UNIVERSITY OF PUERTO RICO
RIO PIEDRAS CAMPUS
FACULTY OF NATURAL SCIENCES
DEPARTMENT OF MATHEMATICS

ST-DISTRIBUTIVE AND *ST*-MODULAR LATTICES

By

Gustavo A. Meléndez Ríos

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

DATE
April 26, 2022

APPROVED BY THE MASTER OF SCIENCE ADVISORY COMMITTEE
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF
MASTER OF SCIENCE IN MATHEMATICS
AT THE UNIVERSITY OF PUERTO RICO

ADVISOR:

M. Reza Emamy-K., Ph.D.
Professor
Department of Mathematics

READERS:

Luis A. Medina Rivera, Ph.D.
Professor
Department of Mathematics

Ivelisse Rubio Canabal, Ph.D.
Professor
Department of Computer Science

Abstract

This thesis proposes two new classes of lattices: ST-distributive and ST-modular lattices. The idea is to define relative distributive and modular properties that are satisfied by some elements over two subsets S and T of a given lattice L. These new classes include the usual distributive and modular lattices. Our main results are (1) establishing some basic properties, (2) completely characterizing the maximal S and T (with some restrictions) to form ST-distributive lattices in the lattice families $\mathbf{M}_n$ and $\mathbf{M}_{n,n}$, and (3) presenting an application of ST-modular lattices to convex sets. This application has been the first example of ST-modularity and the original motivation of our work [7]. All this extends our work in [10]. In addition, we discuss two other problems with new results. First, we present two shortcuts to the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem proof in [5, 4] and design two methods to compare the lengths of the three proofs [11]. Second, we introduce a poset on the cut-complexes of the 4-cube and show that it is a distributive lattice [9].

Acknowledgments

I would like to thank my advisor Professor Reza Emamy for giving me this opportunity to work with him and for his patience and guidance during these past 3 years. I would also like to thank my readers Professors Ivelisse Rubio and Luis Medina for taking their time to read my thesis and for all of their valuable feedback. In addition, I would like to thank the Math Department at UPRRP for this opportunity to further my studies in mathematics, the organizers of SEICCGTC 2021 for the opportunity they gave me to present my work, and the staff at the library of the College of Natural Sciences for their help with my thesis defense. Finally, I would like to thank my family and everyone else who has supported me during my journey as a masters student in mathematics.

Contents

List of Figures

List of Tables

ST-DISTRIBUTIVE AND ST-MODULAR LATTICES

Chapter 1

Introduction

Welcome to the world of lattices! This thesis offers you a mathematical tour of this land. It will be a journey with many twists and turns that will hopefully give you a deeper appreciation of lattices and perhaps, an interest in doing research in this area (plus some ideas of where to begin). This introductory chapter will give you an idea of what to expect on the road ahead.

Lattices are fascinating algebraic structures that posses an order relation. They have been extensively studied since the days of Birkhoff [2] and have also being the subject of numerous books of which we highly recommend *Introduction to Lattices and Order* by Brian A. Davey and Hilary A. Priestley [5]. In addition, they have connections to diverse areas of mathematics such as set theory (power set lattices), number theory (whole number divisibility lattice), and convex polytopes (face lattices). They also include Boolean algebras which have well-known applications to computer science and logic. Furthermore, they are also studied in enumerative combinatorics [21]. They can even serve as inspiration for art! See Figure 1.1.

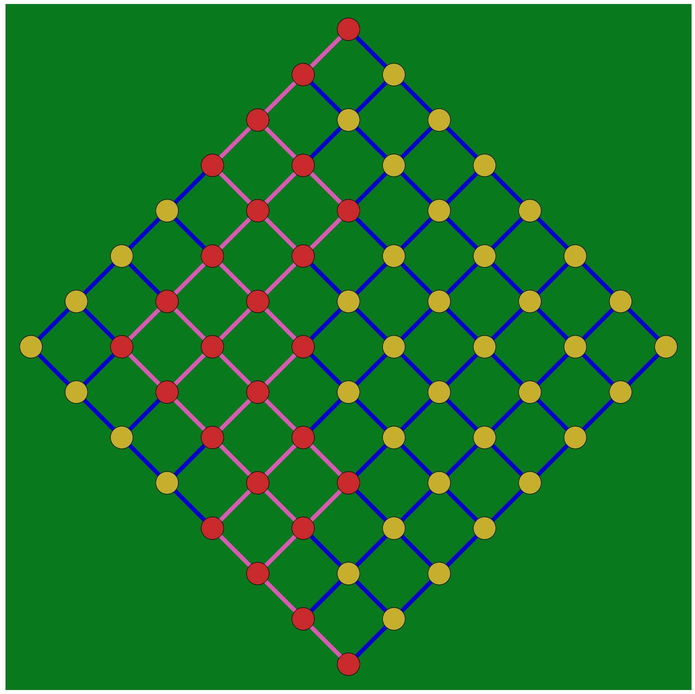


Figure 1.1: Lattice Art

This thesis proposes two new classes of lattices: ST-distributive and ST-modular lattices. These are lattices that satisfy a form of relative distributivity and relative modularity with respect to certain subsets S and T of them. The idea is somewhat similar to relative topologies. The following list summarizes the key achievements to be presented:

1. Define these two new classes of lattices.

2. Establish some elementary properties of them.

3. Characterize certain subsets inducing ST-distributivity in the lattice families $\mathbf{M}_n$ and $\mathbf{M}_{n,n}$.

4. Suggest an application of ST-modularity to convex sets via the lattice of convex sets. This application is the original motivation for these new classes of lattices.

We hope that this will help to start a new research area within lattices.

In addition to introducing ST-distributive and ST-modular lattices, this thesis provides a considerable amount of background on lattice theory starting from posets. It also gives a short summary on convex polytopes in order to help understand the application of ST-modularity to convexity. Along the way, we take two detours to present two additional new results:

1. Two shortcuts to a classical proof of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem with a discussion on how to compare the lengths of the proofs. We introduce two methods to compare the lengths of proofs based on algebraic lattice expressions. This is also in [11].

2. The cut-complex poset: an ordering on the set of cut-complexes of a hypercube that is a distributive lattice.

The rest of this thesis is organized as follows. Chapters 2-6 provide an overview of lattice theory that contains the needed background to understand ST-distributive and ST-modular lattices (and much more). These are introduced respectively in Chapters 8 and 9 after some background on convex polytopes in Chapter 7 for the aforementioned application. We now give a brief overview of each chapter; a more detailed description of the content of each can be found in its introduction section.

- Chapter 2 – Posets: We start from the very beginning by defining posets. We then discuss how to draw them with Hasse diagrams. A variety of concepts follow: maximal/minimal elements, down-sets, Duality Principle, poset constructs, and poset functions.

- Chapter 3 – Lattices: We introduce lattices and discuss their algebraic and order structures. We connect both structures and present the Connecting Lemma. We then touch several aspects: lattice constructs, lattice homomorphisms, irreducible elements, and complete lattices.

- Chapter 4 – Distributive and Modular Lattices: We define distributive and modular lattices. We establish numerous results, chief among them the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. We take the opportunity to present the previously mentioned shorter proofs of the aforementioned theorem and compare the lengths of our proofs with that of the proof in [5] (also in [4]).

- Chapter 5 – Characterization of Finite Distributive Lattice: We show Birkhoff's Representation Theorem for Finite Distributive Lattices which says that every finite distributive lattice is the down-set lattice of its set of join-irreducible elements. We also establish a 1-1 correspondence between finite distributive lattices and finite posets.

- Chapter 6 – Congruences in Lattices: We explore congruences on lattices. We discuss their characterization among equivalence relations, quotient lattices, the lattice of congruences on a lattice, and connections to distributivity.

- Chapter 7 – A New Cut-Complex Poset from Convex Polytopes: We give a short summary of convex polytopes to aid the understanding of the application of ST-modularity to them. We start from the very basics of convex sets and hyperplanes and then build up to convex polytopes. We then digress to cut-complexes in order to present the aforementioned cut-complex poset and show that it is a distributive lattice.

- Chapter 8 – ST-Distributive Lattices: We introduce ST-distributive lattices and establish some basic properties of them. We identify a sub-problem of finding all pairs of subsets (S, T) of a lattice L for which it is ST-distributive and define an algorithm to tackle it. We use this algorithm to solve this sub-problem for $L = \mathbf{M}_n$ and $L = \mathbf{M}_{n,n}$.

- Chapter 9 – ST-Modular Lattices: We present ST-modular lattices. This presentation includes some basic properties and an application to convex sets in which we translate an identity regarding convex sets into the language of lattices.

- Chapter 10 – Conclusion: We summarize the main research results of this thesis and present ideas for future work.

We have strived to make the material of this thesis as accessible as possible for graduate students in mathematics. Thus, we will assume only knowledge of some elementary concepts from group theory, topology, linear algebra, and graph theory. Nevertheless, a full course on these areas is not needed to follow this discussion and the latter three are only used starting in Chapter 7. As such, there are generally no formal prerequisites besides some familiarity with proofs and some mathematical maturity. In particular, we do not assume the reader has any background on posets and lattice theory.

Having established a road map of what is to come, we are ready to begin our journey to lattice land. We truly wish the reader an enjoyable ride full of memorable discoveries!

Chapter 2

Posets

2.1 Introduction

In this chapter, we begin our journey into the realm of lattices and order. The first step is to establish a rigorous mathematical definition of order. This will come in the form of partially ordered sets, or posets for short. The reader probably has encountered posets before even if they have not being identified as such. The set of reals in the number line and the power set of any set are examples of posets. Posets generalize these notions of order and permit the description of any collection of objects that can be ordered in some way. This opens the doors to the fascinating study of all sorts of properties of these orders. This chapter hopes to give the reader a taste of this since it is impossible to be exhaustive.

We provide an overview of the content and structure of the rest of this chapter. Section 2.2 defines what a poset is and provides some elementary examples: power sets, chains, and antichains. Section 2.3 then introduces the covering relation of a poset with the aim of explaining Hasse diagrams, which illustrate the order structure of a poset and can be used to specify a poset. Afterwards, Section 2.4 presents some basic concepts of posets such as sub-posets, maximal/minimal elements, top/bottom elements, and length.

Deeper waters are encountered starting from Section 2.5 with the discussion of down-sets and up-sets. The highly important notion of duality then enters the scene in Section 2.6 in the shape of dual posets and the Duality Principle. Methods of constructing new posets from existing ones are the main focus of the next three sections: products of posets appear in Section 2.7, unions of posets in Section 2.8, and linear sums of posets 2.9. Finally, the chapter comes to an end in Section 2.10 with the introduction of functions between posets and of order-isomorphisms.

2.2 Definitions and Examples

We introduce posets, which are partially ordered sets. The idea behind them is to take a set of elements and order it in some way. For instance, one can take a list of words and order it alphabetically or take a group of people and order them by ancestry. A poset captures these notions of order in a precise mathematical way. We now provide the formal definition of a poset followed by an example.

Definition 2.1. (*poset*) *A poset* $\langle P; \leq \rangle$ *is a set* P *with a relation* $\leq$ *on its elements that is reflexive, antisymmetric, and transitive. By these three conditions, we mean the following:*

1. *reflexive:* $a \leq a \; \forall a \in P$*;*

2. *antisymmetric:* $a \leq b$ *and* $b \leq a \implies a = b$*;*

3. *transitive:* $a \leq b$ *and* $b \leq c \implies a \leq c$*.*

Example 2.1. (*power set*) *Let* S *be a set. Then its power set, denoted by* $\wp(S)$*, with the inclusion relation* $\subseteq$ *gives the poset* $\langle \wp(S); \subseteq \rangle$*. Observe that* $\subseteq$ *satisfies the three conditions:*

1. *reflexive: For any subset* A *of* S*,* $A \subseteq A$*.*

2. *antisymmetric: Given two subsets* A *and* B *of* S*,* $A \subseteq B$ *and* $B \subseteq A$ *imply that* $A = B$*.*

3. *transitive: Given three subsets* A*,* B*, and* C *of* S*, if* $A \subseteq B$ *and* $B \subseteq C$*, then* $A \subseteq C$*.*

We now discuss what is meant by the word "partial" in partial order. The reason these orders are said to be partial is because it is possible that there are two elements that cannot be compared by the order relation. More precisely, we can have two elements a and b for which neither $a \leq b$ nor $b \leq a$ is true. When this happens, we say that a and b are non-comparable and write $a \,||\, b$.

Example 2.2. (*non-comparable elements*) *Consider the power set of the finite set* $S = \{a, b, c\}$*. Observe that* $\{a, b\}$ *and* $\{a, c\}$ *are both elements of* $\wp(S)$*. However, neither set contains the other:* $\{a, b\} \nsubseteq \{a, c\}$ *and* $\{a, c\} \nsubseteq \{a, b\}$*. Thus,* $\{a, b\}$ *and* $\{a, c\}$ *are non-comparable in* $\langle \wp(S); \subseteq \rangle$*,* $\{a, b\} \,||\, \{a, c\}$*.*

There are posets where any two elements can be compared. These are called chains or total orders.

Definition 2.2. (*chain*) *A chain is a poset* $\langle C; \leq \rangle$ *in which for any* $a, b \in C$, *we have that* $a \leq b$ *or* $b \leq a$.

Example 2.3. (*infinite chains of numbers*) *Consider the set of natural numbers* $\mathbb{N}$ *with the usual order, that is,* $a \leq b$ *if and only if* a *"is the less than or equal to"* b *in the usual sense. Then* $\langle \mathbb{N}; \leq \rangle$ *is a poset.*

1. *reflexive: For any natural number* n, $n \leq n$ *since* $n = n$.

2. *antisymmetric: If* m *and* n *are natural numbers with* $m \leq n$ *and* $n \leq m$, *then* $m = n$ *because otherwise we have* $m < n$ *and* $n < m$ *which is not possible.*

3. *transitive: If* k, m, *and* n *are natural numbers with* $k \leq m$ *and* $m \leq n$, *then* $k \leq n$ *because otherwise we have* $k > n \geq m \geq k$ *which implies* $k > k$, *a contradiction.*

In addition, $\langle \mathbb{N}; \leq \rangle$ *is also a chain because for any two natural numbers* a *and* b, $a \leq b$ *or* $b \leq a$. *Note that the same applies if we change* $\mathbb{N}$ *for* $\mathbb{Z}$, $\mathbb{Q}$, *or* $\mathbb{R}$.

Example 2.4. (*finite chains*) *For any natural number* n, *a chain of* n *elements can be formed by taking* $[n] = \{1, 2, 3, ..., n\}$ *with the usual order of* $\mathbb{N}$. *This is called the chain of* n *elements and is denoted* $\mathbf{n}$ (*bold* n).

At the other extreme of chain are antichains. These are posets in which each element is comparable only to itself under the poset's order relation.

Definition 2.3. (*antichain*) *An antichain is a poset* $\langle A; \leq \rangle$ *in which for any* $a, b \in A$, $a \leq b$ *if and only if* $a = b$. *In other words,* $a \neq b \implies a \,||\, b$.

Example 2.5. (*finite antichains*) *For any natural number n, an antichain of n elements can be formed by taking $[n] = \{1, 2, 3, ..., n\}$ and ordering it by equality $(=)$. This is called the antichain of n elements and is denoted $\bar{\mathbf{n}}$ (bold n with a bar).*

We conclude this section with two additional examples that are of interest in number theory and abstract algebra respectively.

Example 2.6. (*divisibility poset*) *Denote by $\mathbb{N}_0$ the set $\mathbb{N} \cup \{0\}$. Then $\mathbb{N}_0$ can be ordered by divisibility: $a \leq b$ if and only if a divides b (denoted $a|b$). Here, we define $a|b$ to mean that there is $k \in \mathbb{N}_0$ such that $b = ka$. The resulting poset is $\langle \mathbb{N}_0; | \rangle$ and is clearly not a chain.*

Example 2.7. (*subgroup posets*) *Let G be a group. Then we can order the set of all subgroups of G (denoted $Sub\,G$) by inclusion. The same can be done for the set of all normal subgroups of G ($\mathcal{N}$-$Sub\,G$). Both are subsets of the power set of G.*

2.3 Visual Representation

Now that we have defined what posets are, we present a method for visually representing them: Hasse diagrams. These diagrams permit visualizing the order structure of a poset. In addition, a poset can be defined by drawing its Hasse diagram. In order to explain how these diagrams are drawn, we must first introduce the covering relation of a poset.

The order relation of a poset induces a second relation on its elements that is called the covering relation of the poset. It identifies the immediate predecessors and successors of any element in the poset. An element x of a poset P is covered by y if y is strictly greater than x and there are no elements in between them (i.e. y is an immediate successor of x). To formalize this concept, we will need to establish a notion of strict inequality in a poset. Given a poset $\langle P; \leq \rangle$, we define a "strict order" $<$ on P by $x < y$ if and only if $x \leq y$ and $x \neq y$.

Definition 2.4. (*covering relation*) *In a poset P, we say that an element x is covered by another element y if $x < y$ and there is no $z \in P$ such that $x < z < y$. We denote this by $x \prec y$. We can also say that y covers x and write $y \succ x$.*

Example 2.8. (*natural numbers*) *In $\langle \mathbb{N}; \leq \rangle$, 2 is covered by 3 ($2 \prec 3$) because $2 < 3$ and there is no natural number n such that $2 < n < 3$. On the other hand, 2 is not covered by 4 because although $2 < 4$, we have that $3 \in \mathbb{N}$ and $2 < 3 < 4$.*

Example 2.9. (*power set*) *Consider the poset $\langle \wp(S); \subseteq \rangle$ with $S = \{a, b, c\}$. Then $\{a, b\}$ covers $\{a\}$ because $\{a\} \subsetneq \{a, b\}$ and there is no subset T of S such that*

$$\{a\} \subsetneq T \subsetneq \{a, b\}. \tag{2.1}$$

On the other hand, $\{a, b\}$ does not cover $\emptyset$ because although $\emptyset \subsetneq \{a, b\}$, we have that $\{a\} \in \wp(S)$ and $\emptyset \subsetneq \{a\} \subsetneq \{a, b\}$. Furthermore, it can be shown that, in general, for any set S and any $X, Y \subseteq S$, X is covered by Y if and only if $Y = X \cup \{z\}$ for some $z \in S \setminus X$.

We are now ready to introduce Hasse diagrams. The Hasse diagram of a (usually but not necessarily finite) poset is a graph-like drawing that represents its order

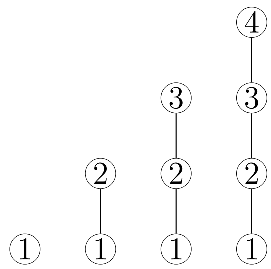


Figure 2.1: Chains **1**, **2**, **3**, and **4**

Figure 2.2: Antichains $\bar{\mathbf{1}}$, $\bar{\mathbf{2}}$, $\bar{\mathbf{3}}$, and $\bar{\mathbf{4}}$

structure. The idea is to be able identify comparable elements by examining the drawing: $x \leq y$ if and only if there exists an upward path from x to y. It is constructed using the covering relation.

Definition 2.5. (*Hasse diagram*) *Given a poset $\langle P; \leq \rangle$ with induced covering relation $-\!\!<$, its Hasse diagram is a graph drawing constructed following two rules:*

1. *Draw exactly one vertex for each element of P such that for any $x, y \in P$, $x < y$ implies that y's vertex is placed in a higher vertical position than x's vertex.*

2. *Draw an edge between every pair of vertices $x, y \in P$ for which $x -\!\!< y$.*

Example 2.10. (*Hasse diagrams of finite chains, finite antichains, and power set*)

1. *Figure 2.1 shows the Hasse diagrams of $\mathbf{n}$ for $1 \leq n \leq 4$.*

2. *Figure 2.2 shows the Hasse diagrams of $\bar{\mathbf{n}}$ for $1 \leq n \leq 4$.*

3. *Figure 2.3 shows the Hasse diagram of $\wp(S)$ for $S = \{a, b, c\}$.*

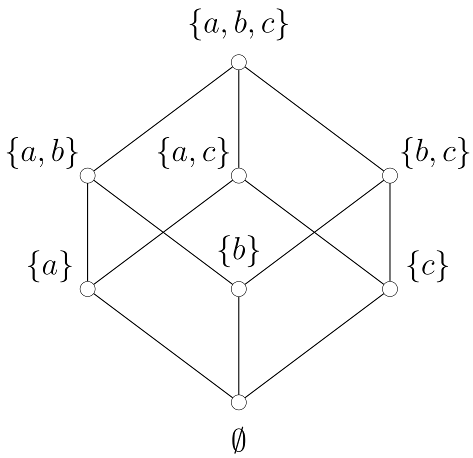


Figure 2.3: $\wp(S)$ for $S = \{a, b, c\}$

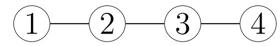


Figure 2.4: Non-Hasse diagram for **4**

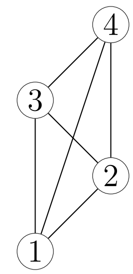


Figure 2.5: Non-Hasse diagram for **4**

Example 2.11. (*non-Hasse diagram of* **4**) *Figure 2.4 and shows a diagram of* **4** *that is not a Hasse diagram. The problem is that it has all four elements at the same vertical level despite the strict inequalities between them, thus violating rule 1 of Definition 2.5.*

Example 2.12. (*another non-Hasse diagram of* **4**) *Figure 2.5 shows a second diagram of* **4** *that is also not a Hasse diagram. The issues is that it does not satisfy rule 2 of Definition 2.5. There is an edge between* 1 *and* 4 *even though* $1 \not\prec 4$.

An important observation to make is that a given poset can have multiple Hasse diagrams representing it but a valid Hasse diagram represents exactly one poset. For the moment, we give only an example of the former. Examples 2.8 and 2.9 will deal with the latter.

Example 2.13. (*alternate diagrams of* **4**) *Consider the poset* **4** *for which a Hasse diagram is given in Figure 2.1. Figures 2.6 and 2.7 provide additional Hasse diagrams of* **4**. *Note that both diagrams satisfy rules 1 and 2 of Definition 2.5.*

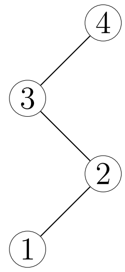


Figure 2.6: Hasse diagram for **4**

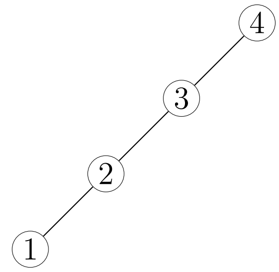


Figure 2.7: Hasse diagram for **4**

We conclude this section with a brief discussion on the relationship between the order relation, the covering relation, and the Hasse diagram of a poset. As mentioned earlier, the order relation of a poset induces a unique covering relation. The converse is also true for finite posets, a covering relation determines a unique order relation. The determined order relation is obtained by applying reflexivity and transitivity to the pairs of the covering relation. The result is that $a \leq b$ if an only if there is a finite sequence of covering relations $a \prec c_1 \prec c_2 \prec \cdots \prec c_n \prec b$.

Now enter the Hasse diagram. As already discussed, a poset (and hence a covering relation) can be represented by a Hasse diagram. On the other hand, a Hasse diagram represents a unique poset. In other words, a poset can be defined by its Hasse diagram without specifying the set P nor the relation $\leq$. These can be obtained from the diagram as follows. Label the vertices of the diagram to get P. Then obtain the covering relation by reading the diagram's edges and, as just mentioned, this is enough to get $\leq$ by reflexivity and transitivity. The relation $\leq$ can then be specified as the list of pairs (x, y) of elements of P for which $x \leq y$. We provide some examples.

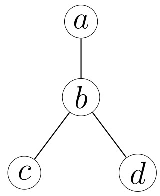


Figure 2.8: Poset P of Example 2.14

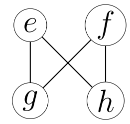


Figure 2.9: Poset Q of Example 2.15

Example 2.14. (*obtaining poset from Hasse diagram 1*) *Figure 2.8 illustrates and defines a poset P with $P = \{a, b, c, d\}$ and*

$$\leq = \{(a,a),(b,b),(c,c),(d,d),(b,a),(c,b),(d,b),(c,a),(d,a)\}. \tag{2.2}$$

Example 2.15. (*obtaining poset from Hasse diagram 2*) *Figure 2.9 illustrates and defines a poset Q with $Q = \{e, f, g, h\}$ and*

$$\leq = \{(e,e),(f,f),(g,g),(h,h),(g,e),(g,f),(h,e),(h,f)\}. \tag{2.3}$$

2.4 Basic Concepts

In this section we discuss some basic concepts about posets. First, we introduce subposets. Then, we define some special elements a poset may have: maximal, minimal, top, and bottom elements. Finally, we explain the length of a poset.

We begin with subposets. Given a poset P, its subsets can naturally be regarded as posets themselves using the same order relation of P. In this context, we call them subposets of P.

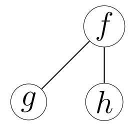


Figure 2.10: subposet R of the poset Q of Example 2.15

Definition 2.6. (*subposet*) *A subposet of a poset* $\langle P; \leq \rangle$ *is a subset* $Q \subseteq P$ *ordered by same order of* P*, which in this context is called the induced or inherited order: For* $a, b \in Q$*,* $a \leq b$ *in* Q *if and only if* $a \leq b$ *in* P*. When necessary to distinguish between the two order relations, we will write* $\leq_P$ *and* $\leq_Q$ *for the order relation of* P *and* Q *respectively.*

Example 2.16. (*chains of numbers*) $\langle \mathbb{N}; \leq \rangle$ *is a subposet of* $\langle \mathbb{Z}; \leq \rangle$*.*

Example 2.17. (*power set*) *For any set* S *with subset* A*,* $\langle \wp(A); \subseteq \rangle$ *is a subposet of* $\langle \wp(S); \subseteq \rangle$*. A concrete instance of this is* $\wp(A)$ *for the subset* $A = \{a, b\}$ *of the set* S *in Figure 2.3.*

Example 2.18. (*Hasse diagram of subposet*) *If we consider the poset* Q *of Figure 2.9, we have that* $R = \{f, g, h\}$ *is a subposet of* Q*. Its Hasse diagram is shown in Figure 2.10.*

We briefly comment on subposets before moving on to maximal and minimal elements. First, we foreshadow that subposets will be crucial in defining the length of a poset. Also, we highlight the fact that all non-empty posets have chain and antichain subposets. Last but not least, we caution that although a subposet has the same order relation that its parent poset, its covering relation may be different due to the removal of elements. This is important to keep in mind when drawing the subposet's Hasse diagram.

Example 2.19. (*covering relation change*) *If we consider the subposet* $\langle \mathbb{N}; \leq \rangle$ *of the poset* $\langle \mathbb{R}; \leq \rangle$*, we have that* 1 *is covered by* 2 *in the former but not in the latter since* $\mathbb{R}$ *contains* 1.5 *and* $1 < 1.5 < 2$ *. In fact,* $\langle \mathbb{N}; \leq \rangle$ *can be described as a sequence of covering relations while* $\langle \mathbb{R}; \leq \rangle$ *has no covering relations at all!*

We now proceed to maximal and minimal elements. A maximal element of a poset is an element that has no element greater than it under the poset's order relation. Similarly, a minimal element is an element that has no element smaller than it.

Definition 2.7. (*maximal and minimal elements*) *Given a poset* P*, a maximal element of* P *is an element* x *of* P *such that* $x \leq y$ *and* $y \in P$ *imply* $y = x$*. Similarly, a minimal element of* P *is an element* z *of* P *such that* $z \geq w$ *and* $w \in P$ *imply* $w = z$*.*

Note that we can also define the maximal or minimal element of a subposet of a poset by changing the poset P by a subposet Q of P in the above definition. Also, a poset may have zero, one, or multiple maximal (or minimal) elements. It is also possible for an element to be both maximal and minimal. The following examples show a variety of cases.

Example 2.20. (*finite chains*) *The chains in Figure 2.1 have each one minimal element,* 1*, and one maximal element,* 1*,* 2*,* 3*, and* 4 *respectively. Note that the only element of* $\mathbf{1}$ *is both maximal and minimal.*

Example 2.21. (*power set*) *The power set* $\langle \wp(S); \subseteq \rangle$ *of any set* S *has one minimal element,* $\emptyset$*, and one maximal element,* S *itself.*

Example 2.22. (*multiple minimal*) *The poset P in Figure 2.8 has two minimal elements, c and d, and one maximal element, a.*

Example 2.23. (*multiple maximal and minimal*) *The poset Q in Figure 2.9 has two minimal elements, g and h, and two maximal elements, e and f.*

Example 2.24. (*natural numbers*) *The poset $\langle \mathbb{N}; \leq \rangle$ has one minimal element,* 1*, and no maximal elements since it is unbounded above.*

Example 2.25. (*integers*) *The poset $\langle \mathbb{Z}; \leq \rangle$ has neither a minimal element nor a maximal element since it is unbounded in both directions.*

Example 2.26. (*finite antichains*) *The antichains in Figure 2.2 have each n minimal elements and n maximal elements. Particularly, each element of an antichain is both minimal and maximal.*

Next, we introduce top and bottom elements. A top element is an element that is greater than or equal to all other elements in the poset. Analogously, a bottom element is an element that is less than or equal to all other elements in the poset.

Definition 2.8. (*top and bottom*) *Given a poset P, a top element of P is an element $\top$ of P such that $\top \geq x$ for all $x \in P$. Similarly, a bottom element of P is an element $\bot$ of P such that $\bot \leq x$ for all $x \in P$.*

Like maximal and minimal elements, the definition of a top and bottom element can be generalized for subposets of a poset. Note also that both a top element and a bottom element have to be comparable with all elements of the poset. In addition, observe that a top element is a maximal element while a bottom element is minimal.

However, a maximal element need not be a top element and likewise with bottom and minimal elements. As with maximal and minimal elements, a poset may or may not have a top or bottom. However, if it does, they are unique. We provide some examples show-casing this variety.

Example 2.27. (*finite chains*) *The chains in Figure 2.1 have each a bottom element,* 1*, and a top element,* 1*,* 2*,* 3*, and* 4 *respectively.*

Example 2.28. (*power set*) *The power set* $\langle \wp(S); \subseteq \rangle$ *of any set* S *has a bottom element* $\emptyset$ *and a top element* S*.*

Example 2.29. (*topped finite poset with no bottom*) *The poset* P *in Figure 2.8 has no bottom element since there is no* $x \in P$ *such that* $x \leq c$ *and* $x \leq d$*. However, it has a top element,* a*.*

Example 2.30. (*finite poset with neither top nor bottom*) *The poset* Q *in Figure 2.9 has no bottom element since there is no* $x \in P$ *such that* $x \leq g$ *and* $x \leq h$*. Similarly, it has no top element since there is no* $y \in P$ *such that* $e \leq y$ *and* $f \leq y$*.*

Example 2.31. (*natural numbers*) *The poset* $\langle \mathbb{N}; \leq \rangle$ *has a bottom element,* 1*, but no top element since for each natural number* n*,* $n < n + 1$ *and* $n + 1 \in \mathbb{N}$*.*

Finally, we define the length of a poset. The idea is to measure how long is the longest strictly increasing sequence of elements of the poset. We will define first the length of a chain and then define the length of any poset based on its chain subposets. Informally, we can say that the length of a chain is the number of edges in its Hasse diagram (viewed as a graph).

Poset P	Figure	$l(P)$
$\mathbf{1}$	2.1	0
$\mathbf{2}$	2.1	1
$\mathbf{3}$	2.1	2
$\mathbf{4}$	2.1	3

Poset P	Figure	$l(P)$
$\bar{\mathbf{1}}$	2.2	0
$\bar{\mathbf{2}}$	2.2	0
$\bar{\mathbf{3}}$	2.2	0
$\bar{\mathbf{4}}$	2.2	0

Poset P	Figure	$l(P)$
$\wp(S)$	2.3	3
P	2.8	2
Q	2.9	1
$\langle \mathbb{N}; \leq \rangle$	NA	∞
$\langle \mathbb{Z}; \leq \rangle$	NA	∞

Table 2.1: Length of some previously discussed posets

Definition 2.9. (*length*) *The length of a chain is one less than the number of elements of the chain. The length of a poset is the length of its longest chain subposet. The length of a poset P is denoted $l(P)$.*

Example 2.32. (*lengths of posets*) *Table 2.1 shows the length of various previously discussed posets. The figure numbers of their Hasse diagrams are provided for reference. Note that the length of each chain $\mathbf{n}$ is $n-1$ while that of each antichain $\bar{\mathbf{n}}$ is 0.*

2.5 Down-Sets and Up-Sets

In this section, we introduce special subsets of a poset called down-sets and up-sets. We discuss two special types of these subsets and make some general remarks. Afterwards, we form a poset with the down-sets of a poset and conclude with a relationship between the down-sets and the antichains of a finite poset.

A down-set of a poset is a subset that is closed under going down. This means that if an element of the poset is less than some element in a down-set, then it is also in the down-set. Similarly, an up-set is a subset that is closed under going up. We now present the formal definition followed by some examples.

Definition 2.10. (*down-set and up-set*) *A down-set of a poset P is a subset $Q \subseteq P$ such that:*

$$\forall\, x, y \in P,\ x \in Q \text{ and } y \leq x \implies y \in Q. \tag{2.4}$$

Similarly, an up-set of a poset P is a subset $Q \subseteq P$ such that:

$$\forall\, x, y \in P,\ x \in Q \text{ and } x \leq y \implies y \in Q. \tag{2.5}$$

Example 2.33. (*power set*) *Consider the power set $\wp(S)$ shown in Figure 2.11.*

1. *$Q = \{\emptyset, \{a\}, \{b\}\}$ is a down-set.*

2. *$Q = \{\{a\}, \{a, b\}, \{a, c\}, S\}$ is an up-set.*

3. *$Q = \{\{a\}, \{a, b\}\}$ is not a down-set because $\emptyset \subseteq \{a\} \in Q$ but $\emptyset \notin Q$.*

4. *$Q = \{\emptyset, \{a, b\}, \{a, c\}\}$ is not an up-set because $\{a\} \supseteq \emptyset \in Q$ but $\{a\} \notin Q$.*

Example 2.34. (*more down-sets and up-sets*) *Consider the poset P in Figure 2.12.*

1. *$Q = \{b, c, d\}$ is a down-set.*

2. *$Q = \{a, b, d\}$ is an up-set.*

3. *$Q = \{a, b, c\}$ is not a down-set because $d \leq a \in Q$ but $d \notin Q$.*

4. *$Q = \{b\}$ is not an up-set because $a \geq b \in Q$ but $a \notin Q$.*

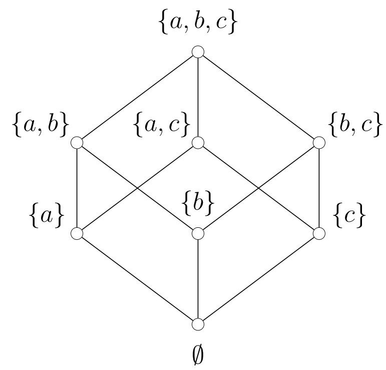


Figure 2.11: $\wp(S)$ for $S = \{a, b, c\}$

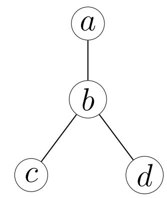


Figure 2.12: Poset P

Now, we introduce some special types of down-sets and up-sets: generated down-sets and up-sets and principal down-sets and up-sets. We begin with the former and then introduce the latter as a special case of it. Given any subset Q of a poset P (not necessarily a down-set), we can generate a down-set from Q by adding all missing elements of P that are "less than" some element in Q. The result is a form of "downward closure" of Q that we call the down-set generated by Q. We can similarly construct the up-set generated by Q.

Definition 2.11. (*generated down-set and up-set*) *Given a poset P and $Q \subseteq P$, the down-set generated by Q, denoted by $\downarrow Q$ (read "down Q"), is the smallest down-set of P containing Q. It is given by*

$$\downarrow Q = \{y \in P \mid \exists x \in Q \text{ such that } y \leq x\}. \tag{2.6}$$

Similarly, the up-set generated by Q, denoted by $\uparrow Q$ (read "up Q"), is the smallest up-set of P containing Q. It is given by

$$\uparrow Q = \{y \in P \mid \exists x \in Q \text{ such that } x \leq y\}. \tag{2.7}$$

The fact that $\downarrow Q$ *and* $\uparrow Q$ *are actually a down-set and an up-set respectively and the fact that they are the smallest such subsets of* P *containing* Q *can be shown easily.*

Example 2.35. (*generated down-set and up-set*)

1. *In* $\wp(S)$ (*Figure 2.11*), *if* $Q = \{\{a\}, \{a, b\}\}$, *then* $\downarrow Q = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

2. *In the poset* P *of Figure 2.12, if* $Q = \{c, d\}$, *then* $\uparrow Q = P$.

A down-set (up-set) generated by a single-element set is called a principal down-set (up-set). It consists of that single element plus all the other elements of the poset that are "less than" ("greater than") it.

Definition 2.12. (*principal down-set and up-set*) *A principal down-set is a down-set that is generated by a single element* (*say* $x \in P$). *It is denoted* $\downarrow x$ (*read "down x"*) *and is given by*

$$\downarrow x = \{y \in P \mid y \leq x\}. \tag{2.8}$$

Similarly, a principal up-set generated by x *is denoted* $\uparrow x$ (*read "up x"*) *and is given by*

$$\uparrow x = \{y \in P \mid x \leq y\}. \tag{2.9}$$

Example 2.36. (*principal down-set*) $\downarrow b = \{b, c, d\}$ *is a principal down-set of the poset* P *shown in Figure 2.12.*

Example 2.37. (*principal up-set*) $\uparrow\{a\} = \{\{a\}, \{a, b\}, \{a, c\}, S\}$ *is a principal up-set of the power set* $\wp(S)$ *shown in Figure 2.11.*

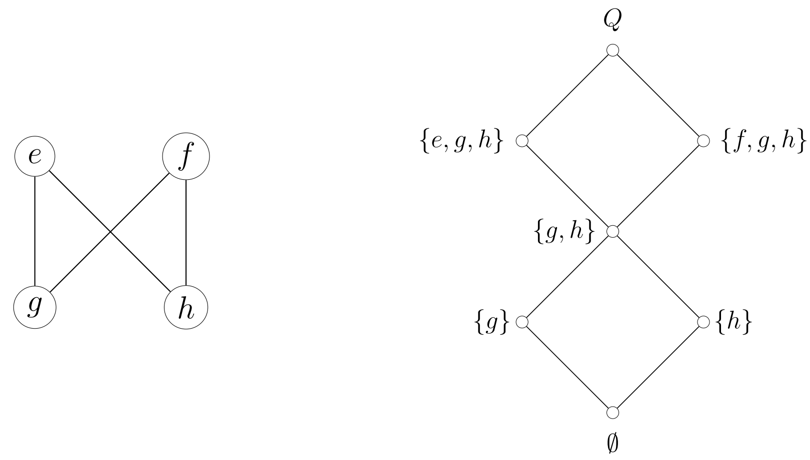


Figure 2.13: A poset Q (left) and its poset of down-sets $O(Q)$ (right)

We take a moment to make some remarks about down-sets and up-sets. We omit their proofs, however, because they are elementary. First, we point out the the empty set and the entire poset are considered both down-sets and up-sets. Second, that the complement of a down-set is an up-set and vice-versa. Third, that for a subset Q of a poset P, $Q = \downarrow Q$ ($\uparrow Q$) if and only if Q is a down-set (up-set). Finally, that for subsets Q and R of a poset P, $Q \subseteq R$ implies that $\downarrow Q \subseteq \downarrow R$ and $\uparrow Q \subseteq \uparrow R$.

For the remainder of this section, we focus on down-sets exclusively. We consider the set of all down-sets of a poset P, denoted $O(P)$.

Definition 2.13. (*poset of down-sets $O(P)$*) *Given a poset P, its poset of down-sets $O(P)$ is the poset consisting of the set of all down-sets of P ordered by inclusion ($\subseteq$).*

Example 2.38. (*poset of down-sets*) *Figure 2.13 shows the Hasse diagrams of a poset Q and its poset of down-sets $O(Q)$.*

Finally, we establish an interesting connection between the down-sets and the antichains (antichain subposets) of a finite poset. The idea is that there is a 1-1 correspondence between the down-sets and the antichains of a finite poset. Each antichain determines a down-set (its generated down-set) while each down-set is uniquely identified by its antichain of maximal elements. We will introduce the formal result followed by an example shortly, but first we have a definition and two lemmas that will be needed to prove the correspondence.

Definition 2.14. (*set of maximal elements* $\max Q$) *Given a subset Q of a poset P, $\max Q$ denotes the set of all maximal elements of Q.*

Lemma 2.1. (*antichain of maximals*) *If Q is a subset of a poset P, then $\max Q$ is an antichain of P.*

Proof *Suppose there exist $a, b \in \max Q$ such that $a < b$. Then a is not maximal in Q because $b \in Q$. This contradicts the assumption that $a \in \max Q$. Therefore, $\max Q$ is an antichain.* □

Lemma 2.2. (*down-set and maximals*) *If P is a finite poset with down-set Q, then $Q = \downarrow\max Q$.*

Proof *We show the desired equality by showing both inclusions. First, suppose $x \in Q$. Since Q is finite (it is a subset of a finite poset), there exists $y \in \max Q$ such that $x \leq y$. Otherwise, for each $z \in Q$ such that $x \leq z$, there must be $w \in Q$ such that $z < w$. This implies that Q contains an infinite chain of non-maximal elements, contradicting its finiteness. Therefore, $x \in \downarrow\max Q$.*

Now, let $x \in \downarrow\max Q$. Since $\max Q \subseteq Q$, this implies that $x \in \downarrow Q$. However, Q is a down-set. Hence, $Q = \downarrow Q$ and we get $x \in Q$. Therefore, $Q = \downarrow\max Q$. □

Theorem 2.1. (*down-sets and antichains*) *There is a 1-1 correspondence between the down-sets and the antichains of any finite poset P.*

Proof *Let P be a finite poset. Denote by* $\mathrm{Anti}(P)$ *the set of antichains of P. We claim that the following function $\phi : \mathrm{Anti}(P) \to O(P)$ gives the desired 1-1 correspondence:*

$$\phi(A) = {\downarrow}A. \tag{2.10}$$

Note that $\phi(A)$ is a down-set of P. Hence, ϕ is well-defined. We now show that it is also 1-1 and onto.

1-1: Suppose that $A, B \in \mathrm{Anti}(P)$ satisfy $\phi(A) = \phi(B)$. Then ${\downarrow}A = {\downarrow}B$. We claim that this implies that $A = B$ because A and B are antichains. We show this by contradiction. Suppose that $A \neq B$. Without loss of generality, let $x \in A \setminus B$. Then $x \in {\downarrow}A = {\downarrow}B$. Hence, there is $y \in B$ such that $x \leq y$ (in fact, $x < y$ because $x \notin B$). This implies $y \in {\downarrow}B = {\downarrow}A$, which requires $z \in A$ with $y \leq z$. However, this results in $x < y \leq z$ with x and z both in A, contradicting the fact that A is an antichain. Therefore, $A = B$ and ϕ is 1-1.

Onto: Let $D \in O(P)$ and define $M = \max D$. By Lemma 2.1, M is an antichain (i.e. $M \in \mathrm{Anti}(P)$). Now, observe that

$$\phi(M) = {\downarrow}M = {\downarrow}\max D = D, \tag{2.11}$$

where the last equality holds by Lemma 2.2 because P is finite. Thus, D has a pre-image under ϕ in $\mathrm{Anti}(P)$ *and ϕ is onto.* $\square$

Down-set	Antichain
$\emptyset$	$\emptyset$
$\{g\}$	$\{g\}$
$\{h\}$	$\{h\}$
$\{g, h\}$	$\{g, h\}$
$\{e, g, h\}$	$\{e\}$
$\{f, g, h\}$	$\{f\}$
$Q = \{e, f, g, h\}$	$\{e, f\}$

Table 2.2: Down-sets of Q in with their corresponding antichains

Example 2.39. (*antichains and down-sets*) *Table 2.2 shows the 1-1 correspondence of Theorem 2.1 for $O(Q)$ of Figure 2.13.*

2.6 Duality

One interesting topic in posets is the construction of new posets from known posets. We identify five methods for this:

1. subposets of a poset,
2. dual of a poset,
3. product of posets,
4. union of posets,
5. linear sum of posets.

We already introduced subposets in Section 2.4. In Sections 2.7-2.9, we will deal with items 3-5 of the list above. For now, we will focus on the dual of a poset. We define

Figure 2.14: Poset P (left) and and its dual P^∂ (right)

it and then discuss the related notion of dual statements. We then conclude with the all-important Duality Principle.

The dual of a poset P is the poset obtained by taking the same elements of P but reversing the order relation. If we have the Hasse diagram of P, we can flip it vertically to obtain the diagram of its dual.

Definition 2.15. (*dual poset*) *Given a poset P, the dual poset of P, denoted P^∂, is the poset defined by $x \leq_{P^\partial} y$ if and only if $y \leq_P x$.*

Example 2.40. (*dual poset*) *Figure 2.14 shows a poset P and its dual P^∂.*

Example 2.41. (*self-dual poset*) *The dual of the chain $\mathbf{n} = \langle [n]; \leq \rangle$ is $\mathbf{n}^\partial = \langle [n]; \geq \rangle$. If we pick any n and look at both Hasse diagrams, we can see that they are identical up to labels. As a result we can say that $\mathbf{n}$ is self-dual. In Section 2.10, we will formalize this "sameness" with order-isomorphisms.*

The analogy of flipping Hasse diagrams can be extended to statements about posets. Given a statement about posets, which we denote by Φ, we can "flip" it to obtain the dual statement of Φ, which is a new statement that is satisfied by the dual of any poset that satisfies Φ.

Definition 2.16. (*dual statement*) *Given a statement Φ about a poset, its dual statement Φ^∂ is the statement obtained by interchanging all occurrences of $\leq$ and $\geq$ in Φ.*

A poset P satisfies a statement Φ if and only if P^∂ satisfies Φ^∂.

Example 2.42. (*dual statement of one poset*) *We consider the posets P and P^∂ of Figure 2.14. Note that P satisfies the following three statements:*

1. *There exists a top element.*

2. *There is exactly one element that covers two other elements.*

3. *There are two minimal elements.*

We now list the duals of these three statements. Note that they are all satisfied by P^∂:

1. *There exists a bottom element.*

2. *There is exactly one element that is covered by two other elements.*

3. *There are two maximal elements.*

The reader may naturally ask where are the inequalities and their flipping in all of this? The answer is that the above statements all have implicit inequalities. They can be made explicit by replacing certain terms by their definitions. We now do this with the first statement and its dual to illustrate the reversing of the inequalities involved. We use an arbitrary poset Q and apply the definition of top and bottom element.

1. Φ*: There is an element $x \in Q$, such that $y \leq x$ for all $y \in Q$.*

2. Φ^∂*: There is an element $x \in Q$, such that $y \geq x$ for all $y \in Q$.*

A similar process can be done with the other two statements using appropriate definitions.

Although the above example considered a statement Φ about a particular poset, we can extend the notion of dual statements to general statements about posets. What is fascinating about this is that a general statement and its dual are both true or both false, a result called the Duality Principle. A truly rigorous proof requires a formal treatment of propositional statements and logic, hence, we state it only and accept it intuitively.

Theorem 2.2. (*Duality Principle*) *If Φ is a true statement about all posets, then Φ^∂ is also true for all posets.*

The importance of the Duality Principle is that for each statement Φ that we prove about posets, we get a second statement proved for free. This can greatly reduce the length of many proofs. We are done with duality.

2.7 Product of Posets

In this section, we learn how we can obtain new posets by multiplying existing posets. The idea is to define an order in the Cartesian product of two or more posets using the order of each of the posets involved.

Definition 2.17. (*product of posets*) *Given posets $P_1, P_2, ..., P_n$, the product of posets $P_1 \times P_2 \times \cdots \times P_n$ is the poset obtained by giving the corresponding Cartesian product the coordinatewise order:*

$$(x_1, x_2, ..., x_n) \leq (y_1, y_2, ..., y_n) \iff x_i \leq_{P_i} y_i,\ 1 \leq i \leq n. \tag{2.12}$$

We discuss a couple of things before giving examples. First, it can be shown from the definition that this product is both commutative and associative. Thus, the following equalities hold for any posets P, Q, and R:

$$P \times Q = Q \times P; \tag{2.13}$$

$$(P \times Q) \times R = P \times (Q \times R). \tag{2.14}$$

Note, however, that $P \times Q$ and $Q \times P$ are still different sets; they just happen to have the same poset structure. Second, we explain how to draw the diagram of the product $P \times Q$. We take the Hasse diagram of P and replace each element with a copy of the Hasse diagram of Q. We then connect the corresponding elements of the copies of Q if the copies replaced two connected elements of P. If we had more than two posets in the product, then we repeat the process for a third poset given the product of the first two and so on. The following example illustrates the case of a binary product.

Example 2.43. (*product of posets*) *Figure 2.15 shows the poset product* $P \times \mathbf{2}$ *where* P *is the poset from Figure 2.8. Each pair* (x, n) *is expressed by* xn *in the diagram:* $a2 = (a, 2)$*, for instance. Observe that* $(c, 1) \leq (b, 2)$ *since* $c \leq_P b$ *and* $1 \leq_{\mathbf{2}} 2$*. Similarly* $(a, 1) \leq (a, 2)$*. On the other hand,* $(c, 2) \not\leq (a, 1)$ *because although* $c \leq_P a$*,* $2 >_{\mathbf{2}} 1$.

Sometimes we multiply a poset with itself. In this case we use an exponential notation P^k to denote $P \times P \times \cdots \times P$ (k times). We conclude with an example.

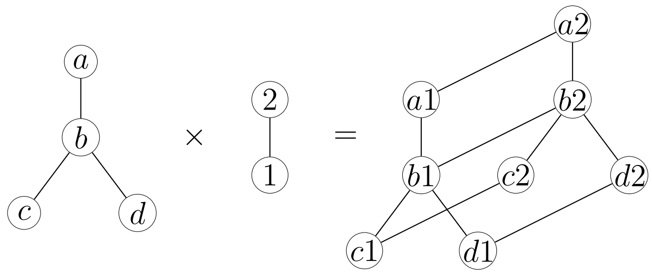


Figure 2.15: The product $P \times \mathbf{2}$

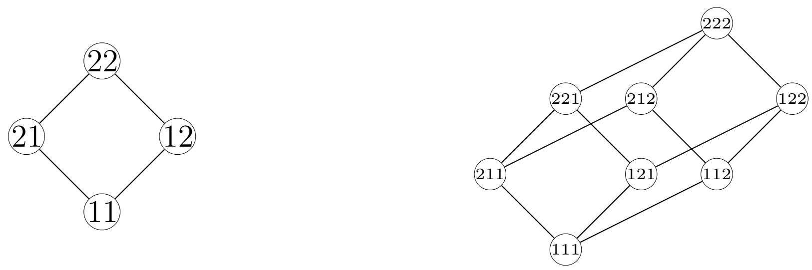


Figure 2.16: Posets $\mathbf{2}^2$ (left) and $\mathbf{2}^3$ (right)

Example 2.44. (*powers of a poset*) *Figure 2.16 shows the first two non-trivial poset powers of* $\mathbf{2}$*:*

$$\mathbf{2}^2 = \mathbf{2} \times \mathbf{2} \qquad\qquad \mathbf{2}^3 = \mathbf{2} \times \mathbf{2} \times \mathbf{2} \tag{2.15}$$

Again the tuples are expressed in abridged fashion, e.g. $122 = (1, 2, 2)$*.*

2.8 Union of Posets

The next construct we present is the union of posets. The basic idea is to take two disjoint posets and form a new poset by putting together the elements of both posets while allowing each to preserve its internal order structure. There is no interaction between them.

Figure 2.17: Two union of posets: $P \cup \mathbf{3}$ (left) and $\mathbf{1} \cup \mathbf{2} \cup \mathbf{3}$ (right)

Definition 2.18. (*union of posets*) *The union of two* (*disjoint*) *posets P and Q is the poset with set $P \cup Q$ and order relation $\leq$ given by*

$$x \leq y \iff x \leq_P y \text{ or } x \leq_Q y. \tag{2.16}$$

As a consequence, $x||y$ for any $x \in P$ and $y \in Q$.

We make some remarks before giving examples. First, we note that we can define the union of three or more posets inductively. Second, it can be shown that the union of posets is commutative and associative. Thus, the following equalities hold for any posets P, Q, and R:

$$P \cup Q = Q \cup P; \tag{2.17}$$

$$(P \cup Q) \cup R = P \cup (Q \cup R). \tag{2.18}$$

Finally, the Hasse diagram of the union of several posets consists of placing the diagrams of all of the posets involved side by side.

Example 2.45. (*unions of posets*) *Figure 2.17 shows the posets $P \cup \mathbf{3}$ and $\mathbf{1} \cup \mathbf{2} \cup \mathbf{3}$ where P is the poset in Figure 2.8.*

2.9 Linear Sum of Posets

While the poset union is one way to define an order relation on the set $P \cup Q$ for posets P and Q, it is not the only one. The linear sum, the topic of this section, is another such way. The idea is to put Q on top of P by making all minimal elements of Q cover all maximal elements of P.

Definition 2.19. (*linear sum of posets*) *The linear sum of two posets P and Q, denoted $P \oplus Q$, is the poset whose set is $P \cup Q$ with order relation $\leq$ defined by*

$$\begin{aligned} x \leq y \iff & x, y \in P \text{ and } x \leq_P y, \\ & \text{or } x, y \in Q \text{ and } x \leq_Q y, \\ & \text{or } x \in P \text{ and } y \in Q. \end{aligned} \tag{2.19}$$

In order to draw the Hasse diagram of $P \oplus Q$, it suffices to draw the diagram of Q above that of P and draw lines connecting each minimal element of Q with each maximal element of P. The following examples illustrate this.

Example 2.46. (*linear sum of antichains*) *Figure 2.20 shows the Hasse diagram of the linear sum $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$. Note that each element of $\bar{\mathbf{3}}$ covers each element of $\bar{\mathbf{2}}$.*

Example 2.47. (*linear sum of posets*) *Figure 2.21 shows the Hasse diagram of the linear sum $P \oplus Q$ where P and Q are the posets from Figures 2.18 and 2.19. Observe that g and h both cover a.*

We comment that it is possible to compute the linear sum of more than two posets by adding the sum of the first two to the third. It can be shown that the linear sum

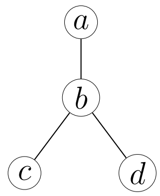


Figure 2.18: Poset P

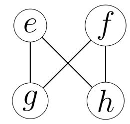


Figure 2.19: Poset Q

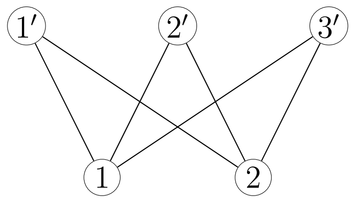


Figure 2.20: Poset $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$

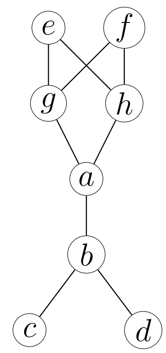


Figure 2.21: Poset $P \oplus Q$

is associative: Hence,

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R) \tag{2.20}$$

for any posets P, Q, and R. However, it is not commutative: If we compute $\bar{\mathbf{3}} \oplus \bar{\mathbf{2}}$, we have three minimal elements and two maximal ones, the opposite of $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$. Thus, $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}} \neq \bar{\mathbf{3}} \oplus \bar{\mathbf{2}}$. We now show an example of a linear sum of three posets.

