Ve203 Discrete Mathematics

Runze Cai

University of Michigan - Shanghai Jiao Tong University
Joint Institute

Spring 2022

JOINT INSTITUTE

交大密西根学院

Part I

Basic Set Theory and Applications

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Sets

Definition

A set is an unordered collection of distinct objects, called ***elements*** or ***members*** of the set. A set is said to contain its elements. We write

- $a \in A$ if a is an element of the set A.
- $a \notin A$ if a is not an element of the set A.

Examples

- The set P of primes less than 10: $P = \{2, 3, 5, 7\}$.
- The set V of all vowels in the English alphabet: $V = \{a, e, i, o, u\}$.
- The set S of all suits $S = \{\heartsuit, \diamondsuit, \clubsuit, \spadesuit\}$.
- Different kinds of objects: $S = \{\text{USA}, \text{USB}, \text{UCSB}, 0.0, \{\text{CAT}\}\}$.
- The empty set $S = \{\} = \varnothing = \emptyset$.

Multisets

Caution

- Elements in a set are ***distinct*** and ***unordered***.

Example

- $\{1, 0, 0, 0\} = \{0, 0, 1, 1\} = \{0, 1\} = \{1, 0\}$
- $\{\pm 1\} = \{(-1)^n \mid n \in \mathbb{N}\} = \{1, -1, 1, -1, \dots\}$

A multiset does allow repeated objects. (but order still does not matter)

Example

- Roots of a polynomial.
- Eigenvalues of a square matrix.
- Stock of drinks.

Set Notation

Number Systems

- $\mathbb{N}$, the natural numbers
- $\mathbb{Z}$, the integers
- $\mathbb{Q}$, the rational numbers
- $\mathbb{R}$, the real numbers
- $\mathbb{C}$, the complex numbers

Cardinality

The ***size*** of a set A is called its cardinality, denoted by $|A|$, $\#A$, or card A.

- $|A| = n \in \mathbb{N}$ if A is a finite set;
- $|A| = \infty$ otherwise. (Question: infinities?)

Set Operations

Let A, B be sets.

Inclusion

- A is a subset of B, denoted by $A \subset B$, if every element of A is an element of B.
- B is called a superset of A, denoted by $B \supset A$.

Remark

Unlike $<$ and $\leq$, $A \subset B$ is the same as $A \subseteq B$. Similarly for $\supset$ and $\supseteq$.

Proper Subset/Superset

A is a proper subset of B if $A \subset B$ and $A \neq B$, denoted by $A \subsetneq B$ or $A \subsetneqq B$. Similarly for proper superset.

Remark

$A = B$ if and only if $A \subset B$ and $B \subset A$. (cf., $x = y$ iff $x \leq y$ and $y \leq x$.)

Set Operations

Let A, B be sets.

Union

The union of A and B is the set of elements in either A or B, denotedy by

$$A \cup B := \{x \mid x \in A \text{ or } x \in B\}$$

Intersection

The intersection of A and B is the set of elements in both A and B, denotedy by

$$A \cap B := \{x \mid x \in A \text{ and } x \in B\}$$

Questions

- $\bigcap \varnothing = ?$
- $\bigcup \varnothing = ?$
- $\{A, B\} = A \cup B$?

Set Operations

Let A, B be sets.

Set Difference

The set difference of A and B, denoted by $A - B$, or $A \setminus B$, is the set of elements in A but not in B, that is,

$$\begin{aligned} A - B &:= \{x \mid x \in A \text{ and } x \notin B\} \\ &= \{x \in A \mid x \notin B\} \end{aligned}$$

Symmetric Difference

The symmetric difference of A and B is the set of elements that are in ***exclusively*** one of A and B, but not the other.

$$A \triangle B = (A - B) \cup (B - A)$$

Set Operations

Power Set

The power set of a set A is the set of all subsets of A, denoted by $\mathcal{P}(A)$ or 2^A.

Example

- $\mathcal{P}(\{j, i\}) = \{\varnothing, \{j\}, \{i\}, \{j, i\}\}$.
- $\mathcal{P}(\{0\}) = \{\varnothing, \{0\}\}$.
- $\mathcal{P}(\{\varnothing\}) = \{\varnothing, \{\varnothing\}\}$.
- $\mathcal{P}(\varnothing) = \{\varnothing\}$.

