Lecture 7: Partial Order and Lattices

Xiaoxing Ma

Nanjing University

xxm@nju.edu.cn

November 13, 2017

Acknowledgement: These Beamer slides are totally based on the textbook *Discrete Mathematical Structures*, by B. Kolman, R. C. Busby and S. C. Ross, and Prof. Daoxu Chen's PowerPoint slides.

At the Last Class

1. Basics of Functions
   - Function as a class of special relations
   - Types of functions
   - Function and comparison of set size
2. Functions and Computer Science
   - Commonly used functions in computer applications
   - Growth of functions
   - Permutation: bijection on one set

Overview

1. Partial Order
    - Order relations and Hasse Diagrams
    - Extremal elements in partially ordered sets
2. Lattices
    - Lattices as a mathematical structure
    - Isomorphic lattices
    - Properties of lattices

Partial Order

Definition

A relation R on a set A is called a **Partial Order** if R is reflexive, antisymmetric, and transitive.

- Generalization of "less than or equal to"
- Denotation: $\preccurlyeq$
- Example 1: set containment
  Note: not any two of sets are "comparable"
- Example 2: divisibility on $\mathbb{Z}^+$

Partially Ordered Set

Definition

A **partially ordered set (poset)** is a set with a partial order defined on it.

- Denotation: $(A, \preccurlyeq)$
- Examples
  - $(\mathbb{Z}, \leq)$ or $(\mathbb{Z}, \geq)$
  - $(\mathbb{Z}^+, |)$
  - $(2^A, \subseteq)$

Product Partial Order

Given two posets $(A, \preccurlyeq_A)$ and $(B, \preccurlyeq_B)$, we can define a new partial order $\preccurlyeq$ on $A \times B$:

$$(a, b) \preccurlyeq (a', b') \ \text{ iff. } \ a \preccurlyeq_A a' \text{ in } A \text{ and } b \preccurlyeq_B b' \text{ in } B$$

It is easy to prove that $(A \times B, \preccurlyeq)$ is a poset.

Product Partial Order

Given two posets $(A, \preccurlyeq_A)$ and $(B, \preccurlyeq_B)$, we can define a new partial order $\preccurlyeq$ on $A \times B$:

$$(a, b) \preccurlyeq (a', b') \text{ iff. } a \preccurlyeq_A a' \text{ in } A \text{ and } b \preccurlyeq_B b' \text{ in } B$$

It is easy to prove that $(A \times B, \preccurlyeq)$ is a poset.

Lexicographic order, as simplified: Given a partial order on a alphabet A, then $\preccurlyeq$ is a simplified "dictionary" order:

$$(a, b) \preccurlyeq (a', b') \text{ iff. } (a \preccurlyeq a' \text{ and } a \neq a') \text{ or } (a = a' \text{ and } b \preccurlyeq b')$$

Product Partial Order

Given two posets $(A, \preccurlyeq_A)$ and $(B, \preccurlyeq_B)$, we can define a new partial order $\preccurlyeq$ on $A \times B$:

$$(a, b) \preccurlyeq (a', b') \text{ iff. } a \preccurlyeq_A a' \text{ in } A \text{ and } b \preccurlyeq_B b' \text{ in } B$$

It is easy to prove that $(A \times B, \preccurlyeq)$ is a poset.

Lexicographic order, as simplified: Given a partial order on a alphabet A, then $\preccurlyeq$ is a simplified "dictionary" order:

$$(a, b) \preccurlyeq (a', b') \text{ iff. } (a \preccurlyeq a' \text{ and } a \neq a') \text{ or } (a = a' \text{ and } b \preccurlyeq b')$$

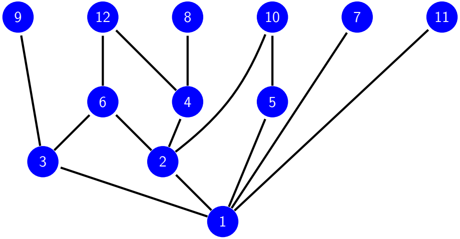
$a \preccurlyeq a'$ and $a \neq a'$ is often denoted as $a \prec a'$.