Example 2.48. ($\mathbf{M}_n$) *For any $n \in \mathbb{N}$, we define $\mathbf{M}_n = \mathbf{1} \oplus \bar{\mathbf{n}} \oplus \mathbf{1}$. Figure 2.22 shows the Hasse diagrams of $\mathbf{M}_n$ for $n = 2, 3, 4$. The linear sum decomposition of $\mathbf{M}_3$ is shown in Figure 2.23. This poset will be important later when we study lattices and when we present our new results.*

Before we finish this section, we take a moment to show how these methods for constructing larger posets from known posets can be used to decompose a poset into smaller posets. In particular, we give an example of how to express a given poset

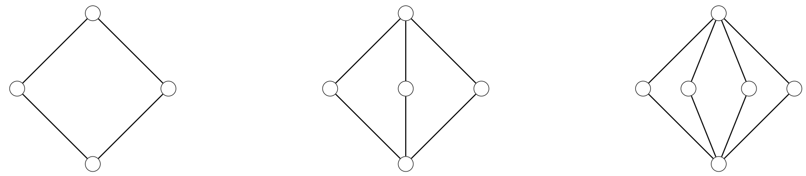


Figure 2.22: Posets $\mathbf{M}_2$ (left), $\mathbf{M}_3$ (center), and $\mathbf{M}_4$ (right)

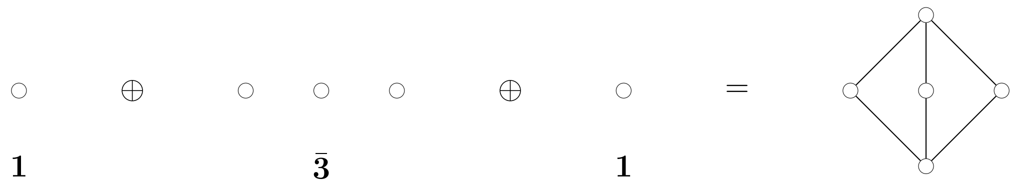


Figure 2.23: Linear sum $\mathbf{M}_3 = \mathbf{1} \oplus \bar{\mathbf{3}} \oplus \mathbf{1}$

as the linear sum of chains and antichains. However, similar decompositions can be done with products and unions of posets.

Example 2.49. (*decomposing posets*) *We decompose the posets P and Q from Figures 2.8 and 2.9:*

$$P = \bar{\mathbf{2}} \oplus \mathbf{1} \oplus \mathbf{1}; \tag{2.21}$$

$$Q = \bar{\mathbf{2}} \oplus \bar{\mathbf{2}}. \tag{2.22}$$

2.10 Maps between Posets

In mathematics, whenever we define a structure consisting of a set with some particular characteristics, it is generally of interest to define and study functions between these structures. Posets are no exception. Hence, we dedicate this section to functions between posets. In particular, we are interested in how functions interact with the order relations of the posets they connect. What does the comparability of two elements say about the comparability of their images? We will study some functions that preserve the order relation. We present definitions, observations, and examples, in that order, concluding with a characterization of the down-sets of a union of posets.

We introduce the terminology of these special functions: order-preserving functions, order-embedding functions, and order-isomorphisms. Each is a special case of the previous ones. An order-preserving function is a function between posets that preserves the order relation. An order-embedding is an order-preserving function where the order is also preserved when going backwards. Finally, an order-isomorphism is a bijective order-embedding.

Definition 2.20. (*order-preserving function*) *Given posets P and Q, an order-preserving function is a map $\phi : P \to Q$ such that $a \leq b \implies \phi(a) \leq \phi(b)$. Such a function may also be called monotone, non-decreasing, or isotone.*

Definition 2.21. (*order-embedding function*) *Given posets P and Q, an order-embedding function is a map $\phi : P \to Q$ such that $a \leq b \iff \phi(a) \leq \phi(b)$.*

Definition 2.22. (*order-isomorphism*) *Given posets P and Q, an order-isomorphism is a 1-1 and onto order-embedding function $\phi : P \to Q$.*

We briefly discuss order-isomorphisms and order-embeddings. The existence of an order-isomorphism between two posets P and Q implies that they have the same order structure. In this case, we say that P and Q are order-isomorphic (or just isomorphic if there is no confusion with other notions of isomorphism) and write $P \cong Q$. This means that they are the "same" poset but with different element names. Consequently, they can be represented with the same Hasse diagram. This will be illustrated in Example 2.53.

An important property of order-embeddings is that they are always 1-1 (proof in Proposition 2.1 below). This implies that if there is an order-embedding $\phi : P \to Q$, then $P \cong \phi(P)$ and hence, Q contains a subposet isomorphic to P. When this happens, we say that P embeds into Q.

Proposition 2.1. (*order-embedding is 1-1*) *If $\phi : P \to Q$ is an order-embedding, then ϕ is 1-1.*

Proof *Let $a, b \in P$. Then*

$$\begin{aligned} \phi(a) = \phi(b) &\implies \phi(a) \leq \phi(b) \text{ and } \phi(b) \leq \phi(a) && (2.23) \\ &\implies a \leq b \text{ and } b \leq a && (2.24) \\ &\implies a = b, && (2.25) \end{aligned}$$

where the second implication follows from the fact that ϕ is an order-embedding. □

Having given enough theory, it is time for some examples. The identity map is trivially an order-isomorphism between a poset and itself. It is also simple to see that a constant map is order-preserving but not order-embedding. We now present some less trivial examples.

Example 2.50. (*non-order-preserving*) *Consider the function $\phi : \wp(\mathbb{N}) \to \mathbb{N}$ given by $\phi(A) = \min(A)$ (the minimum element in the subset A of $\mathbb{N}$). Then ϕ is not order-preserving because if we let $A = \{2, 3\}$ and $B = \{1, 2, 3\}$, then $A \subseteq B$ but $\phi(A) = 2 > 1 = \phi(B)$.*

Example 2.51. (*order-preserving but not order-embedding*) *Let* $[k] = \{1, ..., k\}$. *Consider the function* $\phi : \wp([k]) \to [k]$ *given by* $\phi(A) = |A|$. *Then* ϕ *is order-preserving because*

$$A \subseteq B \implies |A| \leq |B| \implies \phi(A) \leq \phi(B). \tag{2.26}$$

However, it is not order-embedding because if $k \geq 5$, $A = \{1, 2\}$, *and* $B = \{3, 4, 5\}$, *then* $\phi(A) = 2 \leq 3 = \phi(B)$, *but* $A \nsubseteq B$.

Example 2.52. (*order-embedding but not order-isomorphic*) *Again, let* $[k] = \{1, ..., k\}$. *Consider the function* $\phi : [k] \to \wp(\mathbb{N})$ *given by* $\phi(n) = \{1, ..., n\}$. *Then* ϕ *is order-embedding because*

$$a \leq b \implies \{1, ..., a\} \subseteq \{1, ..., b\} \implies \phi(a) \leq \phi(b); \tag{2.27}$$

$$\phi(a) \leq \phi(b) \implies \{1, ..., a\} \subseteq \{1, ..., b\} \implies a \leq b. \tag{2.28}$$

However, it is not an order-isomorphism because it is not onto. Given the form of $\phi(n)$ *for all* n, *there is clearly no natural number* m *such that* $\phi(m) = \{2, 3\} \in \wp(\mathbb{N})$.

Example 2.53. (*order-isomorphism*) *We show that for any* k*-element set* S,

$$\wp(S) \cong \mathbf{2}^k. \tag{2.29}$$

For illustrative purposes, we will represent $\mathbf{2}$ *as* $\{0, 1\}$ *rather than* $\{1, 2\}$, *making thus* $\mathbf{2}^k$ *the set of binary* k*-tuples. Let* $s_1, ..., s_k$ *be an ordering of the elements of* S *and for each subset* A *of* S, *let* χ_A *be its indicator (or characteristic) function:* $\chi_A(s_i) = 1$ *if*

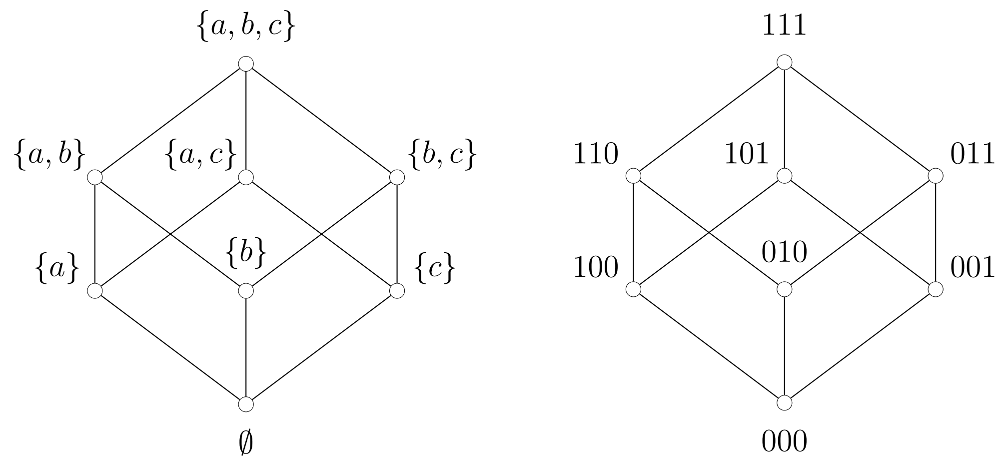


Figure 2.24: Hasse diagrams of $\wp(S)$ for $S = \{a, b, c\}$ and $\mathbf{2}^3$ illustrating that they are order-isomorphic

$s_i \in A$, 0 otherwise. Define $\phi : \wp(S) \to \mathbf{2}^k$ by

$$\phi(A) = (\chi_A(s_1), ..., \chi_A(s_k)). \tag{2.30}$$

We claim that ϕ is an order-isomorphism.

Order-Embedding: Note that for any $A, B \subseteq S$:

$$A \subseteq B \iff \chi_A(s_i) \leq \chi_B(s_i)\, \forall i \iff \phi(A) \leq \phi(B). \tag{2.31}$$

Bijective: Since ϕ is 1-1 because it is an embedding, it suffices to show that it is onto. Let $(x_1, ..., x_k) \in \mathbf{2}^k$. Define $A \subseteq S$ by $s_i \in A \iff x_i = 1$. Then $\phi(A) = (x_1, ..., x_k)$ and hence ϕ is onto.

Figure 2.24 illustrates this isomorphism for $k = 3$ with the Hasse diagrams of $S = \{a, b, c\}$ and $\mathbf{2}^3$.

We conclude this section by showing an interesting isomorphism. It characterizes the down-sets of a poset union. The idea is that each down-set of the union of two posets corresponds to an ordered pair consisting of a down-set from each poset. Hence, the down-set poset of the union is isomorphic to the product of the down-set posets. We formalize this and provide an example.

Theorem 2.3. (*down-sets of poset union*) *Let P and Q be posets. Then*

$$O(P \cup Q) \cong O(P) \times O(Q). \tag{2.32}$$

Proof Sketch *This reduces to showing that a subset D of $P \cup Q$ is a down-set if and only if $D = D_1 \cup D_2$ where D_1 is a down-set of P and D_2 a down-set of Q. The function $\phi(D) = \phi(D_1 \cup D_2) = D_1 \times D_2$ then provides the needed isomorphism. We omit the details.* $\square$

Example 2.54. (*down-sets of union*) *Figures 2.25 and 2.26 illustrate the isomorphism $O(\mathbf{2} \cup \mathbf{3}) \cong O(\mathbf{2}) \times O(\mathbf{3})$. In order to distinguish between the elements of $\mathbf{2}$ and of $\mathbf{3}$, we let $\mathbf{3} = \{1', 2', 3'\}$.*

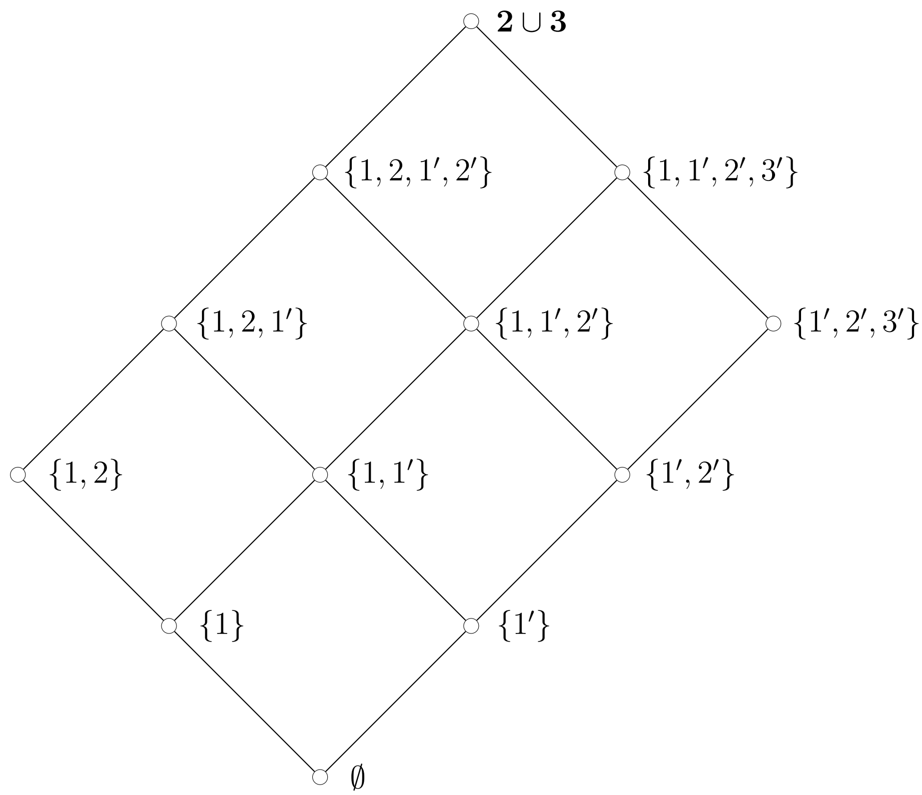


Figure 2.25: Hasse diagram of $O(\mathbf{2} \cup \mathbf{3})$

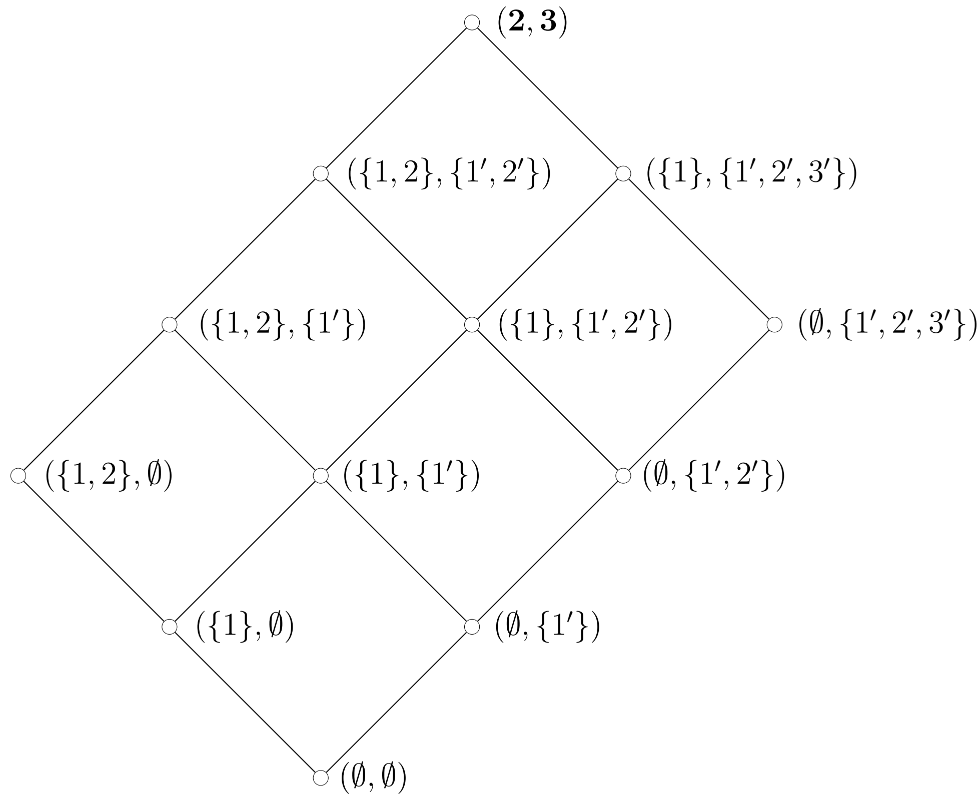


Figure 2.26: Hasse diagram of $O(\mathbf{2}) \times O(\mathbf{3})$

Chapter 3

Lattices

3.1 Introduction

Chapter 2 welcomed us into the realm of lattices and order by presenting posets. The adventure now continues with the study of lattices. We will see that there are two alternative ways to define a lattice: (1) as a poset with special upper and lower bounds for all pairs of elements or (2) as an algebraic structure with two operations that satisfy four pairs of axioms. We will see that both are equivalent. Our exploration will begin with the algebraic perspective and then we will take a bridge to the order point of view. Afterwards, we sample a variety of properties and concepts regarding lattices.

The rest of this chapter is organized as follows. Section 3.2 presents the algebraic definition of a lattice with some examples. We then take a brief but necessary detour on upper and lower bounds in Section 3.3 to introduce the supremum and infimum of posets. With this completed, we return to lattices in Section 3.4 where we define an order relation on a lattice and explore the relationship between lattices and posets.

We then move on to more specific topics during the second half of the chapter. Section 3.5 explains how to take known lattices and build new lattices from them. This is followed by a tour of functions between lattices in Section 3.6. Section 3.7 then adds a numer-theoretic flavor in the form of irreducible elements of a lattice. Finally, Section 3.8 ends the chapter with complete lattices.

3.2 Definitions

In this section, we introduce lattices. A lattice can be defined as an algebraic structure or as an order structure. Both definitions can be shown to be equivalent. In Section 3.4, we will see that a lattice is a poset with special properties but for now, we take the algebraic approach. Thus, we will consider a lattice in terms of operations on a set satisfying certain axioms like groups and rings.

Definition 3.1. (*lattice*) *A lattice* $\langle L; \vee, \wedge \rangle$ *is a set* L *with two closed binary operations called join* $(\vee)$ *and meet* $(\wedge)$ *that satisfy the following four laws for all* $p, q, r \in L$*:*

1. *Associative Law*

$$(p \wedge q) \wedge r = p \wedge (q \wedge r) \tag{3.1}$$

$$(p \vee q) \vee r = p \vee (q \vee r) \tag{3.2}$$

2. *Commutative Law*

$$p \wedge q = q \wedge p \tag{3.3}$$

$$p \vee q = q \vee p \tag{3.4}$$

3. Idempotency Law

$$p \wedge p = p \tag{3.5}$$

$$p \vee p = p \tag{3.6}$$

4. Absorption Law

$$p \wedge (p \vee q) = p \tag{3.7}$$

$$p \vee (p \wedge q) = p. \tag{3.8}$$

There are many concrete examples of lattices. Some of the simplest ones involve sets of numbers with the operations max and min. We present one below. Note that $\mathbb{N}$ can be changed for $\mathbb{Z}$, $\mathbb{Q}$, or $\mathbb{R}$ to obtain more lattices.

Example 3.1. (*natural numbers with max and min operations*) *The set of natural numbers with operations max (join) and min (meet) is a lattice. It is denoted* $\langle \mathbb{N}; \max, \min\rangle$. *Verification of the first 3 laws is trivial. For absorption, observe that for any* $p, q \in \mathbb{N}$, $\max(p, q) \geq p$. *Hence,* $\min(p, \max(p, q)) = p$. *A similar argument shows that* $\max(p, \min(p, q)) = p$.

A lattice may or may not have identities for its two operations. If it does, the identity for meet is called *one* (1) and the identity for join is called *zero* (0). A lattice L that has both $0, 1 \in L$ is called a *bounded lattice.* All finite lattices are bounded. The identities of some infinite lattices are discussed below.

Example 3.2. (*lattices of numbers with max and min*)

1. $\langle \mathbb{Z}; \max, \min\rangle$ *is not bounded because neither* max *nor* min *has an identity.*

2. $\langle \mathbb{N}; \max, \min \rangle$ *is not bounded because although* $\max$ *has identity* 1*,* $\min$ *has no identity.*

3. $\langle \mathbb{R}_{\leq 0}; \max, \min \rangle$ *is not bounded because although* $\min$ *has identity* 0*,* $\max$ *has no identity.*

4. *Given the interval of real numbers* $[0, 1]$ *The lattice* $\langle [0, 1]; \max, \min \rangle$ *is bounded with* $\max$ *identity* 0 *and* $\min$ *identity* 1*.*

We conclude this introduction to lattices with additional examples.

Example 3.3. (*power set lattice*) *The power set of any set* S *is a lattice with operations union (join) and intersection (meet). It is denoted* $\langle \wp(S); \cup, \cap \rangle$*. The four axioms follow from basic set theory. This lattice may be finite or infinite depending on* S*. In either case, it is bounded with identities* $0 = \emptyset$ *and* $1 = S$*.*

Example 3.4. (*divisibility lattice*) *The set* $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ *is a lattice with operations least common multiple (join) and greatest common divisor (meet). It is denoted* $\langle \mathbb{N}_0; \mathrm{lcm}, \gcd \rangle$*. We define* $\mathrm{lcm}(0, a) = 0$ *and* $\gcd(0, a) = a$ *for all* $a \in \mathbb{N}_0$*. The four axioms then follow from basic properties of divisibility. The lattice is infinite but has "reverse" identities* $0 = 1$ *and* $1 = 0$*.*

Example 3.5. (*subgroup lattices*) *The sets* $SubG$ *and* $\mathcal{N}$*-*$SubG$ *are lattices with operations generated subgroup of union (join) and intersection (meet). By the generated subgroup of a union of two subgroups* H *and* K *we mean the subgroup* $\langle H \cup K \rangle$ *which is the smallest subgroup of* G *containing* $H \cup K$*. Recall that subgroups are closed under intersection but not under union. In the case of* $\mathcal{N}$*-*$Sub\, G$*, we can describe*

$H \vee K$ by

$$H \vee K = HK = \{hk \mid h \in H, k \in K\} \tag{3.9}$$

for any normal subgroups H and K of G. Unfortunately, there is no general short formula to describe $H \vee K$ in Sub G. The four axioms follow from basic group theory. In both Sub G and $\mathcal{N}$-Sub G, the identities are $0 = \{e\}$ and $1 = G$ where e is the identity element.

3.3 Upper and Lower Bounds

Having defined lattices, our next objective is to study the relationship between lattices and posets. In the next section, we will see that lattices are posets with special properties but that not all posets are lattices. First, we must backtrack to posets to discuss upper and lower bounds in posets. In particular, we must introduce suprema and infima, special types of bounds. These will play a central role in the connection between lattices and posets. In this section, we define all these terms and provide some examples.

An upper bound of a subset Q of a poset P (which may P itself) is an element x of P that is greater than or equal to all of the elements of Q. This element x may or may not be in Q. A lower bound of Q is defined dually.

Definition 3.2. (*upper and lower bound*) *Let P be a poset and Q be a subset of P.*

1. *An upper bound of Q is an element $x \in P$ such that $y \leq x \, \forall y \in Q$.*

2. *A lower bound of Q is an element $x \in P$ such that $x \leq y \, \forall y \in Q$.*

An interesting observation to make is that a subset may have zero, one, or more upper or lower bounds. Given this, it is sometimes desired to know if some upper bound is tight in the sense that no upper bound of the subset is "smaller" than it. Such a bound is a least upper bound and is called the supremum of the subset. It will not always exist, but is unique if it does. Dually, we can also study the existence of a greatest lower bound called the infimum.

Definition 3.3. (*supremum and infimum*) *Let P be a poset and Q be a subset of P. The supremum of Q, denoted* $\sup(Q)$*, is an element $x \in P$ such that*

1. *x is an upper bound of Q;*

2. *for any upper bound y of Q, $x \leq y$.*

The infimum of Q, $\inf(Q)$*, is defined dually. In the case that $Q = \{a, b\}$, we can also write* $\sup(a, b)$ *and* $\inf(a, b)$*, respectively.*

We now present several examples of upper and lower bounds and of suprema and infima. These will showcase various possibilities with regards to the existence and amount of bounds. They also include cases with and without supremum/infimum.

Example 3.6. (*top and bottom*) *If a poset P has a top element $\top$ and a bottom element $\bot$, then* $\inf(P) = \bot$ *and* $\sup(P) = \top$*. These will also be the only lower and upper bound of P, respectively. For a concrete instance of this, the chain* $\mathbf{n}$ *has* $\inf(\mathbf{n}) = 1$ *and* $\sup(\mathbf{n}) = n$*.*

Example 3.7. (*power set*) *Consider the power set $\wp(S)$ of $S = \{a, b, c, d\}$ and let $Q = \{\{a, b\}, \{b, c\}\}$. Then* $\inf(Q) = \{b\}$ *and* $\sup(Q) = \{a, b, c\}$*. Note that $\emptyset$ is*

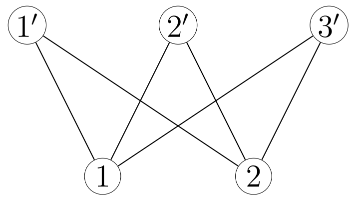


Figure 3.1: Poset $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$

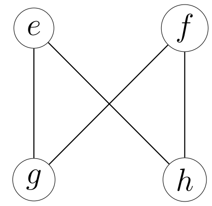


Figure 3.2: Poset Q

another lower bound of Q but is not the infimum because $\{b\}$ is a larger lower bound. Similarly, S is an upper bound of Q that is not the supremum.

Example 3.8. (*no bounds*) *Consider the linear sum $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$ shown in Figure 3.1. It has no upper bounds since there is no element greater than both $1'$ and $2'$. Similarly, it has no lower bounds since there is no element less than both 1 and 2. Hence,* $\sup(\bar{\mathbf{2}} \oplus \bar{\mathbf{3}})$ *and* $\inf(\bar{\mathbf{2}} \oplus \bar{\mathbf{3}})$ *do not exist.*

Example 3.9. (*upper bounds with no supremum*) *Consider the poset Q of Figure 3.2. Let $R = \{g, h\}$. Then R has two upper bounds in Q: e and f. However, it has no supremum because e and f are two distinct minimal upper bounds.*

3.4 Order in Lattices

In this section, we study the relationship between posets and lattices. In particular, we define an order relation on a lattice based on its operations. We then prove that lattice operations preserve this order relation. Afterwards, we characterize the operations of a lattice as the supremum and infimum of its induced order. This is followed by a generalization of the lattice operations to finite sets. Finally, we provide an alternative definition of a lattice that starts with a poset and defines the lattice operations based its order relation.

We define an order $(\leq)$ in a lattice L using its algebraic operations. The result is a poset $\langle L; \leq \rangle$. Note that for any two elements $a, b \in L$, it can be shown using the absorption axioms that $a \wedge b = a \iff a \vee b = b$. This is crucial for the order being defined and will be part of the Connecting Lemma that follows it.

Definition 3.4. (*order,* $\leq$) *Let* L *be a lattice. We define an order relation* $\leq$ *in* L *as follows. Given* $a, b \in L$*, we say that*

$$a \leq b \iff a \wedge b = a \text{ or equivalently } a \vee b = b.$$

We call $\leq$ *the induced order on* L *as it is a relation induced by the lattice operations of* L*.*

Proposition 3.1. ($\leq$ *is partial order*) *Let* L *be a lattice. If* $\leq$ *is defined on* L *as in Definition 3.4, then* $\langle L; \leq \rangle$ *is a poset.*

Proof *We show that* $\leq$ *is reflexive, anti-symmetric, and transitive. Let* $a, b, c \in L$*.*

1. *reflexive: By idempotency of lattice operations,* $a \wedge a = a \implies a \leq a$*.*

2. *antisymmetric: If* $a \leq b$ *and* $b \leq a$*, then* $a \wedge b = a$ *and* $b \wedge a = b$*. Then* $a = b$ *by commutativity of lattice operations.*

3. *transitive: If* $a \leq b$ *and* $b \leq c$*, then* $a \wedge b = a$ *and* $b \wedge c = b$*. Applying this consequence and the associativity of lattice operations, we can show that* $a \leq c$ *as follows:*

$$a \wedge c = (a \wedge b) \wedge c \tag{3.10}$$

$$= a \wedge (b \wedge c) \tag{3.11}$$

$$= a \wedge b \tag{3.12}$$

$$= a \tag{3.13}$$

Therefore, $\langle L; \leq \rangle$ is a poset. □

The relationship between the algebraic operations and the order structure of a lattice is frequently presented as the Connecting Lemma, stated below. We shall make many references to it.

Lemma 3.1. (*Connecting Lemma*) *Let L be a lattice with $a, b \in L$ and induced order $\leq$. Then the following are equivalent:*

1. $a \leq b$;

2. $a \vee b = b$;

3. $a \wedge b = a$.

Example 3.10. (*induced order in lattices*) *For all of the following lattices, the Connecting Lemma translates into:*

1. $\langle \mathbb{Z}; \max, \min \rangle$: $x \leq y \iff \max(x, y) = y \iff \min(x, y) = x$.

2. $\langle \wp(S); \cup, \cap \rangle$: $A \subseteq B \iff A \cup B = B \iff A \cap B = A$.

3. $\langle \mathbb{N}_0; \mathrm{lcm}, \gcd \rangle$: $m|n \iff \mathrm{lcm}(m, n) = n \iff \gcd(m, n) = m$,

where $m|n$ is defined as in Example 2.6.

An important property of the induced order of a lattice is that it is preserved by the meet and join operations. By this we mean that if two elements are ordered, then their ordering does not change if we apply the same lattice operation (with the same element) to both. More generally, the same result holds if we apply the same operation with elements that may be distinct but that are ordered in the same way. This is formalized in the following proposition, which will be used in several proofs.

Proposition 3.2. (*order preserved by meet and join*) *Let L be a lattice with elements $a, b, c, d \in L$.*

1. *If $a \leq b$, then $a \wedge c \leq b \wedge c$ and $a \vee c \leq b \vee c$.*

2. *If $a \leq b$ and $c \leq d$, then $a \wedge c \leq b \wedge d$ and $a \vee c \leq b \vee d$.*

Proof *We show only statement 1 for $\vee$. The proofs for $\wedge$ and statement 2 are nearly identical. Let $a, b, c \in L$ with $a \leq b$. Then*

$$(a \vee c) \vee (b \vee c) = a \vee (c \vee b) \vee c \tag{3.14}$$

$$= a \vee (b \vee c) \vee c \tag{3.15}$$

$$= (a \vee b) \vee (c \vee c) \tag{3.16}$$

$$= b \vee c \tag{3.17}$$

where the first and third equality follow from associativity, the second from commutativity, and the last one from the Connecting Lemma and idempotency. By the Connecting Lemma, we conclude that $a \vee c \leq b \vee c$. □

Our next main point is to show that the join and meet operations of a lattice have a special meaning in its induced order. The join of two elements of the lattice is their supremum while their meet is their infimum. It follows that in a bounded lattice, 0 is the bottom element of the induced order and 1 is the top element.

Proposition 3.3. *(join = sup and meet = inf) Let $\langle L; \vee, \wedge \rangle$ be a lattice with induced order $\leq$. Then*

$$a \vee b = \sup(a, b); \tag{3.18}$$

$$a \wedge b = \inf(a, b). \tag{3.19}$$

Proof *We show only that $a \vee b = \sup(a, b)$, the proof for $a \wedge b = \inf(a, b)$ is similar. Let $c = a \vee b$. We show that $c = \sup(a, b)$ by showing that it is an upper bound of $\{a, b\}$ and that it is the least such bound.*

upper bound: By the absorption axiom we have

$$c \wedge a = (a \vee b) \wedge a = a; \tag{3.20}$$

$$c \wedge b = (a \vee b) \wedge b = b. \tag{3.21}$$

Thus, c is an upper bound of $\{a, b\}$ by the Connecting Lemma.

least upper bound: Suppose that $d \in L$ is another upper bound of $\{a, b\}$. That is, $d \geq a$ and $d \geq b$. Then by associativity of lattice operations, the Connecting Lemma *and our assumption on d, we get that*

$$d \vee c = d \vee (a \vee b) \tag{3.22}$$

$$= (d \vee a) \vee b \tag{3.23}$$

$$= d \vee b \tag{3.24}$$

$$= d. \tag{3.25}$$

Therefore, $d \geq c$ and $c = \sup(a, b)$. $\square$

An interesting consequence of Proposition 3.3 is that it allows us to define the join and meet of a finite subset of a lattice as the supremum and infimum of said subset.

Definition 3.5. (*lattice subset operations*) *Let L be a lattice with induced order $\leq$ and let $S = \{s_1, ..., s_n\} \subseteq L$. Then the join and meet of S, denoted by $\bigvee S$ and $\bigwedge S$ respectively, are defined as follows:*

$$\bigvee S = \sup(S) = s_1 \vee s_2 \vee \cdots \vee s_n; \tag{3.26}$$

$$\bigwedge S = \inf(S) = s_1 \wedge s_2 \wedge \cdots \wedge s_n. \tag{3.27}$$

A couple of remarks about this definition are in order. First, note that the right-most expressions in the above equations are well-defined because $\vee$ and $\wedge$ are commutative and associative. Hence, there is no need to worry about bracketing and ordering. Second, we can show that $\bigvee S$ and $\bigwedge S$ will always exist for finite S by induction on Proposition 3.3. The idea is that for any n, $\bigvee S = \left(\bigvee(S \setminus \{s_n\})\right) \vee s_n$. Infinite subsets are another matter and will be treated in Section 3.8 when we discuss complete lattices. We now provide an example.

Example 3.11. (*power set*) *In the lattice* $\langle \wp(S); \cup, \cap \rangle$, *for a given collection of subsets* T_i *for* $i = 1, ..., n$ *of* S *we have*

$$\bigvee \{T_1, ..., T_n\} = \bigcup_{i=1}^{n} T_i, \tag{3.28}$$

$$\bigwedge \{T_1, ..., T_n\} = \bigcap_{i=1}^{n} T_i. \tag{3.29}$$

Thus and by far, we have treated a lattice as an algebraic structure and defined an order on it based on its operations. However, it is possible to go the other way around: take a poset with an order $\leq$ and define join and meet operations based on its order relation (using the equations of Proposition 3.3). These operations will then satisfy all of the axioms of Definition 3.1 due to the properties of suprema and infima. In addition, we will have that the resulting lattice will be bounded if and only if the initial poset has top and bottom elements: top will be the identity of meet while bottom will be that of join.

Naturally, in order for all this to work, the poset must contain the supremum and infimum of each pair of elements in it. This would also imply that we can define joins and meets of finite subsets like in Definition 3.5. As a result, all lattices are posets but not all posets will be lattices. This leads to an alternative definition of a lattice: a poset in which pairwise suprema and infima exist for all elements.

It can be shown that both lattice definitions are equivalent. That is, a set has an order relation with pairwise suprema and infima for all elements if and only if it has two operations that satisfy the four axioms: associativity, commutativity, idempotency, and absorption. Furthermore, we end up with the same lattice no matter where we start. We conclude this section by showing the equivalence of both definitions and giving some examples.

Proposition 3.4. (*lattice order definition*) *A lattice is a poset* $\langle L; \leq \rangle$ *in which for all* $a, b \in L$, $\sup(a, b)$ *and* $\inf(a, b)$ *exist in* L.

Proof *We must show both* (*1*) *that a lattice* (*as defined in Definition 3.1*) *is a poset in which for all* $a, b \in L$, $\sup(a, b)$ *and* $\inf(a, b)$ *exist in* L *and* (*2*) *that all such posets are lattices.*

Part 1: Let $\langle L; \vee, \wedge \rangle$ *be a lattice. Consider the induced order* $\leq$ *on* L *given in Definition 3.4.* $\langle L; \leq \rangle$ *is a poset by Proposition 3.1. Proposition 3.3 then implies that for all* $a, b \in L$; $\sup(a, b) = a \vee b$ *and* $\inf(a, b) = a \wedge b$ *exist in* L *because* $\vee$ *and* $\wedge$ *are closed operations on* L. *Therefore,* $\langle L; \leq \rangle$ *is the poset with the desired properties.*

Part 2: Now, suppose that $\langle L; \leq \rangle$ *is a poset in which for all* $a, b \in L$, $\sup(a, b)$ *and* $\inf(a, b)$ *exist in* L. *Define binary operations* $\vee : L \times L \to L$ *and* $\wedge : L \times L \to L$ *as follows:*

$$a \vee b = \sup(a, b) \tag{3.30}$$

$$a \wedge b = \inf(a, b). \tag{3.31}$$

We show that $\vee$ *and* $\wedge$ *satisfy the four axioms of Definition 3.1. By the Duality Principle* (*Theorem 2.2 in Section 2.6*), *it suffices to show only that Equations* (*3.2*), (*3.4*), (*3.6*), *and* (*3.8*) *are satisfied for all* $a, b, c \in L$.

1. *Associativity: We begin by showing that*

$$sup(\{a,b,c\}) = \sup(\sup(a,b),c) = \sup(a,\sup(b,c)). \tag{3.32}$$

Let $s = \sup(\{a,b,c\})$. *Then* s *is a lower bound of* $\{\sup(a,b),c\}$ *because*

$$s \geq a,b,c \implies s \geq a \text{ and } s \geq \sup(b,c). \tag{3.33}$$

Now, to see that s *is the least upper bound, suppose there exists* $d \in L$ *such that* $d \geq a$ *and* $d \geq \sup(b,c)$. *Then* $d \geq a,b,c \implies d \geq s$. *Therefore* $s = \sup(\sup(a,b),c)$. *Similarly, we can show that* $s = \sup(a,\sup(b,c))$. *Now, with Equation (3.32) established, we have that*

$$(a \vee b) \vee c = \sup(a,b) \vee c \tag{3.34}$$

$$= \sup(\sup(a,b),c) \tag{3.35}$$

$$= \sup(\{a,b,c\}) \tag{3.36}$$

$$= \sup(a,\sup(b,c)) \tag{3.37}$$

$$= a \vee \sup(b,c) \tag{3.38}$$

$$= a \vee (b \vee c). \tag{3.39}$$

2. *Commutativity: Since the supremum of two elements is independent of the order*

in which they are taken we have that

$$a \vee b = \sup(a, b) = \sup(b, a) = b \vee a. \tag{3.40}$$

3. *Idempotency: Since* $\leq$ *is reflexive, we have that* $a \vee a = \sup(a, a) = a$.

4. *Absorption: Observe that*

$$\begin{aligned} a \wedge (a \vee b) &= \inf(a, a \vee b) && (3.41) \\ &= \inf(a, \sup(a, b)) && (3.42) \\ &= a, && (3.43) \end{aligned}$$

   where the last equality follows from the fact that $a \leq \sup(a, b)$.

Therefore, $\langle L; \vee, \wedge \rangle$ *is a lattice.* $\square$

Example 3.12. (*lattices as posets*) *For all of the following posets, the existence of the given supremum and infimum can be shown:*

1. $\langle \mathbb{Z}; \leq \rangle$: $\sup(x, y) = \max(x, y)$ *and* $\inf(x, y) = \min(x, y)$.

2. $\langle \wp(S); \subseteq \rangle$: $\sup(A, B) = A \cup B$ *and* $\inf(A, B) = A \cap B$.

3. $\langle \mathbb{N}_0; | \rangle$: $\sup(m, n) = \operatorname{lcm}(m, n)$ *and* $\inf(m, n) = \gcd(m, n)$,

where $m|n$, $\operatorname{lcm}(0, a)$, *and* $\gcd(0, a)$ *are defined as in Examples 2.6 and 3.4.*

Example 3.13. (*non-lattice posets*) *The posets* $\bar{\mathbf{2}} \oplus \bar{\mathbf{3}}$ *and* Q *of Examples 3.8 and 3.9 are clearly not lattices due to the non-existence of suprema already mentioned.*

3.5 Lattice Constructs

The next topic of this chapter is the construction of new lattices from existing ones (in fact, even from posets). We introduce four construction methods:

1. sublattices,
2. dual of a lattice,
3. product of lattices,
4. down-set lattice.

We begin with sublattices. A *sublattice* of a lattice L is a nonempty subset of L that is closed under the meet and join operations of L . Sublattices can inherit properties from the lattice that contain them. Two examples are distributivity and modularity, discussed in Chapter 4. We now give the formal definition followed by some examples.

Definition 3.6. (*sublattice*) *A sublattice of a lattice L is a subset $S \subseteq L$ such that:*

1. $S \neq \emptyset$;
2. $a, b \in S \implies a \vee b \in S$;
3. $a, b \in S \implies a \wedge b \in S$.

Example 3.14. (*sublattices: examples and non-examples*)

1. *Any non-empty subset of a chain is a sublattice. For instance,* $\langle \mathbb{N}; \max, \min \rangle$ *is a sublattice of* $\langle \mathbb{Z}; \max, \min \rangle$.

2. *If* $Y \subseteq X$*, then* $\wp(Y)$ *is a sublattice of* $\wp(X)$*.*

3. *Given* $\wp(X)$ *of a set* X *with* $|X| > 1$*, the set of singleton sets is not a sublattice of* $\wp(X)$ *because given distinct* $a, b \in X$*,* $\{a\} \cap \{b\} = \emptyset$ *and* $\emptyset$ *is not a singleton set.*

Note that a lattice is a sublattice of itself. If we want to disregard this trivial sublattice, we must focus on proper sublattices.

Definition 3.7. (*proper sublattice*)

1. *A proper sublattice of a lattice* L *is a sublattice* S *of* L *such that* $S \neq L$*.*

2. *A maximal proper sublattice of a lattice* L *is a proper sublattice* S *of* L *that is not contained in any other proper sublattice of* L*.*

Example 3.15. (*proper sublattices*)

1. *With the usual order,* $\mathbb{N}$ *is a proper sublattice of* $\mathbb{R}$*. It is not maximal because* $\mathbb{Q}$ *is another proper sublattice of* $\mathbb{R}$ *that contains* $\mathbb{N}$*.*

2. *Given the set* $S = \{a, b, c\}$*, the set* $Q = \{\emptyset, \{a\}, \{b\}, \{a, b\}, \{a, c\}, S\}$ *is a maximal proper sublattice of* $\wp(S)$*. It can be manually verified that* Q *is closed under union and intersection. It is maximal proper because if we add either of the two missing elements of* $\wp(S)$*,* $\{c\}$ *and* $\{b, c\}$*, we must add the other to preserve closure of lattice operations given that*

$$\{b, c\} = \{b\} \cup \{c\}; \tag{3.44}$$

$$\{c\} = \{b, c\} \cap \{a, c\}. \tag{3.45}$$

Sublattices present an interesting contrast between lattices and posets. Recall that any subset of a poset is a subposet. However, not all subsets of a lattice are sublattices. Thus, it is of interest to identify the smallest sublattice that contains a given subset. This is called the sublattice generated by the subset and is a form of "closure" of the subset under join and meet. It is obtained by adding to it all of the missing joins and meets of its elements. If the new expanded subset is not closed under join and meet, we repeat the process with it. We continue until we obtain a subset closed under the operations. Note that a sublattice is its own generated sublattice.

Definition 3.8. (*generated sublattice*) *Let X be a subset of L. The sublattice of L generated by X, $[X]$, is the smallest sublattice of L that contains X.*

Proposition 3.5. (*computing generated sublattice*) *If X is a subset of L, then*

$$[X] = \bigcup_{k=0}^{\infty} X_k, \tag{3.46}$$

where $X_0 = X$ and for $k \geq 1, X_k = \{a \vee b \mid a, b \in X_{k-1}\} \cup \{a \wedge b \mid a, b \in X_{k-1}\}$.

Example 3.16. (*generated sublattice*) *Consider the subset $X = \{\{1\}, \{2\}\}$ of $\wp(\mathbb{N})$. X is clearly not a sublattice since it lacks the union and the intersection of its two elements. It can be shown that $[X] = \wp(\{1, 2\})$ by using Proposition 3.5.*

One last concept related to sublattices is the length of a lattice. Recall from Section 2.4 that the length of a chain is one less than its size and that the length of a poset is the length of its longest chain subposet. Since lattices are posets and chains are always sublattices, we can define the length of a lattice in the same way.

We now move on to lattice duality. Given a lattice L, we can obtain another lattice by "flipping its diagram" (note that lattices have Hasse diagrams because they are posets). The new lattice is called the dual lattice of the original lattice and is denoted L^∂. What we just did is invert the order relationship in L and as a consequence we have turned meets into joins and joins into meets. A more algebraic definition is given with an example.

Definition 3.9. (*dual lattice*) *Given a lattice $\langle L; \vee, \wedge \rangle$, its dual lattice L^∂ is the lattice $\langle L; \wedge, \vee \rangle$ obtained by taking the same set of elements and interchanging the meet and join operations. This also reverses the induced order relation and interchanges the identities. As a result, we have the following:*

1. *$a \leq b$ in L^∂ if and only if $a \geq b$ in L;*

2. *$a \wedge b = c$ in L^∂ if and only if $a \vee b = c$ in L;*

3. *$a \vee b = c$ in L^∂ if and only if $a \wedge b = c$ in L;*

4. *$a = 0$ in L^∂ if and only if $a = 1$ in L;*

5. *$a = 1$ in L^∂ if and only if $a = 0$ in L.*

Example 3.17. (*dual lattice*) *A lattice L and its dual L^∂ are shown in Figure 3.3. Note that in L, $d \leq e$, $b \vee c = d$, $b \wedge c = a$, and $a = 0$ while in L^∂, $d \geq e$, $b \vee c = a$, $b \wedge c = d$, and $a = 1$.*

Just like with posets, we can define dual statements for lattices by interchanging $\wedge$ and $\vee$ and reversing the order symbols of a statement. An example of this are

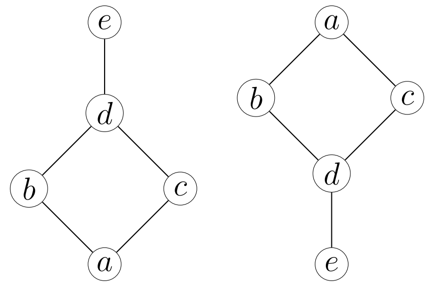


Figure 3.3: A lattice L (left) and its dual L^∂ (right)

the lattice axioms of Definition 3.1, which come in dual pairs. We can also extend Theorem 2.2 to lattices resulting in the Duality Principle for Lattices. This will be an important tool that will lead to efficiency gains in future proofs about lattices.

Our next construct is the product of lattices. We can multiply two or more lattices to get a new lattice. The idea is to define lattice operations in the Cartesian product of two or more lattices using the lattice operations of each of the lattices involved. We present only the formal definition for two lattices, but the idea can be extended to any finite product of lattices $L_1 \times \cdots \times L_n$.

Definition 3.10. (*lattice product*) *Given two lattices L and K, the lattice product of L and K is the lattice on the set $L \times K$ with coordinatewise operations:*

$$(l_1, k_1) \vee (l_2, k_2) = (l_1 \vee_L l_2, k_1 \vee_K k_2); \tag{3.47}$$

$$(l_1, k_1) \wedge (l_2, k_2) = (l_1 \wedge_L l_2, k_1 \wedge_K k_2), \tag{3.48}$$

where $\vee_L$, $\vee_K$, $\wedge_L$, and $\wedge_K$ denote the respective joins and meets of L and K.

Example 3.18. (*lattice product*) *The product lattice* $\mathbf{4} \times \wp(S)$*, where* $S = \{a, b, c\}$*, has* $4 \times 8 = 32$ *elements and operations:*

$$(m, A) \vee (n, B) = (\max(m, n), A \cup B); \tag{3.49}$$

$$(m, A) \wedge (n, B) = (\min(m, n), A \cap B). \tag{3.50}$$

We make a few comments on lattice products before moving on. First, it is straightforward to check that the operations of the product satisfy the 4 lattice axioms; just apply the axioms on each coordinate. Also, the Hasse diagram of a product of lattices can be obtained in the same way as that of a poset product. Finally, given a product of posets that are all lattices, it is possible to define lattice operations using the supremum and infimum of the product order. It can be shown that the resulting lattice is the same as that defined with coordinatewise operations.

We conclude this section with the down-set lattice. Recall from Section 2.5 that given a poset P, we can construct the poset $O(P)$ of all the down-sets of P ordered by set inclusion. It can be shown that down-sets are closed under both union and intersection. Therefore, $\langle O(P); \cup, \cap \rangle$ is a lattice called the down-set lattice of P. It is a sublattice of the power set lattice of P.

3.6 Maps between Lattices

In this section, we discuss maps between lattices. In particular, we introduce lattice homomorphisms which are the lattice equivalent of order-preserving maps for posets (see Section 2.10). We will go over the definitions, some examples, and their relationship with order-preserving maps.

Lattice homomorphisms are functions between lattices that preserves both lattice operations. A special kind of lattice homomorphism is a lattice isomorphism. The existence of a lattice isomorphism between two lattices indicates that they have the same algebraic and order structure. In between them are lattice embeddings: isomorphisms between lattices and sublattices of other lattices. The formal definitions and some examples follow.

Definition 3.11. (*lattice homomorphism*) *Given lattices L and K, a lattice homomorphism is a function $\phi : L \to K$ such that for all $a, b \in L$:*

$$\phi(a \wedge b) = \phi(a) \wedge \phi(b); \tag{3.51}$$

$$\phi(a \vee b) = \phi(a) \vee \phi(b). \tag{3.52}$$

Definition 3.12. (*lattice embedding*) *A lattice embedding is a 1-1 lattice homomorphism. If $\phi : L \to K$ is a lattice embedding, we say that L embeds into K and write $L \rightarrowtail K$.*

Definition 3.13. (*lattice isomorphism*) *A lattice isomorphism is a bijective lattice homomorphism. If $\phi : L \to K$ is a lattice isomorphism, we say that L and K are* *isomorphic and write $L \cong K$. Note that an embedding is an isomorphism between a lattice and its image: $L \rightarrowtail K \iff L \cong \phi(L) \subseteq K$.*

Example 3.19. (*homomorphisms and isomorphisms*)

1. *The identity map on any lattice is an isomorphism.*
2. *Given lattices L and K both with more than one element and a fixed element $a \in K$, the constant map $\phi : L \to K$ given by $\phi(x) = a$ for all $x \in L$ is a homomorphism. It is not an isomorphism because it is not 1-1.*
3. *Figure 3.4 illustrates a homomorphism between the two drawn lattices. It is not an isomorphism because it is not 1-1: $\phi(a) = \phi(b)$.*
4. *Given a lattice product $L \times K$, L and K always embed into $L \times K$. An embedding function of L into the product is $\phi : L \to L \times K$ defined by $\phi(l) = (l, k)$ for a fixed $k \in K$. An embedding for K is obtained similarly. Figure 3.5 illustrates a concrete case: $\mathbf{M}_3 \rightarrowtail \mathbf{M}_3 \times \mathbf{2}$ and $\mathbf{2} \rightarrowtail \mathbf{M}_3 \times \mathbf{2}$.*
5. *The order-isomorphism $\wp(S) \cong \mathbf{2}^k$ of Example 2.53 can be shown to also be a lattice isomorphism. The function given there can be shown to be join-preserving and meet-preserving or we can apply Proposition 3.6, part 2.*

Since lattices are posets, it is natural to ask what relationship, if any, there is between lattice homomorphisms and order-preserving maps. Since the lattice operations determine and are determined by its order structure, it will be no surprise that a lattice homomorphism preserves the order relation. The converse is not true in general: not all order-preserving functions preserve the lattice operations. However,

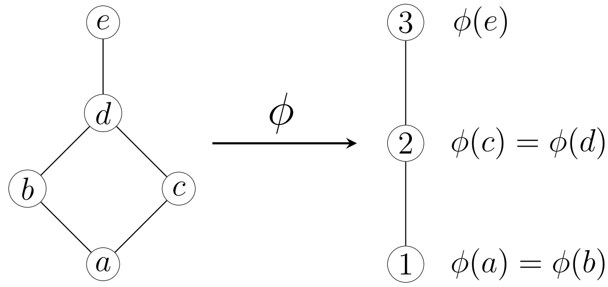


Figure 3.4: A lattice homomorphism ϕ

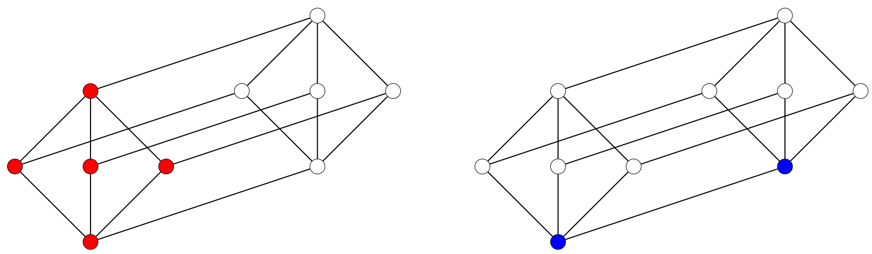


Figure 3.5: Two diagrams of the product $\mathbf{M}_3 \times \mathbf{2}$ showing embeddings of $\mathbf{M}_3$ (left, red) and $\mathbf{2}$ (right, blue).

if we are dealing with bijective functions, then both are equivalent. We conclude this section with a formal statement of all this without proof (which can be found in [5]) and an example of an order-preserving function that is not homomorphic.

Proposition 3.6. (*lattice homomorphism and order preserving maps*) *Let L and K be lattices* (*and hence posets*) *and consider the function $\phi : L \to K$.*

1. *If ϕ is a lattice homomorphism, then ϕ is order-preserving.*

2. *ϕ is a lattice isomorphism if and only if ϕ is an order-isomorphism.*

Example 3.20. (*order-preserving but not homomorphism*) *The function*

$$\phi : \wp([k]) \to [k] \text{ given by } \phi(A) = |A| \tag{3.53}$$

was shown to be order-preserving in Example 2.51. However, it is not a lattice homomorphism because if we let $k \geq 5$, $A = \{1, 2\}$ and $B = \{3, 4, 5\}$, then

$$\phi(A \cup B) = |A \cup B| = 5 \neq 3 = max(|A|, |B|) = max(\phi(A), \phi(B)). \tag{3.54}$$

3.7 Irreducibles

In number theory, one studies how positive integers can be expressed as the product of prime numbers. We now briefly introduce the lattice equivalent of a prime number: an irreducible element. Since a lattice has two operations we will have two types of irreducibles: join-irreducible and meet-irreducible elements. We first define what is a join-irreducible element, then discuss decomposition into join-irreducibles for finite lattices, and finish with meet-irreducibles.

