Introduction to Lattices and Order

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 400

Subsection 1

Lattices Satisfying Additional Identities

Some Lattice Inequalities

Lemma

Let L be a lattice and let $a, b, c \in L$. Then:

(i) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$; and dually,

(ii) $a \geq c$ implies $a \wedge (b \vee c) \geq (a \wedge b) \vee c$; and dually,

(iii) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$.

(i) We have

$$\left.\begin{array}{l} b \leq b \vee c \\ c \leq b \vee c \end{array}\right\} \Rightarrow \left.\begin{array}{l} a \wedge b \leq a \wedge (b \vee c) \\ a \wedge c \leq a \wedge (b \vee c) \end{array}\right\}$$
$$\Rightarrow (a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

(ii) This is a special case of Part (i). By hypothesis,

$$(a \wedge b) \vee c \overset{c \leq a}{\leq} (a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

Some Lattice Inequalities (Cont'd)

(iii)

$$\left.\begin{array}{l} a \wedge b \leq a \leq a \vee b, c \vee a \\ a \wedge b \leq b \leq b \vee c \end{array}\right\} \Rightarrow a \wedge b \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$$

Similarly,

$$\begin{array}{rcl} b \wedge c & \leq & (a \vee b) \wedge (b \vee c) \wedge (c \vee a); \\ c \wedge a & \leq & (a \vee b) \wedge (b \vee c) \wedge (c \vee a). \end{array}$$

Thus,

$$(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a).$$

On the Modular Law

Lemma

Let L be a lattice. Then, the following are equivalent:

(i) $(\forall a,b,c \in L)\ a \geq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c$;

(ii) $(\forall a,b,c \in L)\ a \geq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

(iii) $(\forall p,q,r \in L)\ p \wedge (q \vee (p \wedge r)) = (p \wedge q) \vee (p \wedge r)$.

- The Connecting Lemma gives the equivalence of (i) and (ii).

  (ii)⇒(iii): Assume (ii) holds and let $p,q,r \in L$. Then

  $$p \wedge (q \vee (p \wedge r)) \stackrel{\text{(ii)}}{=} (p \wedge q) \vee (p \wedge (p \wedge r)) = (p \wedge q) \vee (p \wedge r).$$

  (iii)⇒(i): Assume (iii) and let $a,b,c \in L$, with $c \leq a$. Then

  $$a \wedge (b \vee c) \stackrel{c \leq a}{=} a \wedge (b \vee (a \wedge c)) \stackrel{\text{(iii)}}{=} (a \wedge b) \vee (a \wedge c).$$

On the Distributive Law

Lemma

Let L be a lattice. Then the following are equivalent:

(D) $(\forall a, b, c \in L)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

$(\mathrm{D})^\partial$ $(\forall p, q, r \in L)\ p \vee (q \wedge r) = (p \vee q) \wedge (p \vee r)$.

- Assume (D) holds. Then, for $p, q, r \in L$,

$$\begin{array}{rcl} (p \vee q) \wedge (p \vee r) & = & ((p \vee q) \wedge p) \vee ((p \vee q) \wedge r) \quad \text{(by (D))} \\ & = & p \vee (r \wedge (p \vee q)) \quad \text{(by } (\mathrm{L2})^\partial \text{ \& } (\mathrm{L4})^\partial) \\ & = & p \vee ((r \wedge p) \vee (r \wedge q)) \quad \text{(by (D))} \\ & = & p \vee (q \wedge r) \quad \text{(by (L1), } (\mathrm{L2})^\partial \text{ \& (L4))} \end{array}$$

So (D) implies $(\mathrm{D})^\partial$.

By duality, $(\mathrm{D})^\partial$ implies (D) too.

Distributivity and Modularity

Definitions

Let L be a lattice.

(i) L is said to be **distributive** if it satisfies the **distributive law**,

$$(\forall a, b, c \in L)\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c).$$

(ii) L is said to be **modular** if it satisfies the **modular law**,

$$(\forall a, b, c \in L)\ a \geq c \Rightarrow a \wedge (b \vee c) = (a \wedge b) \vee c.$$

Remarks:

(1) Any lattice is "half-way" to being both modular and distributive. To establish distributivity or modularity we only need to check an inequality.

Distributivity and Modularity: Additional Remarks

(2) Any distributive lattice is modular.

Moreover, the rather mysterious modular law can be reformulated as an identity.

The modular law may be regarded as licence to rebracket $a \wedge (b \vee c)$ as $(a \wedge b) \vee c$, provided $a \geq c$.

(3) Providentially, distributivity can be defined either by (D) or by $(D)^\partial$.

Thus the apparent asymmetry between join and meet is illusory.

L is distributive if and only if L^∂ is and L is modular if and only if L^∂ is.

(4) The universal quantifiers in Remark (3) are essential: it is not true that if particular elements a, b and c in an arbitrary lattice satisfy $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, then they also satisfy $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Examples I

(1) Any powerset lattice $\mathcal{P}(X)$ is distributive.

More generally, any lattice of sets is distributive.

(2) Any chain is distributive.

(3) The lattice $\langle \mathbb{N}_0; \mathrm{lcm}, \mathrm{gcd} \rangle$ is distributive.

(4) The subgroup lattice of the infinite cyclic group $\langle \mathbb{Z}; + \rangle$ is isomorphic to $\langle \mathbb{N}_0; \mathrm{lcm}, \mathrm{gcd} \rangle^\partial$. Consequently $\mathrm{Sub}\mathbb{Z}$ is distributive.

