Discrete Mathematics (II)	Spring 2012

Lecture 2: Lattice(II)

Lecturer: Yi Li

1 Introduction

In this lecture, we will introduce some special lattices. And a very special structure called a Boolean algebra will be discussed in detail, which has a great many applications in computer science.

2 Ideal

We have already learned *ideal* of a ring. A lattice is an algebraic structure which looks like a ring for both have two operations. Similarly, a lattice also has a special structure named as the same as *ideal*.

Definition 1. *A subset I of a lattice L is an* ideal *if it is a sublattice of L and $x \in I$ and $a \in L$ imply that $x \cap a \in I$.*

Specially, A *proper* ideal I of L is *prime* if $a, b \in L$ and $a \cap b \in I$ imply that $a \in I$ or $b \in I$.

Specially, $\{0\}$ and L itself are two trivial ideals. Let's consider the following example.

Example 1. *Given a lattice and two sublattices P and I as shown in Figure 1, where $P = \{a, 0\}$ and $I = \{0\}$.*

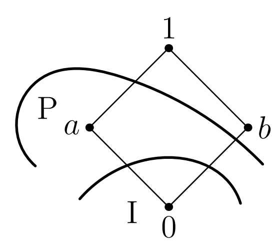

Figure 1: Ideal and prime ideal

According to the definition, P is a prime ideal and I is just an ideal. Why is I not prime?

Since the intersection of any number of *convex* sublattices(ideals) is a convex sublattice(ideal) unless void, we can define the convex sublattice generated by a subset H, and the ideal generated by a subset H of the lattice L, provided that $H = \emptyset$. The ideal generated by a subset H will be denoted by $id(H)$, and if $H = \{a\}$, we write $id(a)$ for $id(a)$; we shall call $id(a)$ a *principal ideal.* A commonly used notation for $id(H)$ is $(H]$ and for $id(a)$ it is $(a]$.

We first introduce a concept. For an order P, a subset $A \subseteq P$ is called *down-set* if $x \in A$ and $y \leq x$ imply that $y \in A$.

Theorem 2. *Let L be a lattice and let H and I be nonempty subsets of L.*

1. *I is an ideal if and only if the following two conditions hold:*
   (a) *$a, b \in I$ implies that $a \cup b \in I$,*
   (b) *I is a down-set.*
2. *$I = id(H)$ if and only if*
$$I = \{x | x \leq h_0 \cup \cdots \cup h_{n-1} \text{ for some } n \geq 1 \text{ and } h_0, \ldots, h_{n-1} \in H\}.$$
3. *For $a \in L$,*
$$id(a) = \{x \cap a | x \in L\}.$$

Proof. We prove the theorem one by one.

1. Let I be an ideal. Then $a, b \in I$ implies that $a \cup b \in I$, since I is a sublattice, verifying (a). If $x \leq a \in I$, then $x = x \cap a \in I$, and (b) is verified.

   Conversely, let I satisfy (a) and (b). Let $a, b \in I$. Then $a \cup b \in I$ by (a), and, since $a \cap b \leq a \in I$, we also have $a \cap b \in I$ by (b); thus I is a sublattice. Finally, if $x \in L$ and $a \in I$, then $a \cap x \leq a \in I$, thus $a \cap x \in I$ by (b), proving that I is an ideal.
2. Let I_0 be the set on the right side of the displayed formula in 2. Using 1, it is clear that I_0 is an ideal, and obviously $H \subseteq I_0$. Finally, if $H \subseteq J$ and J is an ideal, then $I_0 \subseteq J$, and thus I_0 is the smallest ideal containing H; that is, $I = I_0$.
3. This proof is obviously simple or direct to applying 2.

It is proved. □

3 Special Lattice

Before *Boolean lattice* is given, we first introduce some lattice with some special properties.

