# VE203
# Discrete Math
# RC3

Yucheng Huang

University of Michigan
Shanghai Jiao Tong University
Joint Institute

March 17, 2022

1. Partial Order

2. Numbers

3. Q&A

# Partial Order

## Definition

An ordered set (or partially ordered set or poset) is an ordered pair $(P, \leq)$ of a set $P$ and a binary relation $\leq$ contained in $P \times P$, called the order (or the partial order) on $P$ such that $\leq$ is

- reflexive: $a \leq a \Rightarrow \top$
- antisymmetric: $a \leq b \wedge b \leq a \Rightarrow a = b$
- transitive: $a \leq b \wedge b \leq c \Rightarrow a \leq c$

We write $x < y$ if $x \leq y$ and $x \neq y$. (Other notation: $\preceq$ and $\prec$ )

# Partial Order

The divisibility relation $|$ is a partial ordering on the set of positive integers, because it is reflexive, antisymmetric, and transitive. We see that $(\mathbf{Z}^+, |)$is a poset. Recall that ( $\mathbf{Z}^+$denotes the set of positive integers.)

# Partial Order

Show that the "greater than or equal" relation ($\geq$)is a partial ordering on the set of integers.

Solution: Because $a \geq a$ for every integer $a$, $\geq$ is reflexive. If $a \geq b$ and $b \geq a$, then $a = b$. Hence, $\geq$ is antisymmetric. Finally, $\geq$ is transitive because $a \geq b$ and $b \geq c$ imply that $a \geq c$. It follows that $\geq$ is a partial ordering on the set of integers and $(\mathbf{Z}, \geq)$ is a poset.

# Covers in a Poset

Let $P$ be an ordered set. Then $y \in P$ is called a cover of $x \in P$ if $x < y$ and for all $z \in P, x \leq z \leq y$ implies $z \in \{x, y\}$. We also say that $y$ covers $x$, or $x$ is covered by $y$. Such $x$ and $y$ are called adjacent.

# More Definitions

Let $(P, \leq)$ be a poset, and $a, x, y, z \in P$.
If $a \in P$ but $\nexists x \in P$ such that $x < a$, then $a$ is a minimal element.
If $a \leq x$ for all $x \in P$, then $a$ is the minimum element.
If $z \in P$ but $\nexists x \in P$ such that $z < x$, then $z$ is a maximal element.
If $x \leq z$ for all $x \in P$, then $z$ is the maximum element.
If either $x < y$ in $P$ or $y < x$ in $P$, then $x$ and $y$ are comparable in $P$, otherwise $x$ and $y$ are incomparable.

# More Definitions

In the poset $(\mathbf{Z}^{+}, |)$, are the integers 3 and 9 comparable? Are 5 and 7 comparable?

Solution: The integers 3 and 9 are comparable, because $3 \mid 9$. The integers 5 and 7 are incomparable, because $5 \not| 7$ and $7 \not| 5$.

# Total Order

## Definition

If $(S, \preccurlyeq)$ is a poset and every two elements of $S$ are comparable, $S$ is called a totally ordered or linearly ordered set, and $\preccurlyeq$ is called a total order or a linear order. A totally ordered set is also called a chain.

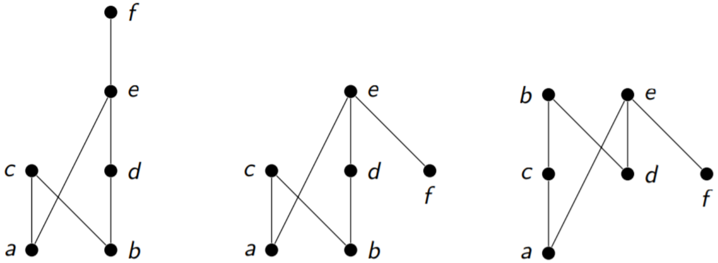
## Examples

The poset $(\mathbf{Z}, \leq)$ is totally ordered, because $a \leq b$ or $b \leq a$ whenever $a$ and $b$ are integers.

The poset $(\mathbf{Z}^{+}, |)$is not totally ordered because it contains elements that are incomparable, such as 5 and 7 .

# Hasse Diagram

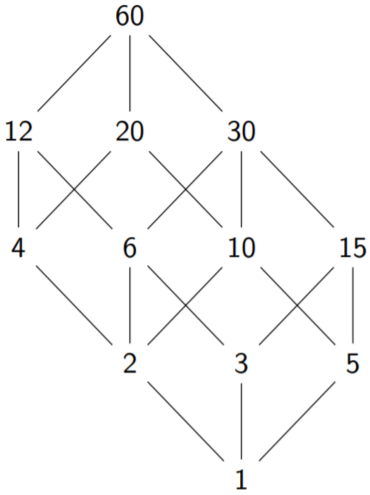
Edges are the cover pairs $(x, y)$ with $x$ covered by $y$;
Edges are drawn such that $x$ is below $y$;
Edges are monotone vertically.