Cardinality of Power sets

Given a finite set A,

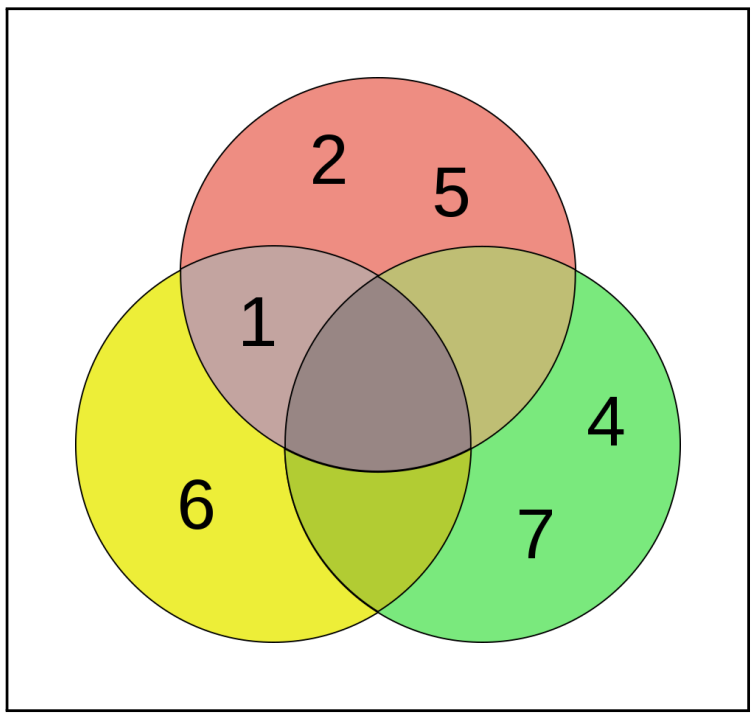
$$|2^A| = |\mathcal{P}(A)| = 2^{|A|}$$

Venn Diagram vs Euler Diagram

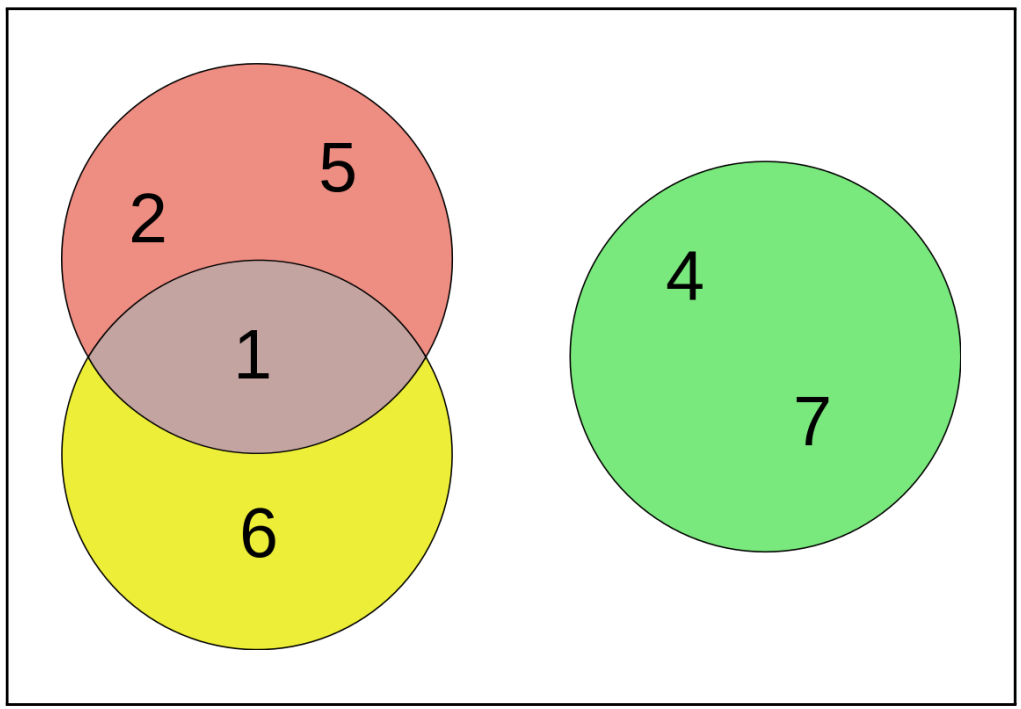
Given

- $A = \{1, 2, 5\}$
- $B = \{1, 6\}$
- $C = \{4, 7\}$

Venn Diagram



Euler Diagram



Set Algebras

Let A, B, C be sets.