A join-irreducible element in a lattice is an element that cannot be expressed as the join of two elements distinct from itself. The zero element of the lattice is excluded from the definition in the same way that 1 is not considered prime (both are the identity of the operation in question). We present the formal definition followed by an example.

Definition 3.14. (*join-irreducible element*) *A join-irreducible element of a lattice L is an element $x \in L$ such that:*

1. $x \neq 0$ (*if L has* 0),
2. $x = a \vee b \implies a = x$ *or* $b = x$.

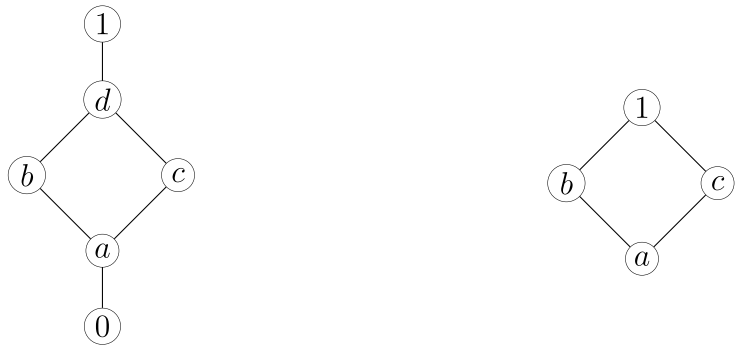


Figure 3.6: A lattice L (left) and its set of join-irreducibles $J(L)$ (right)

The set of all join-irreducible elements of a lattice L *is denoted* $J(L)$*. It is a poset with the order inherited from* L*.*

Example 3.21. (*join-irreducibles and* $J(L)$) *Observe the lattice* L *in Figure 3.6, left. Computing all possible joins of pairs of elements shows that the only joins that produce* a *are* $0 \vee a$ *and* $a \vee a$*. Hence,* a *is join-irreducible. Similarly,* b*,* c*, and 1 are also join-irreducible. On the other hand* d *is not join-irreducible because* $d = b \vee c$ *where* b *and* c *are both distinct from* d*.* $J(L)$ *is illustrated in Figure 3.6, right.*

An important property of join-irreducible elements is that in a finite lattice, any element can be expressed as the join of join-irreducible elements. In particular, it is the join of all of the join irreducible elements that are less than or equal to it in the lattice's order structure. This is similar to the prime factorization of integers. We present this result as a proposition without proof, followed by an example. The interested reader can find the proof in [5].

Proposition 3.7. (*decomposition into join-irreducibles*) *Let* L *be a finite lattice. Then for any* $a \in L$*,*

$$a = \bigvee \{x \in J(L) \mid x \leq a\}. \tag{3.55}$$

Example 3.22. (*singleton sets*) *Given the power set $\wp(X)$ of a finite set X, its join-irreducible elements are exactly the singleton sets because any other subset of X can be written as the union of singleton sets. It then follows that any element of $\wp(X)$ is the join of all the join-irreducible elements less than or equal to it since*

$$Y = \{x_1, x_2, ..., x_n\} \in P(X) \implies Y = \bigcup_{i=1}^{n} \{x_i\}. \tag{3.56}$$

We finish this section by commenting that it is possible to also define a meet-irreducible element as a non-1 element of a lattice that cannot be expressed as the meet of two elements different from itself. The set of meet-irreducible elements of a lattice L is denoted by $M(L)$. In general, however, we will focus only on join-irreducibles for the remainder of this text.

3.8 Complete Lattices

The last section of this chapter quickly presents complete lattices. Recall that a lattice is a poset that contains the supremum and the infimum of any two of its elements. Remember also that this implies that for any finite subset of the poset, its supremum and infimum are also in the poset, as discussed in Section 3.4. However, we left in suspense what happens to infinite subsets. We now return to this matter.

In general, a lattice does not need to contain the supremum and infimum of its infinite subsets. If it does, we say that the lattice is complete. Not all lattices are complete. We now give the precise definition of a complete lattice and some examples.

Definition 3.15. (*complete lattice*) *A complete lattice is a poset L in which for all $S \subseteq L$, $\sup(S)$ and $\inf(S)$ exist in L. These are expressed as $\bigvee S$ (join of S) and $\bigwedge S$ (meet of S) respectively.*

Example 3.23. (*complete lattices*)

1. *All finite lattices are complete because they lack infinite subsets.*

2. *All power set lattices are complete. Given $\wp(S)$ and a set $\{A_i\}_{i\in I}$ where I is some index set and $A_i \subseteq S$ $\forall i$, we have that*

$$\bigvee\{A_i\}_{i\in I} = \bigcup_{i\in I} A_i \quad \textit{and} \quad \bigwedge\{A_i\}_{i\in I} = \bigcap_{i\in I} A_i. \tag{3.57}$$

Example 3.24. (*non-complete lattices*) *The lattices $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ with the usual order are all non-complete since their supremum do not exist in them. In the case of $\mathbb{Q}$, we also have that $\bigvee S$ does not exist in $\mathbb{Q}$ for $S = \{s \in \mathbb{Q} \mid s^2 < 2\}$.*

We bring this section (and chapter) to a close by introducing a special type of complete lattice: a topped intersection structure. It will be helpful in Section 6.5. A topped intersection structure consists of a collection of subsets of a given set X that is closed under arbitrary intersections and that contains X itself.

Definition 3.16. (*topped intersection structure*) *An intersection structure on a set X is a non-empty family $\mathfrak{L}$ of subsets of X that is ordered by inclusion $\subseteq$ and that satisfies the following two properties:*

1. For any non-empty index set I,

$$A_i \in \mathfrak{L},\ \forall i \in I \implies \bigcap_{i \in I} A_i \in \mathfrak{L}; \tag{3.58}$$

2. $X \in \mathfrak{L}$.

It can be shown that any topped intersection structure on a set X is a complete lattice. The meet of collection of subsets in the structure is simply their intersection. On the other hand, the join of a collection of subsets is usually not their union. It is the intersection of all the subsets, in the structure, that contain it (their union). We state this result as a proposition. Its proof can be found in [5].

Proposition 3.8. (*topped intersection structure is complete lattice*) *If $\mathfrak{L}$ is an intersection structure on X, then $\mathfrak{L}$ is a complete lattice with operations:*

$$\bigwedge_{i \in I} A_i = \bigcap_{i \in I} A_i, \tag{3.59}$$

$$\bigvee_{i \in I} A_i = \bigcap \left\{ B \in \mathfrak{L} \mid \bigcup_{i \in I} A_i \subseteq B \right\}, \tag{3.60}$$

where $A_i \in \mathfrak{L}\, \forall i \in I$ over some non-empty index set I.

Chapter 4

Distributive and Modular Lattices

4.1 Introduction

In this chapter, we introduce two distinct classes of lattices that have been extensively studied in the literature; that is, distributive and modular lattices. First, certain basic results on the two classes that include the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem will be reviewed. We then present two modified proofs for a step in the last part of the theorem's proof that are rather shorter than the original proof in both [5] and [4]. To establish this last claim, we propose and apply two original methods for comparing the lengths of certain types of proofs in lattice theory: those based on manipulations of algebraic lattice expressions. We call these methods the proof count method and the proof poset method.

Distributive lattices contain the class of all Boolean algebras as a proper subclass, however they are included in the larger class of modular lattices. The distributive property can be defined by two different dual formats. However in this text, we mostly emphasize on the version where the meet operation distributes into the join operation. The same rule will be followed for the modular lattices, where two dual distinct formats also exist.

This chapter is organized as follows: Section 4.2 defines what are distributive and modular lattices and provides several examples. Section 4.3 presents some elementary results about these lattices (including the relationship between them). Section 4.4 discusses the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem in both theory and application. Section 4.5 lists more results about these lattices that can be derived from the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. Finally, Section 4.6 concludes with a discussion of the last part of the proof of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem, comparing the proof in both [5] and [4] with our modified proofs.

4.2 Basic Definitions

We introduce this chapter's protagonists. We first define distributive and modular lattices. We then survey a variety of examples. We conclude by discussing dual properties satisfied by distributive and modular lattices.

Distributive lattices are lattices where the meet operation distributes into the join operation. This is analogous to the way multiplication distributes into addition in rings except that we will soon see that join also distributes into meet.

Definition 4.1. (*distributive lattice*) *A lattice L is said to be distributive if it satisfies the distributive law:*

$$\forall a, b, c \in L,\ a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c). \tag{4.1}$$

A modular lattice is a lattice in which an expression of the form $a \wedge b \vee c$ defines a unique element without the need of bracketing provided that $a \geq c$.

Definition 4.2. (*modular lattice*) *A lattice L is said to be modular if it satisfies the modular law:*

$$\forall a, b, c \in L,\ a \geq c \implies a \wedge (b \vee c) = (a \wedge b) \vee c. \tag{4.2}$$

We immediately establish a basic and useful relationship between distributive and modular lattices. Distributive lattices are modular. The proof takes advantage of the similarity in the statements of both laws.

Proposition 4.1. (*distributive implies modular*) *A distributive lattice is modular.*

Proof *This is a consequence of the Connecting Lemma.* □

However, the converse of Proposition 4.1 is not true. Example 4.6 will introduce a modular lattice that is not distributive. Thus, the class of modular lattices is larger than the class of distributive lattices.

We now discuss the distributivity and modularity (or lack thereof) of a variety of lattices. Note that in most examples, we will not prove either property directly. Instead, we will make reference to results in subsequent sections that establish the property in question.

Example 4.1. (*power set lattice*) *For any set S, the power set lattice $\wp(S)$ is distributive (and hence modular by Proposition 4.1) because for any sets A, B, and C of S,*

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C). \tag{4.3}$$

Example 4.2. (*chains*) *All chains are distributive and modular. See Example 4.9 for a non-case-exhaustive proof of this.*

Example 4.3. (*divisibility lattice*) *The lattice* $\langle \mathbb{N}_0; \mathrm{lcm}, \mathrm{gcd} \rangle$ *introduced in Example 3.4 is distributive and hence modular by Proposition 4.1. Distributivity will follow from Proposition 4.6. To apply it, it must be shown that for all* $a, b, c \in \mathbb{N}_0$,

$$\mathrm{lcm}(a, b) = \mathrm{lcm}(c, b) \text{ and } \mathrm{gcd}(a, b) = \mathrm{gcd}(c, b) \implies a = c. \tag{4.4}$$

This can be done by expressing each gcd *and each* lcm *in terms of the prime factorizations of the involved numbers except when any of* a, b, *or* c *is* 0. *In that case, it can be shown directly recalling* $\mathrm{lcm}(0, m) = 0$, $\mathrm{gcd}(0, m) = m$, *and the order relation* $\mid$ *on* $\langle \mathbb{N}_0; \mathrm{lcm}, \mathrm{gcd} \rangle$ (*see Example 3.10, item 3*).

Example 4.4. (*subgroup lattices*) *Subgroup lattices are not necessarily distributive nor modular. The lattice* $Sub\, D_4$ *provides a counter-example for both where* D_4 *is the dihedral group of symmetries of a square. This can be shown by drawing its Hasse diagrams and applying Theorem 4.1. However, it can be shown that for any group* G, $Sub\, G$ *is distributive if and only if* G *is locally cyclic. As a result, we have that* $Sub\, G$ *is distributive for any cyclic group* G. *For details on how to prove this, see [17].*

Example 4.5. (*normal subgroup lattices*) *For any group* G, $\mathcal{N}\text{-}Sub\, G$ *is modular. To prove this, we can apply Lemma 4.1 and reduce the problem to showing that if* $H \supseteq N$, *then* $H \cap (KN) \subseteq (H \cap K)N$ *using basic group theory. However,* $\mathcal{N}\text{-}Sub\, G$ *may be non-distributive. A counter-example is* $\mathcal{N}\text{-}Sub\, \mathbb{Z}_2 \times \mathbb{Z}_4$. *This can be seen by*

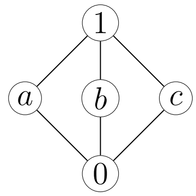


Figure 4.1: The diamond $\mathbf{M}_3$

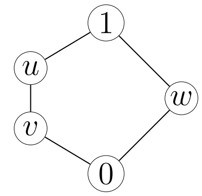


Figure 4.2: The pentagon $\mathbf{N}_5$

drawing its Hasse diagrams and applying Theorem 4.1. Conditions on a finite group G that make $\mathcal{N}$-Sub G distributive can be found in [17].

Example 4.6. (*diamond lattice*) *The lattice $\mathbf{M}_3$, called the diamond and shown in Figure 4.1, is modular but not distributive. Modularity can be verified exhaustively but will also follow from Corollary 4.2 because $\mathbf{M}_3$ has length 2. To see that it is not distributive, note that:*

$$a \wedge (b \vee c) = a \wedge 1 = a; \tag{4.5}$$

$$(a \wedge b) \vee (a \wedge c) = 0 \vee 0 = 0; \tag{4.6}$$

$$\therefore a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c). \tag{4.7}$$

Example 4.7. (*pentagon lattice*) *The lattice $\mathbf{N}_5$, called the pentagon and shown in Figure 4.2, is neither distributive nor modular. Proof of this is shown below: non-distributivity on Equation (4.8), non-modularity on Equation (4.9) (noting $u \geq v$):*

$$u \wedge (v \vee w) = u \wedge 1 = u \neq v = v \vee 0 = (u \wedge v) \vee (u \wedge w); \tag{4.8}$$

$$u \wedge (w \vee v) = u \wedge 1 = u \neq v = 0 \vee v = (u \wedge w) \vee v. \tag{4.9}$$

We remark that $\mathbf{M}_3$ and $\mathbf{N}_5$ will play an important role in the study of distributivity and modularity in lattices. We will see that these are the smallest non-distributive lattices by Theorem 4.1. Said theorem will also imply that $\mathbf{N}_5$ is the smallest non-modular lattice.

We conclude this section by discussing the duals of the distributive and modular laws. These are obtained by interchanging the meets and joins and flipping the inequalities in the statements of the original laws. In the case of distributivity, we get that join distributes into meet. We show that the dual laws are equivalent to the original ones and, thus, distributivity and modularity can be defined using either of them.

Proposition 4.2. (*dual distributive law*) *A lattice L is distributive if and only if it satisfies the following dual distributive law:*

$$\forall a, b, c \in L,\ a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c). \tag{4.10}$$

Proof *We show that a distributive lattice satisfies the dual law. The converse follows by duality. Suppose L is distributive and that $a, b, c \in L$. Then letting (As) denote associatitvity, (C) commutativity, (Ab) absorption, and (D) the distributive law; we get:*

$$\begin{aligned}
(a \vee b) \wedge (a \vee c) &= [(a \vee b) \wedge a] \vee [(a \vee b) \wedge c] && (D) && (4.11)\\
&= a \vee [c \wedge (a \vee b)] && (Ab, C) && (4.12)\\
&= a \vee [(c \wedge a) \vee (c \wedge b)] && (D) && (4.13)
\end{aligned}$$

$$= [a \vee (c \wedge a)] \vee (c \wedge b) \qquad (As) \tag{4.14}$$

$$= a \vee (b \wedge c). \qquad (Ab, C) \tag{4.15}$$

Thus, L satisfies the dual distributive law. □

Proposition 4.3. (*dual modular law*) *A lattice L is modular if and only if it satisfies the following dual modular law:*

$$\forall a, b, c \in L,\ a \leq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c. \tag{4.16}$$

Proof *We show that a modular lattice satisfies the dual law. The converse follows by duality. Suppose L is modular and that $a, b, c \in L$ with $a \leq c$. Then applying commutativity and the modular law with $c \geq a$, we obtain:*

$$(a \vee b) \wedge c = c \wedge (a \vee b) \tag{4.17}$$

$$= c \wedge (b \vee a) \tag{4.18}$$

$$= (c \wedge b) \vee a \tag{4.19}$$

$$= a \vee (b \wedge c). \tag{4.20}$$

Thus, L satisfies the dual modular law. □

Finally, we stress that the equivalence of these dual statements requires the $\forall$ quantifiers. It may be that $p \wedge (q \vee r) = (p \wedge q) \vee (p \wedge r)$ but $p \vee (q \wedge r) \neq (p \vee q) \wedge (p \vee r)$ for particular elements p, q, and, r in a lattice L. An occurrence of this is given in Example 4.8.

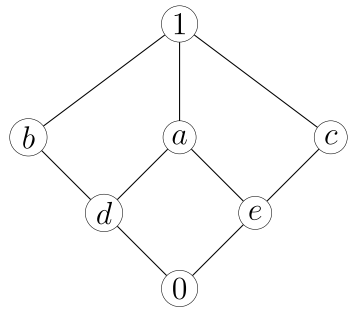


Figure 4.3: Lattice L of Example 4.8

Example 4.8. (*non-equivalence of dual laws for particular elements*) *Consider the lattice* $L = \{0, a, b, c, d, e, 1\}$ *shown in Figure 4.3. Note below that the triple* (a, b, c) *satisfies the distributive law* (*Equation* (*4.21*)) *but not the dual distributive law* (*Equation* (*4.22*))*:*

$$a \wedge (b \vee c) = a \wedge 1 = a = d \vee e = (a \wedge b) \vee (a \wedge c); \tag{4.21}$$

$$a \vee (b \wedge c) = a \vee 0 = a \neq 1 = 1 \vee 1 = (a \vee b) \wedge (a \vee c). \tag{4.22}$$

4.3 Basic Results

With distributive and modular lattices defined, we discuss some basic properties about them in this section. In particular, we show the following:

1. All lattices are halfway to being both distributive and modular.

2. The modular law can be rewritten as an identity.

3. Distributivity and modularity are both preserved by inclusion, products, homomorphisms, and duality of lattices.

We begin by proving that all lattices are "half-distributive" and "half-modular". By this, we mean that if the $=$ sign in the law statements in Definitions 4.1 and 4.2 is changed to $\geq$, then the new statements are true for all lattices. Thus, proving that a lattice satisfies either law reduces to showing only $\leq$.

Lemma 4.1. (*half-way lemma*) *Let L be a lattice with $a, b, c \in L$. Then*

1. $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$;

2. $a \geq c \implies a \wedge (b \vee c) \geq (a \wedge b) \vee c$.

Proof *Part 1: By Proposition 3.2 and idempotency of $\vee$:*

$$(a \wedge b) \vee (a \wedge c) \leq [a \wedge (b \vee c)] \vee [a \wedge (b \vee c)] \tag{4.23}$$

$$= a \wedge (b \vee c). \tag{4.24}$$

Part 2: This is a direct consequence of Part 1 and the Connecting Lemma. □

Our next step is to establish that the modular law can be rewritten as an identity satisfied by any three elements of a modular lattice. This is applied in the proof of Proposition 4.4, Part 3.

Lemma 4.2. (*modular identity*) *Let L be a lattice. Then L is modular if and only if for all $p, q, r \in L$, the following identity holds*

$$p \wedge (q \vee (p \wedge r)) = (p \wedge q) \vee (p \wedge r). \tag{4.25}$$

Proof $\Longrightarrow$ *: Suppose that L is modular. Observe that $p \geq p \wedge r$. Then the modular law with $a = p$ and $c = p \wedge r$ implies that*

$$p \wedge (q \vee (p \wedge r)) = (p \wedge q) \vee (p \wedge r). \tag{4.26}$$

$\Longleftarrow$ *: Suppose that the identity holds. Let $a, b, c \in L$ with $a \geq c$. Then L is modular because*

$$\begin{aligned} a \wedge (b \vee c) &= a \wedge (b \vee (a \wedge c)) && \textit{since } a \wedge c = c && (4.27)\\ &= (a \wedge b) \vee (a \wedge c) && \textit{by our hypothesis} && (4.28)\\ &= (a \wedge b) \vee c && \textit{since } a \wedge c = c. && (4.29) \end{aligned}$$

Therefore, the lemma is proved. □

Next, we present a proposition that is a "factory" that outputs new distributive (or modular) lattices from known distributive (or modular) lattices. It is known that there are multiple ways of creating new lattices from known lattices. Four of these ways (sublattices, lattice product, image under lattice homomorphism, and duality) preserve both distributivity and modularity.

Proposition 4.4. (*lattice constructs that preserve distributivity and moduratity*)

1. *A sublattice of a distributive (modular) lattice is distributive (modular).*

2. *The product of two distributive (modular) lattices is distributive (modular).*

3. *The homomorphic image of a distributive (modular) lattice is distributive*

(modular).

4. *The dual of a distributive (modular) lattice is distributive (modular).*

Proof

1. *This is true because any three elements breaking the distributive (modular) law in the sublattice would do the same in the lattice and produce a contradiction.*

2. *Let L and K be distributive lattices and $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in L \times K$. Applying the coordinatewise definition of meet and join in $L \times K$ and the distributivity of L and K we get*

$$\begin{aligned}
(a_1, a_2) \wedge [(b_1, b_2) \vee (c_1, c_2)] &= (a_1, a_2) \wedge (b_1 \vee c_1, b_2 \vee c_2) && (4.30)\\
&= (a_1 \wedge [b_1 \vee c_1], a_2 \wedge [b_2 \vee c_2]) && (4.31)\\
&= ([a_1 \wedge b_1] \vee [a_1 \wedge c_1], [a_2 \wedge b_2] \vee [a_2 \wedge c_2]) && (4.32)\\
&= (a_1 \wedge b_1, a_2 \wedge b_2) \vee (a_1 \wedge c_1, a_2 \wedge c_2) && (4.33)\\
&= [(a_1, a_2) \wedge (b_1, b_2)] \vee [(a_1, a_2) \wedge (c_1, c_2)]. && (4.34)
\end{aligned}$$

Therefore, $L \times K$ is distributive. The proof for the product of modular lattices is similar keeping in mind that $(a_1, a_2) \geq (c_1, c_2)$ if and only if $a_1 \geq c_1$ and $a_2 \geq c_2$.

3. *Let L be a distributive lattice and ϕ a lattice homomorphism with domain L. Let $K = \phi(L)$ and let $a, b, c \in K$. Then there exist $x, y, z \in L$ such that $a = \phi(x)$,*

$b = \phi(y)$, *and* $c = \phi(z)$. *Since* ϕ *preserves meets and joins we have*

$$a \wedge (b \vee c) = \phi(x) \wedge (\phi(y) \vee \phi(z)) \tag{4.35}$$

$$= \phi(x \wedge (y \vee z)) \tag{4.36}$$

$$= \phi((x \wedge y) \vee (x \wedge z)) \tag{4.37}$$

$$= (\phi(x) \wedge \phi(y)) \vee (\phi(x) \wedge \phi(z)) \tag{4.38}$$

$$= (a \wedge b) \vee (a \wedge c). \tag{4.39}$$

Therefore, $K = \phi(L)$ *is distributive. The proof for the homomorphic image of a modular lattice is similar but using the modular identity (Equation (4.25)) rather than the modular law.*

4. *See Corollary 4.1 in Section 4.5.* □

We finish by illustrating how to apply Proposition 4.4 to construct more distributive and modular lattices from known ones.

Example 4.9. (*chains distributive and modular*) *Let* $\mathbf{n}$ *be the* n*-element chain. We claim that* $\mathbf{n}$ *is distributive and modular. Note that* $\mathbf{n}$ *is a sublattice of* $\wp(X)$ *for any set* X *with cardinality* $n - 1$. *To see this, consider the sequence*

$$\emptyset \subseteq \{x_1\} \subseteq \{x_1, x_2\} \subseteq ... \subseteq X = \{x_1, x_2, ..., x_{n-1}\} \tag{4.40}$$

and apply the Connecting Lemma to it. Our claim follows from $\wp(X)$*'s distributivity and modularity and Proposition 4.4 Part 1.*

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

This section introduces the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem, which characterizes distributive and modular lattices. A sketch of its proof and applications are discussed. The idea is that $\mathbf{N}_5$ is the basic building block of non-modular lattices in the sense that all non-modular lattices contain it. Similarly, $\mathbf{M}_3$ and $\mathbf{N}_5$ are the basic building blocks of non-distributive lattices. The theorem provides a way of showing a lattice is non-modular or non-distributive without having to search directly for three elements that violate the corresponding law. Instead, we must find a sublattice that contains such three elements.

Theorem 4.1. ($\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem*) *Let L be a lattice.*

1. *L is non-modular if and only if $\mathbf{N}_5$ is a sublattice of L.*

2. *L is non-distributive if and only if $\mathbf{N}_5$ or $\mathbf{M}_3$ is a sublattice of L.*

Proof Sketch *We provide a sketch of the proof in Davey and Priestley (page 89 of [5]; also in [4]). Given that sublattices of modular (distributive) lattices are modular (distributive) and that $\mathbf{N}_5$ and $\mathbf{M}_3$ are non-modular and modular but not distributive respectively, it suffices to show that (i) a non-modular lattice has $\mathbf{N}_5$ as a sublattice and (ii) that a non-distributive modular lattice has $\mathbf{M}_3$ as a sublattice.*

Part (i): Suppose that L is a non-modular lattice. Then there exist $d, e, f \in L$ with $d > f$ such that $d \wedge (e \vee f) > (d \wedge e) \vee f$. This is because by Lemma 4.1,

$$d \wedge (e \vee f) \neq (d \wedge e) \vee f \implies d \wedge (e \vee f) > (d \wedge e) \vee f. \tag{4.41}$$

Define $a = (d \wedge e) \vee f$ *and* $b = d \wedge (e \vee f)$*. It can be shown that* $a \wedge e = b \wedge e$ *and* $a \vee e = b \vee e$*. Let* $p = a \wedge e$ *and* $q = a \vee e$*. Then* $K = \{p, q, a, b, e\}$ *is a sublattice of* L *that satisfies the necessary joins and meets to be isomorphic to* $\mathbf{N}_5$*. It can be verified that all 5 elements of* K *are distinct. Therefore,* $K \cong \mathbf{N}_5$ *and* L *has a sublattice isomorphic to* $\mathbf{N}_5$*.*

Part (ii): Suppose that L *is a modular but non-distributive lattice. Then there exist* $d, e, f \in L$ *such that* $d \wedge (e \vee f) > (d \wedge e) \vee (d \wedge f)$*. This is because by Lemma 4.1,*

$$d \wedge (e \vee f) \neq (d \wedge e) \vee (d \wedge f) \implies d \wedge (e \vee f) > (d \wedge e) \vee (d \wedge f). \tag{4.42}$$

Define the following five elements in L*:*

$$p = (d \wedge e) \vee (e \wedge f) \vee (f \wedge d), \tag{4.43}$$

$$q = (d \vee e) \wedge (e \vee f) \wedge (f \vee d), \tag{4.44}$$

$$u = (d \wedge q) \vee p, \tag{4.45}$$

$$v = (e \wedge q) \vee p, \tag{4.46}$$

$$w = (f \wedge q) \vee p. \tag{4.47}$$

It can be shown that $K = \{p, q, u, v, w\}$ *is a sublattice of* L *isomorphic to* $\mathbf{M}_3$*. This requires proving that*

1. $p < q$;

2. $p \leq u, v, w \leq q$;

3. $u \wedge v = v \wedge w = w \wedge u = p$;

4. $u \vee v = v \vee w = w \vee u = q$;

5. All five elements of K are distinct.

We comment that in item 3, the proofs of $u \wedge v = p$, $v \wedge w = p$, and $w \wedge u = p$ are all similar. In Section 4.6, we discuss in detail the proof of $u \wedge v = p$. To be more precise, we review the proof in [5] (and [4]) and propose two new shorter proofs. □

Having proven the theorem, it is time to apply it to determine whether a given lattice is distributive, only modular, or neither. The first step is to search for a copy of $\mathbf{M}_3$ or $\mathbf{N}_5$ in the lattice. If one is found, then the lattice is non-distributive ($\mathbf{M}_3$) or non-modular ($\mathbf{N}_5$). If the search fails, we conjecture the lattice is distributive (or at least modular) and try to show it. One way to do so is to embed the lattice in a product of distributive or modular lattices and apply Proposition 4.4. Sometimes, this is not possible and we must show the non-existence of isomorphic copies of $\mathbf{M}_3$ or $\mathbf{N}_5$ by contradiction using a brute-force argument. We wrap-up the section with some examples.

Example 4.10. (*Applying* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem 1*) *Consider the lattice L_1 shown in Figure 4.4. Observe that $\{0, x, y, z, 1\}$ is a sublattice of L_1 isomorphic to $\mathbf{N}_5$. Then L_1 is non-modular and non-distributive by the* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem.*

Example 4.11. (*Applying* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem 2*) *Consider the lattice L_2 shown in Figure 4.6. Note that it cannot have a sublattice isomorphic* $\mathbf{M}_3$ *because it does not*

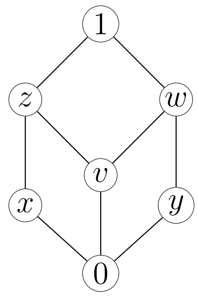


Figure 4.4: The lattice L_1

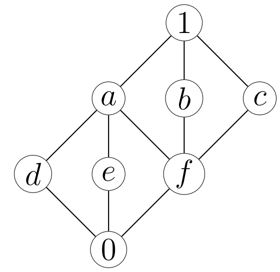


Figure 4.5: Lattice $\mathbf{M}_{3,3}$

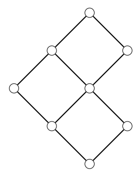


Figure 4.6: The lattice L_2

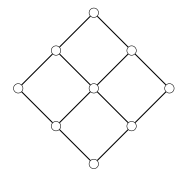


Figure 4.7: The lattice $\mathbf{3} \times \mathbf{3}$

contain antichains of 3 elements. At a glance, it seems to also not have a sublattice isomorphic to $\mathbf{N}_5$*. It happens to be distributive (and hence modular). To show this, note that* L_2 *is a sublattice of* $\mathbf{3} \times \mathbf{3}$ *(Figure 4.7) which is distributive by Example 4.9 and Proposition 4.4 Part 2.*

Example 4.12. *(Applying* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem 3:* $\mathbf{M}_{3,3}$*) Consider the lattice* $\mathbf{M}_{3,3}$ *shown in Figure 4.5. It clearly contains sublattices isomorphic to* $\mathbf{M}_3$ *(e.g.* $\{1, a, b, c, f\}$*). Hence, it is not distributive. It seems not to contain a sublattice isomorphic to* $\mathbf{N}_5$*. We prove that it does not below (an example of the brute-force approach mentioned earlier). Thus, we have the following proposition.*

Proposition 4.5. ($\mathbf{M}_{3,3}$ *modular but not distributive)* $\mathbf{M}_{3,3}$ *is modular but not distributive.*

Proof *By the above discussion, it suffices to show that* $\mathbf{M}_{3,3}$ *has no sublattice isomorphic to* $\mathbf{N}_5$*. We do so by contradiction. Suppose* K *is a sublattice of* $\mathbf{M}_{3,3}$ *isomorphic* *to* $\mathbf{N}_5$*. Then* K *contains a 4-chain* C_4*. Given the structure of* $\mathbf{M}_{3,3}$*,* $C_4 = \{1, u, v, 0\}$ *where* $u = a$ *or* $v = f$*. In addition,* K *must contain an element* w *that is not comparable to neither* u *nor* v*. We show this is not possible if* K *is a sublattice. There are three cases.*

Case 1: $u = a$ *and* $v = f$*. In this case there is no such* w *since all of the remaining elements of* $\mathbf{M}_{3,3}$ *(*b*,*c*,*d*, and* e*) are comparable to either* u *or* v*.*

Case 2: $u = a$ *and* $v \neq f$*. This implies that* $w = b$ *or* $w = c$ *because all other remaining elements are comparable to* u*. However, this implies that* $u \wedge w = f \notin K$*. Therefore,* K *is not a sublattice.*

Case 3: $u \neq a$ *and* $v = f$*. This is the same as Case 2 with* $w = d$ *or* $w = e$ *implying* $v \vee w = a \notin K$*.*

$\therefore$ $\mathbf{M}_{3,3}$ *cannot contain a sublattice isomorphic to* $\mathbf{N}_5$*.* □

4.5 Consequences of the M$_3$-N$_5$ Theorem

The $\mathbf{M}_3$-$\mathbf{N}_5$ theorem leads to more interesting results about distributive and modular lattices . This section presents three of them:

1. preservation of distributivity and modularity by duality

2. modularity of length 2 lattices

3. 2 conditions that characterize distributive and modular lattices.

We begin by showing Part 4 of Proposition 4.4: that duality preserves distributivity and modularity. Recall that the dual of a lattice L is the lattice L^{∂} obtained by taking the elements of L and flipping the order relation (or equivalently interchanging their meets and joins).

Corollary 4.1. (*duals of distributive and modular lattices*) *The dual of a distributive (modular) lattice is distributive (modular).*

Proof *Suppose the L is a distributive lattice. Then L does not have a sublattice isomorphic to neither $\mathbf{M}_3$ or $\mathbf{N}_5$ by the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. Since $\mathbf{M}_3$ and $\mathbf{N}_5$ are both self-dual lattices, L^∂ cannot contain neither of them as a sublattice. Therefore, L^∂ is distributive by the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. The proof for the dual of a modular lattice is the same but using only $\mathbf{N}_5$.* □

Next, we show that all lattices of length 2 are modular. This implies that $\mathbf{M}_n$ is modular for all n.

Corollary 4.2. (*length 2 implies modular*) *Any lattice of length 2 is modular.*

Proof *We show this by contradiction: Suppose that L is a non-modular lattice of length 2. By the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem, L has a sublattice isomorphic to $\mathbf{N}_5$ which contains a chain of length 3. Then L has length ≥ 3. Contradiction.* □

Finally, we establish another characterization of distributive and modular lattices. The idea is to take note of the elements of $\mathbf{M}_3$ and $\mathbf{N}_5$ that violate the laws and construct statements that guarantee their non-existence. In $\mathbf{M}_3$, the problem is in the 3-element antichain whose elements all join and meet pairwise at the same element. Similarly, the problem in $\mathbf{N}_5$ is the 2-element chain whose elements share both meet and join with a third non-comparable element. The conditions in the following proposition state that if a lattice has three elements with said meets and joins, then they are not distinct. This would reduce a hypothetical copy of $\mathbf{M}_3$ or $\mathbf{N}_5$ to $\mathbf{M}_2$ which is both distributive and modular.

Proposition 4.6. (*characterization of distributivity and modularity*) *Let L be a lattice. Then*

(*i*) *L is distributive if and only if*

$$\forall a, b, c \in L,\ (a \wedge b = c \wedge b \text{ and } a \vee b = c \vee b) \implies a = c. \tag{4.48}$$

(*ii*) *L is modular if and only if*

$$\forall a, b, c \in L,\ (a \geq c \text{ and } a \wedge b = c \wedge b \text{ and } a \vee b = c \vee b) \implies a = c. \tag{4.49}$$

Proof *We show that the distributive and modular laws imply the conditions algebraically. To show the reverse implications, we find elements in $\mathbf{M}_3$ and $\mathbf{N}_5$ that do not satisfy the conditions and invoke the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem.*

Part (i): $\implies$ *: Suppose L is distributive and that $a, b, c \in L$ are elements such that*

$$a \wedge b = c \wedge b \text{ and } a \vee b = c \vee b. \tag{4.50}$$

We show that $a = c$. If (A) denotes absorption, (D) distributive property, and (4.50) *the condition in Equation (4.50); we have*

$$
\begin{aligned}
a &= a \wedge (a \vee b) && (A) && (4.51)\\
&= a \wedge (c \vee b) && (\mathit{4.50}) && (4.52)\\
&= (a \wedge c) \vee (a \wedge b) && (D) && (4.53)\\
&= (a \wedge c) \vee (c \wedge b) && (\mathit{4.50}) && (4.54)\\
&= c \wedge (a \vee b) && (D) && (4.55)\\
&= c \wedge (c \vee b) && (\mathit{4.50}) && (4.56)\\
&= c. && (A) && (4.57)
\end{aligned}
$$

$\Longleftarrow$ *: Note that in* $\mathbf{M}_3$ *(Figure 4.8),*

$$a \wedge b = c \wedge b = 0 \tag{4.58}$$

$$a \vee b = c \vee b = 1 \tag{4.59}$$

$$a \neq c. \tag{4.60}$$

Similarly, in $\mathbf{N}_5$ *(Figure 4.9),*

$$u \wedge w = v \wedge w = 0 \tag{4.61}$$

$$u \vee w = v \vee w = 1 \tag{4.62}$$

$$u \neq v. \tag{4.63}$$

$\therefore$ *The condition in (i) is equivalent to the distributive law.*

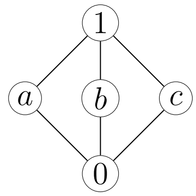


Figure 4.8: The diamond $\mathbf{M}_3$

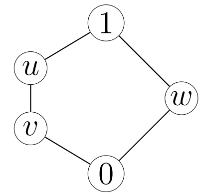


Figure 4.9: The pentagon $\mathbf{N}_5$

Part (ii): $\Longrightarrow$ *: Suppose L is modular and that $a, b, c \in L$ are elements such that*

$$a \geq c,\ a \wedge b = c \wedge b,\ \text{and } a \vee b = c \vee b. \tag{4.64}$$

We show that $a = c$. If (A) denotes absorption, (C) commutativity, (M) modular law, and (4.64) the supposition in Equation (4.64); we have

$$
\begin{aligned}
a &= a \wedge (a \vee b) \quad (A) && (4.65)\\
&= a \wedge (c \vee b) \quad (4.64) && (4.66)\\
&= a \wedge (b \vee c) \quad (C) && (4.67)\\
&= (a \wedge b) \vee c \quad (M) && (4.68)\\
&= (c \wedge b) \vee c \quad (4.64) && (4.69)\\
&= c. \qquad\qquad\ \ (A) && (4.70)
\end{aligned}
$$

$\Longleftarrow$ *: Observe that in $\mathbf{N}_5$ (Figure 4.9),*

$$u \geq v \tag{4.71}$$

$$u \wedge w = v \wedge w = 0 \tag{4.72}$$

$$u \vee w = v \vee w = 1 \tag{4.73}$$

$$u \neq v. \tag{4.74}$$

$\therefore$ *The condition in (ii) is equivalent to the modular law.* □

4.6 Shortcuts to Proof of $\mathbf{M_3}$-$\mathbf{N_5}$ Theorem

As promised, we now return to showing $u \wedge v = p$ in Part (ii) of the proof of Theorem 4.1. To be precise, we present the proof in [5, 4] and then propose two new proofs. One of them is short-cut on the original proof while the other takes a different route. We then compare the length of the three proofs with the two original methods mentioned in Section 4.1: proof count and proof poset. The proof count will consist of comparing their lengths in terms of lines and symbols used while the proof poset will involve graphing posets representing their logical structure. The proofs will be shorter in both methods but the difference will be more noticeable with the first. Afterwards, we do further experimentation with the idea of proof posets.

4.6.1 3 Proofs of $u \wedge v = p$

We now discuss the three proofs of $u \wedge v = p$. All three have the same general strategy: algebraic manipulation of lattice expressions starting from $u \wedge v$ and ending with p. In particular they involve substitution of u, v, p, and q for their definitions and applications of lattice axioms, modular law, and the Connecting Lemma.

We now present the three proofs. Each proof is followed by a list of justifications for each algebraic step. In these justifications, we make several references to the modular law with $a, b, c \in L$ and $a \geq c$ such that $a \wedge (b \vee c) = (a \wedge b) \vee c$. Not all uses of commutativity and associativity in the proofs are mentioned. The reader is advised to consult the proof of Theorem 4.1 in Section 4.4 to recall the definitions of and the relations among the elements treated in the proofs.

We begin with the classical proof given in page 91 of [5] (book by B. A. Davey and H. A. Priestley). It is also in [4]. We will call it Proof 1.

Proof 1. (*Classical proof in [5] and [4]*)

$$
\begin{aligned}
u \wedge v &= ((d \wedge q) \vee p) \wedge ((e \wedge q) \vee p) && \text{(4.75a)}\\
&= (((e \wedge q) \vee p) \wedge (d \wedge q)) \vee p && \text{(4.75b)}\\
&= ((q \wedge (e \vee p)) \wedge (d \wedge q)) \vee p && \text{(4.75c)}\\
&= ((e \vee p) \wedge (d \wedge q)) \vee p && \text{(4.75d)}\\
&= ((d \wedge (e \vee f)) \wedge (e \vee (f \wedge d))) \vee p && \text{(4.75e)}\\
&= (d \wedge ((e \vee f) \wedge (e \vee (f \wedge d)))) \vee p && \text{(4.75f)}\\
&= (d \wedge (((e \vee f) \wedge (f \wedge d)) \vee e)) \vee p && \text{(4.75g)}\\
&= (d \wedge ((f \wedge d) \vee e)) \vee p && \text{(4.75h)}\\
&= ((d \wedge e) \vee (f \wedge d)) \vee p && \text{(4.75i)}\\
&= p && \text{(4.75j)}
\end{aligned}
$$

Justification for each step of Proof 1

- (*4.75a*) *By definition of u and v.*

- *(4.75b) Applying modular law with* $a = (e \wedge q) \vee p$, $b = d \wedge q$, *and* $c = p$.

- *(4.75c) Applying modular law with* $a = q$, $b = e$, *and* $c = p$.

- *(4.75d) By associativity, commutativity, and idempotency on* q.

- *(4.75e) By definitions of* p *and* q, *associativity, commutativity, and absorption.*

- *(4.75f) By associativity.*

- *(4.75g) Applying modular law with* $a = e \vee f$, $b = f \wedge d$, *and* $c = e$.

- *(4.75h) Since* $f \wedge d \leq f \leq e \vee f$.

- *(4.75i) Applying modular law with* $a = d$, $b = e$, *and* $c = f \wedge d$.

- *(4.75j) Since* $(d \wedge e) \vee (f \wedge d) \leq p$ *by definition of* p. $\square$

We now discuss two new proofs of the same result. These will be Proofs 2 and 3 respectively.

1. Proof 2: Proof by M. R. Emamy-K (unpublished before). It takes a short-cut in Proof 1.

2. Proof 3: New proof by G. A. Meléndez Ríos (the author of this thesis). It results from trying to re-create either of the first two proofs from memory but taking a different route to the same result instead.

Proof 2. (*M. R. Emamy-K.*)

$$u \wedge v = ((d \wedge q) \vee p) \wedge ((e \wedge q) \vee p) \tag{4.76a}$$

$$= (((e \wedge q) \vee p) \wedge (d \wedge q)) \vee p \tag{4.76b}$$

$$= ((q \wedge (e \vee p)) \wedge (d \wedge q)) \vee p \tag{4.76c}$$

$$= ((e \vee p) \wedge (d \wedge q)) \vee p \tag{4.76d}$$

$$= ((d \wedge (e \vee f)) \wedge (e \vee (f \wedge d))) \vee p \tag{4.76e}$$

$$= (((e \vee f) \wedge d) \wedge (e \vee (f \wedge d))) \vee p \tag{4.76f}$$

$$= ((e \vee f) \wedge ((d \wedge e) \vee (f \wedge d))) \vee p \tag{4.76g}$$

$$= p \tag{4.76h}$$

Justification for each step of Proof 2

- *(4.76a)-(4.76e) Identical to (4.75a)-(4.75e) in Proof 1.*
- *(4.76f) By commutativity.*
- *(4.76g) By associativity and applying modular law with* $a = d$, $b = e$, *and* $c = f \wedge d$.
- *(4.76h) Since* $((e \vee f) \wedge ((d \wedge e) \vee (f \wedge d))) \leq p$ *by definition of* p. □

Proof 3. (*G. A. Meléndez Ríos*)

$$u \wedge v = [(d \wedge q) \vee p] \wedge [(e \wedge q) \vee p] \tag{4.77a}$$

$$= [q \wedge (d \vee p)] \wedge [q \wedge (e \vee p)] \tag{4.77b}$$

$$= q \wedge \{(d \vee p) \wedge (e \vee p)\} \tag{4.77c}$$

$$= q \wedge \{[d \vee (e \wedge f)] \wedge [e \vee (d \wedge f)]\} \tag{4.77d}$$

$$= q \wedge \{[(d \vee (e \wedge f)) \wedge e] \vee (d \wedge f)\} \tag{4.77e}$$

$$= q \wedge \{[(e \wedge d) \vee (e \wedge f)] \vee (d \wedge f)\} \tag{4.77f}$$

$$= q \wedge \{(e \wedge d) \vee (e \wedge f) \vee (d \wedge f)\} \tag{4.77g}$$

$$= q \wedge p \tag{4.77h}$$

$$= p \tag{4.77i}$$

Justification for each step of Proof 3

- *(4.77a) By definition of u and v.*
- *(4.77b) Applying modular law twice:*
  1. *With $a = q$, $b = d$, and $c = p$.*
  2. *With $a = q$, $b = e$, and $c = p$.*
- *(4.77c) By commutativity, associativity, and idempotency.*
- *(4.77d) By definition of p and absorption.*

- *(4.77e) Applying modular law with $a = d \vee (e \wedge f)$, $b = e$, and $c = d \wedge f$. Modular law can be applied because $a = d \vee (e \wedge f) \geq d \geq d \wedge f = c$.*

- *(4.77f) Applying modular law with $a = e$, $b = d$, and $c = e \wedge f$.*

- *(4.77g) By associativity.*

- *(4.77h) By definition of p.*

- *(4.77i) Because $p < q$.* □

4.6.2 Comparing Proof Lengths

It can readily be seen that Proofs 1, 2, 3 respectively have 10, 8, and 9 lines. However, we know that the length of a proof is not an immutable property since it depends on the level of detail given (and hence on presentation). Thus, we decide to study this matter further by coming up with two methods to compare the length of the three proofs. We will call them proof count and proof poset respectively. The first will be naïve while the second will be more rigorous. Both methods are of our own design.

The proof count method is a straightforward brute-force approach. We measure the length of each proof by counting the lines and characters it uses. To be more precise, we count the following:

1. lines,

2. variables,

3. operation symbols,

Proof	lines	variables	operations	grouping	equal	**symbol total**
Proof 1	10	57	46	72	10	**185**
Proof 2	8	47	38	60	8	**153**
Proof 3	9	50	40	60	9	**159**

Table 4.1: Results of Proof Count

4. grouping symbols,
5. equal signs,
6. all symbols.

Table 4.1 shows the results of comparing the three proofs with the proof count method. The main observation we make is that Proofs 2 and 3 use significantly less symbols than Proof 1 (153 and 159 vs. 185).

The second method we use is the proof poset method. In it, we build a poset (specifically a chain) to represent each of the proofs as follows:

1. Top element: $u \wedge v = [(d \wedge q) \vee p] \wedge [(e \wedge q) \vee p]$;
2. Bottom element: p;
3. Each vertex is a statement in proof;
4. Vertex i covers vertex j if we can go from statement i to statement j by applying only one rule from a small list of basic rules (to be given in Definition 4.3);
5. Must add statements to proof if going from i to $i + 1$ requires more than one rule.

The idea is to examine in detail the logical structure of each of the proofs by decomposing them into their building blocks. We admit the following list of basic rules for the covering relation of the proof posets.

Definition 4.3. (*basic rules for proof poset*)

- *Lattice axioms*

    1. *L1: associative laws*
    2. *L2: commutative laws*
    3. *L3: idempotency laws*
    4. *L4: absorption laws*

- *Modular law*

- *Other rules*

    1. *Def: Substitute an element for its definition or vice-versa.*
    2. *Applying Connecting Lemma or some other order property of lattices.*

In order to shorten the posets, we will also allow the following combinations of the modular law with commutativity as a single step (covering relation of poset).

Definition 4.4. (*list of combinations of modular law with commutativity*)

1. *M: Modular law*

$$a \geq c \implies a \wedge (b \vee c) = (a \wedge b) \vee c \tag{4.78}$$

2. *M1: Modular law with inner commute*

$$a \geq c \implies a \wedge (c \vee b) = (a \wedge b) \vee c \tag{4.79}$$

3. *M2: Modular law with outer commute*

$$a \geq c \implies (b \vee c) \wedge a = (a \wedge b) \vee c \tag{4.80}$$

4. *M3: Modular law with reverse inner commute*

$$a \geq c \implies (b \wedge a) \vee c = a \wedge (b \vee c) \tag{4.81}$$

5. *M4: Modular law with reverse outer commute*

$$a \geq c \implies c \vee (a \wedge b) = a \wedge (b \vee c) \tag{4.82}$$

Needless to say, none of the proofs given above is fully decomposed based the lists of Definitions 4.3 and 4.4. Hence, they require adding intermediate statements. We will not work out the full details here but Example 4.13 will illustrate this proof decomposition process for a particular pair of logical steps. The fully decomposed proofs follow the example.