Note that all three are the same as graphs, but not as posets.

# Hasse Diagram

Divisors of $n \in \mathbb{N}$. $(\mathbb{N}, |)$. Ordered by divisibility. $n = 60$.



# Hasse Diagram

Let $P = \{1, 2, 3, 4, 5, 6\}$, and $\leq = \{(1,1),(2,2),(3,3),(4,4),(5,5),(6,6),(6,1),(6,4),(1,4),(6,5),(3,4),(6,2)\}$. Then

6 and 3 are minimal elements.

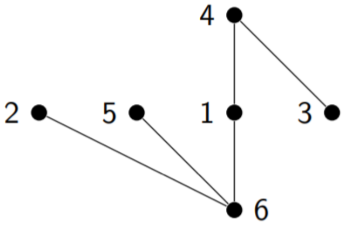
2, 4, and 5 are maximal elements.

4 is comparable to 6 .

2 is incomparable to 3.

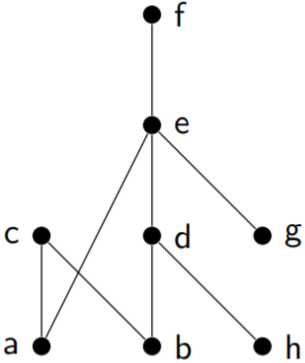
1 covers 6 , and 3 is covered by 4 .

$4 > 6$ but 4 does not cover 6 .



# Hasse Diagram

$c$ and $f$ are maximal elements. $a, b, g$, and h are minimal elements. a is comparable to $f$. $\mathrm{c}$ is incomparable to $\mathrm{h}$. e covers $a$, and $h$ is covered by $d$. $e > h$ but e does not cover $h$.



# Chains and Antichains

Given $(P, \leq)$ poset,
A chain in a poset is a subset $C \subset P$ such that any two elements are comparable.
An antichain in a poset is a subset $A \subset P$ of incomparable elements.

# Chains and Antichains

A chain $C$ in $P$ is
maximal if there exists no chain $C'$ such that $C \subsetneq C'$.
maximum if for all chain $C', |C| \nless |C'|$. The height (not length) of a poset $P$, denoted by $h(P)$, is the maximum size of a chain in $P$.

An antichain $A$ in $P$ is
maximal if there exists no antichain $A'$ such that $A \subsetneq A'$.
maximum if for all chain $A', |A| \nless |A'|$. The width of a poset $P$, denoted by $w(P)$, is the maximum size of an antichain in $P$.

# Hasse diagram

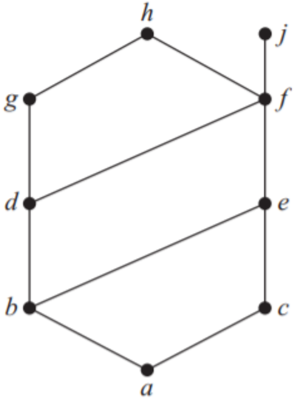
Draw the Hasse diagram representing the partial ordering $\{(a, b) \mid a \text{ divides } b\}$ on $\{1, 2, 3, 4, 6, 8, 12\}$.

# Least Upper and Greatest Lower Bounds

The element $u$ is called the least upper bound (lub) or supremum or join of $A$ if $u \geq A$ and, for all $p \in P$ with $p \geq A$, we have $p \geq u$. The element $l$ is called the greatest lower bound (glb) or infimum or meet of $A$ if $l \leq A$ and, for all $p \in P$ with $p \leq A$, we have $p \geq l$.

# Least Upper and Greatest Lower Bounds

Find the lower and upper bounds of the subsets $\{a, b, c\}$, $\{j, h\}$, and $\{a, c, d, f\}$ in the poset with the Hasse diagram



# Least Upper and Greatest Lower Bounds

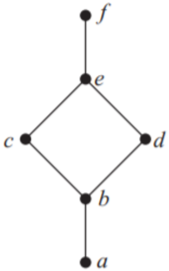
Solution: The upper bounds of $\{a, b, c\}$ are $e, f, j$, and $h$, and its only lower bound is $a$. There are no upper bounds of $\{j, h\}$, and its lower bounds are $a, b, c, d, e$, and $f$. The upper bounds of $\{a, c, d, f\}$ are $f, h$, and $j$, and its lower bound is $a$.

# Lattice

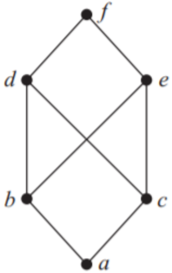
Let $L$ be an ordered set. Then $L$ is called a lattice if any two elements of $L$ have a supremum and an infimum. $L$ is called a complete lattice iff any subset of $L$ has a supremum and an infimum.