Hasse Diagrams

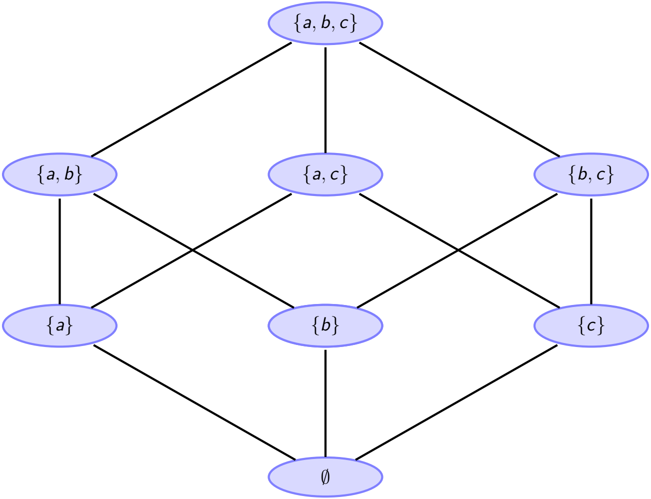
Partial order can be represented by common relation diagram. However, the special properties of partial order can be used to simplifying the diagram.

- Reflexivity: ring everywhere, so no need
- Antisymmetric: no cycle, location dependent
- Transitivity: there is a path, there is a edge

Divisibility on $\{1, 2, \cdots, 12\}$



Containment on $P(\{a, b, c\})$



Isomophism

Definition

Let $(A, \preccurlyeq)$ and $(A', \preccurlyeq')$ be posets and let $f : A \to A'$ be a one-to-one correspondence between A and A'. The function f is called an **isomophism** from $(A, \preccurlyeq)$ to $(A', \preccurlyeq')$ if for any a and b in A, $a \preccurlyeq b$ iff. $f(a) \preccurlyeq' f(b)$. The two posets are called isomophic posets.

Example

$\mathbb{Z}^+$ and the set of positive even number are isomophic under "$\leq$".

Principle of Correspondence.

Maximal and Minimal Elements

Definition

An element $a \in A$ is called a **maximal element** of A if there is no element $c \in A$ such that $a \prec c$.

Definition

An element $b \in A$ is called a **minimal element** of A if there is no element $c \in A$ such that $c \prec b$.

Existence of Maximal/Minimal Elements

Theorem

Given a poset $(A, \preccurlyeq)$, if A is finite, then there is at least one maximal element and at least one minimal element.

Existence of Maximal/Minimal Elements

Theorem

Given a poset $(A, \preccurlyeq)$, if A is finite, then there is at least one maximal element and at least one minimal element.

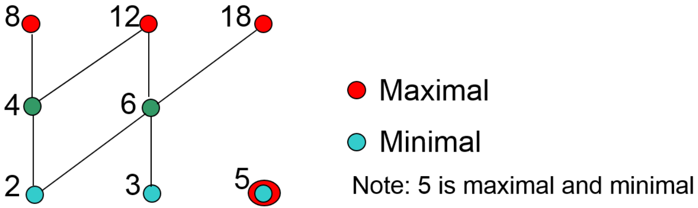
Proof.

Let a be any element of A, If a is not maximal, there must be some a_1, such that $a \preccurlyeq a_1$. If a_1 is not maximal either, there must be some a_2, such that $a_1 \preccurlyeq a_2$. Since a is finite, we can't continue this procedure indefinitely, and find some a_k, which is maximal. Same for the minimal element. $\square$

Examples of Maximal/Minimal Elements

Divisibility on $\{2, 3, 4, 5, 6, 8, 12, 18\}$

- Maximal elements: 5, 8, 12, 18
- Minimal elements: 2, 3, 5



Greatest and Least Elements

Definition

An element $a \in A$ is called a **greatest element** of A if $x \preccurlyeq a$ for all $x \in A$.

Definition

An element $a \in A$ is called a **least element** of A if $a \preccurlyeq x$ for all $x \in A$.

Examples of Greatest and Least Elements

- Containment on $P(\{a, b, c\})$
  - Greatest element: $\{a, b, c\}$
  - Least element: $\emptyset$
- Divisibility on $\{2, 3, 4, 6, 12\}$
  - Greatest element: 12
  - Least element: none (Note: there are two minimal elements: 2 and 3)

Uniqueness of Largest Element

Theorem

A poset has at most one greatest element.

