THE STONE REPRESENTATION THEOREM FOR BOOLEAN ALGEBRAS

RAFAEL WINGESTER RIBEIRO DE OLIVEIRA

Abstract. The study of Boolean algebras, has had a big impact on a variety of fields in mathematics. From functional analysis to other parts of algebra itself, Stone's research along with that of his colleagues working on the same field had a lot of impact and brought in very relevant new insights. This paper attempts to present students with an algebraic approach to Stone's representation theorem for Boolean algebras in a way as self-contained as possible. No prerequisites apart from some prior experience with college-level mathematics is assumed, as even the more complicated results have fairly simple statements. The exposition here follows rather closely the style of Halmos' and Givant's Introduction to Boolean Algebras, and cites briefly other papers by Stone and Huntington. The hope is that this paper will be a useful resource for any student interested in receiving a quick introduction, though without many technical prerequisites, to the topic at hand. Lastly, it is worthwhile to mention the very fortunate fact that both Stone (whose result is the main focus of this piece) and Halmos, author of a very important reference of this paper, were associated with the University of Chicago. Stone was head of the Mathematics department between 1946 and 1952, whereas Halmos also taught in the department between 1946 and 1960.

Contents

1. Preliminaries and getting to the result

We begin our discussion with some motivation for the theory of Boolean algebras. Let X be an arbitrary set and let $\mathcal{P}(X)$ be the class of all subsets of X (the power set of X). In that class, one can consider the usual set theoretic operations of union, intersection, and complementation along with the distinguished elements $\emptyset$ and the universal set X. That said, one would not be mistaken in calling $\mathcal{P}(X)$ with these operations and distinguished elements a Boolean algebra (or a field of sets) of X. Furthermore, subsets of $\mathcal{P}(X)$ closed under the previously defined operations also are a Boolean algebra, and are also called fields of sets. With some degree of inspiration on the set theoretic operations, we go on to define a Boolean algebra in the following manner:

Date: August, 2015.

Definition 1.1. A Boolean algebra is a non empty set A, together with two binary operations $\wedge$, which we call meet, and $\vee$ (on A), which we define as join, and a unary operation $'$, defined as complement, and two distinguished elements 0 and 1, satisfying the following axioms:

(1)
$$0' = 1 \text{ and } 1' = 0$$
(2)
$$p \wedge 0 = 0 \text{ and } p \vee 1 = 1$$
(3)
$$p \vee 0 = p \text{ and } p \wedge 1 = p$$
(4)
$$p \wedge p' = 0 \text{ and } p \vee p' = 1$$
(5)
$$(p')' = p$$
(6)
$$p \wedge p = p \text{ and } p \vee p = p$$
(7)
$$(p \wedge q)' = p' \vee q' \text{ and } (p \vee q)' = p' \wedge q'$$
(8)
$$p \wedge q = q \wedge p \text{ and } p \vee q = q \vee p$$
(9)
$$p \wedge (q \wedge r) = (p \wedge q) \wedge r \text{ and } p \vee (q \vee r) = (p \vee q) \vee r$$
(10)
$$p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r) \text{ and } p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$$

As a first comment, though sufficient, this set of axioms has been proven by the literature to be wastefully large. It is possible to pick a subset of these axioms in a way that the ones chosen imply all the other ones left out. Huntington, for instance, pointed out that the third, the fourth, the eighth, and the tenth axioms are enough to deduce the rest. Still, proving this requires rather refined play with the axioms chosen, making up for quite an exercise in axiomatics, which we chose to avoid in this introduction.

Also, once these operations are defined, it is always possible to define new operations based on them. An example would be the Boolean sum $+$ where $p + q = (p \wedge q') \vee (q \wedge p')$. Furthermore, it is also possible to define meet in terms of join and complement with $p \wedge q = (p' \vee q')'$.

Convention establishes that the order of performing operations without any brackets is the following: complements take priority over meets and joins, while meets take priority over joins. As an example, $p' \vee q \wedge p$ should be read as $(p') \vee (q \wedge p)$.