Consider a finite group G. $\mathrm{Sub}G$ is distributive if G is cyclic.

The converse is also true but much harder to prove.

Examples II

(5) Our examples of classes of modular lattices come from algebra:

(i) The set $\mathcal{N}$-Sub$G$ of normal subgroups of a group G forms a lattice under the operations

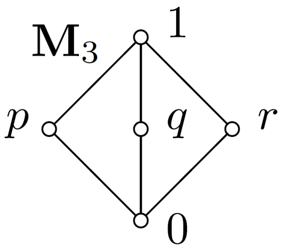
$$H \wedge K = H \cap K \quad \text{and} \quad H \vee K = HK,$$

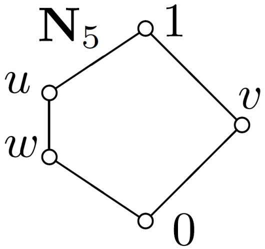
with $\subseteq$ as the underlying order.
Let $H, K, N \in \mathcal{N}$-Sub$G$, with $H \supseteq N$. Take $g \in H \wedge (K \vee N)$, so $g \in H$ and $g = kn$, for some $k \in K$ and $n \in N$. Then $k = gn^{-1} \in H$, since $H \supseteq N$ and H is a subgroup. This proves that $g \in (H \wedge K) \vee N$. Hence $H \wedge (K \vee N) \subseteq (H \wedge K) \vee N$. Since the reverse inequality holds in any lattice, the lattice $\mathcal{N}$-Sub$G$ is modular, for any group G.

(ii) It can be shown in a similar way that the lattice of subspaces of a vector space is modular.

The Diamond and the Pentagon

(6) Consider the lattices $\mathbf{M}_3$ (the **diamond**) and $\mathbf{N}_5$ (the **pentagon**):





- The lattice $\mathbf{M}_3$ arises as $\mathcal{N}$-Sub$\mathbf{V}_4$. Hence, by (5)(i), $\mathbf{M}_3$ is modular. It is, however, not distributive: in the diagram of $\mathbf{M}_3$
  $p \wedge (q \vee r) = p \wedge 1 = p \neq 0 = 0 \vee 0 = (p \wedge q) \vee (p \wedge r)$.
- The lattice $\mathbf{N}_5$ is not modular (and not distributive): in the diagram we have $u \geq w$ and $u \wedge (v \vee w) = u \wedge 1 = u > w = 0 \vee w = (u \wedge v) \vee w$.

- These examples turn out to play a crucial role in the identification of non-modular and non-distributive lattices as seen below.

Sublattices, Products and Homomorphic Images

- New lattices can be manufactured by forming sublattices, products and homomorphic images.
- Modularity and distributivity are preserved by these constructions:
  (i) If L is a modular (distributive) lattice, then every sublattice of L is modular (distributive).
  (ii) If L and K are modular (distributive) lattices, then $L \times K$ is modular (distributive).
  (iii) If L is modular (distributive) and K is the image of L under a homomorphism, then K is modular (distributive).
- Here (i) is immediate and (ii) holds because $\vee$ and $\wedge$ are defined coordinatewise on products.

  For (iii) we use the fact that a join- and meet-preserving map preserves any lattice identity; for the modular case we then invoke that the inequality can be replaced by an identity.

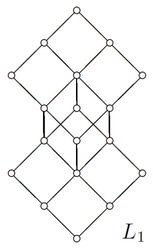
Examples

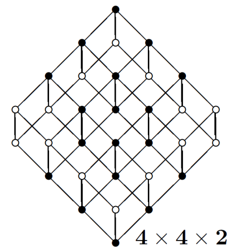
Proposition

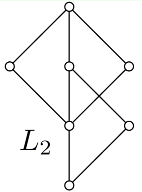
If a lattice is isomorphic to a sublattice of a product of distributive (modular) lattices, then it is distributive (modular).

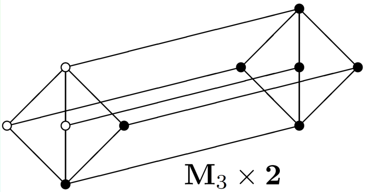
Examples:

The lattice L_1 is distributive because it is a sublattice of $\mathbf{4} \times \mathbf{4} \times \mathbf{2}$.









The lattice L_2 is isomorphic to the shaded sublattice of the modular lattice $\mathbf{M}_3 \times \mathbf{2}$ and so is itself modular.

Subsection 2

The $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem

The $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem

- The $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem implies that it is possible to determine whether or not a finite lattice is modular or distributive from its diagram.
- Recall that we write $M \rightarrowtail L$ to indicate that the lattice L has a sublattice isomorphic to the lattice M.

The $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem

Let L be a lattice.

(i) L is non-modular if and only if $\mathbf{N}_5 \rightarrowtail L$.

(ii) L is non-distributive if and only if $\mathbf{N}_5 \rightarrowtail L$ or $\mathbf{M}_3 \rightarrowtail L$.

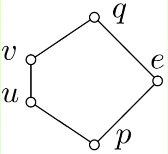
- It is enough to prove that a non-modular lattice has a sublattice isomorphic to $\mathbf{N}_5$ and that a lattice which is modular but not distributive has a sublattice isomorphic to $\mathbf{M}_3$.

