Orders, lattices and Boolean algebras

Tommaso Moraschini

Master in Pure and Applied Logic
University of Barcelona
2020

Contents

CHAPTER 1

Orders and lattices

The main references of the course are [1, 3, 4, 6, 10, 11, 14] for orders, lattices and Boolean algebras, and [2, 5] for universal algebraic constructions.

1.1 Partially ordered sets

A *binary relation* R on set X is a subset of $X \times X$. We write xRy when the ordered pair $\langle x, y\rangle$ belongs to the relation R. A binary relation R on a set X is said to be

(i) *reflexive* when, for every $x \in X$, xRx;

(ii) *transitive* when, for every $x, y, z \in X$, if xRy and yRz, then xRz;

(iii) *antisymmetric* when, for every $x, y \in X$, if xRy and yRx, then $x = y$.

Definition 1.1. A binary relation $\leqslant$ on a set X is said to be a *partial order* if it is reflexive, transitive, and antisymmetric. In this case, the pair $\mathbb{X} = \langle X; \leqslant\rangle$ is said to be a *poset* (a shorthand for a *partially ordered set*).

Given a poset $\mathbb{X}$, we denote by X and $\leqslant^{\mathbb{X}}$, respectively, its underlying set and relation. When no confusion may occur, we drop the superscript from $\leqslant^{\mathbb{X}}$ and write simply $\leqslant$. The set X is sometimes called the *universe* of $\mathbb{X}$. Given a poset $\mathbb{X}$ and $x, y \in X$, we write $x < y$ when both $x \leqslant y$ and $x \neq y$. Lastly, $\mathbb{X}$ is said to be *nontrivial* when $|X| \geqslant 2$ and *trivial* otherwise. Notice that the universe of a poset $\mathbb{X}$ might be empty, in which case $\leqslant$ is the empty set as well.

Example 1.2. The *identity relation* on a set X is the binary relation

$$\mathrm{Id}_X := \{\langle x, x\rangle \in X \times X : x \in X\}$$

and the pair $\langle X; \mathrm{Id}_X\rangle$ is always a poset. Moreover, the pair $\langle \mathcal{P}(X); \subseteq\rangle$, where $\mathcal{P}(X)$ is the powerset of X, is also a poset.

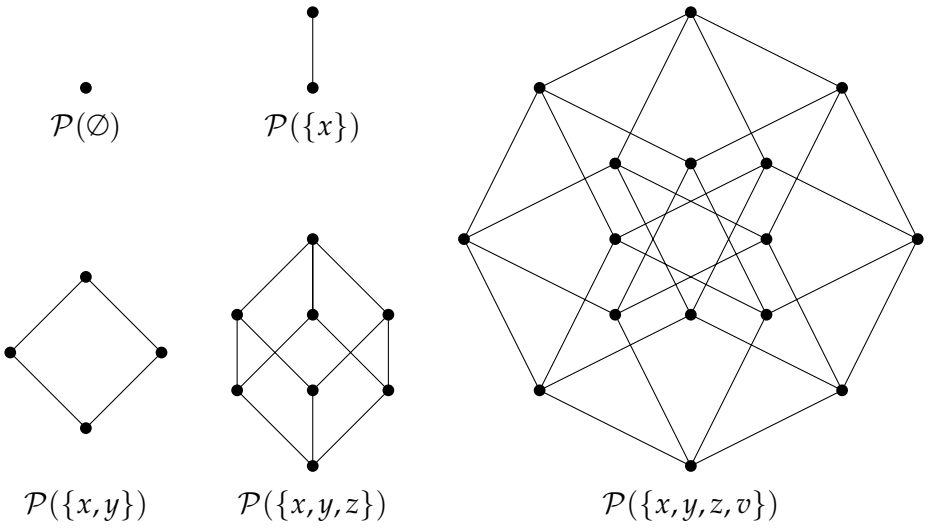
Another example of a poset is the set of natural number $\mathbb{N}$ endowed with the standard order $\leqslant$. Lastly, $\mathbb{N}$ endowed with the *divisibility relation*

$$| := \{\langle n, m\rangle \in \mathbb{N} \times \mathbb{N} : \text{there exists } k \in \mathbb{N} \text{ s.t. } m = n \cdot k\}$$

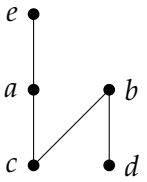
is a poset as well, known as the *division lattice*.

Similarly, the set of integers $\mathbb{Z}$ endowed with the standard order is a poset. However, when endowed with the appropriate divisibility relation, $\mathbb{Z}$ fails to be a poset, because the divisibility relation is not antisymmetric on $\mathbb{Z}$ (as n and $-n$ divide each other, but are distinct, for every positive integer n). ⊠

An attractive feature of posets is that they can often be represented by graphics consisting of circles and lines connecting them, known as *Hasse diagrams*. This is always true for finite posets $\mathbb{X}$ of a manageable size, whose Hasse diagrams can be obtained as follows. First, we depict the elements of X as circles, making sure that if $x < y$, then the circle corresponding to x is below that corresponding to y. Then we connect two circles with a line, provided that they correspond to two points $x, y \in X$ such that $x < y$ and that there is no $z \in X$ such that $x < z < y$. As a result, two elements $x, y \in X$ are such that $x < y$ precisely when there exists an ascending path from x to y. For instance, the Hasse diagrams of the powerset lattices $\langle \mathcal{P}(X); \subseteq \rangle$ with X of size $\leqslant 4$ are depicted below. The reader is encouraged to try to decode them by working out the details of the correspondence between the elements of these powerset lattices and the circles of their Hasse diagrams.



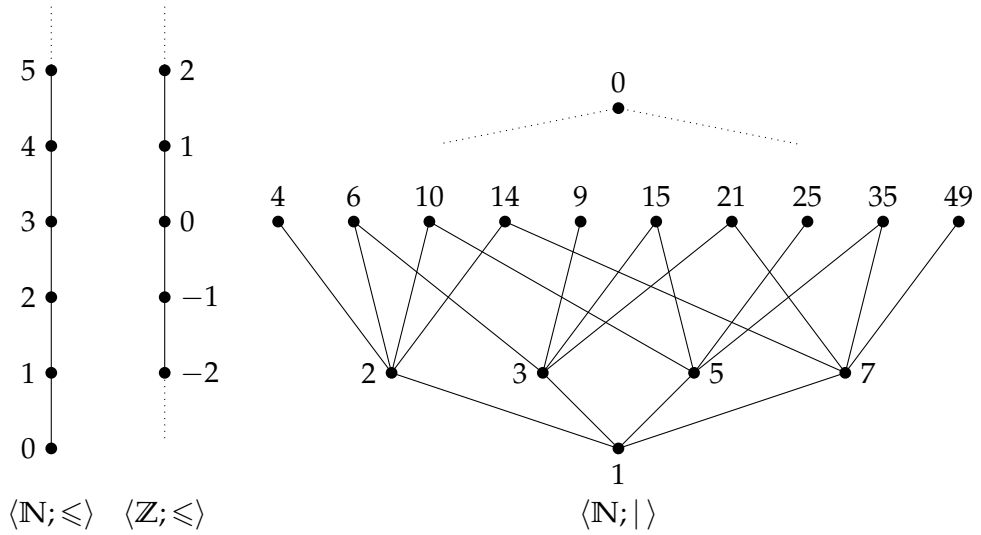
Notably, finite posets can be faithfully reconstructed from their Hasse diagrams. As a consequence, in order to define a finite poset, it suffices to exhibit its Hasse diagram. For instance, the poset $\langle X; \leqslant \rangle$ associated with the Hasse diagram below



has universe $X = \{a, b, c, d, e\}$ and order relation

$$\leqslant^{\mathbb{X}} = \{\langle a,a\rangle, \langle b,b\rangle, \langle c,c\rangle, \langle d,d\rangle, \langle e,e\rangle, \langle c,a\rangle, \langle c,b\rangle, \langle c,e\rangle, \langle a,e\rangle, \langle d,b\rangle\}.$$

Hasse diagrams can also be employed to describe infinite posets, provided that their structure is regular enough to be hinted by dotted lines. For instance, the posets $\langle \mathbb{N}; \leqslant \rangle$ and $\langle \mathbb{Z}; \leqslant \rangle$ are depicted below, together with a portion of the division lattice $\langle \mathbb{N}; | \rangle$.



The following special elements play a fundamental role in order theory:

Definition 1.3. An element x of a poset $\mathbb{X}$ is said to be

(i) a *maximum* of $\mathbb{X}$ if $y \leqslant x$, for all $y \in X$;

(ii) a *minimum* of $\mathbb{X}$ if $x \leqslant y$, for all $y \in X$;

(iii) a *maximal element* of $\mathbb{X}$ if there is no $y \in X$ such that $x < y$;

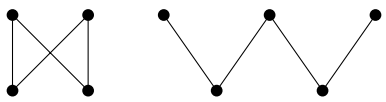
(iv) a *minimal element* of $\mathbb{X}$ if there is no $y \in X$ such that $y < x$;

(v) an *upper bound of a set* $Y \subseteq X$ in $\mathbb{X}$ if $y \leqslant x$, for all $y \in Y$;

(vi) a *lower bound of a set* $Y \subseteq X$ in $\mathbb{X}$ if $x \leqslant y$, for all $y \in Y$.

When $\mathbb{X}$ has both a maximum and a minimum, it is said to be *bounded*.

It follows from the definition that a maximum is always maximal (resp. a minimum is always minimal), but the converse need not hold in general. For instance, every element of the poset $\mathbb{X} = \langle X; \mathrm{Id}_X \rangle$ is both maximal and minimal of $\mathbb{X}$ but, provided that $\mathbb{X}$ is nontrivial, none of them is a maximum or a minimum of $\mathbb{X}$. Moreover, the poset $\langle \mathbb{Z}; \leqslant \rangle$ of integers with the standard order lacks any maximal or minimal element. Lastly, the following poset has 5 maximal and 4 minimal elements, but lacks both a maximum and a minimum.



Proposition 1.4. *In posets, maximum and minimum elements (when they exist) are unique.*

Proof. Let $\mathbb{X}$ be a poset and x, y be maximum elements. Since x is a maximum, $y \leqslant x$. Similarly, since y is a maximum $x \leqslant y$. As $\leqslant$ is antisymmetric $x = y$. The case of minimum elements is analogous. ⊠

In view of the above lemma, the unique maximum and minimum of a poset $\mathbb{X}$, when existing, will be denoted by 1 and 0, respectively.

As we mentioned, infinite posets, such as $\langle \mathbb{Z}; \leqslant \rangle$, may lack maximal and minimal elements. However, this cannot happen in the finite case.

Proposition 1.5. *Every nonempty finite poset has both a maximal and a minimal element.*

Proof. Suppose, with a view to contradiction, that there exists a finite nonempty poset $\mathbb{X}$ without either maximal or minimal elements. We can assume, without loss of generality, that $\mathbb{X}$ lacks maximal elements. As $\mathbb{X}$ is nonempty, there exists $x_0 \in X$. Since x_0 is not maximal, there exists $x_1 \in X$ such that $x_0 < x_1$. Similarly, since x_1 is not maximal, there exists $x_2 \in X$ such that $x_1 < x_2$. Iterating this process, we produce a sequence $\{x_n : n \in \mathbb{N}\}$ of elements of $\mathbb{X}$ such that

$$x_n < x_n + 1, \text{ for all } n \in \mathbb{N}.$$

We claim that $x_n \neq x_m$, for every pair of distinct $n, m \in \mathbb{N}$. Suppose the contrary, with a view to contradiction. Then there are two distinct $n, m \in \mathbb{N}$ such that $x_n = x_m$. We can assume, without loss of generality, that $n < m$, whence, by construction,

$$x_n < x_{n+1} < x_{n+2} < \cdots < x_m.$$

As $\leqslant$ is transitive, this implies $x_{n+1} \leqslant x_m$. Since $x_m = x_n$, this yields also $x_{n+1} \leqslant x_n$. Furthermore, by construction, $x_n < x_{n+1}$. By the antisymmetry of $\leqslant$, we conclude that $x_n = x_{n+1}$, a contradiction with $x_n < x_{n+1}$. This establishes the claim.

Lastly, from the claim it follows that $\{x_n : n \in \mathbb{N}\}$ is an infinite subset of X, a contradiction with the fact that $\mathbb{X}$ is finite. ⊠

Definition 1.6. Given a poset $\mathbb{X}$, two elements $x, y \in X$ are said to be *comparable* when either $x \leqslant y$ or $y \leqslant x$. They are said to be *incomparable* otherwise. Accordingly, we say that $\mathbb{X}$ is

(i) *linearly ordered* or a *chain* when every two elements are comparable, that is, $x \leqslant y$ or $y \leqslant x$, for every $x, y \in X$;

(ii) *discrete* when $\leqslant$ is the identity relation, that is, when every two distinct elements are incomparable.

Linearly ordered posets are sometimes called *totally ordered*.

For instance, both $\langle \mathbb{N}; \leqslant \rangle$ and $\langle \mathbb{Z}; \leqslant \rangle$ are linearly ordered. Most posets, however, are neither linearly ordered nor discrete. For instance, $\langle \mathcal{P}(X); \subseteq \rangle$ is neither a linearly ordered nor discrete, for every set X with at least two elements. To see this, consider two distinct elements $x, y \in X$. Then the sets $\{x\}$ and $\{y\}$ are incomparable elements of $\langle \mathcal{P}(X); \subseteq \rangle$, whence this poset is not linearly ordered. Similarly, $\emptyset$ and $\{x\}$ are two distinct, but comparable elements, whence $\langle \mathcal{P}(X); \subseteq \rangle$ is not discrete.

Given a binary relation R on a set X, the *restriction* of R to a subset $Y \subseteq X$, is the binary relation $R \cap (Y \times Y)$ on Y.

Definition 1.7. Given a poset $\mathbb{X}$, a subset $Y \subseteq X$ is said to be

(i) a *chain in* $\mathbb{X}$ if, when endowed with the restriction of $\leqslant^{\mathbb{X}}$ to Y, it is linearly ordered;

(ii) an *antichain in* $\mathbb{X}$ if, when endowed with the restriction of $\leqslant^{\mathbb{X}}$ to Y, it is discrete.

Recall that an infinite poset may lack both maximal and minimal elements. Because of this, the following principle plays a fundamental role in most proofs that require the existence of maximal (resp. minimal) elements in infinite posets. Notably, it is equivalent to the Axiom of Choice.

Zorn's Lemma 1.8. *Let $\mathbb{X}$ be a poset. If every chain in $\mathbb{X}$ has an upper bound in $\mathbb{X}$, then $\mathbb{X}$ has a maximal element.*

In order to compare distinct posets, it is convenient to introduce maps that preserve their structure.

Definition 1.9. Let $\mathbb{X}$ and $\mathbb{Y}$ be posets. A map $f\colon X \to Y$ is said to be

(i) *order preserving* from $\mathbb{X}$ to $\mathbb{Y}$ when, for every $x, y \in X$,

$$\text{if } x \leqslant^{\mathbb{X}} y, \text{ then } f(x) \leqslant^{\mathbb{Y}} f(y);$$

(ii) *order reflecting* from $\mathbb{X}$ to $\mathbb{Y}$ when, for every $x, y \in X$,

$$\text{if } f(x) \leqslant^{\mathbb{Y}} f(y), \text{ then } x \leqslant^{\mathbb{X}} y;$$

(iii) an *order embedding* of $\mathbb{X}$ into $\mathbb{Y}$ if it is both order preserving and order reflecting, that is, for every $x, y \in X$,

$$x \leqslant^{\mathbb{X}} y \iff f(x) \leqslant^{\mathbb{Y}} f(y).$$

In these cases, we sometimes write $f\colon \mathbb{X} \to \mathbb{Y}$ instead of $f\colon X \to Y$.

For instance, the inclusion map $i\colon \mathbb{N} \to \mathbb{Z}$ is an order embedding of $\langle \mathbb{N}; \leqslant \rangle$ into $\langle \mathbb{Z}; \leqslant \rangle$, while the function $f\colon \mathbb{Z} \to \mathbb{N}$, defined by the rule

$$f(n) \coloneqq \text{the greatest element between } 0 \text{ and } n,$$

is an order preserving map from $\langle \mathbb{Z}; \leqslant \rangle$ to $\langle \mathbb{N}; \leqslant \rangle$ that is not order reflecting.

Notice that order embeddings are necessarily injective. To prove this, consider an order embedding $f\colon \mathbb{X} \to \mathbb{Y}$ and two distinct elements $x, y \in X$. Since $\leqslant^{\mathbb{X}}$ is antisymmetric and $x \neq y$, we can assume, without loss of generality, that $x \not\leqslant^{\mathbb{X}} y$. As f is order reflecting, this yields $f(x) \not\leqslant^{\mathbb{Y}} f(y)$. Thus, from the reflexivity of $\leqslant^{\mathbb{Y}}$ it follows that $f(x) \neq f(y)$, establishing the injectivity of f.

As a consequence, a surjective order embedding is always bijective. It follows that the inverse map of a surjective order embedding is also a surjective order embedding. This motivates the following definition:

Definition 1.10. An *order isomorphism* is a surjective order embedding. Accordingly, two posets $\mathbb{X}$ and $\mathbb{Y}$ are said to be *isomorphic* when there exists an order isomorphism from $\mathbb{X}$ to $\mathbb{Y}$ or, equivalently, from $\mathbb{Y}$ to $\mathbb{X}$. In this case, we write $\mathbb{X} \cong \mathbb{Y}$.

When there exists an order embedding $f\colon \mathbb{X} \to \mathbb{Y}$, the poset $\mathbb{Y}$ contains a copy of $\mathbb{X}$, consisting of the elements of the image $f[X]$ endowed with the restriction of the order relation $\leqslant^{\mathbb{Y}}$ to $f[X]$, as we proceed to explain.

Definition 1.11. Let $\mathbb{X}$ and $\mathbb{Y}$ be posets. Then $\mathbb{Y}$ is said to be a *subposet* of $\mathbb{X}$ when $Y \subseteq X$ and $\leqslant^{\mathbb{Y}}$ is the restriction of $\leqslant^{\mathbb{X}}$ to Y.

In this case, if no confusion may arise, we shall use the same notation for the order relation of $\mathbb{X}$ and $\mathbb{Y}$.

Proposition 1.12. *A poset $\mathbb{X}$ is isomorphic to a subposet of $\mathbb{Y}$ if and only if there exists an order embedding $f\colon \mathbb{X} \to \mathbb{Y}$. In this case, $\mathbb{X}$ is isomorphic to $\langle f[X]; \leqslant \rangle$, where $\leqslant$ is the restriction of $\leqslant^{\mathbb{Y}}$ to $f[X]$.*

Proof. First, suppose that $\mathbb{X}$ is isomorphic to a subposet $\mathbb{Z}$ of $\mathbb{Y}$. Then there exists an order isomorphism $f\colon \mathbb{X} \to \mathbb{Z}$. It follows that the same map $f\colon \mathbb{X} \to \mathbb{Y}$ is an order embedding. Conversely, suppose that there exists an order embedding $f\colon \mathbb{X} \to \mathbb{Y}$ and let $\langle f[X]; \leqslant \rangle$ be the poset in the statement. The map $f\colon \mathbb{X} \to \langle f[X]; \leqslant \rangle$ is clearly surjective. Furthermore, it is an order embedding, as $f\colon \mathbb{X} \to \mathbb{Y}$ is. Hence, we conclude that $f\colon \mathbb{X} \to \langle f[X]; \leqslant \rangle$ is an order isomorphism. ⊠

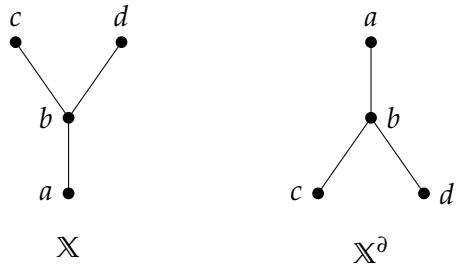
In order theory, it is often useful to construct new posets from old ones.

Definition 1.13. The *dual* $\mathbb{X}^{\partial}$ of a poset $\mathbb{X}$ is the poset $\langle X; \geqslant \rangle$, where $\geqslant$ is the binary relation on X defined, for every $x, y \in X$, as follows:

$$x \geqslant y \iff y \leqslant x.$$

The relation $\geqslant$ is sometimes called the *inverse* of $\leqslant$.

Notice that the dual of $\mathbb{X}$ is essentially the poset obtained putting $\mathbb{X}$ upside down, as the next pictures illustrates.



$\mathbb{X}$ $\qquad$ $\mathbb{X}^{\partial}$

Two of the simplest ways to construct new posets out of old ones are taking disjoint unions and direct products.

Definition 1.14. The *disjoint union* of a family of posets $\{\mathbb{X}_i : i \in I\}$ is the poset

$$\biguplus_{i \in I} \mathbb{X}_i := \langle \bigcup_{i \in I} (X_i \times \{i\}); \leqslant \rangle,$$

whose order relation is defined for every $\langle x, i \rangle, \langle y, j \rangle \in \bigcup_{i \in I} (X_i \times \{i\})$ as follows:

$$\langle x, i \rangle \leqslant \langle y, j \rangle \iff i = j \text{ and } x \leqslant^{\mathbb{X}_i} y.$$

In this case, for every $j \in I$, the map $f_j \colon \mathbb{X}_j \to \biguplus_{i\in I} \mathbb{X}_i$, defined by the rule

$$f_j(x) \coloneqq \langle x, j\rangle,$$

is an order embedding.

Definition 1.15. The *direct product* of a family of posets $\{\mathbb{X}_i : i \in I\}$ is the poset

$$\prod_{i\in I} \mathbb{X}_i \coloneqq \langle \prod_{i\in I} X_i; \leqslant\rangle,$$

whose order relation is defined for every $\vec{x}, \vec{y} \in \prod_{i\in I} X_i$ as follows:

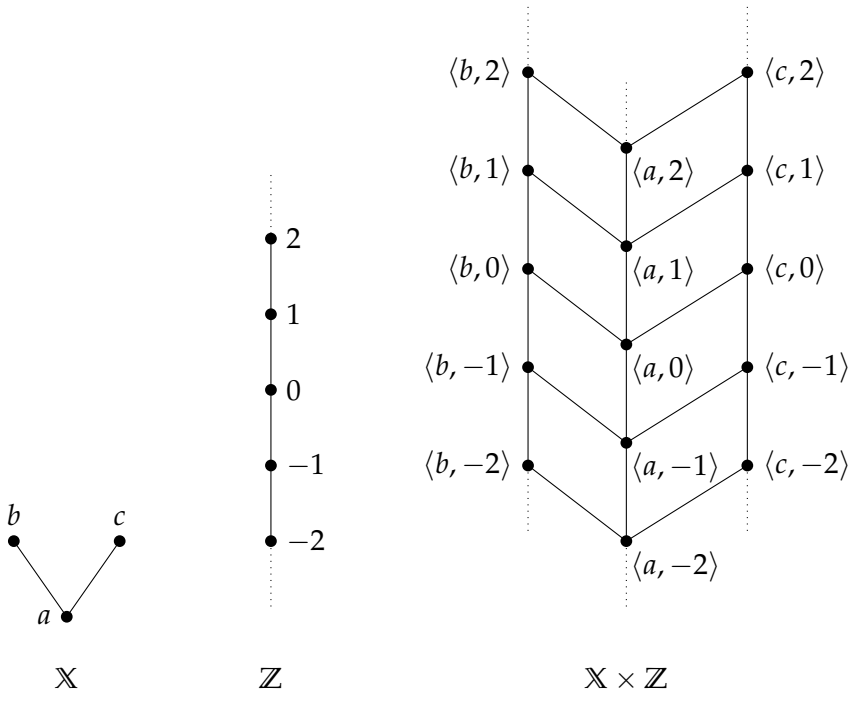
$$\vec{x} \leqslant \vec{y} \iff x_i \leqslant^{\mathbb{X}_i} y_i, \text{ for every } i \in I.$$

In this case, for every $j \in I$, the map $\pi_j \colon \prod_{i\in I} \mathbb{X}_i \to \mathbb{X}_j$, defined by the rule

$$\pi_j(\vec{x}) \coloneqq x_j,$$

is called the *canonical projection* on the j-th coordinate.

When $\{\mathbb{X}_i : i \in I\}$ is a finite set $\{\mathbb{X}_1, \ldots, \mathbb{X}_n\}$, we write $\mathbb{X}_1 \times \cdots \times \mathbb{X}_n$ instead of $\prod_{i\in I} \mathbb{X}_i$. Moreover, when the index set I is empty, $\prod_{i\in I} \mathbb{X}_i$ is the one-element poset. The next picture illustrates the direct product construction in a simple case.



1.2 Chains and antichains

From the knowledge of the length of chains and antichains in a poset $\mathbb{X}$ it is possible to infer useful information on the cardinality of $\mathbb{X}$ itself. For instance, chains and antichains can be used to characterize finite posets, as follows.

Theorem 1.16. *A poset is finite if and only if it lacks both infinite chains and infinite antichains.*

In order to prove this result, it is convenient to recall some notions from combinatorics. Given a map $f\colon X \to C$, we say that the elements of X are *coloured* with colours in C, and that an element $x \in X$ is *coloured* with colour $c \in C$ when $f(x) = c$. In this case, a subset $Y \subseteq X$ is said to be *monochromatic* precisely when its elements have the same colour. Lastly, given $n \in \mathbb{N}$, we denote by $X^{[n]}$ the set of n-element subsets of X. A prominent tool to prove the existence of monochromatic sets is the following.

Ramsey's Theorem 1.17. *Let X be an infinite set, $n, m \in \mathbb{N}$, and $X^{[n]}$ coloured with colours $c_1, \ldots, c_m$. Then there exists an infinite $Y \subseteq X$ such that $Y^{[n]}$ is monochromatic.*

From Ramsey's Theorem we obtain a short proof of Theorem 1.16.

Proof. It is clear that finite posets lack both infinite chains and infinite antichains. To prove the converse, suppose, with a view to contradiction, that there exists an infinite poset $\mathbb{X}$ lacking both infinite chains and infinite antichains. We colour each two-element subset Z of X either in red or in blue, according to the following rule:

(i) Z is coloured in *red* if it is a chain in $\mathbb{X}$; and

(ii) Z is coloured in *blue* if it is an antichain in $\mathbb{X}$.

Notice that no other option is available, because Z is a two-element set.

As the two-element subsets of X are precisely the elements of $X^{[2]}$, we can invoke Ramsey's Theorem obtaining an infinite $Y \subseteq X$ whose two-element subsets are either all chains or all antichains. We detail the case where all the two-element subsets of Y are chains, as the other one is analogous. In this case, every two elements of Y are comparable. It follows that Y is a chain in $\mathbb{X}$. Since Y is infinite, this contradicts the assumption that $\mathbb{X}$ lacks infinite chains, as desired. ⊠

Therefore, it only remains to prove Ramsey's Theorem.

Proof. We reason by induction on n. For the base case, notice that, if $n = 0$, then $X^{[0]} = \{\emptyset\}$. Consequently, all the elements of $X^{[0]}$ have obviously the same color. Hence, taking $Y := X$, we are done.

For the inductive step, suppose that the statement holds for n. We shall prove that it holds for $n + 1$ as well. Accordingly, suppose that $X^{[n+1]}$ is coloured with colours $c_1, \ldots, c_m$. First, define $X_0 := X$. Moreover, choose an element $x_0 \in X$ and let $Z_1 := X_0 \setminus \{x_0\}$. Notice that Z_1 is infinite, because X_0 is. We colour the elements of $Z_1^{[n]}$ with $c_1, \ldots, c_m$ stipulating that an element $A \in Z_1^{[n]}$ is coloured with c_i if and only if $A \cup \{x_0\}$ was coloured with c_i in $X^{[n+1]}$. As Z_1 is infinite, we can apply the inductive hypothesis, obtaining an infinite subset $X_1 \subseteq Z_1$ such that $X_1^{[n]}$ is monochromatic with respect to the colouring of $Z_1^{[n]}$.

We now repeat this construction by choosing an element $x_1 \in X_1$ and considering the infinite set $Z_2 := X_1 \setminus \{x_1\}$. Moreover, we colour the elements of $Z_2^{[n]}$ with $c_1, \ldots, c_m$ stipulating that $A \in Z_2^{[n]}$ is coloured with c_i if and only if $A \cup \{x_1\}$ was

coloured with c_i in $X^{[n+1]}$. Again, as Z_2 is infinite, we can apply the inductive hypothesis, obtaining an infinite subset $X_2 \subseteq Z_2$ such that $X_2^{[n]}$ is monochromatic with respect to the colouring of $Z_2^{[n]}$.

Iterating this process, we obtain a sequence

$$\cdots \subseteq X_{k+1} \subseteq X_k \subseteq \cdots \subseteq X_2 \subseteq X_1 \subseteq X_0 = X \tag{1.1}$$

and an infinite set $\{x_k : k \in \mathbb{N}\} \subseteq X$ such that, for every $k \in \mathbb{N}$:

(i) $x_k \in X_k \setminus X_{k+1}$; and

(ii) $A \cup \{x_k\}$ and $B \cup \{x_k\}$ have the same colour in $X^{[n+1]}$, for all $A, B \in X_{k+1}^{[n]}$.

Since $\{x_k : k \in \mathbb{N}\}$ is infinite, condition (ii) implies the existence of an infinite subset

$$Y \subseteq \{x_k : k \in \mathbb{N}\}$$

such that, for every $x_a, x_c \in Y$, $A \in X_{a+1}^{[n]}$, and $C \in X_{c+1}^{[n]}$,

$$A \cup \{x_a\} \text{ and } C \cup \{x_c\} \text{ have the same colour in } X^{[n+1]}. \tag{1.2}$$

We will prove that $Y^{[n+1]}$ is monochromatic in $X^{[n+1]}$. To this end, consider two generic elements

$$\{x_{k_1}, \ldots, x_{k_{n+1}}\}, \{x_{p_1}, \ldots, x_{p_{n+1}}\} \in Y^{[n+1]}.$$

We can assume, without loss of generality, that

$$k_1 < k_2 < \cdots < k_{n+1} \quad \text{and} \quad p_1 < p_2 < \cdots < p_{n+1}.$$

By (1.1) and (i), this guarantees that $\{x_{k_2}, \ldots, x_{k_{n+1}}\} \subseteq X_{k_1+1}$ and $\{x_{p_2}, \ldots, x_{p_{n+1}}\} \subseteq X_{p_1+1}$, whence

$$\{x_{k_2}, \ldots, x_{k_{n+1}}\} \in X_{k_1+1}^{[n]} \quad \text{and} \quad \{x_{p_2}, \ldots, x_{p_{n+1}}\} \in X_{p_1+1}^{[n]}.$$

Since $x_{k_1}, x_{p_1} \in Y$, we can apply (1.2), obtaining that $\{x_{k_1}, \ldots, x_{k_{n+1}}\}$ and $\{x_{p_1}, \ldots, x_{p_{n+1}}\}$ have the same colour in $X^{[n+1]}$, as desired. ⊠

At this stage, it is natural to wonder whether Theorem 1.16 can be generalized to the infinite case, by replacing "finite" with "of cardinality $< \kappa$" in its statement, where κ is an arbitrary infinite cardinal (notice that the original statement deals with the case where $\kappa = \aleph_0$). This is not the case, however, as shown in the next example.

Example 1.18 (Sierpinski)**.** Recall that a *well-order* $\leqslant$ on a set X is a partial order such that $\langle X; \leqslant \rangle$ is linearly ordered and every nonempty $Y \subseteq X$ has a minimum element with respect to $\leqslant$. Notably, the Axiom of Choice is equivalent to the demand that every set can be endowed with a well-order.

Let $\mathbb{R}$ be the set of real numbers and $\leqslant$ its standard order. We claim that if $X \subseteq \mathbb{R}$ is uncountable, then the restriction of $\leqslant$ to X is not a well-order. To prove this, recall that the set of rational numbers $\mathbb{Q}$ is *dense* in $\mathbb{R}$, in the sense that, for every $x, y \in \mathbb{R}$ such that $x < y$, there exists $z \in \mathbb{Q}$ such that $x < z < y$. Moreover, given $x \in \mathbb{R}$, we set

$$(x, +\infty) := \{y \in \mathbb{R} : x < y\}.$$

Suppose, on the contrary, that there exists an uncountable $X \subseteq \mathbb{R}$ on which $\leqslant$ is a well-order. Let X^- be $X \smallsetminus \{x\}$, if $\langle X; \leqslant \rangle$ has a maximum x, and $X^- := X$ otherwise. For every $x \in X^-$, the set $X \cap (x, +\infty)$ is nonempty. Since $\leqslant$ is a well-order on X, it follows that $X \cap (x, +\infty)$ has a minimum $z_x > x$. Moreover, as $\mathbb{Q}$ is dense in $\mathbb{R}$, there is some $q_x \in \mathbb{Q}$ such that $x < q_x < z_x$.

Accordingly, there exists a map $f \colon X^- \to \mathbb{Q}$ such that

$$x < f(x) < z_x, \text{ for every } x \in X^-.$$

We will prove that f is injective. To this end, consider two $x, y \in X^-$. Since $x \neq y$ and $\langle \mathbb{R}; \leqslant \rangle$ is linearly ordered, we can assume, without loss of generality, that $y \in (x, +\infty)$. By definition of f, this implies $f(x) < z_x \leqslant y$. As also $y < f(y)$, we conclude that $f(x) < f(y)$, whence f is injective. Together with the fact that $\mathbb{Q}$ is countable, this implies that so is X^-. It follows that X is also countable, a contradiction. This establishes the claim.

Now, observe that $\leqslant$ is not a well-order, as the open interval $(0, +\infty)$ is nonempty but has no minimum. However, by the Axiom of Choice, we can find a well-order $\ll$ on $\mathbb{R}$. As the intersection

$$\sqsubseteq \, := \, \leqslant \cap \ll$$

is still a partial order on $\mathbb{R}$, the pair $\langle \mathbb{R}; \sqsubseteq \rangle$ is an uncountable poset. Notice that from the fact that $\ll$ is well-order on $\mathbb{R}$ it follows that so is $\sqsubseteq$.

We shall prove that chains and antichains in $\langle \mathbb{R}; \sqsubseteq \rangle$ are countable. First, let X be a chain in $\langle \mathbb{R}; \sqsubseteq \rangle$. Observe that the restriction of $\leqslant$ to X coincides with that of $\sqsubseteq$, i.e.,

$$\leqslant \cap (X \times X) = \sqsubseteq \cap (X \times X). \tag{1.3}$$

The inclusion from right to left follows from the definition of $\sqsubseteq$. To prove the other one, consider $x, y \in X$ such that $x \leqslant y$. If $x = y$, then $x \sqsubseteq y$, as desired. Then we consider the case where $x < y$ and, therefore, $y \nleqslant x$. Because $\sqsubseteq \, = \, \leqslant \cap \ll$, this implies $y \not\sqsubseteq x$. Since $\langle X; \sqsubseteq \rangle$ is a chain, we conclude that $x \sqsubseteq y$, establishing (1.3).

As $\sqsubseteq$ is a well-order on $\mathbb{R}$, the restriction $\sqsubseteq \cap (X \times X)$ is a well-order on X. Together with (1.3), this implies that the restriction of $\leqslant$ to X is a well-order on X too. Hence, the claim guarantees that X is countable, as desired.

Lastly, consider an antichain X in $\langle \mathbb{R}; \sqsubseteq \rangle$. We shall prove that

$$\langle X; \ll \rangle = \langle X; \leqslant \rangle^\partial. \tag{1.4}$$

To this end, consider $x, y \in X$. We need to prove that $x \ll y$ if and only if $y \leqslant x$. First, suppose that $x \ll y$. If $x = y$, by the reflexivity of $\leqslant$, we obtain $y \leqslant x$, as desired. Then we consider the case $x \neq y$. As $\langle X; \sqsubseteq \rangle$ is an antichain, $x \not\sqsubseteq y$. Together with $\sqsubseteq \, = \, \leqslant \cap \ll$ and $x \ll y$, this implies $x \nleqslant y$. Since $\langle X; \leqslant \rangle$ is linearly ordered, we conclude that $y \leqslant x$, as desired. A similar argument shows that if $y \leqslant x$, then $x \ll y$, thus establishing (1.4).

As the restriction $\sqsubseteq \cap (X \times X)$ is a well-order on X, from (1.4) it follows that restriction of $\geqslant$ to X is also a well-order on X. Since the poset $\langle \mathbb{R}; \leqslant \rangle$ is isomorphic to its dual, our claim implies that that if a set $Y \subseteq \mathbb{R}$ is uncountable, then the restriction of $\geqslant$ to Y is not a well-order. As a consequence, we obtain that X is countable, as desired. ⊠

In view of Theorem 1.16, if the size of chains in a poset $\mathbb{X}$ is bounded above by some $n \in \mathbb{N}$ and, similarly, the size of antichains in $\mathbb{X}$ is bounded above by some $m \in \mathbb{N}$, then $\mathbb{X}$ is finite. It is therefore natural to wonder whether we can obtain a bound on the cardinality of $\mathbb{X}$ in terms of n and m only. Notice that such a bound must be $\geqslant n \times m$, as the disjoint union of m chains of n elements each is a poset that satisfies these restrictions and has precisely $n \times m$ elements. As we shall see, $n \times m$ is indeed a bound on the size of $\mathbb{X}$ and, therefore, the optimal one.

To prove this, we rely on the following notion. A *chain decomposition* of a poset $\mathbb{X}$ is a family $\{Y_i : i \in I\}$ of disjoint chains in $\mathbb{X}$ such that $X = \bigcup_{i \in I} Y_i$. Notice that every poset $\mathbb{X}$ admits at least a chain decomposition, namely $\{\{x\} : x \in X\}$.

Dilworth's Theorem 1.19. *The minimal number m of elements in a chain decomposition of a finite poset $\mathbb{X}$ equals the size n of the largest antichain in $\mathbb{X}$.*

Proof. We claim that every chain decomposition of $\mathbb{X}$ must contain at least n elements. To prove this, consider a chain decomposition $\{Y_i : i \in I\}$ of $\mathbb{X}$. By assumption, $\mathbb{X}$ has an n-element antichain Z. Since $X = \bigcup_{i \in I} Y_i$, for every $z \in Z$ there exists $i_z \in I$ such that $z \in Y_{i_z}$. Furthermore, notice that every two distinct elements x and z of Z are incomparable, because Z is an antichain. Together with the fact that Y_{i_x} and Y_{i_z} are chains such that $x \in Y_{i_x}$ and $z \in Y_{i_z}$, this implies $z \notin Y_{i_x}$ and $x \notin Y_{i_z}$ and, therefore, $Y_{i_x} \neq Y_{i_z}$. As a consequence, the chains $\{Y_{i_z} : z \in Z\}$ are pairwise distinct, whence $n = |Z| \leqslant |I|$. This establishes the claim. As a consequence, we obtain $n \leqslant m$.

To prove that $m \leqslant n$, we reason by complete induction on the cardinality of $\mathbb{X}$. Accordingly, suppose that the inequality holds for all posets of cardinality $< |X|$. We need to prove that $\mathbb{X}$ admits a chain decomposition of size $\leqslant n$, where n is the size of the largest antichain in $\mathbb{X}$.

First, if $\mathbb{X}$ is discrete, then X is itself an antichain and, therefore, $n = |X|$. Consequently, the chain decomposition $\{\{x\} : x \in X\}$ has exactly n elements and we are done.

Then we consider the case where $\mathbb{X}$ is not discrete, that is, there are $\bot, \top \in X$ such that $\bot < \top$. We can assume, without loss of generality, that $\bot$ is minimal and $\top$ is maximal. This is because, as $\mathbb{X}$ is finite, we can apply Proposition 1.5 to the subposet of $\mathbb{X}$ with universe $\{z \in X : \top \leqslant z\}$ to obtain a maximal element $\top^+$ of $\mathbb{X}$ such that $\top \leqslant \top^+$. Then, if $\top$ is not maximal, we replace it with the maximal element $\top^+$. Similarly, if necessary, we replace $\bot$ with a minimal element below it.

Let then $\mathbb{Y}$ be the subposet of $\mathbb{X}$ with universe $X \smallsetminus \{\bot, \top\}$. There are two cases:

(i) either every antichain in $\mathbb{Y}$ has size $\leqslant n - 1$; or

(ii) $\mathbb{Y}$ has an antichain of size n.

If condition (i) holds, then by the inductive hypothesis $\mathbb{Y}$ admits a chain decomposition of size $\leqslant n - 1$. We extend it to a chain decomposition of $\mathbb{X}$ by adding to it the chain $\{\bot, \top\}$. The result is a chain decomposition of $\mathbb{X}$ of size $\leqslant n$, as desired.

On the other hand, if condition (ii) holds, take an antichain Z in $\mathbb{Y}$ of size n. Then define

$$\uparrow Z := \{x \in X : z \leqslant x, \text{ for some } z \in Z\}$$
$$\downarrow Z := \{x \in X : x \leqslant z, \text{ for some } z \in Z\}.$$

We will show that

$$X = \uparrow Z \cup \downarrow Z. \tag{1.5}$$

The inclusion from right to left is obvious. To prove the other, consider an element $x \in X$. Notice that x must be comparable with some element $z \in Z$, otherwise $Z \cup \{x\}$ would be an $(n+1)$-element antichain in $\mathbb{X}$, against the assumption that antichains in $\mathbb{X}$ have size $\leqslant n$ and that Z is an n-element antichain. Thus, $z \leqslant x$ or $x \leqslant z$. In both cases, $x \in \uparrow Z \cup \downarrow Z$.

Now, observe that $\bot \notin \uparrow Z$. For suppose the contrary, with a view to contradiction. Then there exists $z \in Z$ such that $z \leqslant \bot$. Since $z \in Z \subseteq Y = X \smallsetminus \{\bot, \top\}$, this implies $z < \bot$, contradicting the minimality of $\bot$. Therefore,

$$|\uparrow Z| < |X|.$$

Because of this, we can apply the inductive hypothesis to the subposet $\langle \uparrow Z; \leqslant \rangle$ of $\mathbb{X}$, obtaining a chain decomposition $\{Y_1, \ldots, Y_k\}$ of $\langle \uparrow Z; \leqslant \rangle$ with $k \leqslant n$. Now, given $z \in Z$, we denote by Y_z^+ the unique chain Y_i that contains z. Notice that if x and y are distinct elements of Z, then $Y_x^+ \neq Y_y^+$, because x and y are incomparable and Y_x^+ and Y_y^+ are chains such that $x \in Y_x^+$ and $y \in Y_y^+$. Since $|Z| = n$, it follows that the set $\{Y_z^+ : z \in Z\}$ has precisely n elements. Together with the fact that $k \leqslant n$, this yields $\{Y_1, \ldots, Y_k\} = \{Y_z^+ : z \in Z\}$. We conclude that $\{Y_z^+ : z \in Z\}$ is a chain decomposition of $\langle \uparrow Z; \leqslant \rangle$ of size n.

A similar argument shows that there exists a chain decomposition $\{Y_z^- : z \in Z\}$ of size n of the subposet $\langle \downarrow Z; \leqslant \rangle$ of $\mathbb{X}$ such that $z \in Y_z^-$, for every $z \in Z$. We shall prove that the family

$$\{Y_z^+ \cup Y_z^- : z \in Z\}$$

is a chain decomposition of $\mathbb{X}$ of n elements.

The fact that this family has cardinality $\leqslant n$ follows from the assumption that $|Z| = n$. In order to prove that it is indeed a chain decomposition of $\mathbb{X}$, we rely on the following observation: for every $x \in X$ and $z \in Z$,

$$(\text{if } x \in Y_z^+, \text{ then } z \leqslant x) \text{ and } (\text{if } x \in Y_z^-, \text{ then } x \leqslant z). \tag{1.6}$$

To prove this, suppose first that $x \in Y_z^+$. Since Y_z^+ contains z and is a chain, either $x < z$ or $z \leqslant x$. We shall see that the case where $x < z$ never happens. For suppose the contrary, with a view to contradiction. As $x \in Y_z^+ \subseteq \uparrow Z$, there is some $z' \in Z$ such that $z' \leqslant x$. Consequently, $z' \leqslant x < z$, whence there are two distinct elements, namely z and z', of Z that are comparable, contradicting the fact that Z is an antichain. Thus, we conclude that $z \leqslant x$, as desired. A similar argument shows that if $x \in Y_z^-$, then $x \leqslant z$. This establishes (1.6).

To prove that each $Y_z^+ \cup Y_z^-$ is a chain, we need to show that every two elements $x, y \in Y_z^+ \cup Y_z^-$ are comparable. If either $x, y \in Y_z^+$ or $x, y \in Y_z^-$, then x and y are comparable because both Y_z^+ and Y_z^- are chains. Then we can assume, without loss of generality, that $x \in Y_z^+$ and $y \in Y_z^-$. By (1.6), $y \leqslant z \leqslant x$, as desired.

Moreover, if x and y are distinct elements of Z, the chains $Y_x^+ \cup Y_x^-$ and $Y_y^+ \cup Y_y^-$ are disjoint. For suppose the contrary, with a view to contradiction. Then there exists

$$v \in (Y_x^+ \cup Y_x^-) \cap (Y_y^+ \cup Y_y^-). \tag{1.7}$$

Recall that $Y_x^+ \neq Y_y^+$ and $Y_x^- \neq Y_y^-$, since $x \in (Y_x^+ \cap Y_x^-) \smallsetminus (Y_y^+ \cup Y_y^-)$. As $\{Y_z^+ : z \in Z\}$ and $\{Y_z^- : z \in Z\}$ are chain decompositions, this implies $Y_x^+ \cap Y_y^+ = \emptyset$ and

$Y_x^- \cap Y_y^- = \emptyset$. Together with (1.7), this yields that either $v \in Y_x^+ \cap Y_y^-$ or $v \in Y_x^- \cap Y_y^+$. By (1.6), we conclude that either $x \leqslant v \leqslant y$ or $y \leqslant v \leqslant x$. In both cases, x and y are distinct, but comparable, elements of Z, a contradiction with the assumption that Z is an antichain. Thus, $(Y_x^+ \cup Y_y^-) \cap (Y_y^+ \cup Y_x^-) = \emptyset$, as desired.

Hence, $\{Y_z^+ \cup Y_z^- : z \in Z\}$ is a family of $\leqslant n$ disjoint chains. It only remains to prove that its union is X. As $\{Y_z^+ : z \in Z\}$ and $\{Y_z^- : z \in Z\}$ are chain decompositions of $\uparrow Z$ and $\downarrow Z$, respectively, we obtain

$$\bigcup_{z \in Z} Y_z^+ = \uparrow Z \quad \text{and} \quad \bigcup_{z \in Z} Y_z^- = \downarrow Z.$$

Together with (1.5), this yields

$$\bigcup_{z \in Z} (Y_z^+ \cup Y_z^-) = \uparrow Z \cup \downarrow Z = X. \qquad \boxtimes$$

Corollary 1.20. *For every $n, m \in \mathbb{N}$, if chains and antichains in a poset $\mathbb{X}$ are, respectively, of size $\leqslant n$ and $\leqslant m$, then $\mathbb{X}$ has at most $n \times m$ elements.*

Proof. Suppose that chains and antichains in $\mathbb{X}$ are, respectively, of size $\leqslant n$ and $\leqslant m$ and, therefore, finite. Then $\mathbb{X}$ is also finite, by Theorem 1.16. As a consequence, we can apply Dilworth's Theorem, obtaining that $\mathbb{X}$ can be partitioned in $\leqslant m$ chains. Since chains in $\mathbb{X}$ are of size at most n, we conclude that $|X| \leqslant n \times m$. $\boxtimes$

1.3 Lattices

Posets in which certain optimal upper and lower bounds exist will be called *lattices*. The next definition explains what "optimal" means in this context.

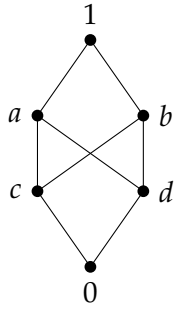
Definition 1.21. Let $\mathbb{X}$ be a poset and $Y \subseteq X$. An element $x \in X$ is said to be

(i) an *infimum of Y in $\mathbb{X}$*, if x is the greatest lower bound of Y in $\mathbb{X}$;

(ii) a *supremum of Y in $\mathbb{X}$*, if x is the least upper bound of Y in $\mathbb{X}$.

When the poset $\mathbb{X}$ is clear from the context, we simply say that x is an infimum (or a supremum) of Y. Furthermore, sometimes we use *meet* and *join* as synonyms for *infimum* and *supremum*. The plural of "infimum" (resp. "supremum") originates from Latin and is *infima* (resp. *suprema*).

Notice that infima and suprema need not exist in posets. For instance, in the poset of natural numbers in $\langle \mathbb{N}; \leqslant \rangle$, the supremum of $\mathbb{N}$ does not exists, because $\mathbb{N}$ has no upper bound in $\langle \mathbb{N}; \leqslant \rangle$. However, even when upper bounds exist, the least one may not exist. For instance, let $\mathbb{X}$ be the poset depicted below.



Every subset $Y \subseteq X$ has both an upper and a lower bound in $\mathbb{X}$. For instance, the unique lower bound of $Y := \{c, d\}$ is 0, while the set of upper bounds of Y is $\{1, a, b\}$. As a consequence, 0 is the greatest lower bound of Y, that is, the infimum of Y. On the other hand, the supremum of Y does not exist, because the set of upper bounds of Y, namely $\{1, a, b\}$, does not have a least element.

Even if infima and suprema need not exists in general, when they do exist, they are necessarily unique.

Proposition 1.22. *If $\mathbb{X}$ is a poset and $Y \subseteq X$, then Y has at most one infimum (resp. supremum) in $\mathbb{X}$.*

Proof. Suppose that $x, y \in X$ are both infima of Y in $\mathbb{X}$. In particular, as x is an infimum of Y, it is a lower bound of Y. Moreover, being an infimum of Y, y is the greatest lower bound of Y. As a consequence, $x \leqslant y$. A similar argument shows that $y \leqslant x$. As the relation $\leqslant$ is antisymmetric, we conclude that $x = y$. The case of suprema is handled similarly. ⊠

In view of the uniqueness of infima and suprema, it makes sense to introduce the following notation. Given a poset $\mathbb{X}$ and a set $Y \subseteq X$,

(i) if the infimum of Y in $\mathbb{X}$ exists, we denote it by $\bigwedge Y$ or $\bigwedge_{y \in Y} y$;

(ii) if the supremum of Y in $\mathbb{X}$ exists, we denote it by $\bigvee Y$ or $\bigvee_{y \in Y} y$.

When it is convenient to stress that these infima and suprema are considered in the poset $\mathbb{X}$, we will add the appropriate superscripts and write

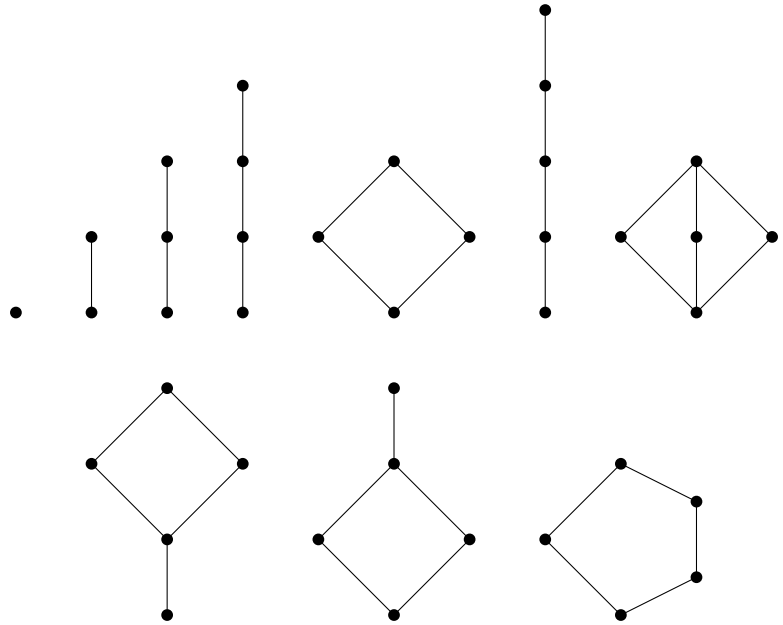
$$\bigwedge^{\mathbb{X}} Y \quad \text{and} \quad \bigvee^{\mathbb{X}} Y.$$

Lastly, when $Y = \{x, y\}$, we will write $x \wedge y$ and $x \vee y$ instead of $\bigwedge Y$ and $\bigvee Y$.

Definition 1.23. A *lattice* is a poset $\mathbb{X}$ such that $X \neq \emptyset$ and in which the infimum and the supremum of $\{x, y\}$ exist, for every pair of elements $x, y \in X$. A lattice $\mathbb{X}$ is said to be *complete* when $\bigwedge Y$ and $\bigvee Y$ exist, for every $Y \subseteq X$.

Every complete lattice $\mathbb{X}$ is bounded, because $\bigvee X$ and $\bigwedge X$ are, respectively, the maximum and the minimum of $\mathbb{X}$.

Lattices of at most 5 elements are depicted below.



Example 1.24 (Powerset lattices)**.** Given a set X, the poset $\langle \mathcal{P}(X); \subseteq \rangle$ is always a complete lattice, known as the *powerset lattice* on X. To prove this, it suffices to show that, for every family $\mathcal{Y} = \{Y_i : i \in I\} \subseteq \mathcal{P}(X)$,

$$\bigwedge^{\mathcal{P}(X)} \mathcal{Y} = \bigcap_{i \in I} Y_i \quad \text{and} \quad \bigvee_{i \in I}^{\mathcal{P}(X)} \mathcal{Y} = \bigcup_{i \in I} Y_i.$$

As an exemplification, we detail the proof of the first equality. Observe that we need to show that $\bigcap_{i \in I} Y_i$ is the greatest lower bound of $\mathcal{Y}$ in $\langle \mathcal{P}(X); \subseteq \rangle$. To this end, notice that $\bigcap_{i \in I} Y_i \subseteq Y_j$, for all $j \in I$, whence $\bigcap_{i \in I} Y_i$ is a lower bound of $\mathcal{Y}$. To prove that $\bigcap_{i \in I} Y_i$ is also the largest such lower bound, consider a lower bound Z of $\mathcal{Y}$ in $\langle \mathcal{P}(X); \subseteq \rangle$. Then $Z \subseteq Y_i$, for all $i \in I$. Consequently, $Z \subseteq \bigcap_{i \in I} Y_i$, as desired. ⊠

Example 1.25 (Chains)**.** Every nonempty chain $\mathbb{X}$ is a lattice. To prove it, notice that, for every $x, y \in X$, the least and greatest elements in $\{x, y\}$ always exist, because $\mathbb{X}$ is a chain and, therefore, x and y must be comparable.

Accordingly, we have that

$$\begin{aligned} x \wedge y &= \text{the least element between } x \text{ and } y, \text{ and} \\ x \vee y &= \text{the greatest element between } x \text{ and } y, \end{aligned}$$

for every $x, y \in X$. To prove the first equality above, let z be the least element of $\{x, y\}$. Then, clearly, $z \leqslant x, y$, whence z is a lower bound of $\{x, y\}$. Furthermore, let $v \in X$ be a lower bound of $\{x, y\}$. As $z \in \{x, y\}$, this implies $v \leqslant z$. We conclude that z is the greatest lower bound of $\{x, y\}$, that is, $z = x \wedge y$. The case of joins is handled similarly.

As every nonempty chain is a lattice, many number systems can be viewed as lattices, including those of natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, and real numbers $\mathbb{R}$ with the standard order. However, none of these lattices is complete, because all of them lack a maximum and, therefore, are not bounded.

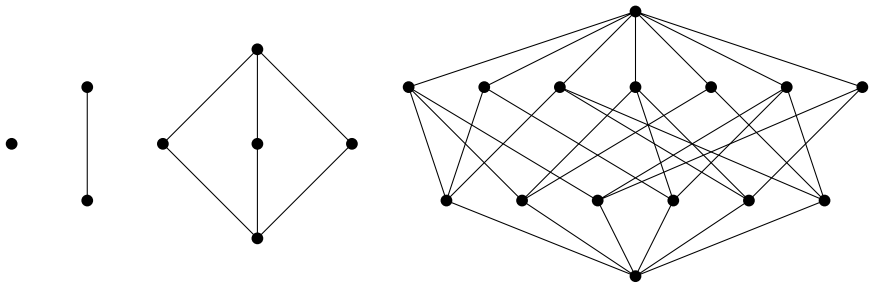
In some cases, this problem can be amended by adding the missing infinity points. For instance, if we add a new minimum $-\infty$ and a new maximum $+\infty$ to $\langle \mathbb{R}; \leqslant \rangle$ or to $\langle \mathbb{Z}; \leqslant \rangle$, we obtain a complete lattice. A similar trick works for the case of $\langle \mathbb{N}; \leqslant \rangle$, where adding a new maximum $+\infty$ is enough.

However, this method does not work for $\langle \mathbb{Q}; \leqslant \rangle$, because the set

$$Y := \{x \in \mathbb{Q} : \pi < x\}$$

lacks an infimum both in $\langle \mathbb{Q}; \leqslant \rangle$ and in its expansion with infinity points. To prove this, suppose, on the contrary, Y has an infimum x (either in $\langle \mathbb{Q}; \leqslant \rangle$ or in its expansion). As π is irrational, $x < \pi$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ (see Example 1.18, if necessary), there exists $y \in \mathbb{Q}$ such that $x < y < \pi$. In particular, y is a lower bound of Y. Together with $x < y$, this contradicts the fact that x is the greatest lower bound of Y. This indicates that the task of completing the lattice $\langle \mathbb{Q}; \leqslant \rangle$ is a more delicate one. We shall come back to this issue in Section 4.4. ⊠

Example 1.26 (Partition Lattices)**.** The *partition lattice* on a nonempty set X is the poset $\langle \mathrm{Eq}(X); \subseteq \rangle$, where $\mathrm{Eq}(X)$ the set of all equivalence relations on X. Partition lattices on nonempty sets of cardinality $1, 2, 3$, and 4 are depicted below.



As the name suggests, partition lattices $\langle \mathrm{Eq}(X); \subseteq \rangle$ are (complete) lattices. To prove this, recall that the *relational product* of two binary relations R and S on X, is the relation

$$R \circ S := \{\langle x, y \rangle \in X \times X : \text{there is } z \in X \text{ such that } \langle x, z \rangle \in R \text{ and } \langle z, y \rangle \in S\}.$$

Moreover, given finitely many binary relations $R_1, \ldots, R_n$ on X, we set

$$R_1 \circ \cdots \circ R_n := (\cdots((R_1 \circ R_2) \circ R_3) \cdots) \circ R_n.$$

Notice that the order of the parentheses in the above definition is immaterial, as relational product is associative.