Definition 1.2. A Boolean homomorphism is a mapping f from a Boolean algebra B to a Boolean algebra A such that

(1)
$$f(p \wedge q) = f(p) \wedge f(q)$$
(2)
$$f(p \vee q) = f(p) \vee f(q)$$

(3)
$$f(p') = f(p)'$$

It is interesting to note that since meet, join and complement are preserved in the homomorphism, so are all Boolean operations defined on their terms. The confirmation of this is just a matter of some very simple computation, which is left to the reader. Furthermore, since $\wedge$ is definable in terms of $\vee$ and $'$, then it becomes redundant in the definition of homomorphism to include meet.

Another important remark is that the range of f is already implied to be a Boolean algebra by the properties in the definition of homomorphism. To see that, it is only necessary to imagine a surjective f with the properties described as a map from a Boolean algebra B to an arbitrary algebraic structure with the binary operations of $\wedge$and $\vee$and the unary operation $'$. It is necessary to check that the Boolean algebra axioms hold with $f(0) = 0$ and $f(1) = 1$ in A. Here we show one of the computations required, as the other ones proceed in a similar fashion. Let us verify the distributive law for meet over join. We are given elements u, v, and w of A. By the assumption of surjectivity, it is the case that there exist in B elements p, q, and r such that $f(p) = u$, $f(q) = v$, and $f(r) = w$. We now use the homomorphism properties and the distributive law in B to make the following statements:

$$u\wedge(v \vee w) = f(p)\wedge(f(q) \vee f(r)) = f(p)\wedge f(q \vee r) = f(p \wedge (q \vee r)) = f((p \wedge q) \vee (p \wedge r))$$
$$= f(p \wedge q) \vee f(p \wedge r) = (f(p) \wedge f(q)) \vee (f(p) \wedge f(r)) = (u \wedge v) \vee (u \wedge w)$$

Lastly, we just note that in the Boolean algebra of the range of f, $f(0) = 0$ by the fact that $f(p \wedge p') = f(p) \wedge f(p') = f(p) \wedge f(p)' = 0$ and that $f(1) = 1$ since $f(p \vee p') = f(p) \vee f(p') = f(p) \vee f(p)' = 1$.

Now that the basics of homomorphisms have been laid out, we turn our discussion to congruences, which are an important aspect of the study of Boolean algebras. They allow for pasting together elements of an algebra to form new structures that are in some way similar to the original algebra but somewhat simpler. In that spirit, we define a Boolean congruence to be the following:

Definition 1.3. A Boolean congruence relation is defined to be an equivalence relation on a Boolean algebra B that preserves the operations of meet, join, and complement. In other words it is a binary relation Θ that is reflexive, symmetric, and transitive in the sense that:

(1)
$$p \equiv p \, mod \, \Theta \; \forall p \in B$$

(2)
$$p \equiv q \, mod \, \Theta \Rightarrow q \equiv p \, mod \, \Theta \; \forall p, q \in B$$

(3)
$$p \equiv q \, mod \, \Theta \, \text{and} \, q \equiv r \, mod \, \Theta \Rightarrow p \equiv r \, mod \, \Theta \; \forall p, q, r \in B$$

and also whenever $p \equiv r \, mod \, \Theta$ and $q \equiv s \, mod \, \Theta$ the following still hold:

(4)
$$p \wedge q \equiv r \wedge s \, mod \, \Theta$$

(5)
$$p \vee q \equiv r \vee s \, mod \, \Theta$$

(6)
$$p' \equiv r' \, mod \, \Theta$$

It is worthwhile to point out once again that since meet, join and complement are preserved in the congruence, one can also deduce that other Boolean operations definable in terms of these three would also be preserved in the congruence relation. We leave it to the reader to prove it using the stated definitions in the case of $+$, for instance.