Proof of Part (i)

- Assume that L is not modular. Then, there exist elements d, e and f such that $d > f$ and $v > u$, where $u = (d \wedge e) \vee f$ and $v = d \wedge (e \vee f)$.

  We aim to prove that $e \wedge u = e \wedge v$ (= p say) and $e \vee u = e \vee v$ (= q say).

  Then our required sublattice has elements u, v, e, p, q (which are clearly distinct).

  The lattice identities give

  $v \wedge e = (d \wedge (e \vee f)) \wedge e = (e \wedge (e \vee f)) \wedge d = d \wedge e$ and

  $u \vee e = ((d \wedge e) \vee f) \vee e = (e \vee (d \wedge e)) \vee f = e \vee f$. Also,

  $d \wedge e = (d \wedge e) \wedge e \leq u \wedge e \leq v \wedge e = d \wedge e$ and, similarly,

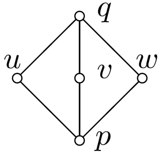
  $e \vee f = u \vee e \leq v \vee e \leq e \vee f \vee e = e \vee f$.

  This proves our claims and so completes the proof of (i).

Proof of Part (ii)

- Now assume that L is modular but not distributive. We build a sublattice isomorphic to $\mathbf{M}_3$. Take d, e and f, such that $(d \wedge e) \vee (d \wedge f) < d \wedge (e \vee f)$.

  Let
  $$\begin{array}{rcl} p & = & (d \wedge e) \vee (e \wedge f) \vee (f \wedge d), \\ q & = & (d \vee e) \wedge (e \vee f) \wedge (f \vee d), \\ u & = & (d \wedge q) \vee p, \\ v & = & (e \wedge q) \vee p, \\ w & = & (f \wedge q) \vee p. \end{array}$$

  Clearly $u \geq p, v \geq p$ and $w \geq p$. Also, $p \leq q$. Hence $u \leq (d \wedge q) \vee q = q$. Similarly, $v \leq q$ and $w \leq q$. Our candidate for a copy of $\mathbf{M}_3$ has elements $\{p, q, u, v, w\}$. We need to check that this subset has the correct joins and meets, and that its elements are distinct. We shall repeatedly appeal to the modular law, viz.

  (M) $\quad a \geq c$ implies $a \wedge (b \vee c) = (a \wedge b) \vee c$.

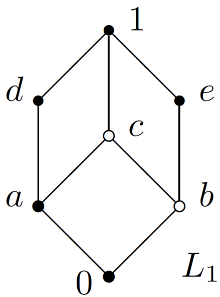
Proof of Part (ii) (Cont'd)

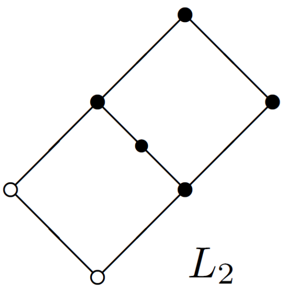
- We have $d \wedge q = d \wedge ((d \vee e) \wedge (e \vee f) \wedge (f \vee d)) \overset{(L4)^\partial}{=} d \wedge (e \vee f)$. Also $d \wedge p = \underline{d} \wedge ((e \wedge f) \vee (\underline{(d \wedge e) \vee (d \wedge f)})) =$ $(d \wedge (e \wedge f)) \vee ((d \wedge e) \vee (d \wedge f)) = (d \wedge e) \vee (d \wedge f)$. Thus $p = q$ is impossible. We conclude that $p < q$. We next prove that $u \wedge v = p$.

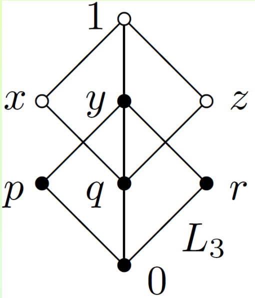
$$\begin{array}{rcll}
u \wedge v & = & ((d \wedge q) \vee \underline{p}) \wedge (\underline{(e \wedge q) \vee p}) & \\
& = & (((e \wedge \underline{q}) \vee \underline{p}) \wedge (d \wedge q)) \vee p & \text{(by (M))} \\
& = & ((q \wedge (e \vee p)) \wedge (d \wedge q)) \vee p & \text{(by (M))} \\
& = & ((e \vee p) \wedge (d \wedge q)) \vee p & \\
& = & ((d \wedge (e \vee f)) \wedge (e \vee (f \wedge d))) \vee p & \text{(by (L4) \& (L4)}^\partial\text{)} \\
& = & (d \wedge ((\underline{e \vee f}) \wedge (\underline{e} \vee (f \wedge d)))) \vee p & \\
& = & (d \wedge (((e \vee f) \wedge (f \wedge d)) \vee e)) \vee p & \text{(by (M))} \\
& = & (\underline{d} \wedge ((\underline{f \wedge d}) \vee e)) \vee p & \text{(since } d \wedge f \leq f \leq e \vee f\text{)} \\
& = & ((d \wedge e) \vee (f \wedge d)) \vee p & \text{(by (M))} \\
& = & p. &
\end{array}$$

In exactly the same way, $v \wedge w = p$ and $w \wedge u = p$. Similar calculations yield $u \vee v = v \vee w = w \vee u = q$. Finally, it is easy to see that if any two of the elements u, v, w, p, q are equal, then $p = q$, which is impossible.