As $\mathrm{Eq}(X)$ is closed under arbitrary intersections, meets in the partition lattice $\langle \mathrm{Eq}(X); \subseteq \rangle$ are intersections, that is, for every $Y = \{R_i : i \in I\} \subseteq \mathrm{Eq}(X)$,

$$\bigwedge^{\mathrm{Eq}(X)} Y = \bigcap_{i \in I} R_i.$$

On the other hand, joins can be described as follows: for every nonempty $Y = \{R_i : i \in I\} \subseteq \mathrm{Eq}(X)$,

$$\bigvee^{\mathrm{Eq}(X)} Y = \bigcup_{i_1, \ldots, i_n \in I} (R_{i_1} \circ \cdots \circ R_{i_n}) \quad \text{and} \quad \bigvee^{\mathrm{Eq}(X)} \emptyset = \mathrm{id}_X.$$

To prove the second equality above, notice that id_X is the least equivalence relation on X and, therefore, the minimum of $\langle \mathrm{Eq}(X); \subseteq \rangle$. It follows that id_X is the least upper bound of $\emptyset$, as desired. Furthermore, observe that

$$R := \bigcup_{i_1,\ldots,i_n \in I} (R_{i_1} \circ \cdots \circ R_{i_n})$$

is an equivalence relation on X. Moreover, the definition of R guarantees that $R_i \subseteq R$, for all $i \in I$. As a consequence, R is an upper bound of Y in $\langle \mathrm{Eq}(X); \subseteq \rangle$. To prove that it is the least one, consider another upper bound S of Y and a pair $\langle x, y \rangle \in R$. By definition of R, there are $i_1, \ldots, i_n \in I$ and $z_1, \ldots, z_{n-1} \in X$ such that

$$\langle x, z_1 \rangle \in R_{i_1}, \langle z_1, z_2 \rangle \in R_{i_2}, \ldots, \langle z_{n-1}, y \rangle \in R_{i_n}.$$

As $R_{i_1} \cup \cdots \cup R_{i_n} \subseteq S$ and S is transitive, we conclude that $\langle x, y \rangle \in S$, whence $R \subseteq S$, as desired. ⊠

Lattices can be viewed as algebraic structures, as we proceed to explain. To this end, it is convenient to recall some fundamentals of general algebraic systems.

Definition 1.27.

(i) A *type* is a map $\rho \colon \mathcal{F} \to \mathbb{N}$, where $\mathcal{F}$ is a set of function symbols. In this case, $\rho(f)$ is said to be the *arity* of the function symbol f, for every $f \in \mathcal{F}$. Function symbols of arity zero are called *constants*.

(ii) An *algebra* of type ρ is a pair $\boldsymbol{A} = \langle A; F \rangle$ where A is a nonempty set and $F = \{f^{\boldsymbol{A}} : f \in \mathcal{F}\}$ is a set of operations on A whose arity is determined by ρ, in the sense that each $f^{\boldsymbol{A}}$ has arity $\rho(f)$. The set A is called the *universe* of $\boldsymbol{A}$.

When $\mathcal{F} = \{f_1, \ldots, f_n\}$, we shall write $\langle A; f_1^{\boldsymbol{A}}, \ldots, f_n^{\boldsymbol{A}} \rangle$ instead of $\langle A; F \rangle$. In this case, we often drop the superscripts, and write simply $\langle A; f_1, \ldots, f_n \rangle$.

Classical examples of algebras are groups and rings. For instance, the type of groups ρ_G consists of a binary symbol $+$, a unary symbol $-$, and a constant symbol 0. Then a group is an algebra $\langle A; +, -, 0 \rangle$ of type ρ_G in which $+$ is associative, 0 is a neutral element for $+$, and $-$ produces inverses.

Given a type $\rho \colon \mathcal{F} \to \mathbb{N}$ and a set of variables X disjoint from $\mathcal{F}$, the set of *terms of type ρ over X* is the least set $T_\rho(X)$ such that

(i) $X \subseteq T_\rho(X)$;

(ii) if $c \in \mathcal{F}$ is a constant, then $c \in T_\rho(X)$; and

(iii) if $\varphi_1, \ldots, \varphi_{\rho(f)} \in T_\rho(X)$ and $f \in \mathcal{F}$, then $f\varphi_1 \ldots \varphi_{\rho(f)} \in T_\rho(X)$.

For the sake of readability, we shall often write $f(\varphi_1, \ldots, \varphi_{\rho(f)})$ instead of $f\varphi_1 \ldots \varphi_{\rho(f)}$. Similarly, if f is a binary operation $+$, we often write $\varphi_1 + \varphi_2$ instead of $f(\varphi_1, \varphi_2)$.

Given a term $\varphi \in T_\rho(X)$, we write $\varphi(x_1, \ldots, x_n)$ to indicate that the variables occurring in φ are among $x_1, \ldots, x_n$. Furthermore, given an algebra $\boldsymbol{A}$ of type ρ and elements $a_1, \ldots, a_n \in A$, we define an element

$$\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n)$$

of A, by recursion on the construction of φ, as follows:

(i) if φ is a variable x_i, then $\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) := a_i$;

(ii) if φ is a constant c, then $c^{\boldsymbol{A}}$ is the interpretation of c in $\boldsymbol{A}$;

(iii) if $\varphi = f(\psi_1, \ldots, \psi_m)$, then

$$\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) := f^{\boldsymbol{A}}(\psi_1^{\boldsymbol{A}}(a_1, \ldots, a_n), \ldots, \psi_m^{\boldsymbol{A}}(a_1, \ldots, a_n)).$$

An *equation of type ρ over X* is an expression of the form $\varphi \approx \psi$, where $\varphi, \psi \in T_\rho(X)$. Such an equation $\varphi \approx \psi$ is *valid* in an algebra $\boldsymbol{A}$ of type ρ, if

$$\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) = \psi^{\boldsymbol{A}}(a_1, \ldots, a_n), \text{ for every } a_1, \ldots, a_n \in A,$$

in which case we say that $\boldsymbol{A}$ *satisfies* $\varphi \approx \psi$.

For instance, groups are precisely the algebras of type ρ_G that validate the following equations:

$$x + (y + z) \approx (x + y) + z \quad x + 0 \approx x \quad 0 + x \approx x \quad x + -x \approx 0 \quad -x + x \approx 0.$$

Lattices admit a similar equational definition, as algebras whose type ρ_L consists of two binary function symbols $\wedge$ and $\vee$.

Definition 1.28. A *lattice* is an algebra $\boldsymbol{A} = \langle A; \wedge, \vee \rangle$ of type ρ_L satisfying the following equations:

$$\begin{aligned}
x \wedge x &\approx x & x \vee x &\approx x && \text{(idempotent laws)}\\
x \wedge y &\approx y \wedge x & x \vee y &\approx y \vee x && \text{(commutative laws)}\\
x \wedge (y \wedge z) &\approx (x \wedge y) \wedge z & x \vee (y \vee z) &\approx (x \vee y) \vee z && \text{(associative laws)}\\
x \wedge (y \vee x) &\approx x & x \vee (y \wedge x) &\approx x. && \text{(absorption laws)}
\end{aligned}$$

As lattice operations are associative, we sometimes drop parentheses and write, for instance,

$$x \wedge y \wedge z, \text{ as a shorthand for } x \wedge (y \wedge z).$$

In order to prove that the order theoretic definition of a lattice (that is, Definition 1.23) is equivalent to the one above, we shall explain how to transform a structure which is a lattice according to the first definition into one that is a lattice according to the second definition and vice versa, and then show that these transformations are one inverse to the other.

To this end, consider a lattice $\boldsymbol{A} = \langle A; \wedge, \vee \rangle$ in the sense of Definition 3.8. Notice that for all $a, c \in A$,

$$a \wedge c = a \iff a \vee c = c. \tag{1.8}$$

This is because, if $a \wedge c = a$, then $a \vee c = (a \wedge c) \vee c$. By commutativity, $(a \wedge c) \vee c = c \vee (a \wedge c)$ and, by absorption, $c \vee (a \wedge c) = c$. Thus, $a \vee c = c$. This establishes the implication from left to right. The other one is proved similarly.

Bearing this in mind, consider the binary relation $\leqslant$ on A, defined for every $a, c \in A$, as

$$a \leqslant c \iff (a \wedge c = a \text{ or, equivalently, } a \vee c = c),$$

where the equivalence in parentheses follows from (1.8). The relational structure associated with $\boldsymbol{A}$ is

$$\boldsymbol{A}^p := \langle A; \leqslant \rangle.$$

On the other hand, given a lattice $\mathbb{X}$ in the sense of Definition 1.23, consider the binary operations

$$\wedge\colon X \times X \to X \quad \text{and} \quad \vee\colon X \times X \to X,$$

whose values on the argument $\langle x, y\rangle$ are, respectively, the meet $x \wedge y$ and the join $x \vee y$ of the set $\{x, y\}$ in $\mathbb{X}$. The algebra associated with $\mathbb{X}$ is

$$\mathbb{X}^a := \langle X; \wedge, \vee\rangle.$$

Proposition 1.29. *Let $\mathbb{X}$ and $\boldsymbol{A}$ be lattices in the sense of Definitions 1.23 and 3.8, respectively. The following conditions hold:*

(i) *$\mathbb{X}^a$ is a lattice in the sense of Definition 3.8;*

(ii) *$\boldsymbol{A}^p$ is a lattice in the sense of Definition 1.23; and*

(iii) *$\mathbb{X} = \mathbb{X}^{ap}$ and $\boldsymbol{A} = \boldsymbol{A}^{pa}$.*

Proof. (i): Consider $x, y, z \in X$. First, $x \wedge x \leqslant x$, since $x \wedge x$ is a lower bound of $\{x\}$. Furthermore, notice that x is also a lower bound of $\{x\}$. Since $x \wedge x$ is the greatest such lower bound, $x \leqslant x \wedge x$. By the antisymmetry of $\leqslant$, we conclude $x = x \wedge x$. A similar argument shows that $x = x \vee x$. Hence, $\mathbb{X}^a$ satisfies the idempotent laws.

The fact that it satisfies also the commutative laws is an immediate consequence of $\{x, y\} = \{y, x\}$.

To prove the associative laws, observe that $x \wedge (y \wedge z) \leqslant x, y \wedge z$, as $x \wedge (y \wedge z)$ is a lower bound of $\{x, y \wedge z\}$. Moreover, $y \wedge z \leqslant y, z$, as $y \wedge z$ is a lower bound of $\{y, z\}$. By the transitivity of $\leqslant$, we obtain $x \wedge (y \wedge z) \leqslant x, y, z$. In particular, $x \wedge (y \wedge z)$ is a lower bound of $\{x, y\}$. Since $x \wedge y$ is the greatest such lower bound, $x \wedge (y \wedge z) \leqslant x \wedge y$. Thus, $x \wedge (y \wedge z) \leqslant x \wedge y, z$, that is, $x \wedge (y \wedge z)$ is a lower bound of $\{x \wedge y, z\}$. Again, since $(x \wedge y) \wedge z$ is the greatest such lower bound,

$$x \wedge (y \wedge z) \leqslant (x \wedge y) \wedge z.$$

Similarly, we obtain $(x \wedge y) \wedge z \leqslant x \wedge (y \wedge z)$ and, therefore, by the antisymmetry of $\leqslant$, $x \wedge (y \wedge z) = (x \wedge y) \wedge z$. An analogous argument shows that $x \vee (y \vee z) = (x \vee y) \vee z$, thus showing that $\mathbb{X}^a$ satisfies the associative laws.

It only remains to prove the absorption laws. To this end, observe that $x \leqslant x, y \vee x$, because $\leqslant$ is reflexive and $y \vee x$ an upper bound of $\{y, x\}$. Then x is a lower bound for $\{x, y \vee x\}$. Since $x \wedge (y \vee x)$ is the largest such lower bound, $x \leqslant x \wedge (y \vee x)$. Furthermore, $x \wedge (y \vee x) \leqslant x$, since $x \wedge (y \vee x)$ is a lower bound of $\{x, y \vee x\}$. By the antisymmetry of $\leqslant$, we conclude that $x \wedge (y \vee x) = x$. A similar argument yields $x \vee (y \wedge x) = x$, thus establishing the validity of the absorption laws in $\mathbb{X}^a$. We conclude that $\mathbb{X}^a$ is a lattice in the sense of Definition 3.8.

(ii): We begin by proving that $\boldsymbol{A}^p = \langle A; \leqslant\rangle$ is a poset. To this end, consider $a, b, c \in A$. By the idempotent laws, $a \wedge a = a$. Consequently, $a \leqslant a$ and, therefore, $\leqslant$ is reflexive. To prove that $\leqslant$ is antisymmetric, suppose that $a \leqslant c$ and $c \leqslant a$. Then $a \wedge c = a$ and $c \wedge a = c$. By the commutative laws,

$$a = a \wedge c = c \wedge a = c,$$

as desired. To prove that $\leqslant$ is transitive, suppose that $a \leqslant b$ and $b \leqslant c$, that is,

$$a \wedge b = a \quad \text{and} \quad b \wedge c = b.$$

Together with the associative laws, this yields

$$a \wedge c = (a \wedge b) \wedge c = a \wedge (b \wedge c) = a \wedge b = a,$$

that is, $a \leqslant c$. Hence, we conclude that $\boldsymbol{A}^p$ is a poset.

Accordingly, to prove that $\boldsymbol{A}^p$ is a lattice in the sense of Definition 1.23, it suffices to show that $a \wedge c$ and $a \vee c$ are, respectively, the infimum and the supremum of $\{a, c\}$ in $\boldsymbol{A}^p$, for all $a, c \in A$. To this end, notice that, applying in succession the commutative, associative, and idempotent laws, we obtain

$$(a \wedge c) \wedge a = a \wedge (a \wedge c) = (a \wedge a) \wedge c = a \wedge c.$$

By definition of $\leqslant$, this means $a \wedge c \leqslant a$. A similar argument yields $a \wedge c \leqslant c$. Thus, $a \wedge c$ is a lower bound of $\{a, c\}$ in $\boldsymbol{A}^p$. To prove that it is the largest one, suppose that b is also a lower bound of $\{a, c\}$ in $\boldsymbol{A}^p$, that is, $b \leqslant a, c$. By definition of $\leqslant$, this means that $b \wedge a = b$ and $b \wedge c = b$. Together with the associative laws, this implies

$$b \wedge (a \wedge c) = (b \wedge a) \wedge c = b \wedge c = b,$$

that is, $b \leqslant a \wedge c$. Thus, we conclude that $a \wedge c$ is the infimum of $\{a, c\}$ in $\boldsymbol{A}^p$. A similar argument shows that $a \vee c$ is the supremum of $\{a, c\}$ in $\boldsymbol{A}^p$.

(iii): To prove that $\mathbb{X} = \mathbb{X}^{ap}$, consider $x, y \in X$. We have

$$x \leqslant^{\mathbb{X}} y \iff x \text{ is the infimum of } \{x, y\} \text{ in } \mathbb{X}.$$

To prove this, suppose first that $x \leqslant^{\mathbb{X}} y$. As $\leqslant^{\mathbb{X}}$ is reflexive, x is a lower bound of $\{x, y\}$ in $\mathbb{X}$. To prove that it is the largest one, consider another such lower bound z. Then $z \leqslant x$, as desired. Thus, x is the infimum of $\{x, y\}$ in $\mathbb{X}$. Conversely, if x is the infimum of $\{x, y\}$ in $\mathbb{X}$, then, clearly, $x \leqslant^{\mathbb{X}} y$.

In view of the above display, we obtain

$$\begin{aligned} x \leqslant^{\mathbb{X}} y &\iff x \text{ is the infimum of } \{x, y\} \text{ in } \mathbb{X} \\ &\iff x = x \wedge^{\mathbb{X}^a} y \\ &\iff x \leqslant^{\mathbb{X}^{ap}} y, \end{aligned}$$

where the last two equivalences follow from the definitions of $\mathbb{X}^a$ and $\mathbb{X}^{ap}$. Hence, we conclude that $\mathbb{X} = \mathbb{X}^{ap}$, as desired.

To prove that $\boldsymbol{A} = \boldsymbol{A}^{pa}$, consider $a, c \in A$. Since $a \wedge^{\boldsymbol{A}^{pa}} c$ is the infimum of $\{a, c\}$ in $\boldsymbol{A}^p$, we have $a \wedge^{\boldsymbol{A}^{pa}} c \leqslant^{\boldsymbol{A}^p} a, c$. By definition of the relation $\leqslant^{\boldsymbol{A}^p}$, this means that

$$(a \wedge^{\boldsymbol{A}^{pa}} c) \wedge^{\boldsymbol{A}} a = a \wedge^{\boldsymbol{A}^{pa}} c \quad \text{and} \quad (a \wedge^{\boldsymbol{A}^{pa}} c) \wedge^{\boldsymbol{A}} c = a \wedge^{\boldsymbol{A}^{pa}} c.$$

Together with the fact that the associative laws are valid in $\boldsymbol{A}$, this yields

$$(a \wedge^{\boldsymbol{A}^{pa}} c) \wedge^{\boldsymbol{A}} (a \wedge^{\boldsymbol{A}} c) = ((a \wedge^{\boldsymbol{A}^{pa}} c) \wedge^{\boldsymbol{A}} a) \wedge^{\boldsymbol{A}} c = (a \wedge^{\boldsymbol{A}^{pa}} c) \wedge^{\boldsymbol{A}} c = a \wedge^{\boldsymbol{A}^{pa}} c,$$

which, by definition of $\boldsymbol{A}^p$, amounts to $a \wedge^{\boldsymbol{A}^{pa}} c \leqslant^{\boldsymbol{A}^p} a \wedge^{\boldsymbol{A}} c$.

Lastly, applying in succession the commutative, associative, and idempotent laws in $\boldsymbol{A}$, we obtain

$$(a \wedge^{\boldsymbol{A}} c) \wedge^{\boldsymbol{A}} a = a \wedge^{\boldsymbol{A}} (a \wedge^{\boldsymbol{A}} c) = (a \wedge^{\boldsymbol{A}} a) \wedge^{\boldsymbol{A}} c = a \wedge^{\boldsymbol{A}} c.$$

By definition of $\boldsymbol{A}^p$, this is $a \wedge^{\boldsymbol{A}} c \leqslant^{\boldsymbol{A}^p} a$. Similarly, we obtain $a \wedge^{\boldsymbol{A}} c \leqslant^{\boldsymbol{A}^p} c$, whence $a \wedge^{\boldsymbol{A}} c$ is a lower bound of $\{a, c\}$ in $\boldsymbol{A}^p$. Since $a \wedge^{\boldsymbol{A}^{pa}} c$ is the largest such lower bound, we obtain that $a \wedge^{\boldsymbol{A}} c \leqslant^{\boldsymbol{A}^p} a \wedge^{\boldsymbol{A}^{pa}} c$. As $\leqslant^{\boldsymbol{A}^p}$ is antisymmetric, we conclude that $a \wedge^{\boldsymbol{A}} c = a \wedge^{\boldsymbol{A}^{pa}} c$. A similar argument shows that $a \vee^{\boldsymbol{A}} c = \vee^{\boldsymbol{A}^{pa}} c$, whence $\boldsymbol{A} = \boldsymbol{A}^{pa}$. ⊠

In view of Proposition 1.29, from now on we shall treat lattices both as posets and algebras without further notice. Furthermore, as the operations of lattices are associative we often drop superfluous parentheses and write, for instance,

$$(a \wedge b \wedge c) \vee (d \vee e \vee f) \text{ as a shorthand for } ((a \wedge b) \wedge c) \vee (d \vee (e \vee f)).$$

In this terminology, we have the following.

Proposition 1.30. *Let $\boldsymbol{A}$ be a lattice. For every $a_1, \dots, a_n \in A$, the elements $a_1 \wedge \cdots \wedge a_n$ and $a_1 \vee \cdots \vee a_n$ are, respectively, the meet and the join of $\{a_1, \dots, a_n\}$ in $\boldsymbol{A}$. Consequently, meets and joins of finite nonempty subsets of A exist in $\boldsymbol{A}$.*

Proof. We detail the case of meets only, as that of joins is analogous. Let

$$c \coloneqq (\dots (a_1 \wedge a_2) \wedge \dots) \wedge a_n.$$

We will prove that c is the meet of $\{a_1, \dots, a_n\}$ in $\boldsymbol{A}$. From the definition of a meet it follows that $a_1 \wedge a_2 \leqslant a_1, a_2$. Similarly, $(a_1 \wedge a_2) \wedge a_3 \leqslant a_1 \wedge a_2, a_3$. Since $\leqslant$ is transitive, we obtain $(a_1 \wedge a_2) \wedge a_3 \leqslant a_1, a_2, a_3$. Iterating this argument, we obtain that c is a lower bound of $\{a_1, \dots, a_n\}$ in $\boldsymbol{A}$. It only remains to prove that it is the largest one. To this end, consider a lower bound b of $\{a_1, \dots, a_n\}$ in $\boldsymbol{A}$. In particular, b is a lower bound of $\{a_1, a_2\}$ in $\boldsymbol{A}$. As $a_1 \wedge a_2$ is the greatest such lower bound, $b \leqslant a_1 \wedge a_2$. Moreover, by assumption, $b \leqslant a_3$, whence b is also a lower bound of $\{a_1 \wedge a_2, a_3\}$ in $\boldsymbol{A}$. Again, since $(a_1 \wedge a_2) \wedge a_3$ is the greatest such lower bound, $b \leqslant (a_1 \wedge a_2) \wedge a_3$. Iterating this process, we obtain that $b \leqslant c$, as desired. ⊠

At this stage it is worth observing that if $\boldsymbol{A}$ is a lattice, then its dual $\boldsymbol{A}^\partial$ is also a lattice. As a consequence, we obtain the following principle, which is sometimes instrumental to shorten proofs.

Duality Principle 1.31. *If a statement Φ is true in all lattices, then the statement obtained by replacing $\bigwedge$ with $\bigvee$, $\bigvee$ with $\bigwedge$, $\leqslant$ with $\geqslant$, and $\geqslant$ with $\leqslant$ in Φ is also true in all lattices.*

1.4 Whitman's representation

Algebras of the same type are called *similar* and can be compared by means of maps that preserve their structure.

Definition 1.32. Given two similar algebras $\boldsymbol{A}$ and $\boldsymbol{B}$, a *homomorphism* from $\boldsymbol{A}$ to $\boldsymbol{B}$ is a map $f\colon A \to B$ such that, for every n-ary operation g of the common type and $a_1, \dots, a_n \in A$,

$$f(g^{\boldsymbol{A}}(a_1, \dots, a_n)) = g^{\boldsymbol{B}}(f(a_1), \dots, f(a_n)).$$

An injective homomorphism is called an *embedding* and, if there exists an embedding from $\boldsymbol{A}$ to $\boldsymbol{B}$, we say that $\boldsymbol{A}$ *embeds* into $\boldsymbol{B}$. Lastly, a surjective embedding is called an *isomorphism*. Accordingly, $\boldsymbol{A}$ and $\boldsymbol{B}$ are said to be *isomorphic* if there exists an isomorphism between them, in which case we write $\boldsymbol{A} \cong \boldsymbol{B}$.

In particular, a homomorphism from a lattice $\boldsymbol{A}$ to a lattice $\boldsymbol{B}$ is a map $f\colon A \to B$ such that, for every $a, c \in A$,

$$f(a \wedge^{\boldsymbol{A}} c) = f(a) \wedge^{\boldsymbol{B}} f(c) \quad \text{and} \quad f(a \vee^{\boldsymbol{A}} c) = f(a) \vee^{\boldsymbol{B}} f(c).$$

For instance, the inclusion map from the lattice $\langle \mathbb{N}; \leqslant \rangle$ into the lattice $\langle \mathbb{Z}; \leqslant \rangle$ is an injective homomorphism, that is, an embedding. Similarly, given two sets $Y \subseteq X$, the inclusion map from the powerset lattice $\langle \mathcal{P}(Y); \subseteq \rangle$ to the powerset lattice $\langle \mathcal{P}(X); \subseteq \rangle$ is also an embedding. On the other hand, if $Y \subsetneq X$, the map

$$(-) \cap Y \colon \mathcal{P}(X) \to \mathcal{P}(Y)$$

that sends every $Z \subseteq X$ to $Z \cap Y$ is a noninjective homomorphism from $\langle \mathcal{P}(X); \subseteq \rangle$ to $\langle \mathcal{P}(Y); \subseteq \rangle$.

Notice that homomorphisms between lattices need not preserve *infinite* meets and joins. For instance, let $\langle \mathbb{N}^+; \leqslant \rangle$ be the complete lattice obtained by adding a maximum $+\infty$ to $\langle \mathbb{N}; \leqslant \rangle$. Then the map

$$f \colon \mathbb{N}^+ \to \mathbb{R},$$

defined as

$$f(+\infty) \coloneqq 2 \quad \text{and} \quad f(n) \coloneqq \frac{2^n - 1}{2^n}, \text{ for every } n \in \mathbb{N},$$

is a an embedding of $\langle \mathbb{N}^+; \leqslant \rangle$ into $\langle \mathbb{R}; \leqslant \rangle$. However, it does not preserve arbitrary joins, because

$$f\Big(\bigvee_{n \in \mathbb{N}}^{\mathbb{N}^+} n\Big) = f(+\infty) = 2 \neq 1 = \bigvee_{n \in \mathbb{N}}^{\mathbb{R}} \Big(\frac{2^n - 1}{2^n}\Big) = \bigvee_{n \in \mathbb{N}}^{\mathbb{R}} f(n).$$

Proposition 1.33. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be lattices and $f \colon A \to B$ a function. The following hold:*

(i) *if f is a homomorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$, then it is an order preserving map from $\boldsymbol{A}$ to $\boldsymbol{B}$;*

(ii) *if f is an embedding from $\boldsymbol{A}$ to $\boldsymbol{B}$, then it is an order embedding from $\boldsymbol{A}$ to $\boldsymbol{B}$;*

(iii) *f is an isomorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$ if and only if it is an order isomorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$.*

Proof. (i): Consider $a, c \in A$ such that $a \leqslant^{\boldsymbol{A}} c$. Then $a = a \wedge^{\boldsymbol{A}} c$. Since f is a homomorphism,

$$f(a) = f(a \wedge^{\boldsymbol{A}} c) = f(a) \wedge^{\boldsymbol{B}} f(c),$$

that is, $f(a) \leqslant^{\boldsymbol{B}} f(c)$. We conclude that f is order preserving.

(ii): We need to prove that, for all $a, c \in A$,

$$a \leqslant^{\boldsymbol{A}} c \iff f(a) \leqslant^{\boldsymbol{B}} f(c).$$

The implication from left to right follows from condition (i). To prove the other one, suppose that $f(a) \leqslant^{\boldsymbol{B}} f(c)$, that is, $f(a) = f(a) \wedge^{\boldsymbol{B}} f(c)$. Since f is a homomorphism,

$$f(a \wedge^{\boldsymbol{A}} c) = f(a) \wedge^{\boldsymbol{B}} f(c) = f(a).$$

As f is injective, this yields $a \wedge^{\boldsymbol{A}} c = a$, whence $a \leqslant^{\boldsymbol{A}} c$.

(iii): First, let f be an isomorphism. By condition (ii), it is also an order embedding. Since f is surjective, we conclude that it is an order isomorphism.

Conversely, suppose that f is an order isomorphism. Since f is a bijection, it suffices to show that f preserves binary infima and suprema. To this end, consider $a, c \in A$. We begin by showing that $f(a \wedge^{\boldsymbol{A}} c)$ is the infimum of $\{f(a), f(c)\}$ in $\boldsymbol{B}$. First, as $a \wedge^{\boldsymbol{A}} c \leqslant^{\boldsymbol{A}} a, c$ and f is order preserving, $f(a \wedge^{\boldsymbol{A}} c) \leqslant^{\boldsymbol{B}} f(a), f(c)$. Hence, $f(a \wedge^{\boldsymbol{A}} c)$

is a lower bound of $\{f(a), f(c)\}$ in $\boldsymbol{B}$. To prove that it is the largest one, consider $b \in B$ such that $b \leqslant^{\boldsymbol{B}} f(a), f(c)$. Since f is surjective, there exists $d \in A$ such that $f(d) = b$. Thus, $f(d) \leqslant^{\boldsymbol{B}} f(a), f(c)$. Since f is order reflecting, $d \leqslant^{\boldsymbol{A}} a, c$. As $a \wedge^{\boldsymbol{A}} c$ is the largest lower bound of $\{a, c\}$ in $\boldsymbol{A}$, this implies $d \leqslant^{\boldsymbol{A}} a \wedge^{\boldsymbol{A}} c$. Lastly, as f is order preserving,

$$b = f(d) \leqslant^{\boldsymbol{B}} f(a \wedge^{\boldsymbol{A}} c).$$

We conclude that $f(a \wedge^{\boldsymbol{A}} c)$ is the infimum of $\{f(a), f(c)\}$ in $\boldsymbol{B}$, that is, $f(a \wedge^{\boldsymbol{A}} c) = f(a) \wedge^{\boldsymbol{B}} f(c)$. Similarly, we obtain $f(a \vee^{\boldsymbol{A}} c) = f(a) \vee^{\boldsymbol{B}} f(c)$. ⊠

Definition 1.34. Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be algebras of the same type $\rho\colon \mathcal{F} \to \mathbb{N}$. Then $\boldsymbol{A}$ is said to be a *subalgebra* of $\boldsymbol{B}$ if $A \subseteq B$ and $f^{\boldsymbol{A}}$ is the restriction of $f^{\boldsymbol{B}}$ to A, for every $f \in \mathcal{F}$. In this case, we write $\boldsymbol{A} \leqslant \boldsymbol{B}$.

The following observation is an immediate consequence of the definitions.

Proposition 1.35. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be algebras of the same type. Then $\boldsymbol{A}$ is isomorphic to a subalgebra of $\boldsymbol{B}$ if and only if there exists an embedding $f\colon \boldsymbol{A} \to \boldsymbol{B}$. In this case, $\boldsymbol{A}$ is isomorphic to the unique subalgebra of $\boldsymbol{B}$ with universe $f[A]$.*

In general algebra, theorems asserting that the operations of certain algebras can be viewed as familiar functions play a fundamental role. Results of this sort are often called *representation theorems* and, typically, express the existence of embeddings from algebras of a certain kind (lattices, groups, rings etc.) into some special algebras, whose basic operations are better understood or perceived as more "concrete". For instance, Cayley's Theorem, stating that every group embeds into a symmetric group, falls in this category, because the operations of a symmetric group are very simple. In the case of lattices, we have the following.

Whitman's Theorem 1.36. *Every lattice embeds into a partition lattice.*

In order to prove this, it is convenient to introduce some new concept. A *weak representation* of a lattice $\boldsymbol{A}$ is a pair $\langle f, X\rangle$, where X is a nonempty set and $f\colon \boldsymbol{A} \to \mathrm{Eq}(X)$ an injective map such that

$$f(a \wedge c) = f(a) \cap f(c), \text{ for all } a, c \in A.$$

Given a pair $\langle f, X\rangle$ and $\langle g, Y\rangle$ of weak representations of $\boldsymbol{A}$, we say that $\langle g, Y\rangle$ *extends* $\langle f, X\rangle$ when

$$X \subseteq Y \text{ and } f(a) = g(a) \cap (X \times X), \text{ for all } a \in A.$$

Lemma 1.37. *Let $\boldsymbol{A}$ be a lattice, X a set, $a, c \in A$, and $x, y \in X$. Every weak representation $\langle f, X\rangle$ of $\boldsymbol{A}$ such that $\langle x, y\rangle \in f(a \vee c)$ can be extended to a weak representation $\langle g, Y\rangle$ of $\boldsymbol{A}$ such that*

$$\langle x, y\rangle \in g(a) \vee^{\mathrm{Eq}(Y)} g(c).$$

Proof. Let Y be the set obtained by adding three new elements p, q, and m to X. Then, for every $b \in A$, let $g(b)$ be the equivalence relation on Y obtained extending $f(b)$ as follows:

(i) if $a, c \leqslant b$, we add p, q, and m to the equivalence class of x;

(ii) if $a \leqslant b$ and $c \not\leqslant b$, we add p to the equivalence class of x and make $\{q, m\}$ a new equivalence class;

(iii) if $a \not\leqslant b$ and $c \leqslant b$, we add m to the equivalence class of y and make $\{p, q\}$ a new equivalence class; and

(iv) if $a, c \not\leqslant b$, we make $\{p\}$, $\{q\}$, and $\{m\}$ new equivalence classes.

Observe that condition (i) could have been equivalently stated as the demand that if $a, c \leqslant b$, we add p, q, and m to the equivalence class of y. This is because, if $a, c \leqslant b$, then

$$\langle x, y\rangle \in f(a \vee c) \subseteq f(b),$$

because f is order preserving and $\langle x, y\rangle \in f(a \vee c)$, by assumption. Notice that this equivalent formulation of (i) yields $\langle m, y\rangle \in g(c)$.

Together with the definition of $g(a)$ and $g(c)$, this implies

$$\langle x, p\rangle, \langle q, m\rangle \in g(a) \text{ and } \langle p, q\rangle, \langle m, y\rangle \in g(c). \tag{1.9}$$

As a consequence,

$$\langle x, y\rangle \in g(a) \circ g(c) \circ g(a) \circ g(c) \subseteq g(a) \vee^{\mathrm{Eq(Y)}} g(c),$$

where the latter inclusion follows from the description of joins in partition lattices given in Example 1.26.

Therefore, to conclude the proof, it only remains to show that $\langle g, Y\rangle$ is a weak representation of $\boldsymbol{A}$ extending $\langle f, X\rangle$. Since, for all $b \in A$, the restriction of $g(b)$ to $X \times X$ is $f(b)$, the injectivity of f implies that of g. By the same token, if $\langle g, Y\rangle$ is a weak representation of $\boldsymbol{A}$, then it extends $\langle f, X\rangle$. Therefore, it only remains to prove that g preserves binary meets.

Consider $b, d \in A$. Since f is a weak representation of $\boldsymbol{A}$, we have $f(b \wedge d) = f(b) \cap f(d)$. We need to prove that also $g(b \wedge d) = g(b) \cap g(d)$. To this end, we treat the following cases separately:

1. $a, c \leqslant b, d$;

2. $a \leqslant b, d$ and ($c \not\leqslant b$ or $c \not\leqslant d$);

3. ($a \not\leqslant b$ or $a \not\leqslant d$) and $c \leqslant b, d$;

4. none of the above conditions holds.

(1): In this case, $g(b)$ is obtained from $f(b)$ by adding p, q, and m to the equivalence class of x, and $g(d)$ is obtained in the same way from $f(d)$. Moreover, from $a, c \leqslant b, d$ it follows $a, c \leqslant b \wedge d$. As a consequence, $g(b \wedge d)$ is obtained from $f(b) \cap f(d)$ (that is, from $f(b \wedge d)$) by adding p, q, and m to the equivalence class of x. It follows that $g(b \wedge d) = g(b) \cap g(d)$.

(2): By symmetry, we can assume, without loss of generality, that $c \not\leqslant b$. As a consequence, $a \leqslant b$ and $c \not\leqslant b$, whence $g(b)$ is obtained from $f(b)$ by adding p to the equivalence class of x and making $\{q, m\}$ a new equivalence class. Moreover, as $a \leqslant b \wedge d$ and $c \not\leqslant b \wedge d$, the relation $g(b \wedge d)$ is obtained in the same way from $f(b) \cap f(d)$. Lastly, the definition of $g(d)$ depends on whether $c \leqslant d$ or $c \not\leqslant d$. If $c \not\leqslant d$, then $g(d)$ is obtained from $f(d)$ by adding p to the equivalence class of x and

making $\{q, m\}$ a new equivalence class. On the other hand, if $c \leqslant d$, then $g(d)$ is obtained from $f(d)$ by adding p, q, and m to the equivalence class of x. In both cases, $g(b \wedge d) = g(b) \cap g(d)$.

(3): This case is handled analogously to the previous one, provided that one uses the equivalent formulation of condition (i) in which y takes the role of x.

(4): We can assume, without loss of generality, that $a \not\leqslant b$ and that $c \not\leqslant b$ or $c \not\leqslant d$. We claim that the equivalence classes of p, q, and m in $g(b) \cap g(d)$ are the singletons

$$\{p\}, \{q\}, \text{ and } \{m\}.$$

First, if $c \not\leqslant b$, then $a \not\leqslant b$ and $c \not\leqslant b$. In this case, the equivalence class of p, q, and m in $g(b)$ are, respectively, $\{p\}, \{q\}$, and $\{m\}$. Hence, the same holds for $g(b) \cap g(d)$, as desired. Then we consider the case where $c \leqslant b$. In this case, $c \not\leqslant d$. Now, since $a \not\leqslant b$, the equivalence classes of p (equiv. of q) in $g(b)$ is $\{p, q\}$. Furthermore, as $c \not\leqslant d$, the equivalence classes of q and m in $g(d)$ are either $\{q\}$ and $\{m\}$ or $\{q, m\}$. In both cases, the equivalence classes of p, q, and m in $g(b) \cap g(d)$ are, respectively, $\{p\}, \{q\}$, and $\{m\}$, establishing the claim.

Lastly, from the claim it follows that $g(b) \cap g(d)$ is $f(b) \cap f(d)$ extended with the new equivalence classes $\{p\}$, $\{q\}$, and $\{m\}$. Moreover, as $a \not\leqslant b$ and $c \not\leqslant b$ or $c \not\leqslant d$, we have $a \not\leqslant b \wedge d$ and $c \not\leqslant b \wedge d$. Thus, $g(b \wedge d)$ is obtained from $f(b) \cap f(d)$ by making $\{p\}$, $\{q\}$, and $\{m\}$ new equivalence classes. As a consequence, we obtain $g(b \wedge d) = g(d) \cap g(d)$. ⊠

Lemma 1.38. *Let γ be limit ordinal, $\boldsymbol{A}$ a lattice, and $\{\langle f_\varepsilon, X_\varepsilon\rangle : \varepsilon < \gamma\}$ a sequence of weak representations of $\boldsymbol{A}$ such that*

$$\text{if } \alpha \leqslant \beta < \gamma, \text{ then } \langle f_\beta, X_\beta\rangle \text{ extends } \langle f_\alpha, X_\alpha\rangle.$$

Then the pair

$$\langle f, X\rangle := \langle \bigcup_{\varepsilon<\gamma} f_\varepsilon, \bigcup_{\varepsilon<\gamma} X_\varepsilon\rangle$$

is a weak representation of $\boldsymbol{A}$ extending all the $\langle f_\varepsilon, X_\varepsilon\rangle$.

Proof. Since γ is limit, $0 < \gamma$. Thus, by assumption, $\langle f_0, X_0\rangle$ is a weak representation of $\boldsymbol{A}$. In particular, X_0 is nonempty, whence so is X. Moreover, notice that $f(a)$ is an equivalence relation on X, for every $a \in A$. To prove this, observe that, by definition, $f(a)$ is a binary relation on X. Then consider $x, y, z \in X$. Since $X = \bigcup_{\varepsilon<\gamma} X_\varepsilon$, there exists $\alpha < \gamma$ such that $x \in X_\alpha$. As $f_\alpha(a)$ is a reflexive relation on X_α, we obtain

$$\langle x, x\rangle \in f_\alpha(a) \subseteq \bigcup_{\varepsilon<\gamma} f_\varepsilon(a) = f(a).$$

Hence, we conclude that $f(a)$ is reflexive. A similar argument shows that it is reflexive. Hence, it only remains to prove that $f(a)$ is transitive. To this end, suppose that $\langle x, y\rangle, \langle y, z\rangle \in f(a)$. Since $f(a) = \bigcup_{\varepsilon<\gamma} f_\varepsilon(a)$, there exist $\alpha, \beta < \gamma$ such that $\langle x, y\rangle \in f_\alpha(a)$ and $\langle y, z\rangle \in f_\beta(a)$. Since every pair of ordinals is comparable, we can assume, without loss of generality, that $\beta \leqslant \alpha$. By the assumptions, this guarantees that $\langle f_\alpha, X_\alpha\rangle$ extends $\langle f_\beta, X_\beta\rangle$. Consequently, $f_\beta(a) \subseteq f_\alpha(a)$ and, therefore, $\langle y, z\rangle \in f_\alpha(a)$. Since $f_\alpha(a)$ is a transitive relation on X_α, this implies

$$\langle x, z\rangle \in f_\alpha(a) \subseteq \bigcup_{\varepsilon<\gamma} f_\varepsilon(a) = f(a).$$

Hence, we conclude that $f(a)$ is transitive and, therefore, that it is an equivalence relation on X. Accordingly, $f\colon A \to \mathrm{Eq}(X)$ is a well-defined map.

We shall prove that f preserves binary meets. To this end, consider $a, c \in A$ and $x, y \in X$. Using the definition of f and the fact that each f_ε preserves binary meets, we obtain

$$\begin{aligned}\langle x, y\rangle \in f(a \wedge c) &\iff \langle x, y\rangle \in \bigcup_{\varepsilon<\gamma} f_\varepsilon(a \wedge c)\\ &\iff \langle x, y\rangle \in f_\varepsilon(a \wedge c), \text{ for some } \varepsilon < \gamma\\ &\iff \langle x, y\rangle \in f_\varepsilon(a) \cap f_\varepsilon(c), \text{ for some } \varepsilon < \gamma.\end{aligned}$$

Moreover, observe that

$$\langle x, y\rangle \in f_\varepsilon(a) \cap f_\varepsilon(c), \text{ for some } \varepsilon < \gamma \iff \langle x, y\rangle \in f_\alpha(a) \cap f_\beta(c), \text{ for some } \alpha, \beta < \gamma.$$

The implication from left to right in the above display is obvious. To prove the other, suppose that $\langle x, y\rangle \in f_\alpha(a) \cap f_\beta(c)$, for some $\alpha, \beta < \gamma$. Since every pair of ordinals is comparable, we can assume, without loss of generality, that $\beta \leqslant \alpha$. As a consequence, $\langle f_\alpha, X_\alpha\rangle$ extends $\langle f_\beta, X_\beta\rangle$ and, therefore, $f_\beta(c) \subseteq f_\alpha(c)$. Since $\langle x, y\rangle \in f_\beta(c)$, this yields $\langle x, y\rangle \in f_\alpha(c)$, whence $\langle x, y\rangle \in f_\alpha(a) \cap f_\alpha(c)$. Thus, taking $\varepsilon := \alpha$, we are done. Lastly, from the definition of f it follows that

$$\begin{aligned}\langle x, y\rangle \in f_\alpha(a) \cap f_\beta(c), \text{ for some } \alpha, \beta < \gamma &\iff \langle x, y\rangle \in \Big(\bigcup_{\varepsilon<\gamma} f_\varepsilon(a)\Big) \cap \Big(\bigcup_{\varepsilon<\gamma} f_\varepsilon(c)\Big)\\ &\iff \langle x, y\rangle \in f(a) \cap f(c).\end{aligned}$$

The above series of equivalences imply that, for every $x, y \in X$,

$$\langle x, y\rangle \in f(a \wedge c) \iff \langle x, y\rangle \in f(a) \cap f(c),$$

whence $f(a \wedge c) = f(a) \cap f(c)$. Thus, f preserves binary meets.

To prove that f is injective, consider $a, c \in A$. Since $\langle f_0, X_0\rangle$ is a weak representation of $\boldsymbol{A}$, the map f_0 is injective. In particular, $f_0(a) \neq f_0(c)$. We can assume, without loss of generality, that there exists $\langle x, y\rangle \in f_0(a) \smallsetminus f_0(c)$. Since $\langle f_\varepsilon, X_\varepsilon\rangle$ extends $\langle f_0, X_0\rangle$, for all $\varepsilon < \gamma$, we obtain

$$\langle x, y\rangle \in \Big(\bigcup_{\varepsilon<\gamma} f_\varepsilon(a)\Big) \smallsetminus \Big(\bigcup_{\varepsilon<\gamma} f_\varepsilon(c)\Big) = f(a) \smallsetminus f(c).$$

Hence, we conclude that $f(a) \neq f(c)$ and, therefore, that f is injective. It follows that $\langle f, X\rangle$ is a weak representation of $\boldsymbol{A}$.

It only remains to prove that $\langle f, X\rangle$ extends $\langle f_\alpha, X_\alpha\rangle$, for every $\alpha < \gamma$. To this end, consider $\alpha < \gamma$. Clearly, $X_\alpha \subseteq \bigcup_{\varepsilon<\gamma} X_\varepsilon = X$. Lastly, we will prove that $f_\alpha(a) = f(a) \cap (X_\alpha \times X_\alpha)$, for every $a \in A$. First, the inclusion $f_\alpha(a) \subseteq f(a) \cap (X_\alpha \times X_\alpha)$ is an immediate consequence of the definition of f. For the other inclusion, consider $\langle x, y\rangle \in f(a) \cap (X_\alpha \times X_\alpha)$. Since $f = \bigcup_{\varepsilon<\gamma} f_\varepsilon$, there exists $\varepsilon < \gamma$ such that $\langle x, y\rangle \in f_\varepsilon(a)$. Since α and ε are comparable, $\langle f_\alpha, X_\alpha\rangle$ extends $\langle f_\varepsilon, X_\varepsilon\rangle$ or $\langle f_\varepsilon, X_\varepsilon\rangle$ extends $\langle f_\alpha, X_\alpha\rangle$. If $\langle f_\alpha, X_\alpha\rangle$ extends $\langle f_\varepsilon, X_\varepsilon\rangle$, then from $\langle x, y\rangle \in f_\varepsilon(a)$ it follows $\langle x, y\rangle \in f_\alpha(a)$, as desired. On the other hand, if $\langle f_\varepsilon, X_\varepsilon\rangle$ extends $\langle f_\alpha, X_\alpha\rangle$, we obtain $f_\alpha(a) = f_\varepsilon(a) \cap (X_\alpha \times X_\alpha)$. Since $\langle x, y\rangle \in f_\varepsilon(a) \cap (X_\alpha \times X_\alpha)$, we conclude that $\langle x, y\rangle \in f_\alpha(a)$. This establishes the inclusion $f(a) \cap (X_\alpha \times X_\alpha) \subseteq f_\alpha(a)$. Hence, $\langle f, X\rangle$ extends $\langle f_\alpha, X_\alpha\rangle$, as desired. ⊠

We are now ready to complete the proof of Whitman's Theorem.

Proof. Our aim is to embed every lattice into a partition lattice. To this end, consider a lattice $\boldsymbol{A}$ and let $\langle f_0, X_0\rangle$ be the pair where $X_0 := A$ and $f_0\colon A \to \mathrm{Eq}(X_0)$ is the map defined, for every $a \in A$, as

$$f_0(a) := \{\langle x, y\rangle \in X_0 \times X_0 : x = y \text{ or } x \vee y \leqslant a\}.$$

It is easy to see that f_0 is well-defined and preserves binary meets, whence $\langle f_0, X_0\rangle$ is a weak representation of $\boldsymbol{A}$.

Now, take an enumeration $\{\langle x_\varepsilon, y_\varepsilon, a_\varepsilon, c_\varepsilon\rangle : \varepsilon < \gamma\}$ of all the quadruples $\langle x, y, a, c\rangle$ such that $x, y \in X_0$ and $\langle x, y\rangle \in f_0(a \vee c)$. We consider a sequence

$$\{\langle g_\varepsilon, Z_\varepsilon\rangle : \varepsilon \leqslant \gamma\}$$

of weak representations of $\boldsymbol{A}$ such that $\langle g_0, Z_0\rangle = \langle f_0, X_0\rangle$ and

(i) if $\varepsilon < \gamma$, then $\langle g_{\varepsilon+1}, Z_{\varepsilon+1}\rangle$ extends $\langle g_\varepsilon, Z_\varepsilon\rangle$ and

$$\langle x_\varepsilon, y_\varepsilon\rangle \in g_{\varepsilon+1}(a_\varepsilon) \vee^{\mathrm{Eq}(Z_{\varepsilon+1})} g_{\varepsilon+1}(c_\varepsilon); \text{ and}$$

(ii) if $\varepsilon \leqslant \gamma$ is a limit ordinal, then $\langle g_\varepsilon, Z_\varepsilon\rangle$ extends $\langle g_\delta, Z_\delta\rangle$, for all $\delta < \varepsilon$.

This can be done using Lemma 1.37 in case (i) and Lemma 1.38 in case (ii).

Then set

$$\langle f_1, X_1\rangle := \langle g_\gamma, Z_\gamma\rangle.$$

Notice that, by construction, $\langle f_1, X_1\rangle$ extends $\langle f_0, X_0\rangle$. Moreover, for every $x, y \in X_0$ and $a, c \in A$,

$$\text{if } \langle x, y\rangle \in f_0(a \vee c), \text{ then } \langle x, y\rangle \in f_1(a) \vee^{\mathrm{Eq}(X_1)} f_1(c).$$

To prove this, observe first that, for all $\varepsilon < \gamma$,

$$g_{\varepsilon+1}(a_\varepsilon) \subseteq f_1(a_\varepsilon) \quad \text{and} \quad g_{\varepsilon+1}(c_\varepsilon) \subseteq f_1(c_\varepsilon), \tag{1.10}$$

since $\langle f_1, X_1\rangle$ extends $\langle g_{\varepsilon+1}, Z_{\varepsilon+1}\rangle$. Suppose then that $\langle x, y\rangle \in f_0(a \vee c)$. There exists $\varepsilon < \gamma$ such that $\langle x, y, a, c\rangle = \langle x_\varepsilon, y_\varepsilon, a_\varepsilon, c_\varepsilon\rangle$. By condition (i), $\langle x_\varepsilon, y_\varepsilon\rangle \in g_{\varepsilon+1}(a_\varepsilon) \vee^{\mathrm{Eq}(Z_{\varepsilon+1})} g_{\varepsilon+1}(c_\varepsilon)$. Consequently, using the description of joins in partition lattices given in Example 1.26 and the inclusions in (1.10), we obtain

$$\begin{aligned}
\langle x_\varepsilon, y_\varepsilon\rangle &\in g_{\varepsilon+1}(a_\varepsilon) \vee^{\mathrm{Eq}(Z_{\varepsilon+1})} g_{\varepsilon+1}(c_\varepsilon)\\
&= \bigcup\{g_{\varepsilon+1}(b_1) \circ \cdots \circ g_{\varepsilon+1}(b_n) : b_1, \ldots, b_n \in \{a_\varepsilon, c_\varepsilon\}\}\\
&\subseteq \bigcup\{f_1(b_1) \circ \cdots \circ f_1(b_n) : b_1, \ldots, b_n \in \{a_\varepsilon, c_\varepsilon\}\}\\
&= f_1(a) \vee^{\mathrm{Eq}(X_1)} f_1(c),
\end{aligned}$$

as desired.

Iterating this construction, we obtain a sequence

$$\{\langle f_n, X_n\rangle : n \in \mathbb{N}\}$$

of weak representations of $\boldsymbol{A}$ such that, for every $n \in \mathbb{N}$, $\langle f_{n+1}, X_{n+1}\rangle$ extends $\langle f_n, X_n\rangle$ and, for every $x, y \in X_n$ and $a, c \in A$,

$$\text{if } \langle x, y\rangle \in f_n(a \vee c), \text{ then } \langle x, y\rangle \in f_{n+1}(a) \vee^{\mathrm{Eq}(X_{n+1})} f_{n+1}(c). \tag{1.11}$$

In view of Lemma 1.38, the pair

$$\langle f, X\rangle := \langle \bigcup_{n\in\mathbb{N}} f_n; \bigcup_{n\in\mathbb{N}} X_n\rangle$$

is a weak representation of $\boldsymbol{A}$ extending the various $\langle f_n, X_n\rangle$.

To conclude the proof, it suffices to show that f is an embedding of $\boldsymbol{A}$ into the partition lattice $\langle \mathrm{Eq}(X); \subseteq\rangle$. Since $\langle f, X\rangle$ is a weak representation of $\boldsymbol{A}$, it is enough to check that f preserves binary joins. To this end, consider $a, c \in A$. Since $a = a \wedge (a \vee c)$ and $c = c \wedge (a \vee c)$ and f preserves binary meets,

$$f(a) = f(a) \cap f(a \vee c) \quad \text{and} \quad f(c) = f(c) \cap f(a \vee c).$$

Thus, $f(a), f(c) \subseteq f(a \vee c)$, whence $f(a) \vee^{\mathrm{Eq}(X)} f(c) \subseteq f(a \vee c)$. To prove the other inclusion, observe that

$$\begin{aligned}
f(a \vee c) &= \bigcup_{n\in\mathbb{N}} f_n(a \vee c)\\
&\subseteq \bigcup_{n\in\mathbb{N}} \left(f_n(a) \vee^{\mathrm{Eq}(X_n)} f_n(c)\right)\\
&= \bigcup_{n\in\mathbb{N}} \{f_n(b_1) \circ \cdots \circ f_n(b_m) : b_1, \ldots, b_m \in \{a, c\}\}\\
&\subseteq \bigcup \{f(b_1) \circ \cdots \circ f(b_m) : b_1, \ldots, b_m \in \{a, c\}\}\\
&= f(a) \vee^{\mathrm{Eq}(X)} f(c).
\end{aligned}$$

The above steps are justified as follows. The first one follows from the definition of f, the second from (1.11), the third and the last one from the description of joins in partition lattices, and the fourth from the fact that $\langle f, X\rangle$ extends each $\langle f_n, X_n\rangle$. ⊠

Remark 1.39. This proof of Whitman's Theorem is due to Jónsson. A closer examination of it shows that every lattice $\boldsymbol{A}$ can be embedded into a partition lattice $\mathrm{Eq}(X)$ by means of an embedding f such that, for every $a, c \in A$,

$$f(a) \vee^{\mathrm{Eq}(X)} f(c) = f(a) \circ f(c) \circ f(a) \circ f(c).$$

This gives a slightly simpler representation of binary joins in $\boldsymbol{A}$. ⊠

A finite variant of Whitman's Theorem holds too. Its proof, however, is much harder.

Theorem 1.40 (Pudlák & Tůma)**.** *Every finite lattice embeds into a finite partition lattice.*

1.5 Complete lattices

Recall that a poset $\mathbb{X}$ is a complete lattice when $\bigvee Y$ and $\bigwedge Y$ exist in $\mathbb{X}$, for every $Y \subseteq X$. Notably, the existence of arbitrary meets or, equivalently, joins in $\mathbb{X}$ suffices.

Proposition 1.41. *Let $\mathbb{X}$ be a poset. If $\bigwedge Y$ (resp. $\bigvee Y$) exists in $\mathbb{X}$, for all $Y \subseteq X$, then $\mathbb{X}$ is a complete lattice.*

Proof. Suppose that $\bigwedge Y$ exists in $\mathbb{X}$, for all $Y \subseteq X$. Then take a set $Y \subseteq X$ and let $U(Y)$ be the set of upper bounds of Y in $\mathbb{X}$. By assumption, the element $x := \bigwedge U(Y)$ exists in $\mathbb{X}$. We shall prove that x is the supremum of Y in $\mathbb{X}$. To this end, notice that, by definition, x is a lower bound of $U(Y)$. Therefore, it only remains to prove that $x \in U(Y)$. To this end, consider an element $y \in Y$. Clearly, y is a lower bound of $U(Y)$. Together with the fact that, by definition, x is the greatest lower bound of $U(Y)$, this implies $y \leqslant x$. Since $y \in U(Y)$ and $x \leqslant y$, we obtain $x \in U(Y)$. Hence, we conclude that $x = \bigvee Y$ and, therefore, that $\mathbb{X}$ is a complete lattice. By the Duality Principle, the dual statement holds too. ⊠

In order to apply the above test to a poset $\mathbb{X}$, it is sometimes useful to distinguish the case where $Y = \emptyset$ from that where Y is nonempty. Because of this, the following description of the meet and the join of the empty set is of special interest.

Proposition 1.42. *The following conditions hold for a poset $\mathbb{X}$.*

(i) *$\mathbb{X}$ has a maximum 1 if and only if $\bigwedge \emptyset$ (resp. $\bigvee X$) exists in $\mathbb{X}$. In this case,*

$$\bigwedge \emptyset = \bigvee X = 1.$$

(ii) *$\mathbb{X}$ has a minimum 0 if and only if $\bigvee \emptyset$ (resp. $\bigwedge X$) exists in $\mathbb{X}$. In this case,*

$$\bigvee \emptyset = \bigwedge X = 0.$$

Proof. We detail only the proof of condition (i), as the other one is proved analogously. First, observe that every element of $\mathbb{X}$ is vacuously a lower bound of $\emptyset$ in $\mathbb{X}$. Moreover, by definition, $\bigwedge \emptyset$ is the greatest lower bound of $\emptyset$ in $\mathbb{X}$. Therefore, if $\bigwedge \emptyset$ exists in $\mathbb{X}$, then $x \leqslant \bigwedge \emptyset$, for all $x \in X$. Hence, we conclude that $\bigwedge \emptyset$ is the maximum of $\mathbb{X}$. Conversely, suppose that $\mathbb{X}$ has a maximum 1. Then 1 is vacuously a lower bound of $\emptyset$ in $\mathbb{X}$. Furthermore, being the maximum of $\mathbb{X}$, 1 is the greatest such lower bound, whence $1 = \bigwedge \emptyset$.

Similarly, recall that $\bigvee X$ is the least upper bound of X in $\mathbb{X}$. Therefore, if it exists, $\bigvee X$ is an upper bound of X and, therefore, the maximum of $\mathbb{X}$. Conversely, suppose that $\mathbb{X}$ has a maximum 1. Then 1 is obviously an upper bound of X in $\mathbb{X}$ and, forcefully, the least one. ⊠

As we mentioned, lattices may fail to be complete, simple counterexamples being number systems. However, this cannot happen in the finite case, as we proceed to explain.

Corollary 1.43. *Every finite lattice is complete.*

Proof. Let $\boldsymbol{A}$ be a finite lattice. In view of Proposition 1.41, it suffices to show that $\bigwedge Y$ exists in $\boldsymbol{A}$, for all $Y \subseteq A$. There are two cases: either $Y = \emptyset$ or Y is nonempty. Suppose first that $Y = \emptyset$. Then recall that $\boldsymbol{A}$ has a maximal element $\top$, by Proposition 1.5. We will prove that $\top$ is the maximum of $\boldsymbol{A}$. To this end, consider an element $a \in A$. Clearly, $\top, a \leqslant \top \vee a$. As $\top$ is maximal, $\top \leqslant \top \vee a$ yields $\top = a \vee \top$, whence $a \leqslant \top \vee a = \top$. Thus, we conclude that $\top$ is the maximum of $\boldsymbol{A}$. By condition (i)

of Proposition 1.42 and $Y = \emptyset$, this implies that $\bigwedge Y$ exists. Then we consider the case where $Y \neq \emptyset$. Since, by assumption, A is finite, the set Y is finite and nonempty. Therefore $\bigwedge Y$ exists in $\boldsymbol{A}$, by Proposition 1.30. ⊠

Another sufficient condition for a lattice to be complete is related to ascending and descending chains.