Now, we note that the equivalence classes of the congruence take the form $p/\Theta = \{q \in B : p \equiv q \, mod \, \Theta\}$ and that reflexivity implies that $p/\Theta = q/\Theta$ if and only if $p \equiv q \, mod \Theta$, making any two classes either equal or disjoint. Also, since the congruence preserves the operations of meet, join, and complement, it is possible to define the said operations on the set of equivalence classes of Θ in the following fashion:

(1)
$$(p/\Theta) \wedge (q/\Theta) = (p \wedge q)/\Theta$$

(2)
$$(p/\Theta) \vee (q/\Theta) = (p \vee q)/\Theta$$

(3)
$$(p/\Theta)' = (p)'/\Theta$$

Of course, it must be checked that these operations are well defined and thus do not depend upon the choice of particular elements of the equivalence classes. These checks are not particularly difficult and in this paper we show the case of $\wedge$ and let the reader proceed with the remaining operations in an analogous fashion. Suppose $p/\Theta = r/\Theta$ and that $q/\Theta = s/\Theta$. So both $p \equiv r \, mod \Theta$ and $q \equiv s \, mod \Theta$, which implies, as we know, that $p \wedge q \equiv r \wedge s \, mod \, \Theta$, so that $(p \wedge q)/\Theta = (r \wedge s)/\Theta$. This is enough to conclude that the particular choice of elements from the equivalence classes does not matter for this operation.

The set of all equivalence classes of Θ will be denoted by as B/Θ, and under the defined operations with the elements of the equivalence classes, it becomes a Boolean algebra, and, in this particular case, it is called the quotient of B modulo Θ. To prove this, one way would be to check all the necessary axioms of Boolean algebras, and here we will provide the example of commutativity of meet since the others all follow in a similar style:

$$(p/\Theta) \wedge (q/\Theta) = (p \wedge q)/\Theta = (q \wedge p)/\Theta = (q/\Theta) \wedge (p/\Theta)$$

Where the first and last equality use the first definition of the operations and the last middle one uses commutativity in the Boolean algebra.

We now know that every Boolean congruence determines its equivalence classes, and it would be profitable now to turn to a closer examination of the congruence class of 0, which is called the kernel of the congruence. There is a very fortunate state of affairs that, not only does a Boolean congruence Θ determine its kernel but the kernel of Θ also determines the congruence entirely. This fact is due to what we know of the Boolean sum $+$. Since $p \equiv q \, mod \, \Theta$ implies $p + q \equiv q + q \, mod \, \Theta$, and, as we know, $q + q = 0$ for any q, we have $p + q \equiv 0 mod \, \Theta$ is implied by $p \equiv q mod \, \Theta$. For the converse it is only necessary to proceed in similar fashion with $p + q \equiv 0 \, mod \, \Theta$ by Boolean adding q to both sides and obtaining that $p \equiv q \, mod \, \Theta$. This all boils down to the fact that $p \equiv q \, mod \, \Theta$ if and only if $p + q \equiv 0 \, mod \, \Theta$. From the discussion on the kernel of a Boolean congruence and what has been discussed of congruences so far, it is clear that:

$$0 \equiv 0 \, mod \, \Theta$$

If $p \equiv 0 \, mod \, \Theta$ and $q \equiv 0 \, mod \, \Theta$, then $p \vee q \equiv 0 \, mod \, \Theta$

If $p \equiv 0 \, mod \, \Theta$ and $q \in B$, then $p \wedge q \equiv 0 \, mod \, \Theta$

Inspired by these properties, we proceed to define a Boolean ideal in the following fashion:

Definition 1.4. A Boolean ideal in a Boolean algebra B is a subset $M \subseteq B$ such that

(1)
$$0 \in M$$

(2)
$$\text{if } p \in M \text{ and } q \in M, \text{ then } p \vee q \in M$$

(3)
$$\text{if } p \in M \text{ and } q \in B, \text{ then } p \wedge q \in M$$

Note that any ideal M is closed under the Boolean operation $+$. If p and q are elements of M, then by the third statement of the definition of a Boolean ideal, so are the meets $p \wedge q'$ and $q \wedge p'$, and hence the join $(p \wedge q') \vee (q \wedge p') \in M$, which is exactly the definition of Boolean addition $+$. Finally, it is worthwhile to say that the third statement of the definition above also implies that a Boolean ideal is closed under meet $\wedge$.

In the discussion of congruences and their kernels, we point out that the kernel of a Boolean congruence is itself an ideal and that any ideal M determines a unique congruence of which it is the kernel. Details of the verification of this fact are left to the reader since they are really no more than basic definitions and straightforward computation.

That said, it is possible to compute directly from the kernel M of a congruence Θ all the equivalence classes of the congruence.