Uniqueness of Largest Element

Theorem

A poset has at most one greatest element.

Proof.

Suppose that there are two greatest elements, a and b. By the definition of the greatest elements, we have $a \preccurlyeq b$, and $b \preccurlyeq a$. So, $a = b$, by the antisymmetry property. $\square$

Uniqueness of Largest Element

Theorem

A poset has at most one greatest element.

Proof.

Suppose that there are two greatest elements, a and b. By the definition of the greatest elements, we have $a \preccurlyeq b$, and $b \preccurlyeq a$. So, $a = b$, by the antisymmetry property. □

It is same for the least element.

Bounds of Subsets of Poset

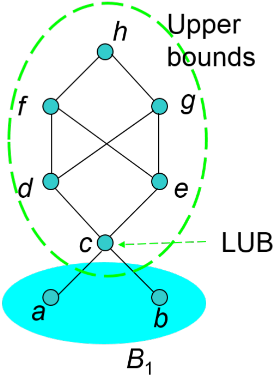
Definition

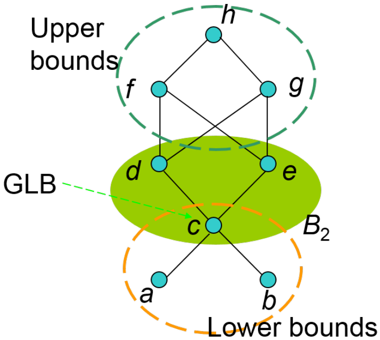
Given a poset A and its subset B, an element $a \in A$ is called an **upper bound** of B if $b \preccurlyeq a$ for all $b \in B$.

For a given subset B, upper bound may not exist. On the other hand, there may be more than one upper bound. The least element (if existing) of the poset consisting of all upper bounds of B is called the **least upper bound (LUB)**.

Lower Bound and **Greatest Lower Bound** can be defined similarly.

Example of Bounds





Linear Ordering and Well-Ordering

$(A, \preccurlyeq)$ is a poset.

- **Linear-ordering** – any two element of A are comparable. Also called **total order**, or **simple order**.
- **Well-ordering** – every nonempty subset of A has a least element.
- If every nonempty subset of A has a least element, then any two elements of A are comparable.
- If any two elements of A are comparable, can it be implied that every nonempty subset of A has a least element?

Linear Ordering and Well-Ordering

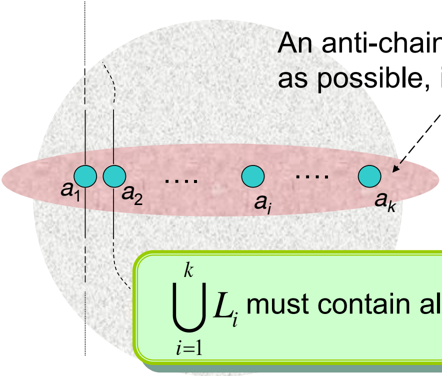
$(A, \preccurlyeq)$ is a poset.

- **Linear-ordering** – any two element of A are comparable. Also called **total order**, or **simple order**.
- **Well-ordering** – every nonempty subset of A has a least element.
- If every nonempty subset of A has a least element, then any two elements of A are comparable.
- If any two elements of A are comparable, can it be implied that every nonempty subset of A has a least element?
  No, for some infinite A.

Chain and Anti-Chain

Definition

A **chain** is a totally ordered subset of a poset S; an **anti-chain** is a subset of a poset S in which any two distinct elements are incomparable.



An anti-chain with elements as many as possible, including k elements

For $i = 1,2,\ldots,k$, starting from a_i, constructing a chain L_i, including as many elements as possible. L_i doesn't contain elements in $L_1,\ldots, L_{i-1}$.

$\bigcup_{i=1}^{k} L_i$ must contain all elements in the poset.