Example 4.13. (*proof decomposition*) *Observe in Proof 3 the transition from step (4.77b) to step (4.77c):*

$$[q \wedge (d \vee p)] \wedge [q \wedge (e \vee p)] \rightarrow q \wedge \{(d \vee p) \wedge (e \vee p)\}. \tag{4.83}$$

Note that it is impossible to justify it by applying only one rule from Definitions 4.3 and 4.4. Thus, we must add the following intermediate steps to Proof 3. The label at the end of each row indicates which basic rule is used to transition from the previous row to it.

$$[q \wedge (d \vee p)] \wedge [q \wedge (e \vee p)] \qquad \textit{start} \tag{4.84}$$

$$[(d \vee p) \wedge q] \wedge [q \wedge (e \vee p)] \qquad L2 \tag{4.85}$$

$$\{[(d \vee p) \wedge q] \wedge q\} \wedge (e \vee p) \qquad L1 \tag{4.86}$$

$$\{(d \vee p) \wedge [q \wedge q]\} \wedge (e \vee p) \qquad L1 \tag{4.87}$$

$$\{(d \vee p) \wedge q\} \wedge (e \vee p) \qquad L3 \tag{4.88}$$

$$\{q \wedge (d \vee p)\} \wedge (e \vee p) \qquad L2 \tag{4.89}$$

$$q \wedge \{(d \vee p) \wedge (e \vee p)\} \qquad L1 \tag{4.90}$$

Decomposed Proof 1.

$$
\begin{aligned}
u \wedge v &= [(d \wedge q) \vee p] \wedge [(e \wedge q) \vee p] && \text{(a1)}\\
&= [((e \wedge q) \vee p) \wedge (d \wedge q)] \vee p && \text{(a2)}\\
&= [(q \wedge (e \vee p)) \wedge (d \wedge q)] \vee p && \text{(a3)}\\
&= [((e \vee p) \wedge q) \wedge (d \wedge q)] \vee p && \text{(a4)}\\
&= [(e \vee p) \wedge (q \wedge (d \wedge q))] \vee p && \text{(a5)}\\
&= [(e \vee p) \wedge (q \wedge (q \wedge d))] \vee p && \text{(a6)}\\
&= [(e \vee p) \wedge ((q \wedge q) \wedge d)] \vee p && \text{(a7)}\\
&= [(e \vee p) \wedge (q \wedge d)] \vee p && \text{(a8)}\\
&= [(e \vee \{(d \wedge e) \vee (e \wedge f) \vee (f \wedge d)\}) \wedge (q \wedge d)] \vee p && \text{(a9)}\\
&= [(e \vee \{(d \wedge e) \vee [(e \wedge f) \vee (f \wedge d)]\}) \wedge (q \wedge d)] \vee p && \text{(a10)}\\
&= [(\{e \vee (d \wedge e)\} \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p && \text{(a11)}\\
&= [(\{e \vee (e \wedge d)\} \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p && \text{(a12)}\\
&= [(e \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p && \text{(a13)}\\
&= [([e \vee (e \wedge f)] \vee (f \wedge d)) \wedge (q \wedge d)] \vee p && \text{(a14)}\\
&= [(e \vee (f \wedge d)) \wedge (q \wedge d)] \vee p && \text{(a15)}\\
&= [(e \vee (f \wedge d)) \wedge (\{(d \vee e) \wedge (e \vee f) \wedge (f \vee d)\} \wedge d)] \vee p && \text{(a16)}
\end{aligned}
$$

$$
\begin{aligned}
u \wedge v &= [(e \vee (f \wedge d)) \wedge (\{[(d \vee e) \wedge (e \vee f)] \wedge (f \vee d)\} \wedge d)] \vee p && \text{(a17)}\\
&= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{(f \vee d) \wedge d\})] \vee p && \text{(a18)}\\
&= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{d \wedge (f \vee d)\})] \vee p && \text{(a19)}\\
&= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{d \wedge (d \vee f)\})] \vee p && \text{(a20)}\\
&= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge d)] \vee p && \text{(a21)}\\
&= [(e \vee (f \wedge d)) \wedge ([(e \vee f) \wedge (d \vee e)] \wedge d)] \vee p && \text{(a22)}\\
&= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge [(d \vee e) \wedge d])] \vee p && \text{(a23)}\\
&= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge [d \wedge (d \vee e)])] \vee p && \text{(a24)}\\
&= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge d)] \vee p && \text{(a25)}\\
&= [(e \vee (f \wedge d)) \wedge (d \wedge (e \vee f))] \vee p && \text{(a26)}\\
&= [(d \wedge (e \vee f)) \wedge (e \vee (f \wedge d))] \vee p && \text{(a27)}\\
&= [d \wedge ((e \vee f) \wedge (e \vee (f \wedge d)))] \vee p && \text{(a28)}\\
&= [d \wedge (((e \vee f) \wedge (f \wedge d)) \vee e)] \vee p && \text{(a29)}\\
&= [d \wedge ((f \wedge d) \vee e)] \vee p && \text{(a30)}\\
&= [(d \wedge e) \vee (f \wedge d)] \vee p && \text{(a31)}\\
&= p \quad \square && \text{(a32)}
\end{aligned}
$$

Decomposed Proof 2.

$$u \wedge v = [(d \wedge q) \vee p] \wedge [(e \wedge q) \vee p] \tag{b1}$$

$$= [((e \wedge q) \vee p) \wedge (d \wedge q)] \vee p \tag{b2}$$

$$= [(q \wedge (e \vee p)) \wedge (d \wedge q)] \vee p \tag{b3}$$

$$= [((e \vee p) \wedge q) \wedge (d \wedge q)] \vee p \tag{b4}$$

$$= [(e \vee p) \wedge (q \wedge (d \wedge q))] \vee p \tag{b5}$$

$$= [(e \vee p) \wedge (q \wedge (q \wedge d))] \vee p \tag{b6}$$

$$= [(e \vee p) \wedge ((q \wedge q) \wedge d)] \vee p \tag{b7}$$

$$= [(e \vee p) \wedge (q \wedge d)] \vee p \tag{b8}$$

$$= [(e \vee \{(d \wedge e) \vee (e \wedge f) \vee (f \wedge d)\}) \wedge (q \wedge d)] \vee p \tag{b9}$$

$$= [(e \vee \{(d \wedge e) \vee [(e \wedge f) \vee (f \wedge d)]\}) \wedge (q \wedge d)] \vee p \tag{b10}$$

$$= [(\{e \vee (d \wedge e)\} \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p \tag{b11}$$

$$= [(\{e \vee (e \wedge d)\} \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p \tag{b12}$$

$$= [(e \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (q \wedge d)] \vee p \tag{b13}$$

$$= [([e \vee (e \wedge f)] \vee (f \wedge d)) \wedge (q \wedge d)] \vee p \tag{b14}$$

$$u \wedge v = [(e \vee (f \wedge d)) \wedge (q \wedge d)] \vee p \tag{b15}$$

$$= [(e \vee (f \wedge d)) \wedge (\{(d \vee e) \wedge (e \vee f) \wedge (f \vee d)\} \wedge d)] \vee p \tag{b16}$$

$$= [(e \vee (f \wedge d)) \wedge (\{[(d \vee e) \wedge (e \vee f)] \wedge (f \vee d)\} \wedge d)] \vee p \tag{b17}$$

$$= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{(f \vee d) \wedge d\})] \vee p \tag{b18}$$

$$= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{d \wedge (f \vee d)\})] \vee p \tag{b19}$$

$$= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge \{d \wedge (d \vee f)\})] \vee p \tag{b20}$$

$$= [(e \vee (f \wedge d)) \wedge ([(d \vee e) \wedge (e \vee f)] \wedge d)] \vee p \tag{b21}$$

$$= [(e \vee (f \wedge d)) \wedge ([(e \vee f) \wedge (d \vee e)] \wedge d)] \vee p \tag{b22}$$

$$= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge [(d \vee e) \wedge d])] \vee p \tag{b23}$$

$$= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge [d \wedge (d \vee e)])] \vee p \tag{b24}$$

$$= [(e \vee (f \wedge d)) \wedge ((e \vee f) \wedge d)] \vee p \tag{b25}$$

$$= [((e \vee f) \wedge d) \wedge (e \vee (f \wedge d))] \vee p \tag{b26}$$

$$= [(e \vee f) \wedge (d \wedge (e \vee (f \wedge d)))] \vee p \tag{b27}$$

$$= [(e \vee f) \wedge ((d \wedge e) \vee (f \wedge d))] \vee p \tag{b28}$$

$$= p \quad \square \tag{b29}$$

Decomposed Proof 3.

$$u \wedge v = [(d \wedge q) \vee p] \wedge [(e \wedge q) \vee p] \tag{c1}$$

$$= [q \wedge (d \vee p)] \wedge [(e \wedge q) \vee p] \tag{c2}$$

$$= [q \wedge (d \vee p)] \wedge [q \wedge (e \vee p)] \tag{c3}$$

$$= [(d \vee p) \wedge q] \wedge [q \wedge (e \vee p)] \tag{c4}$$

$$= \{[(d \vee p) \wedge q] \wedge q\} \wedge (e \vee p) \tag{c5}$$

$$= \{(d \vee p) \wedge [q \wedge q]\} \wedge (e \vee p) \tag{c6}$$

$$= \{(d \vee p) \wedge q\} \wedge (e \vee p) \tag{c7}$$

$$= \{q \wedge (d \vee p)\} \wedge (e \vee p) \tag{c8}$$

$$= q \wedge \{(d \vee p) \wedge (e \vee p)\} \tag{c9}$$

$$= q \wedge \{(d \vee [(d \wedge e) \vee (e \wedge f) \vee (f \wedge d)]) \wedge (e \vee p)\} \tag{c10}$$

$$= q \wedge \{(d \vee [(d \wedge e) \vee [(e \wedge f) \vee (f \wedge d)]]) \wedge (e \vee p)\} \tag{c11}$$

$$= q \wedge \{([d \vee (d \wedge e)] \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (e \vee p)\} \tag{c12}$$

$$= q \wedge \{(d \vee [(e \wedge f) \vee (f \wedge d)]) \wedge (e \vee p)\} \tag{c13}$$

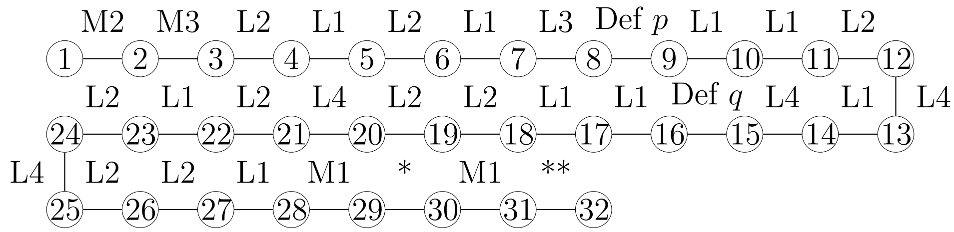
$$= q \wedge \{(d \vee [(f \wedge d) \vee (e \wedge f)]) \wedge (e \vee p)\} \tag{c14}$$

$$= q \wedge \{([d \vee (f \wedge d)] \vee (e \wedge f)) \wedge (e \vee p)\} \tag{c15}$$

$$
\begin{aligned}
u \wedge v &= q \wedge \{([d \vee (d \wedge f)] \vee (e \wedge f)) \wedge (e \vee p)\} && \text{(c16)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge (e \vee p)\} && \text{(c17)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge (e \vee [(d \wedge e) \vee (e \wedge f) \vee (f \wedge d)])\} && \text{(c18)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge (e \vee [(d \wedge e) \vee [(e \wedge f) \vee (f \wedge d)]])\} && \text{(c19)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge ([e \vee (d \wedge e)] \vee [(e \wedge f) \vee (f \wedge d)])\} && \text{(c20)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge ([e \vee (e \wedge d)] \vee [(e \wedge f) \vee (f \wedge d)])\} && \text{(c21)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge (e \vee [(e \wedge f) \vee (f \wedge d)])\} && \text{(c22)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge ([e \vee (e \wedge f)] \vee (f \wedge d))\} && \text{(c23)}\\
&= q \wedge \{[d \vee (e \wedge f)] \wedge [e \vee (f \wedge d)]\} && \text{(c24)}\\
&= q \wedge \{[(d \vee (e \wedge f)) \wedge e] \vee (f \wedge d)\} && \text{(c25)}\\
&= q \wedge \{[(e \wedge d) \vee (e \wedge f)] \vee (f \wedge d)\} && \text{(c26)}\\
&= q \wedge \{[(d \wedge e) \vee (e \wedge f)] \vee (f \wedge d)\} && \text{(c27)}\\
&= q \wedge \{(d \wedge e) \vee (e \wedge f) \vee (f \wedge d)\} && \text{(c28)}\\
&= q \wedge p && \text{(c29)}\\
&= p \quad \square && \text{(c30)}
\end{aligned}
$$

Having the decompositions of Proofs 1-3, we construct their proof posets as indicated above. The result is Figures 4.10-4.12. The label on each indicates the number of the step in the proof it represents (minus the letter). For example, the vertex with label 5 in Figure 4.11 represents equation ($b5$) in the decomposition of Proof 2. Similarly, the labels in the covering edges indicate the basic rule used to go from one expression to the next (see Definitions 4.3 and 4.4 for the meaning of each label). For instance, the label L2 between vertices 3 and 4 in Figure 4.10, indicates that to go from line ($a3$) to line ($a4$) in the decomposition of Proof 1, we must apply rule L2 (commutativity of lattice operations). Finally, we remark that the graphs shown are not Hasse diagrams because the vertical placement of the vertices does not respect the order relation. This was done to save space.

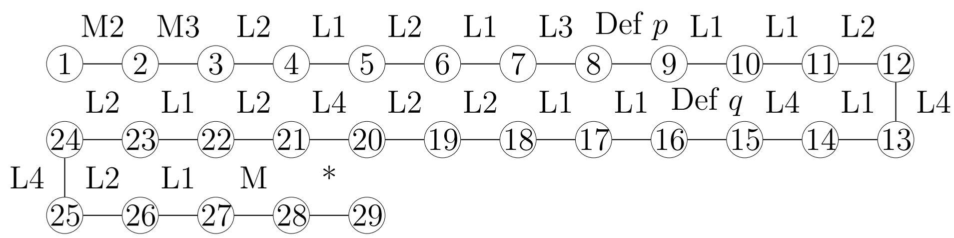
We now discuss the results from the proof poset method. Looking at Figures 4.10-4.12, we can see that the lengths of the decomposed proofs (number of vertices) are as shown in Table 4.2. Hence, based on our notion of "basic rule" in Definitions 4.3 and 4.4, Proofs 2 and 3 are only slightly shorter than Proof 1. In addition, we use the poset graphs to count how many times each proof uses each basic rule. The results are in Table 4.3. The main observation that we make from it is that Proof 2 uses the modular law one time less than the other proofs (3 vs. 4). Noting that the modular law is slightly less basic than the axioms, this could be interpreted as saying the Proof 2 is somehow logically simpler than the other two. We also remark that our decomposition could be improved by breaking the combined modular law rules (M1-M4), which could yield different results. However, this is beyond the scope of the current discussion.



* because $e \vee f \geq f \geq f \wedge d$

** since $(d \wedge e) \vee (f \wedge d) \leq p$

Figure 4.10: Chain graph of Proof 1



* since $[(e \vee f) \wedge ((d \wedge e) \vee (f \wedge d))] \leq p$

Figure 4.11: Chain graph of Proof 2

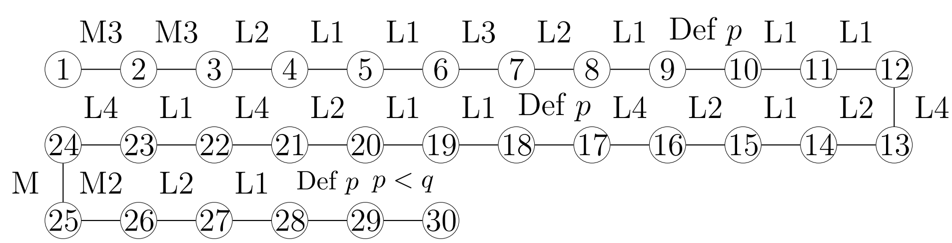


Figure 4.12: Chain graph of Proof 3

Proof 1	32
Proof 2	29
Proof 3	30

Table 4.2: Length of proof posets

Proof	L1	L2	L3	L4	M	M1	M2	M3	M4	Def	Other
1	9	9	1	4	0	2	1	1	0	2	2
2	9	8	1	4	1	0	1	1	0	2	1
3	10	6	1	4	1	0	1	2	0	3	1

Table 4.3: Count of basic rules invoked by Proofs 1-3

Therefore, we conclude the following from our proof comparison exercise:

1. Proof Count Method: Proofs 2 and 3 are shorter than Proof 1.

2. Proof Poset Method: Proofs 2 and 3 are slightly shorter than Proof 1.

3. Proof 2 is the shortest proof either way.

4.6.3 Extras with Proof Poset

We conclude this section by briefly exploring two additional potential applications of the proof posets we created for Proofs 1-3. The first of these is to try to see if a vertex in one of the three chains covers a vertex in one of the other two. This would lead to a new path from top to bottom and hence to a new proof of $u \wedge v = p$. We naturally ignore trivial coverings resulting from the fact that Proofs 1 and 2 share the first 25 vertices. Unfortunately, this search does not yield any new proofs. The main issue is that Proof 3 has an external $\wedge q$ while Proofs 1 and 2 have an external $\vee p$ throughout most of the steps. This makes it impossible to go between their vertices with only one basic rule.

The second idea we pursue is to form and study a combined poset from the three proof chains. We connect the chains by equaling the common vertices (steps of proof): all three share a common top and bottom while Proofs 1 and 2 share 25 vertices. The Hasse diagram of the resulting poset is shown in Figure 4.13. The vertices are labelled with a letter and a number. The letter tells the proof it corresponds to as indicated below:

1. a = proof 1,
2. b = proof 2,
3. c = proof 3.

The number references the specific proof statement (same numbers used in Figures 4.10-4.12).For example, vertex $c5$ represents statement 5 of Proof 3. Vertices labelled with ab corresponds to shared statements of Proofs 1 and 2. Note that

$$1 = a1 = b1 = c1 \quad \text{and} \quad end = a32 = b29 = c30. \tag{4.91}$$

The edges are not labelled. It can be seen from the diagram that this poset is a lattice. It can also be observed that it is a non-modular (and hence, non distributive) because it has a copy of $\mathbf{N}_5$: $\{ab25, a26, a27, b26, end\}$.

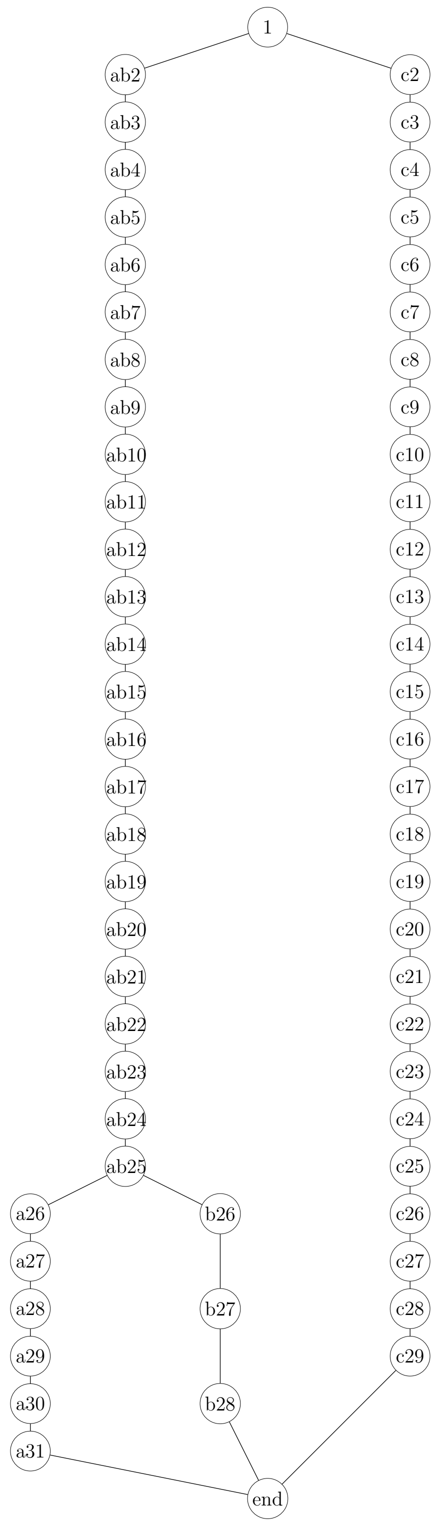


Figure 4.13: Combined poset

Chapter 5

Characterization of Finite Distributive Lattices

5.1 Introduction

In this chapter, we discuss a method to represent each finite distributive lattice: Birkhoff's Representation Theorem for Finite Distributive Lattices. This theorem also yields a way to identify non-distributive finite lattices and a 1-1 correspondence between finite distributive lattices and finite posets. This discussion will use material on join-irreducibles and down-sets that was given in Sections 3.7 and 2.5 respectively.

The rest of this chapter is organized as follows: Section 5.2 presents Birkhoff's Representation Theorem for Finite Distributive Lattices. Afterwards, Section 5.3 discusses how to identify non-distributive lattices using a corollary of the representation theorem. Finally, Section 5.4 concludes by establishing a 1-1 correspondence between finite distributive lattices and finite posets.

5.2 Birkhoff's Representation Theorem

This section presents Birkhoff's Representation Theorem for Finite Distributive Lattices. This theorem characterizes all finite distributive lattices based on special subsets of them. It says that a finite distributive lattice is uniquely determined by its set of join-irreducible elements. In particular, it is the down-set lattice of its set of join-irreducible elements. Recall that a join-irreducible element of a lattice is a non-zero element that cannot be expressed as the join of two elements different from itself. Remember also that the down-set lattice of a poset is the set of all of its down-sets (subsets closed under going down) with the usual set operations. We provide the actual theorem statement preceded by a lemma needed to prove it and followed by an example illustrating the isomorphism it establishes. We omit the proof of the lemma since it is straightforward.

Lemma 5.1. *(join-irreducible $\leq$ finite join condition) Let L be a distributive lattice with $x \in L$ distinct from 0 (if L has zero). Then the following are equivalent:*

1. *x is join-irreducible.*

2. *Given $a, b \in L$, $x \leq a \vee b \implies x \leq a$ or $x \leq b$.*

3. *Given $k \in \mathbb{N}$ and $a_1, ..., a_k \in L$,*

$$x \leq a_1 \vee \cdots \vee a_k \implies x \leq a_i \text{ for some } i \text{ with } 1 \leq i \leq k. \tag{5.1}$$

Theorem 5.1. (*Birkhoff's Representation Theorem for Finite Distributive Lattices*) *Let L be a finite distributive lattice. Then $L \cong O(J(L))$. An isomorphism map is $\eta : L \to O(J(L))$ defined by*

$$\eta(a) = J(L) \cap {\downarrow}a. \tag{5.2}$$

Proof *We must show that η is a bijective lattice homomorphism. To show that it is join-preserving we apply the Connecting Lemma, the distributive property and the definition of join-irreducible element to observe that:*

$$\begin{aligned}
\eta(a \vee b) &= J(L) \cap {\downarrow}(a \vee b) &(5.3)\\
&= \{x \in J(L) \mid x \leq a \vee b\} &(5.4)\\
&= \{x \in J(L) \mid x \wedge (a \vee b) = x\} &(5.5)\\
&= \{x \in J(L) \mid (x \wedge a) \vee (x \wedge b) = x\} &(5.6)\\
&= \{x \in J(L) \mid x \wedge a = x \ \textit{or} \ x \wedge b = x\} &(5.7)\\
&= \{x \in J(L) \mid x \leq a \ \textit{or} \ x \leq b\} &(5.8)\\
&= J(L) \cap ({\downarrow}a \cup {\downarrow}b) &(5.9)\\
&= (J(L) \cap {\downarrow}a) \cup (J(L) \cap {\downarrow}b) &(5.10)\\
&= \eta(a) \cup \eta(b). &(5.11)
\end{aligned}$$

Showing tha η is meet-preserving can also be done similarly. Injectivity follows from Proposition 3.7 ($a = \bigvee \eta(a)$); surjectivity from showing that for any $D \in O(J(L))$,$D = J(L) \cap {\downarrow} a$ for $a = \bigvee D$ using Lemma 5.1. This completes the proof. □

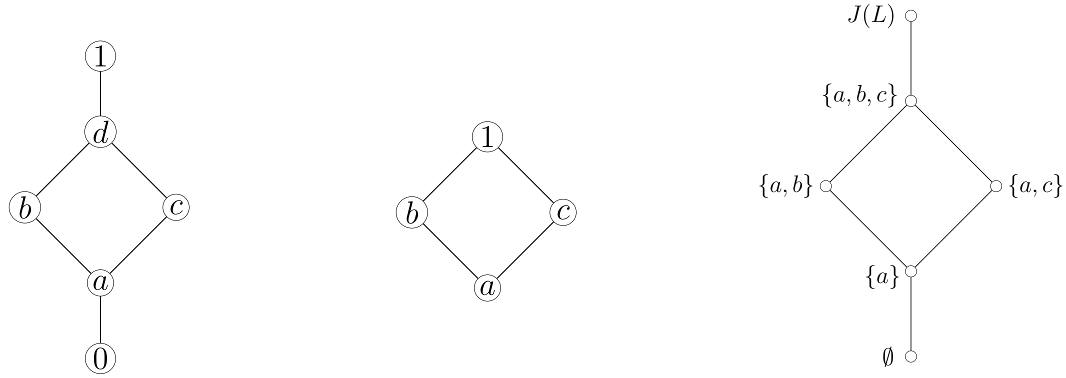


Figure 5.1: A lattice L (left), its $J(L)$ (center) and $O(J(L))$ (right)

Example 5.1. (*illsutrating* $L \cong O(J(L))$) *Figure 5.1 shows a lattice* L *along with its corresponding* $J(L)$ *and* $O(J(L))$*. Note that* L *and* $O(J(L))$ *are isomorphic as expected from Theorem 5.1.*

5.3 Identifying Non-Distributive Lattices

Now, we derive a method of determining the distributivity of a finite lattice from Birkhoff's theorem. The idea is that a down-set lattice is distributive because it is a lattice of sets. Hence, for any lattice L, $O(J(L))$ is distributive. As a result a non-distributive lattice cannot satisfy the result of Birkhoff's theorem. We get the following corollary.

Corollary 5.1. (*characterization of finite distributive lattices*) *Let* L *be a finite lattice. Then* L *is distributive if and only if* $L \cong O(J(L))$.

This corollary provides an alternative to the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem for identifying non-distributive lattices. Given a lattice L, we compute $O(J(L))$. If they are not isomorphic, then L is not distributive. We verify that this works for $\mathbf{M}_3$ and $\mathbf{N}_5$ and then

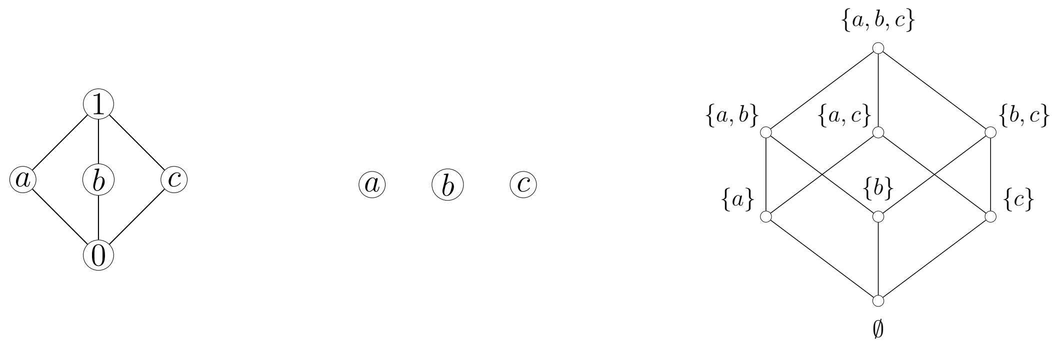


Figure 5.2: $\mathbf{M}_3$ (left), $J(\mathbf{M}_3)$ (center), and $O(J(\mathbf{M}_3))$ (right)

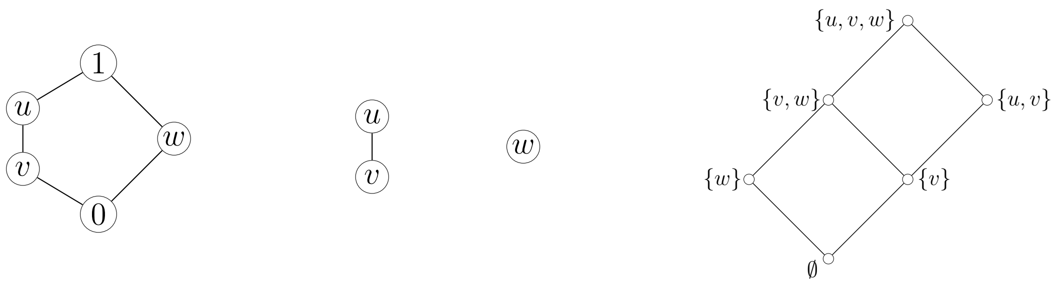


Figure 5.3: $\mathbf{N}_5$ (left), $J(\mathbf{N}_5)$ (center), and $O(J(\mathbf{N}_5))$ (right)

apply this method to a less trivial example.

Example 5.2. ($\mathbf{M}_3$ *and* $\mathbf{N}_5$)

1. *Figure 5.2 shows* $\mathbf{M}_3$, $J(\mathbf{M}_3)$ *and* $O(J(\mathbf{M}_3))$. *Clearly,* $\mathbf{M}_3 \ncong O(J(\mathbf{M}_3))$.

2. *Figure 5.3 shows* $\mathbf{N}_5$, $J(\mathbf{N}_5)$ *and* $O(J(\mathbf{N}_5))$. *Clearly,* $\mathbf{N}_5 \ncong O(J(\mathbf{N}_5))$.

Example 5.3. (*applying corollary*) *Consider the lattice K shown in Figure 5.4* (*left*). *$J(K)$ and $O(J(K))$ are shown next to it. Observe that $|O(J(K))| = 10$ while $|K| = 7$. Hence, these lattices are not isomorphic. Corollary 5.1 then implies that K is not distributive. This is consistent with the* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem since $\{b, c, d, e, 1\}$ is a sublattice of K isomorphic to* $\mathbf{N}_5$.

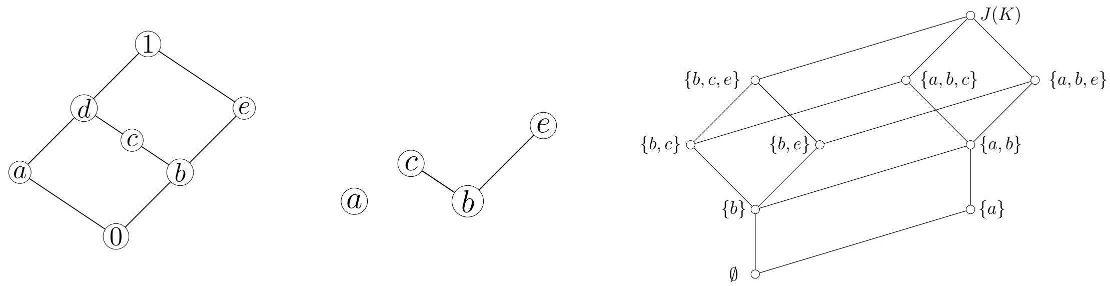


Figure 5.4: A lattice K (left), its $J(K)$ (center) and $O(J(K))$ (right)

5.4 Going Further: 1-1 Correspondence

The result of Birkhoff's theorem can be expanded further. Calculating $J(L)$ can be seen as a function whose input is a lattice and whose output is a poset (not necessarily a lattice). If we restrict L to be finite and distributive, then J becomes a function from the set of finite distributive lattices to the set of finite posets. We will show that J is 1-1 and onto. This provides a 1-1 correspondence between finite distributive lattices and finite posets (up to isomorphism).

To prove that J is 1-1 we will need some new notation and a representation theorem for finite posets analogous to Birkhoff's theorem. We begin with the representation theorem. The result is that every finite poset is isomorphic to the set of join-irreducibles of its down-set lattice. An important idea behind the isomorphism is that the join-irreducible down-sets of a poset are its principal down-sets. We now state the theorem and then provide an example illustrating it.

Theorem 5.2. (*representation of finite posets*) *Let P be a finite poset. Then $P \cong J(O(P))$. An order-isomorphism is $\epsilon : P \to J(O(P))$ defined by*

$$\epsilon(x) = {\downarrow} x. \tag{5.12}$$

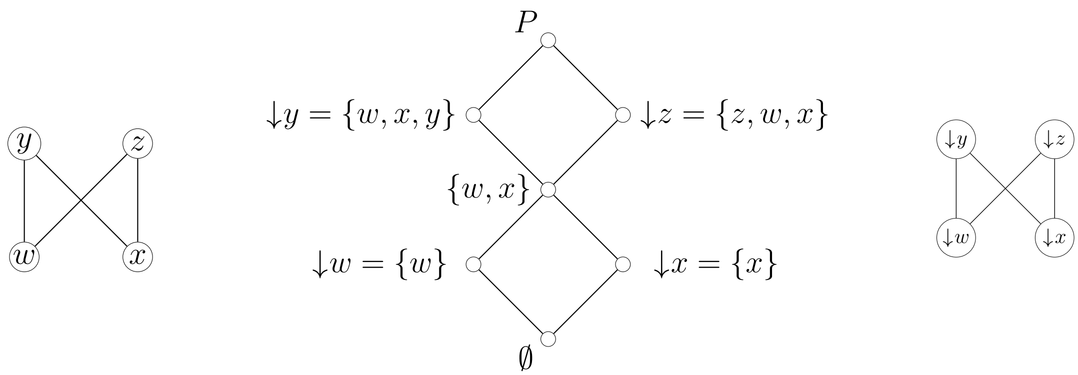


Figure 5.5: A poset P (left), its $O(P)$ (center) and $J(O(P))$ (right)

Proof Sketch *To show that ϵ is and order-embedding it suffices to show that $x \leq y$ if and only if ${\downarrow}x \subseteq {\downarrow}y$ for any $x, y \in P$. It then remains to show that ϵ is onto. For this, it can be shown that $J(O(P)) = \{{\downarrow}x \mid x \in P\}$. It then follows that the image of ϵ is $J(O(P))$.* $\square$

Example 5.4. (*illsutrating $P \cong J(O(P))$*) *Figure 5.5 shows a poset P along its $O(P)$ and $J(O(P))$. Note that P and $J(O(P))$ are isomorphic as expected from Theorem 5.2.*

Now, we define notation that will simplify stating the 1-1 correspondence theorem. Let $\mathbf{D}_F$ denote the class of all finite distributive lattices and $\mathbf{P}_F$ the class of all finite posets. Then J is a map from $\mathbf{D}_F$ to $\mathbf{P}_F$ with inverse O. Here is the 1-1 correspondence theorem. Note that its proof uses both Theorems 5.1 and 5.2.

Theorem 5.3. (*1-1 correspondence*) *There is a 1-1 correspondence between $\mathbf{D}_F$ and $\mathbf{P}_F$. In particular, the maps $J : \mathbf{D}_F \to \mathbf{P}_F$ and $O : \mathbf{P}_F \to \mathbf{D}_F$ defined by $J(L)$ and $O(P)$ are bijections.*

Proof *We show that J is bijective. The proof for O is similar.*

1-1: Suppose that $J(L) \cong J(K)$ for $J, K \in \mathbf{D}_F$. Then $O(J(L)) \cong O(J(K))$. By Birkhoff, $L \cong K$.

Onto: Let $P \in \mathbf{P}_F$ (a finite poset). Then $L = O(P)$ is in $\mathbf{D}_F$. By Theorem 5.2, $P \cong J(O(P)) = J(L)$. Thus, there exists $L \in \mathbf{D}_F$ such that $P \cong J(L)$. □

Theorem 5.3 permits translation of lattice problems into poset problems and vice-versa. The lattice-to-poset direction is the most advantegeous as $J(L)$ is much smaller than L (while $O(P)$ is much larger than P). In this sense, J and O are analogous to the logarithm and exponential functions (as mentioned in [5]). This analogy is strengthened further if we consider the disjoint union of two posets like a sum of posets. Then like $\log(x)$ and $\exp(x)$, J takes products to sums and O sums to products in the sense that:

$$J(L \times K) \cong J(L) \cup J(K); \tag{5.13}$$

$$O(P \cup Q) \cong O(P) \times O(Q). \tag{5.14}$$

Equation (5.14) might seem familiar: it is Theorem 2.3. Equation (5.13) follows from it and Theorem 5.1 given that L and K are finite and distributive. Furthermore, the domain of J is the range of O, both a proper subset of the range of J and domain of O. In this sense, $\mathbf{P}_F$ is to $\mathbb{R}$ as $\mathbf{D}_F$ is to $\mathbb{R}_{>0}$. We conclude with an example showcasing the size difference between a finite poset and its corresponding finite distributive lattice (its down-set lattice).

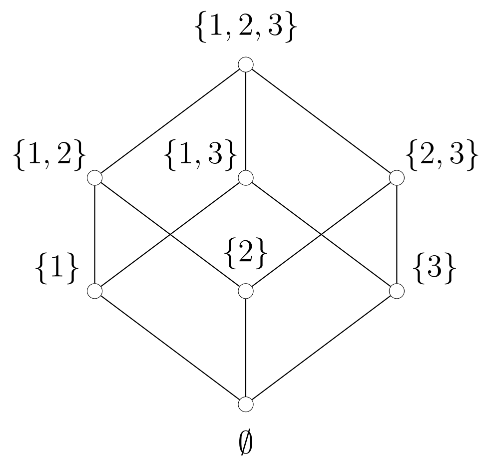


Figure 5.6: The power set $\wp(\{1,2,3\})$ mentioned in Example 5.5

Example 5.5. (*Dedekind numbers [18]*) *The n-th Dedekind number indicates the size of the down-set lattice of the power set of an n-element set (i.e. $|O(\wp(X))|$ for $|X| = n$). The first 5 Dedekind numbers are 3, 6, 20, 168, and 7581 while the 6th is greater than 7 million. These are larger than the sizes of the corresponding power sets: 2, 4, 8, 16, 32, and 64. Only the first 8 have been calculated. Figures 5.6 and 5.7 show that the third Dedekind number is 20.*

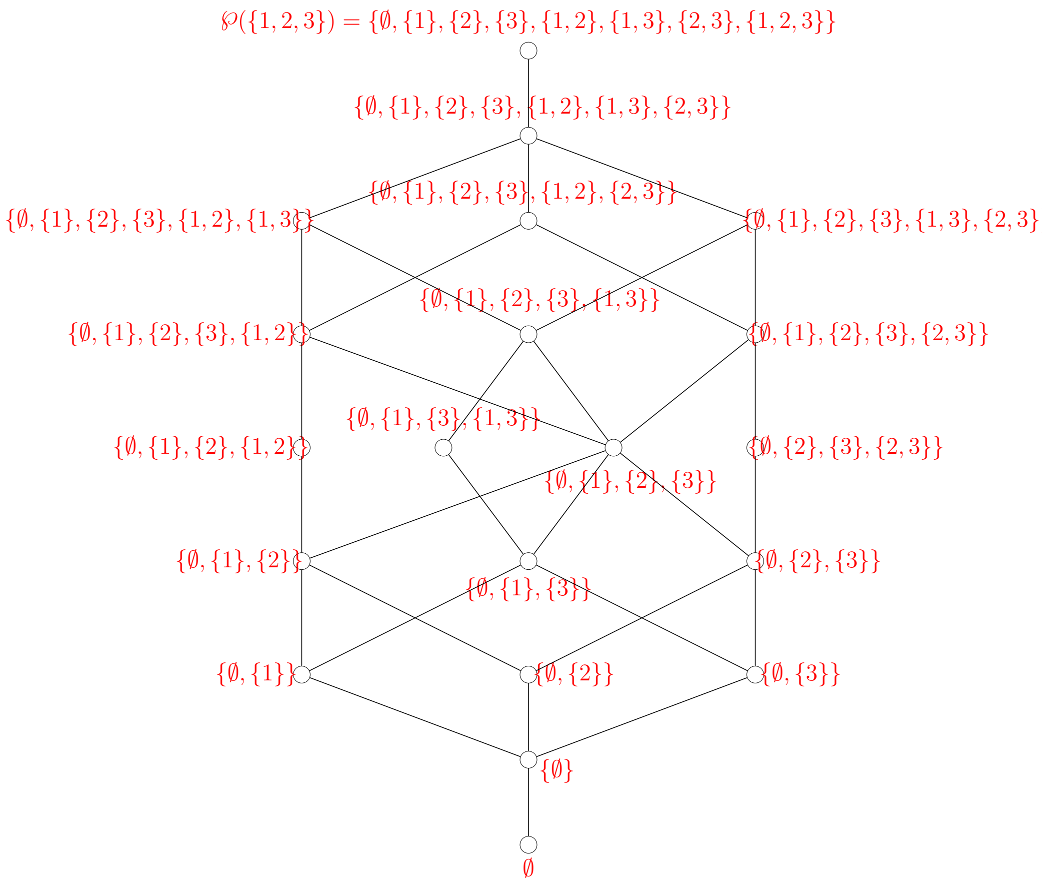


Figure 5.7: The down-set lattice $O(\wp(\{1,2,3\}))$ mentioned in Example 5.5

Chapter 6

Congruences in Lattices

6.1 Introduction

Congruences on algebraic systems are equivalence relations that are well-behaved with respect to the operations of said algebraic systems. In the case of lattices, this translates into interacting adequately with the join and meet operations. This chapter will introduce to the reader the theory of lattice congruences. Some results and definitions will be familiar to those with experience in group and ring theory: kernels, quotients, and ideals.

This journey starts with the precise definition of a congruence on a lattice in Section 6.2. We then encounter quotient lattices in Section 6.3. Afterwards, Section 6.4 gives a characterization of equivalence relations on lattices that are congruences. We move on to a broader view on congruences in Section 6.5 when we explore the lattice of congruences of a lattice. Finally, we discover a method for characterizing distributive lattices using congruences in Section 6.6.

6.2 Basic Definitions

In this section, we introduce the key idea of this chapter: congruences on a lattice. We define this concept and then present several examples including the kernel of a lattice homomorphism. We begin by reviewing what is an equivalence relation and a block (also called equivalence class).

Definition 6.1. (*equivalence relation*) *An equivalence relation on a set S is a relation θ on S that is reflexive, symmetric, and transitive. If a and b are related by θ we write either $(a, b) \in \theta$, $a\,\theta\,b$, $a \equiv b \pmod{\theta}$, or $a \equiv_\theta b$.*

Definition 6.2. (*block*) *Given an equivalence relation θ on a set S and an element x of S, the block (or equivalence class) of x under θ, denoted by $[x]_\theta$, is the subset of S of all elements related to x under θ. This is,*

$$[x]_\theta = \{a \in S \mid a \equiv x \pmod{\theta}\}. \tag{6.1}$$

Recall that the blocks of two elements under an equivalence relation are either equal or disjoint. Hence, the blocks of an equivalence relation form a partition of the set on which it is defined.

Of particular interest to us is when the underlying set of an equivalence relation is a lattice. A natural question to ask is how the relation interacts with the lattice operations. An equivalence relation is said to be compatible with a lattice operation if its blocks are preserved by the operation. By this we mean that the block of the result is unchanged if an operand is swapped for another element of the same block.

Definition 6.3. (*compatibility with join and meet*) *An equivalence relation θ on a lattice L is compatible with the join operation of L if*

$$a \equiv b \pmod{\theta} \text{ and } c \equiv d \pmod{\theta} \implies a \vee c \equiv b \vee d \pmod{\theta}, \tag{6.2}$$

and is compatible with the meet operation of L if

$$a \equiv b \pmod{\theta} \text{ and } c \equiv d \pmod{\theta} \implies a \wedge c \equiv b \wedge d \pmod{\theta}. \tag{6.3}$$

We now are ready to define a congruence. We follow the definitions with some examples. We leave the checking of compatibility in the examples to the reader.

Definition 6.4. (*congruence*) *A congruence on a lattice L is an equivalence relation on L that is compatible with both the join and meet operations of L.*

Example 6.1. (*trivial congruences*) *Any lattice L has the following two congruences:*

1. *The equality relation $(=)$: $a \equiv b \pmod{=} \iff a = b$;*

2. *The single block relation: $a \equiv b \pmod{\theta}\ \forall a, b \in L$.*

The equality congruence and the single block congruence are sometimes denoted **0** *and* **1** *respectively. The reason for this will be seen in Section 6.5.*

Example 6.2. (*chain partition*) *Any partition of a chain into consecutive sub-chains is a congruence on the chain. For instance, the partition of* **12** *given by $\{1, 2, 3, 4, 5, 6\}$ and $\{7, 8, 9, 10, 11, 12\}$ is a congruence. We call it the school partition because it splits*

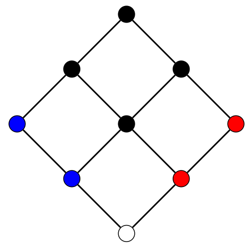


Figure 6.1: A congruence on $\mathbf{3}\times\mathbf{3}$ indicated by colors

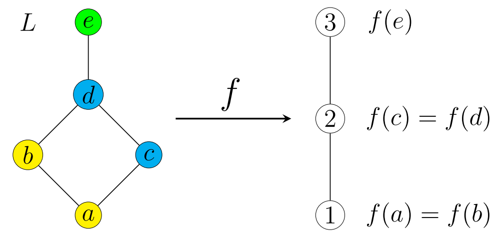


Figure 6.2: A lattice homomorphism f with $\ker f$ indicated by colors

the numbers $1-12$ *based on whether their corresponding grade belongs to elementary or secondary school.*

Example 6.3. (*congruence on grid*) *Figure 6.1 shows a congruence on the lattice* $\mathbf{3}\times\mathbf{3}$*. Each color corresponds to a block. Hence, we have four blocks given respectively by the black, red, blue, and white nodes.*

We now turn our attention to a congruence that can be defined on the domain of a lattice homomorphism, the kernel. The idea is to partition the domain based on the images of its elements. We now formalize this and provide a concrete example.

Definition 6.5. (*kernel of lattice homomorphism*) *Given a lattice homomorphism* $f : L \to K$*, the kernel of* f*, denoted* $\ker f$*, is the relation* θ *defined on* L *by:*

$$a \equiv b \pmod{\theta} \iff f(a) = f(b). \tag{6.4}$$

Proposition 6.1. (*kernel is congruence*) *If* $f : L \to K$ *is a lattice homomorphism, then* $\ker f$ *is a congruence on* L*.*

Proof Sketch *Let* $\theta = \ker f$*. It is straightforward to show that* θ *is an equivalence relation. To show that it is compatible with meet and join, just apply preservation of operations by* f *and the definition of the relation* θ*. The details are omitted.* □

Example 6.4. (*kernel*) *Figure 6.2 shows a lattice homomorphism with the blocks of its kernel indicated by colors:* $f^{-1}(1)$ *is yellow,* $f^{-1}(2)$ *is cyan (sky blue), and* $f^{-1}(3)$ *is green.*

We close this section with a result about kernels that is a lattice-analog of a known result about group homomorphisms. It characterizes 1-1 lattice homomorphisms as those whose kernel is the equality relation $\mathbf{0}$.

Proposition 6.2. (*embeddings and trivial kernels*) *A lattice homomorphism f is an embedding if and only if* $\ker f = \mathbf{0}$.

Proof *Let $f : L \to K$ be a lattice homomorphism with kernel θ.*

$\Longrightarrow$ *: Suppose $f : L \to K$ is an embedding and let $a, b \in L$ Then f is 1-1 and we have that $f(a) = f(b)$ implies $a = b$. Since $a = b$ always implies $f(a) = f(b)$, we get*

$$a = b \iff f(a) = f(b) \iff a \equiv b \pmod{\theta}. \tag{6.5}$$

Then $\theta = \ker f = \{(x, x) \mid x \in L\} = \mathbf{0}$.

$\Longleftarrow$ *: Suppose* $\ker f = \mathbf{0}$. *It suffices to show that it is 1-1. Let $a, b \in L$ be such that $f(a) = f(b)$. Then $a \equiv b \pmod{\theta}$ and $a = b$ by assumption. Hence, f is an embedding.* $\square$

6.3 Quotient Lattice

Having defined congruences on lattices, we proceed to form a lattice out of the blocks of a congruence. The result is called a quotient lattice. This is analogous to quotient groups in abstract algebra. In this section, we define what is a quotient lattice, provide some examples, relate the order of a quotient lattice with that of its base lattice, and establish the Homomorphism Theorem for Lattices.

A quotient lattice is a lattice on the blocks of a congruence. The idea is to define block operations by making the join (meet) of two blocks the block of the join (meet) of their elements. This operations will be well-defined because the equivalence relation in question is a congruence. We now formalize this and give some examples building on the examples of congruences of Section 6.2.

Definition 6.6. (*quotient lattice*) *Let L be a lattice with a congruence θ. The quotient lattice of L modulo θ, denoted L/θ, is the set of blocks of θ with block operations*

$$[a]_\theta \vee [b]_\theta = [a \vee b]_\theta, \tag{6.6}$$

$$[a]_\theta \wedge [b]_\theta = [a \wedge b]_\theta, \tag{6.7}$$

for any $a, b \in L$.

Proposition 6.3. (L/θ *is lattice*) *If L is a lattice with a congruence θ, then the quotient L/θ is a lattice.*

Proof *We show that the block operations are well-defined: that their results are independent of the member chosen from each block. We do only the proof for join. That*

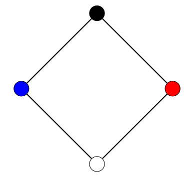


Figure 6.3: The quotient lattice $\mathbf{3} \times \mathbf{3}/\theta$ for the congruence θ of Figure 6.1

of meet is identical. Suppose that $[a_1]_\theta = [a_2]_\theta$ *and* $[b_1]_\theta = [b_2]_\theta$. *Then*

$$[a_1]_\theta \vee [b_1]_\theta = [a_1 \vee b_1]_\theta = [a_2 \vee b_2]_\theta = [a_2]_\theta \vee [b_2]_\theta, \tag{6.8}$$

where the middle equality follows from the fact that θ *is a congruence.* □

Example 6.5. (*quotient lattice of trivial congruences*)

1. *For any lattice* L, *the quotient lattice of* L *modulo* $=$, $L/=$, *is* L *itself.*

2. *For the single block relation* θ *of Example 6.1,* $L/\theta \cong \mathbf{1}$ *since* θ *collapses* L *to one single block.*

Example 6.6. (*quotient lattice of chain partition*) *If* θ *is the partition of the chain* $\mathbf{n}$ *into* m *subintervals, then* $\mathbf{n}/\theta \cong \mathbf{m}$. *If we consider for instance the school partition of* $\mathbf{12}$ *given in Example 6.2, then* $\mathbf{12}/\theta \cong \mathbf{2}$.

Example 6.7. (*quotient lattice of congruence on grid*) *Figure 6.3 shows the quotient lattice of* $\mathbf{3} \times \mathbf{3}$ *modulo* θ *for the congruence* θ *of Figure 6.1. Note that* $\mathbf{3} \times \mathbf{3}/\theta \cong \mathbf{M}_2$. *The block corresponding to each element of the quotient lattice class is identified by its color.*

We now present a result that helps draw the Hasse diagram of a quotient lattice. It establishes a connection between the order relation and lattice operations of the base lattice with those of the quotient lattice. It characterizes the order and covering relation in terms of the order relation of the base lattice. In addition, it tells us that the join (meet) of two elements is contained in the block join (meet) of their corresponding classes. The formal statement is now given followed by a concrete example of the result.

Proposition 6.4. (*relation between orders of L and L/θ*) *Let L be a lattice with congruence θ. Suppose that X and Y are blocks of θ. Then the following hold.*

1. *$X \leq Y$ in L/θ if and only if there exists $a \in X$ and $b \in Y$ such that $a \leq b$ in L.*

2. *$X \prec Y$ in L/θ if and only if $X < Y$ in L/θ and $a \leq c \leq b$ in L implies $c \in X$ or $c \in Y$ for all $a \in X$, $b \in Y$, and $c \in L$.*

3. *If $a \in X$ and $b \in Y$, then $a \vee b \in X \vee Y$ and $a \wedge b \in X \wedge Y$.*

Proof *We prove each part.*

Part 1: $\Longrightarrow$: *Suppose $X \leq Y \in L/\theta$. Let $a \in X$ and $b \in Y$. Then*

$$X = [a]_\theta \text{ and } Y = [b]_\theta \implies [a]_\theta \leq [b]_\theta \tag{6.9}$$

$$\implies [a]_\theta \wedge [b]_\theta = [a]_\theta \tag{6.10}$$

$$\implies [a \wedge b]_\theta = [a]_\theta \tag{6.11}$$

$$\implies a \wedge b \in [a]_\theta = X. \tag{6.12}$$

Note that $a \wedge b \leq b$. Therefore, $a \wedge b \in X$ and $b \in Y$ satisfy the desired condition.

$\Longleftarrow$: *Suppose there exist $a \in X$ and $b \in Y$ such that $a \leq b$. Then $X = [a]_\theta$,*

$Y = [b]_\theta$, *and we get*

$$X \wedge Y = [a]_\theta \wedge [b]_\theta \tag{6.13}$$

$$= [a \wedge b]_\theta \tag{6.14}$$

$$= [a]_\theta \tag{6.15}$$

$$= X. \tag{6.16}$$

Therefore, $X \leq Y$ *by the Connecting Lemma.*

Part 2: $\implies$ *: Suppose* $X \prec Y$*. Then* $X < Y$ *by definition of the covering relation* $\prec$*. For the other required condition, consider* $a \in X$*,* $b \in Y$*, and* $c \in L$ *with* $a \leq c \leq b$*. By Part 1,* $X \leq [c]_\theta \leq Y$*. This implies that* $X = [c]_\theta$ *or* $Y = [c]_\theta$ *because* X *is covered by* Y *by supposition. Therefore,* $c \in X$ *or* $c \in Y$ *as desired.*

$\impliedby$ *: Suppose that* $X, Y \in L/\theta$ *are blocks such that* $X < Y$ *and*

$$a \leq c \leq b \implies c \in X \text{ or } c \in Y \tag{6.17}$$

for any $a \in X, b \in Y$*, and* $c \in L$*. To show that* $X \prec Y$ *it suffices to show that for any* $Z \in L/\theta$*,*

$$X \leq Z < Y \implies X = Z. \tag{6.18}$$

Consider a block $Z \in L/\theta$ *satisfying the hypothesis of Equation (6.18). Let* $a \in X$*,* $b \in Y$*, and* $c \in Z$*. Then* $[a]_\theta \leq [c]_\theta \leq [b]_\theta$ *by supposition on* Z*. This implies that* $a \wedge c \in [a]_\theta = X$ *and* $c \vee b \in [b]_\theta = Y$*. Now, since* $a \wedge c \leq c \leq c \vee b$*, Equation (6.17)* *implies that* $c \in X$ *or* $c \in Y$*. This results in* $X = Z$ *or* $Y = Z$*, which translates to* $X = Z$ *because* $Z < Y$*. Therefore,* $X \prec Y$*.*

Part 3: Suppose that $a \in X$ *and* $b \in Y$*. Note that*

$$X \vee Y = [a]_\theta \vee [b]_\theta \tag{6.19}$$

$$= [a \vee b]_\theta. \tag{6.20}$$

Therefore, $a \vee b \in X \vee Y$*. The proof of* $a \wedge b \in X \wedge Y$ *is identical.* □

Example 6.8. (*illustrating relation between orders of* L *and* L/θ) *Consider the lattice* L *shown in Figure 6.4 (left). The colors of its nodes indicate a congruence* θ *on* L*. The resulting quotient lattice is also shown in Figure 6.4 (right). Observe that* $L/\theta \cong \mathbf{M}_3$*. We illustrate the results of Proposition 6.4 on it.*

1. *Note that* $[b]_\theta \leq [a]_\theta \in L/\theta$ *while* $b \leq a$*.*

2. *Note that* $[e]_\theta \prec [c]_\theta$ *since there are no elements of other blocks between elements of* $[e]_\theta$ *and of* $[c]_\theta$*. In contrast,* $[e]_\theta$ *is not covered by* $[a]_\theta$ *because although* $[e]_\theta < [a]_\theta$ *in* L/θ*, we have* $e \leq d \leq a$ *and* d *is in neither* $[e]_\theta$ *nor* $[a]_\theta$*.*

3. *Note that* $d \vee f = g$ *and* $g \in [a]_\theta = [d \vee f]_\theta = [d]_\theta \vee [f]_\theta$ *where* $[f]_\theta = [c]_\theta$*.*

We now present a definition and a theorem that are a direct importation from group theory: quotient maps and the Homomorphism Theorem. The quotient map is a function from a lattice to a quotient lattice (induced by a congruence on it) that maps each element to its block. The Homomorphism Theorem for Lattices says

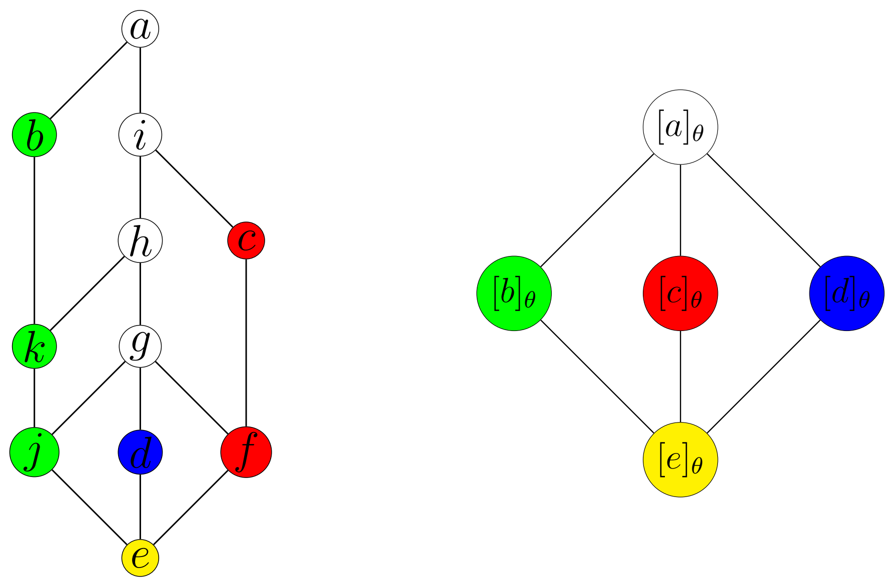


Figure 6.4: A lattice L with a congruence θ indicated with colors (left) and the resulting quotient lattice L/θ (right)

that the quotient lattice of the kernel of an onto homomorphism is isomorphic to the codomain of said homomorphism.

Definition 6.7. (*quotient map*) *Given a lattice L with a congruence θ, the quotient map of L/θ is the function $q : L \to L/\theta$ defined by $q(a) = [a]_\theta$ for all $a \in L$. It is a lattice homomorphism.*

Theorem 6.1. (*Homomorphism Theorem for Lattices*) *Let $f : L \to K$ be an onto lattice homomorphism with kernel θ. Then*

$$L/\theta \cong K. \tag{6.21}$$

Proof Sketch *Consider the map $g : L/\theta \to K$ given by $g([a]_\theta) = f(a)$. It suffices to show that g is well-defined and that it is an isomorphism. The details are elementary and are thus omitted. As an aside, it can also be shown that if $q : L \to L/\theta$ is the* *quotient map of L/θ, then* $\ker q = \theta$ *and* $f = g \circ q$. $\square$

Example 6.9. (*Homomorphism Theorem for Lattices*) *Recall the lattice homomorphism f of Figure 6.2. Note that f is onto and let $\theta = \ker f$. It can be readily seen that L/θ, consisting of $f^{-1}(1) \leq f^{-1}(2) \leq f^{-1}(3)$, is isomorphic to* $\mathbf{3}$, *the codomain of f.*

We conclude this section by explaining why the onto condition is required in Theorem 6.1. If the function f is not onto, then some pre-images of elements of K will be empty. Hence, since L/θ has exactly one element for each potential image of an element of L, it will be smaller than K and thus not isomorphic to it.

6.4 Characterizing Congruences

We now turn to the following question: When is an equivalence relation a congruence? In order to answer it, we discuss convex subsets in posets and quadrilateral-closed partitions of lattices. We then give a theorem that characterizes equivalence relations on lattices that are congruences.

Given an equivalence relation in a lattice (or more precisely, the partition of the lattice into blocks induced by the equivalence relation), we want to find properties of said partition that guarantee that the equivalence relation in question is a congruence. At the end of this section, we will see a theorem that gives three conditions that an equivalence relation must satisfy to be a congruence. It requires three ingredients: sublattices, convex subsets, and quadrilateral-closed partitions. The latter two ingredients are new concepts that we must present first.