Proposition 1.5. *For an arbitrary element p of B and a congruence Θ, the equivalence class p/Θ coincides with the coset $p + M = \{p + r \, : \, r \in M\}$.*

Proof. It is only necessary to check that the two sets in question have the same elements. If q is in B, then

$$q \in p/\Theta \text{ if and only if } p \equiv q \, mod \, \Theta$$

. We know that $p \equiv q \, mod \, \Theta$ if and only if $q \in p/\Theta$, so that

$$q \in p/\Theta \text{ if and only if } \; p + q \in M$$

by the properties discussed of Boolean sums and the kernel. Therefore

$$q \in p/\Theta \; if \; and \; only \; if \; q \in p + M$$

since if $p+q \in M$, then $p+r \in p+M$, for $r = p+q$, since $q = 0+q = p+p+q = p+r$.

Conversely, if $q \in p + M$, then $q = p + r$ for some element $r \in M$. But since $p + q = p + p + r = 0 + r = r$, it follows that $p + q \in M$, finishing the proof □

Additionally, it is worthy of note that the operations in the quotient algebra B/Θ can therefore be expressed in terms of the cosets in the following manner:

$$(p+M)\wedge(q+M)=(p\wedge q)+M$$
$$(p+M)\vee(q+M)=(p\vee q)+M$$
$$(p+M)'=p'+M$$

The Boolean algebra of the cosets under the operations just defined is identical to the Boolean algebra of the equivalence classes of Θ. It is called the quotient algebra of B modulo the ideal M. Notation will thus be B/M for the quotient, p/M for the coset $p+M$, and $p \equiv q \, mod \, M$ for $p \equiv q \, mod \, \Theta$. Furthermore, we will substitute the discussion of ideals for that of congruences and the discussion of cosets for that of equivalence classes, since at this point we now established that they proxy one another. There will be only one exception to this two pages from this point.

It is now worthwhile to briefly introduce two definitions that will be important for some intermediate proofs in the discussion of Stone's result. The first being a partial order $\leq$ in a Boolean algebra B and the second that of a supremum $\vee F$ of a subset F of a Boolean algebra B.

Definition 1.6. For elements p and q of a Boolean Algebra B, it is said that $q \leq p$ if and only if $p \wedge q = q$.

Definition 1.7. For any subset F of a Boolean Algebra B, we say that $\vee F$ exists and equals $p \in B$ if for every element a of F, $a \leq p$ is satisfied and for every element $q \in B$ that satisfies $a \leq q$ for all $a \in F$, it happens that $p \leq q$.

Furthermore, the intersection of every family of ideals in a Boolean algebra B is itself an ideal, and a proof of that would just consist of verifying that the three conditions in the definition of ideal are satisfied by the intersection. Here we show that $if \, p \in M \, \text{and} \, q \in M$, then $p \vee q \in M$ is satisfied and the remaining two to the reader. Let p and q be elements in the intersection of a family of ideals. Since every ideal in the family contains both p and q, then each of them will contain the join $p \vee q$, so that the join is in the intersection. Other conditions follow in an analogous fashion.

A consequence of this fact is that for an arbitrary subset E of B, the intersection of the family of all ideals that happen to include E is also an ideal (as a quick side note, for any subset E of B the improper ideal B contains E). In fact, it is the minimal one to contain E. This ideal M described, in this case, is called the ideal generated by E.

Theorem 1.8. *An element p of a Boolean algebra is in the ideal generated by a set E if and only if there is a finite subset F of E such that $p \leq \vee F$.*

Proof. Let M be the ideal generated by a subset E of a Boolean algebra B and let N be the set of elements p in B such that p is below the join of some finite subset F of E. In this case, we take a quick detour to show that this join is $\vee F$ as defined for a finite set. That it is an upper bound is clear, so that it is left to show it is the least upper bound. For any element r to dominate both p and q, we just use the elementary property $p \leq r$ and $q \leq r$ implying $q \vee p \leq r \vee r = r$ and have the fact established. The aim now is to show that M and N have the same elements. By the definition of ideal, we have that the join of any finite subset of