Applying the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem

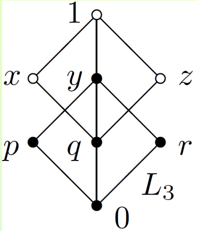


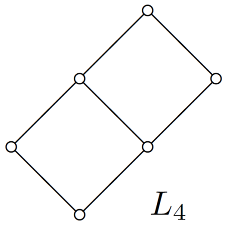




- The lattices L_1 and L_2 have sublattices isomorphic to $\mathbf{N}_5$.
- $\mathbf{M}_3 \rightarrowtail L_3$.
- The $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem implies that L_1 and L_2 are non-modular and that L_3 is non-distributive.

Applying the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem (Cont'd)





- $\mathbf{N}_5$ does not embed in L_3.
- Neither $\mathbf{N}_5$ nor $\mathbf{M}_3$ embeds in L_4.

- To justify such assertions requires a tedious enumeration of cases:

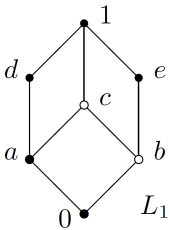
  Suppose $\{u, a, b, c, v\}$, with $u < c < a < v$, $u < b < v$, were a sublattice of L_3 isomorphic to $\mathbf{N}_5$. Since L_3 and $\mathbf{N}_5$ both have length 3, we must have $u = 0$ and $v = 1$. Since $a \wedge b = c \wedge b = 0$ and $a \vee b = c \vee b = 1$, by duality and symmetry we may assume without loss of generality that $a = r$, $c = p$ and $b = x$. But the choice does not satisfy $c < a$ nor is $\{0, r, x, p, 1\}$ a sublattice of L_3, a contradiction.

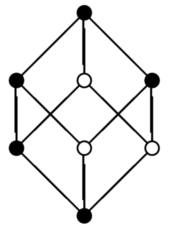
An Important Remark

- The statement of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem refers to the occurrence of the pentagon or diamond as a sublattice of L;

  This means that the joins and meets in a candidate copy of $\mathbf{N}_5$ or $\mathbf{M}_3$ must be the same as those in L.

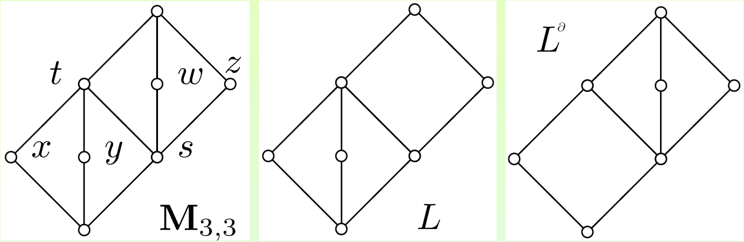
  Example: The pentagon $K = \{0, a, b, d, 1\}$ in L_1 is not a sublattice; $a \vee b = c \notin K$.





In the other direction, in applying the positive proposition, one must be sure to embed the given lattice as a sublattice. $\mathbf{N}_5$ is not distributive: it sits inside the distributive lattice $\mathbf{2}^3$, but not as a sublattice.

Example



- $\mathbf{M}_{3,3}$ is modular:

  To see this, note that for $u \in \{x, y, z\}$, the sublattice $\mathbf{M}_{3,3} \backslash \{u\}$ is isomorphic to L or to its dual L^∂, both of which are modular.

  Thus, any sublattice of $\mathbf{M}_{3,3}$ isomorphic to $\mathbf{N}_5$ would need to contain the antichain $\{x, y, z\}$, which is impossible.

Subsection 3

Boolean Lattices and Boolean Algebras

Complements

Definition

Let L be a lattice with 0 and 1. For $a \in L$, we say $b \in L$ is a **complement** of a if $a \wedge b = 0$ and $a \vee b = 1$. If a has a unique complement, we denote this complement by a'.

- Assume L is distributive and suppose that b_1 and b_2 are both complements of a. Then

$$b_1 = b_1 \wedge 1 = b_1 \wedge (a \vee b_2) = (b_1 \wedge a) \vee (b_1 \wedge b_2) = 0 \vee (b_1 \wedge b_2) = b_1 \wedge b_2.$$

  Hence $b_1 \leq b_2$ by the Connecting Lemma. Interchanging b_1 and b_2 gives $b_2 \leq b_1$. Therefore in a distributive lattice an element can have at most one complement.
- It is easy to find examples of non-unique complements in non-distributive lattices, e.g., in $\mathbf{M}_3$ or $\mathbf{N}_5$.

Boolean Lattices

- A lattice element may have no complement. The only complemented elements in a bounded chain are 0 and 1.
- If $\mathcal{L} \subseteq \mathcal{P}(X)$ is a lattice of sets, then an element $A \in \mathcal{L}$ has a complement if and only if $X \backslash A$ belongs to $\mathcal{L}$.

  Thus, the complemented elements of $\mathcal{O}(P)$ are the sets which are simultaneously down-sets and up-sets.

Definition

A lattice L is called a **Boolean lattice** if:

(i) L is distributive;

(ii) L has 0 and 1;

(iii) each $a \in L$ has a (necessarily unique) complement $a' \in L$.