# Lattice

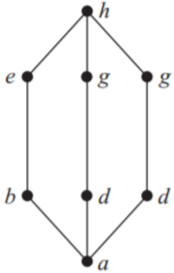
Determine whether the posets represented by each of the Hasse diagrams are lattices.



(a)



(b)



(c)

# Lattice

Solution: The posets represented by the Hasse diagrams in (a) and (c) are both lattices because in each poset every pair of elements has both a least upper bound and a greatest lower bound, as the reader should verify. On the other hand, the poset with the Hasse diagram shown in (b) is not a lattice, because the elements $b$ and $c$ have no least upper bound. To see this, note that each of the elements $d, e$, and $f$ is an upper bound, but none of these three elements precedes the other two with respect to the ordering of this poset.

# Lattice

Determine whether the posets $(\{1,2,3,4,5\},|)$ and $(\{1,2,4,8,16\},|)$ are lattices.

Solution: Because 2 and 3 have no upper bounds in $(\{1,2,3,4,5\},|)$, they certainly do not have a least upper bound. Hence, the first poset is not a lattice.
Every two elements of the second poset have both a least upper bound and a greatest lower bound. The least upper bound of two elements in this poset is the larger of the elements and the greatest lower bound of two elements is the smaller of the elements, as the reader should verify. Hence, this second poset is a lattice.

# Topological Sorting (Optional)

See Whiteboard

1. Partial Order
2. Numbers
3. Q&A

# Division

If $a$ and $b$ are integers with $a \neq 0$, we say that $a$ divides $b$ if there is an integer $c$ such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When $a$ divides $b$ we say that $a$ is a factor or divisor of $b$, and that $b$ is a multiple of $a$. The notation $a \mid b$ denotes that $a$ divides $b$. We write $a \not| b$ when $a$ does not divide $b$.

# Division

Determine whether $3 \mid 7$ and whether $3 \mid 12$.
Solution: We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$.

# Prime Numbers

An integer $p$ greater than 1 is called prime if the only positive factors of $p$ are 1 and $p$. A positive integer that is greater than 1 and is not prime is called composite.

# The Sieve of Eratosthenes

The sieve of Eratosthenes is used to find all primes not exceeding a specified positive integer. For instance, the following procedure is used to find the primes not exceeding 100 . We begin with the list of all integers between 1 and 100 . To begin the sieving process, the integers that are divisible by 2 , other than 2 , are deleted. Because 3 is the first integer greater than 2 that is left, all those integers divisible by 3 , other than 3 , are deleted. Because 5 is the next integer left after 3 , those integers divisible by 5 , other than 5 , are deleted. The next integer left is 7 , so those integers divisible by 7 , other than 7, are deleted. Because all composite integers not exceeding 100 are divisible by $2, 3, 5$, or 7 , all remaining integers except 1 are prime. The integers not underlined are the primes not exceeding 100 . We conclude that the primes less than 100 are 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89, and 97 .

# Prime Numbers

Theorem: There are infinitely many primes.

Proof: We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let

$$Q = p_1 p_2 \cdots p_n + 1$$

By the fundamental theorem of arithmetic, $Q$ is prime or else it can be written as the product of two or more primes. However, none of the primes $p_j$ divides $Q$, for if $p_j \mid Q$, then $p_j$ divides $Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either $Q$, if it is prime, or a prime factor of $Q$. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

# Greatest Common Divisors

Let $a$ and $b$ be integers, not both zero. The largest integer $d$ such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of $a$ and $b$. The greatest common divisor of $a$ and $b$ is denoted by $\gcd(a, b)$.

# Greatest Common Divisors

What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are $1, 2, 3, 4, 6,$ and 12. Hence, $\gcd(24, 36) = 12$.

## Greatest Common Divisors

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers $a$ and $b$ are

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either $a$ or $b$ are included in both factorizations, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Let $a$ and $b$ be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$$

# Least Common Multiple

The least common multiple of the positive integers $a$ and $b$ is the smallest positive integer that is divisible by both $a$ and $b$. The least common multiple of $a$ and $b$ is denoted by $\operatorname{lcm}(a, b)$.

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

# The Euclidean Algorithm

```
procedure $gcd(a, b :$ positive integers$)$
    $x := a$
    $y := b$
while $y \neq 0$
    $r := x \bmod y$
    $x := y$
    $y := r$
return $x\{\text{gcd}(a, b) \text{ is } x\}$
```

# The Euclidean Algorithm

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

$$
\begin{aligned}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41.
\end{aligned}
$$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

1 Partial Order

2 Numbers

3 Q&A

# Q&A

Q&A