E is in M, and consequently every element below such a join is in M, since the statements $if\, p \in M\, and\, q \leq p,\, then\, q \in M$ and $if\, p \in M\, and\, q \in B,\, then\, p \wedge q \in M$ are equivalent by the definition of order $\leq$. This is to say that $q \leq p$ implies $q = q \wedge p \in M$. This gives that N is a subset of M. Reverse inclusion follows by demonstrating that N is an ideal and that, as it includes E, it must contain M. Consider the conditions stated in the definition of ideal. Since the empty set is a finite subset of E and $\vee\emptyset$ is 0, then $\emptyset$ belongs to N. If p and q are elements of N then there are subsets F and G of E such that $p \leq \vee F$ and $q \leq \vee G$. The set $H = F \cup G$ is a finite subset of E, and $p \vee q$ is certainly below $\vee H$, by monotonicity. We have established that $p \vee q$ is in N. Finally, if p is an element of N, as an element below the join (supremum) of some finite subset F of E, then any element $q \in B$ that is below p is also below $\vee F$, since $q = q \wedge p \leq \vee F$, and therefore is in N by the definition of N. Thus, it follows that N satisfies all conditions necessary to be an ideal. □

Lemma 1.9. *Let M be an ideal, and p_0 an element in a Boolean algebra B. The ideal generated by $M \cup \{p_0\}$ is the set $N = \{p \vee q : p \leq p_0\, and\, q \in M\}$.*

Proof. Let $E = M \cup \{p_0\}$and consider the preceding theorem. An element r of the Boolean algebra is in the ideal generated by E only in the case that there is a finite subset F of E such that $r \leq \vee F$. Without loss of generality, we consider that F contains the element p_0 (adding it in would only make the join bigger). Also, since M is closed under join, it is possible to combine all the members of F that are also in M into a single element. This gives that r is in the ideal generated by E if and only if there is an element s in M such that $r \leq s \vee p_0$. This inequality, however, holds by the definition of the order relation only if $r = r \wedge (s \vee p_0) = (r \wedge s) \vee (r \wedge p_0)$. The element $q = r \wedge s$ is a member of M and the element $p = r \wedge p_0$ is below p_0. Therefore, r is in the ideal generated by E if and only if $r = q \vee p$ for some $q \in M$ and $p \leq p_0$. □

Corollary 1.10. *Let M be an ideal and p_0 an element in a Boolean algebra B. If p_0' is not in M, then the ideal generated by $M \cup \{p_0\}$ is proper.*

Proof. The argument goes by contradiction. Let N be the ideal generated by $M \cup \{p_0\}$, and assume N is improper. Since $N = B$, it must contain p_0'. Thus, by the preceding lemma, there must be $p \leq p_0$ and $q \in M$ such that $p_0' = p \vee q$. Now we establish that $p_0' \leq q$ via the following considerations:

$$p_0' = p_0' \wedge p_0' = p_0' \wedge (p \vee q) = (p_0' \wedge p) \vee (p_0' \wedge q) \leq (p_0' \wedge p_0) \vee (p_0' \wedge q) = 0 \vee (p_0' \wedge q) = p_0' \wedge q$$

But we know that $p_0' \wedge q \leq q$ and since $p \leq p_0$ implies that $p_0' \wedge p \leq p_0' \wedge p_0$Thus, p_0' is in M. □

We now proceed to a discussion on maximal ideals.

Definition 1.11. An ideal is maximal if and only if it is a proper ideal that is not contained in any other proper ideal. A maximal ideal M in a Boolean Algebra B is such that $M \neq B$ and for any other ideal A that satisfies $M \subseteq A$ if happens that either $A = M$ or $A = B$

Lemma 1.12. *An ideal M in a Boolean Algebra B is maximal if and only if either p or p' is in M, but not both, for every p in B.*

Proof. Assume that, for some p in B, neither p nor p' is in M. If N is the ideal generated by $\{M\} \cup p$, then N is a proper ideal by a preceding corollary, and it properly includes M since it contains p. Consequently, M is not maximal. Now, to prove the converse, assume that p or p' is in M for every $p \in B$. Suppose further, that N is an ideal that properly includes M. Since $N \neq M$ there is an element p in N that does not belong to M. The assumption implies that p' is in M, so that both p and p' belong to N. This means, by the properties of ideals, that $p \vee p' = 1$ is in N, making it equal to the Boolean algebra B. □

