1
Sets, Functions, and Relations

1.1 Sets, Valuations, and Boolean Algebras

We shall usually work with finite sets. If A is a finite set, let $|A|$ be the number of elements in A. The function $|\cdot|$ satisfies the functional equation

$$|A \cup B| + |A \cap B| = |A| + |B|.$$

The function $|\cdot|$ is one of many functions measuring the "size" of a set. Let v be a function from a collection $\mathcal{C}$ of sets to an algebraic structure $\mathbb{A}$ (such as an Abelian group or the nonnegative real numbers) on which a commutative binary operation analogous to addition is defined. Then v is a *valuation* if for sets A and B in $\mathcal{C}$,

$$v(A \cup B) + v(A \cap B) = v(A) + v(B),$$

whenever the union $A \cup B$ and the intersection $A \cap B$ are in $\mathcal{C}$.

Sets can be combined algebraically and sometimes two sets can be compared with each other. The operations of union $\cup$ and intersection $\cap$ are two basic algebraic binary operations on sets. In addition, if we fix a universal set S containing all the sets we will consider, then we have the unary operation A^c of *complementation,* defined by

$$A^c = S \backslash A = \{a\colon a \in S \text{ and } a \notin A\}.$$

Sets are partially ordered by containment. A collection $\mathcal{C}$ of subsets is a *ring of sets* if $\mathcal{C}$ is closed under unions and intersections. If, in addition, all the sets in $\mathcal{C}$ are subsets of a universal set and $\mathcal{C}$ is closed under complementation, then $\mathcal{C}$ is a *field of sets*. The collection 2^S of all subsets of the set S is a field of sets.

Boolean algebras capture the algebraic and order structure of fields of sets. The axioms of a Boolean algebra abstract the properties of union, intersection,

and complementation, without any mention of elements or points. As John von Neumann put it, the theory of Boolean algebras is "pointless" set theory.

A *Boolean algebra* P is a set with two binary operations, the *join* $\vee$ and the *meet* $\wedge$; a unary operation, *complementation* $\cdot^c$; and two nullary operations or constants, the *minimum* $\hat{0}$ and the *maximum* $\hat{1}$. The binary operations $\vee$ and $\wedge$ satisfy the *lattice axioms*:

L1. Idempotency: $x \vee x = x, \quad x \wedge x = x.$
L2. Commutativity: $x \vee y = y \vee x, \quad x \wedge y = y \wedge x.$
L3. Associativity: $x \vee (y \vee z) = (x \vee y) \vee z, \quad x \wedge (y \wedge z) = (x \wedge y) \wedge z.$
L4. Absorption: $x \wedge (x \vee y) = x, \quad x \vee (x \wedge y) = x.$

Joins and meets also satisfy the *distributive axioms*

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

In addition, the five operations satisfy the *De Morgan laws*

$$(x \vee y)^c = x^c \wedge y^c, \quad (x \wedge y)^c = x^c \vee y^c,$$

two pairs of rules concerning complementation

$$x \vee x^c = \hat{1}, \quad x \wedge x^c = \hat{0}$$

and

$$\hat{0} \neq \hat{1}, \quad \hat{1}^c = \hat{0}, \quad \hat{0}^c = \hat{1}.$$

It follows from the axioms that complementation is an involution; that is, $(x^c)^c = x$. The smallest Boolean algebra is the algebra $\underline{2}$ with two elements $\hat{0}$ and $\hat{1}$, thought of as the *truth values* "false" and "true." The axioms are, more or less, those given by George Boole. Boole, perhaps the greatest simplifier in history, called these axioms "the laws of thought."[1] He may be right, at least for silicon-based intelligence.

A *lattice* is a set L with two binary operations $\vee$ and $\wedge$ satisfying axioms L1–L4. A *partially ordered set* or *poset* is a set P with a relation $\leq$ (or $\leq_P$ when we need to be clear which partial order is under discussion) satisfying three axioms:

PO1. Reflexivity: $x \leq x$.
PO2. Transitivity: $x \leq y$ and $y \leq z$ imply $x \leq z$.
PO3. Antisymmetry: $x \leq y$ and $y \leq x$ imply $x = y$.

