# Discrete Mathematics

## Order Relation

(c) Marcin Sydow

# Contents

- partial order relation
- linear order
- minimal, maximal elements, chains, anti-chains
- dense, continuous, well ordering
- divisibility relation and basic number theory

# Order relation

A binary relation $R \subseteq X^2$ is called a **partial order** if and only if it is:

1. reflexive
2. anti-symmetric
3. transitive

Denotation: a symbol $\preceq$ can be used to denote the symbol of a partial order relation (e.g. $a \preceq b$)

Note: a pair $(X, \preceq)$ where $\preceq$ is a partial order on X is also called a **poset**.

# Examples



are the following partial orders?:

# Examples



are the following partial orders?:
"$\leq$" on pairs of numbers?

# Examples



are the following partial orders?:
"$\leq$" on pairs of numbers? yes
$aRb \Leftrightarrow$ "a divides b" for nonzero integers?

# Examples



are the following partial orders?:
"$\leq$" on pairs of numbers? yes
$aRb \Leftrightarrow$ "a divides b" for nonzero integers? yes
"$<$" on pairs of numbers?

# Examples

are the following partial orders?:
"$\leq$" on pairs of numbers? yes
$aRb \Leftrightarrow$ "a divides b" for nonzero integers? yes
"$<$" on pairs of numbers? no
$\geq$ on pairs of numbers

# Examples

are the following partial orders?:

"$\leq$" on pairs of numbers? yes

$aRb \Leftrightarrow$ "a divides b" for nonzero integers? yes

"$<$" on pairs of numbers? no

$\geq$ on pairs of numbers yes

$\subseteq$ on pairs of subsets of a given universe?

# Examples



are the following partial orders?:
"$\leq$" on pairs of numbers? yes
$aRb \Leftrightarrow$ "a divides b" for nonzero integers? yes
"$<$" on pairs of numbers? no
$\geq$ on pairs of numbers yes
$\subseteq$ on pairs of subsets of a given universe? yes

# Comparable and uncomparable elements

If $\preceq \subseteq X^2$ is a partial order and for some $x, y \in X$ it holds that $x \preceq y$ or $y \preceq x$ we say that elements $x, y$ are **comparable** in $R$.

Otherwise, x and y are **uncomparable**.

If $x \preceq y$ and $x \neq y$ we say x is "smaller" than y or that y is "greater" than x.

The word **partial** reflects that not all pairs of the domain of partial order must be comparable.

# Linear order



A partial order $R$ that satisfies the following additional 4th condition:

- $\forall x, y \in X \; x \preceq y \vee y \preceq x$
  (i.e. all elements of the domain are comparable)

is called **linear order**.

Examples:
which of the following partial orders are linear orders?
(in negative cases show at least one pair of incomparable elements)

# Linear order

A partial order $R$ that satisfies the following additional 4th condition:

- $\forall x, y \in X \; x \preceq y \vee y \preceq x$
  (i.e. all elements of the domain are comparable)

is called **linear order**.

Examples:
which of the following partial orders are linear orders?
(in negative cases show at least one pair of incomparable elements)
$\leq$ on pairs of numbers?

# Linear order

A partial order $R$ that satisfies the following additional 4th condition:

- $\forall x, y \in X \; x \preceq y \vee y \preceq x$
  (i.e. all elements of the domain are comparable)

is called **linear order**.

Examples:
which of the following partial orders are linear orders?
(in negative cases show at least one pair of incomparable elements)
$\leq$ on pairs of numbers? yes
"a divides b" for non-zero integers?

# Linear order



A partial order $R$ that satisfies the following additional 4th condition:

- $\forall x, y \in X \; x \preceq y \vee y \preceq x$
  (i.e. all elements of the domain are comparable)

is called **linear order**.

Examples:
which of the following partial orders are linear orders?
(in negative cases show at least one pair of incomparable elements)
$\leq$ on pairs of numbers? yes
"a divides b" for non-zero integers? no
(show an incomparable pair)
$\subseteq$ on pairs of subsets of a given universe?

# Linear order

A partial order $R$ that satisfies the following additional 4th condition:

- $\forall x, y \in X \; x \preceq y \lor y \preceq x$
  (i.e. all elements of the domain are comparable)

is called **linear order**.

Examples:
which of the following partial orders are linear orders?
(in negative cases show at least one pair of incomparable elements)
$\leq$ on pairs of numbers? yes
"a divides b" for non-zero integers? no
(show an incomparable pair)
$\subseteq$ on pairs of subsets of a given universe? no
(show an incomparable pair)

# Upper and lower bounds



If $(X, \preceq)$ is a poset and $A \subseteq X$ so that for all $a \in A$ it holds that $a \preceq u$ for some u, u is called **upper bound of A**. Similarly, if for all $a \in A$ it holds that $l \preceq a$, for some l, l is called an **lower bound of A**.