Theorem 1.13. *(Maximal Ideal Theorem). Every proper ideal in a Boolean algebra is included in a maximal ideal.*

Proof. Presented at the end of this paper. □

Theorem 1.14. *(First Isomorphism Theorem). If f is a Boolean surjective homomorphism from B to A, and if M is the kernel of f, then B/M is isomorphic to A via the mapping*

$$p/M \to f(p)$$

Proof. Let p and q be elements of B. It clearly follows from the facts about congruence relations and homomorphisms that

$$f(p) = f(q) \text{ if and only if } p/M = q/M$$

because

$$f(p) = f(q) \text{ if and only if } f(p) + f(q) = 0$$

given the definition of the Boolean sum $+$. Then

$$f(p) = f(q) \text{ if and only if } f(p+q) = 0$$

because f is a homomorphism, and

$$f(p) = f(q) \text{ if and only if } p + q \in M.$$

Thus by the facts about congruences

$$f(p) = f(q) \text{ if and only if } p/M = q/M.$$

Let h be the mapping from B/M into A that takes each coset p/M to the image $f(p)$. The work done already shows that h is well defined and is injective. It also is surjective because f maps B onto A and M is the kernel of f. It is now left to show that f is a homomorphism, i.e. it is enough to show that it preserves meet and complement. From what has been said about homomorphisms, meet and complement in the quotient algebra B/M, and the definition of h:

$$h((p/M) \wedge (q/M)) = h(p \wedge q/M) = f(p \wedge q) =$$

$$= f(p) \wedge f(q) = h(p/M) \wedge h(q/M)$$

and

$$h\left((p/M)'\right) = h(p'/M) = f(p') = f(p)' = h(p/M)'$$

Therefore the proof is completed. □

We now state, without the proof, which would prove to be rather lengthy, a famous result from group theory adapted to the context of Boolean algebras:

Theorem 1.15. *For every ideal M in a Boolean algebra B, the correspondence $N \to N/M$ is a bijection from the class of ideals in B that contain M to the class of ideals in B/M.*

Theorem 1.16. *Let M and N be ideals in a Boolean algebra B, with $M \subseteq N$. The quotient B/M by the ideal N/M is isomorphic to the quotient B/N via the mapping*

$$(p/M) / (N/M) \to p/N.$$

Proof. Write

$$A = B/M \quad and \quad C = (B/M) / (N/M)$$

The projection f from B to A and the projection g from A to C are both surjective so that the composition $h = g \circ f$ is also surjective. We proceed to verify that the kernel of the composition projection h is N in two steps. By the operations of the quotient algebra, the kernel of g is the ideal N/M, and the set of elements of B that are mapped into N/M by f is just

$$f^{-1} (N/M) = f^{-1} (f (N)) = N$$

The first isomorphism theorem, applied to the map h, says that the quotient B/N is isomorphic to C through the homomorphism that sends each coset p/N to $h (p)$. Now it is only necessary to finish with the remark that

$$h (p) = g (f (p)) = g (p/M) = (p/M) / (N/M)$$

□

Corollary 1.17. *Let f_0 be a Boolean homomorphism from B into A_0 and suppose that its kernel includes the ideal M. There is then a unique homomorphism g from B/M into A_0 such that $f_0 = g \circ f$ where f is the projection from B to B/M.*

Proof. Let A be the image of B under f_0, and M_0 the kernel of f_0. By assumption, $M \subseteq M_0$. We know by the First Isomorphism Theorem that B/M_0 is isomorphic to A via the function g_0 that maps each coset p/M_0 to $f_0 (p)$. Clearly it follows that g_0 is an injective map from B/M into A. The projection f of B onto B/M is surjective as is the projection g_2 of B/M onto $(B/M) / (M_0/M)$. The latter quotient is isomorphic to B/M_0 through the function g_1 that maps $(p/M) / (M_0/M)$ to p/M_0 by the preceding theorem. So, the composition $g = g_0 \circ g_1 \circ g_2$ is a homomorphism from B/M into A_0 with the property that $f_0 = g \circ f$. This can be shown by the following computation:

$$g (p/M) = g_0 \circ g_1 \circ g_2 (p/M) = g_0 \circ g_1 ((p/M) / (M_0/M)) = g_0 (p/M_0) = f_0 (p)$$