[1] Boole (1854). For careful historical studies, see, for example, Hailperin (1986) and Smith (1982).

The *order-dual* $P^{\downarrow}$ is the partial order obtained from P by inverting the order; that is,

$$x \leq_{P^{\downarrow}} y \quad \text{if and only if} \quad y \leq_P x.$$

Sets are partially ordered by containment. This order relation is not explicit in a Boolean algebra, but can be defined by using the meet or the join. More generally, in a lattice L, we can define a partial order $\leq_L$ compatible with the lattice operations on L by $x \leq_L y$ if and only if $x \wedge y = x$. Using the absorption axiom L4, it is easy to prove that $x \wedge y = x$ if and only if $x \vee y = y$; thus, the following three conditions are equivalent:

$$x \leq_L y, \quad x \wedge y = x, \quad x \vee y = y.$$

The join $x \vee y$ is the *supremum* or *least upper bound* of x and y in the partial order $\leq_L$; that is, $x \vee y \geq_L x$, $x \vee y \geq_L y$, and if $z \geq_L x$ and $z \geq_L y$, then $z \geq_L x \vee y$. The meet $x \wedge y$ is the *infimum* or *greatest lower bound* of x and y. Supremums and infimums can be defined for arbitrary sets in partial orders, but they need not exist, even when the partial order is defined from a lattice. However, supremums and infimums of finite sets always exist in lattices.

By the De Morgan laws, the complementation map $x \mapsto x^c$ from a Boolean algebra P to itself exchanges the operations $\vee$ and $\wedge$. This gives an (order) duality: if a statement P about Boolean algebra holds for all Boolean algebras, then the statement $P^{\downarrow}$, obtained from P by the exchanges $x \leftrightarrow x^c$, $\wedge \leftrightarrow \vee$, $\leq \leftrightarrow \geq$, $\hat{0} \leftrightarrow \hat{1}$, is also valid over all Boolean algebras. A similar duality principle holds for statements about lattices.

We end this section with representation theorems for Boolean algebras as fields of subsets. Let P and Q be Boolean algebras. A function $\phi : P \to Q$ is a *Boolean homomorphism* or *morphism* if

$$\begin{aligned} \phi(x \vee y) &= \phi(x) \vee \phi(y) \\ \phi(x \wedge y) &= \phi(x) \wedge \phi(y) \\ \phi(x^c) &= (\phi(x))^c. \end{aligned}$$

1.1.1. Theorem. A finite Boolean algebra P is isomorphic to the Boolean algebra 2^S of all subsets of a finite set S.

Proof. An *atom* a in P is an element covering the minimum $\hat{0}$; that is, $a > \hat{0}$ and if $a \geq b > \hat{0}$, then $b = a$. Atoms correspond to one-element subsets. Let S be the set of atoms of B and $\psi : P \to 2^S$, $\phi : 2^S \to P$ be the functions defined by

$$\psi(x) = \{a \colon a \in S, a \leq x\}, \quad \phi(A) = \bigvee_{a \in A} a.$$

It is routine to check that both compositions $\psi\phi$ and $\phi\psi$ are identity functions and that ϕ and ψ are Boolean morphisms. □

The theorem is false if finiteness is not assumed. Two properties implied by finiteness are needed in the proof. A Boolean algebra P is *complete* if the supremum and infimum (with respect to the partial order $\leq$ defined by the lattice operations) exist for every subset (of any cardinality) of elements in P. It is *atomic* if every element x in P is a supremum of atoms. The proof of Theorem 1.1.1 yields the following result.

1.1.2. Theorem. A Boolean algebra P is isomorphic to a Boolean algebra 2^S of *all* subsets of a set if and only if P is complete and atomic.