Definition 3. *A lattice L is complete if any(finite or infinite) subset $A = \{a_i | i \in I\}$ where I is a subset of index set of L, has a least upper bound $\cup_{i \in I} a_i$ and a greatest lower bound $\cap_{i \in I} a_i$.*

Definition 4. *A lattice L is bounded if it has a greatest element 1 and a least element 0.*

Theorem 5. *Finite lattice $L = \{a_1, \ldots, a_n\}$ is bounded.*

Proof. Let $1 = \cup_{i=1}^{n} a_i$ and $0 = \cap_{i=1}^{n} a_i$. □

Definition 6. *A lattice L with 0 and 1 is said to be complemented if for every $a \in L$ there exists an a' such that $a \cup a' = 1$ and $a \cap a' = 0$.*

Here, a' is also called a complement of a. Sometimes, we can relax the restrictions by defining complement of b relative to a as $b \cup b_1 = a, b \cap b_1 = 0$ if $b, b_1 \leq a$.

Example 2. *$< \mathcal{P}(S), \subseteq >$ is complemented for any nonempty set S.*

It is easy to verify that $LUB(A_1, A_2) = A_1 \cup A_2$ and $GLB(A_1, A_2) = A_1 \cap A_2$ where $\cup$ and $\cap$ is the operation union and intersection respectively.

And we know $\cap$ and $\cup$ on set is complemented.

Example 3. *Given a poset $< \{0, a, b, c, 1\}, R >$ described in Figure 2.*

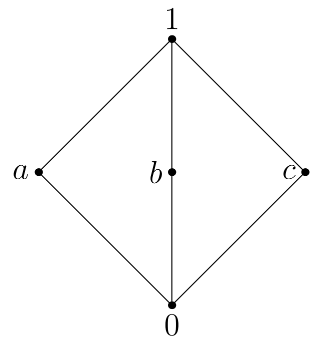

Figure 2: Complemented Lattice.

We can see that a has two complements b and c.

$\cap$ and $\cup$ on set is distributive. Similarly, we have

Definition 7. *A lattice L is distributive if for any $a, b, c \in L$ such that:*

1. $a \cap (b \cup c) = (a \cap b) \cup (a \cap c)$.
2. $a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$.

If a lattice is not distributive, we call it non-distributive.

Example 4. *$< \mathcal{P}(S), \subseteq >$ is distributive for any nonempty set S.*

Based on Example 2, we have that $\cap$ and $\cup$ on set is distributive.

4 Boolean Algebra

Historically, Boolean algebras were the first lattices to be studied. They were introduced by Boole in order to formalize the calculus of propositions. Actually, the theory of Boolean algebra is equivalent to the theory of a special class of rings.

First, we just pay attention to the structure $< \mathcal{P}(S), \subseteq >$. It is used as an example for every property of a lattice in previous sections including ones in lecture 1. It is so special and named as:

Definition 8. *A Boolean algebra is a lattice with 0 and 1 that is distributive and complemented.*

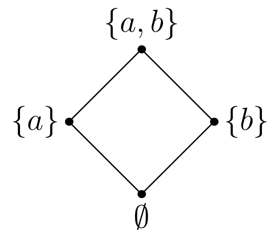

Figure 3: $\mathcal{P}(A)$, where $A = \{a, b\}$.

Example 5. *$< \mathcal{P}(A), \subseteq>$ is a Boolean algebra. Consider a special set $A = \{a, b\}$, its Hasse diagram is Figure 3.*

According to Example 2 and Example 4, it is a Boolean algebra.

Example 6. *$< \{1, 2, 3, 6\}, | >$ is a Boolean algebra.*

First, we can verify that it is distributive and complemented. But it is tedious. In Example **??**, we have proved $< \{1, 2, 3, 6\}, | >$ is isomorphic to $< \mathcal{P}(\{a, b\}), \subseteq>$.

We know the mapping keep the properties of operations $\cap, \cup$. So $< \{1, 2, 3, 6\}, | >$ is also a Boolean algebra.

Generally, we have the following theorem.

Theorem 9 (**Stone**, 1936)**.** *Every finite Boolean algebra is isomorphic to the Boolean algebra of subsets of some finite set S.*

In order to prove it, Boolean algebra is to be represented in another form, which is out of the scope of this course. It is hard and the proof is not easy to be understood. However, the result is elegant.

Corollary 10. *Every finite Boolean algebra has 2^n elements for some n.*

According to this Corollary, if a finite lattice has not 2^n elements, it must not be a Boolean algebra .

Theorem 11. *The complement a' of any element a of a Boolean algebra B is uniquely determined. The mapping $'$ is a one-to-one mapping of B onto itself. It satisfies the conditions.*

$$(a \cup b)' = a' \cap b', \quad (a \cap b)' = a' \cup b'$$

Proof. We prove the theorem one by one.