Finally, to prove uniqueness of g, consider any homomorphism h from B/M into A_0 with the property that $f_0 = h \circ f$. It follows from the assumption and definition of f that $h (p/M) = h (f (p)) = f_0 (p)$ for each coset p/M so that h coincides with g. □

Corollary 1.18. *An ideal in a non-degenerate Boolean algebra B is maximal if and only if B/M is isomorphic to 2.*

Proof. A Boolean algebra is called simple if it is non-degenerate and has no non-trivial proper ideals. The correspondence between the ideals of a quotient algebra and the ideals of B shows that the quotient algebra is simple if and only if M is maximal. In slightly different words, a Boolean quotient B/M is not simple and not degenerate if and only if it has a proper, non-trivial ideal. Again invoking the correspondence theorem, this can be the case if and only if there is an ideal N in B that is between M and B but is different from both. This ideal exists if and only if M is not maximal and proper, by the Maximal Ideal Theorem. In the case of Boolean algebras, it turns out that 2 is the only of such. The algebra 2 is simple since its only two ideals are $\{0\}$ and $\{0, 1\}$. Now assuming that B is some simple Boolean algebra and considering a non-zero element p of B, the ideal generated by it is non-trivial and therefore must be improper (by the simplicity of B). This can only happen if $p = 1$, thus implying that any element of B different from 0 must be 1. For if p is any element different from 1, then the ideal generated by it is included in a maximal ideal and neither of these contain p', so that 1 is not in it, thus making the ideal be proper. Therefore $B = 2$. □

Lemma 1.19. *For every non-zero element p of every Boolean algebra A, there is a 2-valued homomorphism x on A such that $x(p) = 1$.*

Proof. Let p be a non-zero element in a Boolean algebra and consider the principal ideal N generated by the element p'. The elements in N are just the elements j of A that are $j \leq p'$. Since p is not 0, then p' is not 1, and thus 1 is not in N, making N a proper ideal. Extend, by the Theorem of Maximal Ideals, the ideal N to a maximal ideal M. This ideal does not contain p by the lemma 12. Furthermore, as a consequence of the First Isomorphism Theorem and related results, the quotient A/M is a two-element Boolean algebra. If z is the projection from A to A/M that maps each element q of A to the coset q/M, and if y is the unique isomorphism from A/M to 2 that maps $0/M$ to 0, and $1/M$ to 1, as by Corollary 17, then $x = y \circ z$ is the desired 2-valued homomorphism on A. □

Theorem 1.20. *(Stone Representation Theorem for Boolean Algebras) Let X be the set of 2-valued homomorphisms on a Boolean algebra A. Then A is embeddable into $\mathcal{P}(X)$ (notation as discussed in the introduction) via the mapping defined by*

$$f(p) = \{x \in X : x(p) = 1\}$$

Proof. We have first to verify that $f(p)$ is indeed a homomorphism. In checking for the realization of the necessary properties, we begin with the operation of meet:

$$f(p \vee q) = \{x \in X : x(p \vee q) = 1\}$$

by the definition of f.

$$f(p \vee q) = \{x \in X : x(p) \vee x(q) = 1\}$$

by the property of the homomorphism x. This equals

$$\{x \in X : x(p) = 1 \, or \, x(q) = 1\}$$

through the definition of meet in the Boolean ring 2. Thus

$$= \{x \in X : x(p) = 1\} \cup \{x \in X : x(q) = 1\}$$

reusing the definition of f.