Theorem 1.1.2 says that not all Boolean algebras are of the form 2^S for some set S. For a specific example, let S be an infinite set. A subset in S is *cofinite* if its complement is finite. The *finite–cofinite Boolean algebra* on the set S is the Boolean algebra formed by the collection of all finite or cofinite subsets of S. The finite–cofinite algebra on an infinite set is atomic but not complete. Another example comes from analysis. The algebra of measurable sets of the real line, modulo the sets of measure zero, is a nonatomic Boolean algebra in which unions and intersections of countable families of equivalence classes of sets exist.

One might hope to represent a Boolean algebra as a field of subsets constructed from a topological space. The collection of open sets is a natural choice. However, because complements exist and complements of open sets are closed, we need to consider *clopen* sets, that is, sets that are both closed and open.

1.1.3. Lemma. The collection of clopen sets of a topological space is a field of subsets (and forms a Boolean algebra).

Since meets and joins are finitary operations, it is natural to require the topological space to be compact. A space X is *totally disconnected* if the only connected subspaces in X are single points. If we assume that X is compact and Hausdorff, then being totally connected is equivalent to each of the two conditions: (a) every open set is the union of clopen sets, or (b) if p and q are two points in X, then there exists a clopen set containing p but not q. A *Stone space* is a totally disconnected compact Hausdorff space.

1.1.4. The Stone representation theorem.[2] Every Boolean algebra can be represented as the field of clopen sets of a Stone space.

[2] Stone (1936).

There are two ways, topological or algebraic, to prove the Stone representation theorem. In both, the key step is to construct a Stone space X from a Boolean algebra P. A $\underline{2}$-*morphism* of P is a Boolean morphism from P onto the two-element Boolean algebra $\underline{2}$. Let X be the set of $\underline{2}$-morphisms of P. Regarding X as a (closed) subset of the space $\underline{2}^P$ of all functions from P into $\underline{2}$ with the product topology, we obtain a Stone space. Each element x in P defines a continuous function $X \to \underline{2}$, $f \mapsto f(x)$. Using this, we obtain a Boolean morphism from P into the Boolean algebra of clopen sets of X.

The algebraic approach regards a Boolean algebra P as a commutative ring, with addition defined by $x + y = (x \wedge y^c) \vee (x^c \wedge y)$ and multiplication defined by $xy = x \wedge y$. (Addition is an abstract version of symmetric difference of subsets.) Then the set of prime ideals $\mathrm{Spec}(P)$ of P is a topological space under the *Zariski topology*: the closed sets are the order filters in $\mathrm{Spec}(P)$ under set-containment. The order filters are also open, and hence clopen. Then the Boolean algebra P is isomorphic to the Boolean algebra of clopen sets of $\mathrm{Spec}(P)$. Note that in a ring constructed from a Boolean algebra, $2x = x + x = 0$ for all x. In such a ring, every prime ideal is maximal. Maximal ideals are in bijection with $\underline{2}$-morphisms and so $\mathrm{Spec}(P)$ and X are the same set (and less obviously, the same topological space).[3]

The Boolean operations on a field P of subsets of a universal set S can be modeled by addition and multiplication over a ring $\mathbb{A}$ using indicator (or characteristic) functions. If S is a universal set and $A \subseteq S$, then the *indicator function* χ_A *of* A is the function $S \to \mathbb{A}$ defined by

$$\chi_A(a) = \begin{cases} 1 & \text{if } a \in A, \\ 0 & \text{if } a \notin A. \end{cases}$$

The indicator function satisfies

$$\chi_{A \cap B}(a) = \chi_A(a)\chi_B(a),$$
$$\chi_{A \cup B}(a) = \chi_A(a) + \chi_B(a) - \chi_A(a)\chi_B(a).$$

When $\mathbb{A}$ is GF(2), the (algebraic) field of integers modulo 2, then the indicator function gives an injection from P to the vector space $\mathrm{GF}(2)^S$ of dimension $|S|$ with coordinates labeled by S. Since GF(2) is the Boolean algebra $\underline{2}$ as a ring, indicator functions also give an injection into the Boolean algebra $\underline{2}^{|S|}$. Indicator functions give another way to prove Theorem 1.1.1.