- Commutative Laws
  - $A \cup B = B \cup A$
  - $A \cap B = B \cap A$
- Associative Laws
  - $(A \cup B) \cup C = A \cup (B \cup C)$
  - $(A \cap B) \cap C = A \cap (B \cap C)$
- (Left) Distributive Laws
  - $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- De Morgan's Laws
  - $C - (A \cup B) = (C - A) \cap (C - B)$
  - $C - (A \cap B) = (C - A) \cup (C - B)$

Cartesian Product

Definition

The Cartesian product of sets A and B is the set of ordered pairs, such that

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

Definition (Kuratowski)

An ordered pair (a, b) is given by

$$(a, b) := \{\{a\}, \{a, b\}\}$$

Theorem

If $a \in C$ and $b \in C$, then $(a, b) \in \mathcal{P}(\mathcal{P}(C))$.

Proof.

- $a \in C \Rightarrow \{a\} \in \mathcal{P}(C)$; $a, b \in C \Rightarrow \{a, b\} \in \mathcal{P}(C)$.
- Hence $(a, b) = \{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(C))$. □

Cartesian Product

Theorem

$(x, y) = (a, b)$ *iff* $x = a$ *and* $y = b$.

Proof.

- ($\Leftarrow$). Trivial.
- ($\Rightarrow$). Be definition, we need to show that

$$\underbrace{\{\{x\}, \{x, y\}\}}_{U} = \underbrace{\{\{a\}, \{a, b\}\}}_{V} \Rightarrow x = a \text{ and } y = b$$

  - If $x \neq y$, then $|U| = |V| = 2$ (b/c $\{x\} \neq \{x, y\}$), hence $U = V$. By matching sizes we have $\{x\} = \{a\}$ and $\{x, y\} = \{a, b\}$, therefore $x = a$ and $y = b$.
  - If $x = y$, then $|U| = |V| = 1$. Similarly we have $x = y = a = b$.

□

Cartesian Product of Sets

In this manner, we can define Cartesian product of three sets as the set of ***ordered triples***, e.g.,

$$A \times B \times C := \{(a, b, c) \mid a \in A, b \in B, c \in C\}.$$

More generally, the n-fold Cartesian product $A_1 \times \cdots \times A_n$ of sets A_k, $k = 1, \ldots, n$, as the set of ordered ***n-tuple*** $(a_1, \ldots, a_n)$.

If we take the cartesian product of a set with itself, we may abbreviate it using exponents, e.g.,

$$A^2 := A \times A, \qquad A^3 := A \times A \times A, \ldots$$

$$\mathbb{N}^2 := \mathbb{N} \times \mathbb{N}, \qquad \mathbb{N}^3 := \mathbb{N} \times \mathbb{N} \times \mathbb{N}, \ldots$$

Associative Set Operations

Let $A_1, A_2, \ldots, A_n$ be sets, then

- $A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$
- $A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$
- $A_1 \times A_2 \times \cdots \times A_n = \bigtimes_{i=1}^{n} A_i$
- $A_1 \triangle A_2 \triangle \cdots \triangle A_n = \bigtriangleup_{i=1}^{n} A_i$

Remark

Brackets are permitted everywhere but not requried anywhere.

Question

How many ways to put the brackets?

Simple Graphs

k-element subsets

Let X be a finite set. For a positive integer k, let $\binom{X}{k}$ denote the set of all k-element subsets. Note that $\left|\binom{X}{k}\right| = \binom{|X|}{k}$.