Example: $A = (0, 1) \subseteq R$. 5,2,1 are examples of upper bounds of A, -13,-1,0 are examples of lower bounds of A.

# Maximal and minimal elements



- the element $u$ is **maximal** element of $A \subseteq X \Leftrightarrow$ there is no element $v \neq u$ in $A$, so that $u \preceq v$
- the element $u$ is **minimal** element of $A \subseteq X \Leftrightarrow$ there is no element $v \neq u$ in $A$, so that $v \preceq u$

Note: there can be more than one maximal or minimal element of a set if they are non-comparable (but there might be no maximal or minimal element of a set)

Example: the set $(0, 1] \subseteq R$ has no minimal element. The set of odd naturals has no maximal element.

# Greatest and Smallest element

An element is **greatest** $\Leftrightarrow$ if it is a unique maximal element and it is comparable with all the other elements.

An element is **smallest** $\Leftrightarrow$ if it is a unique minimal element and it is comparable with all the other elements.

Note: there could be a unique maximal (minimal) element that is not greatest (smallest), e.g. the poset $(Q, \leq)$ with "artificially" added one element that is not comparable with any other element (it is a unique minimal *and* maximal but is not greatest nor smallest since it is not comparable with anything)

# Successor and predecessor

- $v$ is a **successor** of $u \Leftrightarrow v$ is the minimal of all the elements larger than $u$ (denotation: $v \succ u$)
- $v$ is a **predecessor** of $u \Leftrightarrow v$ is the maximal of all the elements smaller than $u$ (denotation: $v \prec u$)

Example: in the poset $(N, \leq)$ every element n has a successor (it is $n + 1$) and every element except 0 has a predecessor.

In the poset $(Q, \leq)$ no element has a successor nor predecessor.

# Chain and antichain



Let $(X, \preceq)$ be a poset:

- $C \subset X$ is called a **chain** $\Leftrightarrow$ all pairs of elements of $C$ are comparable
- $A \subset X$ is called an **anti-chain** $\Leftrightarrow$ all pairs of elements of $A$ are uncomparable

Examples:

- $(\{2, 4, 16, 64\}, |)$ is a chain
- $(\{3, 5, 8\}, |)$ is an antichain.

# Hasse diagram

If each non-minimal element has a predecessor and each non-maximal element has a successor it is possible to make the **Hasse Diagram** of a poset $(X, \preceq)$, which is a visualisation of a poset.

Hasse Diagram of a poset $(X, \preceq)$ is a picture of a directed graph $G = (V, E)$, where vertices are the elements of X ($V = X$) and directed arcs represent the successor relation ($E = \{(x, y) \in X^2 : x \prec y\}$). By convention, any larger element on Hasse Diagram is placed higher than any smaller element (if they are comparable).

Example: Hasse Diagram of (show which elements are maximal, minimal, largest, smallest, chains, antichains, etc.):

- $(\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}, |)$
- $(P(\{a, b, c\}), \subseteq)$

# Dense order



If a poset $(X, \preceq)$ has the following property:

For any pair $x, y \in X$ such that $x \preceq y$ it holds that there exists $z$ so that:

- $z \neq x$ and $z \neq y$
- $x \preceq z$ and $z \preceq y$

We call the poset a **dense order**

Example: $(R, \leq)$ is a dense order. $(N, \leq)$ is not a dense order.

Notice: Any non-empty dense order must be infinite.

# Well ordering



A poset $(X, \preceq)$ is **well-ordered** $\Leftrightarrow$ each non-empty subset $A \subset X$ has the smallest element.

Example: $(N, \leq)$ is well-ordered. $(Q, \leq)$ is not well ordered (why?).

# Initial Intervals and Real numbers



For a poset $(X, \preceq)$ an **initial interval of X** is any subset $Y$ of $X$ that satifies the following property: $y \in Y \Rightarrow \forall_{x \preceq y} x \in Y$.

Example: for the poset $(Z, \leq)$ and any $z \in Z$ the set of the form $Y_z = \{x \in Z : x \leq z\}$ is an initial interval. For the poset $(Q, \leq)$, any set of the form $(-\infty, a)$, $a \in Q$ or $(-\infty, a]$ is an initial interval.

**Real numbers** can be defined as **all the possible initial intervals of the set of rational numbers that do not have the largest element**.