Definition 1.44. A poset $\mathbb{X}$ satisfies

(i) the *ascending chain condition* if there is no order embedding from $\langle \mathbb{N}; \leqslant \rangle$ into $\mathbb{X}$;

(ii) the *descending chain condition* if there is no order embedding from $\langle \mathbb{N}; \geqslant \rangle$ into $\mathbb{X}$.

Theorem 1.45. *If a lattice satisfies the ACC (resp. DCC) and has a minimum (resp. maximum), then it is complete.*

The proof of the above result is a direct consequence of the following.

Proposition 1.46. *Let $\boldsymbol{A}$ be a lattice satisfying with the ACC (resp. DCC). For every nonempty $X \subseteq A$, there exists a finite nonempty $Y \subseteq X$, whose join (resp. meet) in $\boldsymbol{A}$ coincides with that of X. Consequently, joins (resp. meets) of nonempty sets $X \subseteq A$ exist in $\boldsymbol{A}$.*

Proof. Let $\boldsymbol{A}$ be a lattice satisfying the ACC and $X \subseteq A$ nonempty. Then suppose, with a view to contradiction, that, for every finite nonempty subset $Y \subseteq X$, the join of Y in $\boldsymbol{A}$ does not coincide with that of X (which, in principle, may even fail to exist).

Since $X \neq \emptyset$, we can choose an element $a_1 \in X$. By assumption, the join of the finite set $\{a_1\} \subseteq X$ in $\boldsymbol{A}$, namely a_1, is not the join of X. Thus, a_1 is not the least upper bound of X in $\boldsymbol{A}$. Since $a_1 \in X$, it follows that a_1 is not an upper bound of X in $\boldsymbol{A}$, otherwise it would be the maximum of X and, therefore, its join. Consequently, there exists $a_2 \in X$ such that $a_2 \nleqslant a_1$, whence $a_1 < a_1 \vee a_2$. Now, we repeat this argument letting $\{a_1, a_2\}$ take the role of $\{a_1\}$. In brief, the join of $\{a_1, a_2\}$ in $\boldsymbol{A}$, namely $a_1 \vee a_2$, is not the join of X. Since $a_1, a_2 \in X$, this implies that there exists an element $a_3 \in X$ such that $a_3 \nleqslant a_1 \vee a_2$, whence $a_1 \vee a_2 < a_1 \vee a_2 \vee a_3$. Iterating this argument, we obtain an infinite ascending chain

$$a_1 < a_1 \vee a_2 < a_1 \vee a_2 \vee a_3 < \cdots < a_1 \vee \cdots \vee a_n < \ldots$$

This contradicts the assumption that $\boldsymbol{A}$ satisfies the ACC. Hence, we conclude that $\bigvee X$ coincides with the join of some finite nonempty $Y \subseteq X$. Since, by Proposition 1.30, joins of finite nonempty subsets of A exist in $\boldsymbol{A}$, we conclude that joins of arbitrary nonempty subsets of A exist in $\boldsymbol{A}$ too. By the Duality Principle, the dual statement holds as well. ⊠

As promised, we obtain short proof of Theorem 1.45.

Proof. Suppose that $\boldsymbol{A}$ is a lattice with a minimum satisfying the ACC. In view of Proposition 1.41, in order to prove that $\boldsymbol{A}$ is complete, it suffices to show that $\bigvee X$ exists in $\boldsymbol{A}$, for every $X \subseteq A$. Since $\boldsymbol{A}$ satisfies the ACC, by Proposition 1.46, $\bigvee X$ exists, for every nonempty $X \subseteq A$. In addition, by condition (ii) of Proposition 1.42, $\bigvee \emptyset$ exists, because $\boldsymbol{A}$ has a minimum. It follows that $\boldsymbol{A}$ is complete, as desired. The dual statement follows from the Duality Principle. ⊠

Example 1.47 (Division lattice)**.** As the name suggests, the division lattice $\langle \mathbb{N}; | \rangle$ is indeed a lattice, where

$$\begin{aligned} n \wedge m &= \text{ the greatest common divisor of } n \text{ and } m, \text{ and} \\ n \vee m &= \text{ the least common multiple of } n \text{ and } m, \end{aligned}$$

for every $n, m \in \mathbb{N}$. We shall use the DCC to show that $\langle \mathbb{N}; | \rangle$ is complete.

To this end, observe that every natural number other than zero has only finitely many divisors in $\mathbb{N}$. As a consequence, every element of $\langle \mathbb{N}; | \rangle$ other than zero has only finitely many lower bounds. It follows that $\langle \mathbb{N}; | \rangle$ satisfies the DCC. Furthermore, it has a maximum element, namely zero (which is divisible by every natural number). By Theorem 1.45, we conclude that $\langle \mathbb{N}; | \rangle$ is complete. ⊠

Our aim is to derive a representation theorem for complete lattices. The following notion is instrumental to this purpose.

Definition 1.48. A map $C \colon \mathcal{P}(A) \to \mathcal{P}(A)$ is said to be a *closure operator* on a set A if, for every $X, Y \subseteq A$,

(i) $X \subseteq C(X)$;

(ii) $C(C(X)) \subseteq C(X)$; and

(iii) if $X \subseteq Y$, then $C(X) \subseteq C(Y)$.

Furthermore, a set $X \subseteq A$ is said to be *closed* if $X = C(X)$. Notice that, by conditions (i) and (ii), $C(C(X)) = C(X)$, for all $X \subseteq A$. It follows that $C(X)$ is closed, for all $X \subseteq A$.

When no confusion may occur, given a closure operator C on A and $a_1, \ldots, a_n \in A$, we shall write $C(a_1, \ldots, a_n)$ as a shorthand for $C(\{a_1, \ldots, a_n\})$.

Example 1.49 (Upsets and downsets)**.** Let $\mathbb{X}$ be a poset. A set $V \subseteq X$ is said to be an *upset* (resp. a *downset*) of $\mathbb{X}$ when, for every $x, y \in X$,

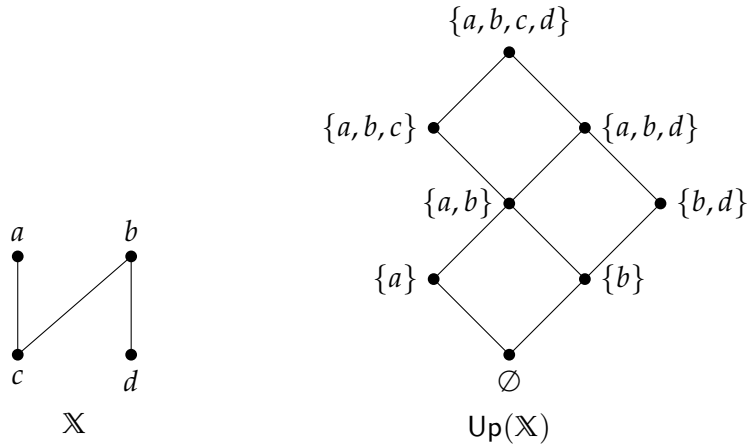
$$\text{if } x \in V \text{ and } x \leqslant y \text{ (resp. } y \leqslant x\text{), then } y \in V.$$

The families of upsets and downsets of $\mathbb{X}$ will be denoted, respectively, by

$$\mathsf{Up}(\mathbb{X}) \quad \text{and} \quad \mathsf{Dw}(\mathbb{X}).$$

When ordered under the inclusion relation, $\mathsf{Up}(\mathbb{X})$ and $\mathsf{Dw}(\mathbb{X})$ are complete lattices in which joins are unions and meets intersections. The picture below illustrates the

structure of the complete lattice $\langle \mathsf{Up}(\mathbb{X}); \subseteq \rangle$ for a concrete poset $\mathbb{X}$.



Given a poset $\mathbb{X}$, let

$$\uparrow^{\mathbb{X}} \colon \mathcal{P}(X) \to \mathcal{P}(X) \quad \text{and} \quad \downarrow^{\mathbb{X}} \colon \mathcal{P}(X) \to \mathcal{P}(X)$$

be the maps defined, for every $Y \subseteq X$, as

$$\uparrow^{\mathbb{X}} Y := \{x \in X : \text{there exists } y \in Y \text{ such that } y \leqslant x\}$$
$$\downarrow^{\mathbb{X}} Y := \{x \in X : \text{there exists } y \in Y \text{ such that } x \leqslant y\}.$$

It is easy to see that $\uparrow^{\mathbb{X}}$ and $\downarrow^{\mathbb{X}}$ are closure operators on X. Furthermore, $\uparrow^{\mathbb{X}} Y$ and $\downarrow^{\mathbb{X}} Y$ are, respectively, the least upset and the least downset of $\mathbb{X}$ extending Y.

When the poset $\mathbb{X}$ is clear from the context, we will drop the superscripts in $\uparrow^{\mathbb{X}}$ and $\downarrow^{\mathbb{X}}$ and write simply $\uparrow$ and $\downarrow$. Furthermore, given $x \in X$, we will write $\uparrow^{\mathbb{X}} x$ and $\downarrow^{\mathbb{X}} x$ as a shorthand for $\uparrow^{\mathbb{X}} \{x\}$ and $\downarrow^{\mathbb{X}} \{x\}$, respectively. ⊠

Example 1.50 (Topological closure)**.** A *topology* on a set X is a family $\tau \subseteq \mathcal{P}(X)$ such that

(i) $\emptyset, X \in \tau$;

(ii) if $Y, Z \in \tau$, then $Y \cap Z \in \tau$; and

(iii) if $\{Y_i : i \in I\} \subseteq \tau$, then $\bigcup_{i \in I} Y_i \in \tau$.

In this case, the pair $\langle X; \tau \rangle$ is said to be a *topological space*. Furthermore, the elements of τ are called *open* and their complements relative to X *closed*. It follows that the collection of closed sets of a topological space $\langle X; \tau \rangle$ contains $\emptyset$ and X and is closed under binary unions and arbitrary intersections.

For instance, let $\mathbb{X}$ be a linearly ordered poset. For every $x, y \in X$, set

$$(x, y) := \{z \in X : x < z < y\}$$
$$(x, +\infty) := \{z \in X : x < z\}$$
$$(-\infty, x) := \{z \in X : z < x\}.$$

Then let τ be the collection arbitrary unions of sets of the above form plus X. The pair $\langle X; \tau \rangle$ is a topological space and τ is called the *order topology* on $\mathbb{X}$. The order topology on $\langle \mathbb{R}; \leqslant \rangle$ is sometimes called the *standard topology* on $\mathbb{R}$.

Given a topological space $\langle X; \tau \rangle$, let

$$\overline{(-)} \colon \mathcal{P}(X) \to \mathcal{P}(X)$$

be the map defined, for every $Y \subseteq X$, as

$$\overline{Y} := \bigcap \{Z \subseteq X : Z \text{ is closed and } Y \subseteq Z\}.$$

Notice that the family $\{Z \subseteq X : Z \text{ is closed and } Y \subseteq Z\}$ is always nonempty, because the total set X is closed. Furthermore, as arbitrary intersections of closed are closed, $\overline{Y}$ is also closed and, therefore, the least closed set extending Y. Because of this, $\overline{Y}$ is called the *topological closure* of Y. It is easy to see that $\overline{(-)}$ is a closure operator on X ,whose closed sets are precisely the closed sets of the topological space $\langle X; \tau \rangle$. ⊠

As we shall see, a closure operator is uniquely determined by its closed sets. Consequently, in order to present a closure operator, it suffices to exhibit the family of its closed sets, whose structure is captured by the following definition.

Definition 1.51. A family $\mathcal{C} \subseteq \mathcal{P}(A)$ is said to be a *closure system* on a set A if

(i) $A \in \mathcal{C}$; and

(ii) $\bigcap \mathcal{V} \in \mathcal{C}$, for every nonempty $\mathcal{V} \subseteq \mathcal{C}$.

As we mentioned, closure operators and systems are two faces of the same coin.

Proposition 1.52. *Let A be a set. The following conditions hold:*

(i) *if $C \colon \mathcal{P}(A) \to \mathcal{P}(A)$ is a closure operator on A, the family of its closed sets is a closure system on A;*

(ii) *if $\mathcal{C}$ is a closure system on A, then the map $C \colon \mathcal{P}(A) \to \mathcal{P}(A)$, defined, for every $X \subseteq A$, as*

$$C(X) := \bigcap \{Y \in \mathcal{C} : X \subseteq Y\},$$

is a closure operator on A; and

(iii) *the above transformations between closure operators and systems on A are inverse one to the other.*

Proof. (i): By condition (i) in the definition of a closure operator, $A \subseteq C(A)$. Furthermore, $C(A) \subseteq A$, since the codomain of C is $\mathcal{P}(A)$. As a consequence, $A = C(A)$, that is, A is a closed set of C.

Then consider a nonempty family of closed sets $\{X_i : i \in I\}$ of C. In order to prove that $\bigcap_{i \in I} X_i$ is also a closed set of C, observe that, by condition (i) in the definition of a closure operator, $\bigcap_{i \in I} X_i \subseteq C(\bigcap_{i \in I} X_i)$. To prove the other inclusion, take an arbitrary $j \in I$. Since $\bigcap_{i \in I} X_i \subseteq X_j$, from condition (iii) in the definition of a closure operator it follows that $C(\bigcap_{i \in I} X_i) \subseteq C(X_j)$. Recall that X_j is a closed set of C, by assumption. As a consequence,

$$C(\bigcap_{i \in I} X_i) \subseteq C(X_j) = X_j.$$

It follows that $C(\bigcap_{i\in I} X_i) \subseteq \bigcap_{i\in I} X_i$. Hence, $\bigcap_{i\in I} X_i$ is a closed set of C, as desired.

(ii): First, notice that, since $A \in \mathcal{C}$, the set $\{Y \in \mathcal{C} : X \subseteq Y\}$ contains A, for every $X \subseteq A$. It follows that C satisfies conditions (i) and (iii) in the definition of a closure operator. To prove condition (ii), consider $X \subseteq A$. Because of the definition of C, in order to prove $C(C(X)) \subseteq C(X)$, it suffices to show that

$$\{Z \in \mathcal{C} : X \subseteq Z\} \subseteq \{Z \in \mathcal{C} : C(X) \subseteq Z\}.$$

To this end, consider $Z \in \mathcal{C}$ such that $X \subseteq Z$. Then $C(X) \subseteq C(Z)$. Furthermore, as $Z \in \mathcal{C}$, from the definition of C it follows $C(Z) = Z$. Hence, $C(X) \subseteq Z$, as desired.

(iii): Given a closure operator C on A, we denote by C_+ the associated closure system. Vice versa, the closure operator associated with a closure system $\mathcal{C}$ on A will be denoted by $\mathcal{C}^+$.

Then consider a closure operator C on A and a set $X \subseteq A$. From the definition of the maps $(-)^+$ and of $(-)_+$ it follows

$$(C_+)^+(X) = \bigcap\{Y \in C_+ : X \subseteq Y\} = \bigcap\{Y \subseteq A : X \subseteq Y \text{ and } Y = C(Y)\}.$$

Now, by condition (i) and (ii) in the definition of a closure operator, $X \subseteq C(X) = C(C(X))$. Thus, $C(X) \in \{Y \subseteq A : X \subseteq Y \text{ and } Y = C(Y)\}$. Together with the above display, this yields $(C_+)^+(X) \subseteq C(X)$. To prove the other inclusion, consider $Y \subseteq A$ such that $X \subseteq Y$ and $Y = C(Y)$. By condition (iii) in the definition of a closure operator, $C(X) \subseteq C(Y) = Y$. In view of the above display, this yields $C(X) \subseteq (C_+)^+(X)$. Hence, we conclude that $C = (C_+)^+$.

Lastly, consider a closure system $\mathcal{C}$ on A. From the definition of the maps $(-)_+$ and of $(-)^+$ it follows

$$(\mathcal{C}^+)_+ = \{Y \subseteq A : Y = \mathcal{C}^+(Y)\} = \{Y \subseteq A : Y = \bigcap\{Z \in \mathcal{C} : Y \subseteq Z\}\}. \tag{1.12}$$

Since $\mathcal{C}$ is a closure system, $A \in \mathcal{C}$. Consequently, for every $Y \subseteq A$,

$$A \in \{Z \in \mathcal{C} : Y \subseteq Z\}.$$

Hence, since $\mathcal{C}$ is closed under intersections of nonempty families,

$$\bigcap\{Z \in \mathcal{C} : Y \subseteq Z\} \in \mathcal{C}, \text{ for every } Y \subseteq A.$$

Together with (1.12), this implies $\mathcal{C} = (\mathcal{C}^+)_+$. ⊠

In view of the above result, closure systems are precisely the families of closed sets of closure operators. For instance, the upsets (resp. downsets) of a poset $\mathbb{X}$ are precisely the closed sets of the closure operator $\uparrow^{\mathbb{X}}$ (resp. $\downarrow^{\mathbb{X}}$). It follows that both $\mathsf{Up}(\mathbb{X})$ and $\mathsf{Dw}(\mathbb{X})$ are closure systems on $\mathbb{X}$. Similarly, the closed sets of a topological space $\langle X; \tau\rangle$ are precisely the closed sets of the closure operator $\overline{(-)}$. Consequently, the family of closed sets of $\langle X; \tau\rangle$ is a closure system.

Closure systems are tightly connected with complete lattices, as we proceed to explain. On the one hand, every closure system can be viewed as a complete lattice.

Proposition 1.53. *If $\mathcal{C}$ is a closure system, the poset $\langle \mathcal{C}; \subseteq\rangle$ is a complete lattice.*

Proof. Let $\mathcal{C}$ be a closure system on A. In view of Proposition 1.41, it suffices to prove that $\bigwedge Y$ exists in $\langle \mathcal{C}; \subseteq \rangle$, for all $Y \subseteq \mathcal{C}$. First, suppose that $Y \neq \emptyset$. In this case, $\bigwedge Y = \bigcap Y \in \mathcal{C}$, because $\mathcal{C}$ is closed under intersection of nonempty subfamilies. Then we consider the case where $Y = \emptyset$. By condition (i) of Proposition 1.42, the meet of $\emptyset$ exists in $\langle \mathcal{C}; \subseteq \rangle$ if and only if $\langle \mathcal{C}; \subseteq \rangle$ has a maximum. Notice that $A \in \mathcal{C}$ and $\mathcal{C} \subseteq \mathcal{P}(A)$, since $\mathcal{C}$ is a closure system on A. As a consequence, A is the maximum of $\langle \mathcal{C}; \subseteq \rangle$. ⊠

In view of the above result, we will often treat closure systems as complete lattices, tacitly assuming that they are ordered under the inclusion relation. On the other hand, every complete lattice is isomorphic to a closure system, yielding the following representation theorem.

Theorem 1.54. *A poset $\mathbb{X}$ is a complete lattice if and only if it is isomorphic to $\langle \mathcal{C}; \subseteq \rangle$, for some closure system $\mathcal{C}$.*

Proof. In view of Proposition 1.53, it suffices to show that every complete lattice $\mathbb{X}$ is isomorphic to $\langle \mathcal{C}; \subseteq \rangle$, for some closure system $\mathcal{C}$. To this end, consider the set

$$\mathcal{C} \coloneqq \{\downarrow x : x \in X\}.$$

We claim that $\mathcal{C}$ is a closure system on X. First, notice that $\mathcal{C} \subseteq \mathcal{P}(X)$. Then recall that $\mathbb{X}$ has a maximum 1, because it is a complete lattice. Thus, $X = \downarrow 1 \in \mathcal{C}$. Lastly, consider a nonempty family $\{\downarrow x_i : i \in I\} \subseteq \mathcal{C}$. We need to prove that its intersection belongs to $\mathcal{C}$. To this end, observe that, for every $y \in X$,

$$y \in \bigcap_{i \in I} \downarrow x_i \iff y \leqslant x_i, \text{ for every } i \in I \iff y \leqslant \bigwedge_{i \in I}^{\mathbb{X}} x_i.$$

As a consequence,

$$\bigcap_{i \in I} \downarrow x_i = \downarrow\Big(\bigwedge_{i \in I}^{\mathbb{X}} x_i \Big) \in \mathcal{C}.$$

Hence, $\mathcal{C}$ is a closure system on X, as desired.

Therefore, to conclude the proof, it only remains to show that $\mathbb{X}$ is isomorphic to $\langle \mathcal{C}; \subseteq \rangle$. To this end, consider the map $\gamma \colon X \to \mathcal{C}$, defined by the rule

$$\gamma(x) \coloneqq \downarrow x, \text{ for every } x \in X.$$

Clearly, δ is a well-defined surjection. Moreover, for every $x, y \in X$,

$$x \leqslant y \iff \downarrow x \subseteq \downarrow y \iff \gamma(x) \subseteq \gamma(y).$$

Hence, γ is an order embedding from $\mathbb{X}$ into $\langle \mathcal{C}; \subseteq \rangle$. Since γ is surjective, we conclude that it is an order isomorphism. ⊠

An element $x \in X$ is said to be a *fixed point* of a map $f \colon X \to X$, if $x = f(x)$. Complete lattices and order preserving maps form the ingredients of a general fixed point theorem.

Knaster & Tarski's Theorem 1.55. *If $\mathbf{A}$ is a complete lattice and $f \colon \mathbf{A} \to \mathbf{A}$ an order preserving map, then f has a fixed point, namely*

$$a \coloneqq \bigvee \{c \in A : c \leqslant f(c)\}.$$

Proof. Let $X \coloneqq \{c \in A : c \leqslant f(c)\}$ and consider $c \in X$. Since f is order preserving, $c \leqslant f(c) \leqslant f(\bigvee X) = f(a)$. Thus, $c \leqslant f(a)$, for every $c \in X$. It follows that

$$a = \bigvee X \leqslant f(a).$$

Since f is order preserving, this implies $f(a) \leqslant f(f(a))$, whence $f(a) \in X$. Since $a = \bigvee X$, we conclude that $f(a) \leqslant a$. Hence, a is a fixed point of f, by the antisymmetry of $\leqslant$. ⊠

Notably, this fixed point theorem can be turn into a characterization of complete lattices.

Theorem 1.56 (Davis)**.** *A lattice $\boldsymbol{A}$ is complete if and only if every order preserving map $f\colon \boldsymbol{A} \to \boldsymbol{A}$ has a fixed point.*

Proof. In view of Knaster & Tarski's Theorem, it suffices to prove that, if a lattice $\boldsymbol{A}$ is not complete, there exists an order preserving map $f\colon \boldsymbol{A} \to \boldsymbol{A}$ without fixed points.

To this end, consider a lattice $\boldsymbol{A}$ that is not complete. We will prove that there are two sequences

$$\{a_\varepsilon : \varepsilon < \gamma\} \quad \text{and} \quad \{c_\delta : \delta < \zeta\}$$

of elements of A satisfying the following requirements:

(i) $a_\varepsilon < c_\delta$, for every $\varepsilon < \gamma$ and $\delta < \zeta$;

(ii) if $\varepsilon < \alpha < \gamma$, then $a_\varepsilon < a_\alpha$;

(iii) if $\delta < \beta < \zeta$, then $c_\delta > c_\beta$; and

(iv) there is no $b \in A$ that is both an upper bound of $\{a_\varepsilon : \varepsilon < \gamma\}$ and a lower bound of $\{c_\delta : \delta < \zeta\}$.

Now, suppose that we proved the existence of the sequences above. Then consider the map $f\colon A \to A$ defined, for every $b \in A$, as follows. If b is a lower bound of $\{c_\delta : \delta < \zeta\}$, then, by condition (iv), b is not an upper bound of $\{a_\varepsilon : \varepsilon < \gamma\}$. Since ordinals are well-ordered, there exists the least $\varepsilon < \gamma$ such that $a_\varepsilon \nleqslant b$. Then we set $f(b) \coloneqq a_\varepsilon$. Similarly, if b is not a lower bound of $\{c_\delta : \delta < \zeta\}$, there exists the least $\delta < \zeta$ such that $b \nleqslant c_\delta$. In this case, we set $f(b) \coloneqq c_\delta$, completing the definition of f.

To prove that f is order preserving, consider $b, d \in A$ such that $b \leqslant d$. If d is a lower bound of $\{c_\delta : \delta < \zeta\}$, then $f(b) = a_\varepsilon$, where ε is the least ordinal $\beta < \gamma$ such that $a_\beta \nleqslant d$. Now, from $b \leqslant d$ it follows that b is also a lower bound of $\{c_\delta : \delta < \zeta\}$. Consequently, $f(b) = a_\alpha$, where α is the least ordinal $\beta < \gamma$ such that $a_\beta \nleqslant b$. Since $b \leqslant d \nleqslant a_\varepsilon$, we obtain $\alpha \leqslant \varepsilon$. By condition (ii), this yields $a_\alpha \leqslant a_\varepsilon$ and, therefore, $f(b) = a_\alpha \leqslant a_\varepsilon = f(d)$, as desired. On the other hand, if b is not a lower bound of $\{c_\delta : \delta < \zeta\}$, an argument similar to the above detailed above shows that $f(b) \leqslant f(d)$. Thus, it only remains to consider the case where b is a lower bound of $\{c_\delta : \delta < \zeta\}$, but d is not. In this case, $f(b) = a_\varepsilon$ and $f(d) = c_\delta$, for some $\varepsilon < \gamma$ and $\delta < \zeta$. By condition (i), we conclude that $f(b) = a_\varepsilon < c_\delta = f(d)$, as desired. Hence, f is order preserving.

Lastly, to prove that f has no fixed points, consider $b \in A$. If b is a lower bound of $\{c_\delta : \delta < \zeta\}$, then $f(b) = a_\varepsilon$, for some $\varepsilon < \gamma$ such that $a_\varepsilon \nleqslant b$. As a consequence, $f(b) \nleqslant b$ and, therefore, b is not a fixed point of f. Similarly, if b is not a lower bound of $\{c_\delta : \delta < \zeta\}$, then $f(b) = c_\delta$, for some $\delta < \zeta$ such that $b \nleqslant c_\delta$. Therefore, also in this

case, b is not a fixed point of f. Thus, $f\colon \boldsymbol{A} \to \boldsymbol{A}$ is an order preserving map without fixed points, as desired.

Therefore, it only remains to prove the existence of the sequences $\{a_\varepsilon : \varepsilon < \gamma\}$ and $\{c_\delta : \delta < \zeta\}$. Since the lattice $\boldsymbol{A}$ is not complete, by Proposition 1.41, there exists a subset X of A whose join does not exist in $\boldsymbol{A}$. We can assume, without loss of generality, that X is closed under existing joins, in the sense that if $Y \subseteq X$ and $\bigvee Y$ exists in $\boldsymbol{A}$, then $\bigvee Y \in X$. This is because the join of X in $\boldsymbol{A}$ exists if and only if that of

$$X^+ \coloneqq \{\bigvee Y : Y \subseteq X \text{ and } \bigvee Y \text{ exists in } \boldsymbol{A}\}$$

does and, moreover, when this is the case, $\bigvee X = \bigvee X^+$. Because of this, henceforth, we will assume that $X = X^+$ and, therefore, that X is closed under existing joins.

Let then $\mathbb{C}$ be the set of well-ordered chains in the subposet $\langle X; \leqslant\rangle$ of $\boldsymbol{A}$. Moreover, let $\preccurlyeq$ be the relation "being an initial segment of" on $\mathbb{C}$, that is, the relation defined as follows:

$$C_1 \preccurlyeq C_2 \iff \text{there exists a downset } V \text{ of } \boldsymbol{A} \text{ such that } C_1 = C_2 \cap V.$$

Notice that $\langle \mathbb{C}; \preccurlyeq\rangle$ closed under unions of nonempty chains. Consequently, every chain in $\langle \mathbb{C}; \preccurlyeq\rangle$ has an upper bound in $\langle \mathbb{C}; \preccurlyeq\rangle$, namely its union. Hence, we can apply Zorn's Lemma, obtaining a maximal element

$$C = \{a_\varepsilon : \varepsilon < \gamma\}$$

of $\langle \mathbb{C}; \preccurlyeq\rangle$ such that $a_\varepsilon < a_\alpha$, for every $\varepsilon < \alpha < \gamma$.

Now, let Y be the set of upper bounds of C in $\boldsymbol{A}$ and $\mathbb{D}$ the set of well-ordered chains in the subposet $\langle Y; \geqslant\rangle$ of $\boldsymbol{A}^\partial$. Furthermore, let $\ll$ be the relation "being an initial segment of" on $\mathbb{D}$, that is, the relation defined as follows:

$$D_1 \ll D_2 \iff \text{there exists an upset } V \text{ of } \boldsymbol{A} \text{ such that } D_1 = D_2 \cap V.$$

With another application of Zorn's Lemma, we obtain a maximal element

$$D = \{c_\delta : \delta < \zeta\}$$

of $\langle \mathbb{D}; \ll\rangle$ such that $c_\delta > c_\beta$, for every $\delta < \beta < \zeta$.

By construction, the sequences C and D satisfy conditions (ii) and (iii). To prove that they validate the remaining conditions too, we claim that $\langle C; \leqslant\rangle$ lacks a maximum and $\langle D; \leqslant\rangle$ a minimum. First, suppose, with a view to contradiction, that C has a maximum a_ε and recall that the join of X does not exist in $\boldsymbol{A}$. As a consequence, a_ε is not an upper bound of X, otherwise it would also be the least one, because $a_\varepsilon \in C \subseteq X$. Therefore, there exists an element $b \in X$ such that $a_\varepsilon < a_\varepsilon \vee b$. Since X is closed under existing joins and binary joins exist in lattices, $a_\varepsilon \vee b \in X$. As a_ε is the maximum of C, this implies that $C \cup \{a_\varepsilon \vee b\}$ is a well-ordered chain in $\langle X; \leqslant\rangle$ strictly greater than C in $\langle \mathbb{C}; \preccurlyeq\rangle$, contradicting the maximality of C. Hence, we conclude that C lacks a maximum, as desired.

Notice that, as a consequence, the join of C does not exist in $\boldsymbol{A}$, otherwise, $C \cup \{\bigvee C\}$ would be a well-ordered chain in $\langle X; \leqslant\rangle$ (because X is closed under existing joins) that, moreover, is strictly greater than C in $\langle \mathbb{C}; \preccurlyeq\rangle$ (because C lacks a maximum), against the maximality of C.

Lastly, suppose, with a view to contradiction, that D has a minimum c_δ. We will prove that c_δ is the join of C, contradicting the fact that $\bigvee C$ does not exist in $\boldsymbol{A}$. Recall that, by construction, D is a set of upper bounds of C. In particular, this implies that c_δ is an upper bound of C. To prove that it is also the least one, consider another upper bound b of C. Then $c_\delta \wedge b$ is also an upper bound of C. Together with the assumption that c_δ is the minimum of D, this guarantees that $D \cup \{c_\delta \wedge b\}$ is a well-ordered chain in $\langle Y; \geqslant \rangle$. By the maximality of D, we obtain $c_\delta \wedge b \in D$. Since c_δ is the minimum of D, we conclude that $c_\delta \leqslant c_\delta \wedge b \leqslant b$. Hence, c_δ is the join of C in $\boldsymbol{A}$, a contradiction. This concludes the proof of the claim.

Then we turn to prove condition (i). Suppose, with a view to contradiction, that there are $\varepsilon < \gamma$ and $\delta < \zeta$ such that $a_\varepsilon \not\leqslant c_\delta$. Observe that $a_\varepsilon \leqslant c_\delta$, since, by construction, $a_\varepsilon \in C$, $c_\delta \in D$, and D is a set of upper bounds of C. Together with $a_\varepsilon \not\leqslant c_\delta$, this yields $a_\varepsilon = c_\delta$. Since c_δ is an upper bound of C, we obtain that so is a_ε. As $a_\varepsilon \in C$, we conclude that a_ε is the maximum of C, a contradiction with the claim.

Lastly, suppose, with a view to contradiction, that condition (iv) fails, that is, there exists an element $b \in A$ that is both an upper bound of C and a lower bound of D. From the maximality of D it follows that $b \in D$. Therefore, as b is a lower bound of D, we conclude that b is the minimum of D, contradicting the claim. ⊠

We conclude this section with two applications of Knaster & Tarski's Theorem, one from set theory and the other from topology.

Corollary 1.57 (Cantor, Schröder & Bernstein)**.** *Let X and Y be sets. If there exist injective maps $f\colon X \to Y$ and $g\colon Y \to X$, then there exists a bijection $h\colon X \to Y$.*

Proof. Consider the map $\gamma\colon \mathcal{P}(X) \to \mathcal{P}(X)$, defined as

$$\gamma(Z) \coloneqq X \smallsetminus g[Y \smallsetminus f[Z]],$$

for every $Z \subseteq X$. Notice that γ is an order preserving map on the complete lattice $\langle \mathcal{P}(X); \subseteq \rangle$. To prove this, consider $V, Z \in \mathcal{P}(X)$ such that $V \subseteq Z$. Clearly, $f[V] \subseteq f[Z]$. This yields $Y \smallsetminus f[Z] \subseteq Y \smallsetminus f[V]$ and, therefore, $g[Y \smallsetminus f[Z]] \subseteq g[Y \smallsetminus f[V]]$. As a consequence, we obtain

$$g(V) = X \smallsetminus g[Y \smallsetminus f[V]] \subseteq X \smallsetminus g[Y \smallsetminus f[Z]] = g(Z).$$

Hence, γ is order preserving.

Accordingly, we can apply Knaster & Tarski's Theorem to γ, obtaining that it has a fixed point, that is, there exists some $Z \subseteq X$ such that

$$Z = \gamma(Z) = X \smallsetminus g[Y \smallsetminus f[Z]].$$

Thus,

$$X \smallsetminus Z = g[Y \smallsetminus f[Z]]. \tag{1.13}$$

Then consider the map $h\colon X \to Y$, defined, for every $x \in X$, as

$$h(x) \coloneqq \begin{cases} f(x) & \text{if } x \in Z \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

From (1.13) and the assumption that g is injective, it follows that h is well-defined.

It only remains to prove that h is a bijection. To show that it is injective, consider $x, y \in X$ such that $h(x) = h(y)$. We claim that

$$\text{either } x, y \in Z \text{ or } x, y \in X \smallsetminus Z. \tag{1.14}$$

Suppose the contrary, with a view to contradiction. We can assume, without loss of generality, that $x \in Z$ and $y \in X \smallsetminus Z$. From the definition of h it follows

$$g^{-1}(y) = h(y) = h(x) = f(x) \in f[Z].$$

Consequently, $g^{-1}(y) \notin Y \smallsetminus f[Z]$ and, therefore, $y \notin g[Y \smallsetminus f[Z]]$. Since $y \in X$, this yields

$$y \in X \smallsetminus g[Y \smallsetminus f[Z]] = \gamma(Z) = Z,$$

where the last equality follows from the fact that Z is a fixed point of γ. This contradicts the assumption that $y \in X \smallsetminus Z$, thus establishing the claim. By (1.14), there are two cases: either $x, y \in Z$ or $x, y \in X \smallsetminus Z$. If $x, y \in Z$, then $f(x) = h(x) = h(y) = f(x)$. Since f is injective, we obtain $x = y$, as desired. On the other hand, if $x, y \in X \smallsetminus Z$, then $g^{-1}(x) = h(x) = h(y) = g^{-1}(y)$, which, in turn, implies $x = y$, because g is injective. We conclude that h is also injective.

Lastly, to prove that h is surjective, consider an element $y \in Y$. As $f[Z] \subseteq h[Z]$, it suffices to consider the case where $y \notin f[Z]$. By (1.13),

$$g(y) \in g[Y \smallsetminus f[Z]] = X \smallsetminus Z.$$

Hence, $h(g(y)) = g^{-1}(g(y)) = y$, as desired. ⊠

Before presenting the second application of Kaster & Tarski's Theorem, it is convenient to recall some topological notions. Let $\langle X; \tau \rangle$ be a topological space and Y a subset of X. An element $x \in X$ is said to be

(i) a *limit point* of Y, if every open set containing x also contains an element of Y other than x; and

(ii) an *isolated point* of Y, if there exists an open set whose intersection with Y is $\{x\}$.

Lastly, Y is said to be *perfect* if it is closed and has no isolated points, and *scattered* if all its nonempty subsets have an isolated point. For instance, $\mathbb{R}$ and $\mathbb{Z}$ are, respectively, perfect and scattered in the standard topology on $\mathbb{R}$. Moreover, every well-ordered set $\mathbb{X}$ endowed with the order topology is scattered, because the minimum of every nonempty $Y \subseteq X$ is isolated in Y.

Corollary 1.58 (Cantor & Bendixson)**.** *Every closed set Y of a topological space $\langle X; \tau \rangle$ is the union of two disjoint subsets of X, one perfect and the other scattered.*

Proof. Given a subset Z of X, the set $d(Z)$ of all the limit points of Z is sometimes called the *derivative* of Z. It is easy to see that $\overline{Z} = Z \cup d(Z)$, whence Z is closed if and only if $d(Z) \subseteq Z$. Furthermore, the demand that Z has no isolated points amounts to $Z \subseteq d(Z)$. Consequently,

$$Z \text{ is perfect} \iff Z = d(Z), \text{ and} \tag{1.15}$$

$$Z \text{ is scattered} \iff \text{there is no } \varnothing \subsetneq V \subseteq Z \text{ such that } V \subseteq d(V). \tag{1.16}$$

Now, consider the map $d_Y\colon \mathcal{P}(X) \to \mathcal{P}(X)$, defined, for every $Z \subseteq X$, as

$$d_Y(Z) \coloneqq d(Z) \cap Y.$$

Notice that d_Y is order preserving on the complete lattice $\langle \mathcal{P}(X); \subseteq \rangle$, whence

$$Z \coloneqq \bigcup \{V \subseteq X : V \subseteq d_Y(V)\}$$

is a fixed point of d_Y, by Knaster & Tarski's Theorem. Consequently, $Z = d_Y(Z) = d(Z) \cap Y \subseteq Y$. Therefore, to conclude the proof, it suffices to show that Z is perfect and $Y \smallsetminus Z$ scattered.

From $Z \subseteq Y$ and the fact that the derivative map $d\colon \mathcal{P}(X) \to \mathcal{P}(X)$ is order preserving it follows $d(Z) \subseteq d(Y)$. As Y is closed, $d(Y) \subseteq Y$, whence $d(Z) \subseteq Y$. It follows that $Z = d(Z) \cap Y = d(Z)$. By (1.15), we conclude that Z is perfect. To prove that $Y \smallsetminus Z$ scattered, consider $V \subseteq Y \smallsetminus Z$ such that $V \subseteq d(V)$. Then $V \subseteq d_Y(V)$. Together with the definition of Z, this yields $V \subseteq Z$. Thus, $V \subseteq Z \cap (Y \smallsetminus Z) = \emptyset$, whence V is empty. By (1.16), we conclude that $Y \smallsetminus Z$ is scattered. ⊠

1.6 Algebraic lattices

Definition 1.59. Let $\boldsymbol{A}$ be a complete lattice.

(i) An element $a \in A$ is said to be *compact* if for every $X \subseteq A$,

$$\text{if } a \leqslant \bigvee X, \text{ then there is a finite } Y \subseteq X \text{ such that } a \leqslant \bigvee Y.$$

(ii) $\boldsymbol{A}$ is said to be *algebraic* if every element is a join of compact elements.

The following result provides a vast array of examples of algebraic lattices:

Proposition 1.60. *If C is a finitary closure operator on a set A, then the lattice of closed sets of C is an algebraic lattice, whose compact elements are those of the form $C(X)$ for some finite $X \subseteq A$.*

Proof. Let $\mathcal{C}$ be the closure system associated with C and recall that $\mathcal{C}$ is a complete lattice. We shall prove that for every $B \in \mathcal{C}$,

$$B \text{ is compact} \iff \text{there is a finite } X \subseteq A \text{ s.t. } C(X) = B. \tag{1.17}$$

First, suppose that B is compact. Clearly,

$$B \subseteq \bigvee_{b \in B} C(b).$$

Since B is compact, there is a finite set $X \subseteq B$ such that

$$B \subseteq \bigvee_{b \in X} C(b) = C(X).$$

As $X \subseteq B$, we conclude that $B = C(X)$.

Conversely, consider a finite $X \subseteq A$. We need to prove that $C(X)$ is compact. To this end, take a family $\{Y_i : i \in I\} \subseteq \mathcal{C}$ such that

$$C(X) \leqslant \bigvee_{i \in I} Y_i = C(\bigcup_{i \in I} Y_i).$$

Since X is finite and C is finitary, this implies that there are $i_1, \ldots, i_n \in I$ such that

$$C(X) \subseteq C(Y_{i_1} \cup \cdots \cup Y_{i_n}) = Y_{i_1} \vee \cdots \vee Y_{i_n}.$$

Hence, we conclude that $C(X)$ is compact. This establishes (1.17).

Finally, notice that, for every element $X \in \mathcal{C}$,

$$X = \bigvee_{x \in X} C(x).$$

By (1.17), we conclude that X is a join of compact elements. ⊠

Notably, the above result can be strengthened to the following representation theorem for algebraic lattices:

Theorem 1.61 (Representation)**.** *A lattice is algebraic if and only if it is isomorphic to the lattice of closed sets of some finitary closure operator.*

Proof. In view of Proposition 1.60, it suffices to show that every algebraic lattice is isomorphic to the lattice of closed sets of some closure operator. To this end, let $\boldsymbol{A}$ be an algebraic lattice and K the set of its compact elements. Then consider the map

$$C \colon \mathcal{P}(K) \to \mathcal{P}(K)$$

defined by the rule

$$C(X) \coloneqq K \cap {\downarrow}(\bigvee X), \text{ for all } X \subseteq K.$$

Clearly, for every $X, Y \subseteq K$ such that $X \subseteq Y$,

$$X \subseteq C(X) \subseteq C(Y).$$

Therefore, in order to prove that C is a closure operator, it only remains to show that $C(C(X)) \subseteq C(X)$. Then take $a \in C(C(X))$. We have

$$a \in K \cap {\downarrow}(\bigvee(K \cap {\downarrow}(\bigvee X))) \subseteq {\downarrow} \bigvee X.$$

As a is compact, $a \in C(X)$. We conclude that C is a closure operator on K.

To prove that C is finitary, consider a set $\{a\} \cup X \subseteq K$ such that $a \in C(X)$. We have $a \leqslant \bigvee X$. Since a is compact, there is a finite subset $Y \subseteq X$ such that $a \leqslant \bigvee Y$, whence $a \in C(Y)$.

Thus, it only remains to prove that $\boldsymbol{A}$ is isomorphic to the lattice $\mathcal{C}$ of closed sets of C. To this end, consider the map

$$f \colon \boldsymbol{A} \to \mathcal{C}$$

defined by the rule

$$f(a) \coloneqq K \cap {\downarrow}a, \text{ for all } a \in A.$$

Clearly, f is order preserving. Furthermore, since every element of $\boldsymbol{A}$ is a join of the compact elements below it, f is an order embedding. As f is clearly surjective, we conclude that it is an isomorphism. ⊠

Example 1.62. Notice that there exist nonfinitary closure operator whose lattice of closed sets are algebraic (cf. with Theorem 1.61). For consider the set $A \coloneqq \mathbb{N} \cup \{\omega\}$ and let $C\colon \mathcal{P}(A) \to \mathcal{P}(A)$ be the map defined, for every $X \subseteq A$, as

$$C(X) \coloneqq \begin{cases} X & \text{if } X \subsetneq \mathbb{N} \\ A & \text{otherwise.} \end{cases}$$

Notice that C is a nonfinitary closure operator on A. Furthermore, the lattice of closed sets of C is isomorphic to $\mathcal{P}(\mathbb{N})$, whence it is algebraic. ⊠

Definition 1.63. An element a of a lattice $\boldsymbol{A}$ is said to be

(i) *meet-irreducible* when a is not the maximum of $\boldsymbol{A}$ and for every $b, c \in A$, if $a = b \wedge c$, then either $a = b$ or $a = c$;

(ii) *join-irreducible* when a is not the minimum of $\boldsymbol{A}$ and for every $b, c \in A$, if $a = b \vee c$, then either $a = b$ or $a = c$;

(iii) *completely meet-irreducible* when for every $X \subseteq A$, if $\bigwedge X$ exists and $\bigwedge X = a$, then $a \in X$;

(iv) *completely join-irreducible* when for every $X \subseteq A$, if $\bigvee X$ exists and $\bigvee X = a$, then $a \in X$.

In view of Proposition 1.42, every completely meet-irreducible (resp. every completely join-irreducible) element is meet-irreducible (resp. join-irreducible). The converse holds for finite lattices, but not for infinite ones. For instance, let $\langle \mathbb{Q}; \leqslant \rangle$ be the chain of rational numbers with the standard order. It is easy to see that every element of $\langle \mathbb{Q}; \leqslant \rangle$ is meet and join-irreducible, but none is completely meet or join-irreducible.

Exercise 1.64. Prove the above assertion on $\langle \mathbb{Q}; \leqslant \rangle$. ⊠

This makes the following property of algebraic lattices appealing:

Theorem 1.65. *Every element in an algebraic lattice is a meet of completely meet-irreducible elements.*

Proof. Let $\boldsymbol{A}$ be an algebraic lattice and $a \in A$. First consider the set

$$M \coloneqq \{c \in A : a \leqslant c \text{ and } c \text{ is completely meet-irreducible}\}.$$

Clearly, $a \leqslant \bigwedge M$. Since $\boldsymbol{A}$ is algebraic, in order to prove that $a = \bigwedge M$, it suffices to show that every compact element $\leqslant \bigwedge M$ is also smaller or equal than a.

Suppose, with a view to contradiction, that there exists a compact element $c \leqslant \bigwedge M$ such that $c \nleqslant a$. Then consider the set

$$X \coloneqq \{b \in A : a \leqslant b \text{ and } c \nleqslant b\}.$$

We want to use Zorn's lemma to construct a maximal element in X. To this end, consider a chain C in X. We can assume, without loss of generality, that $a \in C$. Then $a \leqslant \bigvee C$. Furthermore, $c \nleqslant \bigvee C$. For suppose the contrary, with a view to contradiction. Then $c \leqslant \bigvee C$. Since c is compact, there are $e_1, \ldots, e_n \in C$ such that $c \leqslant e_1 \vee \cdots \vee e_n$. But, since C is a chain, there is $i \leqslant n$ such that $e_1 \vee \cdots \vee e_n = e_i$. Since $e_i \in X$, $c \nleqslant e_i$, a

contradiction. Hence, we conclude that $c \nleqslant \bigvee \mathcal{C}$. In particular, this implies $\bigvee C \in X$. By Zorn's lemma, there exists a maximal element $m \in X$.

Since m is maximal in X, it is straightforward to show that it is completely meet-irreducible. In particular, this implies $m \in M$. Since $c \leqslant \bigwedge M$, we obtain $c \leqslant m$, a contradiction. We conclude that $a = \bigwedge M$. ⊠

*Exercise** 1.66. An *algebra* is a structure $\boldsymbol{A} = \langle A; \{f_i : i \in I\}\rangle$ such that A is a nonempty set and for each $i \in I$ there exists some $n_i \in \omega$ such that f_i is an n_i-ary operation on A, i.e., $f_i \colon A^{n_i} \to A$. Notice that lattices, groups, rings etc. can be viewed as algebras in this sense.

A set $B \subseteq A$ is said to be a *subuniverse* of an algebra $\boldsymbol{A} = \langle A; \{f_i : i \in I\}\rangle$ if $f_i(a_1, \ldots, a_{n_i}) \in B$, for every $i \in I$ and $a_1, \ldots, a_{n_i} \in B$. It is well known that, when ordered under the inclusion relation, the set $\mathrm{Sub}(\boldsymbol{A})$ of all subuniverses of $\boldsymbol{A}$ becomes an algebraic lattice. This exercise asks you to prove a kind of converse, due to Birkhoff and Frink, namely that every algebraic lattice is isomorphic to one of the form $\mathrm{Sub}(\boldsymbol{A})$.

To this end, let $\boldsymbol{D}$ be an algebraic lattice. In view of Theorem 1.61, $\boldsymbol{D}$ is isomorphic to the lattice of closed sets of a finitary closure operator C on some set A. Furthermore, the proof of the theorem tells us that A can be chosen nonempty. For every finite subset $X \cup \{a\} \subseteq A$ such that $a \in C(X)$ and $n = |X|$, let $f_{X,a}$ be the n-ary operation on A, defined as follows. If $n = 0$, then $f_{X,a}$ is a constant whose interpretation in A is a. If $n \geqslant 1$, then for every $c_1, \ldots, c_n \in A$,

$$f_{X,a}(c_1, \ldots, c_n) \coloneqq \begin{cases} a & \text{if } \{c_1, \ldots, c_n\} = X \\ c_1 & \text{otherwise.} \end{cases}$$

Then consider the following algebra

$$\boldsymbol{A} \coloneqq \langle A; \{f_{X,a} : X \cup \{a\} \subseteq A \text{ is finite and } a \in C(X)\}\rangle.$$

Prove that $\mathrm{Sub}(\boldsymbol{A})$ coincides with the lattice of closed sets of C and, therefore, that $\langle \mathrm{Sub}(\boldsymbol{A}); \subseteq\rangle$ is isomorphic to $\boldsymbol{D}$.

A similar (but much more complicated) result by Grätzer and Schmidt states that a lattice is algebraic if and only if it is isomorphic to the lattice of congruences of some algebra [12]. ⊠

CHAPTER 2

Distributivity and representations

2.1 Modular lattices

Definition 2.1. A lattice $\boldsymbol{A}$ is said to be *modular* if it validates the equation

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

Remark 2.2. Notice that the above definition is redundant, as the inequality

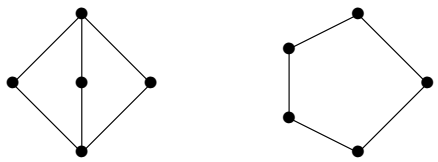
$$((x \wedge z) \vee y) \wedge z \geqslant (x \wedge z) \vee (y \wedge z)$$

holds in every lattice. Thus, a lattice $\boldsymbol{A}$ is modular precisely when there are no $a, b, c \in A$ such that

$$((a \wedge c) \vee b) \wedge c > (a \wedge c) \vee (b \wedge c). \qquad \boxtimes$$

Example 2.3. The lattice of normal subgroups of a given group is modular. More in general, a theorem by Birkhoff states that the lattice of congruences of any algebra (in the sense of Exercise 1.66) whose congruences permute is modular [2, Prop. pag. 137]. $\boxtimes$

Exercise 2.4. Consider the two special lattices depicted below: the *diamond* $\boldsymbol{M}_3$ and the *pentagon* $\boldsymbol{N}_5$.



Prove that $\boldsymbol{M}_3$ is modular and that $\boldsymbol{N}_5$ is not. Use this observation to infer that if $\boldsymbol{N}_5$ embeds into a lattice $\boldsymbol{A}$, then $\boldsymbol{A}$ is not modular. $\boxtimes$

Notably, the above sufficient condition for a failure of modularity is also necessary:

Theorem 2.5 (Dedekind)**.** *A lattice is modular if and only if* $\boldsymbol{N}_5$ *is not embeddable into it.*

Proof. In view of Exercise 2.4, it suffices to show that if a lattice $\boldsymbol{A}$ is not modular, then $\boldsymbol{N}_5$ embeds into it. To this end, consider a nonmodular lattice $\boldsymbol{A}$. Then there are $e_1, e_2, e_3 \in A$ such that

$$((e_1 \wedge e_3) \vee e_2) \wedge e_3 > (e_1 \wedge e_3) \vee (e_2 \wedge e_3).$$

Define

$$a := e_3 \quad b := e_2 \quad c := e_1 \wedge e_3.$$

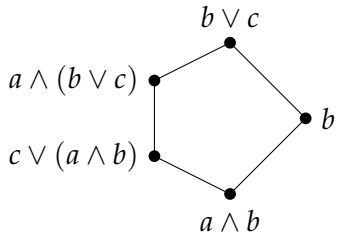
Then

$$c \leqslant a \text{ and } (c \vee b) \wedge a > c \vee (b \wedge a).$$

Consider the set

$$L := \{b \vee c, a \wedge (b \vee c), b, c \vee (a \wedge b), a \wedge b\}.$$

Observe that, since $c \leqslant a$, the following order relations hold in $\boldsymbol{A}$:



We shall prove that L, endowed with the restriction of the operations of $\boldsymbol{A}$, is a lattice isomorphic to $\boldsymbol{N}_5$. To this end, it suffices to check that:

(i) the above elements are all distinct;

(ii) their infima and suprema are as in the above figure.

(ii): Since the order relations depicted above hold, it suffices to show that

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

We detail a proof of the first equality only, as the second one it obtained similarly. First, the inequalities

$$(a \wedge (b \vee c)) \vee b, (c \vee (a \wedge b)) \vee b \leqslant b \vee c.$$

are straightforward. Moreover, from $c \leqslant a$ it follows

$$b \vee c \leqslant (a \wedge (b \vee c)) \vee b, (c \vee (a \wedge b)).$$

(i): Suppose, with a view to contradiction, that two elements in the above picture are equal. Bearing in mind that infima and suprema are as depicted above, this implies that $a \wedge (b \vee c) = c \vee (a \wedge b)$, a contradiction. ⊠

Definition 2.6. A lattice $\boldsymbol{B}$ is a *sublattice* of a lattice $\boldsymbol{A}$ if $B \subseteq A$ and the inclusion map $i\colon B \to A$ is a homomorphism. A set $B \subseteq A$ is called a *subuniverse* of $\boldsymbol{A}$ if either $B = \emptyset$ or B is the universe of a sublattice of $\boldsymbol{A}$.

Given two lattices $\boldsymbol{A}$ and $\boldsymbol{B}$, we write $\boldsymbol{A} \leqslant \boldsymbol{B}$ to indicate that $\boldsymbol{A}$ is a sublattice of $\boldsymbol{B}$.

Proposition 2.7. *Let $\boldsymbol{A}$ be a lattice. The poset of subuniverses of $\boldsymbol{A}$ ordered under inclusion is an inductive closure system on A. The associated finitary closure operator*

$$\mathrm{Sg}^{\boldsymbol{A}} \colon \mathcal{P}(A) \to \mathcal{P}(A)$$

can be described as follows: for every $X \subseteq A$,

$$\mathrm{Sg}^{\boldsymbol{A}}(X) = \{a \in A : \text{there exist a lattice term } \varphi(x_1, \ldots, x_n) \text{ and elements } a_1, \ldots, a_n \in X \text{ such that } a = \varphi^{\boldsymbol{A}}(a_1, \ldots, a_n)\}.$$

Definition 2.8. A lattice $\boldsymbol{A}$ is said to be *generated* by a set $X \subseteq A$ when $\mathrm{Sg}^{\boldsymbol{A}}(X) = A$. In this case, X is called a set of *generators* for $\boldsymbol{A}$. Accordingly, $\boldsymbol{A}$ is said to be *finitely generated* when there is a finite $X \subseteq A$ such that $\mathrm{Sg}^{\boldsymbol{A}}(X) = A$. Lastly, a class of lattices K is *locally finite* if its finitely generated members are finite.

Exercise 2.9. Prove the Proposition 2.7 and describe the compact elements of the algebraic lattice of subuniverses of $\boldsymbol{A}$. ⊠

Theorem 2.10 (Birkhoff)**.** *The class of modular lattices is not locally finite.*

Proof. Consider the set of real numbers $\mathbb{R}$. A nonempty set $V \subseteq \mathbb{R}^3$ is said to be a *vector subspace* of the vector space $\mathbb{R}^3$ if it is closed under component-wise addition and scalar multiplication, i.e., for each $\langle r_1, r_2, r_3\rangle, \langle t_1, t_2, t_3\rangle \in V$ and $s \in \mathbb{R}$,

$$\langle r_1 + t_1, r_2 + t_2, r_3 + t_3\rangle \in V \text{ and } \langle sr_1, sr_2, sr_3\rangle \in V.$$

Let $\boldsymbol{A}$ be the poset of vector subspaces of $\mathbb{R}^3$, ordered under the inclusion relation. Notice that $\boldsymbol{A}$ is a closure system, whence a complete lattice. Furthermore, meets and joins in $\boldsymbol{A}$ can be described as follows for every $a, c \in A$,

$$a \wedge c = a \cap c$$
$$a \vee c = \{\langle r_1 + t_1, r_2 + t_2, r_3 + t_3\rangle : \langle r_1, r_2, r_3\rangle \in a, \text{ and } \langle t_1, t_2, t_3\rangle \in c\}.$$

Consider the following sets

$$a \coloneqq \{\langle r, 0, r\rangle : r \in \mathbb{R}\} \quad b \coloneqq \{\langle 0, 0, r\rangle : r \in \mathbb{R}\}$$
$$c \coloneqq \{\langle 0, r, r\rangle : r \in \mathbb{R}\} \quad d \coloneqq \{\langle r, r, r\rangle : r \in \mathbb{R}\}.$$

Notice that a, b, c, d are vector subspaces of $\mathbb{R}^3$, whence $a, b, c, d \in A$. We shall prove that the sublattice of $\boldsymbol{A}$ generated by $\{a, b, c, d\}$, in symbols $\mathrm{Sg}^{\boldsymbol{A}}(\{a, b, c, d\})$, is infinite but finitely generated. Clearly, $\mathrm{Sg}^{\boldsymbol{A}}(\{a, b, c, d\})$ is finitely generated. To prove that it is infinite, consider the lattice terms

$$\psi_1(y, x_1, x_2, x_3, x_4) \coloneqq (((x_1 \vee x_2) \wedge (x_3 \vee x_4)) \vee y) \wedge (x_2 \vee x_3)$$
$$\psi_2(y, x_1, x_2, x_3, x_4) \coloneqq (((x_1 \vee x_4) \wedge (x_2 \vee x_3)) \vee y) \wedge (x_1 \vee x_2)$$
$$\varphi(y, x_1, x_2, x_3, x_4) \coloneqq (\psi_1 \vee \psi_2) \wedge (x_2 \vee x_4).$$

Moreover, for every positive integer n define

$$e_n \coloneqq \{\langle r, r, 2^n r\rangle : r \in \mathbb{R}\}.$$

Notice that each e_n is a vector subspace of $\mathbb{R}^3$ and that $e_n \neq e_m$, provided that $n \neq m$. Therefore, in order to prove that $\mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\})$ is infinite, it suffices to show that

$$\{e_n : 1 \leqslant n \in \omega\} \subseteq \mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\}). \tag{2.1}$$

To this end, we reason by induction on n. First, using the definition of $\wedge$ and $\vee$ given above, we obtain

$$e_1 = (a \vee c) \wedge (b \vee d) \in \mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\}).$$

For the inductive step, suppose that $e_n \in \mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\})$. Again, using the definition of $\wedge$ and $\vee$ given above, it is not hard to see that

$$\begin{aligned}\psi_1(e_n,a,b,c,d) &= \{\langle 0, r, 2^n r\rangle : r \in \mathbb{R}\}\\ \psi_2(e_n,a,b,c,d) &= \{\langle r, 0, 2^n r\rangle : r \in \mathbb{R}\},\end{aligned}$$

whence

$$e_{n+1} = \varphi^{\boldsymbol{A}}(e_n,a,b,c,d) \in \mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\}).$$

This establishes (2.1) and, therefore, that $\mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\})$ is infinite.