Properties of Complements in Boolean Lattices

Lemma

Let L be a Boolean lattice. Then:

(i) $0' = 1$ and $1' = 0$;

(ii) $a'' = a$, for all $a \in L$;

(iii) de Morgan's laws hold: for all $a, b \in L$, $(a \vee b)' = a' \wedge b'$ and $(a \wedge b)' = a' \vee b'$;

(iv) $a \wedge b = (a' \vee b')'$ and $a \vee b = (a' \wedge b')'$, for all $a, b \in L$;

(v) $a \wedge b' = 0$ if and only if $a \leq b$, for all $a, b \in L$.

- To prove $p = q'$ in L it is sufficient to prove that $p \vee q = 1$ and $p \wedge q = 0$, since the complement of q is unique.

(i) We have $0 \wedge 1 = 0$ and $0 \vee 1 = 1$. Hence $0' = 1$ and $1' = 0$.

Properties of Complements (Cont'd)

(ii) We have, by definition, $a \wedge a' = 0$ and $a \vee a' = 1$. Hence, again by definition, $a'' = (a')' = a$.

(iii) We show $(a \vee b)' = a' \wedge b'$. The other de Morgan Law can be shown dually. We have

$$\begin{array}{rcl}(a \vee b) \wedge (a' \wedge b') & = & (a \wedge a' \wedge b') \vee (b \wedge a' \wedge b') \\ & = & (0 \wedge b') \vee (0 \wedge a') \\ & = & 0 \vee 0 = 0; \\ (a \vee b) \vee (a' \wedge b') & = & (a \vee b \vee a') \wedge (a \vee b \vee b') \\ & = & (1 \vee b) \wedge (a \vee 1) \\ & = & 1 \wedge 1 = 1.\end{array}$$

Hence, $(a \vee b)' = a' \wedge b'$.

- $(a' \vee b')' = a'' \wedge b'' = a \wedge b$.

Properties of Complements (Cont'd)

(v) Suppose $a \wedge b' = 0$. Then:

$$a \wedge b = (a \wedge b) \vee (a \wedge b') = a \wedge (b \vee b') = a \wedge 1 = a.$$

Hence, $a \leq b$.

Suppose, conversely, that $a \leq b$. Then:

$$a \wedge b' = (a \wedge b) \wedge b' = a \wedge (b \wedge b') = a \wedge 0 = 0.$$

Boolean Algebras

- A Boolean lattice was defined to be a special kind of distributive lattice, with 0 and 1, where each element has a (necessarily unique) complement.

Definition

A **Boolean algebra** is defined to be a structure $\langle B; \vee, \wedge, ', 0, 1\rangle$, such that:

(i) $\langle B; \vee, \wedge\rangle$ is a distributive lattice;

(ii) $a \vee 0 = a$ and $a \wedge 1 = a$, for all $a \in B$;

(iii) $a \vee a' = 1$ and $a \wedge a' = 0$, for all $a \in B$.

- A subset A of a Boolean algebra B is a **subalgebra** if A is a sublattice of B which contains 0 and 1 and is such that $a \in A$ implies $a' \in A$.
- Given Boolean algebras B and C, a map $f : B \to C$ is a **Boolean homomorphism** if f is a lattice homomorphism which also preserves 0, 1 and $'$ ($f(0) = 0$, $f(1) = 1$ and $f(a') = (f(a))'$, for all $a \in B$).

Conditions for Boolean Homomorphisms

Lemma

Let $f : B \to C$, where B and C are Boolean algebras.

(i) Assume f is a lattice homomorphism. The following are equivalent:
  (a) $f(0) = 0$ and $f(1) = 1$;
  (b) $f(a') = (f(a))'$, for all $a \in B$.

(ii) If f preserves $'$, then f preserves $\vee$ if and only if f preserves $\wedge$.

(i) (a)⇒(b) Use the equations

$$0 = f(0) = f(a \wedge a') = f(a) \wedge f(a'),$$
$$1 = f(1) = f(a \vee a') = f(a) \vee f(a').$$

(b)⇒(a) Conversely, if (b) holds, we have

$$f(0) = f(a \wedge a') = f(a) \wedge (f(a))' = 0,$$
$$f(1) = f(a \vee a') = f(a) \vee (f(a))' = 1.$$

(ii) Assume f preserves $'$ and $\vee$. For all $a, b \in B$,

$$\begin{aligned} f(a \wedge b) &= f((a' \vee b')') = (f(a' \vee b'))' = (f(a') \vee f(b'))' \\ &= ((f(a))' \vee (f(b))')' = f(a) \wedge f(b). \end{aligned}$$

Example of Boolean Algebras I

(1) For any set X, let $A' := X \backslash A$, for all $A \subseteq X$. Then the structure $\langle \mathcal{P}(X); \cup, \cap, ', \varnothing, X \rangle$ is a Boolean algebra known as the **powerset algebra** on X.

By an **algebra of sets** (also known as a **field of sets**) we mean a subalgebra of some powerset algebra $\mathcal{P}(X)$, that is, a family of sets which forms a Boolean algebra under the set-theoretic operations.

- We will prove that every finite Boolean algebra is isomorphic to $\mathcal{P}(X)$, for some finite set X.
- The following example shows that there are infinite Boolean algebras which are not powerset algebras.

  However, we will also:
  - Show that every Boolean algebra is isomorphic to an algebra of sets;
  - Characterize the powerset algebras among Boolean algebras.

Example of Boolean Algebras II

(2) The **finite-cofinite algebra** of the set X is defined to be

$$\mathrm{FC}(X) = \{A \subseteq X : A \text{ is finite or } X \backslash A \text{ is finite}\}.$$

- It is easily checked that this is an algebra of sets.