# Quasi-order

A binary relation $R \subseteq X^2$ is called a **quasi-order** if and only if it is:

1. reflexive
2. transitive

Note: it is “almost” a partial order but without anti-symmetry.

Example: Asymptotic notation “Big O” for comparing rates of growth of two functions.

# Asymptotic “Big O” notation

Asymptotic notation for functions: For two functions $f, g : N \to N^+$, $(f, g) \in R$ if and only if $\exists_{c \in Z^+} \exists_{n_0 \in N} \forall_{n \geq n_0} f(n) \leq c \cdot g(n)$

We denote this relation as: $f(n) = O(g(n))$ (“Big O” asymptotic notation).

It serves for comparing the **rate of growth of functions**.

Interpretation: $f(n) = O(g(n))$ reads as “the function f has rate of growth not higher than the rate of growth of g”.

Example: $n + 1 = O(n^2)$, n+1 = O(n), log(n) = O(n), etc. But not $n^2 = O(n)$, etc.

# Big O notation is quasi-order



- is reflexive
- is transitive

But is not anti-symmetric, for example:
n+1 = O(n), n = O(n+1)
but: n is a different function than n+1
1/2 n = O(3n), 3n = O(1/2 n)
but 1/2 and 3n are different functions.

# Similarity relation

A relation that is:

- reflexive
- symmetric

is called a **similarity relation**. (notice: similarity is not necessarily transitive)

Denotation: $x \sim y$

Example: $x, y \in R$: $x \sim y \Leftrightarrow |x - y| \leq 1$ is an example of similarity relation.

# Divisibility



For two integers $a, b \in Z$, $a \neq 0$ we say that $a$ **divides** $b \Leftrightarrow$ there exists an integer $c \in Z$ so that $b = a \cdot c$.

We say: a is a **factor** of b, b is a **multiple** of a.

Denotation: $a|b$, if a does not divide b: $a \nmid b$

Example: $17|51$, $7 \nmid 15$

How many are there positive integers divisible by $d \in N^+$ not greater than $n \in N^+$ (e.g.: n = 50, d = 17)?

# Divisibility

For two integers $a, b \in Z$, $a \neq 0$ we say that $a$ **divides** $b \Leftrightarrow$ there exists an integer $c \in Z$ so that $b = a \cdot c$.

We say: a is a **factor** of b, b is a **multiple** of a.

Denotation: $a|b$, if a does not divide b: $a \nmid b$

Example: $17|51$, $7 \nmid 15$

How many are there positive integers divisible by $d \in N^+$ not greater than $n \in N^+$ (e.g.: n = 50, d = 17)? $\lfloor n/d \rfloor$

# Properties of divisibility

For any $a, b, c \in Z$ the following holds:

- if $a|b$ and $a|c$ then $a|(b+c)$
- if $a|b$ then $a|bc$ for any integer $c$
- if $a|b$ and $b|c$ then $a|c$ (transitivity)
- if $a|b$ and $a|c$ then $a|mb+nc$ for any $m, n \in Z$

# Integer Division



For any $a \in Z$ and $d \in Z^+$ **there exist unique integers** $q$ and $r$, where $0 \leq r < d$ such that:

$$a = dq + r$$

Naming: $d$ - **divisor**, $q$ – **quotient**, $r$ – **remainder**

Denotations:

- $q = a \textbf{ div } d$
- $r = a \textbf{ mod } d$ (read: "a modulo d")

# Congruency modulo m



Let $a, b \in Z$ and $m \in Z^+$. A is **congruent to b modulo m** iff m divides (a-b).

Equivalently: $a \equiv b \pmod{m} \Leftrightarrow$ there exists an integer $k \in Z$ such that $a = b + km$

Denotation: $a \equiv b \pmod{m}$

Lemma: $a \equiv b \pmod{m} \Leftrightarrow a\,mod\,m = b\,mod\,m$

Is **congruence equivalence relation**?

# Congruency modulo m



Let $a, b \in Z$ and $m \in Z^+$. A is **congruent to b modulo m** iff m divides (a-b).

Equivalently: $a \equiv b \pmod{m} \Leftrightarrow$ there exists an integer $k \in Z$ such that $a = b + km$

Denotation: $a \equiv b \pmod{m}$

Lemma: $a \equiv b \pmod{m} \Leftrightarrow a \, mod \, m = b \, mod \, m$

Is **congruence equivalence relation**? yes (it is reflexive, symmetric and transitive)

# Properties of congruency



For $a, b, c, d \in Z$ and $m \in Z^+$, if:
$a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then:

- $a + c \equiv b + d \pmod{m}$
- $ac \equiv bd \pmod{m}$

# Prime numbers

A positive integer $p > 1$ is called **prime number** iff it is divisible only by 1 and itself (p). Otherwise it is called a *composite number*.