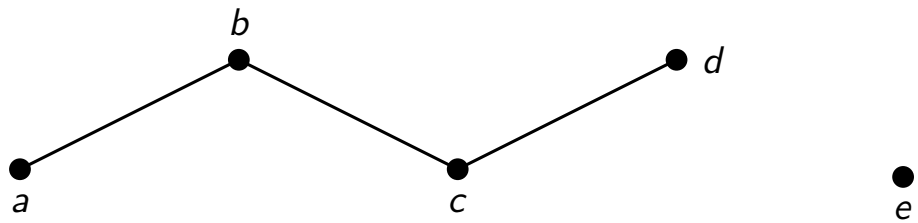
Definition

A finite simple ***graph*** G is a pair (V, E) where V is a non-empty finite set and E is a set of 2-element subsets of V, i.e., $E \subset \binom{V}{2}$. Elements of V are called ***vertices*** and elements of E are called ***edges***. We also call V the ***vertex set*** of G, denoted $V(G)$, and E the ***edge set*** of G, denoted $E(G)$.

Example

Consider the following simple graph $G = (V, E)$, where

- $V(G) = \{a, b, c, d, e\}$,
- $E(G) = \{\{a, b\}, \{b, c\}, \{c, d\}\}$.



For simplicity, we also write

$$E(G) = \{ab, bc, cd\}$$

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Propositional Logic

Definition

A ***proposition*** or ***statement*** is a declarative sentence that is either true or false, but not both.

Examples

- Washington, D.C., is the capital of the United States of America.
- Toronto is the capital of Canada.
- $1 + 1 = 2$.
- $2 + 2 = 3$.

Non-examples

- What time is it?
- Read this carefully.
- $x + 1 = 2$.
- $x + y = z$.

Notation

Propositional/Logical Variables

Denoted by p, q, r, ...

True or False

- True: T, 1, $\top$
- False: F, 0, $\bot$

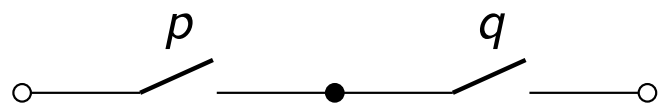
Connectives

- $\neg$, negation/not
- $\wedge$, and
- $\vee$, or (inclusive or)
- $\rightarrow$, implies
- $\leftrightarrow$, if and only if (iff)

Conjunction and disjunction

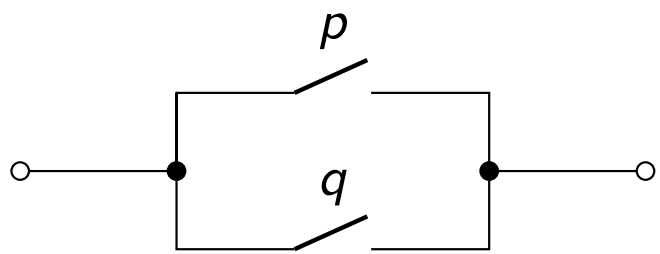
AND

p	q	$p \wedge q$
0	0	0
0	1	0
1	0	0
1	1	1



OR (inclusive or)

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1



Remark

- In the conjunction $p \wedge q$, the proposition p and q are called ***conjuncts***;
- In the disjunction $p \vee q$, the proposition p and q are called ***disjuncts***.

Negation and Exclusive OR

NOT

p	$\neg p$
0	1
1	0

XOR (exclusive or)

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

CNF and DNF

Conjunctive Normal Form (CNF)

A proposition is in **Conjunctive Normal Form (CNF)** if it is a conjunction of one or more clauses, where a clause is a disjunction of literals; i.e., it is a **product of sums** or an **AND of ORs**.

Disjunctive Normal Form (DNF)

A proposition is in **Disjunctive Normal Form (CNF)** if it is a Disjunction of one or more clauses, where a clause is a conjunction of literals; i.e., it is a **sum of products** or an **OR of ANDS**.

Remark

A ***literal*** is a Boolean variable, (i.e., an atomic proposition) or its negation.