  Claim: $\mathrm{FC}(\mathbb{N})$ is not isomorphic to $\mathcal{P}(X)$ for any set X.

  Reasoning by Cardinalities: $\mathrm{FC}(\mathbb{N})$ is countable. On the other hand, Cantor's Theorem implies that any powerset is either finite or uncountable.

  Reasoning Lattice-Theoretically: $\mathrm{FC}(\mathbb{N})$ is not complete. But $\mathcal{P}(X)$ is always complete and an isomorphism must preserve completeness.

Examples of Boolean Algebras III

(3) The family of all clopen subsets of a topological space $(X;\mathcal{T})$ is an algebra of sets. Clearly this example will not be of much interest unless X has plenty of clopen sets. We will show that every Boolean algebra can be concretely represented as such an algebra.

(4) For $n \geq 1$ the lattice $\mathbf{2}^n$ is lattice-isomorphic to $\mathcal{P}(\{1,2,\ldots,n\})$, which is a Boolean algebra. Hence $\mathbf{2}^n$ is a Boolean algebra, with $0 = (0,0,\ldots,0)$ and $1 = (1,1,\ldots,1)$, $(\varepsilon_1,\ldots,\varepsilon_n)' = (\eta_1,\ldots,\eta_n)$, where $\eta_i = 0 \Leftrightarrow \varepsilon_i = 1$.

The simplest non-trivial Boolean algebra of all is $\mathbf{2} = \{0,1\}$. It arises frequently in logic and computer science as an algebra of truth values. In such contexts the symbols F and T, or alternatively $\perp$ and $\top$, are used in place of 0 and 1. We have $\mathsf{F} \vee \mathsf{F} = \mathsf{F} \wedge \mathsf{F} = \mathsf{F} \wedge \mathsf{T} = \mathsf{T}' = \mathsf{F}$, $\mathsf{T} \wedge \mathsf{T} = \mathsf{F} \vee \mathsf{T} = \mathsf{T} \vee \mathsf{T} = \mathsf{F}' = \mathsf{T}$.

Subsection 4

Boolean Terms and Disjunctive Normal Form

Propositional Variables and Logical Connectives

- In propositional calculus, propositions are designated by **propositional variables** which take values in $\{F, T\}$.
- Admissible compound statements are formed using **logical connectives**.
- Connectives include "and", "or" and "not", denoted respectively by $\wedge, \vee$ and $'$.
- Another natural connective is "implies" ($\rightarrow$).
- Compound statements built from these are assigned the expected truth values according to the truth values of their constituent parts.

  Example:
  - $p \wedge q$ has value T if and only if both p and q have value T;
  - $p \rightarrow q$ has value T unless p has value T and q has value F.

Well-Formed Formulas

- We take an infinite set of propositional variables, denoted $p, q, r, \ldots$, and define a **wff** (or **well-formed formula**) by the rules:
  (i) any propositional variable standing alone is a wff (optionally, constant symbols T and F may also be included as wffs);
  (ii) if φ and ψ are wffs, so are $(\varphi \wedge \psi), (\varphi \vee \psi), \varphi', (\varphi \to \psi)$ (this clause is suitably adapted if a different set of connectives is used);
  (iii) any wff arises from a finite number of applications of (i) and (ii).

  Example: $((p \wedge q') \vee r)'$ is a wff; $((p' \to q) \to ((p' \to q') \to p))$ is a wff; $(((p \vee q) \wedge p)$ is not a wff (invalid bracketing); $\vee \to q$ is not a wff.
- The parentheses guarantee non-ambiguity.

  In practice we drop parentheses where no ambiguity would result, just as if we were writing a string of joins, meets and complements in a lattice.

Truth Functions and Truth Tables

- A wff φ involving the propositional variables $p_1, \ldots, p_n$ defines a **truth function** F_φ of n variables.

  For a given assignment of values in $\{F, T\}$ to $p_1, \ldots, p_n$, substitute these values into φ and compute the resulting expression in the Boolean algebra $\{F, T\}$ to obtain the value of F_φ.
- Truth functions are presented via **truth tables**:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

p_1	p_2	p_3	$(p_1 \vee p_2)$	$(p_1' \vee p_3)$	$((p_1 \vee p_2) \wedge (p_1' \vee p_3))'$
T	T	T	T	T	F
T	T	F	T	F	T
T	F	T	T	T	F
T	F	F	T	F	T
F	T	T	T	T	F
F	T	F	T	T	F
F	F	T	F	T	T
F	F	F	F	T	T

Logically Equivalent Formulas

- Two wffs φ and ψ are called **logically equivalent** (written $\varphi \equiv \psi$) if they define the same truth function, i.e., they give rise to the same truth table.
- For any wffs φ and ψ,

$$\begin{array}{ll} (\varphi \wedge \psi) \equiv (\varphi' \vee \psi')', & (\varphi \vee \psi) \equiv (\varphi' \wedge \psi')', \\ (\varphi \to \psi) \equiv (\varphi' \vee \psi), & (\varphi \wedge \psi) \equiv (\varphi \to \psi')'. \end{array}$$

- A proof by induction on the number of connectives then shows that any wff built using $\vee, \wedge$ and $'$ is logically equivalent to one built using $\to$ and $'$, and vice versa.
- Therefore, up to logical equivalence, we arrive at the same set of wffs whether we take $\{\vee, \wedge, ', \to\}$, just $\{\to, '\}$ or just $\{\vee, \wedge, '\}$ as the basic set of connectives.
  - The choice of $\{\to, '\}$ is the most natural for studying logic;
  - $\{\vee, \wedge, '\}$ brings out the connections with Boolean algebras.