Order in Disorder

Theorem

In any permutation of natural numbers $1, 2, 3, \cdots, n^2 + 1$*, there must be a strictly increasing or decreasing sequence with length not less than* $n + 1$*.*

Order in Disorder

Theorem

In any permutation of natural numbers $1, 2, 3, \cdots, n^2 + 1$*, there must be a strictly increasing or decreasing sequence with length not less than* $n + 1$*.*

Proof.

Given a permutation, labeling each number using a pair (p, q), where p is the length of the largest increasing sequence ending at the number, and q is the length of the largest decreasing sequence ending at the number. Note, each number has a unique label (Why?). If p and q are both not larger than n, there are only n^2 possible label value. □

Order in Disorder

Theorem

In any permutation of natural numbers $1, 2, 3, \cdots, n^2 + 1$, *there must be a strictly increasing or decreasing sequence with length not less than* $n + 1$.

The model of partial order:

Set: $A = \{\langle i, v_i\rangle | i = 1, 2, \cdots, n^2 + 1$, each v_i has an unique value in $1, 2, \cdots, n^2 + 1\}$

Two partial orderings:

R_1: $\langle i, v_i\rangle R_1 \langle j, v_j\rangle$ iff. $i < j$ and $v_i < v_j$

R_2: $\langle i, v_i\rangle R_2 \langle j, v_j\rangle$ iff. $i < j$ and $v_i > v_j$

Problem: Prove that there must a subset of A with no less than $n + 1$ elements, which is a chain of R_1 or R_2.

Note: a chain of R_1 is a anti-chain of R_2, and vice versa.

Lattices

Definition

$(L, \preccurlyeq)$ is called a lattice if

- $(L, \preccurlyeq)$ is a poset.
- For any $x, y \in L$, $\{x, y\}$ has a LUB, which is denoted as $x \vee y$ (join).
- For any $x, y \in L$, $\{x, y\}$ has a GLB, which is denoted as $x \wedge y$ (meet).

Lattices

Definition

$(L, \preccurlyeq)$ is called a lattice if

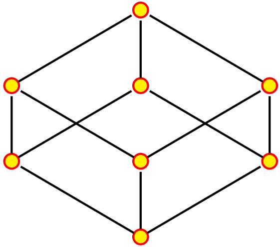
- $(L, \preccurlyeq)$ is a poset.
- For any $x, y \in L$, $\{x, y\}$ has a LUB, which is denoted as $x \vee y$ (join).
- For any $x, y \in L$, $\{x, y\}$ has a GLB, which is denoted as $x \wedge y$ (meet).

Example

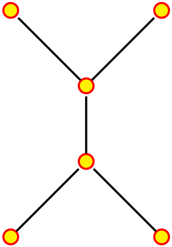
- For $(\{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}, |)$: $x \wedge y = gcd(x, y)$, $x \vee y = lcm(x, y)$;
- For $(P(B), \subseteq)$: $x \wedge y = x \cap y$, $x \vee y = x \cup y$
- For $(\mathbb{Z}, \leq)$: $x \wedge y = min\{x, y\}$, $x \vee y = max\{x, y\}$

Lattice and Hasse Diagram

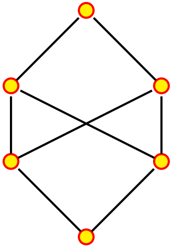
The posets represented by the two Hasse diagram on the right are not lattices.



Yes



No



No

Basic Formula about Lattices

By the definitions of LUB and GLB, it is easy to prove that:

- $a \preccurlyeq a \vee b$, $b \preccurlyeq a \vee b$
- If $a \preccurlyeq c$, $b \preccurlyeq c$, then $a \vee b \preccurlyeq c$
- $a \wedge b \preccurlyeq a$, $a \wedge b \preccurlyeq b$
- If $c \preccurlyeq a$, $c \preccurlyeq b$, then $c \preccurlyeq a \wedge b$

Algebraic Properties of Lattice

Idempotence $a \vee a = a \wedge a = a$

commutativity $a \vee b = b \vee a$; $a \wedge b = b \wedge a$

Associativity $a \vee (b \vee c) = (a \vee b) \vee c$;