1. Suppose a has two complement a' and a_1. We have $a \cup a' = 1, a \cap a' = 0, a \cup a_1 = 1$ and $a \cap a_1 = 0$. So $a_1 = a_1 \cap 1 = a_1 \cap (a \cup a') = (a_1 \cap a) \cup (a_1 \cap a') = a_1 \cap a'$.

   Similarly, we can also prove $a' = a_1 \cap a'$. And it means $a' = a_1$.

2. For every $a \in B$, a is a complement of a' according to definition, so $(a')' = a$. It means that $'$ is a bijection.

3. Let $a \leq b$, $a \cap b' \leq b \cap b' = 0$. So, we have $b' \cap 1 = b' \cap (a \cup a') = (b' \cap a) \cup (b' \cup a') = b' \cap a'$, which implies $b' \leq a'$. It also means $'$ inverts the order.

   Given a, b, let $d = a \cup b$, we have $a, b \leq d$ and $d' \leq a', b'$. Then we have $d' \leq a' \cap b'$. But for any $e' \leq a' \cap b'$, we have $e' \leq a', b'$ and $a, b \leq e$, which imply $e \leq a \cup b = d$. So $e' \leq d'$ and it means $(a \cup b)' = (a' \cap b')$.

   Similarly, we can also prove $(a \cap b)' = a' \cup b'$.

It is proved. □

The technique used in this proof is the same as the one used in the last theorem of the previous lecture.

4.1 Ring and Boolean Algebra

Finally, we will establish a connection between a ring and a Boolean algebra. Actually a Boolean algebra is equivalent to a special class of ring.

Given a Boolean algebra B, we first show you how to derive a ring. The point is to define two operations $+$ and $\cdot$ of a ring. We define them from $\cap$ and $\cup$ as the following:

1. Addition: $a + b = (a \cap b') \cup (a' \cap b)$, it is also called the *symmetric difference* of a and b.

2. Multiplication: $a \cdot b = a \cap b$.

The remaining task is to check these two operations satisfying all laws required by a ring, which is tedious and left as an exercise. Then a Boolean algebra introduces a ring. Furthermore, it is a special ring with $a + a = 0$ and $a \cdot a = a$.

Conversely, a special ring can also introduce a Boolean algebra. We first introduce a concept.

Definition 12. *A ring is called* Boolean *if all of its elements are idempotent.*

Given a Boolean ring B with an identity, we just define $a \cup b = a + b - ab$ and $a \cap b = ab$. It is easy to check that $\langle B, \cup, \cap \rangle$ is a Boolean algebra.

Then we have the following theorem.

Theorem 13. *A Boolean algebra is equivalent to a Boolean ring with identity.*

Exercise

1. A lattice is said to be **modular** if, for all $a, b, c, a \leq c$ implies that $a \cup (b \cap c) = (a \cup b) \cap c$.
   (a) Show that a distributive lattice is modular.
   (b) Show that the lattice in shown in the Figure 4 is a nondistributive lattice that is modular.

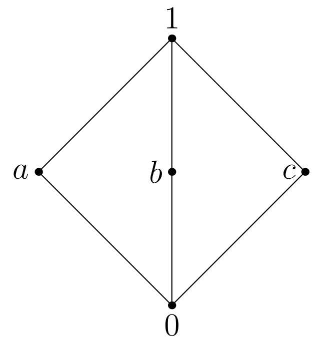

Figure 4: Lattice

2. Show that any complete lattice has a 0 and a 1.

3. Prove that a partially ordered set with 1 in which every nonempty set has a g.l.b. is a complete lattice.

4. In a bounded distributive lattice, an element can have only one complement.

5. Show that in a Boolean algebra the following statements are equivalent for any a and b.

   (a) $a \cup b = b$

   (b) $a \cap b = a$

   (c) $a' \cup b = 1$

   (d) $a \cap b' = 0$

   (e) $a \leq b$

6. Let $A = \{a, b, c, d, e, f, g, h\}$ and R be the relation defined by

$$M_R = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

   (a) Show that the poset (A, R) is complemented and give all pairs of complements.

   (b) Prove or disprove that (A, R) is a Boolean algebra.

7. Prove Theorem 13.