The Algebra of Propositions: A Preview

- The set of wffs, with $\vee, \wedge$ and $'$ as operations, closely resembles a Boolean lattice:
  - The axioms do not hold if = is taken to mean "is the same wff as";
  - The axioms hold if = is read as "is logically equivalent to".

  Example: To establish (L4), note that $\varphi \vee (\varphi \wedge \psi)$ takes value T if and only if φ does. So $\varphi \vee (\varphi \wedge \psi) \equiv \varphi$.
- If F and T are included as wffs, to serve as 0 and 1, we obtain a Boolean algebra, called the **algebra of propositions**.

Boolean Terms

- We define the class **BT** of **Boolean terms** (or **Boolean polynomials**) as follows:

  Let S be a set of variables, whose members will be denoted by letters such as $x, y, z, x_1, x_2, \ldots$, and let $\vee, \wedge, ', 0, 1$ be the symbols used to axiomatize Boolean algebras. Then:

  (i) $0, 1 \in$ **BT** and $x \in$ **BT**, for all $x \in S$;
  (ii) if $p, q \in$ **BT**, then $(p \vee q), (p \wedge q)$ and p' belong to**BT**;
  (iii) every element of **BT** is an expression formed by a finite number of applications of (i) and (ii).

- A Boolean term p whose variables are drawn from among $x_1, \ldots, x_n$ will be written $p(x_1, \ldots, x_n)$.

  Example: Some Boolean terms:

$$1,\ x,\ y,\ y',\ (x \vee y'),\ (1 \wedge (x \vee y')),\ (1 \wedge (x \vee y'))'.$$

Semantics of Boolean Terms

- Just as numbers may be substituted into "ordinary" polynomials, elements of any Boolean algebra B may be substituted for the variables of a Boolean term to yield an element of B.
- If we take, in particular, $B = \mathbf{2}$, every Boolean term $p(x_1, \ldots, x_n)$ defines a map $F_p : \mathbf{2}^n \to \mathbf{2}$.

  The map F_p associated with p can be specified by a "truth table" in just the same way as a wff determines a truth function. The only difference is that each entry of the table is 0 or 1, instead of F or T.
- It is usual to use p to denote both the term and the function F_p it induces.

Equivalence of Boolean Terms

- We say that the Boolean terms $p(x_1, \ldots, x_n)$ and $q(x_1, \ldots, x_n)$ are **equivalent**, and write $p \equiv q$, if p and q have the same truth function, that is, $F_p = F_q$.
  Example: For instance, we may check $(x \wedge y')' \equiv (x' \vee y)$ (both sides give the same truth table).
  The right-hand side can be obtained from the left by applying the laws of Boolean algebra:
  $$(x \wedge y')' = (x' \vee y'') = (x' \vee y).$$
- In general, whenever $q(x_1, \ldots, x_n)$ can be obtained from $p(x_1, \ldots, x_n)$ by the laws of Boolean algebra, we have $p \equiv q$.
- We will see that the converse is also true.
  Notation: Where removal of parentheses from a Boolean term would, up to equivalence, not result in ambiguity, we omit parentheses, e.g., we shall write $x \vee y \vee z$ in place of either $(x \vee (y \vee z))$ or $((x \vee y) \vee z)$.

Every Map is a Boolean Term Function

- Consider the truth table associated with a truth function $F : \mathbf{2}^n \to \mathbf{2}$.
  - For each row (element of $\mathbf{2}^n$) on which F has value 1, form the meet of n symbols by selecting for each variable x either x or x' depending on whether x has value 1 or 0 in that row.
  - Then take the join p of these terms.

Then p, is such that $F = F_p$.

Theorem

Every map $F : \mathbf{2}^n \to \mathbf{2}$ coincides with F_p for some Boolean term $p(x_1, \ldots, x_n)$. A suitable term p may be described as follows: For $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbf{2}^n$, define $p_{\boldsymbol{a}}(x_1, \ldots, x_n)$ by $p_{\boldsymbol{a}}(x_1, \ldots, x_n) = x_1^{\varepsilon_1} \wedge \cdots \wedge x_n^{\varepsilon_n}$, where $x_j^{\varepsilon_j} = \begin{cases} x_j, & \text{if } a_j = 1 \\ x_j', & \text{if } a_j = 0 \end{cases}$. Then define $p(x_1, \ldots, x_n) = \bigvee \{p_{\boldsymbol{a}}(x_1, \ldots, x_n) : F(\boldsymbol{a}) = 1\}$.

