Discrete Mathematics

Yi Li

Software School
Fudan University

March 5, 2013

Review

- Review of a partial order set
- Review of abstract algebra
- Lattice and Sublattice

Outline

- Special Lattices
- Boolean Algebra

Ideal

Definition (Ring)

Given a ring R and a nonempty set $I \subseteq R$. I is an *ideal* of R if it subjects to:

1. For any $a, b \in I, a - b \in I$.
2. For any $a \in I, r \in R, ar, ra \in I$.

Definition (Lattice)

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 $x \cap a \in I$.
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 $b \in I$.

Ideal

Example

Given a lattice and sublattice P and I as shown in the following Figure, where $P = \{a, 0\}$ and $I = \{0\}$.

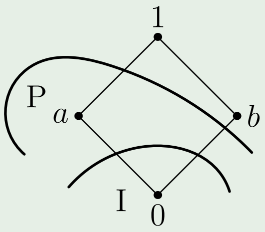

Figure : Ideal and prime ideal

Ideal

Definition

1. 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*.
2. For an order P, a subset $A \subseteq P$ is called *down-set* if $x \in A$ and $y \leq x$ imply that $y \in A$.

Ideal

Theorem

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

Special Lattice

Definition

A lattice L is complete if any(finte or infinite) subset $A = \{a_i | i \in I\}$ has a least upper bound $\cup_{i \in I} a_i$ and a greatest lower bound $\cap_{i \in I} a_i$.

Definition

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

Theorem

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

Special Lattice

Definition

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 $a \cap a' = 0$.

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

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

Special Lattice

Example

Given a poset $< \{0, a, b, c, 1\}, R >$ described in following figure.

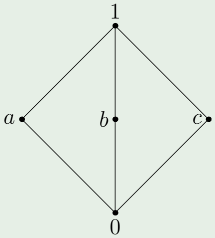

Figure : Complemented Lattice.

Special Lattice

Definition

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

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

Boolean Algebra

Definition

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

Example

$< \mathcal{P}(A), \subseteq >$ is a Boolean algebra. Specially $A = \{a, b\}$.

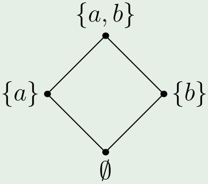

Figure : $\mathcal{P}(A)$, where $A = \{a, b\}$.

Boolean Algebra

Example

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

First, we can verify that it is distributive and complemented. We can prove that $<\{1,2,3,6\},|>$ 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.

Boolean Algebra

Theorem (**Stone**'s Representation Theorem, 1936)

Every finite Boolean algebra is isomorphic to the Boolean algebra of subsets of some finite set S.

Corollary

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

Boolean Algebra

Theorem

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.

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

Boolean Algebra

Definition

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

Theorem

Boolean algebra is equivallent to Boolean ring with identity.

1. Define $a + b = (a \cap b') \cup (a' \cap b)$(*symmetric difference* of a and b) and $a \cdot b = a \cap b$.
2. Conversely, define $a \cup b = a + b - ab$ and $a \cap b = ab$ given a ring.

Next Class

- Introduction to logic
- Some represented concepts