We begin by introducing convex subsets of a poset. These are an adaptation to posets of convexity in Euclidean space. Recall that a convex subset of an Euclidean space is a subset in which for any two points in the subset, the line segment between them is also contained in the subset. In a similar fashion, a convex subset of a poset, is a subset that for any two elements in it, contains all of the elements "between" them in the poset's order relation.

Definition 6.8. (*convex subset*) *A subset Q of a poset P is said to be convex if for any $x, y, \in Q$ and $z \in P$,*

$$x \leq z \leq y \implies z \in Q. \tag{6.22}$$

Example 6.10. (*down-sets and up-sets*) *The down-sets and up-sets of any poset P are convex subsets of P because the compound inequality of Definition 6.8 encompasses the inequality condition of these subsets.*

Example 6.11. (*intervals*) *Intervals on the real line are convex subsets of $\mathbb{R}$ with the usual order. Furthermore, the concept of intervals can be extended to arbitrary posets. Given a poset P with $a, b \in P$, we can define the interval (from a to b) by:*

$$[a, b] = \{x \in P \mid a \leq x \leq b\}. \tag{6.23}$$

It is easily seen that these "generalized" intervals are also convex. On the other hand, unlike the real line counterparts, they need not be chains. For example, consider the

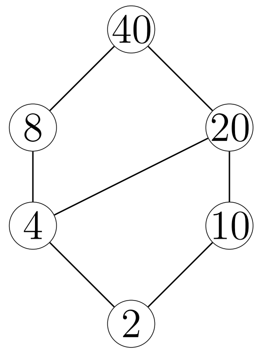


Figure 6.5: The interval subposet $[2, 40]$ of $\mathbb{N}_0$

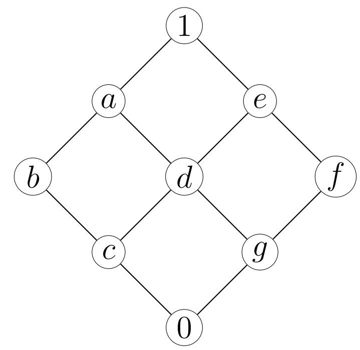


Figure 6.6: The lattice $\mathbf{3} \times \mathbf{3}$ with its elements labeled

following interval of $\mathbb{N}_0$ *ordered by divisibility* (*recall Example 2.6*)*:*

$$[2, 40] = \{x \in \mathbb{N}_0 \mid 2|x \text{ and } x|40\} = \{2, 4, 8, 10, 20, 40\}. \tag{6.24}$$

Its Hasse diagram in Figure 6.5 shows that it is not a chain.

We now briefly comment on the relationship between convex subsets of lattices and sublattices. The main point is that neither of the two types of subsets contains the other. A sublattice need not be convex and a convex subset of a lattice need not be a sublattice.

Example 6.12. (*non-convex sublattice*) *The subset* $Q = \{1, 4\}$ *of* $\mathbf{4}$ *is a sublattice of* $\mathbf{4}$ *but it is not convex since it does not include* 2 *and* 3*.*

Example 6.13. (*non-sublattice convex subset*) *Consider the subset* $Q = \{a, b, c, d, f\}$ *of the lattice* $\mathbf{3} \times \mathbf{3}$ *shown in Figure 6.6.* Q *is convex but is clearly not a sublattice of* $\mathbf{3} \times \mathbf{3}$*.*

We are now done with convex subsets and move on to the second new ingredient: quadrilateral-closed partitions. This will involve playing a geometric game of sorts in the Hasse diagrams of lattices. The first step is to define quadrilaterals in lattices. The idea is to describe properties that if satisfied by two pairs of elements in the lattice, make it possible for them to be the four vertices of a quadrilateral in the lattices's diagram. Be aware however that whether the elements in question form an actual quadrilateral will always depend on how the diagram is drawn.

Definition 6.9. (*opposite sides of a quadrilateral*) *Let L be a lattice with elements a, b, c, and d. We say that a, b and c, d are opposite sides of a quadrilateral if the following conditions all hold:*

1. $a < b$;

2. $c < d$;

3. *One of the following two statements is true:*

   (a) $a \wedge d = c$ *and* $a \vee d = b$,

   (b) $b \wedge c = a$ *and* $b \vee c = d$.

The reader should take a moment to understand how this conditions imply the possibility of a Hasse diagram of L with a quadrilateral with vertices a, b, c, and d. Figure 6.7 illustrates the two scenarios for opposites sides of a quadrilateral based on condition 3. We now show some examples.

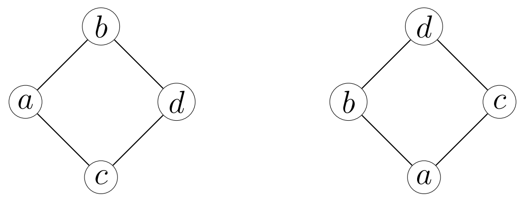


Figure 6.7: Picture of idea of opposite sides of quadrilateral

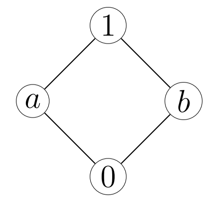


Figure 6.8: $\mathbf{M}_2$

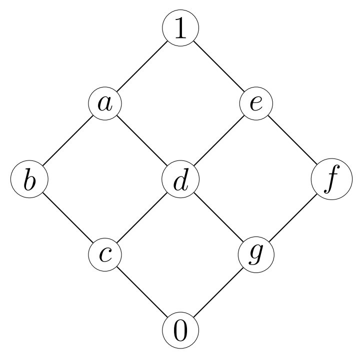


Figure 6.9: The lattice $\mathbf{3} \times \mathbf{3}$ with its elements labeled

Example 6.14. (*minimal example*) *Consider the lattice* $\mathbf{M}_2$ *shown in Figure 6.8. The following are opposite sides of a quadrilateral:*

1. $0, a$ *and* $b, 1$,

2. $0, b$ *and* $a, 1$.

Example 6.15. (*quadrilaterals in the grid*) *Consider the lattice* $\mathbf{3}\times\mathbf{3}$ *shown in Figure 6.9. The following are opposite sides of a quadrilateral:*

1. $a, 1$ *and* g, f,

2. $0, f$ *and* $b, 1$.

We are set to define what is a quadrilateral-closed partition of a lattice. The idea is to put some conditions on how the quadrilaterals in the lattice and the blocks of a partition interact with each other. A quadrilateral-closed partition of a lattice is a partition in which whenever one of two opposites sides of a quadrilateral is contained in a block of the partition, the other opposite side is also contained in some block of the partition (which may be different).

Definition 6.10. (*quadrilateral-closed partition*) *Let L be a lattice with an equivalence relation θ. The blocks of θ are said to be quadrilateral-closed if given a, b and c, d opposites sides of a quadrilateral, we have that*

$$a, b \in X \text{ for some block } X \in L/\theta \implies c, d \in Y \text{ for some block } Y \in L/\theta. \tag{6.25}$$

In the above definition, either $X = Y$ or $X \neq Y$ may hold. We now discuss some examples.

Example 6.16. (*quadrilateral-closed partition + non-example*) *Consider the following two equivalence relations on $\mathbf{3} \times \mathbf{3}$ (see Figure 6.9):*

1. *Block partition: $A = \{1, a, d, e\}$, $B = \{b, c\}$, $C = \{f, g\}$ and $D = \{0\}$;*

2. *Block partition: $X = \{a, b, c, d\}$, $Y = \{1, e\}$, $Z = \{f, g\}$ and $W = \{0\}$.*

The first partition is quadrilateral closed while the second one is not because g, f and d, e are opposites sides of a quadrilateral, g and f are both in Z but d and e belong to different blocks (X and Y respectively). Note that the first partition corresponds to the congruence given in Example 6.3.

We now have all of the ingredients needed to characterize which equivalence relations on a lattice are congruences. The idea is that the blocks must be sublattices, convex, and quadrilateral-closed. These conditions are both necessary and sufficient. We give the formal statement but omit the proof, which can be found it in [5].

Theorem 6.2. (*congruence characterization theorem*) *Let L be a lattice and let θ be an equivalence relation on L. Then θ is a congruence if and only if all three of the following conditions are satisfied:*

1. *the blocks of θ are all sublattices of L,*

2. *the blocks of θ are are all convex,*

3. *the blocks of θ are quadrilateral-closed.*

We finish this section with some examples on how to apply Theorem 6.2. Basically, all we must do is check if a given equivalence relation satisfies all three conditions. If it does, it is a congruence. Otherwise, it is not.

Example 6.17. (*checking for congruence*) *We revisit the two equivalence relations of Example 6.16:*

1. *The equivalence relation with blocks A, B, C, and D is a congruence. We already discussed that it is quadrilateral-closed. It can be observed that its blocks are all sublattices and convex.*

2. *The equivalence relation with blocks X, Y, Z, and W is not a congruence because we already established it is not quadrilateral-closed. This can be double-checked by noting that although $b \equiv c \pmod{\theta}$ and $f \equiv g \pmod{\theta}$, we have that*

$$b \vee f = 1 \not\equiv_\theta d = c \vee g. \tag{6.26}$$

6.5 Lattice of Congruences

The aim of this section is to study the lattice of congruences of a lattice. We view the congruences of a lattice L as subsets of L^2. We explain why the congruences of a lattice form a lattice and how to describe the resulting meet and join operations. Along the way, we present principal congruences.

Thus and by far, we have focused on studying one congruence on a lattice at a time. Now, we change our focus to considering all of the congruences that can be defined on a given lattice. We denote by $\mathrm{Con}\, L$ the set of all congruences of a lattice L. We make some remarks on $\mathrm{Con}\, L$. First, since a congruence is basically a subset of L^2, $\mathrm{Con}\, L$ is a subset of the power set of L^2. Second, this subset can be ordered by inclusion. Finally, if we look at the compatibility with lattice operations from the L^2 perspective we have that they translate to:

$$(a, b), (c, d) \in \theta \implies (a \vee c, b \vee d), (a \wedge c, b \wedge d) \in \theta. \tag{6.27}$$

This implies that a congruence on L is nothing more than an equivalence relation on L that is also as sublattice of L^2.

An interesting consequence of this is that it can be shown that an arbitrary intersection of congruences is a congruence. This reduces to proving (1) that an arbitrary intersection of equivalence relations is an equivalence relation and (2) that a non-empty arbitrary intersection of sublattices is a sublattice. Since L^2 is a congruence on L, we then have that $\mathrm{Con}\, L$ is a topped intersection structure. Recall that a topped intersection structure is a family of a subsets of a set that is closed under arbitrary intersections and that contains the whole set (Definition 3.16 in Section 3.8). Proposition 3.8 then implies that $\mathrm{Con}\, L$ is a complete lattice. We now consider $\mathrm{Con}\, L$ as a lattice with binary operations. Clearly, the meet of two congruences is their intersection on L^2. However, the join of two congruences is more difficult, but not impossible, to describe. We return to it later in this section.

We now take a small detour to discuss principal congruences, which will be useful when labeling the Hasse diagram of a lattice of congruences. Given two elements a and b in a lattice L, it is natural to ask if there is a smallest congruence that collapses a and b into one block, and if it exists, what is it? In other words, we want to know what other elements must be put together into blocks in order to put a and b together in a block. The fact that the intersection of congruences is a congruence guarantees the existence of said smallest congruence as the intersection of all of the congruences that collapse a and b. This is called the principal congruence generated by a and b.

Definition 6.11. (*principal congruence*) *Given a lattice L with $a, b \in L$, the principal congruence generated by a and b, denoted by $\theta(a,b)$ is defined by:*

$$\theta(a,b) = \bigcap\{\theta \in \mathrm{Con}\, L \mid (a,b) \in \theta\}. \tag{6.28}$$

Example 6.18. (*principal congruence*) *Consider the lattice* **4**. *Figure 6.10 shows $\theta(1,2)$ and $\theta(1,3)$. Note that $\theta(1,2)$ is obtained simply by putting 1 and 2 together in a block and leaving the remaining elements of* **4** *in singleton blocks. On the other hand in order to put together 1 and 3 in a block in $\theta(1,3)$, we must add 2 to that same* *block in order to have convex blocks, as required for congruences by Theorem 6.2.*

Before moving on to discuss the join of two congruences, we present the following result on principal congruences. It says (1) that a principal congruence generated by two elements c and d contains another principal congruence (generated by a and b) if and only if it contains a and b together in one block and (2) that the principal congruence generated by two elements equals the one generated by their join and their meet.

Proposition 6.5. (*relations among principal congruences*) *Let L be a lattice with $a, b, c, d \in L$. Then:*

1. $\theta(a, b) \subseteq \theta(c, d) \iff a \equiv b \pmod{\theta(c, d)}$;

2. $\theta(a, b) = \theta(a \wedge b, a \vee b)$.

Proof *Part 1:* $\implies$ *: Suppose $\theta(a, b) \subseteq \theta(c, d)$. Then by definition of $\theta(a, b)$, we have that $(a, b) \in \theta(c, d)$ (i.e. $a \equiv b \pmod{\theta(c, d)}$).*

$\impliedby$ *: Suppose $a \equiv b \pmod{\theta(c, d)}$. Then $(a, b) \in \theta(c, d)$. Recall that*

$$\theta(a, b) = \bigcap\{\theta \in \operatorname{Con} L \mid (a, b) \in \theta\} \tag{6.29}$$

and note that $\theta(c, d) \in \{\theta \in \operatorname{Con} L \mid (a, b) \in \theta\}$. Therefore, $\theta(a, b) \subseteq \theta(c, d)$.

Part 2: We use Part 1 to show both set inclusions.

$\subseteq$: *We show that* $a \equiv b \pmod{\theta(a \wedge b, a \vee b)}$. *By definition of* $\theta(a \wedge b, a \vee b)$,

$$a \wedge b \equiv a \vee b \pmod{\theta(a \wedge b, a \vee b)} \tag{6.30}$$

$$\implies (a \wedge b) \wedge a \equiv (a \vee b) \wedge a \pmod{\theta(a \wedge b, a \vee b)} \tag{6.31}$$

$$\implies a \wedge b \equiv a \pmod{\theta(a \wedge b, a \vee b)}. \tag{6.32}$$

It can be similarly shown that $a \wedge b \equiv b \pmod{\theta(a \wedge b, a \vee b)}$. *Then* $(a, b) \in \theta(a \wedge b, a \vee b)$ *by transitivity and* $\theta(a, b) \subseteq \theta(a \wedge b, a \vee b)$.

$\supseteq$: *We show that* $a \wedge b \equiv a \vee b \pmod{\theta(a, b)}$. *By definition of* $\theta(a, b)$,

$$a \equiv b \pmod{\theta(a, b)} \implies a \wedge b \equiv b \pmod{\theta(a, b)}. \tag{6.33}$$

Similarly, $a \equiv a \vee b \pmod{\theta(a, b)}$. *Transitivity then implies* $a \wedge b \equiv a \vee b \pmod{\theta(a, b)}$. *Therefore,* $\theta(a, b) \supseteq \theta(a \wedge b, a \vee b)$. $\square$

We now turn our attention to characterizing the join of two congruences in $\operatorname{Con} L$. In general, the union of two congruences is not a congruence. However, we know that $\alpha \vee \beta$ exists for all $\alpha, \beta \in \operatorname{Con} L$ because $\operatorname{Con} L$ is a complete lattice. To find it, we need the following strange terminology about sequences that witness the expression $a(\alpha \vee \beta)b$ where a and b are elements of L. The idea is to identify a sequence of elements of L from a to b in which consecutive elements are always related by at least one of α or β.

Definition 6.12. (*witnesses*) *Let L be a lattice with congruences α and β and elements a and b. We say that a sequence of n elements $z_1, ..., z_n$ of L witnesses $a(\alpha \vee \beta)b$ if the following conditions all hold:*

1. $a = z_1$;

2. $b = z_n$;

3. *for each* $i \in [1, n-1]$, *either* $z_i \; \alpha \; z_{i+1}$ *or* $z_i \; \beta \; z_{i+1}$.

It happens that the join of two congruences α and β is given by the relation that relates elements $a, b \in L$ for which there is a sequence that witnesses $a(\alpha \vee \beta)b$. Establishing this fact requires the following lemma whose proof we omit because it is simple. The definition and an example of the congruence given by witnesses follow the lemma.

Lemma 6.1. (*equivalent condition to congruence*) *Let L be a lattice and θ an equivalence relation on L. Then θ is a congruence if and only if for all $a, b, c \in L$,*

$$a \equiv b \pmod{\theta} \implies a \vee c \equiv b \vee c \pmod{\theta} \text{ and } a \wedge c \equiv b \wedge c \pmod{\theta}. \tag{6.34}$$

Definition 6.13. (*congruence given by witnesses*) *Let L be a lattice with congruences α and β. The relation given by the witnesses of $\alpha \vee \beta$ is the relation γ defined by*

$$\begin{gathered}(a, b) \in \gamma \iff \exists \text{ finite sequence } z_1, ..., z_n \text{ of elements of } L \\ \text{that witnesses } a(\alpha \vee \beta)b.\end{gathered} \tag{6.35}$$

Using Lemma 6.1 to show compatibility with lattice operations, it is routine to show that γ is a congruence and that it is the supremum of α and β in $\operatorname{Con} L$.

Example 6.19. (*join of two congruences*) *Consider the congruences $\theta(1,2)$ and $\theta(3,4)$ of* **4** *shown in Figure 6.10. It can be seen that the relation given by the sequences that witness $\theta(1,2)\vee\theta(3,4)$ is the congruence δ also in Figure 6.10. Note that* $(1,2),(3,4)\in\delta$ *because* $1,2$ *and* $3,4$ *are sequences that witness* $1(\theta(1,2)\vee\theta(3,4))2$ *and* $3(\theta(1,2)\vee\theta(3,4))4$ *respectively. Note that δ is not a principal congruence generated by any two elements of* **4**.

We are finally ready to define the lattice of congruences on a lattice.

Definition 6.14. (*lattice of congruences*) *Given a lattice L, the lattice of congruences on L, denoted* $\operatorname{Con} L$, *is the set of all congruences of L with operations:*

$$\alpha \wedge \beta = \alpha \cap \beta, \tag{6.36}$$

$$\alpha \vee \beta = \gamma, \tag{6.37}$$

for all $\alpha,\beta\in\operatorname{Con} L$, where γ is the relation given by the witnesses of $\alpha\vee\beta$.

It is straightforward to see that for any lattice L, the identities of $\operatorname{Con} L$ are

$$\mathbf{0} = \{(a,a) \mid a \in L\}, \tag{6.38}$$

$$\mathbf{1} = L^2. \tag{6.39}$$

We now give an example of a lattice of congruences.

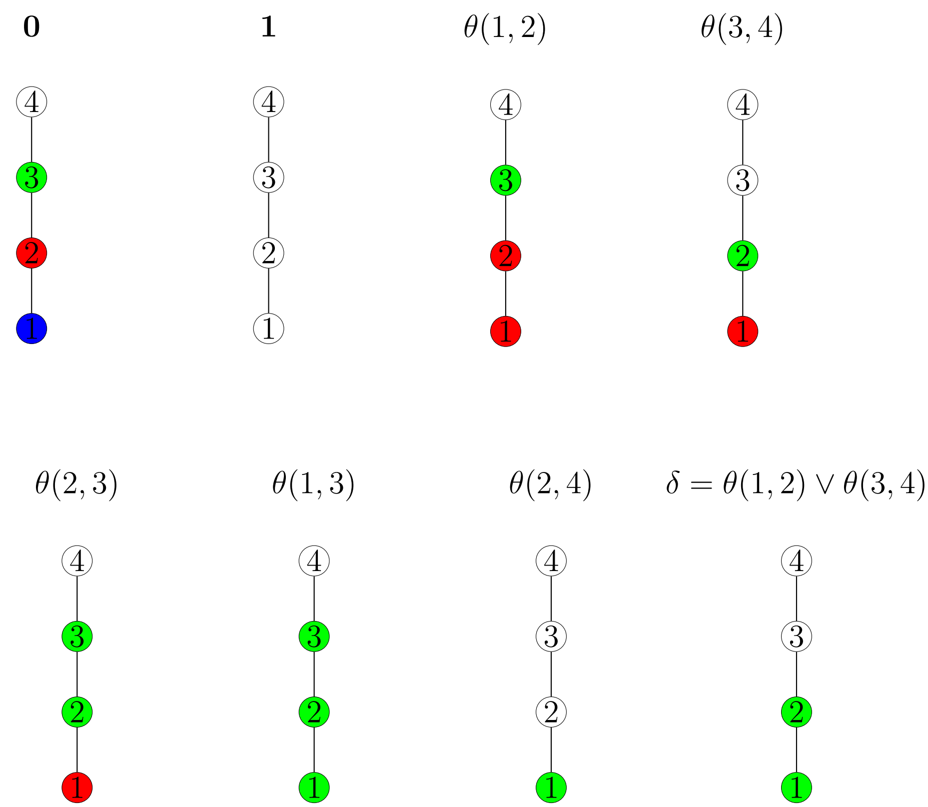


Figure 6.10: All congruences on $\mathbf{4}$: blocks indicated by colors

Example 6.20. (*lattice of congruences*) *Figure 6.10 shows all of the congruences on* $\mathbf{4}$ *using colors to identify the blocks of each one.* $\operatorname{Con}\mathbf{4}$ *is shown in Figure 6.11. It is the cube lattice* $\mathbf{2}^3$.

Observe that the lattice of congruences of Example 6.20 is distributive. A natural question to ask then is if this is always the case. The following theorem answers it affirmatively. Its proof can be found in [5] (page 140). This closes the section.

Theorem 6.3. (*distributivity of lattice of congruences*) *The lattice* $\operatorname{Con} L$ *is distributive for all lattices* L.

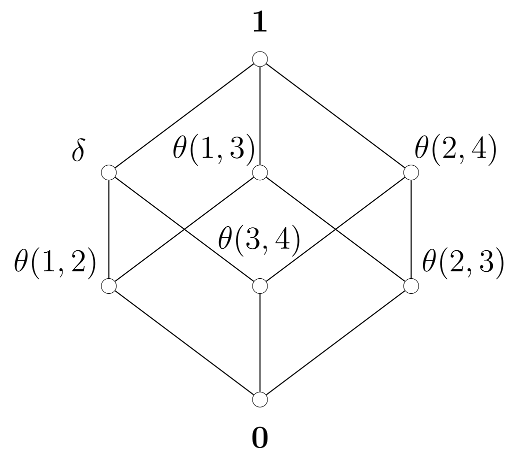


Figure 6.11: Hasse diagram of Con **4**

6.6 Connection to Distributive Lattices

We dedicate the last section of this chapter to establish a result that characterizes distributive lattices using congruences. In order to do so, some background on lattice ideals will be needed. Thus, we begin by defining ideals of lattices.

Lattice ideals are lattice analogs to ring ideals in rings. Those familiar with ring theory might recall that ideals in rings are subrings of the ring that absorb the ring with multiplication. By absorbing the ring we mean that the product of an ideal element with a ring element is always in the ideal. In lattices, we have something similar with join and meet playing the roles of addition and multiplication respectively. Lattice ideals are non-empty down-sets that are closed under join.

Definition 6.15. (*ideal*) *An ideal of a lattice L is a non-empty subset $J \subseteq L$ that satisfies two properties:*

1. *J is a down-set,*

2. *$a, b \in J \implies a \vee b \in J$.*

We briefly comment on ideals. The similarity between join and ring addition is evident (closure). The link between meet and ring multiplication is more subtly contained in the definition. It is implied by the down-set condition. This can be seen from the fact that given an ideal J of a lattice L, $x \wedge a$ will always be in J for all $x \in J$ and $a \in L$ because J is a down-set. Hence, the ideal does absorb the lattice with meet. In addition, it is easy to see that (lattice) ideals are sublattices. We now give some examples of ideals on lattices.

Example 6.21. (*ideals*) *The following can be shown to be ideals of a lattice:*

1. *All principal down-sets of any lattice.*
2. *For any set S and any $x \in S$, the subset of $\wp(S)$ consisting of all subsets of S that do not contain x.*

Having defined ideals we now use them to define relations on lattices. In particular, we take an ideal and relate two lattice elements only if there is an ideal element that has the same join with both lattice elements. We call this relation the ideal join relation on a lattice induced by the ideal. We show that this relation is always an equivalence relation of which the ideal is a block.

Definition 6.16. (*ideal join relation*) *Let L be a lattice and let J be an ideal of L. The ideal join relation on L induced by J is the relation θ_J given by:*

$$\theta_J = \{(a, b) \in L^2 \mid \exists c \in J \text{ such that } a \vee c = b \vee c\}. \tag{6.40}$$

Proposition 6.6. (*ideal join partition with ideal block*) *Let L be a lattice with an ideal J. If θ_J is the ideal join relation on L induced by J, then:*

1. *θ_J is an equivalence relation on L;*

2. *J is a block of θ_J.*

Proof *Part 1: Showing that θ_J is reflexive and symmetric is trivial, hence, we only prove transitivity. Let $a, b, c, d \in L$ be such that $(a, b), (b, c) \in \theta_J$. Then there exist $d, e \in J$ such that $a \vee d = b \vee d$ and $b \vee e = c \vee e$. Then*

$$a \vee (d \vee e) = (a \vee d) \vee e \tag{6.41}$$

$$= (b \vee d) \vee e \tag{6.42}$$

$$= (b \vee e) \vee d \tag{6.43}$$

$$= (c \vee e) \vee d \tag{6.44}$$

$$= c \vee (d \vee e). \tag{6.45}$$

Since J is an ideal, $d \vee e \in J$. Therefore, $(a, c) \in \theta_J$ and θ_J is an equivalence relation.

Part 2: We show that J is a block by showing that (1) all elements of J are in the same block of θ_J and (2) that any element related to an element in J must be in J. For the first claim, suppose that $a, b \in J$. Since J is an ideal, $a \vee b \in J$. Then

$$a \vee (a \vee b) = a \vee b = b \vee (a \vee b) \tag{6.46}$$

and $(a, b) \in \theta_J$. Thus, J is contained in some block of θ_J.

Now for the second claim, let $a \in J$, $b \in L$, and $(a, b) \in \theta_J$. Then there exists $c \in J$ such that $a \vee c = b \vee c$. This implies

$$(a \vee c) \wedge b = (b \vee c) \wedge b \tag{6.47}$$

$$= b. \tag{6.48}$$

Then $b \leq a \vee c$. Since $a \vee c \in J$ and ideals are down-sets, $b \in J$. Therefore, J contains a block of θ_J and we are done. □

We now have all of the parts needed to give the theorem that characterizes distributive lattices with congruences. The idea is that a lattice is distributive if and only if all of its ideal join relations are congruences. The proof will apply Theorem 6.2 on the characterization of equivalence relations that are congruences.

Theorem 6.4. (*characterizing distributive lattices with congruences*) *A lattice L is distributive if and only if for all ideals J of L, θ_J is a congruence and J is a block of θ_J.*

Proof $\Longrightarrow$ *: Suppose that L is distributive and let J be any ideal of L. By Proposition 6.6, θ_J is an equivalence relation of which J is a block. Hence, it suffices to show that θ_J is compatible with the lattice operations. Let $a, b, c, d \in L$ be such that*

$$a \equiv c \pmod{\theta_J} \quad \textit{and} \quad b \equiv d \pmod{\theta_J}. \tag{6.49}$$

Then there exist $x, y \in J$ such that $a \vee x = c \vee x$ and $b \vee y = d \vee y$. Then to show *compatibility with join note that* $x \vee y \in J$ *and that*

$$(a \vee b) \vee (x \vee y) = (a \vee x) \vee (b \vee y) \tag{6.50}$$

$$= (c \vee x) \vee (d \vee y) \tag{6.51}$$

$$= (c \vee d) \vee (x \vee y). \tag{6.52}$$

Similarly, for meet, note again that $x \vee y \in J$ *and observe that*

$$(a \wedge b) \vee (x \vee y) = [a \vee (x \vee y)] \wedge [b \vee (x \vee y)] \tag{6.53}$$

$$= [(a \vee x) \vee y] \wedge [(b \vee y) \vee x] \tag{6.54}$$

$$= [(c \vee x) \vee y] \wedge [(d \vee y) \vee x] \tag{6.55}$$

$$= [c \vee (x \vee y)] \wedge [d \vee (x \vee y)] \tag{6.56}$$

$$= (c \wedge d) \vee (x \vee y), \tag{6.57}$$

where the first and last equalities follow from distributivity of L*. Therefore,* θ_J *is a congruence as required.*

$\Longleftarrow$ *: Suppose that* θ_J *is a congruence on* L *with block* J *for all ideals* J *of* L*. We show that* L *is distributive using the* M_3*-*N_5 *Theorem (4.1). The idea is that* L *cannot have neither* $\mathbf{M}_3$ *nor* $\mathbf{N}_5$ *as a sublattice because both have ideals* J *for which the ideal join relation* θ_J *is not a congruence and the issues raised by these violating ideals will persist even if they are "extended" in a larger lattice.*

We begin with $\mathbf{M}_3$*. We use the element labels from Figure 6.12. Consider the ideal* $J = \downarrow a = \{0, a\}$*. By Proposition 6.6, we already know that* J *is a block of* θ_J*. In*

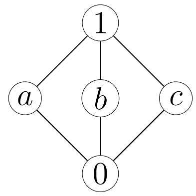


Figure 6.12: The diamond $\mathbf{M}_3$

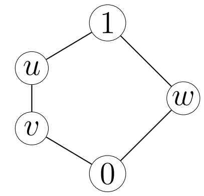


Figure 6.13: The pentagon $\mathbf{N}_5$

addition, observe that $b \equiv c \equiv 1 \pmod{\theta_J}$ *because* $a \in J$ *and* $b \vee a = c \vee a = 1 \vee a = 1$. *Thus, the two blocks of* θ_J *are* $J = \{0, a\}$ *and* $\{b, c, 1\}$. *However,* $\{b, c, 1\}$ *is not a sublattice. Therefore,* θ_J *is not a congruence by Theorem 6.2.*

Now, we deal with $\mathbf{N}_5$. *We use the element labels from Figure 6.13. Consider the ideal* $J = {\downarrow}v = \{0, v\}$. *We show that* θ_J *induces three blocks on* $\mathbf{N}_5$*:* $\{0, v\}$, $\{u\}$, *and* $\{1, w\}$. $J = \{0, v\}$ *is a block by Proposition 6.6. We now show that* $\{1, w\}$ *is a block. Note that* $1 \equiv w \pmod{\theta_J}$ *because* $w \vee v = 1 \vee v = 1$. *Since* $u \vee v = u \vee 0 = u$ *and* $w \vee x, 1 \vee x \in \{1, w\}$ *for all* $x \in \mathbf{N}_5$, u *is not in the same block as* $\{1, w\}$. *Therefore,* θ_J *has the three blocks we mentioned above:* $\{0, v\}$, $\{u\}$, *and* $\{1, w\}$. *Observe that* $0, u$ *and* $w, 1$ *are opposites sides of a quadrilateral. Note however, that* w *and* 1 *are in the same block of* θ_J *while* 0 *and* u *are not. Then the blocks of* θ_J *are not quadrilateral-closed and* θ_J *is not a congruence by Theorem 6.2.* $\square$

We complete the section with an example of how to apply Theorem 6.4 to show that a lattice is distributive.

Example 6.22. (*congruences and distributivity*) *Let* K *be the lattice shown in Figure 6.14. It can be seen that the only ideals of* K *are its principal down-sets:* ${\downarrow}x$ *for each* $x \in K$. *We now list the partitions induced by the corresponding ideal relations:*

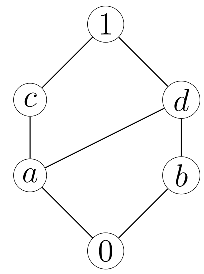


Figure 6.14: The lattice K of Example 6.22

1. $\theta_{\downarrow 0} : \{0\}, \{a\}, \{b\}, \{c\}, \{d\}, \{1\}$,

2. $\theta_{\downarrow a} : \{0, a\}, \{b, d\}, \{c\}, \{1\}$,

3. $\theta_{\downarrow b} : \{0, b\}, \{a, d\}, \{c, 1\}$,

4. $\theta_{\downarrow c} : \{0, a, c\}, \{b, d, 1\}$,

5. $\theta_{\downarrow d} : \{0, a, b, d\}, \{c, 1\}$,

6. $\theta_{\downarrow 1} : \{0, a, b, c, d, 1\} = K$.

It can be observed that all of these equivalence relations have blocks that are sublattices, are convex, and are quadrilateral-closed. Hence, they are all congruences by Theorem 6.2. It can also be noted that the corresponding ideal is a block of each partition (*always listed first*)*. Therefore, K is distributive by Theorem 6.4. This can be verified with Theorem 4.1 and Corollary 5.1 if so desired.*

Chapter 7

A New Cut-Complex Poset from Convex Polytopes

7.1 Introduction

Before we introduce the titular ST-distributive and ST-modular lattices of this thesis, we take a detour to the land of convex polytopes with the purpose of building bridges between it and the realm of order theory where lattices live. Convex polytopes are the generalization of the familiar polygons from high school geometry to any number of dimensions. A particular example is the hypercube which is the d-dimensional generalization of the square. It will be our polytope of interest. In addition, we will also mix in some elementary graph theory given that polytopes can be represented by graphs. Two classical references on convex polytopes are [3] and [14].

One of our main goals in this chapter is to introduce a new poset which also happens to be a distributive lattice. It will be constructed by defining an order relation on the set of cut-complexes of the 4-dimensional cube. We will simply call it the cut-complex poset of the 4-cube and denote it by $\mathcal{C}c(C^4)$.

The other principal objective is to provide some background on convex polytopes to facilitate the understanding of both the cut-complex poset and an application of ST-modular lattices to convex sets to be presented in Section 9.4. In particular, we discuss definitions and results used to prove Theorems 9.1 and 9.2 in said section. Finally, we also take this opportunity to point towards the cubical lattice, a lattice constructed with the faces of a hypercube to which ST-distributivity and ST-modularity may be applied.

The rest of this chapter is organized as follows. Section 7.2 starts with convex sets. Section 7.3 then discusses hyperplanes. This is followed by convex polytopes in Section 7.4. Afterwards, we explain cut-complexes in Section 7.5 which completes setting the stage for finally introducing the cut-complex poset in Section 7.6. The material of these last two sections is not needed for Section 9.4.

7.2 Convex Sets

We begin our journey into the world of convex polytopes by introducing convex sets. Throughout this chapter, we will work exclusively in the Euclidean space $\mathbb{R}^d$. For a point $x \in \mathbb{R}^d$, we give its coordinate representation by $x = (x_1, ..., x_d)$ where each $x_i \in \mathbb{R}$. We assume some familiarity with some concepts of linear algebra and topology such as linear subspace, linear combination, open sets, and closed sets.

We first define and give examples of convex sets and convex hulls. We then briefly

Figure 7.1: A convex and a non-convex set

Figure 7.2: A set and its convex hull

discuss convex combinations and list some results on convex sets. Afterwards, we quickly comment on convex sets that are also compact. This is followed by a brief introduction to affine sets, a sub-class of convex sets. Finally, we define the dimension of affine and convex sets.

Convex sets are an important type of sets in Euclidean space in which it is possible to go between any two points in the set by walking in a straight line without leaving the set. The convex hull of a set consists of the set plus any additional points needed to turn it into a convex set.

Definition 7.1. (*convex set*) *A set $A \subseteq \mathbb{R}^d$ is a convex set if for any two points $x, y \in A$, the line segment connecting x and y is contained in A.*

Definition 7.2. (*convex hull*) *The convex hull of a set $A \subseteq \mathbb{R}^d$, denoted* $\operatorname{conv}(A)$, *is the smallest convex set containing A. Equivalently, it is the intersection of all of the convex sets in $\mathbb{R}^d$ containing A.*

Figure 7.1 shows a convex set and a non-convex set and Figure 7.2 a non-convex set with its convex hull. The convex polytopes of Section 7.4 are also convex sets. We now give some additional concrete examples of convex sets, non-convex sets, and convex hulls. We will not go into the details of showing convexity but suggest that the reader use drawings to get an intuition of why the convex sets given are convex.

Example 7.1. (*convex sets*) *The following are examples of convex sets in Euclidean spaces of different dimensions:*

1. *In $\mathbb{R}$: open and closed intervals, open and closed rays;*

2. *In $\mathbb{R}^2$: lines, circles with their interior, triangles with their interiors, the four quadrants (open or closed);*

3. *In $\mathbb{R}^3$: lines, planes, cubes with their interiors, spheres with their interior;*

4. *In $\mathbb{R}^d$: hyperplanes, halfspaces, and interiors of halfspaces.*

Example 7.2. (*non-convex sets*) *The following are examples of non-convex sets in Euclidean spaces of different dimensions:*

1. *In $\mathbb{R}$: $\mathbb{Z}$;*

2. *In $\mathbb{R}^2$: annuli (flattened donut shape);*

3. *In $\mathbb{R}^3$: tori (donut shape).*

Justifications: $\mathbb{Z}$ excludes all of the real numbers between any two integers, which are in the line segment between them. An annulus and a torus both exclude the points in the hole, which are in line segments connecting two points of the set in question.

Example 7.3. (*convex hulls*) *The following are examples of convex hulls in Euclidean spaces of different dimensions:*

1. *In $\mathbb{R}$: The convex hull of two numbers $a, b \in \mathbb{R}$ is the interval $[a, b]$.*

2. *In $\mathbb{R}^2$: The convex hull of three noncollinear points $a, b, c \in \mathbb{R}^2$ is the closed set of points of $\mathbb{R}^2$ enclosed by the triangle whose sides are the line segments $[a, b]$, $[b, c]$, and $[c, a]$.*

3. *In $\mathbb{R}^3$: The convex hull of two distinct intersecting lines is the plane they define.*

Convex sets and convex hulls are formally described with convex combinations of points in Euclidean space. We will not go into the details here but we give the definition of a convex combination and provide a list of basic results on convex sets. For more details, consult [3].

Definition 7.3. (*convex combination*) *A convex combination of a set of points in Euclidean space is a linear combination of those points whose coefficients are non-negative and add up to 1. More precisely, a convex combination of points $x_1, ...x_d \in \mathbb{R}^d$ is a sum of the form*

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_d x_d, \tag{7.1}$$

where the coefficients λ_i satisfy the following three conditions:

1. $\lambda_i \in \mathbb{R}\, \forall i$,

2. $\lambda_i \geq 0\, \forall i$,

3. $\lambda_1 + \cdots + \lambda_d = 1$.

Proposition 7.1. (*basic facts about convex sets*) *The following is a list of true statements about convex sets.*

1. *For any natural number d, the whole Euclidean space $\mathbb{R}^d$ is convex.*

2. *The intersection of two convex sets is convex.*

3. *The union of two convex sets is not always convex.*

4. *For any set $A \subseteq \mathbb{R}^d$, the convex hull $\mathrm{conv}(A)$ exists and is well-defined.*

5. *If A is a convex set, then $\mathrm{conv}(A) = A$.*

6. *A convex set is a set that is closed under convex combinations.*

7. *The convex hull of a set A is the set of all convex combinations of points in A.*

8. *If A and B are both convex sets, then $\mathrm{conv}(A, B) = \mathrm{conv}(A \cup B)$ is given by the union of all line segments between a point in A and a point in B.*

In addition, we take a brief look at the interplay between convex sets and compact sets in Euclidean space. Recall that a compact set in $\mathbb{R}^d$ (with the usual distance metric) is a set that is closed and bounded [15]. In particular, finite sets are compact. We list two results on convex and compact sets that interest us (proofs in [7]).

Proposition 7.2. (*convex and compact sets*)

1. *The convex hull of a compact set is compact.*

2. *If $S \subseteq \mathbb{R}^d$ is convex and compact and x is a point in $\mathbb{R}^d$ not in S, then there exists a hyperplane H passing through x such that $H \cap S = \emptyset$.*

We continue our tour of convex sets with a brief introduction to affine sets which are a special type of convex set with stronger properties. The main idea is that they contain the entire line through any two points in them rather than only the line segment. We can also define affine hulls and affine combinations just like convex hulls and combinations.

Definition 7.4. (*affine set*) *A set $A \subseteq \mathbb{R}^d$ is an affine set if for any two points $x, y \in A$, the line through x and y is contained in A.*

Definition 7.5. (*affine hull*) *The affine hull of a set $A \subseteq \mathbb{R}^d$, denoted* $\operatorname{aff}(A)$, *is the smallest affine set containing A. Equivalently, it is the intersection of all of the affine sets in $\mathbb{R}^d$ containing A.*

Definition 7.6. (*affine combination*) *An affine combination of a set of points in Euclidean space is a linear combination of those points whose coefficients add up to 1. More precisely, a affine combination of points $x_1, ..., x_d \in \mathbb{R}^d$ is a sum of the form*

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_d x_d, \tag{7.2}$$

where the coefficients λ_i satisfy the following two conditions:

1. $\lambda_i \in \mathbb{R} \, \forall i$,
2. $\lambda_1 + \cdots + \lambda_d = 1$.

Example 7.4. (*affine sets and hulls*)

1. *affine sets: lines, planes;*

2. *convex but not affine: the square S in Figure 7.3;*

3. *affine hulls:*

   - *The affine hull of two points is the line through them.*

   - *The affine hull of three nonconllinear points is the plane they determine.*

   - *For the square S in Figure 7.3,* $\text{aff}(S) = \mathbb{R}^2$.

Finally, we want to define the dimension of a convex or affine set in $\mathbb{R}^d$. To this end, we will introduce the following notion of parallel affine sets. If an affine set is obtained from another via a (possibly trivial) translation in $\mathbb{R}^d$, then we say that they are *parallel*.

Now, recall from linear algebra that subspaces of $\mathbb{R}^d$ have a dimension given by the size of their bases. It can be shown that an affine set is either a linear subspace of $\mathbb{R}^d$ or the translate of such a subspace, which is unique [3]. Hence, each affine set has a unique linear subspace parallel to it. This allows us to define the dimension of an affine set as the dimension of said linear subspace. The dimension of a convex set is then given by the dimension of its affine hull.

Definition 7.7. (*dimension*) *The dimension of a set $A \subseteq \mathbb{R}^d$, denoted* $\dim(A)$*, is defined as follows.*

1. *If A is affine, then* $\dim(A)$ *is the dimension of the unique linear subspace parallel to A.*

2. *If A is convex, then* $\dim(A) = \dim(\text{aff}(A))$.

Example 7.5. (*dimension*) *If S is any square in $\mathbb{R}^3$, then there is a unique plane P that is the affine hull of S. Since a plane in $\mathbb{R}^3$ is the translate of a two-dimensional subspace of $\mathbb{R}^3$, we have that* $\dim(S) = \dim(\text{aff}(S)) = \dim(P) = 2$.

7.3 Hyperplanes

The next step in our convex journey is to introduce hyperplanes, a special type of affine set. We also discuss several related concepts: halfspaces, supporting hyperplanes and a basic separating lemma from convexity theory.

A hyperplane is a generalization of a two-dimensional plane in Euclidean spaces of higher dimensions. It is a $(d-1)$-subspace of $\mathbb{R}^d$ or a translation of such a subspace. Hence, it is an affine set of dimension $d-1$.

Definition 7.8. (*hyperplane*) *A hyperplane is a convex subset H of $\mathbb{R}^d$ of dimension $d-1$ determined by all points $x \in \mathbb{R}^d$ satisfying a linear equation of the form $ax = c$ for constants $a \in \mathbb{R}^d$ and $c \in \mathbb{R}$. In other words,*

$$H = \{x \in \mathbb{R}^d \mid ax = c\}. \tag{7.3}$$

Note that ax is a dot product in $\mathbb{R}^d$ which for $a = (a_1, ..., a_d)$ and $x = (x_1, ..., x_d)$ is defined by

$$ax = \sum_{i=1}^{d} a_i x_i. \tag{7.4}$$

Example 7.6. (*hyperplanes in $\mathbb{R}^2$*) *Lines in the Euclidean plane $\mathbb{R}^2$ are hyperplanes. For instance, consider the line L given by the equation $y = -2x + 1$. If we let $x_1 = x$,* *and* $x_2 = y$*, we can rearrange it to get*

$$x_2 = -2x_1 + 1 \implies 2x_1 + x_2 = 1 \implies (2,1)(x_1, x_2) = 1 \tag{7.5}$$

which is a linear equation of the form specified above. Thus,

$$L = \{(x_1, x_2) \in \mathbb{R}^2 \mid (2,1)(x_1, x_2) = 1\} \tag{7.6}$$

is a hyperplane of $\mathbb{R}^2$*. It is shown in Figure 7.3.*

We emphasize that being a hyperplane depends on both the actual set and its underlying space. For instance, a line is a hyperplane in $\mathbb{R}^2$ but not in $\mathbb{R}^3$. Similarly, a point is a hyperplane in $\mathbb{R}$ but not in $\mathbb{R}^2$ where hyperplanes are lines. Naturally, a hyperplane in $\mathbb{R}^3$ is a plane. In general, a k-dimensional affine set is a hyperplane of $\mathbb{R}^{k+1}$. Therefore, all affine sets are hyperplanes in some Euclidean space.

One particular property of hyperplanes is that they split $\mathbb{R}^d$ in two sets. These are called halfspaces.

Definition 7.9. (*halfspace*) *A halfspace of* $\mathbb{R}^d$ *is either of the two closed subsets into which a hyperplane* H *divides* $\mathbb{R}^d$*. These are determined by the linear inequalities* $ax \geq c$ *and* $ax \leq c$ *and denoted by* H^+ *and* H^- *respectively. In other words, the halfspaces of* $\mathbb{R}^d$ *defined by a hyperplane* H *are the sets*

$$H^+ = \{x \in \mathbb{R}^d \mid ax \geq c\}, \tag{7.7}$$

$$H^- = \{x \in \mathbb{R}^d \mid ax \leq c\}. \tag{7.8}$$

Example 7.7. (*halfspaces in* $\mathbb{R}^2$) *If we consider the line* L *of Example 7.6, we have that it defines the halfpsaces*

$$L^+ = \{(x_1, x_2) \in \mathbb{R}^2 \mid (2, 1)(x_1, x_2) \geq 1\}, \tag{7.9}$$

$$L^- = \{(x_1, x_2) \in \mathbb{R}^2 \mid (2, 1)(x_1, x_2) \leq 1\}, \tag{7.10}$$

which correspond respectively to the linear inequalities $y \geq -2x + 1$ *and* $y \leq -2x + 1$. *These halfspaces can be identified in Figure 7.3.*

A halfspace is sometimes called a *closed halfspace*. This is done to distinguish it from an *open halfspace*, which is its interior (i.e. the halfspace minus its hyperplane boundary). This interior is obtained by simply changing the inequalities in Equations (7.7) and (7.8) to strict inequalities. The resulting sets are denoted by $\text{int}(H^+)$ and $\text{int}(H^-)$ respectively. Observe that both open and closed halfspaces are convex but not affine. One last remark regarding halfspaces is that in order for them to be well-defined, a and c must be fixed in the hyperplane's representation. This is because although the equations $ax = c$ and $(-a)x = -c$ denote the same hyperplane, their corresponding inequalities have different solutions.

Next, we define what is a supporting hyperplane of a convex set, an important concept in convexity theory and optimization. A hyperplane H is said to support a convex set S if S is contained in one of the two closed halfspaces determined by H and has points lying in H. Note that these points in H must be boundary points of S due to the convexity of S.

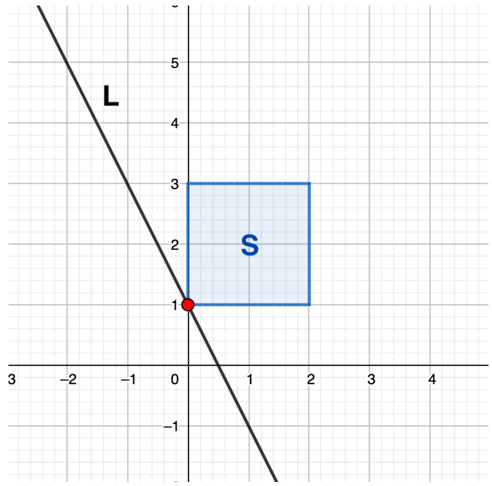


Figure 7.3: A square S and its supporting hyperplane L

Definition 7.10. (*supporting hyperplane*) *A supporting hyperplane of a convex set S is a hyperplane H such that*

1. $S \subseteq H^+$ *or* $S \subseteq H^-$;
2. $S \cap H \neq \emptyset$.

Example 7.8. (*supporting hyperplane in* $\mathbb{R}^2$) *The line L of Example 7.6 is a supporting hyperplane of the square S determined by the points* $(0, 1)$, $(0, 3)$, $(2, 1)$, *and* $(2, 3)$. *Note that $S \subseteq L^+$ and that $S \cap L = \{(0, 1)\}$ which is non-empty. A picture is shown in Figure 7.3.*

An interesting result on hyperplanes is the following lemma from [6] which we restate without proof. It is a basic separating lemma in convexity theory which says that given two finite sets of points separated by a hyperplane, it is possible to pick a point and move it from one set to the other by relocating the separating hyperplane.

a	$(-2,1)$	c	$(2,2)$	e	$(4,-1)$
b	$(-1,-1)$	d	$(3,1)$	x	$(1,-3)$

Table 7.1: Points in $\mathbb{R}^2$ for Example 7.9

Lemma 7.1. (*separating lemma [6]*) *Suppose M_1 and M_2 are two finite sets of points in $\mathbb{R}^d$ that are strictly separated by a hyperplane H in the sense that*

$$M_1 \subseteq \operatorname{int}(H^-) \text{ and } M_2 \subseteq \operatorname{int}(H^+). \tag{7.11}$$

Then there exists $x \in M_1$ such that for some relocation of H, say H_1, we have that

$$M_1 \setminus \{x\} \subseteq \operatorname{int}(H_1^-) \text{ and } M_2 \cup \{x\} \subseteq \operatorname{int}(H_1^+). \tag{7.12}$$

Example 7.9. (*separating lemma in $\mathbb{R}^2$*) *Consider again the line L from Example 7.6 and the points of $\mathbb{R}^2$ in Table 7.1. Let $M_1 = \{a, b, x\}$ and $M_2 = \{c, d, e\}$. Then L strictly separates M_1 and M_2 with $M_1 \subseteq \operatorname{int}(L^-)$ and $M_2 \subseteq \operatorname{int}(L^+)$. See Figure 7.4. If we relocate L to L_1, the y-axis, then we have that $M_1 \setminus \{x\} \subseteq \operatorname{int}(L^-)$ and $M_2 \cup \{x\} \subseteq \operatorname{int}(L^+)$. See Figure 7.5.*

Another peculiarity of hyperplanes is that two distinct intersecting hyperplanes can be used to divide $\mathbb{R}^d$ into four quadrants based on the four possible intersections between their induced halfspaces. This leads to a coordinated system of hyperplanes (CSH) on $\mathbb{R}^d$, an application of Lemma 7.1 that can be used to study convex polytopes. Details of this can be found in [8].

We finish by pointing at the major role that hyperplanes will have in the rest of

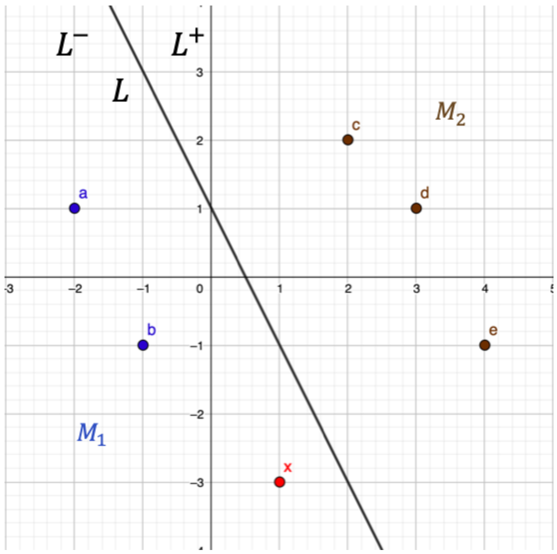


Figure 7.4: Original hyperplane L and points of Example 7.9

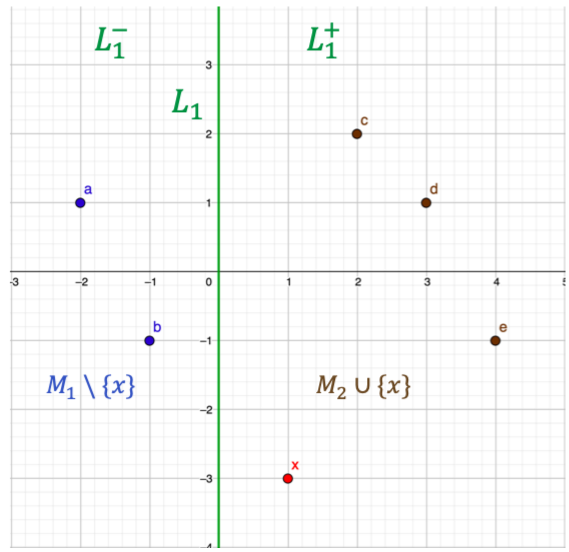


Figure 7.5: Relocated hyperplane L_1 and points of Example 7.9

this chapter. They will be essential in the definition of a cut-complex in Section 7.5. Furthermore, Lemma 7.1 will be crucial in establishing the covering relation on the set of cut-complexes of the 4-cube in Section 7.6 that will yield the titular poset of this chapter.

7.4 Convex Polytopes

We now turn our attention to a special class of convex sets: convex polytopes. Our treatment of them goes over their basic definitions and some examples, discusses their faces and face lattices, and presents a graph-theoretic look at them. Our main interest going forward in this chapter is the hypercube while faces of convex polytopes will be relevant in Section 9.4, where Theorems 9.1 and 9.2 give additional results on convex polytopes.

Convex polytopes are the generalization to any number of dimensions of 2D polygons and 3D polyhedrons. There are two ways to formally define them. We give one of them as a definition and the other as a proposition without proof. Further information on why both are equivalent can be found in [3] and [7].

Definition 7.11. (*convex polytope*) *A convex polytope is the convex hull of a finite set of points in* $\mathbb{R}^d$.

Proposition 7.3. (*alternate definition of convex polytope*) *A subset of* $P \subseteq \mathbb{R}^d$ *is a convex polytope if and only if* P *is the bounded intersection of a finite number of* (*closed*) *halfspaces.*

Note that since a convex polytope is a convex set, it has a dimension by Definition 7.7. A convex polytope of dimension d is called a *convex d-polytope*. Also note that $\emptyset$ is a convex polytope because it is the convex hull of 0 points and the intersection of any two disjoint closed halfspaces. By definition, $\dim(\emptyset) = -1$. We now give some examples.