Every Map is a Boolean Term Function (Cont'd)

- Let $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbf{2}^n$ and $\boldsymbol{b} = (b_1, \ldots, b_n) \in \mathbf{2}^n$. We have carefully chosen the term $p_{\boldsymbol{a}}(x_1, \ldots, x_n)$ so that
$F_{p_{\boldsymbol{a}}}(b_1, \ldots, b_n) = \begin{cases} 1, & \text{if } \boldsymbol{b} = \boldsymbol{a} \\ 0, & \text{if } \boldsymbol{b} \neq \boldsymbol{a} \end{cases}$
Claim: $F = F_p$.
Assume that $F(\boldsymbol{b}) = 1$. Then

$$\begin{array}{rcl} F_p(b_1, \ldots, b_n) & = & \bigvee\{F_{p_{\boldsymbol{a}}}(b_1, \ldots, b_n) : F(\boldsymbol{a}) = 1\} \\ & \geq & F_{p_{\boldsymbol{b}}}(b_1, \ldots, b_n) \\ & = & 1. \end{array}$$

Thus, $F(\boldsymbol{b}) = 1$ implies $F_p(\boldsymbol{b}) = 1$. Assume $F(\boldsymbol{b}) = 0$. Then $F(\boldsymbol{a}) = 1$ implies $\boldsymbol{b} \neq \boldsymbol{a}$. So $F_{p_{\boldsymbol{a}}}(b_1, \ldots, b_n) = 0$. Therefore $F_p(b_1, \ldots, b_n) = \bigvee\{F_{p_{\boldsymbol{a}}}(b_1, \ldots, b_n) : F(\boldsymbol{a}) = 1\} = 0$. Thus $F(\boldsymbol{b}) = 0$ implies $F_p(\boldsymbol{b}) = 0$. Hence $F = F_p$, as claimed.

Disjunctive Normal Form

- A Boolean term $p(x_1, \ldots, x_n)$ is said to be in **full disjunctive normal form**, or **DNF**, if it is a join of distinct meets of the form $x_1^{\varepsilon_1} \wedge \cdots \wedge x_n^{\varepsilon_n}$. By definition, x^{ε} equals x if $\varepsilon = 1$, and x' if $\varepsilon = 0$. Terms of the form x^{ε} are known as **literals**.
- The theorem implies that any Boolean term is equivalent to a term in DNF (in the setting of propositional calculus this is just the classic result that any wff is logically equivalent to a wff in DNF).
- Note that the Boolean term 0 is already in DNF as it is the join of the empty set.
- At the other end of the spectrum, the DNF of the Boolean term 1 is the join of all 2^n meets of the form $x_1^{\varepsilon_1} \wedge \cdots \wedge x_n^{\varepsilon_n}$.

Disjunctive Normal Form and Equivalence

- Each truth function uniquely determines, and is determined by, a DNF term; so $p \equiv q$ in **BT** if and only if each of p and q is equivalent to the same DNF.
- We have already remarked that applying the laws of Boolean algebra to a Boolean term yields an equivalent term.
- This process can be used to reduce any term $p(x_1, \ldots, x_n)$ to DNF, as outlined below:
  (i) Use de Morgan's laws to reduce $p(x_1, \ldots, x_n)$ to literals combined by joins and meets.
  (ii) Use the distributive laws repeatedly, with the lattice identities, to obtain a join of meets of literals.
  (iii) Finally, we require each x_i to occur, either primed or not, once and once only in each meet term. This is achieved by dropping any terms containing both x_i and x_i', for any i. If neither x_j nor x_j' occurs in $\bigwedge_{k \in K} x_k^{\varepsilon_k}$, it can be introduces as follows:
  $\bigwedge_{k \in K} x_k^{\varepsilon_k} \equiv (\bigwedge_{k \in K} x_k^{\varepsilon_k}) \wedge (x_j \vee x_j') \equiv (\bigwedge_{k \in K} x_k^{\varepsilon_k} \wedge x_j) \vee (\bigwedge_{k \in K} x_k^{\varepsilon_k} \wedge x_j')$.
  Repeating this for each missing variable we arrive at a term in DNF.

Example

- Write the term $((p_1 \vee p_2) \wedge (p_1' \vee p_3))'$ in DNF.
  Construct the truth table.

p_1	p_2	p_3	$(p_1 \vee p_2)$	$(p_1' \vee p_3)$	$((p_1 \vee p_2) \wedge (p_1' \vee p_3))'$
T	T	T	T	T	F
T	T	F	T	F	T
T	F	T	T	T	F
T	F	F	T	F	T
F	T	T	T	T	F
F	T	F	T	T	F
F	F	T	F	T	T
F	F	F	F	T	T

Pick the rows, where the value is 1 and construct the corresponding meets. Then, take the join of those meets.

$$(p_1 \wedge p_2 \wedge p_3') \vee (p_1 \wedge p_2' \wedge p_3') \vee (p_1' \wedge p_2' \wedge p_3) \vee (p_1' \wedge p_2' \wedge p_3').$$

The Boolean Algebra of Functions of n Variables

Theorem

Let B be the Boolean algebra $\mathbf{2}^{2^n}$. Then B is generated by n elements, in the sense that there exists an n-element subset X of B, such that the smallest Boolean subalgebra of B containing X is B.

- Identify B with the Boolean algebra $\mathcal{P}(\mathbf{2}^n)$. Define X to be $\{e_1, \ldots, e_n\}$, where $e_i := \{(a_1, \ldots, a_n) \in \mathbf{2}^n : a_i = 1\}$, for $i = 1, \ldots, n$. Then, for each $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbf{2}^n$, we have

$$\{\boldsymbol{a}\} = \bigcap\{e_i : a_i = 1\} \cap \bigcap\{e_i' : a_i = 0\}.$$

  Each non-empty element of B is a union of singletons, $\{\boldsymbol{a}\}$. Hence, it is expressible as a join of meets of elements of the form e_i or e_i'.
  Note that $\varnothing = e_1 \cap e_1'$ takes care of the empty set.