We now proceed to check the property for complementation:

$$\begin{aligned} f(p') &= \{x \in X : x(p') = 1\} \\ &= \left\{x \in X : x(p)' = 1\right\} \\ &= \{x \in X : x(p) = 0\} \\ &= \{x \in X : x(p) = 1\}' \\ &= f(p)' \end{aligned}$$

Since $p \wedge q = (p' \vee q')'$, then checking the condition for meets becomes a purely mechanical and unnecessary task. Now we have to show that the mapping f is one-to-one. This can be accomplished by the use of the preceding lemma. If $p \neq 0$, then there exists a 2-valued homomorphism x on A such that $x(p) = 1$ as guaranteed by the lemma. It follows that the set $f(p) \neq \emptyset$, which in turn is the 0 element of $\mathcal{P}(X)$, leading to the conclusion that the kernel of this homomorphism consists of 0 alone thus making f injective. □

We now state a corollary that makes a remark about the fact that the image of f is a Boolean algebra and its elements are all in $\mathcal{P}(X)$, thus forming a subalgebra of it, i.e. a field of sets.

Corollary 1.21. *Every Boolean algebra is isomorphic to a field of sets.*

2. Appendix

We now restate and prove the Maximal Ideal Theorem

Theorem 2.1. *(Maximal Ideal Theorem) Every proper ideal in a Boolean algebra is included in a maximal ideal.*

Proof. Let M be a proper ideal in a Boolean algebra B. Enumerate the elements of B in a possibly transfinite sequence $\{p_i\}_{i<\alpha}$ indexed by the set of ordinals less than some cardinal α. We now create a sequence $\{M_i\}_{i\leq\alpha}$ of proper ideals of B with the following properties: (1) $M_0 = M$; (2) $M_i \subseteq M_j$ whenever $i \leq j \leq \alpha$; (3) either p_i or p_i' is in M_{i+1} for every $i < \alpha$. The definition of the sequence proceed by induction on the ordinal numbers.

Let $M_0 = M$. So M_0 is a proper ideal by assumption, thus satisfying (1) automatically as (2) and (3) would also automatically hold for $\{M_i\}_{i\leq 0}$. As to the inductive step, we take an ordinal $\kappa \leq \alpha$, and suppose that the proper ideals M_i have been defined for every $i < \kappa$ so that conditions (1), (2), and (3) are satisfied for the whole family of $\{M_i\}_{i<\kappa}$ (changing α for κ in (1) and (2) and with $i+1 < \kappa$ in (3)). When κ is a successor ordinal, i.e. $\kappa = i + 1$, we split the definition in two cases. If either p_i or p_i' is in M_i, let $M_\kappa = M_i$; if that is not the case, define M_κ to be the ideal generated by the set $M_i \cup \{p_i\}$. We know that the ideal M_κ is proper, either from the corollary preceding the statement of the theorem (latter case) or the induction hypothesis (former case). If κ is a limit ordinal, put $M_\kappa = \cup_{i<\kappa} M_i$. This ideal is proper since the union of a non-empty directed family of ideals in a Boolean algebra is itself an ideal, which is proper if and only if each ideal in the family is proper, which happily happens to be the case (for more on this, refer to

Halmos and Givant, page 168). It is now left to check that the conditions (1)-(3) (with α replace by κ) hold for the family $\{M_i\}_{i \leq \kappa}$. The ideal M_α is the called-for maximal extension of M. It is a proper ideal by construction, and by conditions (1) and (2) is an extension of M. We now verify maximality by taking an arbitrary element p in B. This element certainly occurs in the enumeration of the elements of B, say $p = p_i$. By (3), either p_i or its complement p_i' is in M_{i+1}, so that either p or p' is in M_α by condition (2). Both cannot be in M_α, since that would make M_α improper. By the first lemma in the present discussion of maximal ideals, M_α is maximal. □

Acknowledgements. It is a pleasure to thank my mentor, Jonathan Wang, for his crucial support throughout this project and providing answers to my LaTeX questions. Without his help, the author of this paper would have been egregiously lost. Also, it is with delight and deepest respect that I thank Professor May for all his effort in organizing this amazing and altogether unique summer program, to the joy and mathematical advancement of all involved.

References

[1] Paul Halmos and Steven Givant An Introduction to Boolean Algebras Springer. 2007.
[2] M. H. Stone The Representation of Boolean Algebras. Bulletin of the American Mathematical Society Volume 44, Number 12, Part 1, pages 807-816. 1938.
[3] E. V. Huntington Sets of independent postulates for the algebra of logic. Transactions of the American Mathematical Society, Volume 5, pages 288-309. 1904.