{h \in S(A) : h(a) = 1\}\}$$
$$= \{h' \in S(A') : \alpha(h')(a) = 1\}$$

U is equal to $\{h \in S(A') : h(u) = 1\}$ for some $u \in A'$. Then,

$$h(H_{A'}^{-1}(U)) = h(H_A^{-1}(\{h \in S(X) : h(u) = 1\})) = h(H_A^{-1}(H_A(u))) = h(u)$$

By definition, u is the element of A' such that $h \in U$ if and only if $h(u) = 1$. Then,

$$h(H_{A'}^{-1}(U)) = 1 \text{ if and only if } h \in U$$
$$h(H_{A'}^{-1}(U)) = 1 \text{ if and only if } h \in \{h' \in S(A') : \alpha(h')(a) = 1\}$$
$$h(H_{A'}^{-1}(U)) = 1 \text{ if and only if } \alpha(h)(a) = 1$$

Since all the possible values are 0 or 1,

$$h(H_{A'}^{-1}(U)) = \alpha(h)(a)$$
$$(\Phi \circ \Psi)(\alpha) = h \mapsto (a \mapsto \alpha(h)(a))$$
$$(\Phi \circ \Psi)(\alpha) = h \mapsto \alpha(h)$$
$$(\Phi \circ \Psi)(\alpha) = \alpha$$

So, Φ defines a map from the morphisms of the category of Boolean algebras and homomorphisms to the morphisms of the category of Boolean topological spaces and continuous functions. With S mapping the objects, it's a contravariant functor – $\Phi(\mathrm{id}) = \mathrm{id}$ and $\Phi(g \circ f) = \Phi(g) \circ \Phi(f)$ is satisfied.

Similarly Ψ defines a functor mapping the objects $S(X)$ to X (not $B(S(X))$) – the required rules are easy enough to check – and since these are exactly inverses, they form an equivalence of categories.

10 Epilogue: Uses of the Axiom of Choice

We've used two theorems derived from the axiom of choice in the paper – Krull's Theorem, and Tychonoff's Theorem, and I hadn't seen a proof of Zorn's Lemma before, so I thought this might be a nice place to discuss those. It'll also be a nice opportunity to say a few things about compactness.

10.a Zorn's Lemma

Let $\leq$ be a partial order of the set X. Given a totally ordered subset C, define

$$P(C, x) = \{y \in C : y < x\}$$

Suppose every totally ordered subset of X has an upper bound. Assume by contradiction that X must not have a maximal element.

As a remark, this implies that X must not be empty since $\{\}$ is a totally ordered subset, and must have an upper bound.

Given any chain C, we can find an upper bound u, and then, by assumption, an x with $x > u$, so strict upper bound. Using the axiom of choice, assign every totally ordered subset C, a strict upper bound $f(C)$.

Call a subset A of X conforming if $\leq$ defines a well ordering on A, and for each x, $x = f(P(A, x))$.

Lemma: If A and B are conforming subsets, $A \neq B$, then A must be $P(B, x)$ for some x or vice versa.

Proof: If $A \neq B$, either A/B or B/A is nonempty, without loss of generality, assume $A/B \neq \{\}$.

Then, since A is well-ordered, A/B has a least element x. If $k \in A, k < x$, my the minimality of x, k must be in B. Then, by definition of P,

$$P(A, x) \subseteq B$$

We'll prove by contradiction that this is an equality. Assume that $B\ P(A, x)$ is nonempty. Then, it has a least element y.

Let $u \in P(B, y)$. For all $v \in A$, $v < u$, v must be in B. Otherwise,

$$v \in A\ B, \text{ so } x \leq v$$

Now, $u > v \geq x$. $u \in B$, $u \notin \{a \in A : a < x\}$. However, $u < y$ because $u \in P(B, y)$, which contradicts the minimality of y in $B\ P(A, x)$.

Since $v \in B$, $v < u < y$, $vP(B, y)$.

Now, let z be the least element of $A\ P(B, y)$. Note $A\ P(B, y) \supseteq A\ B$, so $z \leq x$. Then, $z \in P(A, x) \subseteq B$.