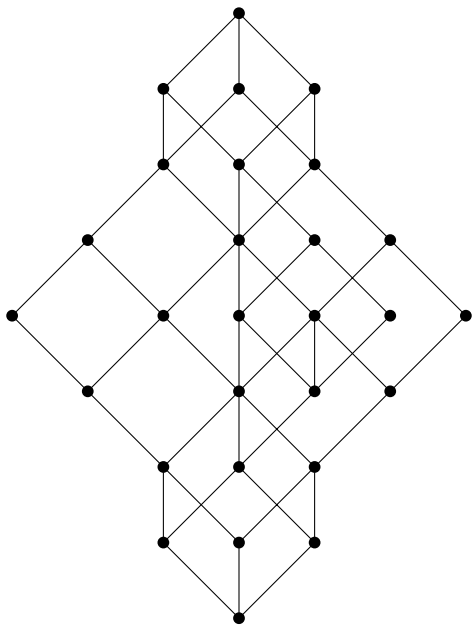
It only remains to prove that $\mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\})$ is modular. This is left as an exercise. ⊠

Corollary 2.11. *Every class of lattices that extends that of modular lattices is not locally finite. In particular, the class of all lattices is not locally finite.*

*Exercise** 2.12. Prove that the lattice $\boldsymbol{A}$ of vector subspaces of $\mathbb{R}^3$ is modular (hint: use the description of $\wedge$ and $\vee$ in $\boldsymbol{A}$ given in the proof of Theorem 2.10). Use this fact to infer that the lattice $\mathrm{Sg}^{\boldsymbol{A}}(\{a,b,c,d\})$ in the proof of Theorem 2.10 is also modular. ⊠

Remark 2.13. Given a positive integer n, a lattice $\boldsymbol{A}$ is said to be *n-generated* if it has a set of generators of size $\leqslant n$. The proof of Theorem 2.10 shows that there is an infinite 4-generated modular lattice. This contrasts with the fact, proved by Dedekind [8], that all 3-generated modular lattices are finite (actually of cardinality $\leqslant 28$).

More precisely, let $\boldsymbol{C}$ be 3-generated modular the lattice depicted below:



Dedekind proved (essentially) that a lattice $\boldsymbol{A}$ is modular and 3-generated if and only if there exists a surjective homomorphism $f\colon \boldsymbol{C} \to \boldsymbol{A}$.* ⊠

2.2 Distributive lattices

Definition 2.14. A lattice $\boldsymbol{A}$ is said to be *distributive* if it validates the following equations:

$$x \wedge (y \vee z) \approx (x \wedge y) \vee (x \wedge z) \quad x \vee (y \wedge z) \approx (x \vee y) \wedge (x \vee z).$$

Exercise 2.15. The above definition is indeed redundant. Show that the following conditions are equivalent for a lattice $\boldsymbol{A}$:

(i) $\boldsymbol{A}$ is distributive;

(ii) $\boldsymbol{A}$ validates the inequality $x \wedge (y \vee z) \leqslant (x \wedge y) \vee (x \wedge z)$;

(iii) $\boldsymbol{A}$ validates the inequality $x \vee (y \wedge z) \geqslant (x \vee y) \wedge (x \vee z)$. ⊠

Example 2.16. For every poset $\mathbb{X}$, the complete lattice $\mathrm{Up}(\mathbb{X})$ is distributive. In particular, taking $\mathbb{X} = \langle X; \mathrm{Id}_X \rangle$, we obtain that the powerset lattice $\langle \mathcal{P}(X); \subseteq \rangle$ is distributive. Lastly, every nonempty chain is a distributive lattice. ⊠

Proposition 2.17. *Every distributive lattice is modular.*

Proof. Let $\boldsymbol{A}$ be a distributive lattice and $a, b, c \in A$. Applying distributivity in the first step, we get

$$((a \wedge c) \vee b) \wedge c = ((a \wedge c) \wedge c) \vee (b \wedge c) = (a \wedge c) \vee (b \wedge c).$$ ⊠

Exercise 2.18. Recall from Exercise 2.4 that $\boldsymbol{M}_3$ is modular, while $\boldsymbol{N}_5$ is not. As distributive lattices are modular, $\boldsymbol{N}_5$ is not distributive. Prove that $\boldsymbol{M}_3$ is not distributive either. Use these observations to infer that if either $\boldsymbol{M}_3$ or $\boldsymbol{N}_5$ embed into a lattice $\boldsymbol{A}$, then $\boldsymbol{A}$ is not distributive. ⊠

Notably, the above sufficient condition for a failure of distributivity is also necessary:

Theorem 2.19 (Birkhoff)**.** *A lattice is distributive if and only if neither $\boldsymbol{M}_3$ nor $\boldsymbol{N}_5$ embeds into it.*

Proof. In view of Exercise 2.18, it suffices to show that if a lattice $\boldsymbol{A}$ is not distributive, then either $\boldsymbol{M}_3$ or $\boldsymbol{N}_5$ embeds into it. To this end, consider a nondistributive lattice $\boldsymbol{A}$. If $\boldsymbol{A}$ is nonmodular, then $\boldsymbol{N}_5$ embeds into it by Theorem 2.5 and we are done.

Then we consider the case where $\boldsymbol{A}$ is modular. Since $\boldsymbol{A}$ fails to be distributive, there are elements $a, b, c \in A$ such that

$$a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c). \tag{2.2}$$

We shall prove that also

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) < (a \vee b) \wedge (a \vee c) \wedge (b \vee c). \tag{2.3}$$

*In fact, what Dedekind proved is that $\boldsymbol{C}$ is the three-generated free modular lattice.

Suppose the contrary, with a view to contradiction. Since it is always the case that $(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) \leqslant (a \vee b) \wedge (a \vee c) \wedge (b \vee c)$, this implies

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \wedge (b \vee c). \tag{2.4}$$

Notice that the following equality always holds:

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

Together with (2.4), this yields

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

As $a \geqslant (a \wedge b) \vee (a \wedge c)$, we get

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

Taking

$$z := a \quad y := b \wedge c \quad x := (a \wedge b) \vee (a \wedge c),$$

and applying the modularity law $((x \wedge z) \vee y) \wedge z \approx (x \wedge z) \vee (y \wedge z)$, we obtain

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

Thus, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, a contradiction with (2.2). This establishes (2.3).

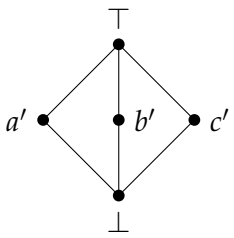
Now, define

$$\begin{aligned} \bot &:= (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) \\ \top &:= (a \vee b) \wedge (a \vee c) \wedge (b \vee c) \\ a' &:= (\bot \vee a) \wedge \top \\ b' &:= (\bot \vee b) \wedge \top \\ c' &:= (\bot \vee c) \wedge \top. \end{aligned}$$

Notice that $\bot < \top$, by (2.3). Consider the of elements

$$L := \{\bot, a', b', c', \top\}.$$

Observe that the following order relations hold in $\boldsymbol{A}$:



We shall prove that L, endowed with the restriction of the operations of $\boldsymbol{A}$, is a lattice isomorphic to $\boldsymbol{M}_3$. To this end, it suffices to check that:

(i) the above elements are all distinct;

(ii) their infima and suprema are as in the above figure.

(ii): Since the order relations between the elements of L depicted above hold, it suffices to prove that

$$a' \wedge b' = b' \wedge c' = a' \wedge c' = \bot \text{ and } a' \vee b' = b' \vee c' = a' \vee c' = \top. \tag{2.5}$$

Notice that by modularity,

$$a' = (\bot \vee a) \wedge \top = ((\bot \wedge \top) \vee a) \wedge \top = (\bot \wedge \top) \vee (a \wedge \top) = \bot \vee (a \wedge \top).$$

Similarly, we obtain

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

Because of the symmetry in the above definitions of a', b', c', to establish (2.5) it suffices to prove that $a' \wedge b' = \bot$. To this end, notice that

$$a \vee \bot = a \vee (a \wedge b) \vee (a \wedge c) \vee (b \wedge c) = a \vee (b \wedge c). \tag{2.6}$$

The first equality above follows from the definition of $\bot$, while the second is straightforward. Then we get

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

The equalities above are justified as follows: the first follows from the definition of a', the second from (2.6), the third from the definition of $\top$, the fourth is straightforward. Similarly, we get

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

Thus,

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

The first equality above follows from the description of a' and b', the second, first, and fifth are straightforward, the fourth and the sixth follow from modularity, and the last one from the definition of $\bot$. Then we conclude that the infima and suprema of elements in L are as in the above figure.

(i): Suppose, with a view to contradiction, that two elements in the above picture are equal. Bearing in mind that infima and suprema are as depicted above, this implies that $\bot = \top$, a contradiction with (2.3). ⊠

Definition 2.20. A lattice term $\varphi(x_1, \ldots, x_n)$ is in *conjunctive normal form* (CNF for short) there are distinct nonempty sets $V_1, \ldots, V_k \subseteq \{x_1, \ldots, x_n\}$ such that

$$\varphi = (\bigvee V_1) \wedge \cdots \wedge (\bigvee V_k).$$

The notion of *disjunctive normal form* (DNF for short) is defined symmetrically.

For instance, the terms

$$x \vee y \quad x \wedge (y \vee z) \wedge (z \vee x) \wedge (z \vee y \vee v)$$

are in CFN, while $x \vee (y \wedge z)$ and $x \wedge x$ are not. Notice that there are finitely many lattice terms in CNF (resp. DNF) in variables $x_1, \ldots, x_n$.

Theorem 2.21. *For every lattice term φ is there is a lattice term ψ in CNF (resp. DNF) such that the equation $\varphi \approx \psi$ holds in the class of distributive lattices.*

Proof. Let DL be the class of distributive lattices. We reason by induction on the construction of φ. First, if φ is a variable, then φ is already in CNF. Then suppose that $\varphi = \psi * \delta$ for some operation $* \in \{\wedge, \vee\}$. By inductive hypothesisthere are terms ψ^+ and δ^+ in CNF such that the equations $\psi \approx \psi^+$ and $\delta \approx \delta^+$ hold in DL. As ψ^+ and δ^+ are in CNF, they are of the form

$$\psi^+ = (\bigvee V_1) \wedge \cdots \wedge (\bigvee V_n) \text{ and } \delta^+ = (\bigvee U_1) \wedge \cdots \wedge (\bigvee U_m).$$

Now, we have two cases: either $* = \wedge$ or $* = \vee$. First, suppose that $* = \wedge$. In this case, let $W_1, \ldots, W_k$ be the distinct elements occurring in the list

$$V_1, \ldots, V_n, U_1, \ldots, U_m.$$

Then define

$$\varphi^+ := (\bigvee W_1) \wedge \cdots \wedge (\bigvee W_k).$$

By inductive hypothesis, φ^+ is in CNF. Furthermore, as the equations $\psi \approx \psi^+$ and $\delta \approx \delta^+$ hold in DL, also the equation $\psi \wedge \delta \approx \varphi^+$ holds in DL. Since $\varphi = \psi \wedge \delta$, we are done.

Then we consider the case in which $* = \vee$. Notice that in the class of distributive lattices the following equation holds:

$$((\bigvee V_1) \wedge \cdots \wedge (\bigvee V_n)) \vee ((\bigvee U_1) \wedge \cdots \wedge (\bigvee U_m)) \approx \bigwedge_{i \leqslant n \& j \leqslant m} (\bigvee (V_i \cup U_j)).$$

Let then $\{W_1, \ldots, W_k\}$ be an enumeration without repetitions of the set

$$\{V_i \cup U_j : i \leqslant n \text{ and } j \leqslant m\}.$$

Then define

$$\varphi^+ := (\bigvee W_1) \wedge \cdots \wedge (\bigvee W_k).$$

Again, by inductive hypothesis, φ^+ is in CNF. Moreover, the equation $\varphi \approx \varphi^+$ holds in DL. ⊠

Corollary 2.22. *The class of distributive lattices is locally finite.*

Proof. Let $\boldsymbol{A}$ be a finitely generated distributive lattice. Then there are $a_1, \ldots, a_n \in A$ such that $\{a_1, \ldots, a_n\}$ is a set of generators for $\boldsymbol{A}$. By Proposition 2.7 and Theorem 2.21,

$$\mathrm{Sg}^{\boldsymbol{A}}(a_1, \ldots, a_n) = \{\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) : \varphi(x_1, \ldots, x_n) \text{ is a lattice term in CNF}\}.$$

Since there are finitely many lattice terms in CNF with variables among $x_1, \ldots, x_n$, we conclude that $A = \mathrm{Sg}^{\boldsymbol{A}}(a_1, \ldots, a_n)$ is finite. ⊠

*Exercise** 2.23. In view of Corollary 2.22, every finitely generated distributive lattice is finite. This poses the following question: given a positive integer n, how large is the largest n-generated distributive lattice? This exercise guides you to an answer to this question.

First, given subset $X \subseteq \mathcal{P}(\{x_1, \ldots, x_n\})$, we define

$$X^* := \{Y \in X : \text{there is no } Z \in X \text{ such that } Z \subsetneq Y\}.$$

A nonempty set $X \subseteq \mathcal{P}(\{x_1, \ldots, x_n\})$ is called *irredundant* when $X = X^*$.

Let D_n be the set of irredundant subsets of $\mathcal{P}(\{x_1, \ldots, x_n\})$. Given $X, Y \in D_n$, we define

$$X \wedge Y := (X \cup Y)^* \text{ and } X \vee Y := \{V \cup U : V \in X \text{ and } U \in Y\}^*.$$

(i) Prove that $\boldsymbol{D}_n := \langle D_n; \wedge, \vee \rangle$ is a distributive lattice;

(ii) Prove that $\{\{\{x_1\}\}, \ldots, \{\{x_n\}\}\}$ is a set of generators of $\boldsymbol{D}_n$, whence $\boldsymbol{D}_n$ is n-generated.

Let now $\boldsymbol{A}$ be any n-generated distributive lattice and $\{a_1, \ldots, a_n\}$ a set of generators for $\boldsymbol{A}$. Let also $f\colon \{x_1, \ldots, x_n\} \to \{a_1, \ldots, a_n\}$ be the map such that $f(x_i) = a_i$ for all $i \leqslant n$.

(iii) Prove that the map $f^+\colon \boldsymbol{D}_n \to \boldsymbol{A}$, defined by the rule

$$f^+(\{V_1, \ldots, V_m\}) := (\bigvee f[V_1]) \wedge \cdots \wedge (\bigvee f[V_m]),$$

is a homomorphism;

(iv) Prove that f^+ is surjective (use the fact that homomorphisms preserve arbitrary lattice terms and that $a_1, \ldots, a_n$ generate $\boldsymbol{A}$).

Hence, $\boldsymbol{D}_n$ is the largest n-generated distributive lattice. The size of $\boldsymbol{D}_n$[†] is known (explicitly) only up to $n = 8$ and is 56130437228687557907788. ⊠

2.3 Prime filters and ideals

Definition 2.24. An element a in a lattice $\boldsymbol{A}$ is said to be

(i) *meet-prime* when it is not the maximum of $\boldsymbol{A}$ and for every $b, c \in A$, if $a \geqslant b \wedge c$, then either $a \geqslant b$ or $a \geqslant c$;

(ii) *join-prime* when it is not the minimum of $\boldsymbol{A}$ and for every $b, c \in A$, if $a \leqslant b \vee c$, then either $a \leqslant b$ or $a \leqslant c$.

[†]Indeed, the exercise implies that $\boldsymbol{D}_n$ is the free n-generated distributive lattice.

Notice that every meet-prime (resp. join-prime) element of a lattice is necessarily meet-irreducible (resp. join-irreducible). The converse, however, does not hold in general. For instance, the three incomparable elements of the modular diamond $\boldsymbol{M}_3$ are both meet and join-irreducible, but neither meet nor join-prime.

Proposition 2.25. *In a distributive lattice, meet-prime (resp. join-prime) and meet-irreducible (resp. join-irreducible) elements coincide.*

Proof. Let $\boldsymbol{A}$ be a distributive lattice. It suffices to show that that every meet-irreducible element $a \in A$ is also meet-prime. To this end, consider $b, c \in A$ such that $b \wedge c \leqslant a$, i.e., $a \vee (b \wedge c) = a$. By distributivity,

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

Since a is meet-irreducible, this yields that either $a = a \vee b$ or $a = a \vee c$. Thus, either $b \leqslant a$ or $c \leqslant a$, as desired. ⊠

Definition 2.26. Let $\boldsymbol{A}$ be a lattice.

(i) A set $F \subseteq A$ is said to be a *filter* if it is an upset and $a \wedge c \in F$, for all $a, c \in F$.

(ii) A set $I \subseteq A$ is said to be a *ideal* if it is a downset and $a \vee c \in I$, for all $a, c \in I$.

A filter F (resp. an ideal I) is said to be *proper* when $F \neq A$ (resp. $I \neq A$). The posets of filters and of ideals of $\boldsymbol{A}$, ordered under the inclusion relation, are denoted, respectively, by

$$\mathcal{F}i\boldsymbol{A} \text{ and } \mathcal{I}d\boldsymbol{A}.$$

Proposition 2.27. *Let $\boldsymbol{A}$ be a lattice. The posets $\mathcal{F}i\boldsymbol{A}$ and $\mathcal{I}d\boldsymbol{A}$ filters and of ideals of $\boldsymbol{A}$ are inductive closure systems on A. The associated finitary closure operators*

$$\mathrm{Fg}^{\boldsymbol{A}} \colon \mathcal{P}(A) \to \mathcal{P}(A) \text{ and } \mathrm{Ig}^{\boldsymbol{A}} \colon \mathcal{P}(A) \to \mathcal{P}(A)$$

can be described as follows: for every $X \subseteq A$,

$$\begin{aligned} \mathrm{Fg}^{\boldsymbol{A}}(X) &= \{a \in A : \textit{there are } c_1, \ldots, c_n \in X \textit{ such that } c_1 \wedge \cdots \wedge c_n \leqslant a\} \\ \mathrm{Ig}^{\boldsymbol{A}}(X) &= \{a \in A : \textit{there are } c_1, \ldots, c_n \in X \textit{ such that } c_1 \vee \cdots \vee c_n \geqslant a\}. \end{aligned}$$

Exercise 2.28. Prove the above statement. ⊠

Let $\boldsymbol{A}$ be a lattice. A filter F of $\boldsymbol{A}$ is said to be *principal* when there is some $a \in A$ such that F is the least filter containing a, that is

$$F = \mathrm{Fg}^{\boldsymbol{A}}(a) = {\uparrow}a.$$

Similarly, an ideal I is said to be *principal* when there is some $a \in A$ such that

$$I = \mathrm{Ig}^{\boldsymbol{A}}(a) = {\downarrow}a.$$

Proposition 2.29. *If $\boldsymbol{A}$ is a finite lattice, then all its nonempty filters and ideals are principal. Consequently, the poset of nonempty filters of $\boldsymbol{A}$ is isomorphic to $\boldsymbol{A}^{\partial}$ and the poset of nonempty ideals is isomorphic to $\boldsymbol{A}$ itself.*

Proof. Let F be a nonempty filter. Since $\boldsymbol{A}$ is finite, we can take an enumeration $F = \{a_1, \dots, a_n\}$. Clearly, $c := a_1 \wedge \cdots \wedge a_n \in F$. Furthermore, $F = {\uparrow}c$, whence F is principal. A similar argument shows that all nonempty ideals are principal.

Now, let $\mathcal{F}i\boldsymbol{A}^-$ be the poset of nonempty filters of $\boldsymbol{A}$. As all nonempty filters are principal, the universe of $\mathcal{F}i\boldsymbol{A}^-$ is $\{{\uparrow}a : a \in A\}$. Bearing this in mind, consider the map $f\colon \boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}^-$ such that $f(a) := {\uparrow}a$, for every $a \in A$. Clearly, f is surjective. It is also injective, because of the antisymmetry of the partial order of $\boldsymbol{A}$. Lastly, for every $a, c \in A$,

$$a \leqslant c \iff c \in {\uparrow}a \iff {\uparrow}c \subseteq {\uparrow}a \iff f(c) \subseteq f(a).$$

Since f is a bijection, we conclude that is an an isomorphism from $\boldsymbol{A}^\partial$ to $\mathcal{F}i\boldsymbol{A}^-$. A similar argument shows that $\boldsymbol{A}$ is isomorphic to the poset of its nonempty ideals. ⊠

In an infinite lattice, however, nonempty filters and ideals need not be principal, as we proceed to explain.

Exercise 2.30. Consider the chain $\langle \mathbb{Q}; \leqslant \rangle$ of rational numbers with the standard ordering. Notice that $\langle \mathbb{Q}; \leqslant \rangle$ is a distributive lattice. Prove that its its filters (resp. ideals) coincide precisely with its upsets (resp. downsets). Prove that $\langle \mathbb{Q}; \leqslant \rangle$ has a continuum of filters and a continuum of ideals, but only countably many principal filters and ideals. ⊠

Definition 2.31. Let $\boldsymbol{A}$ be a lattice.

(i) A filter F of $\boldsymbol{A}$ is said to be *prime* if it is proper, nonempty, and for every $a, c \in A$, if $a \vee c \in F$, then either $a \in F$ or $c \in F$.

(ii) An ideal U of $\boldsymbol{A}$ is said to be *prime* if it is proper, nonempty, and for every $a, c \in A$, if $a \wedge c \in I$, then either $a \in I$ or $c \in I$.

The posets of prime filters and of prime ideals of $\boldsymbol{A}$ will be denoted, respectively, by

$$\mathrm{Prf}\boldsymbol{A} \text{ and } \mathrm{Pri}\boldsymbol{A}.$$

Example 2.32. Let $\mathbb{N}^\partial$ be the dual of the poset of the natural numbers with the standard order and $\mathbb{N}^\partial \times \mathbb{N}^\partial$ its direct product depicted in Figure 2.1. Notice that both $\mathbb{N}^\partial$ and $\mathbb{N}^\partial \times \mathbb{N}^\partial$ are distributive lattices. We shall describe their prime filters.

As the prime filters of a chain coincide with its proper nonempty upsets, the prime filters of $\mathbb{N}^\partial$ are precisely the subsets of $\mathbb{N}$ of the form

$$[\![n]\!] := \{0, 1, 2, \dots, n\}$$

for some $n \in \mathbb{N}$. In particular, every prime filter of $\mathbb{N}^\partial$ is principal. Accordingly, the poset $\mathrm{Prf}\,\mathbb{N}^\partial$ is isomorphic to $\mathbb{N}$ with the standard ordering, as shown in Figure 2.2.

The description of prime filters of $\mathbb{N}^\partial \times \mathbb{N}^\partial$ is slightly more complicated. Looking at Figure 2.1, one sees that

$$\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial) = \{[\![n]\!] \times \mathbb{N} : n \in \mathbb{N}\} \cup \{\mathbb{N} \times [\![n]\!] : n\mathbb{N}\}.$$

Consequently, no prime filter of $\mathbb{N}^\partial \times \mathbb{N}^\partial$ is principal. Furthermore, $\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial)$ is isomorphic to the disjoint union of two copies of $\mathrm{Prf}\,\mathbb{N}^\partial$, i.e., to the disjoint union of two copies of $\mathbb{N}$ endowed with the standard order, as shown in Figure 2.2.

⊠

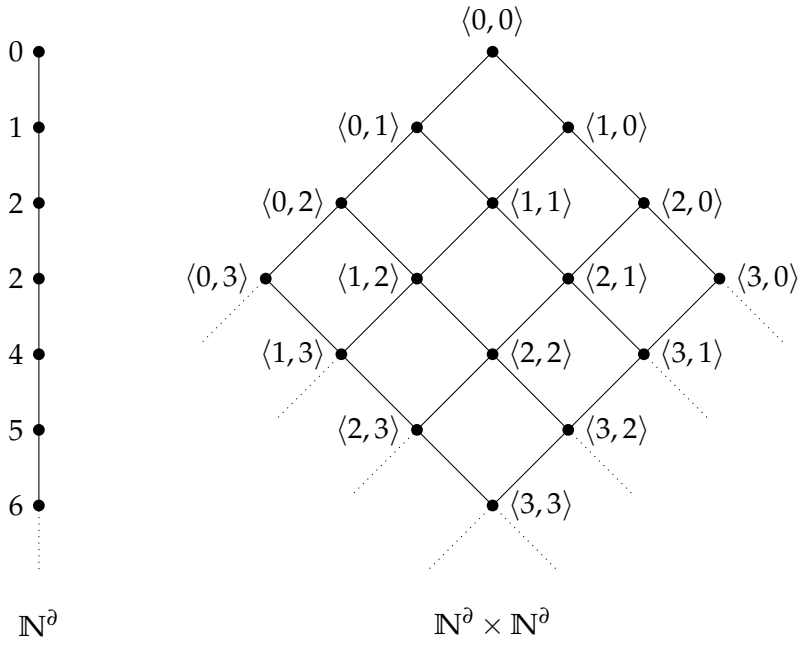


Figure 2.1: The distributive lattices $\mathbb{N}^\partial$ and $\mathbb{N}^\partial \times \mathbb{N}^\partial$.

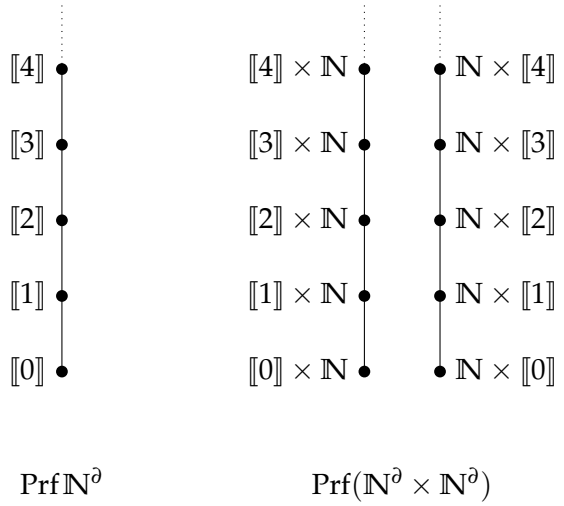


Figure 2.2: The posets $\mathrm{Prf}\,\mathbb{N}^\partial$ and $\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial)$.

Proposition 2.33. *Let $\boldsymbol{A}$ be a lattice, F a filter, and I an ideal. The following conditions hold:*

(i) *F is a prime filter if and only if F^c is a proper nonempty ideal;*

(ii) *I is a prime ideal if and only if I^c is a proper nonempty filter.*

Proof. Immediate from the definitions. ⊠

Proposition 2.34. *Let $\boldsymbol{A}$ be a lattice and $F, I \subseteq A$.*

(i) *F is a principal prime filter of $\boldsymbol{A}$ if and only if $F = {\uparrow}a$ for some join-prime $a \in A$;*

(ii) *I is a principal prime ideal of $\boldsymbol{A}$ if and only if $I = {\downarrow}a$ for some meet-prime $a \in A$;*

Proof. We detail only the proof of condition (i). Let F be a principal prime filter of $\boldsymbol{A}$. Then there exists $a \in A$ such that $F = {\uparrow}a$. As F is proper, $a > 0$. Moreover, consider $b, c \in A$ such that $a \leqslant b \vee c$. As $F = {\uparrow}a$, this implies $b \vee c \in F$. Using the assumption that F is prime, we conclude that either $b \in F$ or $c \in F$. Together with the fact that $F = {\uparrow}a$, this yields that either $a \leqslant b$ or $a \leqslant c$. We conclude that a is join-prime.

Conversely, consider a join-prime element $a \in A$. As $a > 0$, we get that ${\uparrow}a$ is a proper filter. Then consider $b, c \in A$ such that $b \vee c \in {\uparrow}a$. As a is join-prime, either $a \leqslant b$ or $a \leqslant c$, whence either $b \in {\uparrow}a$ or $c \in {\uparrow}a$. It follows that ${\uparrow}a$ is a prime filter. ⊠

Corollary 2.35. *Let $\boldsymbol{A}$ be a finite lattice.*

(i) *The prime filters of $\boldsymbol{A}$ are precisely the principal filters generated by join-prime elements.*

(ii) *The prime ideals of $\boldsymbol{A}$ are precisely the principal filters generated by meet-prime elements.*

Consequently, $\mathrm{Prf}\boldsymbol{A}$ *is isomorphic to the dual of the poset of join-prime elements and* $\mathrm{Pri}\boldsymbol{A}$ *is isomorphic to the poset of meet-prime elements.*

Proof. Immediate from Propositions 2.29 and 2.34. ⊠

The following result explains why prime filters and ideals deserve their name:

Proposition 2.36. *Let $\boldsymbol{A}$ be a distributive lattice, F a proper nonempty filters, and I a proper nonempty ideal.*

(i) *F is prime if and only if it is meet-irreducible in $\mathcal{F}i\boldsymbol{A}$;*

(ii) *F is prime if and only if it is meet-irreducible in $\mathcal{I}d\boldsymbol{A}$.*

Proof. We detail the proof of condition (i), as the other one can be treated similarly. First, suppose, with a view to contradiction, that F is prime but not meet-irreducible in $\mathcal{F}i\boldsymbol{A}$. Then there are two filters G and H of $\boldsymbol{A}$ such that $F = G \cap H$, but $F \neq H, G$. Thus, there are $a \in G \smallsetminus F$ and $c \in H \smallsetminus F$. Since G and H are filters, this yields $a \vee c \in G \cap H = F$. As F is prime, either $a \in F$ or $c \in F$, a contradiction.

Conversely, suppose that F is meet-irreducible in $\mathcal{F}i\boldsymbol{A}$. Then suppose that $a \vee c \in F$. We shall prove that

$$F = \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{a\}) \cap \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{c\}). \tag{2.7}$$

The inclusion from left to right is obvious. To prove the other one, consider $b \in \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{a\}) \cap \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{c\})$. By Proposition 2.27 there are $d_1, \ldots, d_n, e_1, \ldots, e_m \in F$ such that

$$a \wedge d_1 \wedge \cdots \wedge d_n, c \wedge e_1 \wedge \cdots \wedge e_m \leqslant b.$$

Consider the element $g := d_1 \wedge \cdots \wedge d_n \wedge e_1 \wedge \cdots \wedge e_m$. Since F is a filter, $g \in F$. Furthermore,

$$a \wedge g, c \wedge g \leqslant b.$$

Consequently, $(a \wedge g) \vee (c \wedge g) \leqslant b$. Applying distributivity,

$$g \wedge (a \vee c) = (a \wedge g) \vee (c \wedge g) \leqslant b.$$

Since $g, a \vee c \in F$, the above display implies $b \in F$, as desired. This establishes (2.7). Now, since F is meet-irreducible, either $F = \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{a\})$ or $F = \mathrm{Fg}^{\boldsymbol{A}}(F \cup \{c\})$. In particular, either $a \in F$ or $c \in F$, as desired. ⊠

2.4 Representation of distributive lattices

We shall prove a representation theorem for distributive lattices stating that, for distributive lattices, meets and joins can be represented, respectively, as intersections and unions on a certain fields of sets.

Theorem 2.37 (Prime Filter Theorem)**.** *Let $\boldsymbol{A}$ be a distributive lattice. If F is a nonempty filter and I a nonempty ideal such that $F \cap I = \emptyset$, then there exists a prime filter G such that $F \subseteq G$ and $G \cap I = \emptyset$.*

Proof. First notice that F is proper. Suppose the contrary, with a view to contradiction. Then $F = A \supseteq I$. Since I is nonempty, this implies

$$F \cap I = A \cap I = I \neq \emptyset,$$

a contradiction with the assumptions.

Then consider the family

$$\mathcal{F} := \{G \in \mathcal{F}i\boldsymbol{A} : F \subseteq G, G \text{ is proper, and } G \cap I = \emptyset\}.$$

We want to apply Zorn's Lemma. To this end, consider a chain C in $\mathcal{F}$. Since F is proper, we can assume, without loss of generality, that $F \in C$. Then take $G := \bigcup C$. As unions of chains of filters are still filters, $G \in \mathcal{F}i\boldsymbol{A}$. Furthermore, clearly $F \subseteq G$ and $G \cap I = \emptyset$. It only remains to prove that G is proper. But this follows from the assumption that I is nonempty and the observation that $G \cap I = \emptyset$. Thus, G is an upper bound for C. By Zorn's Lemma, there is a maximal element $G \in \mathcal{F}$.

Clearly, G is a filter such that $F \subseteq G$ and $G \cap I = \emptyset$. It only remains to prove that G is prime. Suppose the contrary, with a view to contradiction. Notice that G is nonempty, since F is, and proper. Thus, by Proposition 2.36, there are $H_1, H_2 \in \mathcal{F}i\boldsymbol{A}$ such that $G = H_1 \cap H_2$ and $G \subsetneq H_1, H_2$. Clearly, H_1 and H_2 are proper (otherwise either $G = H_1$ or $G = H_2$) and extend F. Thus, by the maximality of G, we obtain

$$H_1 \cap I \neq \emptyset \text{ and } H_2 \cap I \neq \emptyset.$$

Let $a \in H_1 \cap I$ and $c \in H_2 \cap I$. We have

$$a \vee c \in H_1 \cap H_2 \cap I = G \cap I,$$

a contradiction with $G \cap I = \emptyset$. ⊠

Corollary 2.38. *Let $\boldsymbol{A}$ be a distributive lattice and $a, c \in A$. If $a \not\leqslant c$, then there is a prime filter F such that $a \in F$ and $c \notin F$.*

Proof. Consider the filter $\uparrow a$ and the ideal $\downarrow c$. Since $a \not\leqslant c$, we get $\uparrow a \cap \downarrow c = \emptyset$. Furthermore, $\uparrow a$ and $\downarrow c$ are clearly nonempty. Bearing this in mind, we can apply Theorem 2.37 obtaining a prime filter F such that $a \in F$ and $c \notin F$. ⊠

As a consequence, in distributive lattices, filters are determined by the prime filters that extends them. More precisely, we have the following:

Proposition 2.39. *If $\boldsymbol{A}$ be a distributive lattice and F a nonempty filter, then*

$$F = \bigcap \{G \in \mathrm{Prf}\boldsymbol{A} : F \subseteq G\},$$

where $\bigcap$ is computed in the complete lattice $\mathcal{F}i\boldsymbol{A}$.

Exercise 2.40. Prove the above assertion. ⊠

We are now ready to present the representation theorem for distributive lattices (cf. Example 2.16):

Theorem 2.41 (Birkhoff)**.** *Every distributive lattice embeds into the lattice of upsets of some poset. More precisely, if $\boldsymbol{A}$ is a distributive lattice, then the map*

$$\gamma \colon \boldsymbol{A} \to \mathrm{Up}(\mathrm{Prf}\boldsymbol{A}),$$

defined for every $a \in A$ as

$$\gamma(a) \coloneqq \{F \in \mathrm{Prf}\boldsymbol{A} : a \in F\},$$

is an embedding.

Proof. To shorten the notation, let $\mathbb{X} \coloneqq \mathrm{Prf}\boldsymbol{A}$. First recall from Example 2.16 that $\mathrm{Up}(\mathbb{X})$ is a complete distributive lattice in which infima and suprema are intersections and unions. Then notice that the map γ is well-defined, as $\gamma(a)$ is an upset of $\mathbb{X}$, for every $a \in A$. Furthermore, take $a, c \in A$. We have

$$\gamma(a \wedge c) = \{F \in \mathbb{X} : a \wedge c \in F\} = \{F \in \mathbb{X} : a, c \in F\} = \gamma(a) \cap \gamma(c),$$

where the second equality follows from the fact that F is a filter. Furthermore,

$$\begin{aligned} \gamma(a \vee c) &= \{F \in \mathbb{X} : a \vee c \in F\} \\ &= \{F \in \mathbb{X} : \text{either } a \in F \text{ or } c \in F\} \\ &= \gamma(a) \cup \gamma(c), \end{aligned}$$

where the second equality follows from the fact that F is a prime filter. Thus, $\gamma \colon \boldsymbol{A} \to \mathrm{Up}(\mathbb{X})$ is a homomorphism. To prove that it is injective, consider two distinct elements a and c of A. We can assume, without loss of generality, that $a \not\leqslant c$. By Corollary 2.38, there is a prime filter F such that $a \in F$ and $c \notin F$. Thus, $F \in \gamma(a) \smallsetminus \gamma(c)$, whence $\gamma(a) \neq \gamma(c)$. We conclude that γ is injective and, therefore, an embedding. ⊠

Remark 2.42. The embedding γ in the above theorem need not be an isomorphism. This is because, while the lattice $\mathrm{Up}(\mathbb{X})$ is always complete, the original lattice $\boldsymbol{A}$ need not be. However, if $\boldsymbol{A}$ is finite, γ turns out to be an isomorphism, as we proceed to explain. ⊠

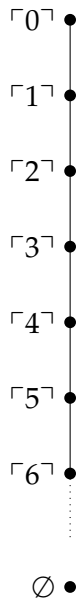


Figure 2.3: The distributive lattice $\mathrm{Up}(\mathrm{Prf}\,\mathbb{N}^\partial)$.

Example 2.43. We shall describe the embedding γ of Theorem 2.41 in the concreter case of the distributive lattices $\mathbb{N}^\partial$ and $\mathbb{N}^\partial \times \mathbb{N}^\partial$, depicted in Figure 2.1.

Following the notation of Example 2.32, for every $n \in \mathbb{N}$, we set

$$\ulcorner n \urcorner := \{[\![m]\!] : n \leqslant m \in \mathbb{N}\}.$$

Recall that the poset $\mathrm{Prf}\,\mathbb{N}^\partial$ is depicted in Figure 2.2. Accordingly, the upsets of $\mathrm{Prf}\,\mathbb{N}^\partial$ are the sets that are either empty or of the form $\ulcorner n \urcorner$ for some $n \in \mathbb{N}$. It follows that the distributive lattice $\mathrm{Up}(\mathrm{Prf}\,\mathbb{N}^\partial)$ is isomorphic to $\mathbb{N}^\partial$ with an additional minimum element (see Figure 2.3). Furthermore, $\gamma\colon \mathbb{N}^\partial \to \mathrm{Up}(\mathrm{Prf}\,\mathbb{N}^\partial)$ is the embedding defined by the rule

$$n \longmapsto \ulcorner n \urcorner, \text{ for all } n \in \mathbb{N}.$$

In order to describe the embedding γ in the case of $\mathbb{N}^\partial \times \mathbb{N}^\partial$, it is convenient to introduce the following notation. For every $n \in \mathbb{N}$, define

$$\ulcorner n \urcorner \otimes \mathbb{N} := \{[\![m]\!] \times \mathbb{N} : [\![m]\!] \in \ulcorner n \urcorner\}$$
$$\mathbb{N} \otimes \ulcorner n \urcorner := \{\mathbb{N} \times [\![m]\!] : [\![m]\!] \in \ulcorner n \urcorner\}.$$

Recall that the poset $\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial)$ is depicted in Figure 2.2. Accordingly, the upsets of $\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial)$ are the sets that are either empty or of the form

$$(\ulcorner n \urcorner \otimes \mathbb{N}) \cup (\mathbb{N} \otimes \ulcorner m \urcorner) \text{ or } \mathbb{N} \otimes \ulcorner n \urcorner \text{ or } \ulcorner n \urcorner \otimes \mathbb{N},$$

for some $n, m \in \mathbb{N}$. It follows that the distributive lattice $\mathrm{Up}(\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial))$ coincides with that depicted in Figure 2.4, whose meets are intersections. Lastly, $\gamma\colon \mathbb{N}^\partial \times \mathbb{N}^\partial \to \mathrm{Up}(\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial))$ is the embedding defined by the rule

$$\langle n, m \rangle \longmapsto (\ulcorner n \urcorner \otimes \mathbb{N}) \cup (\mathbb{N} \otimes \ulcorner m \urcorner), \text{ for all } n, m \in \mathbb{N}. \qquad \boxtimes$$

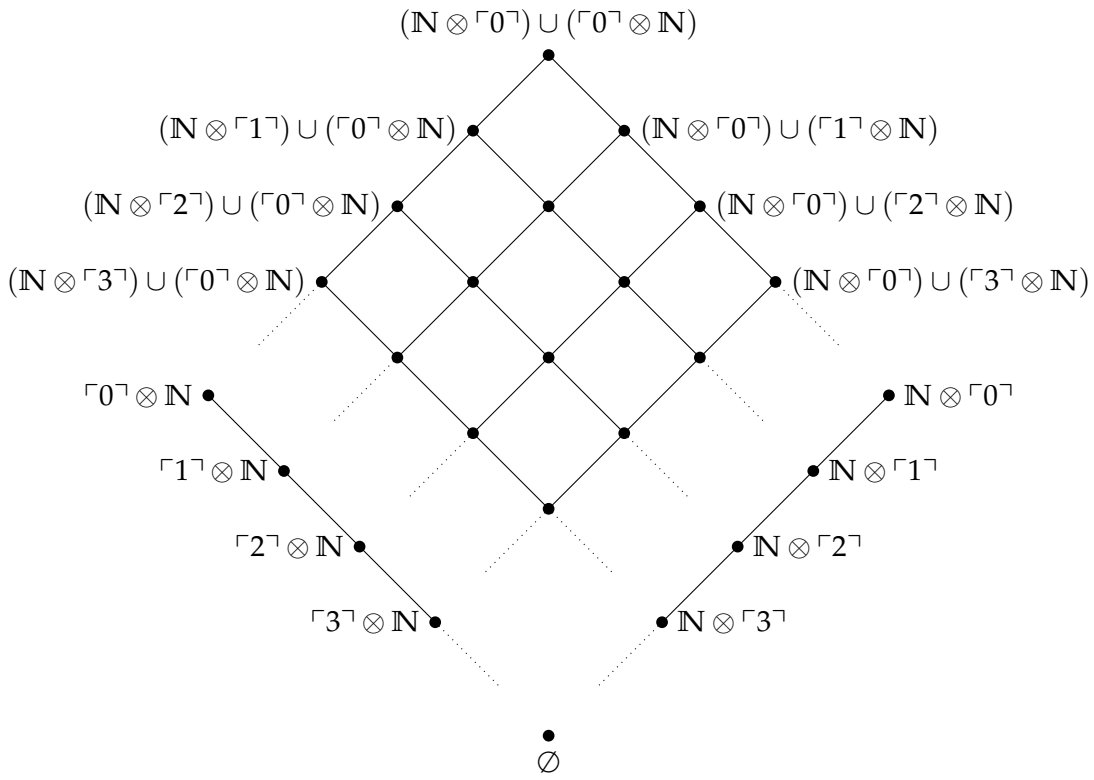


Figure 2.4: The distributive lattice $\mathrm{Up}(\mathrm{Prf}(\mathbb{N}^\partial \times \mathbb{N}^\partial))$.

Corollary 2.44. *Let $\boldsymbol{A}$ be a finite distributive lattice and $\mathbb{X}$ the poset of its join-irreducible elements. Then the map*

$$f \colon \boldsymbol{A} \to \mathrm{Dw}(\mathbb{X}),$$

defined for every $a \in A$ as

$$f(a) \coloneqq \{c \in \mathbb{X} : c \leqslant a\},$$

is an isomorphism.

Proof. Recall from Propositions 2.25 and Corollary 2.35 that the map $\delta \colon \mathbb{X}^\partial \to \mathrm{Prf}\boldsymbol{A}$, defined by the rule $\delta(a) \coloneqq {\uparrow}a$, is an isomorphism. Accordingly, the map $\delta^* \colon \mathrm{Dw}(\mathbb{X}) \to \mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$, defined by the rule

$$\delta^*(U) \coloneqq \{{\uparrow}a : a \in U\},$$

is an isomorphism.

Let γ be the map given by Theorem 2.41. Notice that, for every $a \in A$,

$$f(a) = \{c \in \mathbb{X} : c \leqslant a\} = \delta^{*-1}(\{F \in \mathrm{Prf}\boldsymbol{A} : a \in F\}) = \delta^{*-1} \circ \gamma(a).$$

Thus, $f = \delta^{*-1} \circ \gamma$. Since δ^{*-1} and γ are embeddings, we conclude that f is also an embedding. Therefore, it only remains to show that f is surjective.

To this end, consider a downset $U \in \mathrm{Dw}(\mathbb{X})$. If $U = \emptyset$, then $f(0) = U$, where 0 is the minimum of $\boldsymbol{A}$ (which exists, because $\boldsymbol{A}$ is finite). Then assume that $U \neq \emptyset$. Since $\boldsymbol{A}$ is finite, we can take an enumeration $U = \{a_1, \ldots, a_n\}$ and set

$$c \coloneqq a_1 \vee \cdots \vee a_n.$$

We shall prove that $f(c) = U$. Clearly, $U \subseteq f(c)$. On the other hand, consider an element $e \in f(c)$. We have $e \leqslant c = a_1 \vee \cdots \vee a_n$. Since $\boldsymbol{A}$ is distributive and e join-irreducible, e is also join-prime by Proposition 2.25. Consequently, from $e \leqslant a_1 \vee \cdots \vee a_n$ it follows that $e \leqslant a_i$ for some i. Since U is a downset and $a_i \in U$, we conclude that $e \in U$, as desired. Hence, f is surjective and, therefore, an isomorphism. ⊠

Corollary 2.45. *Up to isomorphism, the finite distributive lattices are precisely the lattices of the form* $\mathrm{Up}(\mathbb{X})$*, where* $\mathbb{X}$ *is a finite poset.*

Remark 2.46. While every finite distributive lattice has the form $\mathrm{Up}(\mathbb{X})$, for a finite poset $\mathbb{X}$, a similar result is not true for arbitrary infinite distributive lattices (because infinite distributive lattices need not be complete). To obtain a concrete description of arbitrary distributive lattices, one needs to add a missing ingredient in the representation of Theorem 2.41: a suitable topology on the poset $\mathbb{X}$, known as *Priestley topology*. The resulting correspondence between distributive lattices and suitable ordered spaces is known as *Priestley duality* [6, Chpt. 11]. ⊠

Birkhoff's Representation Theorem 2.41 can be given a more algebraic flavour, as we proceed to explain. In Section 1.1 we defined the *direct product* $\prod_{i \in I} \mathbb{X}_i$ of a family $\{\mathbb{X}_i : i \in I\}$ of posets. Notice that if each $\mathbb{X}_i$ is a lattice, then $\prod_{i \in I} \mathbb{X}_i$ is also a lattice, whose operations are defined component-wise. Furthermore, if I is empty, then $\prod_{i \in I} \mathbb{X}$ is the trivial lattice. When there exists a poset $\mathbb{X}$ such that $\mathbb{X} = \mathbb{X}_i$ for all $i \in I$, then $\prod_{i \in I} \mathbb{X}_i$ is called a *direct power* of $\mathbb{X}$.

Theorem 2.47. *Every distributive lattice embeds into a direct power of the two-element chain.*

Proof. Let $\boldsymbol{C}$ be the two-element chain with universe $\{0, 1\}$ such that $0 < 1$ and $\boldsymbol{A}$ an arbitrary distributive lattice.

If $\boldsymbol{A}$ is trivial, then $\mathrm{Prf}\boldsymbol{A}$ is empty and, therefore, the direct power $\prod_{\mathrm{Prf}A} \boldsymbol{C}_F$ is also trivial. Consequently, $\boldsymbol{A}$ and $\prod_{\mathrm{Prf}A} \boldsymbol{C}_F$ are isomorphic and we are done.

Then we consider the case where $\boldsymbol{A}$ is nontrivial. In view of Theorem 2.41, there exists an embedding

$$\gamma \colon \boldsymbol{A} \to \mathrm{Up}(\mathrm{Prf}\boldsymbol{A}).$$

Then consider the map

$$\delta \colon \mathrm{Up}(\mathrm{Prf}\boldsymbol{A}) \to \prod_{\mathrm{Prf}\boldsymbol{A}} \boldsymbol{C}_F,$$

defined for every $U \in \mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$ and $F \in \mathrm{Prf}\boldsymbol{A}$ as follows:

$$\delta(U)(F) \coloneqq \begin{cases} 1 & \text{if } F \in U \\ 0 & \text{if } F \notin U. \end{cases}$$

In view of Theorem 2.41, to conclude the proof, it suffices to show that δ is an embedding.

Clearly, δ is a well-defined injective map. To prove that δ is a homomorphism, we need to show that it preserves $\wedge$ and $\vee$. We detail the case of $\wedge$ only, as that of $\vee$ is similar. Consider $U, V \in \mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$. We need to show that

$$\delta(U \vee^{\mathrm{Up}(\mathrm{Prf}\boldsymbol{A})} V) = \delta(U) \vee^{\prod_{\mathrm{Prf}\boldsymbol{A}} \boldsymbol{C}_F} \delta(V).$$

This amounts to showing that for every $F \in \mathrm{Prf}\boldsymbol{A}$,

$$\delta(U \vee^{\mathrm{Up}(\mathrm{Prf}\boldsymbol{A})} V)(F) = (\delta(U) \vee^{\prod_{\mathrm{Prf}\boldsymbol{A}} \boldsymbol{C}_F} \delta(V))(F).$$

Since the join operation in $\mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$ is $\cup$ and the join operation in $\prod_{\mathrm{Prf}\boldsymbol{A}} \boldsymbol{C}_F$ is computed component-wise, this amounts to

$$\delta(U \cup V)(F) = \delta(V)(F) \vee^{\boldsymbol{C}} \delta(U)(F). \tag{2.8}$$

Notice that

$$\begin{aligned}\delta(U \cup V)(F) = 1 &\iff F \in U \cup V \iff \delta(U)(F) = 1 \text{ or } \delta(V)(F) = 1\\ &\iff \delta(V)(F) \vee^{\boldsymbol{C}} \delta(U)(F) = 1,\end{aligned}$$

where the last equivalence depends on the definition of the join operation in $\boldsymbol{C}$. Since $C = \{0, 1\}$, the above equivalences imply that (2.8) holds. Thus, δ preserves $\vee$, as desired. ⊠

Definition 2.48. Let K be a class of lattices. The *equational theory* K is the set of lattice equations valid in K.

Corollary 2.49. *A lattice equation is valid in the class of all distributive lattices if and only if it is valid in the two-element chain. Consequently, the equational theory of distributive lattices is decidable.*

Proof. Notice the validity of lattice equations persists under the formation of direct products, subalgebras, and isomorphic copies of lattices. Consequently, in view of Theorem 2.47, if a lattice equations holds in the two-element chain $\boldsymbol{C}$, it holds in all lattices. The converse implication is straightforward.

It only remains to show that the equational theory of distributive lattices is decidable. To this end, notice that, since $\boldsymbol{C}$ is finite and each lattice equation $\varphi \approx \psi$ involves only a finite number of variables, it is possible to check mechanically whether $\varphi \approx \psi$ holds in $\boldsymbol{C}$ and, therefore, whether it belongs to the equational theory of distributive lattices. ⊠

Remark 2.50. In constrast with the case of distributive lattices (Corollary 2.49), Freese showed that the theory of modular lattices is undecidable [9]. It is therefore natural to wonder whether the equational theory of the class of all lattices is decidable. This is indeed the case, as we will see at the end of this course. ⊠

*Exercise** 2.51. This exercise guides you through a description of prime filters of direct products of finitely many lattices. More precisely, you shall prove that, for every finite set of (possibly infinite) lattices $\{\boldsymbol{A}_1, \dots, \boldsymbol{A}_n\}$, the poset of prime filters of $\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n$ is isomorphic to the disjoint union $\mathrm{Prf}\boldsymbol{A}_1 \uplus \cdots \uplus \mathrm{Prf}\boldsymbol{A}_n$.

To this end, consider the map

$$\sigma\colon (\mathrm{Prf}\boldsymbol{A}_1 \uplus \cdots \uplus \mathrm{Prf}\boldsymbol{A}_n) \to \mathrm{Prf}(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n),$$

defined for every $F \in \mathrm{Prf}\boldsymbol{A}_i$ as

$$\sigma(F) := \{\vec{a} \in A_1 \times \cdots \times A_n : \vec{a}(i) \in F\}.$$

Prove that:

(i) σ is well-defined, i.e., $\sigma(F) \in \mathrm{Prf}(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n)$ for all $i \in I$ and $F \in \mathrm{Prf}\boldsymbol{A}_i$;

(ii) σ is an order embedding.

To prove that σ is surjective, consider $F \in \mathrm{Prf}(\boldsymbol{A}_1 \times \cdots \times \boldsymbol{A}_n)$. Since F is nonempty choose $\vec{a} \in F$ and let $\vec{a} = \langle a_1, \ldots, a_n \rangle$.

(iii) Prove that there exists $i \leqslant n$ such that

$$\langle c_1, \ldots, c_{i-1}, a_i, c_{i+1}, \ldots, c_n \rangle \in F, \text{ for every } c_1 \in A_1, \ldots, c_n \in A_n. \tag{2.9}$$

Hint: suppose the contrary and use the fact that F is prime and $\vec{a} \in F$ to derive a contradiction.

Define

$$F_i := \{c \in A_i : \text{there is } \vec{c} \in F \text{ such that } \vec{c}(i) = c\}.$$

(iv) Prove that F_i is a prime filter of $\boldsymbol{A}_i$ (use the fact that F is prime). Hint: to prove that F_i is proper, suppose the contrary, with a view to contradiction. Then use the fact that F is a proper filter and condition (2.9), to derive a contradiction.

(v) Show that $\sigma(F_i) = F$. To prove the inclusion $\sigma(F_i) \subseteq F$, you will need to use condition (2.9) and $\vec{a} \in F$ again.

Conclude that σ is surjective and, therefore, an isomorphism. ⊠

Exercise 2.52. The isomorphism described in the above exercise does not extend to direct products of infinitely many (distributive) lattices. To prove this, consider an infinite family $\{\boldsymbol{A}_i : i \in I\}$ of nontrivial distributive lattices. By the Prime Filter Theorem 2.37, for every $i \in I$, there exists a prime filter F_i on $\boldsymbol{A}_i$. Consider the set

$$F := \{\vec{a} \in \prod_{i \in I} A_i : \{i \in I : \vec{a}(i) \notin F_i\} \text{ is finite}\}.$$

Prove that F is a nonempty proper filter of $\prod_{i \in I} \boldsymbol{A}_i$. Use the Prime Filter Theorem 2.37 to extend F to a prime filter G of $\prod_{i \in I} \boldsymbol{A}_i$. Then prove that G is not of the form $\sigma(H)$ for any $H \in \bigcup_{i \in I} \mathrm{Prf}\boldsymbol{A}_i$. ⊠

2.5 Congruences

Definition 2.53. Let $\boldsymbol{A}$ be a lattice. An equivalence relation θ on A is said to be a *congruence* of $\boldsymbol{A}$ if for every $a_1, a_2, c_1, c_2 \in A$,

$$\text{if } \langle a_1, a_2 \rangle, \langle c_1, c_2 \rangle \in \theta, \text{ then } \langle a_1 \wedge c_1, a_2 \wedge c_2 \rangle, \langle a_1 \vee c_1, a_2 \vee c_2 \rangle \in \theta.$$

We denote by $\mathrm{Con}\boldsymbol{A}$ the poset of congruences of $\boldsymbol{A}$ ordered under the inclusion relation. Furthermore, given $\theta \in \mathrm{Con}\boldsymbol{A}$ and $a, c \in A$, sometimes we write $a \equiv_\theta c$ as a shorthand for $\langle a, c \rangle \in \theta$.

Given a congruence θ of a lattice $\boldsymbol{A}$, we endow the quotient set A/θ with the structure of a lattice $\boldsymbol{A}/\theta$, stipulating that for every $a, c \in A$,

$$a/\theta \wedge^{\boldsymbol{A}/\theta} c/\theta := (a \wedge^{\boldsymbol{A}} c)/\theta \text{ and } a/\theta \vee^{\boldsymbol{A}/\theta} c/\theta := (a \vee^{\boldsymbol{A}} c)/\theta.$$

Exercise 2.54. Prove that the above operations of $\boldsymbol{A}/\theta$ are well-defined and that $\boldsymbol{A}/\theta$ is still a lattice. ⊠

Let $\boldsymbol{A}$ be a lattice and θ a congruence on it. Notice that the natural projection on the quotient $\pi\colon \boldsymbol{A} \to \boldsymbol{A}/\theta$, i.e., the map that sends the element a to a/θ, is a surjective homomorphism. Furthermore, if $f\colon \boldsymbol{A} \to \boldsymbol{B}$ is a homomorphism, then the *kernel* of f, i.e., the relation

$$\mathrm{Ker}(f) := \{\langle a, c\rangle \in A \times A : f(a) = f(c)\},$$

is a congruence of $\boldsymbol{A}$. A lattice $\boldsymbol{B}$ is said to be a *homomorphic image* of $\boldsymbol{A}$ if there exists a surjective homomorphism $f\colon \boldsymbol{A} \to \boldsymbol{B}$.