The sequence of prime numbers:

2,3,5,7,11,13,17,19,23,29,31,37,41,47...

There is no largest prime (i.e. there are infinitely many primes)

# The Fundamental Theorem of Arithmetic



Every positive integer $a$ greater than 1 can be **uniquely represented** as a **prime or product of primes**:

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

where each $e_i$ is a natural positive number.

Examples:
$3 = 3^1$
$333 = 3^2 \cdot 37^1$

# The Fundamental Theorem of Arithmetic



Every positive integer $a$ greater than 1 can be **uniquely represented** as a **prime or product of primes**:

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

where each $e_i$ is a natural positive number.

Examples:
$3 = 3^1$
$333 = 3^2 \cdot 37^1$

To test whether a given number $a$ is prime it is enough to check its divisibility by all prime numbers up to $\lfloor \sqrt{a} \rfloor$ (why?)

# Infininitude of Primes



There are infinitely many primes.

Proof: (reductio ad absurdum) Assume that there are only n (finitely many) primes: $p_1, ..., p_n$. Lets consider the following number: $p = p_1 \cdot ... \cdot p_n + 1$. The number $p$ is not divisible by any prime (the remainder is 1), so that it is divisible only by 1 and itself. So $p$ is a prime number. But $p$ is different than any of the $n$ primes $p_1, ..., p_n$ (as it is larger), what makes a contradiction of the assumptions.

# Prime Number Theorem



The ratio of prime numbers not exceeding $n \in N$ for $n$ tending to infinity has a limit of $n/ln(n)$.

Example:
for $n = 50$ there are 14 primes not greater than 50. The above approximation works quite well even for such a low value of $n$ since $50/ln(50) = 12.78$.

# Greatest Common Divisor (GCD)



For a pair of numbers $a, b \in Z$ (not both being zero) their **greatest common divisor** d is the largest integer $d$ such that $d|a$ and $d|b$.

Denotation: **gcd(a,b)**

Examples: gcd(10,15)=5, gcd(17,12)=1

The numbers $a, b \in Z$ are **relatively prime** iff gcd(a,b)=1.

Examples: 9 and 20, 35 and 49, etc.

# Least Common Multiple (LCM)



For a pair of positive numbers $a, b \in Z^+$ their **least common multiple** $l$ is the smallest number that is divisible by both a and b.

Denotation: **lcm(a,b)**

Example: lcm(4,6)=12, lcm(10,8)=40

Note: for any $a, b \in Z^+$ the following holds:
$ab = gcd(a, b) \cdot lcm(a, b)$

# GCD and LCM vs prime factorisation

For a pair of two positive integers $a, b \in Z^+$, consider prime factorisations regarding all prime divisors of a and b of the following form:

$a = p_1^{a_1} \cdot \ldots \cdot p_n^{a_n}$ and $b = p_1^{b_1} \cdot \ldots \cdot p_n^{b_n}$, where each $a_i, b_i$ is a natural number (can be 0).

Then:

- $gcd(a, b) = p_1^{min(a_1,b_1)} \cdot \ldots \cdot p_n^{min(a_n,b_n)}$
- $lcm(a, b) = p_1^{max(a_1,b_1)} \cdot \ldots \cdot p_n^{max(a_n,b_n)}$

Example: $10 = 2^1 5^1$, $8 = 2^3 5^0$ and lcm(10,8)=$2^3 5^1 = 40$

# Examples of Applications



- hashing functions ($h(k) = k \; mod \; m$)
- pseudo-random numbers: $x_{n+1} = (ax_n + c)$mod m (linear congruence method)
- cryptology ($y = (ax + c)$ mod m, in particular "Ceasar's code": $y = (x + 3) mod 26$)

# Summary



- partial order relation
- linear order
- minimal, maximal elements, chains, anti-chains
- dense, continuous, well ordering
- divisibility relation and basic number theory

# Example tasks/questions/problems



For each of the following: precise definition and ability to compute on the given example (if applicable):

- Order relation and its variants, and concepts (e.g. comparable, minimal, largest, chain, anti-chain, linear order, upper bound, dense order, well-ordered set, etc.)
- divisibility, prime number, fundamental theorem of arithmetic, factorisation into prime numbers, gcd, lcm, congruence, etc.

Thank you for your attention.