Example 7.10. (*hypercubes*) *The hypercube of dimension* d *or* d*-cube, denoted* c^d*, is a convex polytope for all* $d \in \mathbb{N}$*. In particular, we refer to the unit hypercube, which is drawn starting from the origin of* $\mathbb{R}^d$ *with length 1 line segments so that the entire figure is in the first quadrant of* $\mathbb{R}^d$*. Each corner can be identified with a binary sequence of length* d *indicating its distance from the origin along each possible axis. The most basic examples are the line segment* c^1 *and the square* c^2 (*the latter shown in Figure 7.6*).

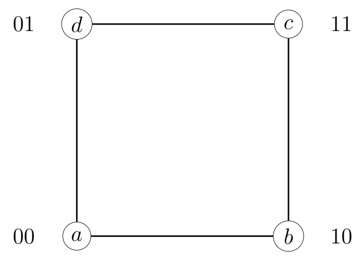


Figure 7.6: Square (c^2)

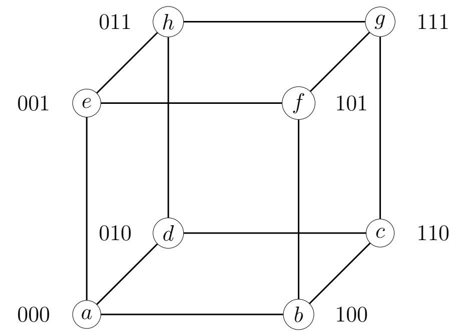


Figure 7.7: Cube (c^3)

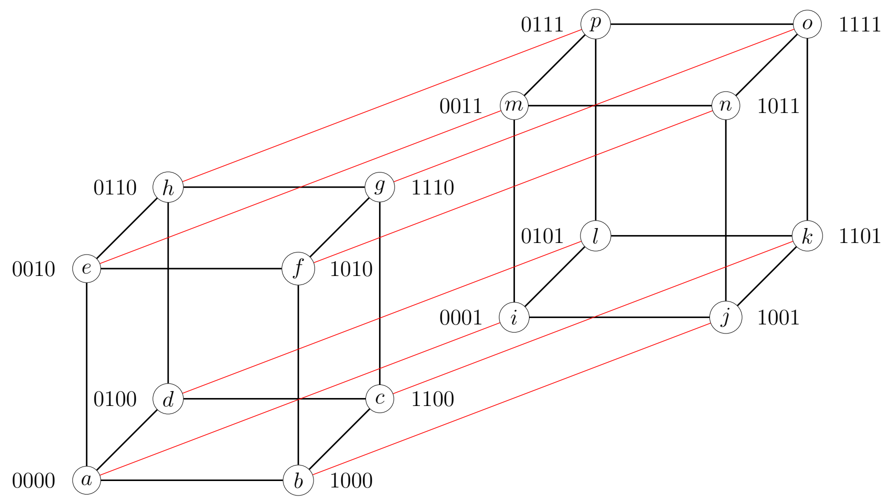


Figure 7.8: Tesseract (c^4)

1. *If $d = 3$, then c^3 is a cube (shown in Figure 7.7). Note that it is the convex hull of $\{a, b, c, d, e, f, g, h\}$ or equivalently of $\{d_1d_2d_3 | d_i \in \{0, 1\}\}$ and the intersection of 6 halfspaces of $\mathbb{R}^3$ determined by the 6 planes containing its 6 square sides.*

2. *If $d = 4$, then c^4 is a tesseract (shown in Figure 7.8). Note that it is the convex hull of $\{a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p\}$ and the intersection of 8 halfspaces of $\mathbb{R}^4$ determined by the 8 3D hyperplanes containing its 8 cubic sides.*

3. *For any $d \in \mathbb{N}$, c^d can be expressed as the convex hull of 2^d points in $\mathbb{R}^d$.*

Example 7.11. (*more convex polytopes*) *The following are all convex polytopes in Euclidean spaces of different dimensions:*

1. *In $\mathbb{R}$: closed and bounded intervals (line segments);*
2. *In $\mathbb{R}^2$: triangles, pentagons, rectangles;*
3. *In $\mathbb{R}^3$: tetrahedrons, octahedrons, rectangular solids.*

We now define a face of a convex polytope, which is a compact subset that is important in convexity theory and optimization. Faces show how a polytope is constructed from polytopes of lower dimensions.

Definition 7.12. (*face of a convex polytope*) *A face of a convex d-polytope P is a subset $F \subseteq P$ such that $F = P \cap H$ for a supporting hyperplane of P in $\mathbb{R}^d$. By definition, $\emptyset$ and P itself are also faces of P.*

It can be shown that a face of a convex polytope is itself a convex polytope (Theorem 9.1 from [7]) and hence, has a dimension. Thus, we can define a *k-face* of P as a face of dimension k for any $-1 \leq k \leq d$. $k = -1$ is admitted because it is the dimension of $\emptyset$. Faces of certain dimensions have special names. Faces of dimension 0 are called vertices while those of dimension 1 are called edges. Those of dimension $d-1$ are called facets. As an example, we discuss the faces of the hypercubes of Example 7.10.

Example 7.12. (*faces of hypercube*) *We examine the d-cubes of Example 7.10.*

1. *c^3 has 8 vertices (a, b, c, d, e, f, g, h); 12 edges*

$$[a, b], [b, c], [c, d], [d, a], [e, f], [f, g], [g, h], [h, e], [a, e], [b, f], [c, g], [d, h]; \tag{7.13}$$

   and 6 facets (square sides):

$$\begin{gathered} \operatorname{conv}(a, b, c, d), \operatorname{conv}(e, f, g, h), \operatorname{conv}(a, d, e, h), \\ \operatorname{conv}(b, c, f, g), \operatorname{conv}(a, b, e, f), \operatorname{conv}(c, d, g, h). \end{gathered} \tag{7.14}$$

2. *c^4 has 16 vertices, 32 edges, 24 2-faces (squares), and 8 facets (cubes). For instance, p is a vertex, $[a, i]$ is an edge, the square $\operatorname{conv}(f, g, n, o)$ is a 2-face, and the cube $\operatorname{conv}(a, b, c, d, i, j, k, l)$ is a facet.*

To illustrate how these sets satisfy Definition 7.12, consider the facet $\operatorname{conv}(a, b, c, d)$ and the vertex $\{a\}$ of c^3. Note that $\operatorname{conv}(a, b, c, d)$ is the intersection of c^3 with the plane through a, b, and c (which is a supporting hyperplane of c^3 in $\mathbb{R}^3$). Similarly, $\{a\}$ is the intersection of c^3 with any plane tangent to it at the point a.

A fascinating aspect about the faces of a convex polytope is that we can define a lattice on them. The idea is that the faces can be partially ordered by inclusion.

Definition 7.13. (*face lattice of a convex polytope*) *The face lattice of a convex polytope P, denoted $L(P)$, is the lattice formed on its set of faces ordered by set* *inclusion with operations*

$$A \wedge B = A \cap B, \tag{7.15}$$

$$A \vee B = \textit{the smallest face of } P \textit{ containing } A \cup B. \tag{7.16}$$

The lattice operations of the face lattice are well-defined. The intersection of two faces of a convex polytopes is a face of the polytope [3]. It can also be shown that for any two faces of a polytope there is a unique minimal face that contains their union [3]. This face is generally not the union itself nor its convex hull. For instance if we consider c^3 (Figure 7.7), we have that neither $\{g\} \cup [e, h]$ nor $\mathrm{conv}(\{g\}, [e, h])$ is a face of c^3. Unfortunately, there is no short-hand description for the join of two faces.

A family of face lattices that is of special interest to us is that of the cubical lattices. These are the face lattices of the hypercubes. As an example, Figure 7.9 shows $L(c^3)$. Each face is represented by the set of points of which it is the convex hull. $L(c^3)$ is non-modular (and hence non-distributive) by Theorem 4.1 because it has a sublattice isomorphic to $\mathbf{N}_5$: $\{\emptyset, c^3, \{a\}, \mathrm{conv}(a, b, c, d), \{g\}\}$. This implies that $L(c^d)$ is non-modular for all $n \geq 3$ because $L(c^d)$ embeds into $L(c^{d+1})$. Thus, cubical lattices are good candidates for the study of ST-distributivity and ST-modularity.

We finish this section by looking at polytopes from a different perspective. Specifically, we study a polytope as a graph whose vertices are its "face" vertices (zero-dimensional faces) and whose edges are its "face" edges (one-dimensional faces). This allows us to apply graph theory to convex polytopes.

We make a few remarks regarding convex polytopes as graphs. First, we denote

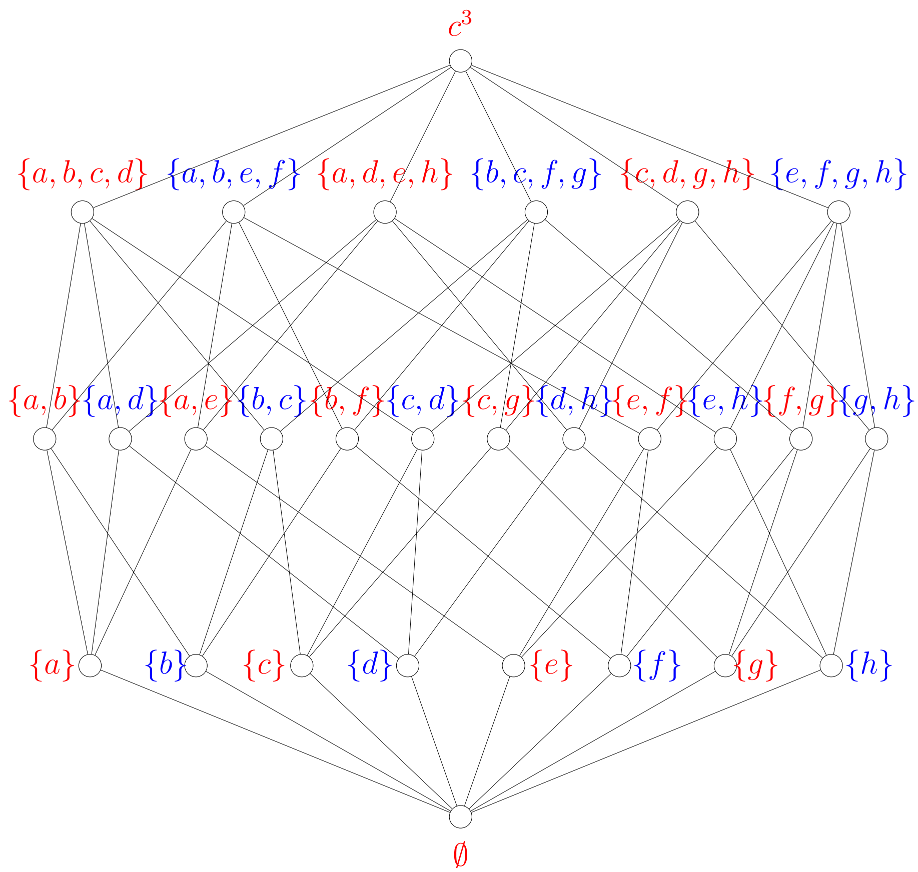


Figure 7.9: The face lattice of c^3 ($L(c^3)$)

by vert(P) the vertex set of a convex polytope P. Second, we look at the subgraphs of a convex polytope. We can easily see that if F is face of P, then F is a subgraph of P and hence, vert(F) $\subseteq$ vert(P). On the other hand, not all subgraphs of P are faces of P. However, these non-face subgraphs may still be of interest as we will see in Section 7.5 where we will consider subgraphs that are complexes.

7.5 Cut-Complexes

In this section, our goal is to define the cut-complexes that are the basis of the new poset in Section 7.6. Cut-complexes represent ways of cutting a hypercube with hyperplanes that result in the partition of its vertex set into two subsets. They are sub-complexes of the boundary complex of a hypercube for which such a partition-inducing hyperplane exists. Understanding this will require a bit of background on complexes of convex polytopes and an additional graph-theoretic definition. We begin with this and then explain cut-complexes. We then finish by discussing a notion of isomorphic cut-complexes that leads to a list of distinct cut-complexes of a hypercube up to isomorphism. More information on complexes can be found in [13]. The reader that is only interested in convex polytopes for the sake of the application in Section 9.4, can skip this section and the next.

A complex is a collection of convex polytopes that is closed under inclusion and intersection. This means that if a polytope belongs to a complex so do all of its faces. Similarly, if two polytopes in the collection have non-empty intersection, then this intersection must be a polytope that belongs to the complex.

Definition 7.14. (*complex*) *A complex is a collection C of convex polytopes in which:*

1. *If $P \in C$ and F is a face of P, then $F \in C$.*

2. *If $P_1, P_2 \in C$, then $P_1 \cap P_2 \in C$.*

Example 7.13. (*complex*) *Consider the triangle $T = \operatorname{conv}(a, b, c)$ and the square $S = \operatorname{conv}(b, c, d, e)$ shown in Figure 7.10. Then the set of all faces of T and S is a complex C explicitly given by*

$$C = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, [a, b], [b, c], [c, a], [c, d], [d, e], [e, b], T, S\}. \tag{7.17}$$

Note that $S \cap T = [b, c] \in C$ and that the intersection of any two edges is a vertex of either S or T which is already in C.

Example 7.14. (*no inclusion*) *If C is the complex of Example 7.13, then the collection $D = C \setminus \{[a, b]\}$ is not a complex because it is not closed under inclusion of faces: $T \in D$ and $[a, b]$ is a face of T but $[a, b] \notin D$.*

Example 7.15. (*no intersection*) *If we take Figure 7.10 and add a point f below T and line segment $U = [b, f]$, we get Figure 7.11. Define $E = C \cup \{U, \{f\}\}$, which consists of all of the faces of S, T, and U. Then E is not a complex because $T, U \in E$ but $T \cap U \notin E$.*

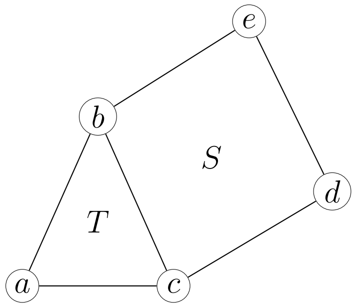


Figure 7.10: Complex of Example 7.13

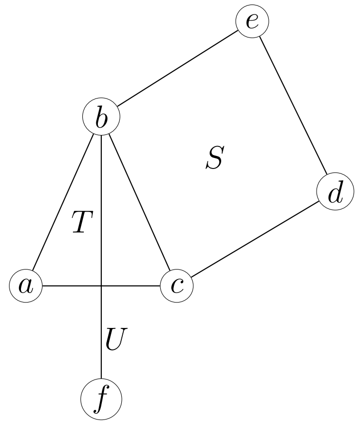


Figure 7.11: Non-complex of Example 7.15

A complex that is of special interest to us is the boundary complex. It can be defined for any given convex polytope but here we will limit ourselves to the hypercube. The boundary complex of a hypercube is the complex formed by all of its faces except the entire hypercube itself. In essence, it describes the facial structure of the boundary between a hypercube and the rest of the Euclidean space it inhabits.

Definition 7.15. (*boundary complex*) *The boundary complex of the hypercube c^d, denoted $B(c^d)$, is the complex consisting of all of the faces of c^d except c^d itself. If $F_{k,1}, ..., F_{k,m_k}$ are all of the k-faces of c^d, then*

$$B(c^d) = \bigcup_{k=-1}^{k=d-1} \{F_{k,1}, ..., F_{k,m_k}\}, \tag{7.18}$$

where $k = -1$ is admitted because $\dim(\emptyset) = -1$.

Example 7.16. (*boundary of* c^3) *The following is the boundary complex of the 3-cube using the labels of Figure 7.7:*

$$\begin{aligned} B(c^3) = \{&\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, \{g\}, \{h\}, \\ &[a, b], [b, c], [c, d], [d, a], [e, f], [f, g], \\ &[g, h], [h, e], [a, e], [b, f], [c, g], [d, h], \\ &\text{conv}(a, b, c, d), \text{conv}(e, f, g, h), \text{conv}(a, d, e, h), \\ &\text{conv}(b, c, f, g), \text{conv}(a, b, e, f), \text{conv}(c, d, g, h)\}. \end{aligned} \tag{7.19}$$

Having introduced complexes, we turn our attention to complexes contained in other complexes. Similar to other objects in mathematics such as sublattices, subgroups, subgraphs, and subspaces, we have sub-complexes. By a sub-complex we mean a sub-collection of a complex that is itself a complex (i.e. closed under inclusion and intersection). Of particular concern to us will be sub-complexes induced by a subgraph of the vertex graph of a hypercube. We formalize and illustrate this.

Definition 7.16. (*sub-complex*) *A sub-complex of a complex C is a subset D of C that is closed under containment of faces and intersection of polytopes.*

Example 7.17. (*sub-complex*) *If we consider the complex C of Example 7.13 and let $D = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, [a, b], [b, c], [c, a], [c, d]\}$, then D is a sub-complex of C consisting of the triangle T plus the edge $[c, d]$ (plus all of their faces).*

Definition 7.17. (*sub-complex induced by subgraph*) *Given a subgraph G of the vertex graph of a hypercube c^d, the sub-complex (of $B(c^d)$) induced by G is the complex C consisting of the following:*

1. *the empty set* $\emptyset$*,*

2. *all the vertices of* G*,*

3. *all the edges of* G*,*

4. *all of the higher-dimensional faces whose edges are all in* G*.*

Example 7.18. (*sub-complex induced by subgraph*) *If* G *is the subgraph of* c^3 *induced by the set of vertices* $\{a, b, c, d, e, f\}$ *(see Figure 7.7), then the sub-complex of* $B(c^3)$ *induced by* G *is the complex*

$$\begin{aligned} C = \{&\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, \{e\}, \{f\}, [a, b], [b, c], [c, d], [d, a], [e, f], [a, e], [b, f], \\ &\operatorname{conv}(a, b, c, d), \operatorname{conv}(a, b, e, f)\}, \end{aligned} \tag{7.20}$$

which consists precisely of the empty set, the vertices and edges of G*, and the two square faces of* c^3 *whose edges are all in* G*.*

In order to finish setting the stage for cut-complexes, we present the graph node-complement of a subgraph of a given graph (not to be confused with the complement of a graph).

Definition 7.18. (*graph node-complement*) *Given a subgraph* H *of a graph* G*, its graph node-complement* $\widetilde{H}$ *is the subgraph of* G *induced by the vertices of* G *that are not in* H*.*

Example 7.19. (*graph node-complement*) *If we let* G *be the graph of the square* c^2 *of Figure 7.6 and* H *be the subgraph corresponding to its face* $[a, b]$*, then* $\widetilde{H}$ *is the subgraph of* G *induced by* $\operatorname{vert}(c^2) \setminus \operatorname{vert}([a, b])$*: the edge* $[c, d]$*.*

We can finally introduce cut-complexes. These are complexes of a hypercube that represent a cut of the hypercube by a hyperplane. Precisely, a cut-complex of a hypercube is a sub-complex of the boundary complex for which there is a hyperplane of the appropriate Euclidean space that strictly separates its vertices from those of its graph node-complement in the hypercube graph.

Definition 7.19. (*cut-complex*) *A cut-complex of the hypercube* c^d *is a sub-complex* C *of the boundary complex* $B(\mathrm{c}^d)$ *such that there exists a hyperplane* H *of* $\mathbb{R}^d$ *strictly separating* $\mathrm{vert}(C)$ *and* $\mathrm{vert}(\widetilde{C})$ *in the sense that*

$$\mathrm{vert}(C) \subseteq \mathrm{int}(H^+) \text{ and } \mathrm{vert}(\widetilde{C}) \subseteq \mathrm{int}(H^-). \tag{7.21}$$

It represents a graph cut of the graph of c^d*.*

Example 7.20. (*cut-complex of square*) $C = \{\emptyset, \{a\}, \{b\}, [a, b]\}$ *is a cut-complex of* c^2*. It is shown in Figure 7.12. Note that* H *is a line* (*hyperplane in* $\mathbb{R}^2$) *that splits* $\mathrm{vert}(C) = \{a, b\}$ *from* $\mathrm{vert}(\widetilde{C}) = \{c, d\}$*.*

Example 7.21. (*cut-complex of cube*) *We claim that*

$$C = \{\emptyset, \{a\}, \{b\}, \{c\}, \{d\}, [a, b], [b, c], [c, d], [d, a], \mathrm{conv}(a, b, c, d)\} \tag{7.22}$$

is a cut-complex of c^3*. Figure 7.13* (*left*) *shows a plane* H *that splits* $\mathrm{vert}(C) = \{a, b, c, d\}$ *from* $\mathrm{vert}(\widetilde{C}) = \{e, f, g, h\}$*.*

We remark that the sub-complex of the boundary complex induced by the graph node-complement of a cut-complex is also a cut-complex given that we can re-use the

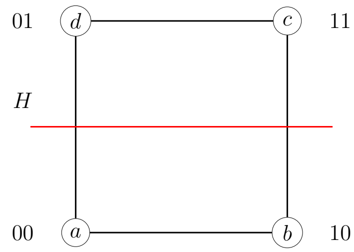


Figure 7.12: Cut-complex of square (c^2) with splitting hyperplane H

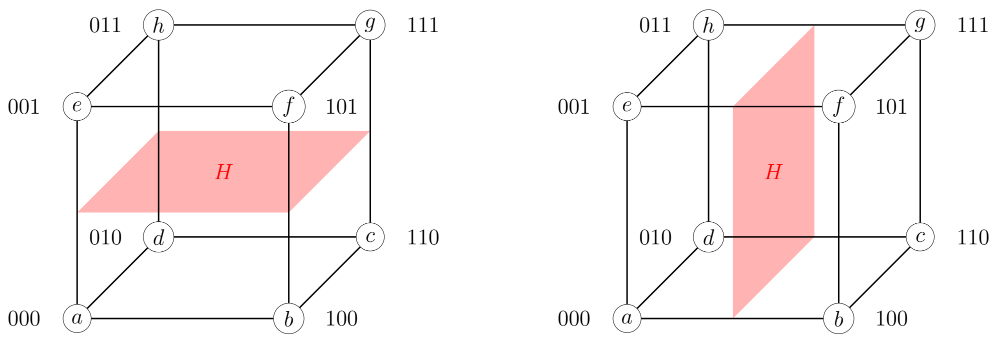


Figure 7.13: Two cut-complexes of cube (c^3) each with a splitting hyperplane H

same hyperplane to get the desired partition of the vertices. For instance, in Example 7.20, $D = \{\emptyset, \{c\}, \{d\}, [c, d]\}$ is also a cut-complex of the square.

An important observation to make about cut-complexes is that some of them have the same complex structure. In other words, they are the same complex up to the labels of the vertices they contain. This is described formally with complex isomorphisms. We will define these using bijective mappings between complex memebers following [13] except that we do not exclude the empty set sub-complex. They can also be defined in terms of isometries of $\mathbb{R}^d$ that are symmetries of the hypercube [19]. Note that by a *face of a complex* we mean a face of any convex polytope that is in the complex (including the polytopes themselves).

Definition 7.20. (*isomorphic complexes*) *Two complexes C and C' of convex polytopes are said to be isomorphic if there exists an inclusion-preserving bijection ϕ between their faces. By inclusion-preserving we mean that if F_1 and F_2 are faces of C with $F_1 \subseteq F_2$, then $\phi(F_1) \subseteq \phi(F_2)$ in C'.*

Isomorphic cut-complexes can also be described with poset isomorphisms. The idea is to define a poset on the set of faces of a complex using the inclusion order. This is a generalization of the face lattice of a convex polytope (Definition 7.13) except that this poset will not be a lattice unless the complex consists of exactly one polytope and its faces. For instance, the poset of the complex in Example 7.13 (Figure 7.10) has two maximal faces given by the triangle T and the square S. Consequently, $T \vee S$ does not exist in it. Given this perspective, two complexes are isomorphic if and only if their corresponding posets are order-isomorphic (Definition 2.22): the inclusion-preserving bijection becomes an order-isomorphism. This is useful to keep in mind during the following example.

Example 7.22. (*isomorphic cut-complexes of cube*) *Consider again the cut-complex C of the cube in Example 7.21. Figure 7.13* (*right*) *shows that*

$$D = \{\emptyset, \{a\}, \{d\}, \{e\}, \{h\}, [a, d], [d, h], [h, e], [e, a], \mathrm{conv}(a, d, e, h)\} \tag{7.23}$$

is also a cut-complex of the cube. Note that C and D are isomorphic. The function

ϕ from the set of faces of C to that of D defined by

$$\begin{aligned}
\phi(a) &= a & \phi([x,y]) &= [\phi(x),\phi(y)]\ \forall x,y \in \mathrm{vert}(C) \\
\phi(b) &= d & & \\
\phi(c) &= h & \phi(\mathrm{conv}(a,b,c,d)) &= \mathrm{conv}(\phi(a),\phi(b),\phi(c),\phi(d)) \\
\phi(d) &= e & \phi(\emptyset) &= \emptyset
\end{aligned} \tag{7.24}$$

gives the necessary inclusion-preserving bijection or order-isomorphism.

Given this identification of isomorphic cut-complexes, we can list the distinct cut-complex up to isomorphism of a hypercube by taking an unlabeled representative of each isomorphic class. This list of cut-complex up to isomorphism is the basis of the cut-complex poset of the next section. In addition, note that in practice we can get a sense of all of the cut-complexes by listing only roughly half of the cut-complexes because the graph node-complement of a cut-complex is also a cut-complex. We say roughly because there are cut-complexes that are isomorphic to their graph node-complement. We conclude this section showcasing this in the 4-cube.

Example 7.23. (*cut-complexes of the tesseract*) *Figure 7.14 gives a list of 14 distinct cut-complexes up to isomorphism of the 4-cube c^4. Adding their respective complements $\widetilde{C}_i = C_{16-i}$ and $\widetilde{C}'_i = C'_{16-i}$ for $i \neq 8$ gives all 25 distinct cut-complexes of c^4. We specify $i \neq 8$ because C_8, C'_8, and C''_8 are all self-complements.*

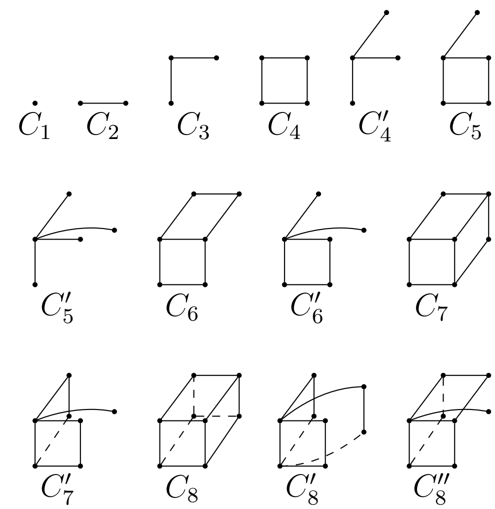


Figure 7.14: Cut-Complexes of 4-cube

7.6 Cut-Complex Poset

As promised at the beginning of the chapter, we define a poset on the cut-complexes of the 4-cube up to isomorphism. For instance, C_2 (see Figure 7.14) may be any edge of the 4-cube but is still only one element of poset. We also show that the resulting poset is a distributive lattice. This poset construction could be extended to any other hypercube, but we will limit ourselves to the 4-cube here.

We begin by defining our proposed order relation on the cut-complexes of the 4-cube. We define first its covering relation and then use that to define its order relation. Recall that given a cut-complex C, $\text{vert}(C)$ and $\widetilde{C}$ denote its vertex set and its graph node-complement respectively.

Definition 7.21. (*Poset of Cut-Complexes of 4-cube*) *Let $\mathcal{C}c(C^4)$ be the set of cut-complexes of C^4. We define an order $\leq$ on $\mathcal{C}c(C^4)$ as follows. Let C and C' be cut-complexes of C^4.*

1. *covering relation: We say that C covers C' if* $\mathrm{vert}(C) = \mathrm{vert}(C') \cup \{x\}$ *where x is obtained by applying Lemma 7.1 to* $\mathrm{vert}(C')$ *and* $\mathrm{vert}(\widetilde{C}')$.

2. *order relation: We say that $C \geq C'$ if there is a finite sequence of cut-complexes $C = C_1, C_2, ..., C_k = C'$ such that C_i covers C_{i+1} for each i.*

Proposition 7.4. *($\mathcal{C}c(C^4)$ is poset) The relation $\leq$ defined on $\mathcal{C}c(C^4)$ in Definition 7.21 is a partial order relation. That is, $\langle \mathcal{C}c(C^4); \leq \rangle$ is a poset.*

Proof *We show that $\leq$ is an order relation.*

Reflexive: If $C \in \mathcal{C}c(C^4)$, then $C \leq C$ because C is a one-element sequence that vacuously satisfies the covering relation condition of item 2.

Antisymmetric: First, observe that by definition of the covering relation , D covers D' implies that $|\mathrm{vert}(D)| = |\mathrm{vert}(D')| + 1$ *for any $D, D' \in \mathcal{C}c(C^4)$. Then $D > D'$ implies that* $|\mathrm{vert}(D)| > |\mathrm{vert}(D')|$ *by how the order relation is defined from the covering relation. Now, suppose that C and C' are cut-complexes of the 4-cube such that $C \leq C'$ and $C \geq C'$. If $C \neq C'$, then this implies that* $|\mathrm{vert}(C)| < |\mathrm{vert}(C')|$ *and* $|\mathrm{vert}(C)| > |\mathrm{vert}(C')|$ *as a result of the above observation. This is not possible. Therefore, $C = C'$.*

Transitive: If $C \geq C'$ and $C' \geq C''$, then the finite sequences of covering relations that go from C to C' and from C' to C'' can be concatenated to get a finite sequence from C to C''. Therefore, $C \geq C''$. □

The Hasse diagram of the resulting poset is shown in Figure 7.15 (see Figure 7.14 for the notation used to identify the cut-complexes). It is an order by inclusion of vertices up to isomorphism. Note that for any $i \geq 8$, $C_i = \widetilde{C}_{16-i}$ and $C'_i = \widetilde{C}'_{16-i}$. We

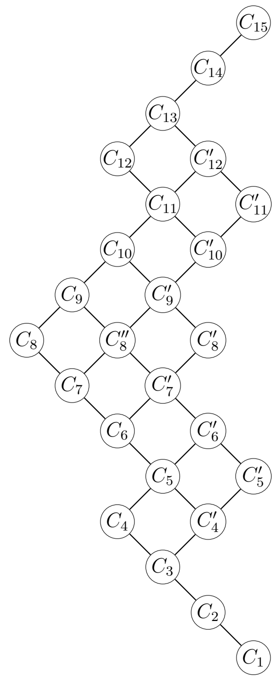


Figure 7.15: $\mathcal{C}c(C^4)$: cut-complex poset of 4-cube

conclude this discussion by proving that $\langle \mathcal{C}c(C^4); \leq \rangle$ is a distributive lattice.

Proposition 7.5. ($\mathcal{C}c(C^4)$ *distributive lattice*) *The poset $\mathcal{C}c(C^4)$ is a distributive lattice.*

Proof *We show that $\mathcal{C}c(C^4)$ is a sublattice of $\mathbf{8} \times \mathbf{8}$. Since $\mathbf{8} \times \mathbf{8}$ is distributive (product of chains), it follows that $\mathcal{C}c(C^4)$ is distributive. By observing Figure 7.16, we can see that $\mathcal{C}c(C^4)$ is a non-empty subset of $\mathbf{8} \times \mathbf{8}$. It then suffices to show that it is closed under the join and meet operations of $\mathbf{8} \times \mathbf{8}$. This is trivial for any comparable pair of elements. Thus, we need only to consider the 2-element antichains of $\mathcal{C}c(C^4)$.*

Table 7.2 lists all such antichains along with their meets and joins. It is constructed by examining Figure 7.16. First, we must identify the antichains. Clearly, C_1, C_2, C_3, C_{13}, C_{14}, and C_{15} cannot form an antichain because they are comparable to all other cut-complexes in the poset. Hence, we need only to consider C_i and C'_j for

$4 \leq i, j \leq 12$ and C''_8. Observe also that all non-prime cut complexes are comparable to each other, that is, $C_i \leq C_j$ or $C_i \geq C_j$ for all i and j. The same holds for the primes (i.e. $C'_i \leq C'_j$ or $C'_i \geq C'_j$). As a result, we must consider only pairs of a non-prime with a prime or those with C''_8. It is worth noting that $\{C_i, C'_i\}$ is always an antichain for $4 \leq i \leq 12$.

We construct the table by considering all non-primes in increasing order of index and checking which primes (or C''_8) form an antichain with it. For instance, when we consider C_4, we note that only C'_4 and C'_5 form an antichain with it, leading to the first two columns of the upper half of Table 7.2. Once we are done with this we must only consider whether each prime can be paired with C''_8, which results in the last column of the lower half of the table.

With all the 2-element antichains listed, we find their meets and joins using Figure 7.16. These are in the third and fourth rows of both halves of Table 7.2. It can be observed that they are all contained in $\mathcal{C}c(C^4)$. Therefore, $\mathcal{C}c(C^4)$ is a sublattice of $\mathbf{8} \times \mathbf{8}$ and we are done. $\square$

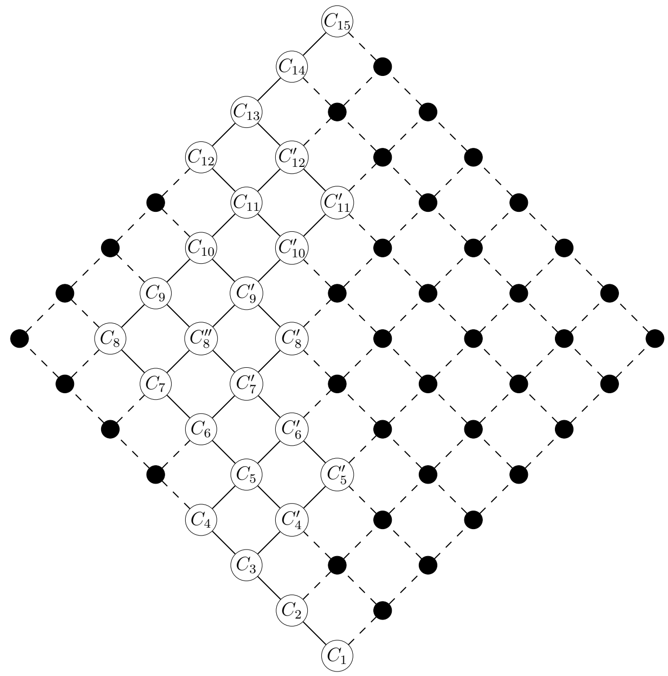


Figure 7.16: $\mathcal{C}c(C^4)$ as a subset of $\mathbf{8} \times \mathbf{8}$: Labeled white vertices and solid lines correspond to $\mathcal{C}c(C^4)$.

x	C_4	C_4	C_5	C_6	C_6	C_7	C_7	C_7	C_8	C_8	C_8	C_8	C_8
y	C'_4	C'_5	C'_5	C'_5	C'_6	C'_5	C'_6	C'_7	C'_5	C'_6	C'_7	C'_8	C''_8
$x \wedge y$	C_3	C_3	C'_4	C'_4	C_5	C'_4	C_5	C_6	C'_4	C_5	C_6	C_6	C_7
$x \vee y$	C_5	C'_6	C'_6	C'_7	C'_7	C''_8	C''_8	C''_8	C_9	C_9	C_9	C_{10}	C_9

x	C_8	C_8	C_8	C_9	C_9	C_9	C_9	C_{10}	C_{10}	C_{11}	C_{12}	C_{12}	C'_8
y	C'_9	C'_{10}	C'_{11}	C'_8	C'_9	C'_{10}	C'_{11}	C'_{10}	C'_{11}	C'_{11}	C'_{11}	C'_{12}	C''_8
$x \wedge y$	C_7	C_7	C_7	C'_7	C''_8	C''_8	C''_8	C'_9	C'_9	C'_{10}	C'_{10}	C_{11}	C'_7
$x \vee y$	C_{10}	C_{11}	C'_{12}	C_{10}	C_{10}	C_{11}	C'_{12}	C_{11}	C'_{12}	C'_{12}	C_{13}	C_{13}	C'_9

Table 7.2: Computations for the proof of Proposition 7.5

Chapter 8

ST-distributive Lattices

8.1 Introduction

After a long road of background material, we finally arrive at the actual research results. The main goal of our work is to propose two new classes of lattices: ST-distributive lattices and ST-modular lattices. These new classes will be based on relative distributive and modular properties that are fulfilled by certain pairs (S, T) of subsets of a lattice L that is not necessarily distributive nor modular. Naturally, we desire that distributive and modular lattices be respectively contained by these new classes (i.e. are a generalized by them). In a way, this is analogous to relative topologies in topological spaces.

This chapter introduces ST-distributive lattices. In particular, it explores one of the most basic questions regarding them: Given a lattice, which pairs of subsets satisfy this relative distributive property? Of course, this question is non-trivial only if the given lattice is non-distributive. The main objective arising from this question is to identify families of lattices with particular characterizations of the subsets that make them ST-distributive. ST-modular lattices are left for Chapter 9.

We summarize our work towards the aforementioned objective. We focus on finding the largest pairs of proper subsets (S, T) of a non-distributive lattice L for which it is ST-distributive (i.e. that satisfy our relative distributive property). These largest pairs are called maximal ST-pairs. Given the complexity of doing this in all generality, we begin with a special case: considering only pairs (S, T) that are disjoint, non-empty, and identity-excluding.

Our strategy is to use algebraic and order properties of lattices to write an algorithm that is a small but practical improvement over brute-force search. We then implement it with SageMath and apply it to two lattice families: $\mathbf{M}_n$ and $\mathbf{M}_{n,n}$. Afterwards, we use the results given by the program to theoretically study the families. In the end, we characterize the maximal ST-pairs of $\mathbf{M}_n$ and $\mathbf{M}_{n,n}$: the former has only one type of such pairs while the latter has five different types.

We outline the itinerary for our tour of ST-distributive lattices. We start with Section 8.2 which defines precisely what is an ST-distributive lattice. Section 8.3 then establishes some basic properties of these lattices. Afterwards, we specify our initial search problem and our methodology to tackle it in Section 8.4. This is followed by the study of ST-distributivity in the family of lattices $\mathbf{M}_n$ in Section 8.5. This serves as a simple example of our search problem in action. The next step is the family of lattices called $\mathbf{M}_{n,n}$. We describe it in Section 8.6 and present our results on its ST-distributivity in Section 8.7. Finally, we briefly make some connections between ST-distributive lattices and other lattice notions in Section 8.8, which ends the tour.

8.2 What is an ST-Distributive Lattice?

We present ST-distributive lattices. These are lattices that fulfill a relative distributive property in relation to certain ordered pairs of subsets. The idea is that given a lattice L with two subsets $S, T \subseteq L$, L is called ST-distributive if all elements of S can be distributed into any two elements of T in both ways: meet into join and join into meet. The formal definition follows.

Definition 8.1. (ST*-distributive Lattice*). *Given a lattice L with subsets $S, T \subseteq L$, we define:*

- *ST-meet Distributive Lattice: L is said to be ST-meet distributive if for all $s \in S$ and $t_1, t_2 \in T$,*

$$s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee (s \wedge t_2) . \tag{8.1}$$

- *ST-join Distributive Lattice: L is said to be ST-join distributive if for all $s \in S$ and $t_1, t_2 \in T$,*

$$s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge (s \vee t_2) . \tag{8.2}$$

- *ST-distributive Lattice: L is said to be ST-distributive if it is both ST-meet distributive and ST-join distributive.*

We take a moment to make some remarks about this definition. First, this definition generalizes distributive lattices which are simply lattices that are ST-distributive for $S = T = L$. Second, every lattice L is vacuously ST-distributive for $S = \emptyset$ or

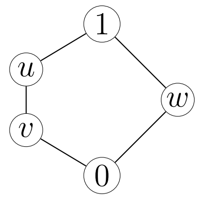


Figure 8.1: The pentagon $\mathbf{N}_5$

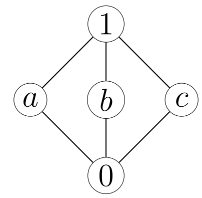


Figure 8.2: The diamond $\mathbf{M}_3$

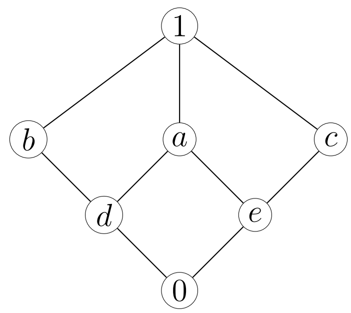


Figure 8.3: Lattice L of proof of Proposition 8.1

$T = \emptyset$. Third, we will sometimes employ the term relative distributive property to talk about the ST-distributivity of a lattice. We now provide an example of an ST-distributive lattice.

Example 8.1. (*Example of ST-distributive Lattice*). *Consider the lattice* $\mathbf{N}_5$ *shown in Figure 8.1. We already established in Section 4.2 that it is non-distributive. Nevertheless, if we let* $S = \{u, v\}$ *and* $T = \{w, 0\}$*, then we have that it is ST-distributive. Verifying this requires checking that it is both ST-meet distributive and ST-join distributive. Table 8.1 gives the necessary computations for the case* $s = u$ *in Equations* (*8.1*) *and* (*8.2*). *Those for* $s = v$ *are identical.*

In practice, performing all the computations done in Example 8.1 will not be necessary. We will show that the order structure of the lattice will guarantee that certain triples (s, t_1, t_2) satisfy Equations (8.1) and (8.2). The details can be found in Property 8.1 of Section 8.3.

ST-meet	ST-join
$u \wedge (w \vee 0) = 0$	$u \vee (w \wedge 0) = u$
$(u \wedge w) \vee (u \wedge 0) = 0$	$(u \vee w) \wedge (u \vee 0) = u$
$u \wedge (0 \vee w) = 0$	$u \vee (0 \wedge w) = u$
$(u \wedge 0) \vee (u \wedge w) = 0$	$(u \vee 0) \wedge (u \vee w) = u$
$u \wedge (0 \vee 0) = 0$	$u \vee (0 \wedge 0) = u$
$(u \wedge 0) \vee (u \wedge 0) = 0$	$(u \vee 0) \wedge (u \vee 0) = u$
$u \wedge (w \vee w) = 0$	$u \vee (w \wedge w) = 1$
$(u \wedge w) \vee (u \wedge w) = 0$	$(u \vee w) \wedge (u \vee w) = 1$

Table 8.1: Computations to show $\mathbf{N}_5$ is ST-distributive in Example 8.1

We now briefly discuss our new definition using some illustrative examples. Recalling that a distributive lattice can be defined using either the distributive property or its dual (see Proposition 4.3), it is natural to ask if ST-meet distributive lattices and ST-join distributive lattices really need to be defined separately. The answer is yes. The proof of the following proposition gives a counter-example showing that ST-meet distributive and ST-join distributive are not equivalent in general. Note that it uses the same lattice of Example 4.8.

Proposition 8.1. (ST*-meet Distributive* $\not\Leftrightarrow$ ST*-join Distributive*). *Let* L *be a lattice with* $S, T \subseteq L$*. Then* ST*-meet distributive and* ST*-join distributive are not equivalent conditions on* L*.*

Proof *We give a counter-example. Consider the lattice* $L = \{0, a, b, c, d, e, 1\}$ *shown in Figure 8.3. Let* $S = \{a\}$ *and* $T = \{b, c\}$*. Then* L *is* ST*-meet distributive but not* ST*-join distributive.*

ST-meet Distributive: There are four cases:

$$a \wedge (b \vee c) \qquad a \wedge (c \vee b) \qquad a \wedge (b \vee b) \qquad a \wedge (c \vee c)\,. \tag{8.3}$$

Observe that the second follows from the first by commutativity of lattice operations while the last two are immediate by idempotency. As a result, it is sufficient to verify only the first:

$$a \wedge (b \vee c) = a \wedge 1 = a = d \vee e = (a \wedge b) \vee (a \wedge c)\,. \tag{8.4}$$

Not ST-join Distributive: Note that

$$a \vee (b \wedge c) = a \vee 0 = a \neq 1 = 1 \wedge 1 = (a \vee b) \wedge (a \vee c)\,. \tag{8.5}$$

Therefore, L is ST-meet distributive but not ST-join distributive for $S = \{a\}$ and $T = \{b, c\}$. □

Another important point to make is that the subsets S and T in our definition are generally not interchangeable, or in other words, that the pair (S, T) is ordered. The proof of the following proposition gives an example showing this.

Proposition 8.2. *(ST-distributive $\not\Leftrightarrow$ TS-distributive). Let L be a lattice with $S, T \subseteq L$. Then ST-distributive and TS-distributive are not equivalent conditions on L.*

Proof *We give a counter-example. Consider the lattice* $\mathbf{M}_3$ *shown in Figure 8.2. Let* $S = \{a, b\}$ *and* $T = \{c\}$*. Then* $\mathbf{M}_3$ *is* ST*-distributive but not* TS*-distributive.*

ST-distributive: This follows from idempotency of lattice operations because T *only has one element. For instance,*

$$a \wedge (c \vee c) = a \wedge c = (a \wedge c) \vee (a \wedge c)\,. \tag{8.6}$$

A similar argument works for the case $s = b$ *in Equation (8.1) and for Equation (8.2) with both possible values of* s*.*

Not TS-distributive: Observe that

$$c \wedge (a \vee b) = c \wedge 1 = c \neq 0 = 0 \vee 0 = (c \wedge a) \vee (c \wedge b)\,. \tag{8.7}$$

Therefore, $\mathbf{M}_3$ *is* ST*-distributive but not* TS*-distributive given* $S = \{a, b\}$ *and* $T = \{c\}$*.* $\square$

We conclude this section by introducing a notion of maximality to ST-distributive lattices. Specifically, we define a maximal ST-pair of a lattice. This is a pair (S, T) of proper subsets of a lattice that makes it ST-distributive but that cannot be further augmented without either, breaking our relative distributive property or becoming the whole lattice. The restriction to proper subsets is done to enable a connection between ST-distributive lattices and proper sublattices in Section 8.8.

Definition 8.2. (*Maximal ST-pair*). *Let S and T be proper subsets of L. A pair (S,T) is called a maximal ST-pair of L if:*

1. *L is ST-distributive.*

2. *There is no proper $S^{'} \supsetneq S$ such that L is $S^{'}T$-distributive.*

3. *There is no proper $T^{'} \supsetneq T$ such that L is $ST^{'}$-distributive.*

Example 8.2. (*Maximal and Non-maximal ST-pairs*). *Recall the pair of (proper) subsets $S = \{u, v\}$ and $T = \{w, 0\}$ from Example 8.1. Although $\mathbf{N}_5$ is ST-distributive, this pair is not a maximal ST-pair because $\mathbf{N}_5$ is $S'T'$-distributive for $S' = \{0, u, v, w\}$ and $T' = \{0, 1, w\}$. This implies that $\mathbf{N}_5$ is $S^{'}T$-distributive with $S^{'} \supsetneq S$ and hence, that (S,T) does not satisfy condition 2 of Definition 8.2.*

Now, (S', T') is a maximal ST-pair of $\mathbf{N}_5$. Clearly, S' cannot be expanded further without becoming $\mathbf{N}_5$. On the other hand, adding either u or v to T breaks the relative distributive property because $u \wedge (v \vee w)$ and $v \vee (u \wedge w)$ do not distribute.

8.3 Basic Properties

Having established the definition of an ST-distributive lattice, we now survey some of its basic properties. We bring special attention to two of them: the efficiency criteria and the closure of S's given fixed T. These will speed-up our search of subsets inducing ST-distributivity in Section 8.4.

We begin with the efficiency criteria stated in Property 8.1 which provides three sufficient conditions on a triple of elements a, b, and c of a lattice for the distribution of the meet (or join) of the first element into the join (or meet) of the other two. The conditions all consists on having certain order relations among the elements of the triple. The advantage that this criteria brings is that for some triples, we can determine distribution without computing the usual meets and joins. We simply compare the elements instead.

Property 8.1. (*Efficiency Criteria*). *Let L be a lattice with $a, b, c \in L$ such that the triple (a, b, c) satisfies any of the following conditions:*

1. *$b \leq c$ or $b \geq c$,*

2. *$a \geq b$ and $a \geq c$,*

3. *$a \leq b$ and $a \leq c$.*

Then the following hold:

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)\,, \tag{8.8}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)\,. \tag{8.9}$$

Proof *We show only that each condition implies Equation (8.8). Duality gives Equation (8.9).*

Condition 1: By commutativity, it is sufficient to show the result for only one of the two inequalities of condition 1. Without loss of generality, suppose that $b \leq c$. Then $a \wedge b \leq a \wedge c$. Applying the Connecting Lemma (Lemma 3.1), we get

$$a \wedge (b \vee c) = a \wedge c = (a \wedge b) \vee (a \wedge c)\,. \tag{8.10}$$

Condition 2: Suppose that $a \geq b$ and $a \geq c$. Then by definition of $\vee$ as the supremum,

$$a \geq b \vee c \implies a \wedge (b \vee c) = b \vee c. \tag{8.11}$$

On the other hand, $a \geq b$ and $a \geq c$ also imply that $a \wedge b = b$ and $a \wedge c = c$. Therefore,

$$a \wedge (b \vee c) = b \vee c = (a \wedge b) \vee (a \wedge c)\,. \tag{8.12}$$

Condition 3: This is similar to the proof for condition 2 except that we get

$$a \wedge (b \vee c) = a = a \vee a = (a \wedge b) \vee (a \wedge c)\,. \tag{8.13}$$

Therefore, the Efficiency Criteria holds. □

We comment a bit on Property 8.1. A natural question arising from conditions 2 and 3 is what happens if a is comparable to both b and c but in different ways. This results in either $b \leq a \leq c$ or $c \leq a \leq b$ and hence, condition 1 holds by transitivity of $\leq$. Thus, there is no need to list this as a separate condition. Furthermore, a simple yet powerful corollary of Property 8.1 is that we can always add 0 and 1 to any S or T without affecting the relative distributive property. If $a = 0$ or $a = 1$, condition 2 or 3 is satisfied and if either b or c is 0 or 1, then condition 1 is satisfied. Finally, we also get the following useful fact.

Example 8.3. (T-chain). *Let L be any lattice (finite or infinite), S any subset of L, and T any chain of L. Then L is ST-distributive by Property 8.1, condition 1.*

We now apply the algebra of sets to ST-distributive lattices. We start with the case in which we are given a lattice L and a fixed subset $T \subseteq L$. We study how the sets $S \subseteq L$ that make L ST-distributive behave under set operations. It is immediate that such sets are closed under intersection. It can also be shown that they are closed under union.

Property 8.2. (*Closure of Intersection of S's with Fixed T*) *Let L be a lattice with $S_1, S_2, T \subseteq L$. If L is S_1T-distributive and S_2T-distributive, then L is $(S_1 \cap S_2)\,T$-distributive.*

Proof *Let $s \in S_1 \cap S_2$. Since L is S_1T-distributive and $s \in S_1$, we have that for all $t_1, t_2 \in T$,*

$$s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee (s \wedge t_2), \tag{8.14}$$

$$s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge (s \vee t_2); \tag{8.15}$$

which implies that L is $(S_1 \cap S_2)T$-distributive. □

Property 8.3. (*Closure of Union of S's with Fixed T*). *Let L be a lattice with $S_1, S_2, T \subseteq L$. If L is S_1T-distributive and S_2T-distributive, then L is $(S_1 \cup S_2)\,T$-distributive.*

Proof *Let $s \in S_1 \cup S_2$. Then $s \in S_1$ or $s \in S_2$. If $s \in S_1$, then for all $t_1, t_2 \in T$,*

$$s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee (s \wedge t_2)\,, \tag{8.16}$$

$$s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge (s \vee t_2) \tag{8.17}$$

because L is S_1T-distributive. The case that $s \in S_2$ is done in the same way. Therefore, L is $(S_1 \cup S_2)\,T$-distributive. $\square$

Property 8.3 has a relevant consequence that will play a central role in computing ST-distributivity in Section 8.4. It implies that for a given T, we can form a maximum S for which L is ST-distributive by checking all elements in $L \setminus T$, and selecting the ones that distribute into any pair of elements of T. This spares us of having to verify each subset of $L \setminus T$ individually.

The results of Properties 8.2 and 8.3 can be extended algebraically in an interesting way.

Lemma 8.1. (*Complete Lattice of S's with Fixed T*). *Let L be any lattice. For a fixed T, the collection of all subsets $S \subseteq L$ such that L is ST-distributive forms a complete distributive lattice of sets. The join and meet operations are given by union and intersection respectively. We denote this lattice $\mathcal{S}_D\,(L, T)$.*

Proof *Similar to Properties 8.2 and 8.3.* $\square$

The lattice $\mathcal{S}_D\,(L, T)$ is finite when L is finite. When this is so, we have that $\mathcal{S}_D\,(L, T)$ is a bounded lattice whose top element is the set of all elements in L that are meet and join distributive in T. If L is distributive, it is L itself. If not, it is a subset of L containing the desired set of step 1 of Algorithm 8.1 (it may be larger since the algorithm has additional restrictions from Problem 8.1). This subset may or may not be proper (e.g. it is all L if T is a chain).

Our study of the algebra of ST-distributive lattices has thus and by far focused on fixing T and letting S roam free. We now interchange their roles by fixing S and letting T vary. The algebraic results that we get are weaker in this case. We show that the T's that make L ST-distributive are closed under intersection but not under union.

Property 8.4. (*Closure of Intersection of T's with Fixed S*) *Let L be a lattice and fix a non-empty $S \subseteq L$. Let $T_1, T_2 \subseteq L$ such that L is ST_1-distributive and ST_2-distributive. Then L is $S(T_1 \cap T_2)$-distributive.*

Proof *Let $t_1, t_2 \in T_1 \cap T_2$. Then $t_1, t_2 \in T_1$. Since L is ST_1-distributive, t_1 and t_2 satisfy Equations (8.1) and (8.2) for any $s \in S$. Therefore, L is $S(T_1 \cap T_2)$-distributive.* □

Example 8.4. (*No Closure of Union of T's with Fixed S*) *Consider the lattice $\mathbf{M}_{3,3}$ shown in Figure 8.4. If $S = \{a\}$, $T_1 = \{b, d, e, f\}$, and $T_2 = \{c, d, e, f\}$, then it can be shown that $\mathbf{M}_{3,3}$ is ST_1-distributive and ST_2-distributive. However, observe that*

$$T_1 \cup T_2 = \{b, c, d, e, f\} \tag{8.18}$$

and that

$$a \wedge (b \vee c) = a \wedge 1 = a \neq f = f \vee f = (a \wedge b) \vee (a \wedge c) \tag{8.19}$$

with $a \in S$. Therefore, $\mathbf{M}_{3,3}$ is not $S(T_1 \cup T_2)$-distributive.

Taking our algebra of ST-distributivity one last step further we can wonder what happens if we do not fix neither set in the pair (S, T). The results follow naturally from the prior cases. We list them below without proof.