Exercise 2.55. Prove that if $f\colon \boldsymbol{A} \to \boldsymbol{B}$ is a *surjective* homomorphism, then $\boldsymbol{A}/\mathrm{Ker}(f) \cong \boldsymbol{B}$. This result is a special instance of what is known in Universal Algebra as the *Fundamental Homomorphism Theorem* [2, Thm. 1.22]. ⊠

Proposition 2.56. *Let $\boldsymbol{A}$ be a lattice. The poset $\mathrm{Con}\boldsymbol{A}$ of congruences of $\boldsymbol{A}$ is an inductive closure system on $A \times A$ whose maximum and minimum are, respectively, the total relation $A \times A$ and the identity Id_A. Moreover, joins in $\mathrm{Con}\boldsymbol{A}$ can be described as follows: for every family $\{\theta_i : i \in I\} \subseteq \mathrm{Con}\boldsymbol{A}$ and $a, c \in A$,*

$$\langle a, c\rangle \in \bigvee_{i\in I} \theta_i \iff \text{either } a = c \text{ or there are } i_1, \dots, i_{n-1} \in I \text{ and } e_1, \dots, e_n \in A$$
$$\text{s.t. } e_1 = a, e_n = c, \text{ and } e_{i_k} \equiv_{\theta_{i_k}} e_{i_{k+1}}, \text{ for all } k < n.$$

Proof. The proof that $\mathrm{Con}\boldsymbol{A}$ is an inductive closure system with maximum $A \times A$ and minimum Id_A is left as an exercise. In order to describe joins in $\mathrm{Con}\boldsymbol{A}$, we reason as follows. First, if $I = \emptyset$, then $\bigvee_{i\in I} \theta_i = \bigvee \emptyset$ is the minimum of $\mathrm{Con}\boldsymbol{A}$, namely the identity relation Id_A and we are done. Then we consider the case where $I \neq \emptyset$. Define

$$R := \{\langle b, d\rangle \in A \times A : \text{there are } i_1, \dots, i_{n-1} \in I \text{ and } e_1, \dots, e_n \in A \text{ such that}$$
$$e_1 = a, e_n = c, \text{ and } e_{i_k} \equiv_{\theta_{i_k}} e_{i_{k+1}} \text{ for all } k < n\}.$$

To conclude the proof, it suffices to prove that

$$R = \bigvee_{i\in I} \theta. \tag{2.10}$$

Notice that, since each θ_i is an equivalence relation on A, so is R. Therefore, in order to prove that R is a congruence of $\boldsymbol{A}$, it only remains to show that R preserves the operations $\vee$ and $\wedge$ of $\boldsymbol{A}$.

We detail the case of $\wedge$, as the case of $\vee$ is analogous. Suppose that $\langle a_1, a_2\rangle, \langle c_1, c_2\rangle \in R$. Since $\langle a_1, a_2\rangle \in R$ there are $1 \leqslant n \in \omega$, $i_1, \dots, i_{n-1} \in I$ and $e_1, \dots, e_n \in A$ such that

$$e_1 = a_1, e_n = a_2, \text{ and } e_{i_k} \equiv_{\theta_{i_k}} e_{i_{k+1}}, \text{ for every } k < n.$$

Similarly, since $\langle c_1, c_2\rangle \in R$ there are $1 \leqslant m \in \omega$, $j_1, \dots, j_{m-1} \in I$ and $g_1, \dots, g_m \in A$ such that

$$g_1 = c_1, g_m = c_2, \text{ and } g_{j_k} \equiv_{\theta_{j_k}} g_{j_{k+1}}, \text{ for every } k < m.$$

We can assume, without loss of generality, that $m = n$. This is because if $n < m$, we can prolong the sequence $\theta_{i_1}, \dots, \theta_{i_n}$ with $m - n$ copies of θ_{i_n} and, similarly, prolong the sequence $e_1, \dots, e_n$ with $m - n$ copies of e_n (the case where $m < n$ is dual). Bearing this in mind, consider the following elements of A:

$$\begin{aligned} q_1 &\coloneqq e_1 \wedge g_1 \\ q_2 &\coloneqq e_2 \wedge g_1 \\ q_3 &\coloneqq e_2 \wedge g_2 \\ q_4 &\coloneqq e_3 \wedge g_2 \\ q_5 &\coloneqq e_3 \wedge g_3 \\ q_6 &\coloneqq e_4 \wedge g_3 \\ &\vdots \\ q_{2n-1} &\coloneqq e_n \wedge g_n. \end{aligned}$$

Moreover, consider the following congruences of $\boldsymbol{A}$:

$$\begin{aligned} \phi_1 &\coloneqq \theta_{i_1} \\ \phi_2 &\coloneqq \theta_{j_1} \\ \phi_3 &\coloneqq \theta_{i_2} \\ \phi_4 &\coloneqq \theta_{j_2} \\ &\vdots \\ \phi_{2n-2} &\coloneqq \theta_{j_{n-1}}. \end{aligned}$$

Lastly, set $a \coloneqq e_1 \wedge g_1$ and $c \coloneqq e_n \wedge g_n$.

Now, by assumption, $e_1 \equiv_{\phi_1} e_2$ and, by reflexivity, $g_1 \equiv_{\phi_1} g_1$. Since ϕ_1 is a congruence, this yields $e_1 \wedge g_1 \equiv_{\phi_1} e_2 \wedge g_1$, i.e., $q_1 \equiv_{\phi_1} q_2$. A similar argument shows that $e_2 \wedge g_1 \equiv_{\phi_2} e_2 \wedge g_2$, i.e., $q_2 \equiv_{\phi_2} q_3$. Indeed, iterating this process, we obtain

$$q_k \equiv_{\phi_k} q_{k+1}, \text{ for all } k \leqslant 2n - 2.$$

By the definition of R, this implies $\langle a, c \rangle \in R$, i.e., $\langle e_1 \wedge g_1, e_n \wedge g_n \rangle \in R$. Since, by assumption, $e_1 = a_1, e_2 = a_2, g_1 = c_1, g_2 = c_2$, we conclude $\langle a_1 \wedge c_1, a_2 \wedge c_2 \rangle \in R$ and, therefore, that R preserves $\wedge$. A similar argument shows that R preserves $\vee$, whence we conclude that R is a congruence of $\boldsymbol{A}$.

Now we turn to prove (2.10). First, it is clear that R extends all congruences in $\{\theta_i : i \in I\}$. Together with the fact that R is a congruence of $\boldsymbol{A}$, this yields

$$\bigvee_{i \in I} \theta_i \subseteq R.$$

Therefore, to establish (2.10), it suffices to prove that R is included into every upper bound ϕ of $\{\theta_i : i \in I\}$. To this end, take a pair $\langle a, c \rangle \in R$. Then there are $1 \leqslant n \in \omega$, $i_1, \dots, i_{n-1} \in I$ and $e_1, \dots, e_n \in A$ such that $e_1 = a, e_n = c$, and $e_{i_k} \equiv_{\theta_{i_k}} e_{i_{k+1}}$ for every $k < n$. Since ϕ is an upper bound of $\{\theta_i : i \in I\}$,

$$\langle e_1, e_2 \rangle, \langle e_2, e_3 \rangle, \dots, \langle e_{n-1}, e_n \rangle \in \phi.$$

By transitivity, this yields $e_1 \equiv_\phi e_n$, which, in turn, is $a \equiv_\phi c$. Thus, $R \subseteq \phi$, as desired. ⊠

Corollary 2.57. *Let $\boldsymbol{A}$ be a lattice, $\theta, \phi \in \mathrm{Con}\boldsymbol{A}$, and $a, c \in A$. Then $\langle a, c\rangle \in \theta \vee \phi$ if and only if there are an odd $1 \leqslant n \in \omega$ and $e_1, \ldots, e_n \in A$ such that $e_1 = a$, $e_n = c$, and*

$$e_1 \equiv_\theta e_2 \equiv_\phi e_3 \equiv_\theta e_4 \cdots \equiv_\phi e_n.$$

Proof. Immediate from Proposition 2.56 and the fact that congruences are reflexive and transitive. ⊠

Exercise 2.58. Complete the proof of Proposition 2.56 by proving that if $\boldsymbol{A}$ is a lattice, $\mathrm{Con}\boldsymbol{A}$ is an inductive closure system on $A \times A$ with maximum $A \times A$ and minimum Id_A. ⊠

Given a lattice $\boldsymbol{A}$, we denote the finitary closure operator associated with the inductive closure system $\mathrm{Con}\boldsymbol{A}$ as follows:

$$\mathrm{Cg}^{\boldsymbol{A}} \colon \mathcal{P}(A \times A) \to \mathcal{P}(A \times A).$$

A congruence θ of $\boldsymbol{A}$ is then said to be *principal* if there are $a, c \in A$ such that $\theta = \mathrm{Cg}^{\boldsymbol{A}}(\{\langle a, c\rangle\})$. Sometimes we write $\mathrm{Cg}^{\boldsymbol{A}}(a, c)$ as a shorthand for $\mathrm{Cg}^{\boldsymbol{A}}(\{\langle a, c\rangle\})$.

Exercise 2.59. Describe principal congruences in distributive lattices. More precisely, prove that for every distributive lattice $\boldsymbol{A}$ and $a, b, c, d \in A$,

$$\langle c, d\rangle \in \mathrm{Cg}^{\boldsymbol{A}}(a, b) \iff a \wedge b \wedge c = a \wedge b \wedge d \text{ and } a \vee b \vee c = a \vee b \vee d.$$

Notice that the above equivalence provide a description of the principal congruence $\mathrm{Cg}^{\boldsymbol{A}}(a, b)$ in terms of equations relating the elements a, b, c, d. A result by McKenzie states that a similar description of principal congruences for arbitrary lattices is impossible. More precisely, the only nontrivial equational class of lattices in which principal congruences can be described by a first-order formula is that of distributive lattices [13]. ⊠

Theorem 2.60 (Funayama & Nakayama)**.** *If $\boldsymbol{A}$ is a lattice, then the lattice* $\mathrm{Con}\boldsymbol{A}$ *is distributive.*

Proof. Consider the lattice term

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

It is easy to see that for every $a, c \in A$, we have

$$m^{\boldsymbol{A}}(a, a, c) = m^{\boldsymbol{A}}(a, c, a) = m^{\boldsymbol{A}}(c, a, a) = a. \tag{2.11}$$

Since the operation $m^{\boldsymbol{A}}(x, y, z)$ is defined as a combination of the basic operations $\wedge$ and $\vee$ of $\boldsymbol{A}$, it is preserved by congruences of $\boldsymbol{A}$.

In view of Exercise 2.15, in order to prove that $\mathrm{Con}\boldsymbol{A}$ is distributive, it suffices to show that for every $\theta, \phi, \eta \in \mathrm{Con}\boldsymbol{A}$,

$$\theta \cap (\phi \vee \eta) \subseteq (\theta \cap \phi) \vee (\theta \cap \eta). \tag{2.12}$$

To this end, take a pair $\langle a, c\rangle \in \theta \cap (\phi \vee \eta)$. This, $\langle a, c\rangle \in \theta$ and $\langle a, c\rangle \in \phi \vee \eta$. By Corollary 2.57 there are an odd $1 \leqslant n \in \omega$ and $e_1, \ldots, e_n \in A$ such that $e_1 = a$, $e_n = c$, and

$$e_1 \equiv_\phi e_2 \equiv_\eta e_3 \equiv_\phi e_4 \cdots \equiv_\eta e_n.$$

Consider the following sequence $g_1, \ldots, g_n$ of elements of $\boldsymbol{A}$:

$$m^{\boldsymbol{A}}(a,c,e_1), m^{\boldsymbol{A}}(a,c,e_2), \ldots, m^{\boldsymbol{A}}(a,c,e_n).$$

Notice that since $\langle a,c\rangle \in \theta$ and θ preserves $m^{\boldsymbol{A}}$, we get

$$\langle m^{\boldsymbol{A}}(a,a,e_1), m^{\boldsymbol{A}}(a,c,e_1)\rangle, \langle m^{\boldsymbol{A}}(a,a,e_2), m^{\boldsymbol{A}}(a,c,e_2)\rangle \in \theta.$$

Together with (2.11), this yields $\langle a, m^{\boldsymbol{A}}(a,c,e_1)\rangle, \langle a, m^{\boldsymbol{A}}(a,c,e_2)\rangle \in \theta$. As θ is an equivalence relation, we conclude that $\langle m^{\boldsymbol{A}}(a,c,e_1), m^{\boldsymbol{A}}(a,c,e_2)\rangle \in \theta$. Moreover, since $\langle e_1,e_2\rangle \in \phi$ and ϕ preserves the operation $m^{\boldsymbol{A}}(x,y,z)$, we obtain that also $\langle m^{\boldsymbol{A}}(a,c,e_1), m^{\boldsymbol{A}}(a,c,e_2)\rangle \in \phi$. Hence, $\langle m^{\boldsymbol{A}}(a,c,e_1), m^{\boldsymbol{A}}(a,c,e_2)\rangle \in \theta \cap \phi$, that is $\langle g_1, g_2\rangle \in \theta \cap \phi$. A similar argument shows that $\langle g_2, g_3\rangle \in \theta \cap \eta$. Iterating this process we get

$$g_1 \equiv_{\theta\cap\phi} g_2 \equiv_{\theta\cap\eta} g_3 \equiv_{\theta\cap\phi} g_4 \cdots \equiv_{\theta\cap\eta} g_n.$$

By transitivity of $(\theta \cap \phi) \vee (\theta \cap \eta)$, we conclude that

$$\langle g_1, g_n\rangle \in (\theta \cap \phi) \vee (\theta \cap \eta). \tag{2.13}$$

Now, recall that $g_1 = m^{\boldsymbol{A}}(a,c,e_1)$ and $g_n = m^{\boldsymbol{A}}(a,c,e_n)$ and that $e_1 = a$ and $e_n = c$. Thus,

$$g_1 = m^{\boldsymbol{A}}(a,c,a) \text{ and } g_n = m^{\boldsymbol{A}}(a,c,c).$$

By (2.11), we conclude that $g_1 = a$ and $g_n = c$. Hence, by (2.13), we get $\langle a,c\rangle \in (\theta \cap \phi) \vee (\theta \cap \eta)$, thus establishing (2.12). ⊠

Remark 2.61. The proof of Theorem 2.60 depends only on the properties of the operation $m(x,y,z)$ in (2.11). A classical result of Jónsson in Universal Algebra states that an equational class K of algebras (not necessarily lattices) is such that the congruence lattices of its members are distributive if and only if there exist terms that, when interpreted in K, generalize the behaviour of $m(x,y,z)$ [2, Thm. 4.66]. ⊠

2.6 Subdirect representation

Observe that, given a homomorphism $f\colon \boldsymbol{A} \to \boldsymbol{B}$ between two lattices $\boldsymbol{A}$ and $\boldsymbol{B}$, the image $f[A]$ is the universe of a sublattice of $\boldsymbol{B}$. We denote this sublattice by $f[\boldsymbol{A}]$.

Definition 2.62. Let $\boldsymbol{A} \cup \{\boldsymbol{A}_i : i \in I\}$ be a family of lattices.

(i) $\boldsymbol{A}$ is said to be a *subdirect product* of $\{\boldsymbol{A}_i : i \in I\}$ if $\boldsymbol{A} \leqslant \prod_{i\in I} \boldsymbol{A}_i$ and the canonical projection $\pi_j\colon \prod_{i\in I} \boldsymbol{A}_i \to \boldsymbol{A}_j$ is surjective, for every $j \in J$.

(ii) An embedding $f\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{A}_i$ is said to be *subdirect* if the image $f[\boldsymbol{A}]$ is a subdirect product of $\{\boldsymbol{A}_i : i \in I\}$.

(iii) $\boldsymbol{A}$ is said to be *subdirectly irreducible* if for every subdirect embedding $f\colon \boldsymbol{A} \to \prod_{j\in J} \boldsymbol{B}_j$ there is $j \in J$ such that the composition $\pi_j \circ f\colon \boldsymbol{A} \to \boldsymbol{B}_j$ is an isomorphism.

We shall illustrate these definitions in the case of distributive lattices:

Theorem 2.63. *The following conditions hold:*

(i) *Every distributive lattice is isomorphic to a subdirect product of two-element chains.*

(ii) *A distributive lattice is subdirectly irreducible if and only if it is a two-element chain.*

In particular, every distributive lattice is isomorphic to a subdirect product of subdirectly irreducible distributive lattices.

Proof. (i): Recall from 2.47 that every distributive lattice $\boldsymbol{A}$ embeds into a direct power of the two-element chain $\boldsymbol{C}$. This embedding is given by the map

$$f\colon \boldsymbol{A} \to \prod_{F \in \mathrm{Prf}\boldsymbol{A}} \boldsymbol{C}_F,$$

defined for every $a \in A$ and $F \in \mathrm{Prf}\boldsymbol{A}$ as follows:

$$f(a)(F) \coloneqq \begin{cases} 1 & \text{if } a \in F \\ 0 & \text{if } a \notin F. \end{cases}$$

We shall prove that f is a subdirect embedding. To this end, it only remains to show that the canonical projection $\pi_F \circ f\colon \boldsymbol{A} \to \boldsymbol{C}$ is surjective, for every $F \in \mathrm{Prf}\boldsymbol{A}$. To this end, consider $F \in \mathrm{Prf}\boldsymbol{A}$. Since F is proper and nonempty, there are $a \in F$ and $c \in A \setminus F$. We have $\pi_F \circ f(a) = 1$ and $\pi_F \circ f(c) = 0$, whence $\pi_F \circ f$ is surjective.

We conclude that every distributive lattice $\boldsymbol{A}$ is isomorphic to a subdirect product of the two-element chain $\boldsymbol{C}$.

(ii): From (i) it follows that no distributive lattice, except from two-element chains, is subdirectly irreducible. Therefore, it only remains to prove that the two-element chain $\boldsymbol{C}$ is subdirectly irreducible. Suppose the contrary, with a view to contradiction. Then there is a subdirect embedding $f\colon \boldsymbol{C} \to \prod_{i \in I} \boldsymbol{B}_i$ such that $\pi_i \circ f\colon \boldsymbol{C} \to \boldsymbol{B}_i$ is noninjective for every $i \in I$. Notice that the only congruences of $\boldsymbol{C}$ are Id_C and $C \times C$. Then consider an arbitrary $i \in I$. Observe that $\pi_i \circ f$ is injective if and only if $\mathrm{Ker}(\pi_i \circ f) = \mathrm{Id}_C$. As a consequence, $\mathrm{Ker}(\pi_i \circ f) \neq \mathrm{Id}_C$, whence $\mathrm{Ker}(\pi_i \circ f) = C \times C$. It follows that $\boldsymbol{B}_i$ is a one-element lattice, that is, trivial. But then also $\prod_{i \in I} \boldsymbol{B}_i$ is trivial. This contradicts the fact that $\boldsymbol{C}$ embeds into $\prod_{i \in I} \boldsymbol{B}_i$. ⊠

In this section we shall generalize the above theorem by proving that every lattice is isomorphic to a subdirect product of a family of subdirectly irreducible lattices (Theorem 2.71). To this end, we rely on the following observations:

Proposition 2.64. *Let $\boldsymbol{A}$ be a lattice and $\{\theta_i : i \in I\} \subseteq \mathrm{Con}\boldsymbol{A}$ such that*

$$\bigcap_{i \in I} \theta_i = \mathrm{Id}_A.$$

Then the map

$$f\colon \boldsymbol{A} \to \prod_{i \in I} \boldsymbol{A}/\theta_i,$$

defined for every $a \in A$ and $i \in I$ as

$$f(a)(i) \coloneqq a/\theta_i,$$

is a subdirect embedding.

Proof. Notice that f is injective, since $\bigcap_{i\in I}\theta_i = \mathrm{Id}_A$. Moreover, by the definition of f, the composition $\pi_i \circ f\colon \boldsymbol{A} \to \boldsymbol{A}/\theta_i$ is surjective, for every $i \in I$. It only remains to prove that f is a homomorphism. To this end, consider $a, c \in A$ and $i \in I$. We have

$$f(a \wedge^{\boldsymbol{A}} c)(i) = (a \wedge^{\boldsymbol{A}} c)/\theta_i = a/\theta_i \wedge^{\boldsymbol{A}/\theta_i} c/\theta_i = f(a)(i) \wedge^{\boldsymbol{A}/\theta_i} f(c)(i).$$

Thus, f preserves $\wedge$. Similarly, it preserves $\vee$. ⊠

Proposition 2.65. *Let $\boldsymbol{A} \cup \{\boldsymbol{A}_i : i \in I\}$ be a family of lattices and*

$$f\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{A}_i$$

an embedding. Then

$$\bigcap_{i\in I} \mathrm{Ker}(\pi_i \circ f) = \mathrm{Id}_A.$$

Proof. It suffices to prove $\bigcap_{i\in I}\mathrm{Ker}(\pi_i \circ f) \subseteq \mathrm{Id}_A$. To this end, consider two distinct $a, c \in A$. Since f is an embedding, $f(a) \neq f(c)$. Consequently, there is some $i \in I$ such that $f(a)(i) \neq f(c)(i)$, that is $\langle a, c\rangle \notin \mathrm{Ker}(\pi_i \circ f)$. ⊠

As a consequence, we obtain the following description of subdirectly irreducible lattices:

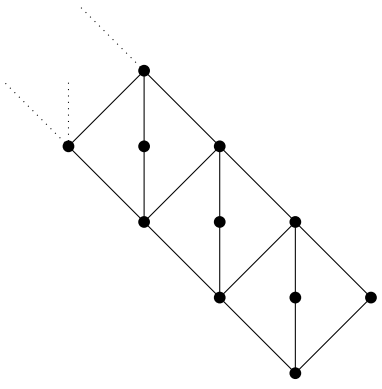
Corollary 2.66. *A lattice $\boldsymbol{A}$ is subdirectly irreducible if and only if the identity relation Id_A is completely meet-irreducible in the lattice $\mathrm{Con}\boldsymbol{A}$.*

Proof. From Proposition 2.64 it follows that if Id_A is not completely meet-irreducible in $\mathrm{Con}\boldsymbol{A}$, then $\boldsymbol{A}$ is not subdirectly irreducible. Then suppose that Id_A is completely meet-irreducible in $\mathrm{Con}\boldsymbol{A}$ and consider a subdirect embedding $f\colon \boldsymbol{A} \to \prod_{i\in I}\boldsymbol{A}_i$. By Proposition 2.65 we obtain that $\bigcap_{i\in I}\mathrm{Ker}(\pi_i \circ f) = \mathrm{Id}_A$. Since Id_A is completely meet-irreducible, there is $i \in I$ such that $\mathrm{Id}_A = \mathrm{Ker}(\pi_i \circ f)$. In particular, this implies that the composition $\pi_i \circ f\colon \boldsymbol{A} \to \boldsymbol{A}_i$ is injective. Since f is a subdirect embedding, this implies that $\pi_i \circ f$ is an isomorphism. Hence, we conclude that $\boldsymbol{A}$ is subdirectly irreducible. ⊠

Definition 2.67. A lattice $\boldsymbol{A}$ is called *simple* when $\mathrm{Con}\boldsymbol{A}$ is a two-element set.

In view of Corollary 2.66, every simple lattice is subdirectly irreducible.

Exercise 2.68. Prove that the modular diamond $\boldsymbol{M}_3$ and the two-element chain $\boldsymbol{C}$ are simple and, therefore, subdirectly irreducible. Then use Corollary 2.66 to show that the nonmodular pentagon $\boldsymbol{N}_5$ is subdirectly irreducible, but not simple. Lastly, let $\boldsymbol{M}_\infty$ be the infinite lattice depicted below:



Use the fact that $\boldsymbol{M}_3$ is simple to prove that $\boldsymbol{M}_\infty$ is also simple. ⊠

We shall also rely on the following observation:

Proposition 2.69. *If $\boldsymbol{A}$ is a lattice and $\theta \in \mathrm{Con}\boldsymbol{A}$, then the lattice $\mathrm{Con}(\boldsymbol{A}/\theta)$ is isomorphic to the upset $\uparrow\theta$ of $\mathrm{Con}\boldsymbol{A}$ via the map*

$$\gamma\colon \uparrow\theta \to \mathrm{Con}(\boldsymbol{A}/\theta),$$

defined for every $\phi \in \uparrow\theta$ by the rule

$$\gamma(\phi) := \{\langle a/\theta, c/\theta\rangle \in A/\theta \times A/\theta : \langle a, c\rangle \in \phi\}.$$

Exercise 2.70. Prove the above statement, which is a special instance of what is known in Universal Algebra as the *Correspondence Theorem* [2, Thm. 3.6]. ⊠

We are now ready to prove the desired result:

Theorem 2.71 (Birkhoff)**.** *Every lattice is isomorphic to a subdirect product of a family of subdirectly irrecucible lattices.*

Proof. Consider an arbitrary lattice $\boldsymbol{A}$. By Propositions 1.60 and 2.56 the lattice $\mathrm{Con}\boldsymbol{A}$ is algebraic. Thus, by Theorem 1.65, the identity relation Id_A is the meet of a family of completely meet-irreducible congruences $\{\theta_i : i \in I\} \subseteq \mathrm{Con}\boldsymbol{A}$, i.e.,

$$\mathrm{Id}_A = \bigcap_{i\in I} \theta_i.$$

By Proposition 2.64, this implies that there is a subdirect embedding

$$f\colon \boldsymbol{A} \to \prod_{i\in I} \boldsymbol{A}/\theta_i.$$

Thus, $\boldsymbol{A}$ is isomorphic to a subdirect product of the family $\{\boldsymbol{A}/\theta_i : i \in I\}$.

To conclude the proof, it only remains to prove that each $\boldsymbol{A}/\theta_i$ is subdirectly irreducible. To this end, consider an arbitrary $i \in I$. Since θ_i is completely meet-irreducible in $\mathrm{Con}\boldsymbol{A}$, using Proposition 2.69, we conclude that the identity relation Id_{A/θ_i} is completely meet-irreducible in $\mathrm{Con}(\boldsymbol{A}/\theta_i)$. By Corollary 2.66, we conclude that $\boldsymbol{A}/\theta_i$ is subdirectly irreducible. ⊠

CHAPTER 3

Boolean algebras

3.1 Complemented lattices

Recall that the minimum and the maximum of a bounded lattice $\boldsymbol{A}$ are denoted, respectively, by 0 and 1.

Definition 3.1. Let $\boldsymbol{A}$ be a bounded lattice. An element $a \in A$ is said to be *complemented* if there is some $a^* \in A$ such that

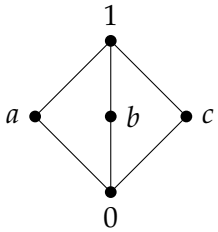
$$a \wedge a^* = 0 \text{ and } a \vee a^* = 1.$$

In this case, a^* is said to be a *complement* of a. Accordingly, $\boldsymbol{A}$ is said to be *complemented* if each of its elements has a complement.

Notice that, in a bounded lattice $\boldsymbol{A}$, the minimum 0 is always a complement of the maximum 1 (and vice-versa), whence 0 and 1 are always complemented. Moreover, if a^* is a complement of a in $\boldsymbol{A}$, then a is a complement of a^* in $\boldsymbol{A}$.

Exercise 3.2. Prove that a bounded nonempty chain is complemented if and only if it has at most two elements. ⊠

Complements need not be unique in general. For instance, in the diamond $\boldsymbol{M}_3$, the element a has two complements, namely b and c.



This contrasts with the case of distributive lattices in which complements are unique (when existing):

Theorem 3.3. *In a bounded distributive lattice, every element has at most one complement.*

Proof. Consider a bounded distributive lattice $\boldsymbol{A}$ and elements $a, b, c \in A$ such that b and c are complements of a. We have

$$c = c \vee 0 = c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b) = 1 \wedge (c \vee b) = c \vee b.$$

The above equalities are justified as follows. The first follows from the fact that 0 is the minimum, the second from the fact that b is a complement of a, the third from distributivity, the fourth from the fact that c is a complement of a, and the last one from the fact that 1 is the maximum.

From the above display it follows that $b \leqslant c$. A similar argument shows that $c \leqslant b$. By antisymmetry, we conclude that $b = c$. ⊠

Definition 3.4. A lattice $\boldsymbol{A}$ is said to be *Boolean* if it is bounded, distributive, and complemented.

In view of Theorem 3.3, complements in a Boolean lattice $\boldsymbol{A}$ are unique, whence we denote by

$$(\cdot)^* \colon A \to A$$

the operation that associates every $a \in A$ with its unique complement a^*.

Proposition 3.5. *Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be a Boolean lattices and $f \colon \boldsymbol{A} \to \boldsymbol{B}$ a lattice homomorphism. If $f(0^{\boldsymbol{A}}) = 0^{\boldsymbol{B}}$ and $f(1^{\boldsymbol{A}}) = 1^{\boldsymbol{B}}$, then $f(a^*) = f(a)^*$, for every $a \in A$.*

Proof. Consider $a \in A$. Since f preserves meets, joins, and the bounds, and since a^* is a complement of a in $\boldsymbol{A}$, we get

$$\begin{aligned} 0^{\boldsymbol{B}} &= f(0^{\boldsymbol{A}}) = f(a \wedge^{\boldsymbol{A}} a^*) = f(a) \wedge^{\boldsymbol{B}} f(a^*) \\ 1^{\boldsymbol{B}} &= f(1^{\boldsymbol{A}}) = f(a \vee^{\boldsymbol{A}} a^*) = f(a) \vee^{\boldsymbol{B}} f(a^*). \end{aligned}$$

Thus, $f(a^*)$ is a complement of $f(a)$ in $\boldsymbol{B}$. Since complements in $\boldsymbol{B}$ are unique, we conclude $f(a^*) = f(a)^*$. ⊠

3.2 Boolean algebras

Definition 3.6. A *Boolean algebra* is a structure $\boldsymbol{A} = \langle A; \wedge, \vee, {}^*, 0, 1\rangle$ such that $\langle A; \wedge, \vee, 0, 1\rangle$ is a Boolean lattice, whose complement operation is *.

Example 3.7. The most prototypical example of a Boolean algebra is the *powerset Boolean algebra*. More precisely, let X be a set. The structure

$$\langle \mathcal{P}(X); \cap, \cup, -, \emptyset, X\rangle,$$

where $-$ is set-theoretic complementation relative to X, is a complete Boolean algebra. The powerset Boolean algebras of sets of cardinality $\leqslant 4$ are depicted in Figure 3.1.

In view of Exercises 3.2, nontrivial Boolean algebras $\boldsymbol{A}$ whose underlying lattice is a chain have exactly two elements, namely the minimum 0 and the maximum 1. Thus, up to isomorphism, the only nontrivial Boolean chain is the two-element chain with universe $\{0, 1\}$ such that $0 < 1$, $0^* = 1$, and $1^* = 0$. We denote this algebra by $\boldsymbol{B}_2$. Notice that $\boldsymbol{B}_2$ is isomorphic to the powerset Boolean algebra of the empty set.

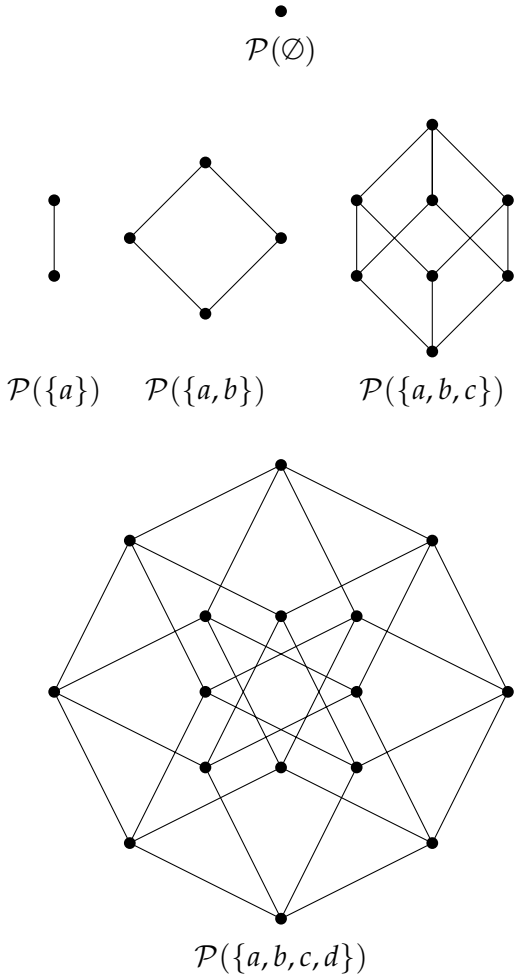


Figure 3.1: Powerset Boolean algebras $\mathcal{P}(X)$ such that $|X| \leqslant 4$.

A more exotic kind of Boolean algebras can be constructed as follows. A set $Y \subseteq X$ is called *cofinite* (relative to X) if $X \smallsetminus Y$ is finite. Define

$$\mathcal{FC}(X) \coloneqq \{Y \subseteq X : Y \text{ is either finite or cofinite}\}.$$

Then the structure

$$\langle \mathcal{FC}(X); \cap, \cup, -, \emptyset, X \rangle$$

is a also a Boolean algebra. We call it the *finite cofinite Boolean algebra*. Notice that $\mathcal{P}(X) = \mathcal{FC}(X)$ if and only if X is finite. ⊠

Boolean algebras can be axiomatized by equations, as we proceed to explain. The set of *Boolean terms* over *Var* is the smallest set T such that

(i) $Var \cup \{0, 1\} \subseteq T$; and

(ii) if $\varphi, \psi \in T$, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi^* \in T$.

Given a Boolean term φ, we write $\varphi(x_1, \dots, x_n)$ to denote the fact that the variables occurring in φ are among $x_1, \dots, x_n$. A *Boolean equation* is an expression of the form $\varphi \approx \psi$, where φ and ψ are Boolean terms.

Now, let $\boldsymbol{A} = \langle A; \wedge, \vee, ^*, 0, 1\rangle$ be a structure where A is a nonempty set, $\wedge$ and $\vee$ are binary functions on A, * is a unary function on A, and $0, 1 \in A$. A Boolean equation $\varphi \approx \psi$ is *valid* in $\boldsymbol{A}$ if $\varphi^{\boldsymbol{A}}(a_1, \dots, a_n) = \psi^{\boldsymbol{A}}(a_1, \dots, a_n)$ for every $a_1, \dots, a_n \in A$, where the elements $\varphi^{\boldsymbol{A}}(a_1, \dots, a_n), \psi^{\boldsymbol{A}}(a_1, \dots, a_n) \in A$ are defined by recursion on the construction of the Boolean terms φ and ψ in the natural way. In this case, $\boldsymbol{A}$ is said to be a *model* of the equation $\varphi \approx \psi$. Bearing this in mind, we are ready to give an equational definition of Boolean algebras.

Definition 3.8. A *Boolean algebra* is a structure $\boldsymbol{A} = \langle A; \wedge, \vee, ^*, 0, 1\rangle$, where A is a nonempty set, $\wedge$ and $\vee$ are binary functions on A, * is a unary function on A, and $0, 1 \in A$, such that the following equations are valid in $\boldsymbol{A}$:

$$\begin{aligned}
x \wedge x &\approx x \quad x \wedge y \approx y \wedge x \quad x \wedge (y \wedge z) \approx (x \wedge y) \wedge z\\
x \vee x &\approx x \quad x \vee y \approx y \vee x \quad x \vee (y \vee z) \approx (x \vee y) \vee z\\
x \wedge (y \vee x) &\approx x \qquad x \vee (y \wedge x) \approx x\\
x \wedge (y \vee z) &\approx (x \wedge y) \vee (x \wedge z)\\
x \wedge 0 &\approx 0 \qquad\qquad x \vee 1 \approx 1\\
x \wedge x^* &\approx 0 \qquad\qquad x \vee x^* \approx 1.
\end{aligned}$$

The first four lines of the above display state that $\langle A; \wedge, \vee\rangle$ is a distributive lattice, the fifth one that 0 is the minimum and 1 the maximum of $\langle A; \wedge, \vee\rangle$, and the last one that a^* is a complement of a, for every $a \in A$. Bearing this in mind, it should be clear that this equational definition of a Boolean algebra is equivalent to Definition 3.6.

The following properties of Boolean algebras have many applications in algebra and logic:

Proposition 3.9. *The following conditions hold for every Boolean algebra $\boldsymbol{A}$ and $a, c \in A$:*

(i) *Double negation elimination: $a^{**} = a$;*

(ii) *De Morgan laws: $a \vee c = (a^* \wedge c^*)^*$ and $a \wedge c = (a^* \vee c^*)^*$;*

(iii) *$a \leqslant c$ if and only if $c^* \leqslant a^*$;*

(iv) *a^* is the largest (resp. least) element $b \in A$ such that $a \wedge b = 0$ (resp. $a \vee b = 1$).*

Proof. (i): As a^* is a complement of a, then a is a complement of a^*. By the uniqueness of complements in Boolean algebras, this implies $a = a^{**}$.

(ii): We detail the proof of $(a \vee c)^* = a^* \wedge c^*$ only, as the other one is analogous. First, notice that $a^* \wedge c^*$ is a complement of $a \vee c$. This is because:

$$\begin{aligned}
(a^* \wedge c^*) \wedge (a \vee c) &= ((a^* \wedge c^*) \wedge a) \vee ((a^* \wedge c^*) \wedge c)\\
&= ((a^* \wedge a) \wedge c) \vee ((c^* \wedge c) \wedge a)\\
&= (0 \wedge c) \vee (0 \wedge a) = 0 \vee 0 = 0.
\end{aligned}$$

The first equality above follows from distributivity, the second from the commutativity and associativity of $\wedge$, the third from the fact that a^* and c^* are complements, respectively of a and c, the fourth from the fact that 0 is the minimum, and the last one from the idempotency of $\vee$.

Similarly, we obtain

$$\begin{aligned}(a \vee c) \vee (a^* \wedge c^*) &= ((a \vee c) \vee a^*) \wedge ((a \vee c) \vee c^*) \\ &= ((a \vee a^*) \vee a) \wedge ((c \vee c^*) \vee a) \\ &= (1 \vee a) \wedge (1 \vee a) = 1 \wedge 1 = 1.\end{aligned}$$

We conclude that

$$(a^* \wedge c^*) \wedge (a \vee c) = 0 \text{ and } (a^* \wedge c^*) \vee (a \vee c) = 1,$$

that is, $a \vee c$ is a complement of $a^* \wedge c^*$. By the uniqueness of complements in Boolean algebras, $(a^* \wedge c^*)^* = a \vee c$.

(iii): The following equivalences hold:

$$\begin{aligned}a \leqslant c &\iff a \vee c = c \\ &\iff (a^* \wedge c^*)^* = c \\ &\iff (a^* \wedge c^*)^{**} = c^* \\ &\iff a^* \wedge c^* = c^* \\ &\iff c^* \leqslant a^*.\end{aligned}$$

The above equivalences are justified as follows. The first and the last one follow immediately from the definition of $\leqslant$ in a lattice. The second from condition (ii), the third from the uniqueness of complements in Boolean algebras, and the fourth one from (i).

(iv): We shall detail the proof that a^* is the largest element $b \in A$ such that $a \wedge b = 0$, as the proof of the other part of the statement is analogous. To this end, consider $b \in A$ such that $a \wedge b = 0$. It suffices to prove that $b \leqslant a^*$, i.e., $a^* = a^* \vee b$. We have

$$a^* = a^* \vee 0 = a^* \vee (a \wedge b) = (a^* \vee a) \wedge (a^* \vee b) = 1 \wedge (a^* \vee b) = a^* \vee b.$$

The above equalities are justified as follows. The first follows from the fact that 0 is the minimum, the second from the assumption that $a \wedge b = 0$, the third from distributivity, the fourth from the fact that a^* is a complement of a, and the last one from the fact that 1 is the maximum. ⊠

Let $\boldsymbol{A}$ and $\boldsymbol{B}$ be Boolean algebras. A *homomorphism* from $\boldsymbol{A}$ to $\boldsymbol{B}$ is a map $f\colon A \to B$ such that for every $a, c \in A$,

$$\begin{gathered}f(a \wedge^{\boldsymbol{A}} c) = f(a) \wedge^{\boldsymbol{B}} f(c) \quad f(a \vee^{\boldsymbol{A}} c) = f(a) \vee^{\boldsymbol{B}} f(c) \\ f(0^{\boldsymbol{A}}) = 0^{\boldsymbol{B}} \quad f(1^{\boldsymbol{A}}) = f(1^{\boldsymbol{B}}) \quad f(a^*) = f(a)^*.\end{gathered}$$

In view of Proposition 3.5, the demand that $f(a^*) = f(a)^*$ in the above display is redundant. An injective homomorphism from $\boldsymbol{A}$ to $\boldsymbol{B}$ is called an *embedding*. Lastly, a surjective embedding is called an *isomorphism*. We say that $\boldsymbol{A}$ and $\boldsymbol{B}$ are *isomorphic*, in symbols $\boldsymbol{A} \cong \boldsymbol{B}$, when there exists an isomorphism between them.

Definition 3.10. A Boolean algebra $\boldsymbol{B}$ is a *subalgebra* of a Boolean algebra $\boldsymbol{A}$ if $B \subseteq A$ and the inclusion map $i\colon B \to A$ is a homomorphism. A set $B \subseteq A$ is called a *subuniverse* of $\boldsymbol{A}$ if B is the universe of a subalgebra of $\boldsymbol{A}$.

Notice that the subuniverses of a Boolean algebra $\boldsymbol{A}$ are always nonempty, since they must contain the bounds 0 and 1 (this contrasts with the case of lattices).

As in the case of lattices, the poset of subuniverses of a Boolean algebra $\boldsymbol{A}$ ordered under inclusion is an inductive closure system on A. The associated finitary closure operator

$$\mathrm{Sg}^{\boldsymbol{A}}\colon \mathcal{P}(A) \to \mathcal{P}(A)$$

can be described as follows: for every $X \subseteq A$,

$$\mathrm{Sg}^{\boldsymbol{A}}(X) = \{a \in A : \text{there exist a Boolean term } \varphi(x_1, \dots, x_n) \text{ and elements } a_1, \dots, a_n \in X \text{ such that } a = \varphi^{\boldsymbol{A}}(a_1, \dots, a_n)\}.$$

Accordingly, a Boolean algebra $\boldsymbol{A}$ is said to be *generated* by a set $X \subseteq A$ when $\mathrm{Sg}^{\boldsymbol{A}}(X) = A$. In this case, X is called a set of *generators* for $\boldsymbol{A}$. Accordingly, $\boldsymbol{A}$ is said to be *finitely generated* when there is a finite $X \subseteq A$ such that $\mathrm{Sg}^{\boldsymbol{A}}(X) = A$.

Definition 3.11. A Boolean term $\varphi(x_1, \dots, x_n)$ is in *conjunctive normal form* (CNF for short) there are distinct nonempty sets

$$V_1, \dots, V_k \subseteq \{x_1, \dots, x_n, x_1^*, \dots, x_n^*\}$$

such that

$$\varphi = (\bigvee V_1) \wedge \cdots \wedge (\bigvee V_k).$$

The notion of *disjunctive normal form* (DNF for short) is defined symmetrically.

Notice that there are finitely many Boolean terms in CNF (resp. DNF) in variables $x_1, \dots, x_n$.

Theorem 3.12. *For every Boolean term φ is there is a Boolean term ψ in CNF (resp. DNF) such that the equation $\varphi \approx \psi$ holds in the class of Boolean algebras.*

Corollary 3.13. *The class of Boolean algebras is locally finite, in the sense that finitely generated Boolean algebras are finite.*

*Exercise** 3.14. Prove Theorem 3.12 for the case of CNFs and 3.13. Hint: prove, by induction on the construction of Boolean terms, that for every Boolean term $\varphi(x_1, \dots, x_n)$ there exists a Boolean term $\varphi^+(x_1, \dots, x_n)$ in CNF such that the equation $\varphi \approx \varphi^+$ holds in every Boolean algebra. To this end, you might wish to use the following strategy:

(i) Explain why, in view of Proposition 3.9(ii), we can assume, without loss of generality, that the symbol $\vee$ does not occur in φ;

(ii) Explain why, in view of the fact that the equations $x \wedge x^* \approx 0$ and $x \vee x^* \approx 1$ hold in every Boolean algebra, we can assume, without loss of generality, that the symbols 0 and 1 do not occur in φ.

Thus, we can always assume that the only connectives that occur in φ are $\wedge$ and $(\cdot)^*$ (this does not mean that the same can be assumed of φ^+, however). Now that you know that the symbols $\vee, 0$, and 1 do not occur in φ, take inspiration from the proofs of Theorem 2.21 and of Corollary 2.22 to develop the necessary inductive argument.

The inductive step will comprise two parts: one for the case where $\varphi = \psi_1 \wedge \psi_2$ (for some Boolean terms ψ_1 and ψ_2) and one for the case where $\varphi = \psi^*$ (for some Boolean term ψ). In the case of ψ^* you might wish to use the properties in Proposition 3.9 and distributivity. ⊠

3.3 Powerset = atomic and complete

As we mentioned, the canonical example of a Boolean algebra is the powerset Boolean algebra $\mathcal{P}(X)$ (Example 3.7). Our aim is to characterize Boolean algebras isomorphic to a powerset one. To this end, it is convenient to introduce the following concepts.

Definition 3.15. An element a of a Boolean algebra $\boldsymbol{A}$ is said to be an *atom* if $a > 0$ and there is no $c \in A$ such that $0 < c < a$. Accordingly, a Boolean algebra $\boldsymbol{A}$ is said to be *atomic* if, for every $c \in A$, there exists an atom $a \leqslant c$.

Atoms in Boolean algebras can be described as follows:

Lemma 3.16. *An element a of a Boolean algebra $\boldsymbol{A}$ is an atom if and only if it is join-irreducible. Consequently, the poset of join-irreducible elements of $\boldsymbol{A}$ is discrete, in the sense that every two distinct elements are incomparable.*

Proof. The fact that atoms are join-irreducible follows immediately from the definition of an atom. Conversely, consider a join-irreducible element $a \in A$. By definition of join-irreducibility, $a > 0$. Then consider $c \in A$ such that $0 < c \leqslant a$. We have

$$a = a \wedge 1 = a \wedge (c \vee c^*) = (a \wedge c) \vee (a \wedge c^*).$$

Since a is join-irreducible, either $a = a \wedge c$ or $a = a \wedge c^*$. Consequently, either $a \leqslant c$ or $a \leqslant c^*$. If $a \leqslant c^*$, then $c \leqslant c^*$ (because $c \leqslant a$), whence $c \wedge c^* = c$. Since, by assumption, $c > 0$, this yields $c \wedge c^* > 0$, which is false. Hence, we conclude that $a \leqslant c$. Since $c \leqslant a$, we conclude that $a = c$ and, therefore, that a is an atom.

Lastly, it is clear that the poset of atoms of $\boldsymbol{A}$ is discrete. Therefore, since atoms and join-irreducible elements coincide in $\boldsymbol{A}$, we are done. ⊠

The next proposition illustrates these definitions in the case of powerset Boolean algebras.

Proposition 3.17. *Let X be a set and $\mathcal{P}(X)$ the associated powerset Boolean algebra. The atoms of $\mathcal{P}(X)$ are precisely the singletons $\{x\}$ for $x \in X$. Consequently, $\mathcal{P}(X)$ is atomic.*

Proof. Notice that the minimum 0 of $\mathcal{P}(X)$ is $\emptyset$. We begin by proving that $\{x\}$ is an atom of $\mathcal{P}(X)$, for all $x \in X$. Consider $x \in X$. As $\{x\}$ is nonempty, we have $\emptyset \subsetneq \{x\}$. Furthermore, there is no $Y \in \mathcal{P}(X)$ such that $0 = \emptyset \subsetneq Y \subsetneq \{x\}$. Thus, $\{x\}$ is an atom of $\mathcal{P}(X)$.

Conversely, consider an atom Y of $\mathcal{P}(X)$. As $\emptyset \subsetneq Y$, there is some $y \in Y$. Clearly, $\emptyset \subsetneq \{y\} \subseteq Y$. Since Y is an atom, this implies $Y = \{y\}$. It follows that the atoms of $\mathcal{P}(X)$ are precisely the singletons $\{x\}$ for $x \in X$.

To prove that $\mathcal{P}(X)$ is atomic, consider any element $Y \in \mathcal{P}(X)$ such that $\emptyset \subsetneq Y$. As $Y \neq \emptyset$, there is $y \in Y$, whence $\{y\} \subseteq Y$. Since $\{y\}$ is an atom, we are done. ⊠

Notably, in an atomic Boolean algebra, every element can be obtained as a join of atoms. This turns out to be a characterization of atomic Boolean algebras, as we proceed to explain.

Proposition 3.18. *The following conditions are equivalent for a Boolean algebra $\boldsymbol{A}$:*

(i) *$\boldsymbol{A}$ is atomic;*

(ii) *Every element of* $\boldsymbol{A}$ *is a join of atoms;*

(iii) *Let* X *be the set of atoms of* $\boldsymbol{A}$*. For every* $a \in A$*,*

$$a = \bigvee(X \cap {\downarrow}a).$$

Proof. (i)⇒(ii): Conversely, suppose, with a view to contradiction, that $\boldsymbol{A}$ is atomic and that there exists $a \in A$ that is not a join of atoms. In particular, $a \neq \bigvee(X \cap {\downarrow}a)$, where X is the set of atoms of $\boldsymbol{A}$. As a is an upper bound of $X \cap {\downarrow}a$, this implies that there exists an upper bound c of $X \cap {\downarrow}a$ such that $a \not\leqslant c$. Then either a and c are incomparable or $c < a$. In both cases, $a \wedge c < c$ and $a \wedge c$ is an upper bound of $X \cap {\downarrow}a$, whence we can assume, without loss of generality, that $c < a$ (otherwise, we replace c by $a \wedge c$).

From $0 \leqslant c < a$ and the assumption that $\boldsymbol{A}$ is atomic, it follows that there exists $x \in X \cap {\downarrow}a$. As c is an upper bound of $X \cap {\downarrow}a$, we have $0 < x \leqslant c$. Thus,

$$0 < c < a.$$

We claim that $0 < a \wedge c^*$. Suppose the contrary, with a view to contradiction. Then $a \wedge c^* = 0$. By Proposition 3.9(iv), we get $c^* \leqslant a^*$. Moreover, by Proposition 3.9(iii), $a^{**} \leqslant c^{**}$, whence $a = a^{**} \leqslant c^{**} = c$, a contradiction with $c < a$. This concludes the proof of the claim.

Now, since $0 < a \wedge c^*$ and $\boldsymbol{A}$ is atomic, there is an atom $x \leqslant a \wedge c^*$. In particular, $x \in X \cap {\downarrow}a$. Since c is an upper bound of $X \cap {\downarrow}a$, we get $x \leqslant c$. Also, as $x \leqslant a \wedge c^*$, we get $x \leqslant c^*$. We conclude that $0 < x \leqslant c \wedge c^*$, a contradiction with $c \wedge c^* = 0$.

(ii)⇒(iii): Straightforward.

(iii)⇒(i): Suppose that $a = \bigvee(X \cap {\downarrow}a)$, for every $a \in A$. Then consider $a \in A \smallsetminus \{0\}$. Since

$$\bigvee \emptyset = 0 \neq a = \bigvee(X \cap {\downarrow}a),$$

we get $X \cap {\downarrow}a \neq \emptyset$. Consequently, exists $x \in X$ such that $x \leqslant a$. We conclude that $\boldsymbol{A}$ is atomic. ⊠

We rely on the following property of atoms in Boolean algebras:

Lemma 3.19. *Let* $\boldsymbol{A}$ *be a Boolean algebra and* $X \cup \{a\}$ *a set of atoms of* $\boldsymbol{A}$*. If* $\bigvee X$ *exists and* $a \leqslant \bigvee X$*, then* $a \in X$*.*

Proof. Suppose, with a view to contradiction, that $a \leqslant \bigvee X$ and $a \notin X$. Then consider $c \in X$. As a is an atom, ${\downarrow}a = \{a, 0\}$. Thus, $a \wedge c \in \{a, 0\}$. Now, if $a \wedge c = a$, then $a \leqslant c$. As a is an atom, this implies $0 < a \leqslant c$. Together with the fact that c is also an atom, we conclude that $a = c$, a contradiction with $a \notin X$. Thus, necessarily $a \wedge c = 0$. It follows that

$$a \wedge c = 0, \text{ for all } c \in X.$$

Together with 3.9(iv), this implies $c \leqslant a^*$, for all $c \in X$. Thus, $\bigvee X \leqslant a^*$. But this implies $a \leqslant \bigvee X \leqslant a^*$ and, therefore, $0 = a \wedge a^* = a$, contradicting the fact that $a > 0$ (as a is an atom). ⊠

We are now ready to present the classical description of powerset Boolean algebras.

Theorem 3.20 (Lindenbaum & Tarski)**.** *A Boolean algebra* $\boldsymbol{A}$ *is isomorphic to a powerset one if and only if it is complete and atomic.*

Proof. Powerset Boolean algebras are atomic, by Proposition 3.17, and complete. Since these properties are preserved by isomorphisms, we conclude that if $\boldsymbol{A}$ is isomorphic to a powerset Boolean algebra, it is also complete and atomic.

To prove the converse, suppose that $\boldsymbol{A}$ is complete and atomic. Then let X be the set of atoms of $\boldsymbol{A}$ and consider the function $f\colon \boldsymbol{A} \to \mathcal{P}(X)$, defined by the rule

$$f(a) := X \cap {\downarrow}a, \text{ for all } a \in A.$$

We shall prove that f is an isomorphism. Notice that, as complements are unique, it suffices to show that f is an isomorphism of posets, i.e., that f is surjective and for every $a, c \in A$,

$$a \leqslant c \iff f(a) \subseteq f(c).$$

To this end, consider then $a, c \in A$. If $a \leqslant c$, then, by definition of f, clearly $f(a) \subseteq f(c)$. Conversely, suppose that $a \not\leqslant c$. By Proposition 3.18, there is an atom x such that $x \leqslant a$ and $x \not\leqslant c$. Thus, $x \in f(a) \smallsetminus f(c)$, whence $f(a) \not\subseteq f(c)$. This establishes that f is an order embedding. It only remains to prove that it is surjective. To this end, consider $Y \subseteq X$. As $\boldsymbol{A}$ is complete, the supremum $\bigvee Y$ exists in $\boldsymbol{A}$. Clearly, $Y \subseteq f(\bigvee Y)$. To prove the other inclusion, consider $x \in f(\bigvee Y)$. Then $x \leqslant \bigvee Y$. By Lemma 3.19, this yields $x \in Y$, whence $f(\bigvee Y) \subseteq Y$, as desired. ⊠

As a consequence, we obtain a description of all finite Boolean algebras.

Corollary 3.21. *Up to isomorphism, finite Boolean algebras coincide with powerset Boolean algebras of the form $\mathcal{P}(X)$, where X is a finite set. Consequently,*

(i) *Any two finite Boolean algebras of the same cardinality are isomorphic;*

(ii) *Every finite Boolean algebra has cardinality 2^n for some $n \in \omega$.*

Proof. Finite Boolean algebras are, of course, complete and atomic. Therefore the result follows from Theorem 3.20. ⊠

Remark 3.22. Notably, Corollary 3.21 could have been derived directly from the representation of finite distributive lattices given in Corollary 3.21. To explain how, consider a finite Boolean algebra $\boldsymbol{A}$. By Corollary 3.21, the lattice underlying $\boldsymbol{A}$ is isomorphic to the distributive lattice $\mathrm{Dw}(\mathbb{X})$, where $\mathbb{X}$ is the poset of join-irreducible elements of $\boldsymbol{A}$. Now, in view of Lemma 3.16, the order of $\mathbb{X}$ is the identity relation. Consequently, $\mathrm{Dw}(\mathbb{X}) = \mathcal{P}(X)$. It follows that the lattice underlying $\boldsymbol{A}$ is isomorphic to $\mathcal{P}(X)$. Since this isomorphism preserves the bounds and the lattice operations, it is an isomorphism of Boolean algebras as well. ⊠

As it happens, both assumptions (i.e., atomicity and completeness) in Theorem 3.20 are necessary. The next example describes a family of atomic Boolean algebras that fail to be complete. On the other hand, a nontrivial Boolean algebra that is not atomic will be presented in Example 3.37.*

Example 3.23. In order to construct an atomic Boolean algebra that is not complete, consider an infinite set X. An argument, similar to the one detailed in the proof of

*Complete and nonatomic Boolean algebras also exists, but their construction is too involved to be presented here.

Proposition 3.17, shows that the finite cofinite Boolean algebra $\mathcal{FC}(X)$ is atomic, its atoms being the singletons $\{x\}$ for $x \in X$.

We shall see that $\mathcal{FC}(X)$ is not complete. Suppose the contrary, with a view to contradiction. Then consider a set $Y \subseteq X$ that is neither finite nor infinite (such an Y exists, because X is infinite). Notice that the singletons $\{y\}$ are finite, for all $y \in Y$, and, therefore, belong to $\mathcal{FC}(X)$. As $\mathcal{FC}(X)$ is complete, this implies that following join exists in $\mathcal{FC}(X)$:

$$x := \bigvee_{y \in Y} \{y\}.$$

We will prove that $x = Y$. By definition of join, $\{y\} \subseteq x$, for all $y \in Y$, whence $Y \subseteq x$. Conversely, consider $z \in x$. Then

$$\{z\} \subseteq x = \bigvee_{y \in Y} \{y\}.$$

As $\{z\}$ and each $\{y\}$ are atoms, we can apply Lemma 3.19, obtaining that $z \in Y$. Hence, we conclude that $x = Y$. Since $x \in \mathcal{FC}(X)$, this implies that Y is either finite or cofinite, a contradiction. Hence, $\mathcal{FC}(X)$ is not complete. ⊠

3.4 Filters and congruences

It is well-known that the lattice of congruences of a group (resp. a ring) is isomorphic to that of its normal subgroups (resp. its ideals). In this section we shall prove that a similar isomorphism connects the filters, ideals, and congruences of a Boolean algebra. To this end, it is convenient to introduce the following notation.

Definition 3.24. Let $\boldsymbol{A}$ be a Boolean algebra and $a, c \in A$. We set

$$a \to c := a^* \vee c \text{ and } a - c := a \wedge c^*.$$

The operations $\to$ and $-$ are called, respectively, *implication* and *subtraction*.

Notice that, in a powerset Boolean algebra $\mathcal{P}(X)$, implication and subtraction can be described as follows: for every $Y, Z \subseteq X$,

$$Y \to Z = \{x \in X : \text{if } x \in Y, \text{ then } x \in Z\}$$
$$Y - Z = \{x \in X : x \in Y \text{ and } x \notin Z\}.$$

More in general, the behaviour of implication and subtraction is governed by the following laws:

Proposition 3.25. *The following conditions hold for every Boolean algebra $\boldsymbol{A}$ and $a, b, c \in A$:*

(i) $(a \to c)^* = a - c$ *and* $(a - c)^* = a \to c$;

(ii) $a^* = a \to 0 = 1 - a$;

(iii) $a \to a = 1$ *and* $a - a = 0$;

(iv) *Residuation laws:* $a \to c$ *is the largest element* $d \in A$ *such that* $a \wedge d \leqslant c$*, i.e., for every* $d \in A$*,*

$$a \wedge d \leqslant c \iff d \leqslant a \to c.$$

Moreover, $a - c$ *is the least element* $d \in A$ *such that* $a \leqslant c \vee d$*, i.e., for every* $d \in A$*,*

$$a \leqslant c \vee d \iff a - c \leqslant d;$$

(v) $(a \to b) \wedge (b \to c) \leqslant a \to c$ *and* $(a - c) \leqslant (a - b) \vee (b - c)$*;*

(vi) $(a \vee b) \to c = (a \to b) \wedge (a \to c)$ *and* $(a \vee b) - c = (a - b) \vee (b - c)$*;*

(vii) $a \to (b \wedge c) = (a \to b) \wedge (a \to c)$ *and* $a - (b \wedge c) = (a - b) \vee (b - c)$*.*

Proof. (i): From the double negation elimination and De Morgan laws it follows

$$(a \to c)^* = (a^* \vee c)^* = (a^* \vee c^{**})^* = a \wedge c^* = a - c.$$

Consequently, also $(a - c)^* = (a \to c)^{**} = a \to c$.