If $w \in P(A, z)$, $w \in A$, $w < z$, so $w \notin A\ P(B, y)$ by the minimality of z in that set. Then, $w \in P(B, y)$.

If $w \in P(B, y)$, since $z \in B$, w and z must be comparable, since B is well-ordered. If $z < w$, $z \in P(B, y)$ as we discussed. This is impossible, since $z \in A\ P(B, y)$. $z = w$ also implies $z \in P(B, y)$. Then, we conclude that $w < z$,

Also, note that y is minimal in $B\ P(A, x)$. $w \in B$, $w < y$, $w < z \leq x$. So, w must be in A to not contradict the minimality of y. Then, $w \in P(A, z)$.

We conclude that

$$P(A, z) = P(B, y)$$

But, since A and B are conforming,

$$z = f(P(A,z)) = f(P(B,y)) = y$$

Since $x \in A \ B$, $y \in B$ implies $z \neq x$. Then, $z < x$, $z \in A$, so $z \in P(A,x)$. But, y should be in $B \ P(A,x)$, which is the contradiction. This concludes the proof of the lemma.

Now, if A is a conforming subset of X, $a \in A$, and $y < a$, $y \notin A$, y cannot be in any conforming subset B – then, since either A is a subset of B or vice versa, and $y \in B \ A$, A must be $P(B,x)$ for some x. Then, $y < a < x$, which means y should be in A.

Let U be the union of all conforming subsets of X. Then, any subset of U must be contained in a single conforming subset – assume by contradiction there is a subset S not contained in a single conforming set. Then, it must have two elements a, b with $a \in A - B$, $b \in B - A$ for conforming subsets A, B. This is a contradiction, since we've proved that given any two conforming subsets, one must be a subset of the other. So, any subset of U must be well-ordered.

Also, for all $x \in U$, $x \in A$ for some conforming subset A, so $x = f(P(A,x))$. But then, if $u \in U$, $u < x$, $u \in A$ since otherwise u can not be in any other conforming subset, so it can't be in U. So,

$$P(A,x) = \{a \in A : a < x\} = \{u \in U : u < x\} = P(U,x)$$

$$x = f(P(A,x)) = f(P(U,x))$$

So, U is a conforming subset.

Let $x = f(U)$. Since x is greater than any element of U, $U \cup \{x\}$ is still well-ordered. For all $u \in U$, $P(U,y) = P(U \cup \{x\}, y)$ since $x > u$ anyway, and

$$f(x) = f(P(U \cup \{x\}, x)) = f(U)$$

So $\{x\} \cup U$ is a conforming subset, which contradicts the assumption that U was the union of all the conforming subsets. Then, X must have a maximal element.

10.b Krull's Theorem

Let R be a commutative ring, I be a proper ideal. We'll prove that it must be included in some maximal proper ideal.

$$E = \{\text{ideal J of R} : I \subseteq J\}$$

Let C be some totally ordered subset. If it's empty, I is an upper bound, and included in E.

If it's nonempty, consider the set

$$I_0 = \bigcup_{J \in C} J$$

$0 \in I_0$ since it's nonempty, and all of its elements are ideals, which must contain 0. If it contains x, one of its elements J contains x, then it contains $-x$ as well, and so does I_0.

If $x, y \in I_0$, $x \in J_1, y \in J_2$ for some $J_1, J_2 \in C$. C is totally ordered – without loss of generality, $J_1 \subseteq J_2$. Then, $x, y \in J_2$, so $x + y \in J_2 \subseteq I_0$.

Finally, if $r \in R$, $x \in I_0$, $x \in J$ for some ideal J, $rx \in J \subseteq I_0$.

Also $a \notin I_0$ since it can't be in any of its elements.

So, I_0 is a proper ideal which contains I and all the elements of C, so an upper bound in C. Then, by Zorn's Lemma, E must contain a maximal element, a maximal proper ideal containing I.

Note that this argument is easily generalized to find a maximal left or right ideal containing a given left of right ideal respectively.

10.c Tychonoff's Theorem