It will be useful to have the notion of a multiset. Informally, a multiset is a set in which elements can occur in multiple copies. For example, $\{a, a, b, a, b, c\}$

[3] See Halmos (1974) for the topological approach. A no-nonsense account of the algebraic approach is in Atiyah and MacDonald (1969, p. 14). See also Johnstone (1982).

is a multiset in which the element a occurs with multiplicity 3. One way to define multisets formally is to generalize indicator functions. If S is a universal set and $A \subseteq S$, then a *multiset* M is defined by a *multiplicity function* $\chi_M : S \to \mathbb{N}$ (where $\mathbb{N}$ is the set of nonnegative integers). The *support* of M is the subset $\{a \in S\colon \chi_M(a) > 0\}$. Unions and intersections of multisets are defined by

$$\chi_{A\cap B}(a) = \min\{\chi_A(a), \chi_B(a)\},$$
$$\chi_{A\cup B}(a) = \max\{\chi_A(a), \chi_B(a)\}.$$

We have defined union so that it coincides with set-union when both multisets are sets. We also have the notion of the *sum* of two multisets, defined by

$$\chi_{A+B}(a) = \chi_A(a) + \chi_B(a).$$

This sum is an analog of disjoint union for sets.

Exercises

1.1.1. *Distributive and shearing inequalities.*

Let L be a lattice. Prove that for all $x, y, z \in L$,

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

and

$$(x \wedge y) \vee (x \wedge z) \leq x \wedge (y \vee (x \wedge z)).$$

1.1.2. *Sublattices forbidden by the distributive axioms.*[4]

A *sublattice* of a lattice L is a subset of elements of L closed under meets and joins. Show that a lattice L is distributive if and only if L does not contain the *diamond* M_5 and the *pentagon* N_5 as a sublattice (see Figure 1.1).

1.1.3. *More on the distributive axioms.*

(a) Assuming the lattice axioms, show that the two identities in the distributive axioms imply each other. Show that each identity is equivalent to the self-dual identity

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

(b) Show that a lattice L is distributive if and only if for all $a, x, y \in L$, $a \vee x = a \vee y$ and $a \wedge x = a \wedge y$ imply $x = y$.

[4] Birkhoff (1934).

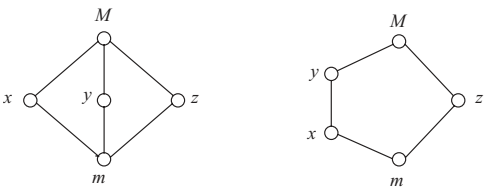

Figure 1.1 The diamond and the pentagon.

1.1.4. *Implication.*

Define the binary operation $\rightarrow$ of *implication* on a Boolean algebra P by

$$x \rightarrow y = x^c \vee y.$$

Show that the binary operation $\rightarrow$ and the constant $\hat{0}$ generate the operations $\vee, \wedge, \cdot^c$ and the constant $\hat{1}$. Give a set of axioms using $\rightarrow$ and $\hat{0}$.

1.1.5. *Conditional disjunction.*

Define the ternary operation $[x, y, z]$ of *conditional disjunction* by

$$[x, y, z] = (x \wedge y) \vee (y \wedge z) \vee (z \wedge x).$$

Note that $[x, y, z]$ is invariant under permutations of the variables. Show that $\vee$ and $\wedge$ can be defined using conditional disjunction and the constants $\hat{1}$ and $\hat{0}$. Find an elegant set of axioms for Boolean algebras using conditional disjunction and complementation.

1.1.6. *Huntington's axiom.*[5]

Show that a Boolean algebra P can be defined as a nonempty set with a binary operation $\vee$ and a unary operation $\cdot^c$ satisfying the following three axioms:

H1. $\vee$ is associative.
H2. $\vee$ is commutative.
H3. *Huntington's axiom:* For all x and y,

$$(x^c \vee y^c)^c \vee (x^c \vee y)^c = x.$$

1.1.7. *The Sheffer stroke.*[6]

Show that a Boolean algebra P can be defined as a set P with at least two elements with single binary operation $|$ satisfying the axioms:

Sh1. $(a|a)|(a|a) = a$.