(ii): We have $a^* = a^* \vee 0 = a \to 0$. Similarly, $a^* = 1 \wedge a^* = 1 - a$.

(iii): Immediate from the definition of a complement.

(iv): We detail only the case of $\to$, as the other one is analogous. First, observe that

$$a \wedge (a \to c) = a \wedge (a^* \vee c) = (a \wedge a^*) \vee (a \wedge c) = 0 \vee (a \wedge c) = a \wedge c \leqslant c.$$

Therefore, it only remains to prove that every $d \in A$ such that $a \wedge d \leqslant c$ is $\leqslant a \to c$. Consider such a $d \in A$. We have

$$d = d \wedge 1 = d \wedge (a \vee a^*) = (d \wedge a) \vee (d \wedge a^*) \leqslant c \vee a^* = a \to c.$$

The inequality above follows from the assumption that $a \wedge b \leqslant c$ and the fact that $b \wedge a^* \leqslant a^*$.

(v): Again, we detail only the case of $\to$, as the other one is analogous. By the residuation law, we have

$$a \wedge (a \to b) \leqslant b \text{ and } b \wedge (b \to c) \leqslant c.$$

Then

$$a \wedge (a \to b) \wedge (b \to c) \leqslant b \wedge (b \to c) \leqslant c.$$

With another application of the residuation law, we obtain

$$(a \to b) \wedge (b \to c) \leqslant a \to c.$$

(vi): We detail only the case of $\to$ only. For every $x \in A$, we have

$$\begin{aligned} x \leqslant (a \vee b) \to c &\iff x \wedge (a \vee b) \leqslant c \\ &\iff (x \wedge a) \vee (x \wedge b) \leqslant c \\ &\iff x \wedge a, x \wedge b \leqslant c \\ &\iff x \leqslant a \to c, b \to c \\ &\iff x \leqslant (a \to c) \wedge (b \to c). \end{aligned}$$

The equivalences above are justified as follows. The first follows from the residuation law, the second from distributivity, the third from the definition of $\vee$, the fourth from the residuation law, and the last one from the definition of $\wedge$. We conclude that $(a \vee b) \to c = (a \to c) \wedge (b \to c)$, as desired.

(vii): We detail only the case of $\to$ only. For every $x \in A$, we have

$$\begin{aligned} x \leqslant a \to (b \wedge c) &\iff x \wedge a \leqslant b \wedge c \\ &\iff x \wedge a \leqslant b, c \\ &\iff x \leqslant a \to b, a \to c \\ &\iff x \leqslant (a \to b) \wedge (a \to c). \end{aligned}$$

The equivalences above are justified as follows. The first follows from the residuation law, the second the definition of $\wedge$, the third from the residuation law, and the last one from the definition of $\wedge$. We conclude that $a \to (b \wedge c) = (a \to b) \wedge (a \to c)$, as desired. ⊠

Now, we turn our attention to the definition of a congruence in the case of Boolean algebras. In this respect, we expect the congruences of a Boolean algebra $\boldsymbol{A}$ to be the equivalence relations on A that preserve the operations of $\boldsymbol{A}$. The next proposition states that these are precisely the congruences of the lattice reduct $\langle A; \wedge, \vee \rangle$ of $\boldsymbol{A}$.

Proposition 3.26. *Let $\boldsymbol{A}$ be a Boolean algebra, θ a congruence of $\langle A; \wedge, \vee \rangle$, and $a, c \in A$. If $a \equiv_\theta c$, then $a^* \equiv_\theta c^*$.*

Proof. Suppose that $a \equiv_\theta c$. Using distributivity and the definition of a complement, we obtain

$$\begin{aligned} c^* \wedge (a \vee a^*) &= c^* \wedge 1 = c^* \\ c^* \wedge (c \vee a^*) &= (c^* \wedge c) \vee (c^* \wedge a^*) = 0 \vee (c^* \wedge a^*) = c^* \wedge a^*. \end{aligned}$$

Moreover, since $a \equiv_\theta c$, also $c^* \wedge (a \vee a^*) \equiv_\theta c^* \wedge (c \vee a^*)$. Together with the above display, this implies $c^* \equiv_\theta c^* \wedge a^*$. An analogous argument shows that $a^* \equiv_\theta a^* \wedge c^*$, thus

$$a^* \equiv_\theta c^* \wedge a^* \equiv_\theta c^*.$$

By the transitivity of θ, we conclude that $a^* \equiv_\theta c^*$. ⊠

In view of the above result, the congruences of the lattice reduct of a Boolean algebra preserve complements. Because of this, given a congruence θ of the lattice reduct $\langle A; \wedge, \vee \rangle$ of a Boolean algebra $\boldsymbol{A}$, we can endow the quotient set A/θ with the structure of a Boolean algebra $\boldsymbol{A}/\theta$, stipulating that for every $a, c \in A$,

$$\begin{aligned} a/\theta \wedge^{\boldsymbol{A}/\theta} c/\theta &:= (a \wedge^{\boldsymbol{A}} c)/\theta \\ a/\theta \vee^{\boldsymbol{A}/\theta} c/\theta &:= (a \vee^{\boldsymbol{A}} c)/\theta \\ (a/\theta)^{*\boldsymbol{A}/\theta} &:= a^{*\boldsymbol{A}}/\theta \\ 1^{\boldsymbol{A}/\theta} &:= 1^{\boldsymbol{A}}/\theta \\ 0^{\boldsymbol{A}/\theta} &:= 0^{\boldsymbol{A}}/\theta. \end{aligned}$$

Notice that the structure $\boldsymbol{A}/\theta$ is well-defined because θ preserves complements.

Exercise 3.27. Prove $\boldsymbol{A}/\theta$ is indeed a well-defined Boolean algebra. ⊠

This motivates the following definition:

Definition 3.28. A *congruence* of a Boolean algebra $\boldsymbol{A}$ is just a congruence of the lattice underlying $\boldsymbol{A}$.

Accordingly, from Proposition 2.56 it follows that the set $\mathrm{Con}\boldsymbol{A}$ of congruence of $\boldsymbol{A}$ is an inductive closure system on $A \times A$. Furthermore, when seen as a complete lattice, $\mathrm{Con}\boldsymbol{A}$ is distributive, by Theorem 2.60.

We shall now introduce the notions of a filter and an ideal of a Boolean algebra.

Definition 3.29. Let $\boldsymbol{A}$ be a Boolean algebra, and $F, I \subseteq A$.

(i) F is said to be a *filter* if it is a nonempty filter of the lattice reduct of $\boldsymbol{A}$;

(ii) I is said to be an *ideal* if it is a nonempty ideal of the lattice reduct of $\boldsymbol{A}$.

In this case, $1 \in F$ and $0 \in I$. The sets of filters and ideals of $\boldsymbol{A}$ are inductive closure systems on A and, therefore, complete lattices. We denote them, respectively, by

$$\mathcal{F}i\boldsymbol{A} \text{ and } \mathcal{I}d\boldsymbol{A}.$$

Our aim is to prove that, for every Boolean algebra $\boldsymbol{A}$, the complete lattices $\mathcal{F}i\boldsymbol{A}, \mathcal{I}d\boldsymbol{A}$, and $\mathrm{Con}\boldsymbol{A}$ are isomorphic. On the one hand, in Boolean algebras, we can associate a congruence with every filter (resp. ideal), as we proceed to explain.

Proposition 3.30. *Let $\boldsymbol{A}$ be a Boolean algebra, F a filter, and I an ideal. The following relations are congruences of $\boldsymbol{A}$:*

$$\theta_F := \{\langle a, c\rangle \in A \times A : a \to c, c \to a \in F\}$$
$$\theta_I := \{\langle a, c\rangle \in A \times A : a - c, c - a \in I\}.$$

Proof. We shall detail the case of θ_F only, as the other one is analogous. We begin by proving that θ_F is an equivalence relation on A. To this end, consider $a, b, c \in A$. By Proposition 3.25(iii) and the fact that $1 \in F$, we obtain $a \to a = 1 \in F$. Thus, $\langle a, a\rangle \in \theta_F$, whence θ_F is reflexive. The fact that θ_F is symmetric is straightforward. To prove that it is transitive, suppose that $\langle a, b\rangle, \langle b, c\rangle \in \theta_F$. We have $a \to b, b \to c \in F$, whence also $(a \to b) \wedge (b \to c) \in F$ (as F is closed under binary meets). Since $(a \to b) \wedge (b \to c) \leqslant a \to c$, by Proposition 3.25(v), and F is an upset, we conclude that $a \to c \in F$. A similar argument shows $c \to a \in F$, whence $\langle a, c\rangle \in \theta_F$, as desired. It follows that θ_F is transitive and, therefore, an equivalence relation on A.

It only remains to prove that θ_F preserves $\wedge$ and $\vee$. To this end, consider $\langle a_1, a_2\rangle, \langle c_1, c_2\rangle \in \theta_F$, i.e.,

$$a_1 \to a_2, a_2 \to a_1, c_1 \to c_2, c_2 \to c_1 \in F.$$

In particular, since F is closed under binary meets,

$$(a_1 \to a_2) \wedge (c_1 \to c_2), (a_2 \to a_1) \wedge (c_2 \to c_1) \in F. \tag{3.1}$$

To prove that θ_F preserves meets, observe that, by the residuation law,

$$a_1 \wedge (a_1 \to a_2) \leqslant a_2 \text{ and } c_1 \wedge (c_1 \to c_2) \leqslant c_2, \tag{3.2}$$

whence

$$(a_1 \wedge c_1) \wedge (a_1 \to a_2) \wedge (c_1 \to c_2) \leqslant a_2 \wedge c_2.$$

With another application of the residuation law,

$$(a_1 \to a_2) \wedge (c_1 \to c_2) \leqslant (a_1 \wedge c_1) \to (a_2 \wedge c_2).$$

Together with (3.1) and the fact that F is an upset, this yields $(a_1 \wedge c_1) \to (a_2 \wedge c_2) \in F$. A similar argument shows that $(a_2 \wedge c_2) \to (a_1 \wedge c_1) \in F$, whence $\langle a_1 \wedge c_1, a_2 \wedge c_2 \rangle \in \theta_F$. We conclude that θ_F preserves $\wedge$.

To prove that θ_F preserves joins, observe that, by (3.2),

$$a_1 \wedge (a_1 \to a_2) \leqslant a_2 \vee c_2 \text{ and } c_1 \wedge (c_1 \to c_2) \leqslant a_2 \vee c_2.$$

By the residuation law,

$$a_1 \to a_2 \leqslant a_1 \to (a_2 \vee c_2) \text{ and } c_1 \to c_2 \leqslant c_1 \to (a_2 \vee c_2),$$

whence

$$(a_1 \to a_2) \wedge (c_1 \to c_2) \leqslant (a_1 \to (a_2 \vee c_2)) \wedge (c_1 \to (a_2 \vee c_2)).$$

By Proposition 3.25(vii),

$$(a_1 \to a_2) \wedge (c_1 \to c_2) \leqslant (a_1 \vee c_1) \to (a_2 \vee c_2).$$

Together with (3.1) and the fact that F is an upset, this yields $(a_1 \vee c_1) \to (a_2 \vee c_2) \in F$. A similar argument shows that $(a_2 \vee c_2) \to (a_1 \vee c_1) \in F$, whence $\langle a_1 \vee c_1, a_2 \vee c_2 \rangle \in \theta_F$. We conclude that θ_F preserves $\vee$. ⊠

On the other hand, every congruence of a Boolean algebra can be associated with a filter and an ideal.

Proposition 3.31. *Let θ be a congruence of a Boolean algebra $\boldsymbol{A}$. The equivalence classes*

$$F_\theta := 1/\theta \text{ and } I_\theta = 0/\theta$$

are, respectively, a filter and an ideal of $\boldsymbol{A}$.

Proof. We shall detail the proof that F_θ is a filter only, as the other part is analogous. First, notice that F_θ is nonempty, since it contains 1. Thus, it only remains to prove that F is an upset closed under binary meets. To this end, consider two elements $a, c \in A$. First, suppose that $a \in F_\theta$ and $a \leqslant c$. In this case,

$$c = a \vee c \equiv_\theta 1 \vee c = 1,$$

where the first equality follows from $a \leqslant c$. Therefore, $c \equiv_\theta 1$, that is, $c \in F_\theta$. We conclude that F_θ is an upset. To prove that it is closed under binary meets, suppose that $a, c \in F_\theta$. We have

$$a \wedge c \equiv_\theta 1 \wedge 1 = 1,$$

whence $a \wedge c \equiv_\theta 1$, that is, $a \wedge c \in F_\theta$. ⊠

Notably, the correspondence between filters, ideals, and congruences detailed above turns out to be an isomorphism.

Theorem 3.32. *The following conditions hold for a Boolean algebra* $\boldsymbol{A}$*:*

(i) *The maps*

$$\theta_{(\cdot)} \colon \mathcal{F}i\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A} \text{ and } F_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}$$

are well-defined lattice isomorphism, one inverse to the other;

(ii) *The maps*

$$\theta_{(\cdot)} \colon \mathcal{I}d\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A} \text{ and } I_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{I}d\boldsymbol{A}$$

are well-defined lattice isomorphism, one inverse to the other.

Consequently, the lattices $\mathcal{F}i\boldsymbol{A}, \mathcal{I}d\boldsymbol{A}$*, and* $\mathrm{Con}\boldsymbol{A}$ *are isomorphic.*

Proof. We shall detail the proof of condition (i) only, as that of (ii) is analogous. First, recall that the maps

$$\theta_{(\cdot)} \colon \mathcal{F}i\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A} \text{ and } F_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}$$

are well-defined by Propositions 3.30 and 3.31.

We shall prove that they are one inverse to the other. To this end, consider $G \in \mathcal{F}i\boldsymbol{A}$ and $a \in A$. We have

$$a \in G \iff \{1, a\} \subseteq G \iff \{a \to 1, 1 \to a\} \subseteq G \iff a \equiv_{\theta_G} 1 \iff a \in F_{\theta_G}$$

The equivalences in the above display are justified as follows. The first follows from the fact that $1 \in G$, as G is a filter, the second from the fact that $a \to 1 = a^* \vee 1 = 1$ and $1 \to a = 1^* \vee a = 0 \vee a = a$, the third from the definition of θ_G, and the last one from the definition of F_{θ_G}. Hence, we conclude that $G = F_{\theta_G}$.

Then consider $\phi \in \mathrm{Con}\boldsymbol{A}$ and $a, c \in A$. Observe that

$$\langle a, c \rangle \in \phi \iff (a \to c \equiv_\phi 1 \text{ and } c \to a \equiv_\phi 1). \tag{3.3}$$

To prove this, observe that if $\langle a, c \rangle \in \phi$, then $a \to a \equiv_\phi c \to a$ and $a \to a \equiv_\phi a \to c$. By Proposition 3.25(iii), we know that $a \to a = 1$, whence $a \to c \equiv_\phi 1$ and $c \to a \equiv_\phi 1$. Conversely, suppose that $a \to c \equiv_\phi 1$ and $c \to a \equiv_\phi 1$. Then

$$\begin{aligned} a = a \wedge 1 &\equiv_\phi a \wedge (a \to c) = (a \wedge c) \wedge (a \to c) \\ c = c \wedge 1 &\equiv_\phi c \wedge (c \to a) = (a \wedge c) \wedge (c \to a). \end{aligned}$$

We detail the proof of the first line of the display, as the second one is proved analogously. The first step follows from the fact that 1 is the maximum, the second from the assumption that $a \to c \equiv_\phi 1$, and the third from the residuation law, which guarantees that $a \wedge (a \to c) \leqslant c$.

Together with assumption that $a \to c \equiv_\phi 1$ and $c \to a \equiv_\phi 1$, the above display implies

$$a = (a \wedge c) \wedge (a \to c) \equiv_\phi (a \wedge c) \wedge (c \to a) = c.$$

Hence $\langle a, c \rangle \in \phi$, as desired. This establishes (3.3).

As a consequence, we obtain

$$\langle a, c \rangle \in \phi \iff a \to c \equiv_\phi 1 \equiv_\phi c \to a \iff \{a \to c, c \to a\} \subseteq F_\phi \iff \langle a, c \rangle \in \theta_{F_\phi}.$$

The first equivalence above follows from (3.3), the second from the definition of F_ϕ, and the last one from that definition of θ_{F_ϕ}. Hence, we conclude that $\phi = \theta_{F_\phi}$.

It follows that the maps in (i) are one inverse to the other. In particular, they are bijections. Therefore, in order to prove that they are also lattice isomorphisms, it suffices to show that they preserve and reflect the order. It is straightforward that they are order preserving. To prove that $\theta_{(\cdot)} \colon \mathcal{F}i\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A}$ reflects the order, consider $G, H \in \mathcal{F}i\boldsymbol{A}$ such that $\theta_G \subseteq \theta_H$. As $F_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}$ is order preserving, $F_{\theta_G} \subseteq F_{\theta_H}$. But, as the maps $\theta_{(\cdot)} \colon \mathcal{F}i\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A}$ and $F_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}$ are one inverse to the other, this yields

$$G = F_{\theta_G} \subseteq F_{\theta_H} = H.$$

It follows that $\theta_{(\cdot)} \colon \mathcal{F}i\boldsymbol{A} \to \mathrm{Con}\boldsymbol{A}$ reflects the order and, therefore, is a lattice isomorphism. A similar argument shows that the same is true for $F_{(\cdot)} \colon \mathrm{Con}\boldsymbol{A} \to \mathcal{F}i\boldsymbol{A}$. ⊠

Corollary 3.33. *If $\boldsymbol{A}$ is a Boolean algebra and $X \subseteq A \times A$, then*

$$\begin{aligned}\mathrm{Cg}^{\boldsymbol{A}}(X) = \{\langle a, c\rangle \in A \times A : \textit{there are } \langle b_1, d_1\rangle, \dots, \langle b_n, d_n\rangle \in X \\ \textit{such that } \bigwedge_{i\leqslant n}((b_i \to d_i) \wedge (d_i \to b_i)) \leqslant (a \to c) \wedge (c \to a)\}.\end{aligned}$$

Proof. By definition, $\mathrm{Cg}^{\boldsymbol{A}}(X)$ is the least congruence extending X. In view of the of correspondence between filters and congruences in Theorem 3.32,

$$\mathrm{Cg}^{\boldsymbol{A}}(X) = \theta_F$$

where F is the least filter such that $\{b \to d, d \to b : \langle b, d\rangle \in X\} \subseteq F$. Using the description of filter generation in Proposition 2.27, this yields

$$\begin{aligned}F = \{c \in A : \text{there are } \langle b_1, d_1\rangle, \dots, \langle b_n, d_n\rangle \in X \\ \text{such that } \bigwedge_{i\leqslant n}((b_i \to d_i) \wedge (d_i \to b_i)) \leqslant c\}.\}\end{aligned}$$

In view of the display, the definition of θ_F specializes to the following:

$$\begin{aligned}\theta_F = \{\langle a, c\rangle \in A \times A : \text{there are } \langle b_1, d_1\rangle, \dots, \langle b_n, d_n\rangle \in X \\ \text{such that } \bigwedge_{i\leqslant n}((b_i \to d_i) \wedge (d_i \to b_i)) \leqslant (a \to c) \wedge (c \to a)\}.\end{aligned}$$

Since $\mathrm{Cg}^{\boldsymbol{A}}(X) = \theta_F$, we are done. ⊠

Exercise 3.34. Prove that the isomorphism between filters and congruences cannot be extended to distributive lattices. More precisely, find a distributive lattice $\boldsymbol{A}$ whose lattice of (nonempty) filters is not isomorphic to $\mathrm{Con}\boldsymbol{A}$. ⊠

Exercise 3.35. Given a Boolean algebra $\boldsymbol{A}$ and $\theta, \phi \in \mathrm{Con}\boldsymbol{A}$, we define

$$\theta \circ \phi := \{\langle a, c\rangle \in A \times A : \text{there is } b \in A \text{ such that } a \equiv_\theta b \equiv_\phi c\}.$$

Prove that the class of Boolean algebras is *congruence permutable* in the sense that, for every Boolean algebra $\boldsymbol{A}$ and $\theta, \phi \in \mathrm{Con}\boldsymbol{A}$,

$$\theta \circ \phi = \phi \circ \theta.$$

Hint: consider the Boolean term

$$p(x,y,z) := (x \wedge z) \vee (x \wedge y^* \wedge z^*) \vee (x^* \wedge y^* \wedge z).$$

Prove that for every $a, c \in A$,

$$a = p^{\boldsymbol{A}}(a,c,c) = p^{\boldsymbol{A}}(c,c,a). \tag{3.4}$$

Use the fact that the congruences of $\boldsymbol{A}$ preserve the operation $p^{\boldsymbol{A}}(x,y,z)$ to prove that $\theta \circ \phi \subseteq \phi \circ \theta$ and, therefore, $\theta \circ \phi = \phi \circ \theta$.

Now, use congruence permutability to infer that the join $\theta \vee \phi$ in $\mathrm{Con}\boldsymbol{A}$ coincides with $\theta \circ \phi$. Hint: use Corollary 2.57. Lastly, find a distributive lattice whose congruences do not permute. ⊠

Remark 3.36. The proof of the fact that the class of Boolean algebras is congruence permutable depends only on the properties of the operation $p(x,y,z)$ in (3.4). A classical result of Maltsev in Universal Algebra states that an equational class K of algebras (not necessarily Boolean algebras) is such that the congruences of its members permute if and only if there exist a term that, when interpreted in K, satisfies condition (3.4) [2, Thm. 4.664]. ⊠

Example 3.37. At the end of Section 3.3 we promised the example of a nontrivial Boolean algebra that is not atomic. We shall construct it exploiting the correspondence between filters and congruences in Boolean algebras.

Let X be an infinite set. The *Fréchet filter* on $\mathcal{P}(X)$ is the set

$$F := \{Y \subseteq X : Y \text{ is cofinite}\}.$$

Notice that F is a filter of the Boolean algebra $\mathcal{P}(X)$. Then we consider the congruence θ_F of $\mathcal{P}(X)$ associated with F. Clearly, $\mathcal{P}(X)/\theta_F$ is a Boolean algebra. Thus, it only remains to prove that $\mathcal{P}(X)/\theta_F$ is not atomic.

We shall prove a stronger result, namely that $\mathcal{P}(X)/\theta_F$ is *atomless*, i.e., it has no atoms at all. To this end, consider an element $Y/\theta_F \in \mathcal{P}(X)/\theta_F$ different from the minimum $\emptyset/\theta_F$. To show that $Y/\theta_F \in \mathcal{P}(X)$ is not an atom, it suffices to exhibit an element Z/θ_F such that $\emptyset/\theta_F \subsetneq Z/\theta_F \subsetneq Y/\theta_F$. First, notice that $\langle Y, \emptyset\rangle \notin \theta_F$, as $Y/\theta_F \neq \emptyset/\theta_F$. By definition of θ_F, this means that

$$-Y = (-Y \cup \emptyset) \cap (-\emptyset \cup Y) = (Y \to \emptyset) \wedge (\emptyset \to Y) \notin F.$$

By the definition of the Fréchet filter, this means that Y is infinite. Then there exists a set $Z \subseteq Y$ such that both Z and $Y - Z$ are infinite. As $Z \subseteq Y$, we have $Z/\theta_F \subsetneq Y/\theta_F$. Furthermore, from the fact that Z is infinite, it follows that $-Z$ is not cofinite, whence $Z \to \emptyset = -Z \cup \emptyset = -Z \notin F$. As a consequence, $\langle \emptyset, Z\rangle \notin \theta_F$, whence $\emptyset/\theta_F \subsetneq Z/\theta_F$. It only remains to prove that $Z/\theta_F \neq Y/\theta_F$, i.e., $\langle Z, Y\rangle \notin \theta_F$. Observe that the set $Y \to Z$ is not cofinite, because $Y - Z$ is infinite and

$$-(Y \to Z) = -(-Y \cup Z) = Y \cap -Z = Y - Z.$$

Thus, $Y \to Z \notin F$ and, therefore, $\langle Z, Y\rangle \notin \theta_F$.

It only remains to prove that $\mathcal{P}(X)/\theta_F$ is nontrivial. Notice that it suffices to show that $\langle \emptyset, X\rangle \notin \theta_F$. Since X is infinite, the set $X \to \emptyset = -X \cup \emptyset = \emptyset$ is not cofinite, whence it does not belong to F. It follows that $\langle X, \emptyset\rangle \notin \theta_F$, as desired. ⊠

3.5 Ultrafilters and representation

Prime filters in Boolean algebras are called *ultrafilters*. More precisely, we have the following:

Definition 3.38. Let $\boldsymbol{A}$ be a Boolean algebra. A subset $U \subseteq A$ is said to be a *ultrafilter* of $\boldsymbol{A}$ if it is a proper filter of $\boldsymbol{A}$ such that for every $a, c \in A$,

$$\text{if } a \vee c \in U, \text{ then either } a \in F \text{ or } c \in U.$$

In this case, $1 \in U$, as filters on a Boolean algebra are nonempty.

Ultrafilters admit several equivalent descriptions, as we proceed to explain. First, recall from Corollary 3.21(i) that there exists a unique two-element Boolean algebra, namely the chain $\boldsymbol{B}_2$ described in Example 3.7. Bear this in mind, while reading condition (iv) of the next proposition.

Proposition 3.39. *The following conditions are equivalent for a Boolean algebra $\boldsymbol{A}$ and $F \in \mathcal{F}i\boldsymbol{A}$:*

(i) *F is a ultrafilter of $\boldsymbol{A}$;*

(ii) *F is proper and for every $a \in A$, either $a \in F$ or $a^* \in F$;*

(iii) *$\boldsymbol{A}/\theta_F$ is the two-element Boolean algebra;*

(iv) *F is maximal among the proper filters of $\boldsymbol{A}$.*

Proof. (i)⇒(ii): Recall that prime filters are proper, by definition. Consequently, F is also proper. Then consider $a \in A$. As prime filters are nonempty, so is F. In particular, $1 \in F$. Together with the fact that $a \vee a^* = 1$, this yields $a \vee a^* \in F$. Since F is prime, either $a \in F$ or $a^* \in F$.

(ii)⇒(iii): We claim that, for every $a \in A$, either $a \equiv_{\theta_F} 1$ or $a \equiv_{\theta_F} 0$. To prove this, consider $a \in F$. We have two cases: either $a \in F$ or $a^* \in F$. If $a \in F$, then $a \to 1, 1 \to a \in F$, as $a \to 1 = 1$ and $1 \to a = a$. Consequently, $a \equiv_{\theta_F} 1$, by definition of θ_F. If $a^* \in F$, then a similar argument shows that $a^* \equiv_{\theta_F} 1$. As θ_F preserves complements, we conclude that $a = a^{**} \equiv_{\theta_F} 1^* = 0$, whence $a \equiv_{\theta_F} 0$. This establishes the claim.

From the claim it follows that $\boldsymbol{A}/\theta_F$ has at most two elements, namely $0/\theta_F$ and $1/\theta_F$. Thus, conclude the proof, it suffices to show that $0/\theta_F \neq 1/\theta_F$. To this end, notice that $1 \to 0 = 0 \notin F$, as F is a proper upset. Consequently, $\langle 0, 1\rangle \notin \theta_F$, as desired. Hence, we conclude that $\boldsymbol{A}/\theta_F$ is a two-element Boolean algebra.

(iii)⇒(iv): Consider a proper filter G such that $F \subseteq G$. Suppose the contrary, with a view to contradiction. Then there exists some $a \in G \smallsetminus F$. In particular, $1 \to a = a \notin F$, whence $\langle a, 1\rangle \notin \theta_F$. Since $\boldsymbol{A}/\theta_F$ is a two-element Boolean algebra, every element of $\boldsymbol{A}$ belongs either to $1/\theta_F$ or $0/\theta_F$. Together with $\langle a, 1\rangle \notin \theta_F$, this implies $a \equiv_{\theta_F} 0$. Since θ_F preserves complements, $a^* \equiv_{\theta_F} 1$ and, therefore, $1 \to a^* \in F$. Since $a^* = 1 \to a^*$, we conclude that $a^* \in F \subseteq G$. Thus, both a and a^* belong to G. Since G is closed under binary meets, $0 = a \wedge a^* \in G$. But, since G is an upset, this implies $G = A$, a contradiction with the assumption that G is proper.

(iv)⇒(i): Since F is maximal among the proper filters of $\boldsymbol{A}$, it is also meet-irreducible in $\mathcal{F}i\boldsymbol{A}$. As F is nonempty (being a filter of a Boolean algebra), we can apply Proposition 2.36, obtaining that F is prime. ⊠

Corollary 3.40. *The poset* $\mathrm{Prf}\boldsymbol{A}$ *of ultrafilters of a Boolean algebra* $\boldsymbol{A}$ *is discrete, in the sense that its order relation is the identity.*

Proof. Immediate from the fact that the ultrafilters of $\boldsymbol{A}$ coincide with its maximal proper filters by Proposition 3.39. ☒

Recall that not every Boolean algebra is isomorphic to a powerset one. This is because Boolean algebras need not be atomic and complete (cf. Theorem 3.20). However, the next representation theorem states that every Boolean algebra emebeds into a powerset one. As a consequence, for Boolean algebras, meets, joins, and complements can be represented, respectively, as intersections, unions, and set-theoretic complements on a certain fields of sets.

Theorem 3.41 (Stone)**.** *Every Boolean algebra embeds into a powerset one. More precisely, if* $\boldsymbol{A}$ *is a Boolean algebra, then the map*

$$\gamma\colon \boldsymbol{A} \to \mathcal{P}(\mathrm{Prf}\boldsymbol{A}),$$

defined for every $a \in A$ *as*

$$\gamma(a) \coloneqq \{F \in \mathrm{Prf}\boldsymbol{A} : a \in F\},$$

is an embedding.

Proof. Recall from Corollary 3.40 that the order of the poset $\mathrm{Prf}\boldsymbol{A}$ is the identity relation. Consequently, $\mathcal{P}(\mathrm{Prf}\boldsymbol{A}) = \mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$. Because of this, Theorem 2.41 states that the map

$$\gamma\colon \boldsymbol{A} \to \mathcal{P}(\mathrm{Prf}\boldsymbol{A})$$

is an injective map that preserves binary meets and joins. We shall prove that γ preserves the bounds. First, since the ultrafilters of $\boldsymbol{A}$ are proper upsets, they do not contain the minimum element 0. Consequently, $\gamma(0) = \emptyset$. Moreover, as every ultrafilters of $\boldsymbol{A}$ contain 1, we get $\gamma(1) = \mathrm{Prf}\boldsymbol{A}$. Thus, γ is a lattice embedding between Boolean lattices that preserves bounds. From Proposition 3.5 it follows that it is an embedding of Boolean algebras. ☒

Corollary 3.42. *Every Boolean algebra embeds into a direct product of the two-element Boolean algebra* $\boldsymbol{B}_2$*.*

Proof. Consider the map

$$f\colon \boldsymbol{A} \to \prod_{F \in \mathrm{Prf}\boldsymbol{A}} (\boldsymbol{B}_2)_F,$$

defined, for every $a \in A$ and $F \in \mathrm{Prf}\boldsymbol{A}$, as

$$f(a)(F) \coloneqq \begin{cases} 1 & \text{if } a \in F \\ 0 & \text{if } a \notin F. \end{cases}$$

The proof of Theorem 2.47 shows that f is a lattice embedding. Since all ultrafilters of $\boldsymbol{A}$ omit 0 and contain 1, it is easy to see that f preserves also the bounds. By Proposition 3.5, we conclude that f is an embedding of Boolean algebras. ☒

Corollary 3.43. *A Boolean equation is valid in the class of all Boolean algebras if and only if it is valid in* $\boldsymbol{B}_2$*. Consequently, the equational theory of Boolean algebras is decidable.*

Proof. Analogous to the proof of Corollary 2.49. ⊠

In finite Boolean algebras, ultrafilters can be described as follows:

Proposition 3.44. *Let $\boldsymbol{A}$ be a Boolean algebra.*

(i) *A set $F \subseteq A$ is a principal ultrafilter of $\boldsymbol{A}$ if and only if $F = {\uparrow}a$ for some atom $a \in A$;*

(ii) *The ultrafilters of a finite Boolean algebra are precisely the principal filters generated by the atoms.*

Proof. Recall that atoms and join-prime elements coincide in a Boolean algebra. Thus, the statement follows immediately from Proposition 2.34 and Corollary 2.35. ⊠

While in finite Boolean algebras ultrafilters are principal, in infinite Boolean algebras this is not the case. The motivates the following definition:

Definition 3.45. Ultrafilters that are not principal are called *free*.

Definition 3.46. The *generalized Fréchet filter* on a Boolean algebra $\boldsymbol{A}$ is the set

$$F := \{1\} \cup \{a_1^* \wedge \cdots \wedge a_n^* : a_1, \ldots, a_n \text{ are atoms of } \boldsymbol{A}\}.$$

Notice that the generalized Fréchet filter on a powerset Boolean algebra $\mathcal{P}(X)$ coincides with the Fréchet filter defined in Example 3.37.

Proposition 3.47. *The following conditions hold for a ultrafilter U on a Boolean algebra $\boldsymbol{A}$:*

(i) *The generalized Fréchet filter on $\boldsymbol{A}$ is a filter of $\boldsymbol{A}$;*

(ii) *U is free if and only if it extends the generalized Fréchet filter on $\boldsymbol{A}$.*

Proof. (i): Let F be the generalized Fréchet filter on $\boldsymbol{A}$. Notice that F is nonempty and closed under binary meets, by definition. Thus, it only remains to prove that it is an upset. To this end, consider $a, c \in A$ such that $a \in F$ and $a \leqslant c$. If $a = 1$, then $c = 1 \in F$ and we are done. Then suppose that $a \neq 1$. By the definition of F, there are atoms $a_1, \ldots, a_n$ such that

$$a = a_1^* \wedge \cdots \wedge a_n^*.$$

Hence, $a_1^* \wedge \cdots \wedge a_n^* \leqslant c$. Applying Proposition 3.9(iii), double negation elimination, and the De Morgan laws, we obtain

$$c^* \leqslant a_1 \vee \cdots \vee a_n. \tag{3.5}$$

We can assume, without loss of generality, that there is not $X \subsetneq \{a_1, \ldots, a_n\}$ such that $c^* \leqslant \bigvee X$, otherwise we replace $\{a_1, \ldots, a_n\}$ by X. Bearing this in mind, notice that

$$c^* = c^* \wedge (a_1 \vee \cdots \vee a_n) = (c^* \wedge a_1) \vee \cdots \vee (c^* \wedge a_n), \tag{3.6}$$

where the first equality follows from (3.5) and the second from distributivity. As each a_i is an atom, $c^* \wedge a_i \in \{a_i, 0\}$. Notice that if there exists $i \leqslant n$ such that $c^* \wedge a_i = 0$, we would obtain

$$\begin{aligned} c^* &= (c^* \wedge a_1) \vee \cdots \vee (c^* \wedge a_n) \\ &= (c^* \wedge a_1) \vee \ldots (c^* \vee a_{i-1}) \vee (c^* \vee a_{i+1}) \vee \cdots \vee (c^* \wedge a_n) \\ &= c^* \wedge (a_1 \vee \cdots \vee a_{i-1} \vee a_{i+1} \vee \cdots \vee a_n). \end{aligned}$$

This means that $c^* \leqslant a_1 \vee \cdots \vee a_{i-1} \vee a_{i+1} \vee \cdots \vee a_n$, contradicting the assumption of the minimality of $\{a_1, \ldots, a_n\}$. Hence, we conclude that $c^* \wedge a_i = a_i$, for all $i \leqslant n$. By (3.6), this implies

$$a_1 \vee \cdots \vee a_n = c^*.$$

With an application of the De Morgan laws and the double negation elimination, we conclude that

$$c = a_1^* \wedge \cdots \wedge a_n^* = a \in F.$$

(ii): First, let U be a free ultrafilter of $\boldsymbol{A}$. Suppose, with a view to contradiction, that U does not extend the generalized Fréchet ultrafilter on $\boldsymbol{A}$. As $1 \in U$, this implies that there exist atoms $a_1, \ldots, a_n$ such that $a_1^* \wedge \cdots \wedge a_n^* \notin U$. By the De Morgan laws and double negation elimination,

$$(a_1 \vee \cdots \vee a_n)^* = a_1^* \wedge \cdots \wedge a_n^* \notin U$$

Applying condition (ii) of Proposition 3.39, this obtains $a_1 \vee \cdots \vee a_n \in U$. Since U is prime, $a_i \in U$ for some $i \leqslant n$. Now, as U is an upset, this yields $\uparrow a_i \subseteq U$. Furthermore, since a_i is an atom, $\uparrow a_i$ is also a ultrafilter of $\boldsymbol{A}$, by Proposition 3.44(i). Thus U and $\uparrow a_i$ are two comparable ultrafilters of $\boldsymbol{A}$. By Corollary 3.40, we conclude that $U = \uparrow a_i$, a contradiction with the assumption that U is free.

Conversely, let U be a ultrafilter of $\boldsymbol{A}$ that extends the generalized Fréchet filter F on $\boldsymbol{A}$. Then consider an atom $a \in A$. Since $a^* \in F \subseteq U$ and U is proper, we obtain $a \notin U$ (otherwise $0 = a \wedge a^* \in U$). Then U does not contain any atom. By Proposition 3.44(i), we conclude that U is free. ⊠

Corollary 3.48 (Tarski)**.** *Every infinite Boolean algebra has a free ultrafilter.*

Proof. Let $\boldsymbol{A}$ be an infinite Boolean algebra and F the generalized Fréchet filter on it. We begin by proving that F is proper. To this end, it suffices to show that $0 \notin F$. Notice that, since $\boldsymbol{A}$ is nontrivial, $0 \neq 1$. Therefore, by the definition of F, it suffices to show that there are no atoms $a_1, \ldots, a_n$ such that $0 = a_1^* \wedge \cdots \wedge a_n^*$. For suppose the contrary, with a view to contradiction. Then

$$a_1 \vee \cdots \vee a_n = 1.$$

As a consequence, every ultrafilter U of $\boldsymbol{A}$ must contain extend a filter of the form $\uparrow a_i$. Since each $\uparrow a_i$ is an ultrafilter, by Proposition 3.44(i), and ultrafilters are incomparable, by Corollary 3.40, we conclude that $U = \uparrow a_i$. It follows that the only ultrafilters of $\boldsymbol{A}$ are $\uparrow a_1, \ldots, \uparrow a_n$. In particular, $\mathrm{Prf}\boldsymbol{A}$ is finite. It follows that also the lattice $\mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$ is finite. But this contradicts the fact that the lattice reduct of $\boldsymbol{A}$, which is infinite, embeds into $\mathrm{Up}(\mathrm{Prf}\boldsymbol{A})$, by Theorem 2.41. Hence, we conclude that F is proper.

Being a proper filter, F extends to a ultrafilter U by Theorem 2.37. The ultrafilter U is free by Proposition 3.47(ii). ⊠

Notice that the above proof yields the following conclusion:

Corollary 3.49. *A Boolean algebra $\boldsymbol{A}$ is finite if and only if there is a finite set X of atoms such that $\bigvee X = 1$.*

Exercise 3.50. Show that the natural generalization of Corollary 3.48 to distributive lattices fails. More precisely, show that there are infinite distributive lattices in which every prime filter in principal. Hint: counterexamples already occur in the class of chains. ⊠

*Exercise** 3.51. Prove that the unique free ultrafilter on $\mathcal{FC}(X)$, for an infinite set X, is the generalized Fréchet filter. Use this observation to provide a description of all the ultrafilters of $\mathcal{FC}(X)$. ⊠

The above exercise asks you to describe the ultrafilters of $\mathcal{FC}(X)$. It is therefore natural to wonder which are the ultrafilters on $\mathcal{P}(X)$. As it happens, the answer to this question is independent from ZFC (e.g., the existence of the so-called *Ramsey ultrafilters* on $\mathcal{P}(\omega)$ is not decided by ZFC). On the other hand, we shall prove that if X is infinite $\mathcal{P}(X)$ has as many ultrafilters as possible, that is $2^{2^{|X|}}$. To this end, it is convenient to introduce the following notion.

Definition 3.52. Given a set X, a family $Y \subseteq \mathcal{P}(X)$ is said to have the *finite intersection property* (FIP, for short) if $\bigcap Z \neq \emptyset$ for every finite nonempty $Z \subseteq Y$.

In other words, Y has the FIP if $V_1 \cap \cdots \cap V_n \neq \emptyset$, for every $V_1, \ldots, V_n \in Y$.

Lemma 3.53. *Let X be a set and $Y \subseteq \mathcal{P}(X)$ nonempty. Then Y can be extended to a ultrafilter of $\mathcal{P}(X)$ if and only if it has the FIP.*

Proof. If Y can be extended to a ultrafilter U of $\mathcal{P}(X)$, then U has the FIP, because U is a proper upset. Conversely, suppose that Y has the FIP. Then consider the set

$$F := \{Z \in \mathcal{P}(X) : \text{there are } V_1, \ldots, V_n \in Y \text{ such that } Y_1 \cap \cdots \cap Y_n \subseteq Z\}.$$

Clearly, F is a filter of $\mathcal{P}(X)$. Moreover, it is proper, Since Y has the FIP. Lastly, F is nonempty, because $Y \subseteq F$ and $Y \neq \emptyset$, by assumption. As F is a proper nonempty filter of $\mathcal{P}(X)$, we can use Theorem 2.37 to extend it to a ultrafilter. ⊠

We are now ready to prove the desired result on ultrafilters of powerset Boolean algebras:

Proposition 3.54 (Pospíšil)**.** *The following conditions hold:*

(i) *If X is finite, then $\mathcal{P}(X)$ has $|X|$ ultrafilters, namely the principal filters generated by the atoms;*

(ii) *If X is an infinite set, then $\mathcal{P}(X)$ has $2^{2^{|X|}}$ ultrafilters.*

Proof. Condition (i) follows immediately from Proposition 3.44(ii). For (ii), consider the set

$$X^+ := \{\langle Y, Z\rangle : Y \subseteq X \text{ is finite and } Z \subseteq \mathcal{P}(Y)\}.$$

Notice that $|X| = |X^+|$, when $\mathcal{P}(X) \cong \mathcal{P}(X^+)$. Consequently, it suffices to show that $\mathcal{P}(X^+)$ has $2^{2^{|X|}}$ ultrafilters.

To this end, for each $A \subseteq X$, set

$$V_A := \{\langle Y, Z\rangle \in X^+ : A \cap Y \in Z\} \text{ and } -V_A := X^+ - V_A.$$

Furthermore, for each $W \subseteq \mathcal{P}(X)$, we define

$$F_W := \{V_A : A \in W\} \cup \{-V_A : A \in \mathcal{P}(X) - W\}.$$

We shall prove that F_W has the FIP. To this end, consider

$$V_{A_1}, \ldots, V_{A_n}, -V_{B_1}, \ldots, -V_{B_m} \in F_W.$$

For every $i \leqslant n$ and $j \leqslant m$, we choose an element $x_{ij} \in (A_i - B_j) \cup (B_j - A_i)$. This is possible, otherwise $A_i = B_j$, whence $V_{A_i} = V_{B_j}$, contradicting the assumption that $V_{A_i} \in F_W$ and $V_{B_j} \notin F_W$. Then set

$$Y := \{x_{ij} : i \leqslant n \text{ and } j \leqslant m\} \text{ and } Z := \{A_1 \cap Y, \ldots, A_n \cap Y\}.$$

Clearly, $\langle Y, Z\rangle \in V_{A_i}$, for all $i \leqslant n$. Then consider $j \leqslant m$. We have

$$\langle Y, Z\rangle \in V_{B_j} \iff Y \cap B_j \in Z \iff Y \cap B_j = Y \cap A_i, \text{ for some } i \leqslant n. \tag{3.7}$$

But notice that for every $i \leqslant n$,

$$x_{ij} \in Y \cap B_j \iff x_{ij} \notin Y \cap A_i,$$

because $x_{ij} \in Y$ and $x_{ij} \in (A_i - B_j) \cup (B_j - A_i)$. Consequently, $Y \cap B_j \neq Y \cap A_i$, for every $i \leqslant n$. Together with (3.7), this yields $\langle Y, Z\rangle \in -V_{B_j}$, for all $j \leqslant m$. Consequently,

$$\langle Y, Z\rangle \in V_{A_1} \cap \cdots \cap V_{A_n} \cap -V_{B_1} \cap \cdots \cap -V_{B_m}.$$

Hence, we conclude that F_W has the FIP. Furthermore, notice that F_W is nonempty, by definition. Thus, we can apply Lemma 3.53, obtaining that, for every $W \subseteq \mathcal{P}(W)$, the exists a ultrafilter U_W on $\mathcal{P}(X^+)$ that extends F_W.

Now, consider two distinct subsets $W_1, W_2 \subseteq \mathcal{P}(X)$. We can assume, without loss of generality, that there exists $A \in W_1 \smallsetminus W_2$, whence $V_A \in F_{W_1}$ and $-V_A \in F_{W_2}$. Since U_{W_1} is proper (being a ultrafilter) and $V_A \in F_{W_1} \subseteq U_{W_1}$, we get $-V_A \notin U_{W_1}$. As $-V_A \in F_{W_2} \subseteq U_{W_2}$, we conclude that $U_{W_1} \neq U_{W_2}$. Thus,

$$\{U_W : W \subseteq \mathcal{P}(X)\}$$

is a family of ultrafilters of $\mathcal{P}(X^+)$ of cardinality $|\mathcal{P}(\mathcal{P}(X))| = 2^{2^{|X|}}$. As the ultrafilters of $\mathcal{P}(X^+)$ are belong to $\mathcal{P}(\mathcal{P}(X^+))$, there are at most $|\mathcal{P}(\mathcal{P}(X^+))| = 2^{2^{|X^+|}} = 2^{2^{|X|}}$ of them. Thus, we conclude that $\mathcal{P}(X^+)$ has precisely $2^{2^{|X|}}$ ultrafilters, as desired. ⊠

3.6 Classical propositional logic

In this section we shall present an algebraic proof of the completeness theorem of classical propositional logic with respect to the two-element Boolean algebra.

We begin by explaining what is classical propositional logic is, from a purely syntactic point of view. To this end, we rely on an Hilbert-style presentation of it. The

axioms of our calculus are the Boolean terms

$$x \to (y \to x) \tag{Ax1}$$
$$(x \to (y \to z)) \to ((x \to y) \to (x \to z)) \tag{Ax2}$$
$$x \to (x \vee y) \tag{Ax3}$$
$$y \to (x \vee y) \tag{Ax4}$$
$$(x \to z) \to ((y \to z) \to ((x \vee y) \to z)) \tag{Ax5}$$
$$(x \wedge y) \to x \tag{Ax6}$$
$$(x \wedge y) \to y \tag{Ax7}$$
$$(x \to y) \to ((x \to z) \to (x \to (y \wedge z))) \tag{Ax8}$$
$$(x \to y^*) \to (y \to x^*) \tag{Ax9}$$
$$(x \to x)^* \to y \tag{Ax10}$$
$$x \to x \tag{Ax11}$$
$$1 \tag{Ax12}$$
$$0^* \tag{Ax13}$$

where $x \to y$ is a shorthand for $x^* \vee y$, while the only *rule* of our calculus is *modus ponens*, that is,

$$x, x \to y \rhd y.$$

This Hilbert calculus can be viewed as a concise (and indeed finite) presentation of classical propositional logic, as we proceed to explain. To this end, recall that the set T of Boolean terms was defined over a denumerable set of variables $Var = \{x_1, x_2, x_3 \dots\}$.

Definition 3.55. A *substitution* is a map $\sigma\colon Var \to T$. In this case, given a Boolean term $\varphi(x_1, \dots, x_n)$, we set

$$\sigma(\varphi) \coloneqq \varphi(\sigma(x_1), \dots, \sigma(x_n)).$$

Notice that $\sigma(\varphi)$ is still a Boolean term. For instance, if $\varphi = x_4 \vee (x_1 \wedge x_2)^*$ and

$$\sigma(x_1) = x_2 \vee x_3 \qquad \sigma(x_2) = x_1^* \qquad \sigma(x_4) = x_5 \wedge x_1,$$

then

$$\sigma(\varphi) = (x_5 \wedge x_1) \vee ((x_2 \vee x_3) \wedge x_1^*)^*.$$

In the context of logic, Boolean terms are often called *formulas*. Classical propositional logic is a system that tells us when a formula φ is *provable* from a set of formulas Γ. Notably, the suitable notion of "provability" can be defined in terms of the Hilbert calculus described above. More precisely,

Definition 3.56. Let $\Gamma \cup \{\varphi\} \subseteq T$. A *proof* of φ from Γ is a finite sequence $\langle \psi_1, \dots, \psi_n \rangle$ of Boolean terms such that $\psi_n = \varphi$ and for every $m \leqslant n$, one of the following conditions holds:

(i) either ψ_m is a substitution instance of some axiom, i.e., $\psi_m = \sigma(\gamma)$, for some axiom γ and substitution σ;

(ii) or $\psi_m \in \Gamma$;

(iii) or ψ_m is obtained by applying modus ponens to formulas in the initial segment $\langle \psi_1, \dots, \psi_{m-1} \rangle$, i.e., there are $t, k < m$ such that $\psi_t = \psi_k \to \psi_m$.

Accordingly, we say that φ is *provable* from Γ, if there exists a proof of φ from Γ. In this case, we write

$$\Gamma \vdash \varphi.$$

Formally speaking, *classical propositional logic* is the provability relation $\vdash \subseteq \mathcal{P}(T) \times T$.

The completeness theorem of classical propositional logic states that $\vdash$ coincides with another relation $\models$, defined semantically in terms of truth values of formulas (i.e., Boolean terms). To clarify this point, given a Boolean algebra $\boldsymbol{A}$, a sequence $\vec{a} \in A^\omega$ (that is, a sequence $\vec{a} = \{a_n : n \in \omega\} \subseteq A$), and a Boolean term $\varphi(x_{n_1}, \dots, x_{n_k})$, we set

$$\varphi^{\boldsymbol{A}}(\vec{a}) := \varphi^{\boldsymbol{A}}(a_{n_1}, \dots, a_{n_k}).$$

If one regards the elements of the algebras $\boldsymbol{A}$ as ordered truth values, where the minimum 0 represents absolute falsity, the maximum 1 absolute truth, then $\varphi^{\boldsymbol{A}}(\vec{a})$ can be viewed as the truth value of the formula φ in under the interpretation $\vec{a}$. This reading becomes more tangible when $\boldsymbol{A}$ is the two-element Boolean algebra $\boldsymbol{B}_2$ with universe $\{0, 1\}$ and, therefore, the only truth values available are absolute truth and absolute falsity. From this point of view, the relation $\Gamma \models \varphi$ defined below can be read as "if the premises in Γ are true, then the conclusion φ is also true".

Definition 3.57. Let $\models \subseteq \mathcal{P}(T) \times T$ be the relation defined as follows: for every $\Gamma \cup \{\varphi\} \subseteq T$,

$$\Gamma \models \varphi \iff \text{for every } \vec{a} \subseteq \{0,1\}^\omega, (\text{if } \gamma^{\boldsymbol{B}_2}(\vec{a}) = 1 \text{ for all } \gamma \in \Gamma, \text{ then } \varphi^{\boldsymbol{B}_2}(\vec{a}) = 1).$$

The completeness theorem of classical propositional logic states that the syntactic and the semantic consequences $\vdash$ and $\models$ coincide:

Theorem 3.58 (Completeness)**.** *For every $\Gamma \cup \{\varphi\} \subseteq T$,*

$$\Gamma \vdash \varphi \iff \Gamma \models \varphi.$$

The proof of the implication from left to right depends on the next two lemmas.

Lemma 3.59. *If φ is an axiom of the calculus, then the equation $\varphi \approx 1$ holds in every Boolean algebra.*

Proof. Let $\boldsymbol{A}$ be a Boolean algebra. We need to show that $\varphi^{\boldsymbol{A}}(\vec{a}) = 1$, for all $\vec{a} \in A^\omega$. As an exemplification, we detail the case where φ is the second axiom $(x \to (y \to z)) \to ((x \to y) \to (x \to z))$. To this end, consider $a, b, c \in A$. By the residuation law,

$$a \wedge (a \to (b \wedge (b \to c)) \leqslant b \wedge (b \to c) \text{ and } b \wedge (b \to c) \leqslant c,$$

whence $a \wedge (a \to (b \wedge (b \to c)) \leqslant c$. Again by residuation,

$$(a \to (b \wedge (b \to c)) \leqslant a \to c. \tag{3.8}$$

Moreover,

$$\begin{aligned} a \to (b \wedge (b \to c)) &= a^* \vee (b \wedge (b^* \vee c)) \\ &= (a^* \vee b) \wedge (a^* \vee (b^* \vee c)) \\ &= (a \to b) \wedge (a \to (b \to c)) \\ &= 1 \wedge (a \to b) \wedge (a \to (b \to c)). \end{aligned}$$

The equalities above are obtained as follows. The first and the third follow from the definition of the implication, the second from distributivity, and the fourth from the fact that 1 is the maximum.

Together with (3.8), this yields

$$1 \wedge (a \to b) \wedge (a \to (b \to c)) \leqslant a \to c.$$

By applying the residuation law a number of times, we obtain

$$1 \leqslant (a \to (b \to c)) \to ((a \to b) \to (a \to c)),$$

whence $(a \to (b \to c)) \to ((a \to b) \to (a \to c)) = 1$, as desired. ⊠

Lemma 3.60. *For every Boolean algebra* $\mathbf{A}$ *and* $a, c \in A$,

$$\text{if } a = a \to c = 1, \text{ then } c = 1.$$

Proof. From $a = a \to c = 1$ it follows $1 \leqslant a \to c$. By the residuation law, we obtain $a \leqslant c$. Together with $a = 1$, this implies $c = 1$. ⊠

Proposition 3.61 (Soundness)**.** *For every* $\Gamma \cup \{\varphi\} \subseteq T$,

$$\text{if } \Gamma \vdash \varphi, \text{ then } \Gamma \vDash \varphi.$$

Proof. Consider $\Gamma \cup \{\varphi\} \subseteq T$ and suppose that $\Gamma \vdash \varphi$. Then there exists a proof $\langle \psi_1, \ldots, \psi_n \rangle$ of φ from Γ. We claim that $\Gamma \vDash \psi_m$, for every $m \leqslant n$. To prove this, we reason by complete induction on m, that is, we assume that $\Gamma \vDash \psi_k$, for all $k < m$, and we prove that $\Gamma \vDash \psi_m$.

Since $\langle \psi_1, \ldots, \psi_n \rangle$ is a proof of φ from Γ, the initial segment $\langle \psi_1, \ldots, \psi_m \rangle$ is a proof of ψ_m from Γ. By the definition of a proof, we have the following cases:

(i) either ψ_m is a substitution instance of some axiom, i.e., $\psi_m = \sigma(\gamma)$, for some axiom γ and substitution σ;

(ii) or $\psi_m \in \Gamma$;

(iii) or ψ_m is obtained by applying modus ponens to formulas in the initial segment $\langle \psi_1, \ldots, \psi_{m-1} \rangle$, i.e., there are $k, i < m$ such that $\psi_i = \psi_k \to \psi_m$.

We handle these cases separately.

(i): In this case, let $\gamma = \gamma(x_{p_1}, \ldots, x_{p_j})$ and consider the Boolean terms $\delta_1, \ldots, \delta_j$ such that $\sigma(x_{p_1}) = \delta_1, \ldots, \sigma(x_{p_j}) = \delta_j$. Moreover, consider a sequence $\vec{a} \in \{0,1\}^\omega$. We have

$$\psi_m^{\mathbf{B}_2}(\vec{a}) = \sigma(\gamma)^{\mathbf{B}_2}(\vec{a}) = \gamma(\delta_1, \ldots, \delta_j)^{\mathbf{B}_2}(\vec{a}) = \gamma^{\mathbf{B}_2}(\delta_1^{\mathbf{B}_2}(\vec{a}), \ldots, \delta_j^{\mathbf{B}_2}(\vec{a})) = 1.$$

The only obvious step in the above series of equalities is the last one, which follows from Lemma 3.59. Hence, we conclude that $\emptyset \vDash \psi_m$ and, therefore, that $\Gamma \vDash \psi_m$.

(ii): In this case, $\Gamma \vDash \psi_m$ vacuously.

(iii): By the inductive hypothesis, $\Gamma \vDash \psi_k \to \psi_m$ and $\Gamma \vDash \psi_k$. Then consider a sequence $\vec{a} \in \{0,1\}^\omega$ such that $\gamma^{\mathbf{B}_2}(\vec{a}) = 1$, for all $\gamma \in \Gamma$. Since $\Gamma \vDash \psi_k \to \psi_m$ and $\Gamma \vDash \psi_k$, we obtain

$$(\psi_k \to \psi_m)^{\mathbf{B}_2}(\vec{a}) = 1 = \psi_k^{\mathbf{B}_2}(\vec{a}).$$

By Lemma 3.60, we obtain that $\psi_m^{\mathbf{B}_2}(\vec{a}) = 1$. Hence, we conclude that $\Gamma \vDash \psi_m$, as desired.