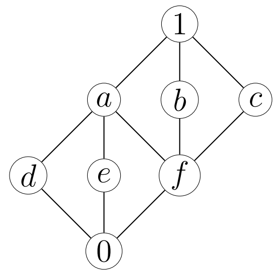


Figure 8.4: Lattice $\mathbf{M}_{3,3}$

Property 8.5. (*Algebra of ST-Distributive Lattices with Nothing Fixed*) *Let L be a lattice with subsets S_1, S_2, T_1, and T_2. Then we have the following.*

1. *S_1T_1-distributive and S_2T_2-distributive imply:*

   (a) *$(S_1 \cap S_2)(T_1 \cap T_2)$-distributive,*

   (b) *$(S_1 \cup S_2)(T_1 \cap T_2)$-distributive.*

2. *S_1T_1-distributive and S_2T_2-distributive do NOT imply:*

   (a) *$(S_1 \cap S_2)(T_1 \cup T_2)$-distributive,*

   (b) *$(S_1 \cup S_2)(T_1 \cup T_2)$-distributive.*

The final matter that we touch is the construction of new ST-distributive lattices from known ones. It was established in Section 4.3 that the distributive property of lattices is preserved by four different lattice constructs: sublattices, products of lattices, lattice homomorphisms, and dual lattices. We now extend this to ST-distributive lattices. The proofs are obtained directly from the definitions and are thus omitted.

Proposition 8.3. (*Preservation of ST-distributivity by Lattice Constructs*). *Let L be a lattice with subsets S and T such that L is ST-distributive.*

1. *If K is a sublattice of L, then K is S_1T_1-distributive for $S_1 = S \cap K$ and $T_1 = T \cap K$.*

2. *If L' is another lattice with subsets S' and T' such that L' is $S'T'$-distributive, then $L \times L'$ is $(S \times S')\,(T \times T')$-distributive.*

3. *If $\phi : L \to K$ is a lattice homomorphism that is onto, then K is $\phi\,(S)\,\phi\,(T)$-distributive.*

4. *If L^∂ represents the dual lattice of L and S and T are sublattices with duals S^∂ and T^∂, then L^∂ is $S^\partial T^\partial$-distributive.*

8.4 Search Problem and Algorithm

Our goal is to study non-distributive lattices to find the subsets S and T for which they are ST-distributive. In particular, we wish to find lattice families for which we can provide a characterization of the subsets inducing this. The first step in this direction is to tackle the following problem, which will be the focus of the rest of this chapter. For a lattice L, we denote by L^* the set of its non-identity elements, i.e. $L^* = L \setminus \{0, 1\}$.

Problem 8.1. (ST-distributive Search). *Given a non-distributive lattice L, we want to find all of its maximal ST-pairs subject to the following conditions:*

1. $S \cap T = \emptyset$;
2. $S, T \subseteq L^*$;
3. $S \neq \emptyset$ *and* $T \neq \emptyset$.

We take a moment to explain why we add additional conditions to our problem. The disjointness of S and T is for reducing the search space. We disregard 0 and 1 because their addition to any S or T does not affect the relative distributive property of the pair. This follows from Property 8.1, as mentioned earlier. Finally, the non-emptiness of both S and T focuses our search on non-trivial pairs with actual distribution of elements.

A *very important clarification* must be made before moving forward. *From now on, when we refer to a maximal ST-pair of a lattice L, we will mean a pair (S, T) that satisfies not only Definition 8.2 but also the conditions of Problem 8.1.* In particular, we emphasize that the maximality of a set of the pair will be altered by both the disjointness condition and the disregard of proper subsets of L not contained in L^*.

With the specifications of our search properly established, we present our method for carrying in out. We write a SageMath program that does an "intelligent" exhaustive search by applying Properties 8.1 and 8.3. An overview of how it works is given in Algorithm 8.1 while the code can be found in the Appendix (Program A.1). Property 8.3 allows us to build a maximum S for each T by iterating across all elements of $L^* \setminus T$, placing those that distribute in one set. The resulting pair (S, T) is a maximal

ST-pair unless there is a T' strictly larger than T that has the same maximum S. This is why we process the subsets T by increasing size. Property 8.1 reduces the computations done when deciding who can be added to S. After running the code, we manually verify the correctness and completeness of the results. This finishes the discussion of our search problem and the section.

Algorithm 8.1. *(ST-program Algorithm).*

- *Specifications:*
  1. *Input: lattice L*
  2. *Output: list of maximal ST-pairs of L with Problem 8.1 conditions*
- *Process Overview:*

  For each $T \subseteq L^*$ (by increasing size):
  1. *Build largest possible set S such that L is ST-distributive.*
     (a) *Add to the candidate set S all elements s of $L^* \setminus T$ such that s distributes into T.*
  2. *If returned S is non-empty, add pair (S, T) to list of pairs and remove any pairs contained by (S, T).*

8.5 $\mathbf{M}_n$ Results

The first lattice family in which we study Problem 8.1 is the family $\mathbf{M}_n$ for $n \geq 3$. This will provide a small and simple example of what Problem 8.1 means and how to tackle it. The results of this search are the topic of this section. In fact, we establish a complete characterization of the maximal ST-pairs for this family. We proceed in three steps: (1) review of the family $\mathbf{M}_n$, (2) computational results, and (3) theoretical results. Before we start, we introduce terminology to name an ordered triple of a lattice for which distributivity does not hold.

Definition 8.3. (*forbidden triple*) *Given a lattice L, a forbidden triple is an ordered triple of three distinct elements of L (a, b, c) such that at least one of the following two conditions holds:*

$$a \wedge (b \vee c) \neq (a \wedge b) \vee (a \wedge c), \tag{8.20}$$

$$a \vee (b \wedge c) \neq (a \vee b) \wedge (a \vee c). \tag{8.21}$$

We begin with some quick remarks about the lattices $\mathbf{M}_n$. First, recall that $\mathbf{M}_n = \mathbf{1} \oplus \bar{\mathbf{n}} \oplus \mathbf{1}$ where $\oplus$ denotes the linear sum of posets (explained in Section 2.9). Second, we will denote the elements of $\mathbf{M}_n$ by $0, 1, a_1, a_2, ..., a_n$ where 0 and 1 are the identity elements and the a_i's for i from 1 to n are the elements in the middle antichain of $\mathbf{M}_n$. See Figure 8.5 for an example with $n = 3$. Third and lastly, we note that we do our search only for $n \geq 3$ because $\mathbf{M}_2 \cong \mathbf{2}^2$ and $\mathbf{M}_1 \cong \mathbf{3}$ are distributive.

We now finally discuss the results of our search for maximal ST-pairs in. $\mathbf{M}_n$.

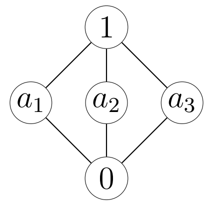


Figure 8.5: $\mathbf{M}_3$ with described notation

$\mathbf{M}_3$	
S	T
$\{a_2, a_3\}$	$\{a_1\}$
$\{a_1, a_3\}$	$\{a_2\}$
$\{a_1, a_2\}$	$\{a_3\}$

$\mathbf{M}_4$	
S	T
$\{a_2, a_3, a_4\}$	$\{a_1\}$
$\{a_1, a_3, a_4\}$	$\{a_2\}$
$\{a_1, a_2, a_4\}$	$\{a_3\}$
$\{a_1, a_2, a_3\}$	$\{a_4\}$

$\mathbf{M}_5$	
S	T
$\{a_2, a_3, a_4, a_5\}$	$\{a_1\}$
$\{a_1, a_3, a_4, a_5\}$	$\{a_2\}$
$\{a_1, a_2, a_4, a_5\}$	$\{a_3\}$
$\{a_1, a_2, a_3, a_5\}$	$\{a_4\}$
$\{a_1, a_2, a_3, a_4\}$	$\{a_5\}$

Table 8.2: Maximal ST-pairs of $\mathbf{M}_3$, $\mathbf{M}_4$, and $\mathbf{M}_5$

We run Program A.1 with $\mathbf{M}_n$ for $n = 3, 4, 5$ which returns the pairs listed in Table 8.2. We observe that all of the resulting maximal ST-pairs consist of one non-identity element in T and all of the remaining non-identity elements in S. For instance for $\mathbf{M}_3$, we have $S = \{a_1, a_2\}$ and $T = \{a_3\}$. This is not surprising because if we put two or more non-identity elements in T, any two of them will form a forbidden triple with any other non-identity element of $\mathbf{M}_n$. Lemma 8.2 formalizes this.

Lemma 8.2. (*Forbidden Triples in* $\mathbf{M}_n$) *If* $a_i, a_j, a_k \in \bar{\mathbf{n}}$ *are three distinct non-identity elements of* $\mathbf{M}_n = \mathbf{1} \oplus \bar{\mathbf{n}} \oplus \mathbf{1}$, *then*

$$a_i \wedge (a_j \vee a_k) \neq (a_i \wedge a_j) \vee (a_i \wedge a_k). \tag{8.22}$$

Proof *Note that for all* $a_i, a_j, a_k \in \bar{\mathbf{n}}$*,*

$$a_i \wedge (a_j \vee a_k) = a_i \wedge 1 = a_i \neq 0 = 0 \vee 0 = (a_i \wedge a_j) \vee (a_i \wedge a_k), \tag{8.23}$$

which implies the desired result. $\square$

We are now ready to completely describe the maximal ST-pairs of $\mathbf{M}_n$. We show that the pairs of the form found by Program A.1 are the only such pairs using Lemma 8.2. This bring the section to a close.

Proposition 8.4. (*Maximal ST-Pairs in* $\mathbf{M}_n$) *For any* $n \in \mathbb{N}$*, the maximal* ST*-pairs of* $\mathbf{M}_n$ *are exactly the pairs of sets* (S, T) *of the form* $(\mathbf{M}_n^* \setminus \{a\}, \{a\})$ *for each* $a \in \mathbf{M}_n^*$*.*

Proof *We begin by showing that pairs of the given form are maximal* ST*-pairs. Pick any* $a \in \mathbf{M}_n^*$ *and let* $T = \{a\}$*. Set* $S = \mathbf{M}_n^* \setminus \{a\}$*. Then* $\mathbf{M}_n$ *is* ST*-distributive by Property 8.1 and* (S, T) *is a maximal* ST*-pair because* $S \cup T = \mathbf{M}_n^*$*.*

We now show that there cannot be any maximal ST*-pairs that are not of this form. Suppose such a pair exists. Then we have* $S, T \subseteq \mathbf{M}_n^*$ *with* $S \cap T = \emptyset$ *and* $\mathbf{M}_n$ ST*-distributive. Then* $|T| > 1$ *because it is not of the form in the proposition statement. In particular, there exists* $t_1, t_2 \in T$ *with* $t_1 \neq t_2$*. Lemma 8.2 then implies that there can be no non-empty* $S \subseteq \mathbf{M}_n^* \setminus T$ *such that* $\mathbf{M}_n$ *is* ST*-distributive. Therefore, the maximal* ST*-pairs of* $\mathbf{M}_n$ *are those of the form* $(\mathbf{M}_n^* \setminus \{a\}, \{a\})$*.* $\square$

8.6 $\mathbf{M}_{n,n}$ Family

Now that we are done with the family $\mathbf{M}_n$, we continue our search of ST-distributive lattices with a family derived from it: $\mathbf{M}_{n,n}$. We describe it on this section and then discuss our results on it in Section 8.7. For each natural number $n \geq 3$, the lattice $\mathbf{M}_{n,n}$ is obtained by gluing two copies of $\mathbf{M}_n = \mathbf{1} \oplus \bar{\mathbf{n}} \oplus \mathbf{1}$ as follows. Take the rightmost edge from the top element in the Hasse diagram of one of the copies and make it equal to the leftmost edge from the bottom element of the other copy's diagram. Definition 8.4 formally describes the family and presents relevant notation while Example 8.5 illustrates its smallest members.

Definition 8.4. (*Lattice* $\mathbf{M}_{n,n}$). *For a natural number $n \geq 3$, the lattice $\mathbf{M}_{n,n}$ has element set $\{0, 1, a_1, ..., a_n, b_1, ..., b_n\}$ with 0 and 1 being the bottom and top element respectively. Its order relation is completely determined by the following covering relations:*

1. *0 is covered by all of the a_i's.*

2. *1 covers all of the b_j's.*

3. *a_n is covered by all the b_j's.*

4. *b_1 covers all of the a_i's.*

Note that this results in $\mathbf{M}_{n,n}$ having 2 isomorphic copies of $\mathbf{M}_n$:

$$\{0, a_1, a_2, ..., a_n, b_1\} \text{ and } \{a_n, b_1, b_2, ..., b_n, 1\}, \tag{8.24}$$

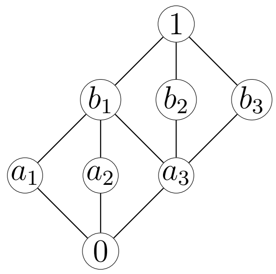


Figure 8.6: Lattice $\mathbf{M}_{3,3}$

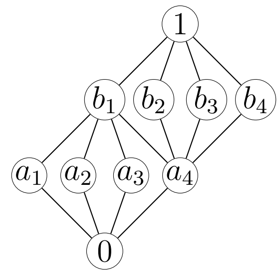


Figure 8.7: Lattice $\mathbf{M}_{4,4}$

and that both copies share a_n and b_1 (the shared edge from the pictorial description above).

Example 8.5. (*Examples of* $\mathbf{M}_{n,n}$). $\mathbf{M}_{3,3}$ *and* $\mathbf{M}_{4,4}$ *are shown in Figures 8.6 and 8.7 respectively. Note that*

$$\mathbf{M}_3 \cong \{0, a_1, a_2, a_3, b_1\} \cong \{a_3, b_1, b_2, b_3, 1\}, \tag{8.25}$$

$$\mathbf{M}_4 \cong \{0, a_1, a_2, a_3, a_4, b_1\} \cong \{a_4, b_1, b_2, b_3, b_4, 1\}. \tag{8.26}$$

We take a quick moment to discuss the family $\mathbf{M}_{n,n}$. First, we introduce some terminology for referring to particular subsets and elements of $\mathbf{M}_{n,n}$ that will facilitate the presentation of our results in the next section.

Definition 8.5. (*Level*). *In $\mathbf{M}_{n,n}$, a level refers to either of the sets $\{a_1, ..., a_n\}$ and $\{b_1, ..., b_n\}$.*

Definition 8.6. (*Link Element*). *In $\mathbf{M}_{n,n}$, a link element (or link) is one of the two elements shared by both isomorphic copies of $\mathbf{M}_n$, that is, a_n and b_1.*

Next, we remark that the lattice $\mathbf{M}_{n,n}$ is both modular and non-distributive for $n \geq 3$. Both properties follow from the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem (Theorem 4.1). $\mathbf{M}_{n,n}$

always contains isomorphic copies of $\mathbf{M}_3$ because it has two copies of $\mathbf{M}_n$, as already mentioned, for $n \geq 3$ and $\mathbf{M}_n$ always has isomorphic copies of $\mathbf{M}_k$ for all $k \leq n$. On the other hand, $\mathbf{M}_{n,n}$ never has an isomorphic copy of $\mathbf{N}_5$. This is proven for $n = 3$ in Example 4.12 and can be easily generalized for all n. All of this results in that we have a family of modular and non-distributive lattices. This gives us the convenience of studying ST-distributivity non-trivially in a relatively "controlled" environment.

We complete our introduction to the family $\mathbf{M}_{n,n}$ by justifying our specification that $n \geq 3$. Although it is possible to construct $\mathbf{M}_{2,2}$ and $\mathbf{M}_{1,1}$ following Definition 8.4, the resulting lattices would be distributive because they are isomorphic to $\mathbf{2} \times \mathbf{3}$ and $\mathbf{4}$ respectively.

8.7 $\mathbf{M}_{n,n}$ Results

Having introduced the $\mathbf{M}_{n,n}$ family of lattices in the previous section, we now go over our current progress in the study of its ST-distributivity. We start with some computational results and then present theoretical results derived from them. In particular, we identify five forms of pairs of subsets of $\mathbf{M}^*_{n,n}$ from the data, show that these forms always produce maximal ST-pairs for all n, and then prove that these forms are the only maximal ST-pairs possible. As a corollary, we count the number of maximal ST-pairs of $\mathbf{M}_{n,n}$. Throughout the whole discussion, the reader should bear in mind the clarification we made in Section 8.4 about what we mean when we refer to a maximal ST-pair.

8.7.1 Computational Results

We start by running Program A.1 on the smallest members of the family: $\mathbf{M}_{3,3}$, $\mathbf{M}_{4,4}$, and $\mathbf{M}_{5,5}$. It finds 27, 42, and 59 maximal ST-pairs respectively, which are listed in Tables 8.3, 8.4, and 8.5. Manual verification of these lists corroborates their correctness and completeness. Further study of these pairs results in identifying 5 types into which they can be classified based on the structural role of the elements involved.

Remark 8.1. (*5 Types of Maximal ST-pairs*). *All of the maximal ST-pairs of* $\mathbf{M}_{3,3}$, $\mathbf{M}_{4,4}$, *and* $\mathbf{M}_{5,5}$ *are of one of the following 5 types:*

1. T-chain: *T is a chain. S has all other elements.*

2. S-link: *S has only one of the two links. T has one more element in this link's level and all of the elements in the other level.*

3. S-2-links: *S has both links. T has one non-link element of each level*

4. S-level: *S is one of the two levels. T has two elements in the other level (including its link).*

5. S-level-minus-link: *S is one of the two levels minus its link. T is both links plus another element from the level that does not contain S.*

The type of each pair is indicated in Tables 8.3-8.5. An example of each type in $\mathbf{M}_{4,4}$ *is illustrated in Figures 8.8–8.12 with S in cyan (sky blue) and T in black.*

Table 8.3: Maximal ST-pairs of $\mathbf{M}_{3,3}$

	S	T	Type
1	$\{a_2, a_3, b_1, b_2, b_3\}$	$\{a_1\}$	1
2	$\{a_1, a_3, b_1, b_2, b_3\}$	$\{a_2\}$	1
3	$\{a_1, a_2, b_1, b_2, b_3\}$	$\{a_3\}$	1
4	$\{a_1, a_2, a_3, b_2, b_3\}$	$\{b_1\}$	1
5	$\{a_1, a_2, a_3, b_1, b_3\}$	$\{b_2\}$	1
6	$\{a_1, a_2, a_3, b_1, b_2\}$	$\{b_3\}$	1
7	$\{a_2, a_3, b_2, b_3\}$	$\{a_1, b_1\}$	1
8	$\{a_1, a_3, b_2, b_3\}$	$\{a_2, b_1\}$	1
9	$\{a_1, a_2, b_2, b_3\}$	$\{a_3, b_1\}$	1
10	$\{a_1, a_2, b_1, b_3\}$	$\{a_3, b_2\}$	1
11	$\{a_1, a_2, b_1, b_2\}$	$\{a_3, b_3\}$	1
12	$\{b_1\}$	$\{a_1, a_2, a_3, b_2\}$	2
13	$\{b_1\}$	$\{a_1, a_2, a_3, b_3\}$	2
14	$\{a_3\}$	$\{a_1, b_1, b_2, b_3\}$	2
15	$\{a_3\}$	$\{a_2, b_1, b_2, b_3\}$	2
16	$\{a_3, b_1\}$	$\{a_1, b_2\}$	3
17	$\{a_3, b_1\}$	$\{a_1, b_3\}$	3
18	$\{a_3, b_1\}$	$\{a_2, b_2\}$	3
19	$\{a_3, b_1\}$	$\{a_2, b_3\}$	3
20	$\{a_1, a_2, a_3\}$	$\{b_1, b_2\}$	4
21	$\{a_1, a_2, a_3\}$	$\{b_1, b_3\}$	4
22	$\{b_1, b_2, b_3\}$	$\{a_1, a_3\}$	4
23	$\{b_1, b_2, b_3\}$	$\{a_2, a_3\}$	4
24	$\{a_1, a_2\}$	$\{a_3, b_1, b_2\}$	5
25	$\{a_1, a_2\}$	$\{a_3, b_1, b_3\}$	5
26	$\{b_2, b_3\}$	$\{a_1, a_3, b_1\}$	5
27	$\{b_2, b_3\}$	$\{a_2, a_3, b_1\}$	5

Table 8.4: Maximal ST-pairs of $\mathbf{M}_{4,4}$

	S	T	Type
1	$\{a_2, a_3, a_4, b_1, b_2, b_3, b_4\}$	$\{a_1\}$	1
2	$\{a_1, a_3, a_4, b_1, b_2, b_3, b_4\}$	$\{a_2\}$	1
3	$\{a_1, a_2, a_4, b_1, b_2, b_3, b_4\}$	$\{a_3\}$	1

	S	T	Type
4	$\{a_1, a_2, a_3, b_1, b_2, b_3, b_4\}$	$\{a_4\}$	1
5	$\{a_1, a_2, a_3, a_4, b_2, b_3, b_4\}$	$\{b_1\}$	1
6	$\{a_1, a_2, a_3, a_4, b_1, b_3, b_4\}$	$\{b_2\}$	1
7	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_4\}$	$\{b_3\}$	1
8	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_3\}$	$\{b_4\}$	1
9	$\{a_2, a_3, a_4, b_2, b_3, b_4\}$	$\{a_1, b_1\}$	1
10	$\{a_1, a_3, a_4, b_2, b_3, b_4\}$	$\{a_2, b_1\}$	1
11	$\{a_1, a_2, a_4, b_2, b_3, b_4\}$	$\{a_3, b_1\}$	1
12	$\{a_1, a_2, a_3, b_2, b_3, b_4\}$	$\{a_4, b_1\}$	1
13	$\{a_1, a_2, a_3, b_1, b_3, b_4\}$	$\{a_4, b_2\}$	1
14	$\{a_1, a_2, a_3, b_1, b_2, b_4\}$	$\{a_4, b_3\}$	1
15	$\{a_1, a_2, a_3, b_1, b_2, b_3\}$	$\{a_4, b_4\}$	1
16	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, b_2\}$	2
17	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, b_3\}$	2
18	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, b_4\}$	2
19	$\{a_4\}$	$\{a_1, b_1, b_2, b_3, b_4\}$	2
20	$\{a_4\}$	$\{a_2, b_1, b_2, b_3, b_4\}$	2
21	$\{a_4\}$	$\{a_3, b_1, b_2, b_3, b_4\}$	2
22	$\{a_4, b_1\}$	$\{a_1, b_2\}$	3
23	$\{a_4, b_1\}$	$\{a_1, b_3\}$	3
24	$\{a_4, b_1\}$	$\{a_1, b_4\}$	3
25	$\{a_4, b_1\}$	$\{a_2, b_2\}$	3
26	$\{a_4, b_1\}$	$\{a_2, b_3\}$	3
27	$\{a_4, b_1\}$	$\{a_2, b_4\}$	3
28	$\{a_4, b_1\}$	$\{a_3, b_2\}$	3
29	$\{a_4, b_1\}$	$\{a_3, b_3\}$	3
30	$\{a_4, b_1\}$	$\{a_3, b_4\}$	3
31	$\{a_1, a_2, a_3, a_4\}$	$\{b_1, b_2\}$	4
32	$\{a_1, a_2, a_3, a_4\}$	$\{b_1, b_3\}$	4
33	$\{a_1, a_2, a_3, a_4\}$	$\{b_1, b_4\}$	4
34	$\{b_1, b_2, b_3, b_4\}$	$\{a_1, a_4\}$	4
35	$\{b_1, b_2, b_3, b_4\}$	$\{a_2, a_4\}$	4
36	$\{b_1, b_2, b_3, b_4\}$	$\{a_3, a_4\}$	4
37	$\{a_1, a_2, a_3\}$	$\{a_4, b_1, b_2\}$	5
38	$\{a_1, a_2, a_3\}$	$\{a_4, b_1, b_3\}$	5

	S	T	Type
39	$\{a_1, a_2, a_3\}$	$\{a_4, b_1, b_4\}$	5
40	$\{b_2, b_3, b_4\}$	$\{a_1, a_4, b_1\}$	5
41	$\{b_2, b_3, b_4\}$	$\{a_2, a_4, b_1\}$	5
42	$\{b_2, b_3, b_4\}$	$\{a_3, a_4, b_1\}$	5

Table 8.5: Maximal ST-pairs of $\mathbf{M}_{5,5}$

	S	T	Type
1	$\{a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5\}$	$\{a_1\}$	1
2	$\{a_1, a_3, a_4, a_5, b_1, b_2, b_3, b_4, b_5\}$	$\{a_2\}$	1
3	$\{a_1, a_2, a_4, a_5, b_1, b_2, b_3, b_4, b_5\}$	$\{a_3\}$	1
4	$\{a_1, a_2, a_3, a_5, b_1, b_2, b_3, b_4, b_5\}$	$\{a_4\}$	1
5	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, b_5\}$	$\{a_5\}$	1
6	$\{a_1, a_2, a_3, a_4, a_5, b_2, b_3, b_4, b_5\}$	$\{b_1\}$	1
7	$\{a_1, a_2, a_3, a_4, a_5, b_1, b_3, b_4, b_5\}$	$\{b_2\}$	1
8	$\{a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_4, b_5\}$	$\{b_3\}$	1
9	$\{a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_5\}$	$\{b_4\}$	1
10	$\{a_1, a_2, a_3, a_4, a_5, b_1, b_2, b_3, b_4\}$	$\{b_5\}$	1
11	$\{a_2, a_3, a_4, a_5, b_2, b_3, b_4, b_5\}$	$\{a_1, b_1\}$	1
12	$\{a_1, a_3, a_4, a_5, b_2, b_3, b_4, b_5\}$	$\{a_2, b_1\}$	1
13	$\{a_1, a_2, a_4, a_5, b_2, b_3, b_4, b_5\}$	$\{a_3, b_1\}$	1
14	$\{a_1, a_2, a_3, a_5, b_2, b_3, b_4, b_5\}$	$\{a_4, b_1\}$	1
15	$\{a_1, a_2, a_3, a_4, b_2, b_3, b_4, b_5\}$	$\{a_5, b_1\}$	1
16	$\{a_1, a_2, a_3, a_4, b_1, b_3, b_4, b_5\}$	$\{a_5, b_2\}$	1
17	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_4, b_5\}$	$\{a_5, b_3\}$	1
18	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_5\}$	$\{a_5, b_4\}$	1
19	$\{a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4\}$	$\{a_5, b_5\}$	1
20	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, a_5, b_2\}$	2
21	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, a_5, b_3\}$	2
22	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, a_5, b_4\}$	2
23	$\{b_1\}$	$\{a_1, a_2, a_3, a_4, a_5, b_5\}$	2
24	$\{a_5\}$	$\{a_1, b_1, b_2, b_3, b_4, b_5\}$	2
25	$\{a_5\}$	$\{a_2, b_1, b_2, b_3, b_4, b_5\}$	2
26	$\{a_5\}$	$\{a_3, b_1, b_2, b_3, b_4, b_5\}$	2
27	$\{a_5\}$	$\{a_4, b_1, b_2, b_3, b_4, b_5\}$	2
28	$\{a_5, b_1\}$	$\{a_1, b_2\}$	3

	S	T	Type
29	$\{a_5, b_1\}$	$\{a_1, b_3\}$	3
30	$\{a_5, b_1\}$	$\{a_1, b_4\}$	3
31	$\{a_5, b_1\}$	$\{a_1, b_5\}$	3
32	$\{a_5, b_1\}$	$\{a_2, b_2\}$	3
33	$\{a_5, b_1\}$	$\{a_2, b_3\}$	3
34	$\{a_5, b_1\}$	$\{a_2, b_4\}$	3
35	$\{a_5, b_1\}$	$\{a_2, b_5\}$	3
36	$\{a_5, b_1\}$	$\{a_3, b_2\}$	3
37	$\{a_5, b_1\}$	$\{a_3, b_3\}$	3
38	$\{a_5, b_1\}$	$\{a_3, b_4\}$	3
39	$\{a_5, b_1\}$	$\{a_3, b_5\}$	3
40	$\{a_5, b_1\}$	$\{a_4, b_2\}$	3
41	$\{a_5, b_1\}$	$\{a_4, b_3\}$	3
42	$\{a_5, b_1\}$	$\{a_4, b_4\}$	3
43	$\{a_5, b_1\}$	$\{a_4, b_5\}$	3
44	$\{a_1, a_2, a_3, a_4, a_5\}$	$\{b_1, b_2\}$	4
45	$\{a_1, a_2, a_3, a_4, a_5\}$	$\{b_1, b_3\}$	4
46	$\{a_1, a_2, a_3, a_4, a_5\}$	$\{b_1, b_4\}$	4
47	$\{a_1, a_2, a_3, a_4, a_5\}$	$\{b_1, b_5\}$	4
48	$\{b_1, b_2, b_3, b_4, b_5\}$	$\{a_1, a_5\}$	4
49	$\{b_1, b_2, b_3, b_4, b_5\}$	$\{a_2, a_5\}$	4
50	$\{b_1, b_2, b_3, b_4, b_5\}$	$\{a_3, a_5\}$	4
51	$\{b_1, b_2, b_3, b_4, b_5\}$	$\{a_4, a_5\}$	4
52	$\{a_1, a_2, a_3, a_4\}$	$\{a_5, b_1, b_2\}$	5
53	$\{a_1, a_2, a_3, a_4\}$	$\{a_5, b_1, b_3\}$	5
54	$\{a_1, a_2, a_3, a_4\}$	$\{a_5, b_1, b_4\}$	5
55	$\{a_1, a_2, a_3, a_4\}$	$\{a_5, b_1, b_5\}$	5
56	$\{b_2, b_3, b_4, b_5\}$	$\{a_1, a_5, b_1\}$	5
57	$\{b_2, b_3, b_4, b_5\}$	$\{a_2, a_5, b_1\}$	5
58	$\{b_2, b_3, b_4, b_5\}$	$\{a_3, a_5, b_1\}$	5
59	$\{b_2, b_3, b_4, b_5\}$	$\{a_4, a_5, b_1\}$	5

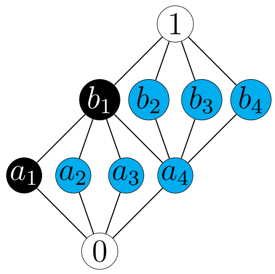


Figure 8.8: T-chain pair

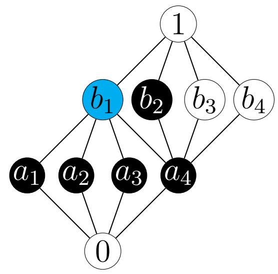


Figure 8.9: S-link pair

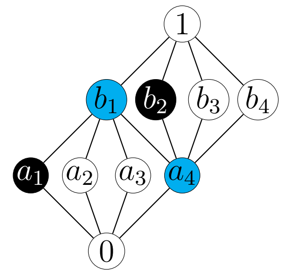


Figure 8.10: S-2-links pair

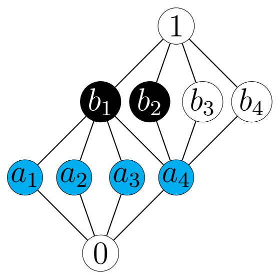


Figure 8.11: S-level pair

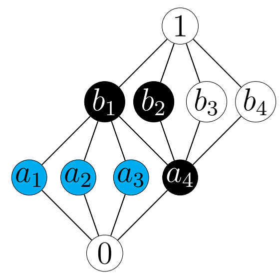


Figure 8.12: S-level-minus-link pair

8.7.2 Theoretical Results 1: Generalization of 5 Types

We now make some theoretical generalizations of our computational results. Given the findings in Remark 8.1, it is natural to ask the following two questions:

1. Do these constructions of maximal ST-pairs work for all other $\mathbf{M}_{n,n}$? $(n \geq 3)$

2. Do other forms of maximal ST-pairs appear in $\mathbf{M}_{n,n}$ for larger n's?

We already know that type T-chain will always work by Example 8.3. We prove that the remaining constructions work for all lattices of the $\mathbf{M}_{n,n}$ family and that these five constructions are the only ones possible in it. Hence, the answer to our questions are Yes and No respectively.

To show that maximal ST-pairs of types 2–5 in Remark 8.1 generalize for all n, some preliminary results are needed: the modular comparability criteria for distributivity (MCCD) and Proposition 8.6. The MCCD gives a simple condition that guarantees distribution for any triple of elements in a non-distributive but modular lattice.

Proposition 8.5. (*Modular Comparability Criteria for Distributivity — MCCD*). *Let L be a modular lattice with elements $a, b, c \in L$. If there is any comparability between any 2 of the 3 elements, then*

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)\,, \tag{8.27}$$

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)\,. \tag{8.28}$$

Proof *By duality, we need only to show Equation (8.27). There are three cases. First, If $b \leq c$ or $b \geq c$, we are done by Property 8.1. Second, if $a \leq b$ or $a \leq c$, then $a \leq b \vee c$. Thus, the Connecting Lemma and the absorption property of lattices give*

$$a \wedge (b \vee c) = a = (a \wedge b) \vee (a \wedge c)\,. \tag{8.29}$$

Finally, we consider $a \geq b$ or $a \geq c$. Suppose that $a \geq c$, then by modularity and the Connecting Lemma,

$$a \wedge (b \vee c) = (a \wedge b) \vee c = (a \wedge b) \vee (a \wedge c)\,. \tag{8.30}$$

The sub-case $a \geq b$ then follows from commutativity of $\vee$. Therefore, Equation (8.27) is satisfied whenever $\{a, b, c\}$ is not an antichain. □

The MCCD is important because it reduces the problem of checking for relative distributivity to checking only triples that are antichains. Note that the converse of MCCD is not true in general: a triple that is an antichain may distribute (e.g. a triple of singleton sets in a power set lattice). However, in $\mathbf{M}_{n,n}$, antichains never distribute.

Proposition 8.6. (*Antichains Not Distributive in* $\mathbf{M}_{n,n}$). *Suppose that* $n \geq 3$ *and that* $x, y, z \in \mathbf{M}_{n,n}$ *are distinct elements. If* $\{x, y, z\}$ *is an antichain, then*

$$x \wedge (y \vee z) \neq (x \wedge y) \vee (x \wedge z)\,, \tag{8.31}$$

$$y \wedge (x \vee z) \neq (y \wedge x) \vee (y \wedge z)\,, \tag{8.32}$$

$$z \wedge (x \vee y) \neq (z \wedge x) \vee (z \wedge y)\,. \tag{8.33}$$

Proof *There are four general ways of choosing* $x, y, z \in \mathbf{M}_{n,n}$ *such that* $\{x, y, z\}$ *is an antichain.*

Case 1: $\{x, y, z\} = \{a_i, a_j, a_k\}$*. Done by the fact that* a_i, a_j, a_k *are a forbidden triple of an isomorphic copy of* $\mathbf{M}_n$ *in* $\mathbf{M}_{n,n}$ *by Lemma 8.2.*

Case 2: $\{x, y, z\} = \{b_i, b_j, b_k\}$*. Same as Case 1.*

Case 3: $\{x, y, z\} = \{a_i, a_j, b_k\}$ *with* $i, j \neq n, k \neq 1$

$$a_i \wedge (a_j \vee b_k) = a_i \wedge 1 = a_i \neq 0 = 0 \vee 0 = (a_i \wedge a_j) \vee (a_i \wedge b_k)\,, \tag{8.34}$$

$$a_j \wedge (a_i \vee b_k) = a_j \wedge 1 = a_j \neq 0 = 0 \vee 0 = (a_j \wedge a_i) \vee (a_j \wedge b_k)\,, \tag{8.35}$$

$$b_k \wedge (a_i \vee a_j) = b_k \wedge b_1 = a_n \neq 0 = 0 \vee 0 = (b_k \wedge a_i) \vee (b_k \wedge a_j)\,. \tag{8.36}$$

Case 4: $\{x, y, z\} = \{a_i, b_j, b_k\}$ *with* $i \neq n, j, k \neq 1$

$$a_i \wedge (b_j \vee b_k) = a_i \wedge 1 = a_i \neq 0 = 0 \vee 0 = (a_i \wedge b_j) \vee (a_i \wedge b_k)\,, \tag{8.37}$$

$$b_j \wedge (a_i \vee b_k) = b_j \wedge 1 = b_j \neq a_n = 0 \vee a_n = (b_j \wedge a_i) \vee (b_j \wedge b_k)\,, \tag{8.38}$$

$$b_k \wedge (a_i \vee b_j) = b_k \wedge 1 = b_k \neq a_n = 0 \vee a_n = (b_k \wedge a_i) \vee (b_k \wedge b_j)\,. \tag{8.39}$$

Therefore, $\{x, y, z\}$ *does not distribute in any way if it is an antichain.* □

The implication of Proposition 8.6 is that for a pair of subsets S and T of a lattice L to be a maximal ST-pair, there cannot exist an antichain of three distinct elements in L that has one element in S and two in T. This motivates the following definition.

Definition 8.7. (ST*-breaking Antichain*). *Given* $S, T \subseteq \mathbf{M}^*_{n,n}$*, an* ST*-breaking antichain is an antichain* $\{x, y, z\} \subseteq \mathbf{M}_{n,n}$ *such that* $x \in S$ *and* $y, z \in T$.

We are now ready to prove that the constructions 2–5 in Remark 8.1 generalize to all $\mathbf{M}_{n,n}$. Note the extensive use of the MCCD and of ST-breaking antichains in the proofs and keep in mind our implicit assumption that $n \geq 3$.

Proposition 8.7. (S*-link*). *Let* L_1, L_2 *be the two levels of* $\mathbf{M}_{n,n}$*. Let* $l, x \in L_1$ *where* l *is the link. If* $S = \{l\}$ *and* $T = L_2 \cup \{x\}$*, then* (S, T) *is a maximal* ST*-pair of* $\mathbf{M}_{n,n}$*.*

Proof *ST-distributivity: Let* $s \in S$ *and* $t_1, t_2 \in T$*. If* $t_1 = t_2 = x$*, we are done by Property 8.1. Else,* $t_1 \in L_2$ *or* $t_2 \in L_2$*. Since* $s = l$ *(given* $S = \{l\}$*), then* s *is comparable to either* t_1 *or* t_2 *and MCCD guarantees the needed distributions.*

Maximality: Note that the only elements left in $\mathbf{M}^*_{n,n}$ *are those in* $L_1 \setminus \{l, x\}$*. Let* $y \in L_1 \setminus \{l, x\}$*. If* $y \in S$*, then* $\{y, x, z\}$ *is an* ST*-breaking antichain for any* $z \in L_2$

except the link. Similarly, if $y \in T$, then $\{l, x, y\}$ is an ST-breaking antichain. Hence, neither S nor T can be expanded. $\square$

Proposition 8.8. (*S-2-links*). *Let L_1, L_2 be the two levels of $\mathbf{M}_{n,n}$. Let l_1 be L_1's link and l_2 be L_2's link. Suppose $x \in L_1 \setminus \{l_1\}$ and $y \in L_2 \setminus \{l_2\}$. If $S = \{l_1, l_2\}$ and $T = \{x, y\}$, then (S, T) is a maximal ST-pair of $\mathbf{M}_{n,n}$.*

Proof *ST-distributivity: Let $s \in S$ and $t_1, t_2 \in T$. If $t_1 = t_2$, we are done by Property 8.1. If not, without loss of generality, suppose that $t_1 = x$ and $t_2 = y$. If $s = l_1$, then s is comparable to t_2. Otherwise $s = l_2$ and hence, is comparable to t_1. In either case, MCCD implies the necessary distributions.*

Maximality: Note that the only elements left in $\mathbf{M}^*_{n,n}$ are those in

$$(L_1 \setminus \{l_1, x\}) \cup (L_2 \setminus \{l_2, y\})\,. \tag{8.40}$$

Let z be an element in this union. If $z \in S$, then $\{z, x, y\}$ is an ST-breaking antichain. Now, suppose $z \in T$. Then either $\{l_1, x, z\}$ or $\{l_2, y, z\}$ is an ST-breaking antichain depending on whether $z \in L_1$ or $z \in L_2$. $\square$

Proposition 8.9. (*S-level*). *Let L_1, L_2 be the two levels of $\mathbf{M}_{n,n}$. Let $l, x \in L_1$ where l is the link. If $S = L_2$ and $T = \{l, x\}$, then (S, T) is a maximal ST-pair of $\mathbf{M}_{n,n}$.*

Proof *ST-distributivity: Let $s \in S$ and $t_1, t_2 \in T$. If $t_1 = t_2 = x$, we are done by Property 8.1. Else, $t_1 = l$ or $t_2 = l$. Then l is comparable to s because a link in one level can be compared to all of the elements of the other level. Thus, the triple distributes by MCCD.*

Maximality: Note that the only elements left in $\mathbf{M}^*_{n,n}$ are those in $L_1 \setminus \{l, x\}$.

Suppose $y \in L_1 \setminus \{l, x\}$. If $y \in S$, then $\{y, x, l\}$ is an ST-breaking antichain.

If $y \in T$, then $\{z, x, y\}$ is an ST-breaking antichain for all $z \in S = L_2$ except the link. □

Observe that the only difference between ST-pairs of the type S-level-minus-link and those of type S-level is that pairs of type S-level-minus-link take the link element in the S of a type S-level and add it to its T.

Proposition 8.10. (*S-level-minus-link*). *Let L_1, L_2 be the two levels of $\mathbf{M}_{n,n}$ with respective links l_1, l_2. Suppose $x \in L_1 \setminus \{l_1\}$. If $S = L_2 \setminus \{l_2\}$ and $T = \{l_1, l_2, x\}$, then (S, T) is a maximal ST-pair of $\mathbf{M}_{n,n}$.*

Proof *ST-distributivity: Let $s \in S$ and $t_1, t_2 \in T$. If $t_1 = t_2$, we are done by Property 8.1. If not, we have two possibilities. One of them is that $t_1 = l_1$ or $t_2 = l_1$. In that case, l_1 is comparable to s because a link in one level can be compared to all of the elements of the other level. The other case is that neither t_1 nor t_2 is l_1. Without loss of generality, this implies that $t_1 = l_2$ and $t_2 = x$ and hence, they are comparable. In both cases, MCCD implies distribution.*

Maximality: The same argument of Proposition 8.9 can be applied with $l = l_1$. □

8.7.3 Theoretical Results 2: No More Pairs

Having established that all 5 types in Remark 8.1 generalize, we now show that we have identified all ways of constructing a maximal ST-pair of $\mathbf{M}_{n,n}$. The intuition behind this is that although the number of elements of $\mathbf{M}_{n,n}$ increases as n does, many of the new triples are ST-breaking antichains since only the links, which are fixed at

2 for all n, may be comparable with the new elements. We begin with the following lemma, which greatly reduces the subsets of $\mathbf{M}^*_{n,n}$ to consider when choosing T.

Lemma 8.3. (*Restriction on T*) *If $S, T \subseteq \mathbf{M}^*_{n,n}$ are disjoint subsets such that $\mathbf{M}_{n,n}$ is ST-distributive, then T cannot contain four elements, two from each level of $\mathbf{M}_{n,n}$.*

Proof *We show this by contradiction. Suppose that $T \supseteq \{a_i, a_j, b_k, b_l\}$ for $i \neq j$ and $k \neq l$. If $a_m \in S$ for any $m \in \mathbb{N}_n \setminus \{i, j\}$, then $\{a_m, a_i, a_j\}$ is an ST-breaking antichain, contradicting the ST-distributivity of $\mathbf{M}_{n,n}$. A similar argument works for any $b_m \in S$ distinct from b_k and b_l. This implies that $S = \emptyset$; contradiction. Therefore, $T \not\supseteq \{a_i, a_j, b_k, b_l\}$ for $i \neq j$ and $k \neq l$.* □

Without further delay, we complete the characterization of maximal ST-pairs of $\mathbf{M}_{n,n}$ in Theorem 8.1. Table 8.6 provides a formal description of the 5 types of maximal ST-pairs of $\mathbf{M}_{n,n}$ of Remark 8.1, each with its possible variations. It will be a helpful reference when following the different cases of the proof of Theorem 8.1.

Theorem 8.1. (*Characterization of maximal ST-pairs of $\mathbf{M}_{n,n}$*) *For all $n \in \mathbb{N}$ such that $n \geq 3$, the maximal ST-pairs of $\mathbf{M}_{n,n}$ all fall into one of the 5 types listed in Remark 8.1* (*or Table 8.6*).

Proof *We show that if (S, T) is a maximal ST-pair of $\mathbf{M}_{n,n}$, then (S, T) is of one of Types 1-5. Suppose that (S, T) is a a maximal ST-pair of $\mathbf{M}_{n,n}$. If T is a chain, then (S, T) is of Type 1 and we are done. For the remainder of the proof, we assume that T is not a chain. By Lemma 8.3, T cannot contain two elements of both levels of $\mathbf{M}_{n,n}$ at the same time. Hence, there are two cases:*

Type 1	T-chain		
4 forms	S	T	index restrictions
	$\{a_1, ..., a_{i-1}, a_{i+1}, ..., a_n, b_1, ..., b_n\}$	$\{a_i\}$	none
	$\{a_1, ..., a_n, b_1, ..., b_{i-1}, b_{i+1}, ..., b_n\}$	$\{b_i\}$	none
	$\{a_1, ..., a_{i-1}, a_{i+1}, ..., a_n, b_2, ..., b_n\}$	$\{a_i, b_1\}$	none
	$\{a_1, ..., a_{n-1}, b_1, ..., b_{i-1}, b_{i+1}, ..., b_n\}$	$\{a_n, b_i\}$	none
Type 2	S-link		
2 forms	S	T	index restrictions
	$\{b_1\}$	$\{a_1, ..., a_n, b_i\}$	$i \neq 1$
	$\{a_n\}$	$\{a_i, b_1, ..., b_n\}$	$i \neq n$
Type 3	S-2-links		
1 form	S	T	index restrictions
	$\{a_n, b_1\}$	$\{a_i, b_j\}$	$i \neq n, j \neq 1$
Type 4	S-level		
2 forms	S	T	index restrictions
	$\{b_1, ..., b_n\}$	$\{a_i, a_n\}$	$i \neq n$
	$\{a_1, ..., a_n\}$	$\{b_1, b_i\}$	$i \neq 1$
Type 5	S-level-minus-link		
2 forms	S	T	index restrictions
	$\{b_2, ..., b_n\}$	$\{a_i, a_n, b_1\}$	$i \neq n$
	$\{a_1, ..., a_{n-1}\}$	$\{a_n, b_1, b_i\}$	$i \neq 1$

Table 8.6: Formal descriptions of the 5 Types of Maximal ST-pairs of $\mathbf{M}_{n,n}$

1. *T is contained in one level: $T \subseteq \{a_1, ..., a_n\}$ or $T \subseteq \{b_1, ..., b_n\}$.*

2. *T is contained in one level except for exactly one element:*

   $T \subseteq \{a_i, b_1, ..., b_n\}$ with $a_i \in T$ or $T \subseteq \{a_1, ..., a_n, b_i\}$ with $b_i \in T$.

Case 1: *T is contained in one level. We do the case $T \subseteq \{a_1, ..., a_n\}$. The case $T \subseteq \{b_1, ..., b_n\}$ is done similarly. Since T is not a chain, $|T| \geq 2$. That is T contains a_i and a_j with $i \neq j$. Then no other a_k can be in S because $\{a_k, a_i, a_j\}$ would be an ST-breaking antichain. Thus, $S \subseteq \{b_1, ..., b_n\}$. This reduces the problem to determining how many a_i's and b_j's can be put in T and S respectively.*

To begin, we have $b_1 \in S$ by MCCD since $b_1 \geq a_i$ for all i. Now, observe that if T contains two non-link and distinct a_i and a_j, then $S = \{b_1\}$ because $\{b_k, a_i, a_j\}$ is an ST-breaking antichain for any $k \neq 1$. However, this implies that this pair will be properly contained in a pair of Type 2 contradicting its maximality. Hence, T cannot have two distinct non-link elements.

We are left with the possibility that $|T| = 2$ with $a_n \in T$. In this case, we must add all of the b_i's to S because $a_n \leq b_i$ for all i (MCCD). Thus, $S = \{b_1, ..., b_n\}$ and $T = \{a_i, a_n\}$ with $i \neq n \implies (S, T)$ is a maximal ST-pair of Type 4.

Case 2: *T is contained in one level except for exactly one element. There are two cases: (a) $|T| = 2$ and (b) $|T| \geq 2$.*

Sub-case 2a: *If $|T| = 2$, then $T = \{a_i, b_j\}$. Since T is not a chain, we must have $i \neq n$ and $j \neq 1$. Hence, T is an antichain of two elements. This implies that for any non-link a_k or b_k, $\{a_k, a_i, b_j\}$ and $\{b_k, a_i, b_j\}$ is an ST-breaking antichain. Thus, $S \subseteq \{a_n, b_1\}$. Given that $a_n \leq b_j$ and $b_1 \geq a_i$, the MCCD allows us to add both links* *to S. Thus we have $S = \{a_n, b_1\}$ and $T = \{a_i, b_j\}$ with $i \neq n$ and $j \neq 1 \implies (S,T)$ is a maximal ST-pair of Type 3.*

<u>Sub-case 2b</u>*: Suppose $|T| > 2$. We work with the case that $T \subseteq \{a_i, b_1, ..., b_n\}$ with $a_i \in T$. The case $T \subseteq \{a_1, ..., a_n, b_i\}$ with $b_i \in T$ is done similarly. We have that T contains $\{a_i, b_j, b_k\}$ for $j \neq k$ because $|T| > 2$. Then S cannot contain any b_l's because $\{b_l, b_j, b_k\}$ is an ST-breaking antichain for any b_l distinct from b_j and b_k. Thus,*

$$S \subseteq \{a_1, ..., a_{i-1}, a_{i+1}, ..., a_n\}. \tag{8.41}$$

Again, we have two cases: (i) a_i is a link $(i = n)$ and (ii) a_i is a non-link $(i \neq n)$.

<u>*Sub-sub-case 2b-i*</u>*: If a_i is a link $(i = n)$, then $S \subseteq \{a_1, ..., a_{n-1}\}$ by (8.41). Note, however, that for any non-link a_l (i.e. $l \neq n$), $\{a_l, b_j, b_k\}$ is an ST-breaking antichain if both b_j and b_k are non-link elements. As a result, T can have at most one non-link b_j if we want S to be non-empty. In addition, b_1 can be added to T because $b_1 \geq a_l$ (MCCD). We can also add one non-link b_k without affecting the content of S since $a_n \leq b_k$ (MCCD). Thus, $T = \{a_n, b_1, b_k\}$ with $k \neq 1$. Maximality then gives $S = \{a_1, ..., a_{n-1}\}$. Therefore, (S,T) is a maximal ST-pair of Type 5.*

<u>*Sub-sub-case 2b-ii*</u>*: If a_i is a non-link $(i \neq n)$, then we know for sure that T has two non-link elements because it will have at least one b_j with $j \neq 1$ (recall $|T| > 2$) and a_i. Then for any non-link a_l, $\{a_l, a_i, b_j\}$ is an ST-breaking antichain. Given (8.41), the only possible element of S is a_n. Since $a_n \leq b_k$ for all k, MCCD implies that $S = \{a_n\}$. Maximality forces $T = \{a_i, b_1, ..., b_n\}$ with $i \neq n \implies (S,T)$ is a maximal ST-pair of Type 2.*

$\therefore (S,T)$ *is of Type m for some $m \in \{1, 2, 3, 4, 5\}$.* $\square$

8.7.4 Combinatorial Corollary

As a corollary of Theorem 8.1, we can count how many maximal ST-pairs $\mathbf{M}_{n,n}$ has for each n. Observe that the 5 types of pairs are all pairwise disjoint, e.g., it is not possible for a pair to be both a T-chain pair and an S-link pair. Therefore, we just have to count how many of each type there are using basic combinatorics and then add them up. We conclude this section with the proof of this count.

Corollary 8.1. (*Count of maximal ST-pairs of $\mathbf{M}_{n,n}$*) *Let $n \geq 3$. Then $\mathbf{M}_{n,n}$ has $n^2 + 8n - 6$ maximal ST-pairs which are divided among the 5 types as follows:*

1. *T-chain: $4n - 1$,*
2. *S-link: $2n - 2$,*
3. *S-2-links: $n^2 - 2n + 1$,*
4. *S-level: $2n - 2$,*
5. *S-level-minus-link: $2n - 2$.*

Proof *We count how many pairs there are of each type and then sum them up. We point to Table 8.6 as a useful reference for following this proof.*

T-chain: Since S is completely determined by T ($S = \mathbf{M}^*_{n,n} \setminus T$), then there is exactly one T-chain pair for each chain of $\mathbf{M}^*_{n,n}$. There are $2n$ size 1 chains, $2n - 1$ size 2 chains, and no larger chains. The number of size 1 chains is the number of elements of $\mathbf{M}^*_{n,n}$: $2n$. As for the size 2 chains, note that they are all of the following two forms: $\{a_n, b_i\}$ and $\{a_i, b_1\}$. Each of these forms has n pairs, giving $2n$. However, *we must subtract one because $\{a_n, b_1\}$ is counted twice. Adding these up gives $4n-1$ pairs of type T-chain.*

S-link: Note that S consists of only a_n or b_1. Given S, T automatically has all of the elements of the level not containing S's link, but may differ by one non-link element of the level containing S's link. Hence,

$$\#pairs = (\#\text{link choices})(\#\text{choices of non-link in } T) \tag{8.42}$$

$$= 2 \times (n-1) \tag{8.43}$$

$$= 2n-2. \tag{8.44}$$

S-2-links: Observe that S is fixed as $\{a_n, b_1\}$. Thus, the number of pairs of this type are determined by the number of ways of choosing T. Since T consists of one non-link a_i and one non-link b_j, we have

$$\#pairs = (\#\text{non-link choices of } a_i)(\#\text{non-link choices of } b_j) \tag{8.45}$$

$$= (n-1) \times (n-1) \tag{8.46}$$

$$= n^2 - 2n + 1. \tag{8.47}$$

S-level: Since S is one of the two levels of $\mathbf{M}_{n,n}$, it has two options. Given S, T has two elements from the other level. One of these must be the link while the other *may be any of the non-links. As a result,*

$$\#pairs = (\#levels)(\#choices\ for\ T\text{'s non-link}) \tag{8.48}$$

$$= 2 \times (n-1) \tag{8.49}$$

$$= 2n - 2. \tag{8.50}$$

S-level-minus-link: Observe that each ST-pair of the type S-level-minus-link is obtained from a type S-level pair by taking the link element in the S of a type S-level and adding it to its T. Therefore, there is a 1-1 correspondence between these pairs and hence $2n-2$ pairs of type S-level-minus-link.

Total: It remains to add up the totals of pairs of each type. It can be verified that

$$(4n-1) + (2n-2) + (n^2 - 2n + 1) + (2n-2) + (2n-2) = n^2 + 8n - 6, \tag{8.51}$$

which is the total amount of pairs initially claimed. □

8.8 Connections

Before moving on to the next chapter, we establish some connections between our ST-distributive lattices and three other concepts in lattice theory: distributive elements, SS-lattices, and sublattices of distributive lattices.