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

Absorption $a \vee (a \wedge b) = a$; $a \wedge (a \vee b) = a$

More Properties of Lattices

Let L be a lattice, $\forall a, b, c, d \in L$, If $a \preccurlyeq b$, $c \preccurlyeq d$, then $a \wedge c \preccurlyeq b \wedge d$, $a \vee c \preccurlyeq b \vee d$

- $\because$ $a \wedge c \preccurlyeq a \preccurlyeq b$, $a \wedge c \preccurlyeq c \preccurlyeq d$, then $a \wedge c$ is one lower bound of $\{b, d\}$, $\therefore$ $a \wedge c \preccurlyeq b \wedge d$;
- $\because$ $a \preccurlyeq b \preccurlyeq b \vee d$, $c \preccurlyeq d \preccurlyeq b \vee d$, so, $b \vee d$ is one of the upper bound of $\{a, c\}$, $\therefore$ $a \vee c \preccurlyeq b \vee d$

More Properties of Lattice

Theorem (Distributive Inequality)

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

More Properties of Lattice

Theorem (Distributive Inequality)

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

Proof.

Since $a \preccurlyeq a$ and $b \wedge c \preccurlyeq b$, we have $a \vee (b \wedge c) \preccurlyeq (a \vee b)$, on the other hand, since $a \preccurlyeq a$ and $b \wedge c \preccurlyeq c$, we have $a \vee (b \wedge c) \preccurlyeq (a \vee c)$, i.e. $a \vee (b \wedge c)$ is a lower bound of $\{(a \vee b), (a \vee c)\}$, so $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$. $\square$

More Properties of Lattice

Theorem (Distributive Inequality)

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

Proof.

Since $a \preccurlyeq a$ and $b \wedge c \preccurlyeq b$, we have $a \vee (b \wedge c) \preccurlyeq (a \vee b)$, on the other hand, since $a \preccurlyeq a$ and $b \wedge c \preccurlyeq c$, we have $a \vee (b \wedge c) \preccurlyeq (a \vee c)$, i.e. $a \vee (b \wedge c)$ is a lower bound of $\{(a \vee b), (a \vee c)\}$, so $a \vee (b \wedge c) \preccurlyeq (a \vee b) \wedge (a \vee c)$. □

Similarily, it is easy to prove that:

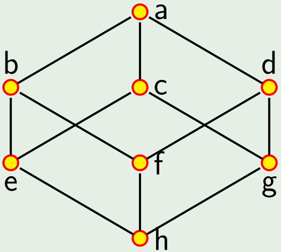
$$(a \wedge b) \vee (a \wedge c) \preccurlyeq a \wedge (b \vee c)$$

Sublattice

Definition

Let $(L, \wedge, \vee)$ is a lattice, S is a nonempty subset of L. If S is close under the operations $\wedge$ and $\vee$, then S is a **sublattice** of L.

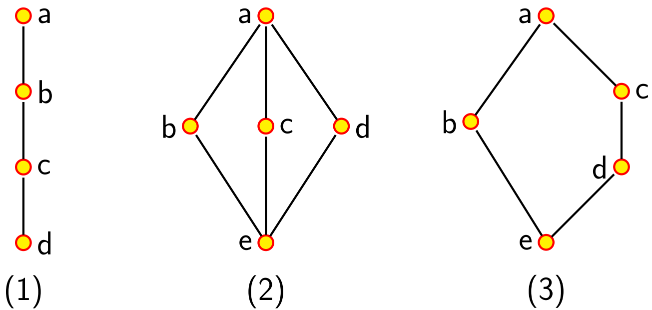
Example



Let $S_1 = \{a, b, d, h\}$; $S_2 = \{a, b, d, f\}$, Then S_2 is a sublattice, but S_1 is not ($b \wedge d \notin S_1$).

Several Special Lattice

1. Chain
2. Diamond lattice. Note: $b \vee (c \wedge a) = (b \vee c) \wedge a = a$
3. Pentagon lattice. Note:
   $c \vee (b \wedge d) = c \vee e = c \neq (c \vee b) \wedge d = a \wedge d = d$



Distributive Lattice

Definition

L is a lattice, if for all $a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, then L is called a **distributive lattice**.

Note: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ iff.
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Distributive Lattice

Definition

L is a lattice, if for all $a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, then L is called a **distributive lattice**.