This conclude the inductive proof. Since $\psi_n = \varphi$, we obtain $\Gamma \vDash \varphi$. ⊠

The proof of the implication from right to left in Theorem 3.58 is more interesting and relies on properties of ultrafilters in Boolean algebras. We begin by associating an equivalence relation $\equiv_\Gamma$ with every set of term Γ, as follows:

Definition 3.62. Given $\Gamma \subseteq T$, let $\equiv_\Gamma$ be the binary relation on T defined, for every $\varphi, \psi \in T$, as follows:

$$\varphi \equiv_\Gamma \psi \iff (\Gamma \vdash \varphi \to \psi \text{ and } \Gamma \vdash \psi \to \varphi).$$

Intuitively, the relation $\equiv_\Gamma$ should be read as "the formulas φ and ψ are logically equivalent modulo Γ". Notably, $\equiv_\Gamma$ is an equivalence relation that respects the function symbols. More precisely,

Lemma 3.63. *For every $\Gamma \subseteq T$, $\equiv_\Gamma$ is an equivalence relation that preserves $\wedge, \vee, (\cdot)^*$, in the sense that, for every $\varphi_1, \varphi_2, \psi_1, \psi_2 \in T$ such that $\varphi_1 \equiv_\Gamma \varphi_2$ and $\psi_1 \equiv_\Gamma \psi_2$,*

$$\varphi_1 \wedge \psi_1 \equiv_\Gamma \varphi_2 \wedge \psi_2 \qquad \varphi_1 \vee \psi_1 \equiv_\Gamma \varphi_2 \vee \psi_2 \qquad \varphi_1^* \equiv_\Gamma \varphi_2^*.$$

Proof. This proof is based on a series of routine (and tedious) proofs in the sense of Definition 3.56. While going through all the cases would not be very enlightening, still understand how a couple of them work might help to grasp what is going on. Because of this we detail the proof of the fact that $\equiv_\Gamma$ is an equivalence relation.

To this end, consider a Boolean term φ. Since $\varphi \to \varphi$ is a substitution instance of axiom (Ax11), we conclude $\Gamma \vdash \varphi \to \varphi$, that is, $\varphi \equiv_\Gamma \varphi$. Hence, the relation $\equiv_\Gamma$ is reflexive. The fact that it is symmetric follows immediately from its definition. To prove that it is transitive, consider $\varphi, \psi, \gamma \in T$ such that $\varphi \equiv_\Gamma \psi$ and $\psi \equiv_\Gamma \gamma$. In order to prove $\varphi \equiv_\Gamma \gamma$, we need to show that

$$\Gamma \vdash \varphi \to \gamma \text{ and } \Gamma \vdash \gamma \to \varphi.$$

We detail the proof that $\Gamma \vdash \varphi \to \gamma$, as that of $\Gamma \vdash \gamma \to \varphi$ is analogous. To this end, notice that the following is a substitution instances of axiom (Ax1):

$$(\psi \to \gamma) \to (\varphi \to (\psi \to \gamma)).$$

Since $\psi \equiv_\Gamma \gamma$, we have $\Gamma \vdash \psi \to \gamma$. By modus ponens,

$$\Gamma \vdash \varphi \to (\psi \to \gamma).$$

Now, consider the following substitution instance of axiom (Ax2):

$$(\varphi \to (\psi \to \gamma)) \to ((\varphi \to \psi) \to (\varphi \to \gamma)).$$

Applying modus ponens to the two displays above, we obtain

$$\Gamma \vdash (\varphi \to \psi) \to (\varphi \to \gamma).$$

Furthermore, from $\varphi \equiv_\Gamma \psi$ it follows $\Gamma \vdash \varphi \to \psi$. Therefore, by modus ponens, we obtain $\Gamma \vdash \varphi \to \gamma$, as desired. A similar proof yields $\Gamma \vdash \gamma \to \varphi$, whence $\varphi \equiv_\Gamma \gamma$. We conclude that $\equiv_\Gamma$ is transitive and, therefore, an equivalence relation. ⊠

Let $\Gamma \subseteq T$. In view of Lemma 3.63, $\equiv_\Gamma$ is an equivalence relation on T, whence we can consider the quotient set $T/\equiv_\Gamma$. We endow it with the structure of an algebra

$$T/\equiv_\Gamma := \langle T/\equiv_\Gamma; \wedge, \vee, (\cdot)^*, 0, 1\rangle,$$

whose operations are defined, for every $\varphi, \psi \in T$, as follows:

$$\begin{aligned}
\varphi/\equiv_\Gamma \wedge^{T/\equiv_\Gamma} \psi/\equiv_\Gamma &:= (\varphi \wedge \psi)/\equiv_\Gamma \\
\varphi/\equiv_\Gamma \vee^{T/\equiv_\Gamma} \psi/\equiv_\Gamma &:= (\varphi \vee \psi)/\equiv_\Gamma \\
(\varphi/\equiv_\Gamma)^{*T/\equiv_\Gamma} &:= \varphi^*/\equiv_\Gamma \\
1^{T/\equiv_\Gamma} &:= 1/\equiv_\Gamma \\
0^{T/\equiv_\Gamma} &:= 0/\equiv_\Gamma .
\end{aligned}$$

Notice that the operations of $T/\equiv_\Gamma$ are well-defined, because $\equiv_\Gamma$ preserves the operations, by Lemma 3.63. Accordingly, we stipulate the following:

Definition 3.64. Given $\Gamma \subseteq T$, the structure $T/\equiv_\Gamma$ is called the *Lindenbaum-Tarski algebra* of Γ.

It turns out that the Lindenbaum-Tarski algebra is always a Boolean algebra.

Proposition 3.65. *The following conditions hold.*

(i) *The Lindenbaum-Tarski algebra $T/\equiv_\Gamma$ is a Boolean algebra, for every $\Gamma \subseteq T$.*

(ii) *For every $\Gamma \cup \{\varphi\} \subseteq T$, if $\Gamma \nvdash \varphi$, then there exists $\vec{a} \in (T/\equiv_\Gamma)^\omega$ such that*

$$\gamma^{T/\equiv_\Gamma}(\vec{a}) = 1, \text{ for all } \gamma \in \Gamma, \text{ and } \varphi^{T/\equiv_\Gamma}(\vec{a}) \neq 1.$$

Proof. (i): We need to check that the equations in the definition of a Boolean algebra are valid in $T/\equiv_\Gamma$. To this end, we need to prove that for every equation $\varphi \approx \psi$ in the definition of a Boolean algebra, $T/\equiv_\Gamma \vDash \varphi \approx \psi$. This means precisely, that for every $\delta_1, \ldots, \delta_n \in T$,

$$\begin{aligned}
\Gamma &\vdash \varphi(\delta_1, \ldots, \delta_n) \to \psi(\delta_1, \ldots, \delta_n) \\
\Gamma &\vdash \psi(\delta_1, \ldots, \delta_n) \to \varphi(\delta_1, \ldots, \delta_n).
\end{aligned}$$

Again, this is a routine computation and we omit the tedious details.

(ii): Suppose that $\Gamma \nvdash \varphi$. We claim that

(i) $1 \equiv_\Gamma \gamma$, for every $\gamma \in \Gamma$; and

(ii) $1 \not\equiv_\Gamma \varphi$.

(i): Consider $\gamma \in \Gamma$ and observe that, vacuously, $\Gamma \vdash \gamma$. Now, two substitution instances of axiom (Ax1) are $\gamma \to (1 \to \gamma)$ and $1 \to (\gamma \to 1)$. Applying modus ponens to $\Gamma \vdash \gamma$ and the axiom instance $\gamma \to (1 \to \gamma)$, we obtain $\Gamma \vdash 1 \to \gamma$. Since $\Gamma \vdash 1$, by axiom (Ax12), a similar argument (which replaces $\gamma \to (1 \to \gamma)$ by $1 \to (\gamma \to 1)$) yields $\Gamma \vdash \gamma \to 1$. Hence,

$$\Gamma \vdash 1 \to \gamma \text{ and } \Gamma \vdash \gamma \to 1,$$

that is, $1 \equiv_\Gamma \gamma$.

(ii): By definition of $\equiv_\Gamma$, it suffices to show that $\Gamma \nvdash 1 \to \varphi$. Then suppose, with a view to contradiction, that $\Gamma \vdash 1 \to \varphi$. By axiom (Ax12) and modus ponens, we conclude that $\Gamma \vdash \varphi$, a contradiction. This establishes the claim.

Now, consider the sequence $\vec{a} = \{x_n/\equiv_\Gamma : n \in \omega\}$ of ω elements of the Boolean algebra $T/\equiv_\Gamma$. Consider $\gamma(x_{n_1}, \dots, x_{n_k}) \in \Gamma$. We have

$$\begin{aligned}
\gamma^{T/\equiv_\Gamma}(\vec{a}) &= \gamma^{T/\equiv_\Gamma}(x_{n_1}/\equiv_\Gamma, \dots, x_{n_k}/\equiv_\Gamma) \\
&= \gamma(x_{n_1}, \dots, x_{n_k})/\equiv_\Gamma \\
&= \gamma/\equiv_\Gamma \\
&= 1/\equiv_\Gamma \\
&= 1^{T/\equiv_\Gamma}.
\end{aligned}$$

The only nonobvious equality above is the second to last, which is a consequence of (i). Similarly, let $\varphi = \varphi(x_{m_1}, \dots, x_{m_k})$. Then

$$\begin{aligned}
\varphi^{T/\equiv_\Gamma}(\vec{a}) &= \varphi^{T/\equiv_\Gamma}(x_{m_1}/\equiv_\Gamma, \dots, x_{m_k}/\equiv_\Gamma) \\
&= \varphi(x_{m_1}, \dots, x_{m_k})/\equiv_\Gamma \\
&= \varphi/\equiv_\Gamma \\
&\neq 1/\equiv_\Gamma \\
&= 1^{T/\equiv_\Gamma}.
\end{aligned}$$

Againm the only nonobvious equality above is the second to last, which is a consequence of (ii). ⊠

Corollary 3.66. *Let $\Gamma \cup \{\varphi\} \subseteq T$ be such that $\Gamma \nvdash \varphi$. Then there exists a Boolean algebra $\boldsymbol{A}$ and $\vec{a} \in A^\omega$ such that*

$$\gamma^{\boldsymbol{A}}(\vec{a}) = 1, \textit{ for all } \gamma \in \Gamma, \textit{ and } \varphi^{\boldsymbol{A}}(\vec{a}) \neq 1.$$

The following result, which relies on the Prime Filter Theorem 2.37, completes the proof of the implication from right to left in Theorem 3.58.

Proposition 3.67 (Completeness)**.** *For every $\Gamma \cup \{\varphi\} \subseteq T$,*

$$\textit{if } \Gamma \vDash \varphi, \textit{ then } \Gamma \vdash \varphi.$$

Proof. We reason by contraposition. Accordingly, suppose that $\Gamma \nvdash \varphi$. In view of Corollary 3.66, there exists a Boolean algebra $\boldsymbol{A}$ and $\vec{a} \in A^\omega$ such that

$$\gamma^{\boldsymbol{A}}(\vec{a}) = 1, \text{ for all } \gamma \in \Gamma, \text{ and } \varphi^{\boldsymbol{A}}(\vec{a}) \neq 1.$$

As $\varphi^{\boldsymbol{A}}(\vec{a}) \neq 1$ and 1 is the maximum, we get $1 \nleqslant \varphi^{\boldsymbol{A}}(\vec{a})$. By Corollary 2.38, there exists a ultrafilter F of $\boldsymbol{A}$ such that $\varphi^{\boldsymbol{A}}(\vec{a}) \notin F$. As F is a nonempty upset, $1 \in F$, we obtain

$$\gamma^{\boldsymbol{A}}(\vec{a}) \in F, \text{ for all } \gamma \in \Gamma, \text{ and } \varphi^{\boldsymbol{A}}(\vec{a}) \notin F. \tag{3.9}$$

Now, consider the congruence θ_F of $\boldsymbol{A}$ associated with the ultrafilter F. Recall from Proposition 3.39 that $\boldsymbol{A}/\theta_F$ is the two-element Boolean algebra. Moreover, consider the sequence

$$\vec{c} := \{a_n/\theta_F : n \in \omega\} \subseteq (A/\theta_F)^{\omega}.$$

For every $\psi(x_{n_1}, \ldots, x_{n_k}) \in T$, we have

$$\begin{aligned}
\psi^{\boldsymbol{A}/\theta_F}(\vec{c}) = 1^{\boldsymbol{A}/\theta_F} &\iff \psi^{\boldsymbol{A}/\theta_F}(a_{n_1}/\theta_F, \ldots, a_{n_k}/\theta_F) = 1^{\boldsymbol{A}/\theta_F} \\
&\iff \psi^{\boldsymbol{A}}(a_{n_1}, \ldots, a_{n_k})/\theta_F = 1^{\boldsymbol{A}}/\theta_F \\
&\iff \psi^{\boldsymbol{A}}(a_{n_1}, \ldots, a_{n_k}) \equiv_{\theta_F} 1 \\
&\iff \psi^{\boldsymbol{A}}(\vec{a}) \to 1, 1 \to \psi^{\boldsymbol{A}}(\vec{a}) \in F \\
&\iff 1, \psi^{\boldsymbol{A}}(\vec{a}) \in F \\
&\iff \psi^{\boldsymbol{A}}(\vec{a}) \in F.
\end{aligned}$$

The equivalences above are justified as follows. The first three are obvious. The fourth follows from the definition of θ_F, the fifth from the fact that

$$\psi^{\boldsymbol{A}}(\vec{a}) \to 1 = \psi^{\boldsymbol{A}}(\vec{a})^* \vee 1 = 1 \text{ and } 1 \to \psi^{\boldsymbol{A}}(\vec{a}) = 1^* \vee \psi^{\boldsymbol{A}}(\vec{a}) = 0 \vee \psi^{\boldsymbol{A}}(\vec{a}) = \psi^{\boldsymbol{A}}(\vec{a}),$$

and the last one from $1 \in F$.

Together with (3.9), the above series of equivalences yields

$$\gamma^{\boldsymbol{A}/\theta_F}(\vec{c}) = 1^{\boldsymbol{A}/\theta_F}, \text{ for all } \gamma \in \Gamma, \text{ and } \varphi^{\boldsymbol{A}/\theta_F}(\vec{c}) \neq 1^{\boldsymbol{A}/\theta_F}.$$

Since $\boldsymbol{A}/\theta_F$ is the two-element Boolean algebra, we conclude $\Gamma \nvDash \varphi$. ⊠

One of the consequences of the Completenss Theorem 3.58 is the following:

Corollary 3.68. *Classical propositional logic is decidable, in the sense that the problem of determining whether $\Gamma \vdash \varphi$, for finite sets of Boolean terms $\Gamma \cup \{\varphi\}$, is decidable.*

Proof. Consider a finite set of Boolean terms $\Gamma \cup \{\varphi\}$. In view of the Completenss Theorem 3.58, $\Gamma \vdash \varphi$ if and only if $\Gamma \vDash \varphi$. Since $\vDash$ is defined in terms of a finite algebra (namely the two-element Boolean algebra) and only a finite number of variables occurs in $\Gamma \cup \{\varphi\}$, it is possible to check mechanically whether $\Gamma \vDash \varphi$. ⊠

3.7 Atomless Boolean algebras

A Boolean algebra is said to be *atomless* if it has no atoms. We described a series of infinite atomless Boolean algebras in Example 3.37. In relation to this, one might wonder whether finite Boolean algebras exist. The answer is essentially negative, as we proceed to explain.

Proposition 3.69. *The only finite atomless Boolean algebra is the trivial one.*

Proof. The trivial Boolean algebra is atomless, because, by definition, atoms must be strictly greater than the minimum. Therefore, it only remains to prove that every finite nontrivial Boolean algebra has at least one atom. To this end, consider a finite nontrivial Boolean algebra $\boldsymbol{A}$. By Corollary 3.21, there exists a nonempty finite set X such that $\boldsymbol{A} \cong \mathcal{P}(X)$. Accordingly, consider $x \in X$. The element $\{x\}$ is an atom of $\mathcal{P}(X)$, whence $\mathcal{P}(X)$ is not atomless. Since $\boldsymbol{A} \cong \mathcal{P}(X)$, the same holds for $\boldsymbol{A}$. ⊠

As a consequence, interesting examples of atomless Boolean algebras are necessarily infinite. Accordingly, the aim of this section is to prove the following classical result:

Theorem 3.70 (Tarski)**.** *Up to isomorphism, there is a unique denumerable atomless Boolean algebra.*

In Model Theory, this result is usually phrased stating that the theory of atomless Boolean algebras is *ω-categorical*, that is, has only one model of cardinality ω. Even if we shall not prove this, the above theorem fails for every uncountable cardinality.

Before we move to the proof of the main result, we review a few other constructions of atomless Boolean algebras. The first one is based on Lindenbaum-Tarski algebras. More precisely, for every infinite cardinal κ, consider a set of variables

$$Var_\kappa := \{x_\alpha : \alpha < \kappa\}.$$

We denote by T_κ the set of formulas obtained using Var_κ as a set of variables. More precisely, T_κ is the least set such that

(i) $Var_\kappa \cup \{0, 1\} \subseteq T_\kappa$; and

(ii) if $\varphi, \psi \in T_\kappa$, then $\varphi \wedge \psi, \varphi \vee \psi, \varphi^* \in T_\kappa$.

Notice that, in this terminology, $T_{\aleph_0} = T$.

Accordingly, given a Boolean algebra $\boldsymbol{A}$, a sequence $\vec{a} \in A^\kappa$ (that is, a sequence $\vec{a} = \{a_\alpha : \alpha < \kappa\} \subseteq A$), and a formula $\varphi(x_{\alpha_1}, \dots, x_{\alpha_k}) \in T_\kappa$, we set

$$\varphi^{\boldsymbol{A}}(\vec{a}) := \varphi^{\boldsymbol{A}}(a_{\alpha_1}, \dots, a_{\alpha_k}).$$

Then we extend classical propositional logic to formulas in T_κ, by defining a relation $\vdash_\kappa \subseteq \mathcal{P}(T_\kappa) \times T_\kappa$ as follows:

$$\begin{aligned} \Gamma \vdash_\kappa \varphi \iff & \text{for every } \vec{a} = \{a_\alpha : \alpha < \kappa\} \subseteq \{0, 1\}^\kappa, \\ & \text{if } \gamma^{\boldsymbol{B}_2}(\vec{a}) = 1, \text{ for all } \gamma \in \Gamma, \text{ then } \varphi^{\boldsymbol{B}_2}(\vec{a}) = 1. \end{aligned}$$

Notice that, by the Completeness Theorem 3.58, $\vdash_{\aleph_0}$ coincides with classical propositional logic $\vdash$.

As in the previous section, given $\Gamma \subseteq T_\kappa$, we define a binary relation $\equiv_\Gamma$ on T_κ as follows:

$$\varphi \equiv_\Gamma \psi \iff (\Gamma \vdash_\kappa \varphi \to \psi \text{ and } \Gamma \vdash_\kappa \psi \to \varphi),$$

for every $\varphi, \psi \in T_\kappa$. A routine argument shows that $\equiv_\Gamma$ is an equivalence relation on T_κ that preserves the connectives $\wedge, \vee$, and $(\cdot)^*$. As a consequence, we can endow T_κ with the structure of an algebra

$$T_\kappa / \equiv_\Gamma := \langle T_\kappa / \equiv_\Gamma; \wedge, \vee, (\cdot)^*, 0, 1 \rangle,$$

whose operations are defined, for every $\varphi, \psi \in T_\kappa$, as follows:

$$\begin{aligned}
\varphi/\equiv_\Gamma \wedge^{T_\kappa/\equiv_\Gamma} \psi/\equiv_\Gamma &:= (\varphi \wedge \psi)/\equiv_\Gamma \\
\varphi/\equiv_\Gamma \vee^{T_\kappa/\equiv_\Gamma} \psi/\equiv_\Gamma &:= (\varphi \vee \psi)/\equiv_\Gamma \\
(\varphi/\equiv_\Gamma)^{*T_\kappa/\equiv_\Gamma} &:= \varphi^*/\equiv_\Gamma \\
1^{T_\kappa/\equiv_\Gamma} &:= 1/\equiv_\Gamma \\
0^{T_\kappa/\equiv_\Gamma} &:= 0/\equiv_\Gamma .
\end{aligned}$$

A proof similar to the one of Proposition 3.65 shows that

Proposition 3.71. *For every infinite cardinal κ and $\Gamma \subseteq T_\kappa$, the structure $T_\kappa/\equiv_\Gamma$ is Boolean algebra.*

More interestingly, for the present purpose, is the observation that algebras of the form $T_\kappa/\equiv_\emptyset$ are atomless.

Proposition 3.72. *For every infinite cardinal κ, the Boolean algebra $T_\kappa/\equiv_\emptyset$ is atomless and of cardinality κ.*

Proof. We begin by proving that $T_\kappa/\equiv_\emptyset$ is atomless. Suppose the contrary, with a view to contradiction. Then $T_\kappa/\equiv_\emptyset$ has an atom $\varphi/\equiv_\emptyset$, for some $\varphi = \varphi(x_{\alpha_1}, \dots, x_{\alpha_n})$. As $\varphi/\equiv_\emptyset$ is an atom, $0/\equiv_\emptyset \neq \varphi/\equiv_\emptyset$. By the definition of $\equiv_\emptyset$, this means that

$$\text{either } \emptyset \nvdash_\kappa \varphi \to 0 \text{ or } \emptyset \nvdash_\kappa 0 \to \varphi. \tag{3.10}$$

We shall prove that $\emptyset \vdash_\kappa 0 \to \varphi$. To this end, consider $a_{\alpha_1}, \dots, a_{\alpha_n} \in \{0, 1\}$. In $\boldsymbol{B}_2$, we have

$$0 \to \varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) = 0^* \vee \varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) = 1 \vee \varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) = 1.$$

By definition of $\vdash_k$, this yields $\emptyset \vdash_\kappa 0 \to \varphi$, as desired. By (3.10), we conclude that $\emptyset \nvdash_\kappa \varphi \to 0$. This means that there are $a_{\alpha_1}, \dots, a_{\alpha_n} \in \{0, 1\}$ such that, in $\boldsymbol{B}_2$,

$$\varphi(a_{\alpha_1}, \dots, a_{\alpha_n})^* = \varphi(a_{\alpha_1}, \dots, a_{\alpha_n})^* \vee 0 = \varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) \to 0 \neq 1.$$

Since $\varphi(a_{\alpha_1}, \dots, a_{\alpha_n})^* \in B_2 = \{0, 1\}$, this implies $\varphi(a_{\alpha_1}, \dots, a_{\alpha_n})^* = 0$, whence

$$\varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) = 1. \tag{3.11}$$

Now, consider a variable $y \in Var_\kappa \smallsetminus \{x_{\alpha_1}, \dots, x_{\alpha_n}\}$. Since $\varphi/\equiv_\emptyset$ is an atom,

$$\text{either } \varphi/\equiv_\emptyset \leqslant y/\equiv_\emptyset \text{ or } \varphi/\equiv_\emptyset \wedge\, y/\equiv_\emptyset = 0/\equiv_\emptyset.$$

Accordingly, either $(\varphi \vee y)/\equiv_\emptyset = y/\equiv_\emptyset$ or $(\varphi \wedge y)/\equiv_\emptyset = 0/\equiv_\emptyset$. From the definition of $\equiv_\emptyset$, this yields

$$\text{either } \emptyset \vdash_\kappa (\varphi \vee y) \to y \text{ or } \emptyset \vdash_\kappa (\varphi \wedge y) \to 0. \tag{3.12}$$

Now, notice that in $\boldsymbol{B}_2$ we have

$$(\varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) \vee 0) \to 0 = (1 \vee 0) \to 0 = 1 \to 0 = 1^* \vee 0 = 0 \vee 0 = 0.$$

The first equality above follows from (3.11), while the others are straightforward. Hence, we conclude that $\emptyset \nvdash_\kappa (\varphi \vee y) \to y$. By (3.12), this yields $\emptyset \vdash_\kappa (\varphi \wedge y) \to 0$. As a consequence, in $\boldsymbol{B}_2$ we have

$$1 = (\varphi(a_{\alpha_1}, \dots, a_{\alpha_n}) \wedge 1) \to 0 = (1 \wedge 1) \to 0 = 1 \to 0 = 1^* \vee 0 = 0 \vee 0 = 0.$$

The above equalities are justified as follows. The first follows from $\emptyset \vdash_\kappa (\varphi \wedge y) \to 0$, the second from (3.11), and the others are straightforward. The above display implies $0 = 1$, which is false. Hence, we reached the desired contradiction. We conclude that the Boolean algebra $T_\kappa / \equiv_\emptyset$ is atomless.

Now, we turn to prove that $T_\kappa / \equiv_\emptyset$ has cardinality κ. To this end, observe that, by construction, $|T_\kappa| = \kappa$. As a consequence, $|T_\kappa / \equiv_\emptyset| \leqslant \kappa$. Thus, it suffices to construct κ distinct elements of $T_\kappa / \equiv_\emptyset$. Consider two distinct $\alpha, \beta < \kappa$. It is easy to see that $\emptyset \nvdash x_\alpha \to x_\beta$. By definition of $\equiv_\emptyset$, this yields $x_\alpha / \equiv_\emptyset \neq x_\beta / \equiv_\emptyset$. We conclude that the elements in $\{x_\alpha / \equiv_\emptyset : \alpha < \kappa\}$ are all different, as desired. ⊠

Corollary 3.73. *$T / \equiv_\emptyset$ is a denumerable atomless Boolean algebra.*

Another family of atomless Boolean algebras, can be constructed as follows. Given a chain $\mathbb{X}$ and $x \in X$, we set

$$(-\infty, x) := (\downarrow x) \smallsetminus x.$$

Then let $\boldsymbol{B}(\mathbb{X})$ be the subalgebra of the powerset Boolean algebra $\mathcal{P}(X)$ generated by the elements in the following set

$$\{(-\infty, x) : x \in X\}.$$

Notice that, if $\mathbb{X}$ is infinite, $\boldsymbol{B}(\mathbb{X})$ has cardinality $|X|$.

Proposition 3.74. *Let $\mathbb{X}$ an infinite dense chain without a maximum. Then the Boolean algebra $\boldsymbol{B}(\mathbb{X})$ is an atomless and of cardinality $|X|$.*

Proof. We already know that $\boldsymbol{B}(\mathbb{X})$ is a Boolean algebra of cardinality $|X|$. Therefore, it only remains to prove that $\boldsymbol{B}(\mathbb{X})$ is atomless. To this end, consider an element a of $\boldsymbol{B}(\mathbb{X})$ different from $\emptyset$. By Theorem 3.12, there $c_1, \dots, c_n \in X$ and a Boolean term $\varphi(x_1, \dots, x_n)$ in conjunctive normal form such that

$$\varphi^{\boldsymbol{B}(\mathbb{X})}((-\infty, c_1), \dots, (-\infty, c_n)) = a.$$

Since φ is in CNF, there are

$$\begin{aligned} V_1, \dots, V_k &\subseteq \{(-\infty, c_1), \dots, (-\infty, c_n), (-\infty, c_1)^*, \dots, (-\infty, c_n)^*\} \\ &= \{(-\infty, c_1), \dots, (-\infty, c_n), \uparrow^{\mathbb{X}} c_1, \dots, \uparrow^{\mathbb{X}} c_n\} \end{aligned}$$

such that

$$a = (\bigvee^{\boldsymbol{B}(\mathbb{X})} V_1) \wedge^{\boldsymbol{B}(\mathbb{X})} \dots \wedge^{\boldsymbol{B}(\mathbb{X})} (\bigvee^{\boldsymbol{B}(\mathbb{X})} V_k) = (\bigcup V_1) \cap \dots \cap (\bigcup V_k).$$

Since $a \neq \emptyset$, there exists $b \in X$ such that $b \in \bigcup V_i$, for all $i \leqslant k$. Then we can assume, without loss of generality, that there are $d_1, \dots, d_m, d_{m+1}, \dots, d_k \in X$ such that

$$b \in \uparrow^{\mathbb{X}} d_i \in V_i \text{ for all } i \leqslant m \text{ and } b \in (-\infty, d_i) \in V_i \text{ for all } i > m.$$

There are two cases: either $m = k$ or $m < k$. If $m = k$, then we consider $b' \in X$ such that $b < b'$. Such a b' exists, since $\mathbb{X}$ lacks a maximum. In this case, $[b, b'] = \{x \in X : b \leqslant x \leqslant b'\} \subseteq a$. Then, consider the element $a \cap (-\infty, b') \in B(X)$. We have that $(-\infty, b') \neq \emptyset$ and $(-\infty, b') \subsetneq a$. Hence, we conclude that a is not an atom.

Then we consider the case where $m < k$. In this case, $b < d_i$, for all $i > m$ (otherwise, $b \in (-\infty, d_i) \notin V_i$). Since $\mathbb{X}$ is dense, there exists $b' \in X$ such that $b < b' < d_{m+1}, \ldots, d_k$. Then consider the element $a \cap (-\infty, b') \in B(X)$. Also in this case, $(-\infty, b') \neq \emptyset$ and $(-\infty, b') \subsetneq a$. Hence, we conclude that a is not an atom. ⊠

Corollary 3.75. *$\boldsymbol{B}(\mathbb{Q})$ is a denumerable atomless Boolean algebra.*

We are now ready to prove the main result of the section.

Proof of Theorem 3.70. We already established the existence of denumerable atomless Boolean algebras. Therefore it only remains to prove that they are unique up to isomorphism. Accordingly, let $\boldsymbol{A}$ and $\boldsymbol{B}$ be denumerable atomless Boolean algebras. First, we enumerate of their universes as follows:

$$A = \{a_n : n \in \omega\} \text{ and } B \coloneqq \{b_n : n \in \omega\}.$$

We also assume that $a_0 = 0^{\boldsymbol{A}}$ and $b_0 = 0^{\boldsymbol{B}}$.

We will construct a family of functions $\{f_n : n \in \omega\}$ such that each $f_n : \boldsymbol{A}_n \to \boldsymbol{B}_n$ is an isomorphism from a finite subalgebra $\boldsymbol{A}_n$ of $\boldsymbol{A}$ to a finite subalgebra $\boldsymbol{B}_n$ of $\boldsymbol{B}$. Moreover, this family will satisfy the following conditions for every $n \in \omega$:

(i) $f_n \subseteq f_{n+1}$, for every $n \in \omega$;

(ii) $a_n \in A_n$ and $b_n \in B_n$.

Now, suppose that we constructed such a family $\{f_n : n \in \omega\}$. Then let

$$f \coloneqq \bigcup_{n \in \omega} f_n.$$

From condition (i) it follows that f is a well-defined map from $\bigcup_{n\in\omega} A_n$ to $\bigcup_{n\in\omega} B_n$. Furthermore, condition (ii) guarantees that $A = \bigcup_{n\in\omega} A_n$ and $B = \bigcup_{n\in\omega} B_n$, whence $f \colon A \to B$. Lastly, since each f_n is an isomorphism, this easily implies that $f \colon \boldsymbol{A} \to \boldsymbol{B}$ is also an isomorphism. Thus, $\boldsymbol{A} \cong \boldsymbol{B}$, as desired.

Therefore, to conclude the proof, it only remains to construct a family of functions $\{f_n : n \in \omega\}$ as above. First, let $\boldsymbol{A}_0$ be the subalgebra of $\boldsymbol{A}$ with universe $\{0^{\boldsymbol{A}}, 1^{\boldsymbol{A}}\}$ and $\boldsymbol{B}_0$ be the subalgebra of $\boldsymbol{B}$ with universe $\{0^{\boldsymbol{B}}, 1^{\boldsymbol{B}}\}$. Then let f_0 be the unique isomorphism from $\boldsymbol{A}_0$ and $\boldsymbol{B}_0$. Clearly, $a_0 = 0^{\boldsymbol{A}} \in A_0$ and $b_0 = 0^{\boldsymbol{B}} = B_0$.

Now, suppose that we already constructed the sequence $\{f_m : m \leqslant n\}$ and that we need to construct f_{n+1}. To this end, recall that $f_n \colon \boldsymbol{A}_n \to \boldsymbol{B}_n$ is an isomorphism between finite Boolean algebras. Since $\boldsymbol{A}_n$ and $\boldsymbol{B}_n$ are finite, they are isomorphic to powerset Boolean algebras and, therefore, are atomic. Let $p_1, \ldots, p_m$ be the atoms of $\boldsymbol{A}_n$ and $q_1, \ldots, q_m$ those of $\boldsymbol{B}_n$. We can assume, without loss of generality, that $f_n(p_i) = q_i$ for all $i \leqslant m$. Furthermore, as $\boldsymbol{A}_n$ and $\boldsymbol{B}_n$ are atomic, they are generated by their atoms by Proposition 3.18 (actually each of their element is a join of some of their atoms).

First, we extend f_n to an isomorphism $f_n^+ \colon \boldsymbol{A}_n^+ \to \boldsymbol{B}_n^+$ from a finite subalgebra $\boldsymbol{A}_n^+$ of $\boldsymbol{A}$ to a finite subalgebra $\boldsymbol{B}_n^+$ of $\boldsymbol{B}$, whose domain contains a_{n+1}. To this end, we claim that there exists $b \in B$ such that for every $i \leqslant m$,

$$p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}} \iff q_i \wedge^{\boldsymbol{B}} b = 0^{\boldsymbol{B}}$$
$$p_i \wedge^{\boldsymbol{A}} a_{n+1}^* = 0^{\boldsymbol{A}} \iff q_i \wedge^{\boldsymbol{B}} b^* = 0^{\boldsymbol{B}}.$$

For every $i \leqslant m$, we define an element $c_i \in B$ as follows:

(i) if $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$, then $c_i := 0^{\boldsymbol{B}}$;

(ii) if $p_i \wedge^{\boldsymbol{A}} a_{n+1}^* = 0^{\boldsymbol{A}}$, then $c_i := q_i$.

Notice that the above conditions are mutually exclusive, because if both $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$ and $p_i \wedge^{\boldsymbol{A}} a_{n+1}^* = 0^{\boldsymbol{A}}$, then

$$0^{\boldsymbol{A}} = (p_i \wedge^{\boldsymbol{A}} a_{n+1}) \vee^{\boldsymbol{A}} (p_i \wedge^{\boldsymbol{A}} a_{n+1}^*) = p_i \wedge^{\boldsymbol{A}} (a_{n+1} \vee^{\boldsymbol{A}} a_{n+1}^*) = p_i \wedge^{\boldsymbol{A}} 1 = p_i,$$

a contradiction with the fact that p_i is an atom of $\boldsymbol{A}_n$.

If none between (i) and (ii) holds, then recall that q_i is not an atom of $\boldsymbol{B}$, since $\boldsymbol{B}$ is atomless. As atoms in Boolean algebras coincide with join-irreducible elements, q_i is not join-irreducible in $\boldsymbol{B}$. Together with the fact that $q_i > 0^{\boldsymbol{B}}$ (because q_i is an atom of $\boldsymbol{B}_n$), this implies that there are $x_i, y_i \in B$ such that $0 < x_i, y_i < q_i$ and $x_i \vee^{\boldsymbol{B}} y_i = q_i$. Furthermore, we can assume, without loss of generality, that $x_i \wedge^{\boldsymbol{B}} y_i = 0^{\boldsymbol{B}}$ (otherwise we replace y_i by $x_i^* \wedge y_i$). In this case, we let $c_i := x_i$. This completes the definition of c_i. Notice that

$$c_i \leqslant q_i, \text{ for all } i \leqslant m. \tag{3.13}$$

Bearing this in mind, set

$$b := c_1 \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} c_m.$$

To prove the claim, consider $i \leqslant m$. We have four cases:

1. $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$;
2. $p_i \wedge^{\boldsymbol{A}} a_{n+1} \neq 0^{\boldsymbol{A}}$;
3. $p_i \wedge^{\boldsymbol{A}} a_{n+1}^* = 0^{\boldsymbol{A}}$;
4. $p_i \wedge^{\boldsymbol{A}} a_{n+1}^* \neq 0^{\boldsymbol{A}}$.

We shall treat them separately.

(1): In this case, $c_i = 0^{\boldsymbol{B}}$. We have

$$\begin{aligned}
q_i \wedge^{\boldsymbol{B}} b &= q_i \wedge^{\boldsymbol{B}} (c_1 \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} c_m) \\
&= (q_i \wedge^{\boldsymbol{B}} c_1) \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} (q_i \wedge^{\boldsymbol{B}} c_m) \\
&\leqslant (q_i \wedge^{\boldsymbol{B}} q_1) \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} (q_i \wedge^{\boldsymbol{B}} q_{i-1}) \vee^{\boldsymbol{B}} (q_i \wedge^{\boldsymbol{B}} c_i) \vee (q_i \wedge^{\boldsymbol{B}} q_{i+1}) \vee^{\boldsymbol{B}} \ldots (q_i \wedge^{\boldsymbol{B}} q_m) \\
&= q_i \wedge^{\boldsymbol{B}} c_i \\
&= 0^{\boldsymbol{B}}.
\end{aligned}$$

The above inequalities are justifies as follows. The first follows from the definition of b, the second from distributivity, the third from (3.13), the fourth from the fact that for every $j \leqslant m$ such that $j \neq i$, the elements q_i and q_j are distinct atoms of $\boldsymbol{B}_n$, and the fifth from $c_i = 0^{\boldsymbol{B}}$.

(2): In this case, either $c_i = q_i$ or $c_i = x_i$. In both cases, $0^{\boldsymbol{B}} < q_i \wedge^{\boldsymbol{B}} c_i$, whence

$$q_i \wedge^{\boldsymbol{B}} b = q_i \wedge^{\boldsymbol{B}} (c_1 \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} c_m) = (q_i \wedge^{\boldsymbol{B}} c_1) \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} (q_i \wedge^{\boldsymbol{B}} c_m) > 0^{\boldsymbol{B}}.$$

(3): In this case, $c_i = q_i$, whence $q_i \wedge^{\boldsymbol{B}} c_i^* = 0^{\boldsymbol{B}}$. It follows that

$$\begin{aligned} q_i \wedge^{\boldsymbol{B}} b^* &= q_i \wedge^{\boldsymbol{B}} (c_1 \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} c_m)^* \\ &= q_i \wedge^{\boldsymbol{B}} c_1^* \wedge^{\boldsymbol{B}} \cdots \wedge^{\boldsymbol{B}} c_m^* \\ &= 0^{\boldsymbol{B}}. \end{aligned}$$

(4): I this case, either $c_i = 0^{\boldsymbol{B}}$ or $c_i = x_i$. First suppose that $c_i = 0^{\boldsymbol{B}}$, that is, $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$ holds. We already showed that this implies $q_i \wedge^{\boldsymbol{B}} b = 0^{\boldsymbol{B}}$. Notice that if $q_i \wedge^{\boldsymbol{B}} b^* = 0^{\boldsymbol{B}}$, then we would obtain $q_i = 0^{\boldsymbol{B}}$, a contradiction. Hence, we conclude that $q_i \wedge^{\boldsymbol{B}} b^* \neq 0^{\boldsymbol{B}}$, as desired. Then we consider the case where $c_i = x_i$. Consider $j \neq i$. We shall prove that $y_i \leqslant c_j^*$. To prove this, recall from (3.13) that $c_j \leqslant q_j$. Thus, $q_j^* \leqslant c_j^*$. Since $i \neq j$, we also have $q_i \leqslant q_j^*$, whence

$$y_i \leqslant q_i \leqslant q_j^* \leqslant c_j^*.$$

As a consequence, we obtain

$$q_i \wedge^{\boldsymbol{B}} b^* = q_i \wedge^{\boldsymbol{B}} (c_1 \vee^{\boldsymbol{B}} \cdots \vee^{\boldsymbol{B}} c_m)^* = q_i \wedge^{\boldsymbol{B}} c_1^* \wedge^{\boldsymbol{B}} \cdots \wedge^{\boldsymbol{B}} c_m^* \geqslant q_i \wedge^{\boldsymbol{B}} y_i \wedge^{\boldsymbol{B}} c_i^*.$$

Therefore, to conclude the proof of this case, it suffices to show that $q_i \wedge^{\boldsymbol{A}} y_i \wedge^{\boldsymbol{B}} c_i^* > 0^{\boldsymbol{B}}$. To this end, observe that $q_i \wedge^{\boldsymbol{B}} y_i \wedge^{\boldsymbol{B}} c_i^* = y_i \wedge^{\boldsymbol{B}} c_i^*$, since $y_i \leqslant q_i$. Furthermore, recall that $c_i = x_i$ and $x_i \wedge^{\boldsymbol{B}} y_i$. Since, by Proposition 3.9(iv), c_i^* is the largest element of $\boldsymbol{B}$ whose infimum with c_i is $0^{\boldsymbol{B}}$, we conclude that $c_i^* \geqslant y_i$, whence $y_i \wedge^{\boldsymbol{B}} c_i^* = y_i$. As a consequence, $q_i \wedge^{\boldsymbol{B}} b^* \geqslant y_i > 0^{\boldsymbol{B}}$, as desired. This concludes the proof of the claim.

Now, let b be the element given by the claim. Then define

$$\boldsymbol{A}_n^+ := \mathrm{Sg}^{\boldsymbol{A}}(\{p_1, \ldots, p_m, a_{n+1}\}) \text{ and } \boldsymbol{B}_n^+ := \mathrm{Sg}^{\boldsymbol{B}}(\{q_1, \ldots, q_m, b\}).$$

Notice that $\boldsymbol{A}_n^+$ and $\boldsymbol{B}_n^+$ are finite, because the class of Boolean algebras is locally finite, by Corollary 3.13. It follows that $\boldsymbol{A}_n^+$ and $\boldsymbol{B}_n^+$ are atomic.

We claim that the atoms of $\boldsymbol{A}_n^+$ are precisely the nonzero elements of the form $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ and $p_i \wedge^{\boldsymbol{A}} a_{n+1}^*$. Similarly, the atoms of $\boldsymbol{B}_n^+$ are the nonzero elements of the form $q_i \wedge^{\boldsymbol{B}} b$ and $q_i \wedge^{\boldsymbol{B}} b^*$. We detail the proof for the case of $\boldsymbol{A}_n^+$ only, as the case of $\boldsymbol{B}_n^+$ is analogous.

To prove this, we begin by showing that for every atom c of $\boldsymbol{A}_n^+$ there exists $i \leqslant m$ such that either $c \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}$ or $c \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}^*$. Suppose the contrary, with a view to contradiction. Then for every $i \leqslant n$,

$$c \not\leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1} \text{ and } c \not\leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}^*.$$

As c is an atom of $\boldsymbol{A}_n^+$ and, therefore, join-prime in $\boldsymbol{A}_n^+$, this implies

$$c \not\leqslant (p_i \wedge^{\boldsymbol{A}} a_{n+1}) \vee^{\boldsymbol{A}} (p_i \wedge^{\boldsymbol{A}} a_{n+1}^*) = p_i \wedge^{\boldsymbol{A}} (a_{n+1} \vee^{\boldsymbol{A}} a_{n+1}^*) = p_i \wedge^{\boldsymbol{A}} 1^{\boldsymbol{A}} = p_i.$$

As $c \leqslant 1^{\boldsymbol{A}} = p_i \vee^{\boldsymbol{A}} p_i^*$ and c is join-prime in $\boldsymbol{A}_n^+$, this implies $c \leqslant p_i^*$, for all $i \leqslant m$. Thus,

$$c \leqslant p_1^* \wedge^{\boldsymbol{A}} \cdots \wedge^{\boldsymbol{A}} p_m^* = 0^{\boldsymbol{A}},$$

where the latter equality follows from the fact that $p_1, \ldots, p_m$ are the atoms of $\boldsymbol{A}_n$ and $\boldsymbol{A}_n$ is finite, whence $p_1 \vee^{\boldsymbol{A}} \cdots \vee^{\boldsymbol{A}} p_m = 1^{\boldsymbol{A}}$. But the above display contradicts the fact that c is an atom of $\boldsymbol{A}_n^+$, as desired. Now, since every atom of $\boldsymbol{A}_n^+$ is below some element of the form $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ or $p_i \wedge^{\boldsymbol{A}} a_{n+1}^*$, to conclude the proof it suffices to show that if an element of this form is different from $0^{\boldsymbol{A}}$, then it is an atom of $\boldsymbol{A}_n^+$. We detail the case of nonzero elements of the form $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ as the other case is analogous. Accordingly, consider $i \leqslant m$ such that $p_i \wedge^{\boldsymbol{A}} a_{n+1} > 0^{\boldsymbol{A}}$. Moreover, let $c \in A_n^+$ be such that $0^{\boldsymbol{A}} < c \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}$. Since

$$c \in A_n^+ := \mathrm{Sg}^{\boldsymbol{A}}(\{p_1, \ldots, p_m, a_{n+1}\}),$$

we can apply Theorem 3.12, obtaining a Boolean term φ in DNF which, when applied to $p_1, \ldots, p_m, a_{n+1}$ gives us c. More precisely, there are

$$V_1, \ldots, V_k \subseteq \{p_1, \ldots, p_m, a_{n+1}, p_1^*, \ldots, p_m^*, a_{n+1}^*\}$$

such that

$$c = \varphi^{\boldsymbol{A}}(p_1, \ldots, p_m, a_{n+1}) = (\bigwedge^{\boldsymbol{A}} V_1) \vee^{\boldsymbol{A}} \cdots \vee^{\boldsymbol{A}} (\bigwedge^{\boldsymbol{A}} V_k).$$

Since $c \neq 0^{\boldsymbol{A}}$, there is V_j such that $\bigwedge^{\boldsymbol{A}} V_j \neq 0^{\boldsymbol{A}}$. Notice that it suffices to prove that $p_i \wedge^{\boldsymbol{A}} a_{n+1} \leqslant \bigwedge^{\boldsymbol{A}} V_j$, as this implies $p_i \wedge^{\boldsymbol{A}} a_{n+1} = c$, because

$$\bigwedge^{\boldsymbol{A}} V_j \leqslant c \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}.$$

As $\bigwedge^{\boldsymbol{A}} V_j \neq 0^{\boldsymbol{A}}$ and $\bigwedge^{\boldsymbol{A}} V_j \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1} \leqslant p_i$, we obtain $p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_m \notin V_j$ (otherwise we would have $\bigwedge^{\boldsymbol{A}} V_j = 0^{\boldsymbol{A}}$, because $p_i \wedge^{\boldsymbol{A}} p_t = 0^{\boldsymbol{A}}$, for all $t \neq i$). Similarly, $p_i^*, a_{n+1}^* \notin V_j$, because $\bigwedge^{\boldsymbol{A}} V_j \leqslant p_i \wedge^{\boldsymbol{A}} a_{n+1}$ and $\bigwedge^{\boldsymbol{A}} V_j \neq 0^{\boldsymbol{A}}$. Summing up,

$$V_j \subseteq \{p_i, p_1^*, \ldots, p_{i-1}^*, p_{i+1}^*, \ldots, p_m^*, a_{n+1}^*\}$$

and, therefore,

$$p_i \wedge^{\boldsymbol{A}} p_1^* \wedge^{\boldsymbol{A}} \cdots \wedge^{\boldsymbol{A}} p_{i-1}^* \wedge^{\boldsymbol{A}} p_{i+1}^* \wedge^{\boldsymbol{A}} \cdots \wedge^{\boldsymbol{A}} p_m^* \wedge^{\boldsymbol{A}} a_{n+1}^* \leqslant \bigwedge^{\boldsymbol{A}} V_j.$$

Now, as $p_1, \ldots, p_m$ are the atoms of $\boldsymbol{A}_n^+$, we have $p_i \leqslant p_1^*, \ldots, p_{i-1}^*, p_{i+1}^* \ldots, p_m^*$. Together with the above display, this implies

$$p_i \wedge^{\boldsymbol{A}} a_{n+1} \leqslant p_i \wedge^{\boldsymbol{A}} p_1^* \wedge^{\boldsymbol{A}} \cdots \wedge^{\boldsymbol{A}} p_{i-1}^* \wedge^{\boldsymbol{A}} p_{i+1}^* \wedge^{\boldsymbol{A}} \cdots \wedge^{\boldsymbol{A}} p_m^* \wedge^{\boldsymbol{A}} a_{n+1}^* \leqslant \bigwedge^{\boldsymbol{A}} V_j.$$

This concludes the proof of the second claim.

Let X_A and X_B be the set of atoms of $\boldsymbol{A}_n^+$ and $\boldsymbol{B}_n^+$, respectively. We define a map $g\colon X_A \to X_B$ by the rule

$$p_i \wedge^{\boldsymbol{A}} a_{n+1} \longmapsto q_i \wedge^{\boldsymbol{B}} b \text{ and } p_i \wedge^{\boldsymbol{A}} a_{n+1}^* \longmapsto q_i \wedge^{\boldsymbol{B}} b^*.$$

We shall prove that g is well-defined. To this end, consider an element $c \in X_A$. By the second claim we know that c is either of the form $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ or $p_i \wedge^{\boldsymbol{A}} a^*_{n+1}$. This representation is indeed unique (if it was not, we would obtain either $c \leqslant p_i, p_j$ for different i, j or $c \leqslant a_{n+1}, a^*_{n+1}$, which implies $c = 0^{\boldsymbol{A}}$, against the assumption that c is an atom of $\boldsymbol{A}^+_n$). Therefore, it only remains to prove that if $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ (resp. $p_i \wedge^{\boldsymbol{A}} a^*_{n+1}$) is an atom of $\boldsymbol{A}^+_n$, then $q_i \wedge^{\boldsymbol{B}} b$ (resp. $q_i \wedge^{\boldsymbol{B}} b^*$) is an atom of $\boldsymbol{B}^+_n$. To this end, suppose that $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ is an atom of $\boldsymbol{A}^+_n$. Then $p_i \wedge^{\boldsymbol{A}} a_{n+1} > 0^{\boldsymbol{A}}$. By the first claim, $q_i \wedge^{\boldsymbol{B}} b > 0^{\boldsymbol{B}}$. Hence, by the second claim, $q_i \wedge^{\boldsymbol{B}} b$ is an atom of $\boldsymbol{B}^+_n$, as desired. The case of $p_i \wedge^{\boldsymbol{A}} a^*_{n+1}$ is handled analogously. We conclude that g is well-defined. A similar argument shows that the map $h\colon X_B \to X_A$, defined by the rule

$$q_i \wedge^{\boldsymbol{B}} b \longmapsto p_i \wedge^{\boldsymbol{A}} a_{n+1} \text{ and } q_i \wedge^{\boldsymbol{B}} b^* \longmapsto p_i \wedge^{\boldsymbol{A}} a^*_{n+1},$$

is also well-defined. As g and h are inverse one to the other, we conclude that g is a bijection. It follows that $\boldsymbol{A}^+_n$ and $\boldsymbol{B}^+_n$ are finite Boolean algebras with the same number of atoms.

Notice that, by Corollary 3.21, $\boldsymbol{A}^+_n \cong \mathcal{P}(X_A)$ and $\boldsymbol{B}^+_n \cong \mathcal{P}(X_B)$. Consequently, the fact that $g\colon X_A \to X_B$ is a bijection implies that the map $f^+_n\colon A^+_n \to B^+_n$, defined as

$$f^+_n(a) \coloneqq \bigvee^{\boldsymbol{B}} \{g(c) : c \in X_A \text{ and } c \leqslant a\},$$

is an isomorphism from $\boldsymbol{A}^+_n$ to $\boldsymbol{B}^+_n$. Moreover, a_{n+1} belongs to the domain of f^+_n. Our aim is to show that f^+_n extends f_n. To this end, observe that, for every $i \leqslant m$,

$$f^+_n(p_i) = \bigvee^{\boldsymbol{B}} \{g(c) : c \in X_A \text{ and } c \leqslant p_i\} = q_i = f_n(p_i). \tag{3.14}$$

The only nontrivial equality in the above display is the second. To justify it, recall from the second claim that X_A is the set of nonzero elements of $\boldsymbol{A}^+_n$ of the form $p_j \wedge^{\boldsymbol{A}} a_{n+1}$ or $p_j \wedge^{\boldsymbol{A}} a^*_{n+1}$ for $j \leqslant m$. As a consequence, the elements $c \in X_A$ such that $c \leqslant p_i$ are the nonzero elements of of $\boldsymbol{A}^+_n$ the form $p_i \wedge^{\boldsymbol{A}} a_{n+1}$ or $p_i \wedge^{\boldsymbol{A}} a^*_{n+1}$. This is because, if $j \neq i$, then $p_j \wedge^{\boldsymbol{A}} a_{n+1} \nleqslant p_i$ and $p_j \wedge^{\boldsymbol{A}} a^*_{n+1} \nleqslant p_i$, otherwise $p_j \leqslant p_i$, against the assumption that p_i and p_j are distinct atoms of $\boldsymbol{A}_n$. As a consequence,

$$\{g(c) : c \in X_A \text{ and } c \leqslant p_i\} \subseteq \{p_i \wedge^{\boldsymbol{A}} a_{n+1}, p_i \wedge^{\boldsymbol{A}} a^*_{n+1}\}.$$

We have two cases: either $p_i \wedge^{\boldsymbol{A}} a_{n+1} \notin \{c \in X_A : c \leqslant p_i\}$ or $p_i \wedge^{\boldsymbol{A}} a_{n+1} \in \{c \in X_A : c \leqslant p_i\}$. If $p_i \wedge^{\boldsymbol{A}} a_{n+1} \notin \{c \in X_A : c \leqslant p_i\}$, then $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$. By Proposition 3.9(iv), $p_i \leqslant a^*_{n+1}$. As a consequence, $0^{\boldsymbol{A}} < p_i = p_i \wedge^{\boldsymbol{A}} a^*_{n+1}$, whence $\{c \in X_A : c \leqslant p_i\} = \{p_i \wedge^{\boldsymbol{A}} a^*_{n+1}\}$. It follows that

$$\bigvee^{\boldsymbol{B}} \{g(c) : c \in X_A \text{ and } c \leqslant p_i\} = \bigvee^{\boldsymbol{B}} \{g(p_i \wedge^{\boldsymbol{A}} a^*_{n+1})\} = q_i \wedge^{\boldsymbol{B}} b^*.$$

Now, from $p_i \wedge^{\boldsymbol{A}} a_{n+1} = 0^{\boldsymbol{A}}$ and the first claim it follows $q_i \wedge^{\boldsymbol{B}} b = 0^{\boldsymbol{B}}$. By Proposition 3.9(iv), this yields $q_i \leqslant b^*$, whence $q_i = q_i \wedge^{\boldsymbol{B}} b^*$. Together with the above display, this establishes (3.14). Then we consider the case where $p_i \wedge^{\boldsymbol{A}} a_{n+1} \in \{c \in X_A : c \leqslant p_i\}$. Now, if $p_i \wedge^{\boldsymbol{A}} a^*_{n+1} \notin \{c \in X_A : c \leqslant p_i\}$, then we repeat the proof described above

(inverting the role of a_{n+1} and a^*_{n+1}). Then we detail only the case where $\{c \in X_A : c \leqslant p_i\} = \{p_i \wedge^{\boldsymbol{A}} a_{n+1}, p_i \wedge^{\boldsymbol{A}} a^*_{n+1}\}$. We have

$$\begin{aligned}\bigvee^{\boldsymbol{B}}\{g(c) : c \in X_A \text{ and } c \leqslant p_i\} &= g(p_i \wedge^{\boldsymbol{A}} a_{n+1}) \vee^{\boldsymbol{B}} g(p_i \wedge^{\boldsymbol{A}} a^*_{n+1})\\ &= (q_i \wedge^{\boldsymbol{B}} b) \vee^{\boldsymbol{B}} (q_i \wedge^{\boldsymbol{B}} b^*)\\ &= q_i \wedge^{\boldsymbol{B}} (b \vee^{\boldsymbol{B}} b^*)\\ &= q_i \wedge^{\boldsymbol{B}} 1^{\boldsymbol{B}}\\ &= q_i.\end{aligned}$$

This establishes condition (3.14). Since $\boldsymbol{A}_n$ is finite atomic, its elements are finite joins of the atoms $p_1, \ldots, p_m$. By (3.14), f_n^+ and f_n agree on the atoms of $\boldsymbol{A}_n$ and, therefore, on finite joins of them. This implies that f_n^+ extends f_n, as desired. Thus, f_n^+ is an isomorphism from a finite subalgebra of $\boldsymbol{A}$ to a finite subalgebra of $\boldsymbol{B}$ extending f_n and whose domain contains a_{n+1}.

In order to conclude the proof, we reason as follows. First, $f_n^{+-1} \colon \boldsymbol{B}_n^+ \to \boldsymbol{A}_n^+$ is an isomorphism between finite subalgebras of $\boldsymbol{B}$ and $\boldsymbol{A}$. Repeating the argument described above where b_{n+1} takes the role of a_{n+1}, we construct an isomorphism $j \colon \boldsymbol{B}^+ \to \boldsymbol{A}^+$ between finite subalgebras of $\boldsymbol{B}$ and $\boldsymbol{A}$, respectively, whose domain contains b_{n+1}. Then the map $f_{n+1} \coloneqq j^{-1}$ is an isomorphism from a finite subalgebra of $\boldsymbol{A}$ to a finite subalgebra of $\boldsymbol{B}$ that extends f_n, whose domain contains a_{n+1}, and whose image contains b_{n+1}. ⊠

Corollary 3.76. *All denumerable atomless Boolean algebras are isomorphic to $\boldsymbol{B}(\mathbb{Q})$ (equiv. to $T/{\equiv_\emptyset}$).*

*Exercise** 3.77. By the *Cantor space* $\boldsymbol{X}$ we understand the topological product of ω copies of the two-element discrete space. A subset U of X is said to be *clopen* if it is both open and closed. Prove that the family of clopen sets of $\boldsymbol{X}$ forms a subalgebra of the Boolean algebra $\mathcal{P}(X)$. As a consequence, the clopens of $\boldsymbol{X}$ form a Boolean algebra $\boldsymbol{A}$. Prove that $\boldsymbol{A}$ is denumerable and atomless. Conclude that this is yet another description of the unique denumerable atomless Boolean algebra. ⊠

CHAPTER 4

Completions

4.1 Polarities and residuation

Definition 4.1. Let $\mathbb{X}$ and $\mathbb{Y}$ be posets. A *residuated map* from $\mathbb{X}$ to $\mathbb{Y}$ is a function $f\colon X \to Y$ for which there exists a map $g\colon Y \to X$ such that, for all $x \in X$ and $y \in Y$, the following condition holds:

$$f(x) \leqslant^{\mathbb{Y}} y \iff x \leqslant^{\mathbb{X}} g(y). \tag{*residuation law*}$$

In this case, the map g is unique, as we proceed to explain.