[5] Huntington (1933). [6] Sheffer (1913).

Sh2. $a|(b|(b|b)) = a|a$.
Sh3. $(a|(b|c))|(a|(b|c)) = ((b|b)|a)|((c|c)|a)$.

1.1.8. Let S be the countable set $\{1/n\colon 1 \le n < \infty\}$ and consider the topological space $S \cup \{0\}$ with the topology induced from the real numbers. Show that the finite–cofinite algebra on S is the collection of open sets of $S \cup \{0\}$.

1.1.9. (a) Let $\mathcal{H}$ be the collection of all unions of a finite number of subsets of rational numbers of the following form:

$$\{r\colon r < b\},\ \{r\colon a \le r < b\},\ \text{or } \{r\colon a \le r\}.$$

Show that $\mathcal{H}$ is a countable Boolean algebra (under set-containment) with no atoms.

(b) Show that any two countable Boolean algebras with no atoms are isomorphic.

1.1.10. Is there a natural description of the Stone space of the Boolean algebra of measurable sets of real numbers modulo sets of measure zero?

1.1.11. *Infinite distributive axioms.*

The infinite distributive axioms for the lattice operations say

$$\bigwedge_{i\colon i\in I}\ \bigvee_{j\colon j\in J} x_{ij} = \bigvee_{f\colon f\colon I\to J}\ \bigwedge_{i\colon i\in I} x_{i,f(i)}, \qquad \bigvee_{i\colon i\in I}\ \bigwedge_{j\colon j\in J} x_{ij} = \bigwedge_{f\colon f\colon I\to J}\ \bigvee_{i\colon i\in I} x_{i,f(i)},$$

with f ranging over all functions from I to J. To see that this is the correct infinite extension, interpret $\wedge$ as multiplication and $\vee$ as addition. Then formally

$$(x_{11}+x_{12}+x_{13}+\cdots)(x_{21}+x_{22}+x_{23}+\cdots)(x_{31}+x_{32}+x_{33}+\cdots)\cdots = \sum_{f\colon f\colon I\to J} x_{1,f(1)}x_{2,f(2)}x_{3,f(3)}\cdots.$$

Prove the following theorem of Tarski.[7] Let P be a Boolean algebra. Then the following conditions are equivalent:

1. P is complete and satisfies the infinite distributivity axioms.
2. P is complete and atomic.
3. P is the Boolean algebra of all subsets of a set.

1.1.12. *Universal valuations for finite sets.*

Let S be a finite set, $\{x_a\colon a \in S\}$ be a set of variables, one for each element of S, x_0 be another variable, and $\mathbb{A}[\underline{x}]$ be the ring of polynomials in the

[7] Tarski (1929).

set of variables $\{x_a : a \in S\} \cup \{x_0\}$ with coefficients in a ring $\mathbb{A}$. Show that $v : 2^S \to \mathbb{A}[\underline{x}]$ defined by

$$v(A) = x_0 + \sum_{a : a \in A} x_a$$

is a valuation taking values in $\mathbb{A}[\underline{x}]$ and every valuation taking values in $\mathbb{A}$ can be obtained by assigning a value in $\mathbb{A}$ to each variable in $\{x_a : a \in S\} \cup \{x_0\}$.

1.2 Partially Ordered Sets

Let P be a partially ordered set. An element x *covers* the element y in the partially ordered set if $x > y$ and there is no element z in P such that $x > z > y$. An element m is *minimal* in the partial order P if there are no elements y in P such that $y < m$. A *maximal* element is a minimal element in the dual $P^{\downarrow}$.