Note: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ iff.
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Example

Diamond (2) and pentagon (3) are not distributive lattices.

- In (2), $b \wedge (c \vee d) = b$, but $(b \wedge c) \vee (b \wedge d) = e$.
- In (3), $d \vee (b \wedge c) = d$, but $(d \vee b) \wedge (d \vee c) = c$

Distributive Lattice

Definition

L is a lattice, if for all $a, b, c \in L$, $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, then L is called a **distributive lattice**.

Note: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ iff.
$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Example

Diamond (2) and pentagon (3) are not distributive lattices.

- In (2), $b \wedge (c \vee d) = b$, but $(b \wedge c) \vee (b \wedge d) = e$.
- In (3), $d \vee (b \wedge c) = d$, but $(d \vee b) \wedge (d \vee c) = c$

Characteristics of Distributive Lattices

Lattice L is a distributive lattice if and only if it does not contain sublattice isomorphic to diamond lattice or pentagon lattice.

Bounded Lattice

A lattice L is bounded if L has both a greatest element $\mathbf{1}$ and a least element $\mathbf{0}$.

- Finite lattice is bounded lattice
  - $\mathbf{1}$ is $a_1 \vee a_2 \vee \cdots \vee a_n$
  - $\mathbf{0}$ is $a_1 \wedge a_2 \wedge \cdots \wedge a_n$
- If L is a bounded lattice, then for all x in L
  - $\mathbf{1} \wedge x = x$; $\mathbf{1} \vee x = \mathbf{1}$
  - $\mathbf{0} \wedge x = \mathbf{0}$; $\mathbf{0} \vee x = x$

Complement

Definition

Let L is a bounded lattice. For any given element a in L, if there exists some b in L, such that $a \vee b = \mathbf{1}$ and $a \wedge b = \mathbf{0}$, then b is called the **complement** of a.

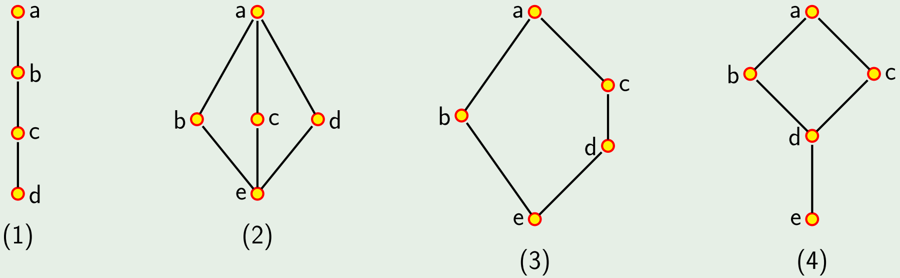
Note: $\mathbf{0}$ and $\mathbf{1}$ are complement of each other.

Complement

Definition

Let L is a bounded lattice. For any given element a in L, if there exists some b in L, such that $a \vee b = \mathbf{1}$ and $a \wedge b = \mathbf{0}$, then b is called the **complement** of a.

Example



Note: $\mathbf{0}$ and $\mathbf{1}$ are complement of each other.

Uniqueness of Complement

Theorem

Let L be a bounded distributive lattice. If a complement exists, it is unique.

Uniqueness of Complement

Theorem

Let L be a bounded distributive lattice. If a complement exists, it is unique.

Proof.

Suppose that b and c are both complements of a, i.e. $a \vee b = 1$, $a \wedge b = 0$; $a \vee c = 1$, $a \wedge c = 0$, then:

$b = b \vee 0 = b \vee (a \wedge c) = (b \vee a) \wedge (b \vee c) = (b \vee c)$

Also, $c = c \vee 0 = c \vee (a \wedge b) = (c \vee a) \wedge (c \vee b) = (b \vee c)$

So, $b = c$ $\square$

Home Assignments

To be checked

- Ex. 6.1: 10, 13, 14, 16, 18, 26-28, 29, 30, 34-36, 38, 40
- Ex. 6.2: 6, 8, 12, 14, 17-19, 20, 22, 23-26, 32, 33, 35-38
- Ex. 6.3: 1-6, 13-15, 18-20, 22, 24-26, 27, 29, 34, 37-40

The End