We begin with distributive elements. These have a history of changing in meaning. In Garret Birkhoff's *Lattice Theory* [2], they are defined as being synonymous to neutral elements (Chapter III, Section 9). However, distributive and neutral elements are more recently defined as two separate concepts, as can be seen in George Grätzer's *Lattice Theory: Foundation* [12] (Chapter III, Section 2). Nevertheless, we will define a distributive element as in [2] for reasons that will be clarified shortly. Thus, a distributive element is an element of a lattice with the property that any three-element subset of the lattice containing it generates a distributive sublattice.

Definition 8.8. (*distributive element*) *A distributive element of a lattice L is an element $a \in L$ such that for all $x, y \in L$, $[\{a, x, y\}]$ is distributive. Recall that $[\{a, x, y\}]$ is the sublattice of L generated by $\{a, x, y\}$. The set of all distributive elements of L is denoted* Distr *L.*

We now consider two weaker variations of distributive elements that we will call meet distributive elements and join distributive elements. These really are, respectively, dually distributive elements and distributive elements as defined in [12] in disguise. We renamed them to make their connection to ST-distributivity more apparent. This is also why we define distributive elements as in [2].

Definition 8.9. (*meet distributive element*) *A meet distributive element of a lattice L is an element $a \in L$ such that*

$$a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y) \tag{8.52}$$

for all $x, y \in L$. The set of all meet distributive elements of L is denoted mDistr *L.*

Definition 8.10. (*join distributive element*) *A join distributive element of a lattice L is an element $a \in L$ such that*

$$a \vee (x \wedge y) = (a \vee x) \wedge (a \vee y) \tag{8.53}$$

for all $x, y \in L$. The set of all join distributive elements of L is denoted $\mathrm{jDistr}\, L$.

Note that all elements of a distributive lattice are trivially distributive, meet distributive, and join distributive. In addition, it is immediate from Definitions 8.8-8.10 that all distributive elements are meet distributive and join distributive. We use this fact to give the first non-trivial example of these three types of elements.

Example 8.6. (*lattice identities*) *The identity elements* 0 *and* 1 *of any lattice L are distributive. This is because $[\{0, x, y\}]$ is either a chain, $\mathbf{M}_2$, or $\mathbf{1} \oplus \mathbf{M}_2$ with dual reasoning for $[\{1, x, y\}]$. This results in* 0 *and* 1 *both being meet and join distributive as well.*

Next, we make a few additional comments regarding the relationships between these three types of lattice elements. It follows naturally from their definitions that meet distributive elements and join distributive elements are dual concepts. However, they are not equivalent. Furthermore, although all distributive elements are both meet distributive and join distributive, it is possible for an element to be both meet distributive and join distributive but not distributive.

We now give three more examples, two of which will illustrate the relations just discussed. They involve the lattices $\mathbf{M}_3$ and $\mathbf{N}_5$, which we repeat in Figures 8.13

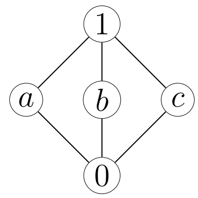


Figure 8.13: The diamond $\mathbf{M}_3$

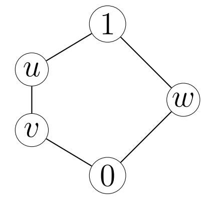


Figure 8.14: The pentagon $\mathbf{N}_5$

and 8.14 for ease of reference. We omit the computations involved because they are elementary.

Example 8.7. (*meet distributive* $\not\Leftrightarrow$ *join distributive*) *An element that is meet distributive but not join distributive is* $v \in \mathbf{N}_5$. *By Property 8.1 and idempotency of lattice operations, proving that* v *is meet distributive reduces to checking Equation* (*8.52*) *for the case* $a = v$, $x = u$, *and* $y = w$. *On the other hand, to see that it is not join distributive, consider the case* $a = v$, $x = u$, *and* $y = w$ *in Equation* (*8.53*). *It can be similarly shown that* $u \in \mathbf{N}_5$ *is join distributive but not meet distributive.*

Example 8.8. (*meet and join distributive but not distributive*) *The element* $w \in \mathbf{N}_5$ *is both meet distributive and join distributive but not distributive. To see that it is both meet and join distributive it suffices to consider only the cases where* x *and* y *are both distinct from each other and from* w *in Equations* (*8.52*) *and* (*8.53*). *To see that it is not distributive note that* $[\{w, u, v\}] = \mathbf{N}_5$.

Example 8.9. (*complete non-example*) *The element* $a \in \mathbf{M}_3$ *is neither meet distributive nor join distributive. To see this, it is enough to substitute* $a = a$, $x = b$, *and* $y = c$ *in Equations* (*8.52*) *and* (*8.53*). *This also implies that* a *is not distributive, which can also be verified by observing that* $[\{a, b, c\}] = \mathbf{M}_3$.

Another important aspect about distributive elements and their variations is finding ways to characterize them. The following characterization theorems do just that. Each gives conditions on an element of a lattice that are equivalent to one of Definitions 8.8-8.10. These theorems are adaptations from Theorems 252 and 254 of Chapter III, Section 2 of [12] where their proofs can be found. Once our terminology is translated to that of [12] (as discussed earlier), we get that Theorem 8.2 is the dual of Theorem 252, Theorem 8.3 is Theorem 252, and Theorem 8.4 is Theorem 254.

Theorem 8.2. (*characterization of meet distributive elements*) *Let L be a lattice with $a \in L$.*

1. $a \in \mathrm{mDistr}\, L \iff$ *the function $\phi : L \to L$ defined by*

$$\phi(x) = a \wedge x \tag{8.54}$$

is a lattice homomorphism.

2. $a \in mDistr L \iff$ *the equivalence relation α_a in L defined by*

$$x \equiv y \pmod{\alpha_a} \iff a \wedge x = a \wedge y \tag{8.55}$$

is a congruence on L.

Theorem 8.3. (*characterization of join distributive elements*) *Let L be a lattice with $a \in L$.*

1. $a \in \mathrm{jDistr}\, L \iff$ *the function $\phi : L \to L$ defined by*

$$\phi(x) = a \vee x \tag{8.56}$$

is a lattice homomorphism.

2. $a \in \mathrm{jDistr}\, L \iff$ *the equivalence relation* α_a *in* L *defined by*

$$x \equiv y \pmod{\alpha_a} \iff a \vee x = a \vee y \tag{8.57}$$

is a congruence on L*.*

Theorem 8.4. (*characterization of distributive elements*) *Let* L *be a lattice with* $a \in L$*.*

1. $a \in \mathrm{Distr}\, L \iff$ *for all* $x, y \in L$*,*

$$(a \wedge x) \vee (x \wedge y) \vee (y \wedge a) = (a \vee x) \wedge (x \vee y) \wedge (y \vee a). \tag{8.58}$$

2. $a \in \mathrm{Distr}\, L \iff$ *there is an embedding* $\phi : L \to A \times B$ *where* A *is a lattice with* 1*,* B *a lattice with* 0*, and* $\phi(a) = (1, 0)$*.*

3. $a \in \mathrm{Distr}\, L \iff a \in (\mathrm{mDistr}\, L) \cap (\mathrm{jDistr}\, L)$ *and for any* $x, y \in L$*,*

$$a \wedge x = a \wedge y \text{ and } a \vee x = a \vee y \implies x = y. \tag{8.59}$$

Finally, we mention the connection between distributive elements and ST-distributive lattices. This is that Definitions 8.8-8.10 provide choices of $S \subseteq L$ that guarantee ST-distributivity for $T = L$. In particular, we have that any lattice L is

1. $(\mathrm{mDistr}\, L)L$-meet distributive,

2. $(\mathrm{jDistr}\, L)L$-join distributive,

3. $(\mathrm{Distr}\, L)L$-distributive.

We continue by placing our ST-distributive lattices in the context of Stanley's SS-lattices (see [20]). We will see that these are lattices that satisfy a condition regarding distributivity in certain pairs of chain sublattices that is stronger than the relative distributivity of ST-distributive lattices, which are thus, more general. First, we recall the definition of an SS-lattice.

Definition 8.11. *(SS-lattice [20]). Consider a lattice L with a maximal chain Δ. (L, Δ) is called a supersolvable lattice (SS-lattice) if for all chains K of L, $[\Delta, K]$ is distributive. Here, $[\Delta, K]$ denotes the sublattice of L generated by $\Delta \cup K$.*

From this definition, we can immediately observe that an SS-lattice (L, Δ) is ΔK-distributive and $K\Delta$-distributive for all its chains K by Example 8.3. In addition, it is also ST-distributive for all subsets $S, T \subseteq [\Delta, K]$ given any chain K. On the other hand, the class of ST-distributive lattices is larger given that the conditions specified on Definition 8.1 are more flexible than those required for an SS-lattice. First, S and T are allowed to be any subsets of the initial lattice rather than just chains. In addition, we only ask that S distributes into T instead of demanding that the generated sublattice $[S, T]$ be distributive.

We conclude this section by linking the search for ST-distributive lattices to the study of sublattices of distributive lattices. Although our present discussion of ST-distributive lattices has been limited to finding ST-distributive lattices in non-distributive lattices, this need not always be the case. To begin with, Definition 8.1 does not require the initial lattice L to be non-distributive. In fact, we mentioned in Section 8.2 that a lattice L is distributive if and only if it is ST-distributive for

$S = T = L$. Therefore, the study of ST-distributive lattices can encompass problems regarding distributive lattices such as finding and describing their maximal proper sublattices as done in [16]. In such a context, it is helpful to observe that for a proper sublattice S of L, the fact that L is an SS-distributive lattice is equivalent to S being a distributive (proper) sublattice of L. Furthermore, if (S, S) is a maximal (S, S)-pair, then S is a proper maximal distributive sublattice of L.

Chapter 9

ST-modular Lattices

9.1 Introduction

After introducing ST-distributive lattices in Chapter 8, we now explore ST-modular lattices. Naturally, an ST-modular lattice will be to a modular lattice what an ST-distributive lattice is to a distributive lattice. In fact, the relative modular property that will be needed to define them is obtained from the relative distributive property by replacing the distributive law by the modular law. As a result of this, we will have that ST-distributive lattices are always ST-modular.

Our treatment of ST-modular lattices will be shorter than that of ST-distributive ones since their state of the art is less developed. At first, we will translate some of the basic results from the previous chapter to ST-modular lattices. Afterwards, however, our approach to them will differ significantly from that of ST-distributive lattices. We will not search lattices for sets that make them ST-modular but will focus instead in suggesting a potential application of ST-modularity to convex sets.

This application is the original motivation for our relative distributive and modular properties and follows from a result in [7] which we will discuss in Section 9.4.

We proceed as follows. Section 9.2 begins with the basic definition and some examples. Section 9.3 then generalizes to ST-modular lattices most of the basic properties established for ST-distributive lattices in Section 8.3. Finally, Section 9.4 proposes an application of ST-modular lattices to convex sets by showing that an identity regarding the intersection of an affine set with the convex hull of two convex sets can be translated into ST-meet modularity in the lattice of convex sets.

9.2 What is an ST-Modular Lattice?

We begin this chapter by introducing ST-modular lattices, our proposed generalization of modular lattices that is analogous to ST-distributive lattices. In this section, we define them, relate them to ST-distributive lattices, and give some illustrative examples of them (which are found in the proofs of the propositions). In a way, we will mirror the structure and content of Section 8.2. The first parallel between the two sections is the similarity between Definition 8.1 and the following definition:

Definition 9.1. (ST*-modular Lattice*). *Given a lattice L with subsets $S, T \subseteq L$, we define:*

- <u>*ST-meet Modular Lattice*</u>*: L is said to be ST-meet modular if for all $s \in S$ and $t_1, t_2 \in T$,*

$$s \geq t_2 \implies s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee t_2. \tag{9.1}$$

- *<u>ST-join Modular Lattice</u>: L is said to be ST-join modular if for all $s \in S$ and $t_1, t_2 \in T$,*

$$s \leq t_2 \implies s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge t_2. \tag{9.2}$$

- *<u>ST-modular Lattice</u>: L is said to be ST-modular if it is both ST-meet modular and ST-join modular.*

Some quick remarks on ST-modular lattices are in order. For starters, these are less intuitive to describe than ST-distributive lattices in the sense that there is no analog to saying "S distributes into T." We could try saying "S modulates into T" but it would not be meaningful. In addition, we have that Definition 9.1 generalizes modular lattices: ST-modular lattices for $S = T = L$. Next, we explore the relationship between ST-modular and ST-distributive lattices. We establish that ST-distributive lattices are ST-modular. This follows directly from the modularity of distributive lattices (see Proposition 4.1).

Proposition 9.1. (ST*-distributive* $\implies$ ST*-modular*). *Let L be a lattice with subsets $S, T \subseteq L$. If L is ST-distributive, then L is ST-modular.*

Proof *This follows from the definitions and the Connecting Lemma.* □

As a result of Proposition 9.1, the ST-distributive lattice from Example 8.1 is also an ST-modular lattice. Proposition 9.2 proves that the converse of Proposition 9.1 is not true with a counter-example. Thus, the class of ST-modular lattices properly contains that of ST-distributive ones. This is not surprising given that not all modular lattices are distributive (see Example 4.6).

Proposition 9.2. *(ST-modular $\not\Rightarrow$ ST-distributive). Let L be a lattice with subsets $S, T \subseteq L$. It is possible for L to be ST-modular but not ST-distributive.*

Proof *We give a counter-example. Consider the lattice L from Figure 9.1 and its subsets $S = \{b, d\}$ and $T = \{a, c\}$. We claim the L is ST-modular but not ST-distributive.*

<u>ST-modular</u>: Note that there is no $s \in S$ and $t \in T$ such that $s \geq t$. Thus, L is vacuously ST-meet modular. To prove that it is ST-join modular, it suffices to consider the case when $d \leq a$. This leads to two cases where the required equalities hold. Note the use of absorption in the rightmost equality of the first case.

$$d \vee (a \wedge a) = d \vee a = a = (d \vee a) \wedge a, \tag{9.3}$$

$$d \vee (c \wedge a) = d \vee e = a = 1 \wedge a = (d \vee c) \wedge a. \tag{9.4}$$

<u>Not ST-distributive</u>: Note that $b \in S$ and $a, c \in T$ yet,

$$b \wedge (a \vee c) = b \wedge 1 = b \neq d = d \vee 0 = (b \wedge a) \vee (b \wedge c)\,. \tag{9.5}$$

Therefore, L is ST-modular but not ST-distributive for our choice of S and T. $\square$

We conclude this section with two additional propositions that illustrate similarities in the behavior of ST-modular lattices and ST-distributive lattices. In particular, both share (a) the distinction between their ST-meet and ST-join sub-definitions and (b) the ordered nature of the pair of subsets (S, T).

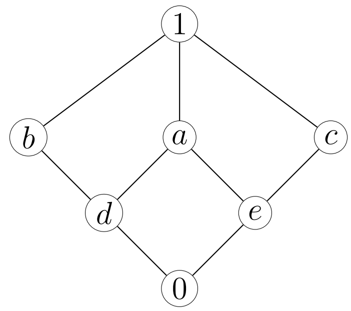


Figure 9.1: Lattice L of proofs of Propositions 9.2, 9.3, and 9.4

$0 \vee (c \wedge c) = c$	$0 \vee (c \wedge d) = 0$
$(0 \vee c) \wedge c = c$	$(0 \vee c) \wedge d = 0$
$0 \vee (d \wedge c) = 0$	$0 \vee (d \wedge d) = d$
$(0 \vee d) \wedge c = 0$	$(0 \vee d) \wedge d = d$

Table 9.1: Computations to show that L is ST-join modular in the proof of Proposition 9.3

Proposition 9.3. *(ST-meet Modular $\not\Leftrightarrow$ ST-join Modular). Let L be a lattice with $S, T \subseteq L$. Then ST-meet modular and ST-join modular are not equivalent conditions on L.*

Proof *We give a counter-example. Recall the lattice L from Figure 9.1 and consider the subsets $S = \{0, b\}$ and $T = \{c, d\}$. We claim the L is ST-join modular but not ST-meet modular.*

ST-join Modular: Since $0 \leq c$ and $0 \leq d$, we have four cases to verify. The computations in Table 9.1 show that all of them satisfy the modular law. In the next section, Property 9.1 will make these computations unnecessary.

Not ST-meet Modular: Observe that although $b \in S$, $c, d \in T$ and $b \geq d$, we have:

$$b \wedge (c \vee d) = b \wedge 1 = b \neq d = 0 \vee d = (b \wedge c) \vee d. \tag{9.6}$$

Thus, L is ST-join modular but not ST-meet modular for our chosen (S,T). $\square$

Proposition 9.4. *(ST-modular $\not\Leftrightarrow$ TS-modular). Let L be a lattice with $S, T \subseteq L$. Then ST-modular and TS-modular are not equivalent conditions on L.*

Proof *We give a counter-example. Recall the lattice L from Figure 9.1 and consider the subsets $S = \{b, c\}$ and $T = \{a, d\}$. We claim the L is ST-modular but not TS-modular.*

<u>ST-modular</u>: Given that there is no $s \in S$ and $t \in T$ such that $s \le t$, L is vacuously ST-join modular. To show that it is ST-meet modular, we only need to consider when $b \ge d$. This leads to two cases where the necessary equalities hold. Note the use of absorption in the rightmost equality of the first case. In the following section, Corollary 9.2 of Property 9.1 will eliminate the need for the justifications of this paragraph because the set T is a chain sub-lattice of L.

$$b \wedge (d \vee d) = b \wedge d = d = (b \wedge d) \vee d, \tag{9.7}$$

$$b \wedge (a \vee d) = b \wedge a = d = d \vee d = (b \wedge a) \vee d. \tag{9.8}$$

<u>Not TS-modular</u>: To see this, note that although $d \in T$, $b, c \in S$, and $d \le b$, we have

$$d \vee (c \wedge b) = d \vee 0 = d \neq b = 1 \wedge b = (d \vee c) \wedge b. \tag{9.9}$$

Thus, L is ST-modular but not TS-modular for our chosen (S,T). $\square$

9.3 Basic Properties

In this section, we discuss some basic properties of ST-modular lattices. In essence, we extend to ST-modular lattices most of the properties of ST-distributive lattices discussed in Section 8.3. Chief among these are the efficiency criteria and the results on the algebra of sets.

To start, we generalize the efficiency criteria of Property 8.1 to ST-modular lattices. In particular, Condition 1 of said property gets carried over while Conditions 2 and 3 are substituted by a more flexible condition requiring only that a and b be comparable. This relaxation is not surprising if one considers that the modular law itself imposes a second order relation to the triple of elements and the fact that distributivity implies modularity.

Property 9.1. (*Efficiency Criteria*). *Let L be a lattice with $a, b, c \in L$ such that the triple (a, b, c) satisfies any of the following conditions:*

1. *$b \leq c$ or $b \geq c$,*

2. *$a \leq b$ or $a \geq b$.*

Then the following hold:

$$a \geq c \implies a \wedge (b \vee c) = (a \wedge b) \vee c, \tag{9.10}$$

$$a \leq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c. \tag{9.11}$$

Proof *We show only that each condition implies Equation (9.10). Duality gives Equation (9.11).*

Condition 1: Suppose that $b \leq c$. If $a \geq c$, then we have that

$$a \wedge (b \vee c) = a \wedge c = c = b \vee c = (a \wedge b) \vee c, \tag{9.12}$$

where the first equality from the right follows from transitivity: $a \geq c \geq b$. Thus, $b \leq c$ implies Equation (9.10). Now, suppose that $b \geq c$. Again if $a \geq c$, then we get

$$a \wedge (b \vee c) = a \wedge b = (a \wedge b) \vee c, \tag{9.13}$$

where the rightmost equality follows from the fact that $a, b \geq c$ implies that $a \wedge b \geq c$. Therefore, $b \geq c$ also implies Equation (9.10).

Condition 2: Suppose that $a \leq b$. If $a \geq c$, then we have that

$$a \wedge (b \vee c) = a = a \vee c = (a \wedge b) \vee c, \tag{9.14}$$

where the first equality from the left follows from the fact that $a \leq b$ implies that $a \leq b \vee c$. Thus, $a \leq b$ implies Equation (9.10). Now, suppose that $a \geq b$. Again if $a \geq c$, then we get

$$a \wedge (b \vee c) = b \vee c = (a \wedge b) \vee c, \tag{9.15}$$

where the leftmost equality follows from the fact that $a \geq b, c$ implies that $a \geq b \vee c$. Therefore, $a \geq b$ also implies Equation (9.10). $\square$

Like with ST-distributive lattices, this criteria leads immediately to the following two corollaries. The first says that we can add 0 and 1 to any set S or T without affecting ST-modularity while the second says that ST-modularity is guaranteed for any chain T.

Corollary 9.1. (ST*-modularity invariant under inclusion of* 0 *and* 1) *Let* L *be a lattice and* $S, T \subseteq L$ *such that* L *is* ST*-modular. Then* L *is also* $S_{01}T_{01}$*-modular for* $S_{01} = S \cup \{0, 1\}$ *and* $T_{01} = T \cup \{0, 1\}$.

Proof *It suffices to verify that Equations* (*9.10*) *and* (*9.11*) *are satisfied by any triple* (a, b, c) *in which one of the three elements is replaced by* 0 *or* 1. *If* $a = 0$ *or* $a = 1$, *then the equations hold by Property 9.1 because one of the two inequalities of Condition 2 is satisfied. Likewise, if* b *is* 0 *or* 1. *Finally if* c *is* 0 *or* 1, *then Condition 1 is fulfilled and modularity follows.* □

Corollary 9.2. (T*-chain*) *Let* L *be a lattice with* $S, T \subseteq L$. *If* T *is a chain, then* L *is* ST*-modular.*

Proof *If* T *is a chain then all* $t_1, t_2 \in T$ *satisfy Condition 1 of Property 9.1 which implies that Equations* (*9.1*) *and* (*9.2*) *of Definition 9.1 hold for all* $s \in S$. □

Next, we repeat with ST-modular lattices the algebra of sets exercise that we did with ST-distributive lattices. The results are identical. If we fix T and let S roam free, we have that the S's are closed under both intersection and union. As a result, we can also define a complete lattice with them. Similarly, fixing S while letting T roam free gives only closure under intersection. All of this leads to repeating the same results when neither set is fixed. The formal statements and proofs follow.

Property 9.2. (*Closure of Intersection of* S*'s with Fixed* T) *Let* L *be a lattice with* $S_1, S_2, T \subseteq L$. *If* L *is* S_1T*-modular and* S_2T*-modular, then* L *is* $(S_1 \cap S_2)\,T$*-modular.*

Proof *Let $s \in S_1 \cap S_2$ and $t_1, t_2 \in T$ with $s \geq t_2$. Since $s \in S_1$ and L is S_1 T-modular, we have that*

$$s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee t_2. \tag{9.16}$$

Similarly, if $s \leq t_2$, then

$$s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge t_2 \tag{9.17}$$

and L is $(S_1 \cap S_2)\, T$-modular. □

Property 9.3. (*Closure of Union of S's with Fixed T*) *Let L be a lattice with $S_1, S_2, T \subseteq L$. If L is S_1T-modular and S_2T-modular, then L is $(S_1 \cup S_2)\, T$-modular.*

Proof *Let $s \in S_1 \cup S_2$ and $t_1, t_2 \in T$. If $s \in S_1$, then L S_1T-modular implies*

$$s \geq t_2 \implies s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee t_2, \tag{9.18}$$

$$s \leq t_2 \implies s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge t_2. \tag{9.19}$$

A similar argument shows that the above equations hold if $s \in S_2$ instead. Therefore, L is $(S_1 \cup S_2)\, T$-modular. □

Lemma 9.1. (*Complete Lattice of S's with Fixed T*). *Let L be any lattice. For a fixed T, the collection of all subsets $S \subseteq L$ such that L is ST-modular forms a complete distributive lattice of sets. The join and meet operations are given by union and intersection respectively. We denote this lattice $\mathcal{S}_M(L, T)$.*

Proof *This is similar to Properties 9.2 and 9.3.* □

Property 9.4. (*Closure of Intersection of T's with Fixed S*) *Let L be a lattice and fix a non-empty $S \subseteq L$. Let $T_1, T_2 \subseteq L$ such that L is ST_1-modular and ST_2-modular. Then L is $S(T_1 \cap T_2)$-modular.*

Proof *Let $s \in S$ and $t_1, t_2 \in T_1 \cap T_2$. Then $t_1, t_2 \in T_1$ and since L is ST_1-modular we have*

$$s \geq t_2 \implies s \wedge (t_1 \vee t_2) = (s \wedge t_1) \vee t_2, \tag{9.20}$$

$$s \leq t_2 \implies s \vee (t_1 \wedge t_2) = (s \vee t_1) \wedge t_2, \tag{9.21}$$

which implies that L is $S(T_1 \cap T_2)$-modular. □

Example 9.1. (*No Closure of Union of T's with Fixed S*) *Consider the lattice $\mathbf{N}_5$ shown in Figure 9.2. If $S = \{0, v\}$, $T_1 = \{u\}$, and $T_2 = \{w\}$, then it can be shown that $\mathbf{N}_5$ is ST_1-modular and ST_2-modular. However, observe that*

$$T_1 \cup T_2 = \{u, w\} \tag{9.22}$$

and that despite the fact that $v \geq u$,

$$v \wedge (w \vee u) = v \wedge 1 = v \neq u = 0 \vee u = (v \wedge w) \vee u \tag{9.23}$$

with $v \in S$. Therefore, $\mathbf{N}_5$ is not $S(T_1 \cup T_2)$-modular.

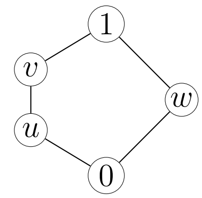


Figure 9.2: The pentagon $\mathbf{N}_5$

Property 9.5. (*Algebra of ST-Modular Lattices with Nothing Fixed*) *Let L be a lattice with subsets S_1, S_2, T_1, and T_2. Then we have the following.*

1. *S_1T_1-modular and S_2T_2-modular imply:*
   (a) *$(S_1 \cap S_2)(T_1 \cap T_2)$-modular,*
   (b) *$(S_1 \cup S_2)(T_1 \cap T_2)$-modular.*
2. *S_1T_1-modular and S_2T_2-modular do NOT imply:*
   (a) *$(S_1 \cap S_2)(T_1 \cup T_2)$-modular,*
   (b) *$(S_1 \cup S_2)(T_1 \cup T_2)$-modular.*

Proof *Similar to those of the previous three properties and example.* □

Yet another property of ST-distributivity that (almost) applies to ST-modularity is its preservation by lattice constructs discussed in Proposition 8.3. Specifically, it is preserved by sublattices, lattice products, and duality of lattices. We now present the formal result albeit without proof since it is elementary.

Proposition 9.5. (*Preservation of ST-modularity by Lattice Constructs*). *Let L be a lattice with subsets S and T such that L is ST-modular.*

1. *If K is a sublattice of L, then K is S_1T_1-modular for $S_1 = S \cap K$ and $T_1 = T \cap K$.*

2. *If L' is another lattice with subsets S' and T' such that L' is $S'T'$-modular, then $L \times L'$ is $(S \times S')\,(T \times T')$-modular.*

3. *If L^{∂} represents the dual lattice of L and S and T are sublattices with duals S^{∂} and T^{∂}, then L^{∂} is $S^{\partial}T^{\partial}$-modular.*

We conclude by remarking that SS-lattices (see Definition 8.11) are also a source of ST-modular lattices. If for a lattice L and a maximal chain Δ of L, (L, Δ) is an SS-lattice, then L is ΔK-modular and $K\Delta$-modular for all chains K in L because L is ΔK and $K\Delta$-distributive (Proposition 9.1).

9.4 Application to Convex Sets

Following the similarity between Sections 8.2-8.3 and 9.2-9.3, our discussion of ST-modular lattices will take a different route from that of ST-distributive lattices. We will not search lattices for pairs of subsets (S, T) inducing ST-modularity. Instead, we discuss the original motivation for our relative distributive and modular properties: a potential application of relative modularity to convex sets that is suggested by results in [7].

The inspiration of this application are new proofs by Emamy [7] of two classical convex polytope theorems (Theorems 9.1 and 9.2) that use a special identity about convex sets (Proposition 9.6). The crux is that we can represent this identity about convex sets with ST-meet modularity in the lattice of convex sets. Thus, these new proofs hint at the possibility of using lattices to prove results about convex polytopes.

We devote this section to presenting this idea backwards (in a way, at least). We first review the two main ingredients: the lattice of convex sets and the property of convex hulls in Proposition 9.6. Afterwards, we establish the lattice representation of this property (enter ST-meet modularity). Finally, we go over the new proofs from [7] to illustrate the origins of this proposed application.

We begin by defining the first ingredient: the lattice of convex sets. Note that $\operatorname{conv}(A, B)$ denotes the convex hull of $A \cup B$ for two sets A and B.

Definition 9.2. (*Lattice of Convex Sets [1]*). *The lattice of convex sets of* $\mathbb{R}^d$ *is the lattice* $\langle L, \vee, \wedge \rangle$ *where* L *is the set of all convex sets of* $\mathbb{R}^d$ *with lattice operations*

$$A \wedge B = A \cap B \qquad A \vee B = \operatorname{conv}(A, B) \ . \tag{9.24}$$

We note that this lattice is ordered by inclusion ($\subseteq$). In addition, we provide a counter-example to show that it is non-modular, which makes our proposed relative modularity non-trivial.

Example 9.2. (*lattice of convex sets non-modular*) *We show that the lattice of convex sets of* $\mathbb{R}^2$ *is not modular. Consider the convex sets in the Euclidean plane shown in Figure 9.3:* $A = T = conv(f, g, h)$ *(a triangle),* $B = \{x\}$*, and* $C = \{y\}$*. Observe that* $A \geq C$ *since* $T \supseteq \{y\}$*. However, we have that*

$$\begin{aligned} A \wedge (B \vee C) &= T \cap conv(\{x\}, \{y\}) && (9.25) \\ &= T \cap [x, y] && (9.26) \\ &= [z, y] && (9.27) \end{aligned}$$

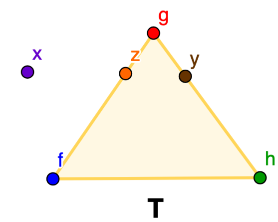


Figure 9.3: The convex sets A, B, and C of $\mathbb{R}^2$ used in Example 9.2

while

$$(A \wedge B) \vee C = conv(T \cap \{x\}, \{y\}) \tag{9.28}$$

$$= conv(\emptyset, \{y\}) \tag{9.29}$$

$$= conv(\{y\}) \tag{9.30}$$

$$= \{y\}. \tag{9.31}$$

Therefore, $A \geq C$ *but* $A \wedge (B \vee C) \neq (A \wedge B) \vee C$.

Next, we present our second ingredient: an identity regarding the intersection of an affine set with the convex hull of two convex sets. It gives conditions under which the intersection can be "absorbed" by the convex hull.

Proposition 9.6. (*Interesection of Affine Set and Convex Hull [7]*). *Suppose we have* $A, B, C \subseteq \mathbb{R}^d$ *with* A *affine,* B *and* C *convex, and* $A \supseteq C$*. Then:*

$$A \cap \operatorname{conv}(B, C) = \operatorname{conv}(A \cap B, C)\,. \tag{9.32}$$

Proof *The inclusion* $\supseteq$ *is trivial by Definition 7.2 because* $A \cap \operatorname{conv}(B, C)$ *is convex and contains both* $A \cap B$ *and* $C = A \cap C$*. For* $\subseteq$*, let* $x \in A \cap \operatorname{conv}(B, C)$*. Then* $x \in \operatorname{conv}(B, C)$ *and since* $\operatorname{conv}(B, C)$ *is the union of all line segments connecting a* *point in B with a point in C (Proposition 7.1, item 8), there exist $b \in B$, $c \in C$ and $0 \leq \alpha \leq 1$ such that*

$$x = (1 - \alpha)\, b + \alpha c. \tag{9.33}$$

If $\alpha = 0$, then $x = b \in B$ and given that $x \in A$, $x \in A \cap B$ and we are done. Similarly, if $\alpha = 1$, then $x = c \in C$ and we are done. Otherwise, solve Equation (9.33) for b to get

$$b = \frac{1}{1 - \alpha} x - \frac{\alpha}{1 - \alpha} c. \tag{9.34}$$

It follows that $b \in A$. This due to the fact that $x, c \in A$ (recall $C \subseteq A$), the sum of their coefficients is 1, and A is affine (Proposition 7.1, item 6). This means that the convex combination presentation in Equation (9.33) is a convex combination of a point in $A \cap B$ and a point in C. Therefore, $x \in \operatorname{conv}(A \cap B, C)$ by Proposition 7.1, item 7. $\square$

We can now discuss the potential application of ST-modularity to convex sets that is the reason for this section. The main idea is to describe certain behaviors of convex sets using our relative modularity. For instance, we can translate Proposition 9.6 into the language of the lattice of convex sets to get ST-meet modularity in said lattice. We remark that in this context, the inclusion $\supseteq$ in the proof of said proposition is the manifestation of the second lattice inequality of Lemma 4.1 in the lattice of convex sets.

Corollary 9.3. (*ST-meet Modularity in the Lattice of Convex Sets*). *Let L be the lattice of convex sets of $\mathbb{R}^d$. If S is the set of all affine sets of $\mathbb{R}^d$ and $T = L$, then L is ST-meet modular.*

Proof *By Proposition 9.6, if $A \in S$, $B, C \in T$, and $A \geq C$, then*

$$A \wedge (B \vee C) = (A \wedge B) \vee C, \tag{9.35}$$

and L is ST-meet modular. □

As mentioned earlier, this connection is important because this ST-meet modularity can be used to prove classical theorems on convex polytopes. We will now present the two examples of this from [7]. To be more precise, the proofs really use Proposition 9.6 rather than Corollary 9.3. The idea is to hint at the potential relevance of Corollary 9.3 rather than apply it directly.

Before presenting the theorems and proofs, we review some definitions and notations to be used in them. We define a *convex polytope* as the convex hull of a finite set of points in $\mathbb{R}^d$ and a *face* of a convex polytope as the intersection of the polytope with a supporting hyperplane (following Section 7.4). A *vertex* is a 0-dimensional face. Given a hyperplane H in $\mathbb{R}^d$, H^+ denotes one of the closed halfspaces of $\mathbb{R}^d$ that it defines and $int\,(H^+)$ its corresponding open halfspace. Finally, for a finite set of points $\{x_1, ..., x_n\}$, we write $\text{conv}\,(x_1, ..., x_n)$ as short hand for $\text{conv}\,(\{x_1, ..., x_n\})$.

Theorem 9.1. (*Faces of Convex Polytope [7]*).

1. *A convex polytope has a finite number of faces.*

2. *Each face is a convex polytope.*

Proof *We prove Statement 2 first and then derive Statement 1 from it. Since $\emptyset$ is a convex polytope whose only face is itself, we assume that P and F are non-empty in what follows.*

Statement 2: Let $P = \operatorname{conv}(x_1, ..., x_n)$ be a convex polytope and let F be a face of P. Then there exists a supporting hyperplane H of P such that $F = P \cap H$ with $x_1, ..., x_j \in F$ and $x_{j+1}, ..., x_n \in int\,(H^+)$ for some $j \in \{1, ..., n\}$. Then

$$F = H \cap P \tag{9.36}$$

$$= H \cap \operatorname{conv}(x_1, ..., x_n) \tag{9.37}$$

$$= H \cap \operatorname{conv}(\operatorname{conv}(x_{j+1}, ..., x_n), \operatorname{conv}(x_1, ..., x_j)). \tag{9.38}$$

Since H is affine, $\operatorname{conv}(x_1, ..., x_j)$ and $\operatorname{conv}(x_{j+1}, ...x_n)$ are both convex, and $H \supseteq \operatorname{conv}(x_1, ..., x_j)$, we can rewrite the right-side expression using Proposition 9.6:

$$F = \operatorname{conv}(H \cap \operatorname{conv}(x_{j+1}, ..., x_n), \operatorname{conv}(x_1, ..., x_j)) \tag{9.39}$$

$$= \operatorname{conv}(\emptyset, \operatorname{conv}(x_1, ..., x_j)) \tag{9.40}$$

$$= \operatorname{conv}(x_1, ..., x_j). \tag{9.41}$$

Therefore, F is a convex polytope.

Statement 1: Now, observe that we just showed that each non-empty face of P is the convex hull of a subset of $\{x_1, ..., x_n\}$, which is a finite set. Thus, the number of faces of P must be finite. $\square$

Theorem 9.2. (*Vertices of Convex Polytope [7]*). *A convex polytope is the convex hull of its vertices.*

Proof *Let P be a convex polytope. If $P = \emptyset$, then it has no vertices and the result is vacuously true. Now, consider a non-empty $P = \text{conv}\,(x_1, ..., x_n)$. Suppose that this convex hull presentation of P is minimal in the sense that*

$$P \neq \text{conv}\,(x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) = S_i \tag{9.42}$$

for all i in $\{1, ..., n\}$. We show that this implies that each x_i is a vertex and hence, P is the convex hull of its vertices.

First, note that by supposition, $x_i \notin S_i$. Second, we have that S_i is compact because it is the convex hull of a compact set $\{x_1, ..., x_{i-1}, x_{i+1}, ..., x_n\}$ (Proposition 7.2, item 1). Putting these together we get that S_i is a convex and compact set not containing x_i. Proposition 7.2, item 2 then implies the existence of a hyperplane H passing through x_i such that $S_i \subseteq int\,(H^+)$. We claim that H is an appropriate hyperplane to establish that x_i is a vertex.

We must show that (a) $\{x_i\} = H \cap P$ and (b) $P \subseteq H^+$. For the former, observe that

$$H \cap P = H \cap \text{conv}\,(S_i, \{x_i\})\,. \tag{9.43}$$

Since H is affine, $\{x_i\}$ and S_i are both convex, and $H \supseteq \{x_i\}$, we can rewrite the right-hand side of Equation (9.43) with Proposition 9.6 to obtain:

$$H \cap P = \mathrm{conv}\left(H \cap S_i, \{x_i\}\right) \tag{9.44}$$

$$= \mathrm{conv}\left(\emptyset, \{x_i\}\right) \tag{9.45}$$

$$= \{x_i\}\,. \tag{9.46}$$

It remains to show that P is contained in H^+. Note that $\{x_i\}$ and S_i are both subsets of H^+ and that $P = \mathrm{conv}\left(\{x_i\}, S_i\right)$. Then $P \subseteq H^+$ because halfspaces are convex. Therefore, x_i is a vertex of P. $\square$

We close this section by underlining once more its main takeaway: that ST-modularity may have applications in the study of convex sets and polytopes.

Chapter 10

Conclusion

10.1 Introduction

For nine chapters, we have travelled across lattice wonder-land. We encountered the fundamentals of posets and lattices. We also marched along the fields of distributive and modular lattices, visited the characterization of finite lattices, and took a tour on lattice congruences. We even briefly crossed the boundary into the territory of convex polytopes. Two relevant landmarks that must be mentioned were the cut-complex poset and the short-cuts to the proof of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. Of course, the main milestone of our quest was discovering ST-distributive and ST-modular lattices.

We now bring this journey to an end in this final chapter. We first look back at what we have accomplished in terms of new results in Section 10.2. We then finish with diverse ideas for extending our research in Section 10.3 that may be the starting point for future travels to the world of lattices.

10.2 Summary of Results

10.2.1 ST-Distributive and ST-Modular Lattices

Our main contribution is to have defined two new classes of lattices that generalize, respectively, distributive and modular lattices: ST-distributive lattices and ST-modular lattices (Chapters 8 and 9). These were based on relative distributive and modular properties that a lattice L may satisfy with respect to a pair of subsets (S, T) of it. Unsurprisingly, it turned out that ST-distributive implies ST-modular but not vice-versa. We also established several basic shared properties including:

1. ST-meet distributive (modular) and ST-join distributive (modular) are not equivalent.

2. ST-distributive (modular) and TS-distributive (modular) are not equivalent.

3. Efficiency criteria that provide conditions on order relations among a triple of elements (a, b, c) that guarantee that the expressions $a \wedge (b \vee c)$ and $a \vee (b \wedge c)$ satisfy the required distributive (modular) statements.

4. A lattice L is ST-distributive (modular) for any $S \subseteq L$ if T is a chain sublattice of L.

5. For a fixed subset $T \subseteq L$, the set of subsets S of L for which L is ST-distributive (modular) is a complete lattice under set operations.

Afterwards, our treatment of the two new lattice classes diverged. In the case of ST-distributive lattices, we defined maximal ST-pairs as pairs of proper subsets of a lattice that cannot be expanded further without losing either ST-distributivity or proper-ness. We then proposed the searching of lattices for maximal ST-pairs subject to three additional restrictions: disjointness, exclusion of lattice identities, and non-emptiness. Finally, we developed an algorithm for this search and used it to characterize the maximal ST-pairs of the $\mathbf{M}_n$ and $\mathbf{M}_{n,n}$ families.

In contrast, for ST-modular lattices, we discussed the original motivation for our work: an application to convex sets based on the following convex set identity from [7] (where $A, B, C \subseteq \mathbb{R}^d$ with A affine, B and C convex, and $A \supseteq C$):

$$A \cap \operatorname{conv}(B, C) = \operatorname{conv}(A \cap B, C) \tag{10.1}$$

that we translated to ST-meet modularity in the lattice of convex sets (which is non-modular). We then showed that this identity can be used to reprove two classical theorems on convex polytopes (Theorems 9.1 and 9.2). As a result, we proposed the use of ST-modularity as a tool in the study of convex polytopes.

10.2.2 Additional Results

In addition to introducing ST-distributive and ST-modular lattices, this thesis also presented some additional results related to lattices: the cut-complex poset [9] of Section 7.6 and two short-cuts to the proof of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem [11] in Section 4.6.

The cut-complex poset was the result of defining an order relation on the set of cut-complexes of a hypercube (up to isomorphism). The order relation was based on whether one cut-complex could be obtained from another by adding a finite sequence of vertices of the d-cube. We applied this to the 4-cube c^4 and showed that the resulting poset $\mathcal{C}c(C^4)$ is a distributive lattice.

The short-cuts of the proof of the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem were the result of "algebraic efficiencies" in proving the statement $u \wedge v = p$ in the theorem's proof found in [5, 4]. We proposed and applied two methods for comparing the length of the three proofs: the proof count method and the proof poset method. The former was more intuititve while the latter was more rigorous. Both demonstrated that the new proofs were shorter than the proof in [5, 4] but the difference was more marked in the proof count method.

10.3 Future Work

In this final section, we suggest ideas for continuing the research presented in this thesis. We will focus mostly on the study of ST-distributive and ST-modular lattices, which we will call ST-theory from now on, but we will also touch the cut-complex poset and the proof length comparisons.

We have barely scratched the surface of the fascinating new field that ST-theory can become if properly nurtured. Thus, there is plenty to do. Some natural first steps are to repeat the search problem in Problem 8.1 with other lattice families and with ST-modularity and to try variations of this search problem. The knowledge gained from this process can then lead to the development of a more general ST-theory. A major goal in this new theory is try to characterize the subsets that induce these relative properties in a manner similar to the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem. Another important aspect to consider is finding more applications and connections of ST-theory to other areas of mathematics. We now give list of open problems that can serve as an entry point for anyone interested in joining the study of ST-theory.

Problem 10.1. (*Search expansion*) *Repeat the search problem in Problem 8.1 with other families of lattices and with ST-modularity when applicable. Some families to try include:*

1. *Lattices of the form $M_{n_1,\ldots,n_k}$, which generalize further the $M_{n,n}$ family (see Figure 10.1 for an example);*

2. *Cubical lattices (see Definition 7.13);*

3. *Subgroup lattices: In particular, the following for $n \geq 4$ (see [17]):*

   (a) $\mathrm{Sub}\, A_n$ (alternating group),

   (b) $\mathrm{Sub}\, D_{2^n}$ (dihedral group),

   (c) $\mathrm{Sub}\, Q_{2^n}$ (generalized quaternions).

Problem 10.2. (*Search variations*) *Perform searches of pairs inducing ST-distributivity and/or ST-modularity but modifying the restrictions of Problem 8.1. For instance, we can try:*

1. *considering non-disjoint S and T,*

2. *allowing 0 and 1 in S and T,*

3. *allowing empty S and T,*

4. requiring that S and T be sublattices.

Problem 10.3. (*Efficient algorithms*) *Find faster algorithms to improve on Algorithm 8.1* (*important to search larger lattices*)*.*

Problem 10.4. (*Tricks*) *Find more conditions on a triple of elements that guarantee the distributive* (*modular*) *law for that triple* (*in the vein of the Efficiency Criteria of Properties 8.1 and 9.1*)*. In particular, search for conditions for distributivity in modular non-distributive lattices.*

Problem 10.5. (*Complete lattice*) *Study the complete lattices of S's with fixed T in Lemmas 8.1 and 9.1.*

Problem 10.6. (*Homomorphic ST-modularity*) *Determine if ST-modularity is preserved by homomorphic image* (*see Proposition 9.5*)*.*

Problem 10.7. (*Convex set application*) *Deepen the connection between ST-theory and convex sets. For instance:*

1. *Look for more examples where the ST-meet modularity of the lattice of convex sets discussed in Section 9.4 can be applied.*
2. *Find further examples of ST-modularity in convex sets.*
3. *Find examples of ST-distributivity in convex sets.*
4. *Reprove more convexity theory results using ST-theory if possible. This could eventually strengthen the connection between polytopes and lattice theory to the point that we may tackle open problems in convexity theory with this new language of ST-theory.*

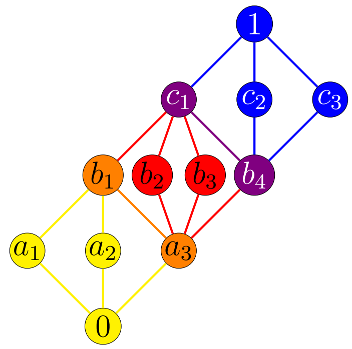


Figure 10.1: Lattice $\mathbf{M}_{3,4,3}$: Primary colors (red, blue, and yellow) indicate the glued sublattices while their mixes (orange, purple) identify shared vertices and edges.

We remark that items 2-4 need not be restricted to the lattice of convex sets. Other lattices constructed from convex sets and polytopes may be considered.

Problem 10.8. (*Relative* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem*) *Establish a characterization of* ST*-distributive and* ST*-modular lattices similar to the* $\mathbf{M}_3$-$\mathbf{N}_5$ *Theorem.*

In addition to discussing future work in ST-theory, we also provide some ideas to extend the work on the "detour" problems of Sections 7.6 and 4.6: the cut-complex poset and the proof length problem of the short-cuts to the $\mathbf{M}_3$-$\mathbf{N}_5$ Theorem proof.

Problem 10.9. (*Cut-complex problems*) *Generalize the cut-complex poset* $\mathcal{C}c(C^4)$ *to all dimensions and study the resulting family of posets* $\mathcal{C}c(C^d)$ *in the following ways:*

1. *Verify if distributive and modular properties are preserved in higher dimensions (if not, apply* ST*-theory).*

2. *Try to gather more informations about the cut-complexes from their posets.*

Problem 10.10. (*Proof length comparison problems*) *Develop further both proof length comparison methods and apply them to other proofs in lattice theory. Ideas for this development include:*

1. *Proof count method:*

    (a) *Consider other aspects that can be counted.*

    (b) *Add different weights to different symbols.*

2. *Proof poset method:*

    (a) *Refine better basic rules.*

    (b) *Add different weights to different rules based on how basic they are.*

This concludes our journey to the realm of lattices. Nevertheless, there are clearly many reasons to return.

Appendix A

Program

Here we include the SageMath code for the program mentioned in Section 8.4.

Program A.1. (*SageMath Code*) *Implementation of Algorithm 8.1*

Note: Some lines of code have been split in order to make the program text fit within the page margins.

```
#function that checks if meet of s distributes into
#join of t1 and t2
def meet_distr(L,s,t1,t2):
    if L.meet(s,L.join(t1,t2)) ==
    L.join(L.meet(s,t1),L.meet(s,t2)):
        return true
    else:
        return false
#function that checks if join of s distributes into
```

```
#meet of t1 and t2

def join_distr(L,s,t1,t2):

    if L.join(s,L.meet(t1,t2)) ==

    L.meet(L.join(s,t1),L.join(s,t2)):

        return true

    else:

        return false

#function that checks if one of the efficiency criteria

#can be applied to the triple s,t1,t2.

def eff_check(L,s,t1,t2):

    if (L.is_gequal(t1,t2) or L.is_lequal(t1,t2)):

        return true

    elif (L.is_gequal(s,t1) and L.is_gequal(s,t2)):

        return true

    elif (L.is_lequal(s,t1) and L.is_lequal(s,t2)):

        return true

    else:

        return false

#function that checks if s distributes into

#pairs of elements of T (both forms of distribution)

def s_distr_check(L,T,s):

    m = len(T)

    for i in range(m):
```

```
        for j in range(i+1,m):

            if eff_check(L,s,T[i],T[j]):

                continue

            if not (meet_distr(L,s,T[i],T[j]) and

            join_distr(L,s,T[i],T[j])):

                return false

    return true

#function that given a fixed subset T of L,

#finds largest S such that L is ST-distributive

def find_S_for_T(L,T):

    S = []

    top = L.top()

    bottom = L.bottom()

    Lset = Set(L.list())

    Tset = Set(T)

    #candidates for S

    maybe_S =

    list(Lset.difference(Tset.union(Set([bottom,top]))))

    #check if each candidate s can be added to S

    for s in maybe_S:

        if s_distr_check(L,T,s):

            S.append(s)

    return Set(S)
```

```
#function that adds a new ST-pair to a list of such pairs,
#removing any pairs contained by the new pair
def add_st_pair(pairs,S,T):
    num_pairs = len(pairs)
    i = 0
    #removing any pairs contained by the new pair
    #(same S, larger T)
    while i < num_pairs:
        if pairs[i][0] == S and pairs[i][1].issubset(T):
            pairs.remove(pairs[i])
            i-=1
            num_pairs-=1
        i+=1
    pairs.append([S,T])
    return pairs
#function that given a lattice L, finds all pairs S,T
#such that L is maximal ST-distributive
def find_maximal_st_pairs(L):
    pairs = []
    size = len(L.list())
    top = L.top()
    bottom = L.bottom()
    Lset = Set(L.list()) #turning L to a set
```

```
    K = Lset.difference([bottom,top])
    #Checking all possible T's by increasing size and
    #finding largest S for which L is ST-distributive
    for m in range(1,size-1):
        powK = Subsets(K,m).list()
        for T in powK:
            S = find_S_for_T(L,T)
            if S.is_empty():
                continue
            else:
                pairs = add_st_pair(pairs,S,T)
    return pairs
#function that finds and prints all maximal ST-pairs of L
def print_maximal_st_pairs(L):
    pairs = find_maximal_st_pairs(L)
    for pair in pairs:
        print pair
######
#Examples: M_n,n
#Creating lattices M_n,n for different n's
x33 = [0,1,'a1','a2','a3','b1','b2','b3']
e33 = [[0,'a1'],[0,'a2'],[0,'a3'],['a1','b1'],['a2','b1'],
['a3','b1'],['a3','b2'],['a3','b3'],['b1',1],['b2',1],['b3',1]]
```

```
M33 = LatticePoset((x33,e33),cover_relations = true,)

x44 = [0,1,'a1','a2','a3','a4','b1','b2','b3','b4']

e44 = [[0,'a1'],[0,'a2'],[0,'a3'],[0,'a4'],['a1','b1'],

['a2','b1'],['a3','b1'],['a4','b1'],['a4','b2'],['a4','b3'],

['a4','b4'],['b1',1],['b2',1],['b3',1],['b4',1]]

M44 = LatticePoset((x44,e44),cover_relations = true,)

print_maximal_st_pairs(M33)

print_maximal_st_pairs(M44)
```

Bibliography

[1] George Bergman. On lattices of convex sets in $\mathbb{R}^n$. *Algebra Universalis*, 53(2–3):357–395, 2005.

[2] Garrett Birkhoff. *Lattice Theory*. American Mathematical Society, New York, 3rd edition, 1967.

[3] Arne Brønsted. *An Introduction to Convex Polytopes*. Springer-Verlag, New York, 1st edition, 1983.

[4] Stanley Burris and Hanamantagouda P. Sankappanavar. *A Course in Universal Algebra*. Springer-Verlag, 1st edition, 1981. Retrieved from the Millenium Edition, an online reprint from 2009 (updated in 2012) of the original 1981 Springer-Verlag edition.

[5] Brian Davey and Hilary Priestley. *Introduction to Lattices and Order*. Cambridge University Press., Cambridge, UK, 2nd edition, 2002.

[6] M. Reza Emamy-K. On the cuts and cut number of the 4-cube. *Journal of Combinatorial Theory Series A*, 41(2):221–227, 1986.

[7] M. Reza Emamy-K. Elements of convex polytopes: An application of projective functionals. UPR Preprint, 2000.

[8] M. Reza Emamy-K. A cartesian system of rotational hyperplanes and elements of convex polytopes. UPR Preprint, 2022.

[9] M. Reza Emamy-K and Gustavo A. Meléndez Ríos. On a convex geometric connection to threshold logic. UPR Preprint, 2021.

[10] M. Reza Emamy-K and Gustavo A. Meléndez Ríos. ST-distributive and ST-modular lattices. UPR Preprint, 2021.

[11] M. Reza Emamy-K and Gustavo A. Meléndez Ríos. Notes on a short-cut to the proof of the M_3-N_5 Theorem. UPR Preprint, 2022.

[12] George Grätzer. *Lattice Theory: Foundation*. Springer, Basel, 1st edition, 2011.

[13] Branko Grünbaum. Polytopes, graphs, and complexes. *Bull. Amer. Math. Soc.*, 76(6):1131–1201, 1970.

[14] Branko Grünbaum. *Convex Polytopes*. Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 2003.

[15] James R. Munkres. *Topology*. Pearson, New York, 2nd edition, 2018. Originally published in 2000, reissued in 2018 as part of Pearson's modern classic series.

[16] Ivan Rival. Maximal sublattices of finite distributive lattices. *Proc. Am. Math. Soc.*, 37(2):417–420, 1973.

[17] Roland Schmidt. *Subgroup Lattices of Groups*. Walter de Gruyter, Berlin, 1st edition, 1994.

[18] N.J.A. Sloane. Sequence A000372 (Dedekind Numbers) at The On-Line Encyclopedia of Integer Sequences, 2021.

[19] Christian Sohler and Martin Ziegler. Computing cut numbers. In *Proceedings of the 12th Canadian Conference on Computational Geometry (CCCG'00)*, page 73–79, 2000.

[20] Richard Stanley. Supersolvable lattices. *Algebra Universalis*, 2(1):197–217, 1972.

[21] Richard Stanley. *Enumerative Combinatorics, Volume I*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2nd edition, 2011.