Proposition 4.2. *If f is residuated from $\mathbb{X}$ to $\mathbb{Y}$, then there exists a unique map $g\colon Y \to X$ satisfying the residuation law for f. Moreover, for every $x \in X$ and $y \in Y$,*

$$f(x) = \min\{z \in Y : x \leqslant^{\mathbb{X}} g(z)\} \quad \textit{and} \quad g(y) = \max\{z \in X : f(z) \leqslant^{\mathbb{Y}} y\}.$$

Proof. Let $g\colon Y \to X$ be a map satisfying the residuation law and consider $y \in Y$. From $g(y) \leqslant^{\mathbb{X}} g(y)$ and the residuation law it follows $f(g(y)) \leqslant^{\mathbb{Y}} y$. Consequently,

$$g(y) \in \{z \in X : f(z) \leqslant^{\mathbb{Y}} y\}.$$

Then consider $z \in X$ such that $f(z) \leqslant^{\mathbb{Y}} y$. By the residuation law, $z \leqslant^{\mathbb{X}} g(y)$. Thus, we conclude that $g(y) = \max\{z \in X : f(z) \leqslant^{\mathbb{Y}} y\}$. As a consequence, there exists a unique unique map satisfying the residuation law with respect to f. A similar argument shows that $f(x) = \min\{z \in Y : x \leqslant^{\mathbb{X}} g(z)\}$, for every $x \in X$. ⊠

Accordingly, given a residuated map f from $\mathbb{X}$ to $\mathbb{Y}$, we denote by f^+ the unique map g satisfying the residuation law for f. In this case, f^+ is called the *residual* of f and $\langle f, f^+\rangle$ a *residuated pair* between $\mathbb{X}$ and $\mathbb{Y}$.

Remark 4.3. Readers familiar with category theory will be eager to recognize that residuated pairs are precisely adjunctions between posets, viewed as categories. ⊠

Prototypical examples of residuated pairs can be constructed as follows.

Definition 4.4. A *polarity* is a triple $\langle X, Y, R\rangle$ where X and Y are sets and $R \subseteq X \times Y$.

Example 4.5 (Residuated maps)**.** Every polarity $\langle X, Y, R\rangle$ induces a residuated pair, as we proceed to explain. Consider the maps

$$(-)^{\blacktriangleright}\colon \mathcal{P}(X) \to \mathcal{P}(Y) \text{ and } (-)^{\blacktriangleleft}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$$

defined, for every $A \subseteq X$ and $B \subseteq Y$, as

$$\begin{aligned} A^{\blacktriangleright} &:= \{y \in Y : \text{there is } x \in A \text{ such that } \langle x, y\rangle \in R\} \\ B^{\blacktriangleleft} &:= \{x \in X : \text{for all } y \in Y, \text{ if } \langle x, y\rangle \in R, \text{ then } y \in B\}. \end{aligned}$$

Then $\langle (-)^{\blacktriangleright}, (-)^{\blacktriangleleft}\rangle$ is a residuated pair between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$. To prove this, consider $A \subseteq X$ and $B \subseteq Y$. We need to show that $\langle (-)^{\blacktriangleright}, (-)^{\blacktriangleleft}\rangle$ is a residuated pair. First, suppose that $A^{\blacktriangleright} \subseteq B$ and consider $x \in A$ and $y \in Y$ such that $\langle x, y\rangle \in R$. Then $y \in A^{\blacktriangleright} \subseteq B$. Hence, we conclude that $x \in B^{\blacktriangleleft}$. Conversely, suppose that $A \subseteq B^{\blacktriangleleft}$ and consider $y \in A^{\blacktriangleright}$. Then there exists $x \in A$ such that $\langle x, y\rangle \in R$. Since $x \in A \subseteq B^{\blacktriangleleft}$, this implies that $y \in B$, as desired. ⊠

The next result collects some useful properties of residuated maps.

Proposition 4.6. *If f is residuated from $\mathbb{X}$ to $\mathbb{Y}$, then the following conditions hold:*

(i) *for every $x \in X$ and $y \in Y$,*

$$x \leqslant^{\mathbb{X}} f^+(f(x)) \quad \text{and} \quad f(f^+(y)) \leqslant^{\mathbb{Y}} y;$$

(ii) *f preserves existing joins, that is, if $Z \subseteq X$ and $\bigvee^{\mathbb{X}} Z$ exists, then*

$$f(\bigvee_{z\in Z}^{\mathbb{X}} z) = \bigvee_{z\in Z}^{\mathbb{Y}} f(z);$$

(iii) *f^+ preserves existing meets, that is, if $Z \subseteq Y$ and $\bigwedge^{\mathbb{Y}} Z$ exists, then*

$$f(\bigwedge_{z\in Z}^{\mathbb{X}} z) = \bigwedge_{z\in Z}^{\mathbb{X}} f(z);$$

(iv) *f and f^+ are order preserving;*

(v) *$f = f \circ f^+ \circ f$ and $f^+ = f^+ \circ f \circ f^+$;*

(vi) *f is injective if and only if f^+ is surjective; and*

(vii) *f is surjective if and only if f^+ is injective.*

Proof. (i): Clearly, $f(x) \leqslant^{\mathbb{Y}} f(x)$. Thus, by the residuation law, $x \leqslant^{\mathbb{X}} f^+(f(x))$. Similarly, we obtain $f(f^+(y)) \leqslant^{\mathbb{Y}} y$.

(ii): Suppose that $\bigvee^{\mathbb{X}} Z$ exists. We shall prove that $f(\bigvee^{\mathbb{X}} Z)$ is the join of $f[Z]$ in $\mathbb{Y}$. First, consider $z \in Z$. We have $z \leqslant^{\mathbb{X}} \bigvee^{\mathbb{X}} Z$. By (i), we get

$$z \leqslant^{\mathbb{X}} \bigvee^{\mathbb{X}} Z \leqslant^{\mathbb{X}} f^+(f(\bigvee^{\mathbb{X}} Z)).$$

Thus, by the residuation law, $f(z) \leqslant f(\bigvee^{\mathbb{X}} Z)$. Hence, $f(\bigvee^{\mathbb{X}} Z)$ is an upper bound of $f[Z]$ in $\mathbb{Y}$. To prove that it is the least one, consider an upper bound y of $f[Z]$ in $\mathbb{Y}$. Then, for every $z \in Z$, we have $f(z) \leqslant^{\mathbb{Y}} y$ and, by the residuation law, $z \leqslant^{\mathbb{X}} f^+(y)$. Thus $f^+(y)$ is an upper bound of Z, whence $\bigvee^{\mathbb{X}} Z \leqslant^{\mathbb{X}} f^+(y)$. By the residuation law, $f(\bigvee^{\mathbb{X}} Z) \leqslant^{\mathbb{Y}} y$. Then we conclude that $f(\bigvee^{\mathbb{X}} Z)$ is the least upper bound of $f[Z]$ in $\mathbb{Y}$, that is, the join of $f[Z]$ in $\mathbb{Y}$.

(iii): Similar to the proof of (ii).

(iv): Consider $x, z \in X$ such that $x \leqslant^{\mathbb{X}} z$. Then $z = x \vee^{\mathbb{X}} z$. By (ii), we obtain

$$f(z) = f(x \vee^{\mathbb{X}} z) = f(x) \vee^{\mathbb{Y}} f(z),$$

which means that $f(x) \leqslant^{\mathbb{Y}} f(z)$. Hence, we conclude that f is order preserving. A similar argument shows the same for f^+.

(v): Consider $x \in X$. By (i), $x \leqslant^{\mathbb{X}} f^+(f(x))$. Since, by (iv), f is order preserving, $f(x) \leqslant^{\mathbb{Y}} f(f^+(f(x)))$. Moreover, taking $y := f(x)$ in (i), we obtain $f(f^+(f(x))) \leqslant^{\mathbb{Y}} f(x)$. Hence, $f(x) = f(f^+(f(x)))$. We conclude that $f = f \circ f^+ \circ f$. A similar argument shows that $f^+ = f^+ \circ f \circ f^+$.

(vi): Suppose that f is injective and consider $x \in X$. From (v) it follows $f(x) = f(f^+(f(x)))$. Since f is injective, this yields $x = f^+(f(x))$, whence $x \in f^+[Y]$. We conclude that f^+ is surjective. Conversely, suppose that f^+ is surjective and consider $x_1, x_2 \in X$ such that $f(x_1) = f(x_2)$. Since f^+ is surjective, there are $y_1, y_2 \in Y$ such that $x_1 = f^+(y_1)$ and $x_2 = f^+(y_2)$. We have

$$\begin{aligned} x_1 = f^+(y_1) = f^+(f(f^+(y_1))) = f^+(f(x_1)) \\ = f^+f((x_2)) = f^+(f(f^+(y_2))) = f^+(y_2) = x_2. \end{aligned}$$

The second and the sixth equalities above follows from (v), the fourth from the assumption that $f(x_1) = f(x_2)$. The other ones are obvious. From the above display it follows that f is injective, as desired.

(vii): Similar to the proof of (vi). ⊠

The next results establishes a criteriaon for a map to be residuated.

Proposition 4.7. *Let $\mathbb{X}$ and $\mathbb{Y}$ be posets and $f\colon X \to Y$. The following conditions are equivalent:*

(i) *f is residuated from $\mathbb{X}$ to $\mathbb{Y}$;*

(ii) *f is order preserving and there exists an order preserving map $g\colon Y \to X$ such that, for all $x \in X$ and $y \in Y$,*

$$x \leqslant^{\mathbb{X}} g(f(x)) \text{ and } f(g(y)) \leqslant^{\mathbb{Y}} y;$$

(iii) *inverse images under f of principal downsets in $\mathbb{Y}$ are principal downsets in $\mathbb{X}$.*

Proof. (i)⇒(ii): Immediate from conditions (i) and (ii) of Proposition 4.6.

(ii)⇒(iii): Consider $y \in Y$. We will prove that

$$f^{-1}(\downarrow y) = \downarrow g(y).$$

To this end, consider $x \in f^{-1}(\downarrow y)$. Then $f(x) \leqslant^{\mathbb{Y}} y$. Since g is order preserving, we obtain $g(f(x)) \leqslant^{\mathbb{X}} g(y)$. As, by assumption, $x \leqslant^{\mathbb{X}} g(f(x))$, we conclude that

$x \leqslant^{\mathbb{X}} g(y)$, that is, $x \in {\downarrow}g(y)$. It follows that $f^{-1}({\downarrow}y) \subseteq {\downarrow}g(y)$. To prove the other inclusion, consider an element $x \in {\downarrow}g(y)$, that is, such that $x \leqslant^{\mathbb{X}} g(y)$. Since f is order preserving $f(x) \leqslant^{\mathbb{Y}} f(g(y))$. Together with the assumption that $f(g(y)) \leqslant^{\mathbb{Y}} y$, this yields $f(x) \leqslant^{\mathbb{Y}} y$, that is, $x \in f^{-1}({\downarrow}y)$.

(iii)⇒(i): Suppose that inverse images under f of principal downsets in $\mathbb{Y}$ are principal downsets in $\mathbb{X}$. Then let $g\colon Y \to X$ be the map defined, for every $y \in Y$, as follows:

$$g(y) \coloneqq \text{the unique } x \text{ such that } f^{-1}({\downarrow}y) = {\downarrow}x.$$

From the assumptions it follows that g is well-defined. Then consider $x \in X$ and $y \in Y$. We have

$$\begin{aligned} f(x) \leqslant^{\mathbb{Y}} y &\iff f(x) \in {\downarrow}y \\ &\iff x \in f^{-1}({\downarrow}y) \\ &\iff x \in {\downarrow}g(y) \\ &\iff x \leqslant^{\mathbb{X}} g(y). \end{aligned}$$

Hence, we conclude that $\langle f, g\rangle$ is a residuated pair. ⊠

As a consequence, we obtain a simpler characterization of residuated maps between complete lattices.

Corollary 4.8. *Let $\mathbb{X}$ and $\mathbb{Y}$ be complete lattices. A map $f\colon \mathbb{X} \to \mathbb{Y}$ is residuated (resp. a residual) if and only if it preserves arbitrary joins (resp. meets).*

Proof. We detail the case of residuated maps only, as that of residuals is analogous. The "only if" part is condition (ii) of Proposition 4.6. To prove the "if' part, suppose that f preserves arbitrary joins. In view of Proposition 4.7, it suffices to show that inverse images under f of principal downsets in $\mathbb{Y}$ are principal downsets in $\mathbb{X}$. To this end, consider $y \in Y$. Since $\mathbb{X}$ is a complete lattice, we can set

$$x \coloneqq \bigvee^{\mathbb{X}} f^{-1}({\downarrow}y).$$

We need to show that ${\downarrow}x = f^{-1}({\downarrow}y)$. The inclusion $f^{-1}({\downarrow}y) \subseteq {\downarrow}x$ follows from the definition of x. To prove the other one, observe that, since f preserves arbitrary joins,

$$\begin{aligned} f(x) &= f(\bigvee^{\mathbb{X}} f^{-1}({\downarrow}y)) \\ &= \bigvee^{\mathbb{Y}} \{f(z) : z \in f^{-1}({\downarrow}y)\} \\ &= \bigvee^{\mathbb{Y}} \{f(z) : z \in X \text{ and } f(z) \leqslant^{\mathbb{Y}} y\} \\ &\leqslant^{\mathbb{Y}} y, \end{aligned}$$

that is, $f(x) \leqslant^{\mathbb{Y}} y$. Now, consider $z \in {\downarrow}x$. Since f is order preserving $f(z) \leqslant^{\mathbb{Y}} f(x)$. Together with $f(x) \leqslant^{\mathbb{Y}} y$, this yields $f(z) \leqslant^{\mathbb{Y}} y$, i.e., $z \in f^{-1}({\downarrow}y)$. Hence, ${\downarrow}x \subseteq f^{-1}({\downarrow}y)$, as desired. ⊠

As we mentioned in Example 4.5, every polarity $\langle X, Y, R\rangle$ induces a residuated pair $\langle (-)^{\blacktriangleright}, (-)^{\blacktriangleleft}\rangle$ between the powerset lattices $\mathcal{P}(X)$ and $\mathcal{P}(Y)$. Notably, all residuated pairs between powerset lattices arise in this way.

Theorem 4.9. *A pair $\langle f, g\rangle$ of maps $f\colon \mathcal{P}(X) \to \mathcal{P}(Y)$ and $g\colon \mathcal{P}(Y) \to \mathcal{P}(X)$ is residuated between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$ if and only if there exists a polarity $\langle X, Y, R\rangle$ for which*

$$f = (-)^{\blacktriangleright} \quad \text{and} \quad g = (-)^{\blacktriangleleft}.$$

Proof. In view of Example 4.5, it suffices to prove the "only if" part. To this end, consider a residuated pair $\langle f, f^+\rangle$ between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$. We define a relation $R \subseteq X \times Y$ setting

$$R := \{\langle x, y\rangle \in X \times Y : y \in f(\{x\})\}.$$

Then consider $Z \subseteq X$. We have

$$f(Z) = f(\bigcup_{z\in Z} \{z\}) = f(\bigvee^{\mathbb{X}}_{z\in Z} \{z\}) = \bigvee^{\mathbb{Y}}_{z\in Z} f(\{z\}) = \bigcup_{z\in Z} f(\{z\}) = Z^{\blacktriangleright}.$$

The above equalities are justified as follows. The first one is trivial, the second and the fourth hold because joins in powerset lattices are unions, and the third follows from the fact that f preserves joins, by Proposition 4.6(ii). Lastly, to prove the fifth equality, consider an element $y \in \bigcup_{z\in Z} f(\{z\})$. Then there exists $z \in Z$ such that $y \in f(\{z\})$. By the definition of R, this yields $\langle z, y\rangle \in R$ and, therefore, $y \in Z^{\blacktriangleright}$. Thus, $\bigcup_{z\in Z} f(\{z\}) \subseteq Z^{\blacktriangleright}$. To prove the other inclusion, consider $y \in Z^{\blacktriangleright}$. Then there exists $z \in Z$ such that $\langle z, y\rangle \in R$. By the definition of R, this means that $y \in f(\{z\})$, whence $y \in \bigcup_{z\in Z} f(\{z\})$. Hence, $Z^{\blacktriangleright} \subseteq \bigcup_{z\in Z} f(\{z\})$, as desired. We conclude that $f = (-)^{\blacktriangleright}$.

As the pair $\langle (-)^{\blacktriangleright}, (-)^{\blacktriangleleft}\rangle$ is residuated between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$ and $f = (-)^{\blacktriangleright}$, the map $(-)^{\blacktriangleleft}$ is a residual of f. From the uniqueness of residuals (Proposition 4.2) it follows that $f^+ = (-)^{\blacktriangleleft}$. ⊠

The following variant of the notion of a residuated map plays a central role in the theory of completions.

Definition 4.10. Let $\mathbb{X}$ and $\mathbb{Y}$ be posets, $f\colon X \to Y$, and $g\colon Y \to X$. The pair $\langle f, g\rangle$ is a *Galois connection* between $\mathbb{X}$ and $\mathbb{Y}$ if it is a residuated pair between $\mathbb{X}$ and $\mathbb{Y}^\partial$, that is,

$$y \leqslant^{\mathbb{Y}} f(x) \iff x \leqslant^{\mathbb{X}} g(y),$$

for every $x \in X$ and $y \in Y$.

Example 4.11 (Galois connections)**.**

(i) Let $\mathbb{X}$ be a poset. Given a set $Y \subseteq X$, we define

$$Y^u := \{x \in X : x \text{ is an upper bound of } Y\}$$
$$Y^l := \{x \in X : x \text{ is a lower bound of } Y\}.$$

These operations can be viewed as maps

$$(-)^u\colon \mathcal{P}(X) \to \mathcal{P}(X) \text{ and } (-)^l\colon \mathcal{P}(X) \to \mathcal{P}(X).$$

Notice that $\langle (-)^u, (-)^l\rangle$ is a Galois connection between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(X); \subseteq\rangle$. To prove this, consider $Y, Z \subseteq X$. We have

$$\begin{aligned} Z \subseteq Y^u &\iff Z \text{ is a set of upper bounds of } Y \\ &\iff Y \text{ is a set of lower bounds of } Z \\ &\iff Y \subseteq Z^l. \end{aligned}$$

(ii) Every polarity $\langle X, Y, R\rangle$ induces a Galois connection as follows. Let

$$(-)^{\triangleright}\colon \mathcal{P}(X) \to \mathcal{P}(Y) \text{ and } (-)^{\triangleleft}\colon \mathcal{P}(Y) \to \mathcal{P}(X)$$

be the maps defined, for every $A \subseteq X$ and $B \subseteq Y$, as

$$A^{\triangleright} := \{y \in Y : \langle x, y\rangle \in R, \text{for all } x \in A\}$$
$$B^{\triangleleft} := \{x \in X : \langle x, y\rangle \in R, \text{for all } y \in B\}.$$

Then $\langle (-)^{\triangleright}, (-)^{\triangleleft}\rangle$ is a Galois connection between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$. ⊠

*Exercise** 4.12. Prove that if $\langle X, Y, R\rangle$ is a polarity, then $\langle (-)^{\triangleright}, (-)^{\triangleleft}\rangle$ is a Galois connection between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$. Then show that every Galois connection between $\langle \mathcal{P}(X); \subseteq\rangle$ and $\langle \mathcal{P}(Y); \subseteq\rangle$ arises in this way. ⊠

The following notion is instrumental to described Galois connections.

Definition 4.13. A *closure* on a poset $\mathbb{X}$ is a map $\gamma\colon X \to X$ such that, for every $x, y \in X$,

(i) $x \leqslant \gamma(x)$;

(ii) $\gamma(x) = \gamma(\gamma(x))$; and

(iii) if $x \leqslant y$, then $\gamma(x) \leqslant \gamma(y)$.

Notice that (ii) can be equivalently replaced by the demand that $\gamma(\gamma(x)) \leqslant \gamma(x)$.

Notice that closures abstract the behaviour of closure operators in the sense that the closures on powerset lattices $\langle \mathcal{P}(X); \subseteq\rangle$ are precisely the closure operators on X. Further examples of closers arise from Galois connections, as we proceed to explain.

Example 4.14 (Closures)**.** Let $\langle f, g\rangle$ be a Galois connection between $\mathbb{X}$ and $\mathbb{Y}$. Then the compositions

$$\gamma := g \circ f \quad \text{and} \quad \delta := f \circ g$$

are closures on $\mathbb{X}$ and $\mathbb{Y}$, respectively. Furthermore, the restrictions

$$f\restriction_{\gamma[X]}\colon \gamma[X] \to \delta[Y] \quad \text{and} \quad g\restriction_{\delta[Y]}\colon \delta[Y] \to \gamma[X]$$

are well-defined isomorphisms, one inverse to the other, between the posets $\langle \gamma[X]; \leqslant^{\mathbb{X}}\rangle$ and $\langle \delta[Y]; \geqslant^{\mathbb{Y}}\rangle$.

To prove this, consider $x, y \in X$. Recall that $\langle f, g\rangle$ is a residuated pair between $\mathbb{X}$ and $\mathbb{Y}^{\partial}$ and, therefore, it falls in the scope of Proposition 4.6. Accordingly, from conditions (i) and (v) of Proposition 4.6 it follows

$$x \leqslant^{\mathbb{X}} g(f(x)) = g(f(g(f(x)))),$$

that is, $x \leqslant^{\mathbb{X}} \gamma(x) = \gamma(\gamma(x))$. Lastly, by condition (iv) of Proposition 4.6, the maps $f\colon \mathbb{X} \to \mathbb{Y}^{\partial}$ and $g\colon \mathbb{Y}^{\partial} \to \mathbb{X}$ are order preserving. As a consequence, the composition $\gamma = g \circ f$ is order preserving on $\mathbb{X}$. Hence, we conclude that γ is a closure on $\mathbb{X}$. A similar argument shows that δ is a closure on $\mathbb{Y}$, the only (small) difference being the proof that $y \leqslant^{\mathbb{Y}} f(g(y)) = \delta(y)$, for all $y \in Y$. To prove this, recall that $\langle f, g\rangle$ is a residuated pair between $\mathbb{X}$ and $\mathbb{Y}^{\partial}$. As the poset $\mathbb{Y}$ appears here with the dual order, from condition (i) of Proposition 4.6 it follows that $y \geqslant^{\mathbb{Y}} f(g(y))$, as desired.

Then consider the restrictions $f\restriction_{\gamma[X]}\colon \gamma[X] \to \delta[Y]$ and $g\restriction_{\delta[Y]}\colon \delta[Y] \to \gamma[X]$. Notice that they are well-defined, since

$$f(\gamma(x)) = f(g(f(x))) \in \delta[Y] \quad \text{and} \quad g(\delta(y)) = g(f(g(y))) \in \gamma[X],$$

for all $x \in X$ and $y \in Y$. Furthermore, as we mentioned, $f\colon \mathbb{X} \to \mathbb{Y}^\partial$ and $g\colon \mathbb{Y}^\partial \to \mathbb{X}$ are order preserving maps, consequently, the restrictions

$$f\restriction_{\gamma[X]}\colon \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle \to \langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle \quad \text{and} \quad g\restriction_{\delta[Y]}\colon \langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle \to \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle$$

are also order preserving. To prove that they are one inverse to the other, consider $x \in \gamma[X]$ and $y \in \delta[Y]$. Since γ and δ are closures, $x = \gamma(x)$ and $y = \delta(y)$, that is, $x = g(f(x))$ and $y = f(g(y))$, as desired. To prove that $f\restriction_{\gamma[X]}$ and $g\restriction_{\delta[Y]}$ are isomorphisms, it only remains to show that they are order reflecting. We detail the case of $f\restriction_{\gamma[X]}$ only, as that of $g\restriction_{\delta[Y]}$ is analogous. To this end, consider $x, z \in \gamma[X]$ such that $f(x) \geqslant^{\mathbb{Y}} f(z)$. As $g\restriction_{\delta[Y]}$ is order preserving and $f\restriction_{\gamma[X]}$ and $g\restriction_{\delta[Y]}$ are one inverse to the other,

$$x = g(f(x)) \leqslant^{\mathbb{X}} g(f(z)) = z. \qquad \boxtimes$$

The relation between closures and Galois connections is made precise by the following result.

Theorem 4.15. *Let $\mathbb{X}$ and $\mathbb{Y}$ be posets, $f\colon X \to Y$, and $g\colon Y \to X$. The pair $\langle f, g\rangle$ is a Galois connection between $\mathbb{X}$ and $\mathbb{Y}$ if and only if there are two closures γ and δ, on $\mathbb{X}$ and $\mathbb{Y}$ respectively, and an isomorphism $h\colon \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle \to \langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle$ such that*

$$f = h \circ \gamma \quad \text{and } g = h^{-1} \circ \delta.$$

Proof. First, suppose that $\langle f, g\rangle$ is a Galois connection between $\mathbb{X}$ and $\mathbb{Y}$. In Example 4.14 we showed that $\gamma := g \circ f$ and $\delta := f \circ g$ are closures on $\mathbb{X}$ and $\mathbb{Y}$, respectively, and that the map

$$h := f\restriction_{\gamma[X]}\colon \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle \to \langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle$$

is an isomorphism such that $h^{-1} = g\restriction_{\delta[Y]}$. From condition (v) of Proposition 4.6 it follows that $f = h \circ \gamma$ and $g = h^{-1} \circ \delta$.

Conversely, suppose that γ, δ, and h are as in the statement. Then consider the maps $f := h \circ \gamma$ and $g := h^{-1} \circ \delta$. For every $x \in X$ and $y \in Y$, we have

$$\begin{aligned} y \leqslant^{\mathbb{Y}} f(x) &\iff y \leqslant^{\mathbb{Y}} h(\gamma(x)) \\ &\iff \delta(y) \leqslant^{\mathbb{Y}} h(\gamma(x)) \\ &\iff \gamma(x) \leqslant^{\mathbb{X}} h^{-1}(\delta(y)) \\ &\iff x \leqslant^{\mathbb{X}} h^{-1}(\delta(x)) \\ &\iff x \leqslant^{\mathbb{X}} g(y). \end{aligned}$$

The first and the last equivalences above follows from the definitions of f and g, respectively. The third follows from the fact that $h :=: \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle \to \langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle$ is an isomorphism. Lastly, the second holds because δ is a closure and $h(\gamma(x))$ one of its fixed points (since $h\colon \gamma[X] \to \delta[Y]$). The fourth follows from a similar argument. $\boxtimes$

As a consequence, we obtain the following description of closures.

Corollary 4.16. *A map $\gamma\colon X \to X$ is a closure on a poset $\mathbb{X}$ if and only if there exists a Galois connection $\langle f, g\rangle$ between $\mathbb{X}$ and some poset $\mathbb{Y}$ such that $\gamma = g \circ f$.*

Proof. The "if" part was established in Example 4.14. To prove the converse, suppose that γ is a closure on $\mathbb{X}$. Then let

$$\mathbb{Y} := \langle \gamma[X]; \geqslant^{\mathbb{X}} \rangle$$

and δ the identity map on Y. Clearly, δ is a closure on $\mathbb{Y}$. Furthermore,

$$\langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle = \langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle.$$

Consequently, the identity map $h\colon \gamma[X] \to \delta[Y]$ is an isomorphism from $\langle \gamma[X]; \leqslant^{\mathbb{X}} \rangle$ to $\langle \delta[Y]; \geqslant^{\mathbb{Y}} \rangle$.

Now, set $f := h \circ \gamma$ and $g := h^{-1} \circ \delta$. From Theorem 4.15 it follows that $\langle f, g\rangle$ is a Galois connection between $\mathbb{X}$ and $\mathbb{Y}$. Furthermore, as h and δ are identity maps,

$$g \circ f = h^{-1} \circ \delta \circ h \circ \gamma = \gamma. \qquad \boxtimes$$

4.2 Completions

Definition 4.17. A *completion* of a poset $\mathbb{X}$ is a pair $\langle f, \mathbb{Y}\rangle$, where $\mathbb{Y}$ is a complete lattice and $f\colon \mathbb{X} \to \mathbb{Y}$ an order embedding.

Our aim to to establish a correspondence between polarities and completions. To this end, it is convenient to introduce the following concept.

Definition 4.18. A polarity $\langle \mathcal{F}, \mathcal{I}, R\rangle$ is said to be *compatible* with a poset $\mathbb{X}$ if

(i) $\mathcal{F}$ is set of upsets of $\mathbb{X}$ containing the principal ones;

(ii) $\mathcal{I}$ is a set of downsets of $\mathbb{X}$ containing the principal ones;

(iii) for every $x \in X$ and $F \in \mathcal{F}$ and $I \in \mathcal{I}$,

$$x \in F \iff \langle F, {\downarrow}x\rangle \in R \quad \text{and} \quad x \in I \iff \langle {\uparrow}x, I\rangle \in R;$$

(iv) for every $F, G \in \mathcal{F}$ and $I, J \in \mathcal{I}$,

$$\text{if } F \subseteq G \text{ and } \langle F, I\rangle \in R, \text{ then } \langle G, I\rangle \in R$$

and

$$\text{if } I \subseteq J \text{ and } \langle F, I\rangle \in R, \text{ then } \langle F, J\rangle \in R.$$

Example 4.19 (Compatible polarities)**.** Let $\mathbb{X}$ be a poset, $\mathcal{F}$ a set of upsets containing the principal ones, and $\mathcal{I}$ a set of downsets containing the principal ones. Then let $R \subseteq \mathcal{F} \times \mathcal{I}$ be the relation defined, for every $F \in \mathcal{F}$ and $I \in \mathcal{I}$, as

$$\langle F, I\rangle \in R \iff F \cap I \neq \emptyset.$$

Then the polarity $\langle \mathcal{F}, \mathcal{I}, R\rangle$ is compatible with $\mathbb{X}$. Furthermore, if $\langle \mathcal{F}, \mathcal{I}, S\rangle$ is also a polarity compatible with $\mathbb{X}$, then $R \subseteq S$. To prove this, suppose that $\langle F, I\rangle \in R$. Then there exists $x \in F \cap I$. Since $x \in F$, from condition (iii) in the definition of a compatible polarity it follows that $\langle F, {\downarrow}x\rangle \in S$. Furthermore, since $x \in I$ and I is a downset, ${\downarrow}x \subseteq I$. By condition (iii) in the definition of a compatible polarity, we conclude that $\langle F, I\rangle \in S$. Thus, $R \subseteq S$, as desired. $\boxtimes$

Polarities compatible with a poset $\mathbb{X}$ can be used to construct completions of X, as we proceed to explain.

Proposition 4.20. *Let $\langle \mathcal{F}, \mathcal{I}, R\rangle$ be a polarity compatible with a poset $\mathbb{X}$ and $\mathbb{Y}$ the closure system associated with the closure operator $(-)^{\triangleright\triangleleft}\colon \mathcal{P}(\mathcal{F}) \to \mathcal{P}(\mathcal{F})$. Moreover, let $f\colon \mathbb{X} \to \mathbb{Y}$ be the map defined by the rule*

$$f(x) := \{F \in \mathcal{F} : x \in F\}.$$

Then the pair $\langle f, \mathbb{Y}\rangle$ is a completion of $\mathbb{X}$ such that every element of $\mathbb{Y}$ is both a meet of joins and a join of meets of elements of $f[X]$.

Proof. We begin by proving that f is well-defined. To this end, it suffices to show that

$$f(x) = \{\uparrow x\}^{\triangleright\triangleleft}, \text{ for all } x \in X.$$

Accordingly, let $F \in \mathcal{F}$. We have

$$\begin{aligned} F \in \{\uparrow x\}^{\triangleright\triangleleft} &\iff \langle F, I\rangle \in R, \text{ for all } I \in \mathcal{I} \text{ such that } \langle \uparrow x, I\rangle \\ &\iff \langle F, I\rangle \in R, \text{ for all } I \in \mathcal{I} \text{ such that } x \in I \\ &\iff \langle F, \downarrow x\rangle \in R \\ &\iff x \in F \\ &\iff F \in f(x). \end{aligned}$$

The first equivalence above follows from the definition of the maps $(-)^{\triangleright}$ and $(-)^{\triangleleft}$, the second and the fourth follow from condition (iii) in the definition of a compatible polarity, the third from $\downarrow y \in \mathcal{I}$ and condition (iv) in the definition of a compatible polarity, and the last one from the definition of F. Thus, f is well-defined.

Moreover, for every $x, y \in X$,

$$x \leqslant^{\mathbb{X}} y \iff f(x) \leqslant^{\mathbb{Y}} f(y).$$

The implication from left to right follows immediately from the definition of f and the fact that $\mathcal{F}$ is a set of upsets of $\mathbb{X}$. To prove the converse, suppose that $f(x) \leqslant^{\mathbb{Y}} f(y)$. Since $\uparrow x \in \mathcal{F}$, whence $\uparrow x \in f(x)$. Since the order relation of $\mathbb{Y}$ is the inclusion, we obtain $\uparrow x \in f(y)$, whence $y \in \uparrow x$, that is, $x \leqslant^{\mathbb{X}} y$. We conclude that f is an order embedding.

This shows that $\langle f, \mathbb{Y}\rangle$ is a completion of $\mathbb{X}$. It only remains to prove that every element of $\mathbb{Y}$ is both a meet of joins and a join of meets of elements of $f[X]$. To this end, consider a $Z \in Y$. We shall prove that

$$Z = \bigvee_{F \in Z}^{\mathbb{Y}} \bigwedge^{\mathbb{Y}} f[F] \quad \text{and} \quad Z = \bigwedge_{I \in Z^{\triangleright}}^{\mathbb{Y}} \bigvee^{\mathbb{Y}} f[I]. \tag{4.1}$$

To prove the first equality above, observe that, Z is an upset of $\langle \mathcal{F}; \subseteq\rangle$. To prove this, consider $F, G \in \mathcal{F}$ such that $F \in Z$ and $F \subseteq G$. Since $F \in Z$, for every $I \in Z^{\triangleright}$, we have $\langle F, I\rangle \in R$. By condition (iv) in the definition of a compatible polarity, we obtain $\langle G, I\rangle \in R$, for all $I \in Z^{\triangleright}$. Hence, $G \in Z^{\triangleright\triangleleft} = Z$, as desired.

Then consider an element $G \in Z$. From the definition of f and the fact that meets in $\mathbb{Y}$ are intersections (because $\mathbb{Y}$ is a closure system), it follows

$$G \in \bigcap_{x \in G} f(x) = \bigcap f[G] = \bigwedge^{\mathbb{Y}} f[G].$$

Moreover, as $G \in Z$ and $\leqslant^{\mathbb{Y}}$ is the inclusion relation,

$$G \in \bigwedge^{\mathbb{Y}} f[G] \subseteq \bigvee_{F \in Z}^{\mathbb{Y}} \bigwedge^{\mathbb{Y}} f[F].$$

To prove the other inclusion, $F \in Z$. We have

$$\bigwedge^{\mathbb{Y}} f[F] = \bigcap_{x \in F} f(x) = \{G \in \mathcal{F} : F \subseteq G\}.$$

Since $F \in Z$ and Z is an upset of $\langle \mathcal{F}; \subseteq \rangle$, this yields $\bigwedge^{\mathbb{Y}} f[F] \subseteq Z$ (that is, $\bigwedge^{\mathbb{Y}} f[F] \leqslant^{\mathbb{Y}} Z$), whence

$$\bigvee_{F \in Z}^{\mathbb{Y}} \bigwedge^{\mathbb{Y}} f[F] \leqslant^{\mathbb{Y}} Z.$$

This establishes the first equality in (4.1).

To prove the second equality in (4.1), let $\mathbb{V}$ be the closure system associated with the closure operator $(-)^{\triangleleft\triangleright}$ on $\mathcal{I}$. Furthermore, recall from Example 4.14 that the map

$$(-)^{\triangleright} \colon \mathbb{Y} \to \mathbb{V}^{\partial}$$

is a well-defined isomorphism. Therefore, in order to prove the second equality in (4.1), it suffices to show that

$$Z^{\triangleright} = \bigvee_{I \in Z^{\triangleright}}^{\mathbb{V}} \bigwedge_{x \in I}^{\mathbb{V}} (f(x))^{\triangleright}.$$

Using the fact that $Z^{\triangleright}$ is an upset of $\langle \mathcal{I}; \subseteq \rangle$ and that $(f(x))^{\triangleright} = \{I \in \mathcal{I} : x \in I\}$, for all $x \in X$, we can replicate the proof that we used for the first equality in (4.1). ⊠

Remark 4.21. Even if we will not pursue this here, it can be shown that the completions $\langle f, \mathbb{Y} \rangle$ of a poset $\mathbb{X}$ such that every element of $\mathbb{Y}$ is both a meet of joins and a join of meets of elements of $f[X]$ are in one-to-one correspondence with polarities that are compatible with $\mathbb{X}$. ⊠

In view of the above result, every polarity $\langle \mathcal{F}, \mathcal{I}, R \rangle$ compatible with a poset $\mathbb{X}$ can be associated with a completion $\langle f, \mathbb{Y} \rangle$ of $\mathbb{X}$. We call $\langle f, \mathbb{Y} \rangle$ the completion of $\mathbb{X}$ *induced* by $\langle \mathcal{F}, \mathcal{I}, R \rangle$.

4.3 Structural properties

Let $\langle f, \mathbb{Y} \rangle$ be a completion of a poset $\mathbb{X}$. We say that f *preserves existing binary meets* if

$$f(x \wedge^{\mathbb{X}} y) = f(x) \wedge^{\mathbb{Y}} f(y),$$

for every $x, y \in X$ such that the meet of x and y exists in $\mathbb{X}$. The statement that f preserves binary joins should be interpreted similarly. The same applies to statements demanding that f preserves arbitrary existing meets or joins.

Proposition 4.22. *Let $\langle f, \mathbb{Y}\rangle$ be the completion of a poset $\mathbb{X}$ induced by a polarity $\langle \mathcal{F}, \mathcal{I}, R\rangle$ compatible with $\mathbb{X}$. Then the following conditions hold:*

(i) *f preserves existing binary meets if and only if the elements of $\mathcal{F}$ are closed under existing binary meets;*

(ii) *f preserves existing binary joins if and only if the elements of $\mathcal{I}$ are closed under existing binary joins;*

(iii) *f preserves existing arbitrary meets if and only if the elements of $\mathcal{F}$ are closed under existing arbitrary meets;*

(iv) *f preserves existing arbitrary joins if and only if the elements of $\mathcal{I}$ are closed under existing arbitrary joins.*

Proof. We detail the proof of (i), as an exemplification. Consider $x, y \in X$ such that the meet of x and y exists in $\mathbb{X}$. We need to prove that

$$f(x \wedge^{\mathbb{X}} y) = f(x) \wedge^{\mathbb{Y}} f(y) \iff x \wedge^{\mathbb{X}} y \in F, \text{for all } F \in \mathcal{F} \text{ such that } x, y \in F.$$

We have

$$\begin{aligned} f(x \wedge^{\mathbb{X}} y) = f(x) \wedge^{\mathbb{Y}} f(y) &\iff f(x \wedge^{\mathbb{X}} y) = f(x) \cap f(y) \\ &\iff x \wedge^{\mathbb{X}} y \in F \text{ if and only if } x, y \in F, \text{for all } F \in \mathcal{F} \\ &\iff x \wedge^{\mathbb{X}} y \in F, \text{for all } F \in \mathcal{F} \text{ such that } x, y \in F. \end{aligned}$$

The first equivalence above follows from the fact that meets in $\mathbb{Y}$ are intersections, the second from the definition of f, and the last one from the fact $\mathcal{F}$ is a set of upsets of $\mathbb{X}$ and $x \wedge^{\mathbb{X}} y \leqslant x, y$. ⊠

Notably, completions induced by polarities preserve the property of being finite.

Proposition 4.23. *Let $\langle f, \mathbb{Y}\rangle$ be the completion of a poset $\mathbb{X}$ induced by a polarity compatible with $\mathbb{X}$. If $\mathbb{X}$ is finite, $\mathbb{Y}$ is also finite.*

Proof. Let $\langle \mathcal{F}, \mathcal{I}, R\rangle$ be the polarity that induces $\langle f, \mathbb{Y}\rangle$. Then

$$Y \subseteq \mathcal{P}(\mathcal{F}) \subseteq \mathcal{P}(\mathcal{P}(X))$$

and, therefore, $|Y| \leqslant 2^{2^{|X|}}$. Since X is finite, we conclude that so is Y. ⊠

4.4 Dedekind-MacNeille completions

Given a poset $\mathbb{X}$, let $\langle \mathcal{F}, \mathcal{I}, R\rangle$ be the polarity, where

$$\mathcal{F} = \{\uparrow x : x \in X\} \quad \text{and} \quad \mathcal{I} = \{\downarrow x : x \in X\}$$

and R is the relation of "having nonempty intersection", i.e.,

$$\langle F, I\rangle \in R \iff F \cap I \neq \emptyset.$$

In view of Remark 4.19, this polarity is compatible with $\mathbb{X}$. Because of this, the following definition makes sense.

Definition 4.24. The *Dedekind-MacNeille completion* of $\mathbb{X}$ is the completion of $\mathbb{X}$ induced by $\langle \mathcal{F}, \mathcal{I}, R \rangle$.

The Dedekind-MacNeille completion of a poset $\mathbb{X}$ admits a very transparent description, as we proceed to explain. Recall from Example 4.11 that the maps

$$(-)^u \colon \mathcal{P}(X) \to \mathcal{P}(X) \text{ and } (-)^l \colon \mathcal{P}(X) \to \mathcal{P}(X)$$

form a Galois connection between $\langle \mathcal{P}(X); \subseteq \rangle$ and itself. Therefore, in view of Example 4.14, the composition

$$(-)^{ul} \colon \mathcal{P}(X) \to \mathcal{P}(X)$$

is a closure operator on X, whose closed sets are precisely subsets Y of X such that $Y = Y^{ul}$. It turns out that the Dedekind-MacNeille completion of $\mathbb{X}$ can be identified with the closure system associated with $(-)^{ul}$.

Theorem 4.25. *Let $\langle f, \mathbb{Y} \rangle$ be the Dedekind-MacNeille completion of a poset $\mathbb{X}$ and Z the closure system associated with the closure operator $(-)^{ul} \colon \mathcal{P}(X) \to \mathcal{P}(X)$. Then $\mathbb{Y}$ is isomorphic to $\mathbb{Z} = \langle Z; \subseteq \rangle$ via the map $g \colon Y \to Z$, defined by the rule*

$$g(y) \coloneqq \{x \in X : {\uparrow}x \in y\}.$$

Proof. Let $\langle \mathcal{F}, \mathcal{I}, R \rangle$ be the polarity that induces the Dedekind-MacNeille completion of $\mathbb{X}$ and

$$(-)^{\triangleright} \colon \mathcal{P}(\mathcal{F}) \to \mathcal{P}(\mathcal{I}) \text{ and } (-)^{\triangleleft} \colon \mathcal{P}(\mathcal{I}) \to \mathcal{P}(\mathcal{F})$$

the associated Galois connection between $\langle \mathcal{P}(\mathcal{F}); \subseteq \rangle$ and $\langle \mathcal{P}(\mathcal{I}); \subseteq \rangle$.

In order to prove that g is well-defined, consider $y \in Y$. We need to show that $\{x \in X : {\uparrow}x \in y\}$ is a closed set of $(-)^{ul}$. Clearly, $\{x \in X : {\uparrow}x \in y\} \subseteq X$. Therefore, since $(-)^{ul}$ is a closure operator on X, it suffices to prove the inclusion

$$\{x \in X : {\uparrow}x \in y\}^{ul} \subseteq \{x \in X : {\uparrow}x \in y\}.$$

To this end, consider an element $z \in X \smallsetminus \{x \in X : {\uparrow}x \in y\}$. Clearly, ${\uparrow}z \notin y$. We need to show that $z \notin \{x \in X : {\uparrow}x \in y\}^{ul}$. Since Y is the closure system associated with the closure operator $(-)^{\triangleright\triangleleft}$ on $\mathcal{F}$ and $y \in Y$, we know that $y = y^{\triangleright\triangleleft}$. In particular, ${\uparrow}z \notin y = y^{\triangleright\triangleleft}$. By the definition of $(-)^{\triangleright\triangleleft}$, this means that there exists $I \in \mathcal{I}$ such that $I \in y^{\triangleright}$ and $\langle {\uparrow}z, I \rangle \notin R$. Recall that $\mathcal{F}$ and $\mathcal{I}$ are, respectively, the sets of principal upsets and principal downsets of $\mathbb{X}$, and that R is the relation of "having nonempty intersection". In particular, $I = {\downarrow}v$, for some $v \in X$. Bearing this in mind, from $\langle {\uparrow}z, I \rangle \notin R$ it follows that ${\uparrow}z \cap {\downarrow}v = \emptyset$, that is, $z \not\leqslant v$. We shall prove that v is an upper bound of $\{x \in X : {\uparrow}x \in y\}$. To this end, consider an element $w \in \{x \in X : {\uparrow}x \in y\}$. Then ${\uparrow}w \in y = y^{\triangleright\triangleleft}$. Since ${\downarrow}v = I \in y^{\triangleright}$, this implies $\langle {\uparrow}w, {\downarrow}v \rangle \in R$, that is, ${\uparrow}w \cap {\downarrow}v \neq \emptyset$. As a consequence, $w \leqslant v$. Hence, we conclude that $v \in \{x \in X : {\uparrow}x \in y\}^u$. Since $z \not\leqslant v$, we obtain that $z \notin \{x \in X : {\uparrow}x \in y\}^{ul}$, as desired. Thus, g is well-defined.

The fact that g is order preserving is an immediate consequence of its definition. To prove that it is also order reflecting, consider $y, z \in Y$ such that $g(y) \subseteq g(z)$ and $F \in y$. Since $\mathcal{F}$ is the set of principal upsets of $\mathbb{X}$, there exists $x \in X$ such that $F = {\uparrow}x$. By the definition of g, this yields $x \in g(y)$. Furthermore, $x \in g(z)$, since $g(y) \subseteq g(z)$. Thus, the definition of g implies that $F = {\uparrow}x \in z$. We conclude that $y \subseteq z$, as desired.

Hence, g is an order embedding. It only remains to prove that it is surjective. To this end, consider $V \in Z$ and set

$$y := \{\uparrow x : x \in V\}.$$

It suffices to prove that $y \in Y$, because, in that case, $g(y) = V$. To this end, it is enough to show that $y^{\triangleright\triangleleft} \subseteq y$. Then consider an arbitrary element $F \in \mathcal{F} \smallsetminus y$. Since $\mathcal{F}$ is the set of principal upsets of $\mathbb{X}$, there exists $x \in X$ such that $F = \uparrow x$. Moreover, $x \in X \smallsetminus V$, otherwise $\uparrow x \in y$. As $V = V^{ul}$, there exists an upper bound z of V such that $x \not\leqslant z$. Observe that $\downarrow z \in \mathcal{I}$. Moreover, the fact that z is an upper bound of V guarantees that $\downarrow z$ has nonempty intersection with every members of y. Consequently, $\downarrow z \in y^{\triangleright}$. Lastly, since $x \not\leqslant z$, we have $\uparrow x \cap \downarrow z = \emptyset$, that is, $\langle \uparrow x, \downarrow z\rangle \notin R$. Hence, $F = \uparrow x \notin y^{\triangleright\triangleleft}$, as desired. ⊠

In view of the above theorem, it is natural to identify the Dedekind-MacNeille completion of a poset $\mathbb{X}$ with the pair $\langle f, \mathbb{Y}\rangle$, where $\mathbb{Y}$ is the closure system associated with the closure operator $(-)^{ul} \colon \mathcal{P}(X) \to \mathcal{P}(X)$ on X and $f \colon X \to Y$ the map defined by the rule

$$f(x) := \downarrow x.$$

Now, a *cut* in a chain $\mathbb{X}$ is a downset which is principal or its complement is not principal. Under the above identification, we obtain the following.

Corollary 4.26. *The Dedekind-MacNeille completion of a chain $\mathbb{X}$ is the pair $\langle f, \mathbb{Y}\rangle$, where $\mathbb{Y}$ is the set of cuts of $\mathbb{X}$ and $f \colon \mathbb{X} \to \mathbb{Y}$ is the map defined by the rule $f(x) := \downarrow x$.*

Proof. This is a consequence of the fact that the cuts of $\mathbb{X}$ are precisely the closed sets of the closure operator $(-)^{ul} \colon \mathcal{P}(X) \to \mathcal{P}(X)$. ⊠

As a consequence, the Dedekind-MacNeille completion of the poset of rational numbers $\langle \mathbb{Q}; \leqslant\rangle$ is the set of its cuts, which is well known to be isomorphic to the expansion of $\langle \mathbb{R}; \leqslant\rangle$ with infinity points. This is why Dedekind-MacNeille completions generalize Dedekind's classical construction of the real numbers as "cuts" of the rational ones.

As we proceed to explain, Dedekind-MacNeille completions can be used to obtain the an elegant proof of the decidability of the equational theory of lattices. First, the following is a direct consequence of Proposition 4.22 and the definition of Dedekind-MacNeille completions.

Proposition 4.27. *If $\langle f, \mathbb{Y}\rangle$ is the Dedekind-MacNeille completion of a poset $\mathbb{X}$, then f preserves existing arbitrary meets and joins.*

Furthermore, the set $\mathrm{Sub}(\varphi)$ of *subterms* of a lattice term φ is defined by recursion on the construction of φ, as follows. If x is a variable, then $\mathrm{Sub}(x) := \{x\}$. If ψ_1 and ψ_2 are lattice terms and $* \in \{\wedge, \vee\}$, then

$$\mathrm{Sub}(\psi_1 * \psi_2) := \mathrm{Sub}(\psi_1) \cup \mathrm{Sub}(\psi_2) \cup \{\psi_1 * \psi_2\}.$$

For instance,

$$\mathrm{Sub}(z \vee (x \wedge y)) = \{x, y, z, x \wedge y, z \vee (x \wedge y)\}.$$

Theorem 4.28 (McKinsey)**.** *If a lattice equation fails in a lattice, it fails in a finite lattice as well.*

Proof. Let $\varphi(x_1, \ldots, x_n)$ and $\psi(x_1, \ldots, x_n)$ be lattice terms such that the lattice equation $\varphi \approx \psi$ fails is some lattice $\boldsymbol{A}$. Therefore, there are $a_1, \ldots, a_n \in A$ such that

$$\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) \neq \psi^{\boldsymbol{A}}(a_1, \ldots, a_n).$$

Then consider the set

$$X := \{\delta^{\boldsymbol{A}}(a_1, \ldots, a_n) : \delta \in \mathrm{Sub}(\varphi) \cup \mathrm{Sub}(\psi)\}.$$

Notice that the subposet $\mathbb{X} = \langle X; \leqslant \rangle$ of $\boldsymbol{A}$ is finite, because every lattice term has only finitely many subterms. Then let $\langle f, \mathbb{Y} \rangle$ be the Dedekind-MacNeille completion of $\mathbb{X}$. Observe that $\mathbb{Y}$ is a finite lattice, by Proposition 4.23.

It only remains to prove that the equation $\varphi \approx \psi$ fails in $\mathbb{Y}$. Notice that it is sufficient to show that

$$\delta^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) = f(\delta^{\boldsymbol{A}}(a_1, \ldots, a_n)), \tag{4.2}$$

for every $\delta \in \mathrm{Sub}(\varphi) \cup \mathrm{Sub}(\psi)$. This is because, in this case,

$$\begin{aligned} \varphi^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) &= f(\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n)) \\ \psi^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) &= f(\psi^{\boldsymbol{A}}(a_1, \ldots, a_n)). \end{aligned}$$

Since f is injective and, by assumption, $\varphi^{\boldsymbol{A}}(a_1, \ldots, a_n) \neq \psi^{\boldsymbol{A}}(a_1, \ldots, a_n)$, we conclude that $\varphi^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) \neq \psi^{\mathbb{Y}}(f(a_1), \ldots, f(a_n))$, whence the equation $\varphi \approx \psi$ fails in $\mathbb{Y}$, as desired.

Then we turn to prove that condition (4.2) holds. We detail the case where $\delta \in \mathrm{Sub}(\varphi)$, as the case where $\delta \in \mathrm{Sub}(\psi)$ is analogous, and reason by induction on the construction of δ. In the base case, $\delta = x_i$, for some variable x_i. Then, obviously,

$$\delta^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) = f(a_i) = f(\delta^{\boldsymbol{A}}(a_1, \ldots, a_n)).$$

For the step case, suppose that $\delta = \varepsilon_1 * \varepsilon_2$ for some $\varepsilon_1, \varepsilon_2 \in \mathrm{Sub}(\varphi)$ and $* \in \{\wedge, \vee\}$. We detail the case where $* = \wedge$, as the one where $* = \vee$ is analogous. Since $\mathbb{X}$ is a subposet of $\boldsymbol{A}$ and

$$\varepsilon_1^{\boldsymbol{A}}(a_1, \ldots, a_n) \wedge^{\boldsymbol{A}} \varepsilon_2^{\boldsymbol{A}}(a_1, \ldots, a_n) = \delta^{\boldsymbol{A}}(a_1, \ldots, a_n) \in X,$$

we have that $\delta^{\boldsymbol{A}}(a_1, \ldots, a_n)$ is the meet of $\varepsilon_1^{\boldsymbol{A}}(a_1, \ldots, a_n)$ and $\varepsilon_2^{\boldsymbol{A}}(a_1, \ldots, a_n)$ in $\mathbb{X}$. As $f : \mathbb{X} \to \mathbb{Y}$ preserves existing binary meets, by Proposition 4.27, we conclude that

$$\begin{aligned} f(\delta^{\boldsymbol{A}}(a_1, \ldots, a_n)) &= f(\varepsilon_1^{\boldsymbol{A}}(a_1, \ldots, a_n) \wedge^{\mathbb{X}} \varepsilon_2^{\boldsymbol{A}}(a_1, \ldots, a_n)) \\ &= f(\varepsilon_1^{\boldsymbol{A}}(a_1, \ldots, a_n)) \wedge^{\mathbb{Y}} f(\varepsilon_2^{\boldsymbol{A}}(a_1, \ldots, a_n)). \end{aligned}$$

Moreover, by the inductive hypothesis, $f(\varepsilon_i^{\boldsymbol{A}}(a_1, \ldots, a_n)) = \varepsilon_i^{\mathbb{Y}}(f(a_1), \ldots, f(a_n))$ for $i = 1, 2$. Therefore, we conclude that $\delta^{\mathbb{Y}}(f(a_1), \ldots, f(a_n)) = f(\delta^{\boldsymbol{A}}(a_1, \ldots, a_n))$. ⊠

Corollary 4.29 (Whitman)**.** *The equational theory of lattices is decidable.*

Proof. It is well known that, in order to prove that a set X is recursive, it suffices to show that both X and its complement are recursively enumerable. As the equational theory of lattices is finitely axiomatizable, it is clearly recursively enumerable. It only remains to prove that its complement is also recursively enumerable. To this end,

consider the algorithm that, given a lattice equation $\varphi \approx \psi$, lists the finitely many (up to isomorphism) lattices with one element and check whether $\varphi \approx \psi$ fails in them. If so, it halts and accepts the input $\varphi \approx \psi$. Otherwise, it lists the finitely many (up to isomorphism) lattices with two elements and check whether $\varphi \approx \psi$ fails in them. If so, it halts and accepts the input $\varphi \approx \psi$. Otherwise, it lists the finitely many (up to isomorphism) lattices with three elements and so on. In view of Theorem 4.28, this algorithm enumerates the complement of the equational theory of lattices. ⊠

Remark 4.30. Whitman's decidability result is older than McKinsey's theorem and its original proof is substantially different from the one presented here. The reader might have noticed that McKinsey's theorem yields a stronger conclusion, i.e., that the quasiequational theory of lattices is decidable. Lastly, the proof of McKinsey's theorem described above is due to Dean. It is worth stressing that the same proof works if we replace in it the Dedekind-MacNeille completion with any completion induced by a compatible polarity $\langle \mathcal{F}, \mathcal{I}, R \rangle$ such that the elements of $\mathcal{F}$ are closed under existing binary meets and those of $\mathcal{I}$ under existing binary joins. ⊠

*Exercise** 4.31. Prove that every element of the Dedekind-MacNeille completion $\langle f, \mathbb{Y} \rangle$ of a poset $\mathbb{X}$ is both a join and a meet of elements of $f[X]$. To this end, you might wish to use the description of the Dedekind-MacNeille completion of $\mathbb{X}$ as the closure system associated of the closure operator $(-)^{ul} \colon \mathcal{P}(X) \to \mathcal{P}(X)$, but be careful: while meets in the Dedekind-MacNeille completion are intersections, joins are not unions. ⊠

Observe that the property in the above exercise strengthens the one in the statement of Proposition 4.20. A result of Banaschewski and Bruns states that this indeed a universal property of Dedekind-MacNeille completion, in the sense that the Dedekind-MacNeille completion of a poset $\mathbb{X}$ is the unique (up to isomorphism) completion $\langle f, \mathbb{Y} \rangle$ of $\mathbb{X}$ such that every element of Y is both a meet and a join of elements of $f[X]$.

Bibliography

[1] R. Balbes and P. Dwinger. *Distributive lattices*. University of Missouri Press, Columbia, Mo., 1974.

[2] C. Bergman. *Universal Algebra: Fundamentals and Selected Topics*. Chapman & Hall Pure and Applied Mathematics. Chapman and Hall/CRC, 2011.

[3] G. Birkhoff. *Lattice Theory*, volume XXV of *Colloquium Publications*. American Mathematical Society, Providence, 3rd. edition, 1973. (1st. ed. 1940).

[4] T. S. Blyth, editor. *Lattices and ordered algebraic structures*. Springer, 2006.

[5] S. Burris and H. P. Sankappanavar. *A course in Universal Algebra*. Available in internet https://www.math.uwaterloo.ca/~snburris/htdocs/ualg.html, the millennium edition, 2012.

[6] B. A. Davey and H. A. Priestley. *Introduction to lattices and order*. Cambridge University Press, New York, second edition, 2002.

[7] A. C. Davis. A characterization of complete lattices. *Pacific Journal of Mathematics*, 5:311–319, 1955.

[8] R. Dedekind. Ueber die von drei Moduln erzeugte Dualgruppe. *Mathematische Annalen*, 53:371–403, 1900.

[9] R. Freese. Free modular lattices. *Transactions of the Americal Mathematical Society*, 261:81–91, 1980.

[10] S. Givant and P. Halmos. *Introduction to Boolean Algebras*. Undergraduate Texts in Mathematics. Springer, 2009.

[11] G. Grätzer. *Lattice Theory: Foundation*. Birkhäusser, 2011.

[12] G. Grätzer and E. T. Schmidt. Characterizations of congruence lattices of abstract algebras. *Acta Sci. Math. (Szeged)*, 24:34–59, 1963.

[13] R. McKenzie. Para primal varieties: A study of finite axiomatizability and definable principal congruences in locally finite varieties. *Algebra Universalis*, 8:336–348, 1978.

[14] S. Roman. *Lattices and ordered sets*. Springer, New York, 2008.