Two elements x and y in P are *comparable* if $x \leq y$ or $y \leq x$; they are *incomparable* if neither $x \leq y$ nor $y \leq x$. A subset $C \subseteq P$ is a *chain* if any two elements in C are comparable. A subset $A \subseteq P$ is an *antichain* if any two elements in A are incomparable. If C is a finite chain and $|C| = n + 1$, then the elements in C can be *linearly ordered,* so that

$$x_0 < x_1 < x_2 < \cdots < x_n.$$

The *length* of the chain C is n, 1 less than the number of elements in C. A chain $x_0 < x_1 < \cdots < x_n$ in the partial order P is *maximal* or *saturated* if x_{i+1} covers x_i for $1 \leq i \leq n$. A function r defined from P to the nonnegative integers is a *rank function* if $r(x) = 0$ for every minimal element and $r(y) = r(x) + 1$ whenever y covers x. The partial order P is *ranked* if there exists a rank function on P. The *rank* of the entire partially ordered set P is the maximum $\max\{r(x) : x \in P\}$. If $x \leq y$ in P, the *interval* $[x, y]$ is the set $\{z : x \leq z \leq y\}$.

If P is finite, then we draw a picture of P by assigning a vertex or dot to each element of P and putting a directed edge or arrow from y to x if x covers y. Thinking of the arrows as flexible, we can draw the picture so that if $x > y$, then x is above y. It is not required that the edges do not cross each other. Helmut Hasse drew such pictures for field extensions. For this reason, pictures of partial orders are often called *Hasse diagrams*.

Let P and Q be partially ordered sets. A function $f : P \to Q$ is *order-preserving* if for elements x and y in P, $x \leq_P y$ implies $f(x) \leq_Q f(y)$. A function f is *order-reversing* if $x \leq_P y$ implies $f(x) \geq_Q f(y)$.

A subset $I \subseteq P$ is an *(order) ideal* of P if it is "down-closed;" that is, $y \leq x$ and $x \in I$ imply $y \in I$. Note that we do not require ideals to be closed under joins if P is a lattice. The union and intersection of an arbitrary collection of

ideals are ideals. There is a bijection between ideals and antichains: an ideal I is associated with the antichain $A(I)$ of maximal elements in I. If a is an element of P, then the set $I(a)$ defined by

$$I(a) = \{x\colon x \leq a\}$$

is an ideal. An ideal is *principal* if it has this form or, equivalently, if it has exactly one maximal element a. The element a *generates* the principal ideal $I(a)$.

If A is a set of elements of P, then the *ideal* $I(A)$ *generated by* A is the ideal defined, in two equivalent ways, by

$$I(A) = \{x\colon x \leq a \text{ for some } a \in A\}$$

or

$$I(A) = \bigcup_{a\colon a\in A} I(a).$$

Ideals are also in bijection with order-preserving functions from P to the Boolean algebra $\underline{2}$: the ideal I corresponds to the function $f : P \to \underline{2}$ defined by $f(x) = \hat{0}$ if $x \in I$ and $f(x) = \hat{1}$ otherwise.

Filters are "up-closed;" in other words, filters are ideals in the order-dual $P^{\downarrow}$. The set complement $P\backslash I$ of an ideal is a filter. Any statement about ideals inverts to a statement about filters. In particular, the map sending a filter to the antichain of its minimal elements is a bijection. Hence, there is a bijection between the ideals and the filters of a partially ordered set. If A is a set of elements of P, then the *filter* $F(A)$ *generated by* A is the filter defined by

$$F(A) = \{x\colon x \geq a \text{ for some } a \in A\}.$$

When A is a single-element set $\{a\}$, the filter $F(\{a\})$, written $F(a)$, is the *principal filter* generated by a.

Let P be a partial order and Q be a partial order on the same set P. The partial order Q is an *extension* of P if $x \leq_P y$ implies $x \leq_Q y$ or, equivalently, as a subset of the Cartesian product $P \times P$, the relation $\leq_P$ is contained in $\leq_Q$. If Q is a chain, then it is a *linear extension* of P.

1.2.1. Lemma.[8] Let P be a finite partially ordered set. If x is incomparable with y, then there is a linear extension L of P such that $x <_L y$.

Proof. We can construct a linear extension in the following way: let $\min(P)$ be the set of minimal elements of P. Then choose an element x_1 from $\min(P)$,

[8] Dushnik and Miller (1941).