Example

- CNF: $(\neg p \vee q \vee r) \wedge (\neg q \vee \neg r) \wedge (r)$
- DNF: $(\neg p \wedge q \wedge r) \vee (\neg q \wedge \neg r) \vee (r)$

Conditional Statements

Conditional statement (implication)

- p:hypothesis/antecedent/premise
- q:thesis/conclusion/consequence

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Equivalent forms

- if p, then q
- if p, q
- p is sufficient for q
- q if p
- q when p
- a necessary condition for p is q
- p implies q
- p only if q
- a sufficient condition for q is p
- q whenever p
- q is necessary for p
- q follows from p

Conditional Statements

"No underage drinking"

If somebody is drinking alcohol, then they are over 18 y/o.

- A is drinking beer
- B is drinking coda
- C is 55 y/o
- D is 15 y/o

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

Remark

We seek to find out whether a certain promise or guarantee is kept. That is,

- either p is false,
- or q is true.

p	q	$\neg p$	$\neg p \vee q$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	0	1

Converse/Inverse/Contrapositive/Negation

Given $p \to q$,

- Converse: $q \to p$
- Inverse: $\neg p \to \neg q$
- Contrapositive: $\neg q \to \neg p$
- Negation: $\neg(p \to q)$

Remark

A proposition is equivalent to its contrapositive.

p	q	$p \to q$	$\neg q \to \neg p$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Biconditional Statements

if and only if (iff)

p	q	$p \to q$	$q \to p$	$p \leftrightarrow q$
0	0	1	1	1
0	1	1	0	0
1	0	0	1	0
1	1	1	1	1

Compound proposition

Order of operations (use brackets "(. . .)" when in doubt)

- $\neg$
- $\wedge$
- $\vee$
- $\rightarrow$
- $\leftrightarrow$

Tautology and Contradiction

In the truth table,

- Tautology: All cases evaluates to 1. (e.g., $p \vee \neg p$)
- Contradiction: All cases evaluates to 0. (e.g., $p \wedge \neg p$)

Equivalence

p and q are called ***equivalent*** iff $p \leftrightarrow q$ is a tautology, denoted by $p \Leftrightarrow q$.

Examples

- $p \vee \neg p \Leftrightarrow 1$
- $p \wedge \neg p \Leftrightarrow 0$
- $p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p \Leftrightarrow \neg p \vee q$

Tautological Equivalence

- Commutativity

$$p \wedge q \Leftrightarrow q \wedge p$$

$$p \vee q \Leftrightarrow q \vee p$$

- Associativity

$$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$$

$$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$$

$$(p \leftrightarrow q) \leftrightarrow r \Leftrightarrow p \leftrightarrow (q \leftrightarrow r)$$

$$(p \oplus q) \oplus r \Leftrightarrow p \oplus (q \oplus r)$$

- Distributivity

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$$

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \vee r)$$

Tautological Equivalence

- Negation

$$\neg\neg p \Leftrightarrow p$$

$$p \to q \Leftrightarrow \neg q \to \neg p$$

$$\neg(p \vee q) \Leftrightarrow (\neg p) \wedge (\neg q)$$

$$\neg(p \wedge q) \Leftrightarrow (\neg p) \vee (\neg q)$$

- Identity

$$p \vee 0 \Leftrightarrow p \qquad (\max\{p, 0\} = p)$$

$$p \wedge 1 \Leftrightarrow p \qquad (\min\{p, 1\} = p)$$

- Null

$$p \wedge 0 \Leftrightarrow 0 \qquad (\min\{p, 0\} = 0)$$

$$p \vee 1 \Leftrightarrow 1 \qquad (\max\{p, 1\} = 1)$$

Tautological Equivalence

- Idempotent

$$p \wedge p \Leftrightarrow p$$

$$p \vee p \Leftrightarrow p$$

- Absorption

$$p \wedge (p \vee q) \Leftrightarrow p$$

$$p \vee (p \wedge q) \Leftrightarrow p$$

- Cases

$$(p \to q) \wedge (p \to r) \Leftrightarrow p \to (q \wedge r)$$

$$(p \to q) \vee (p \to r) \Leftrightarrow p \to (q \vee r)$$

$$(p \to r) \wedge (q \to r) \Leftrightarrow (p \vee q) \to r$$

$$(p \to r) \vee (q \to r) \Leftrightarrow (p \wedge q) \to r$$

- Added premise

$$(p \wedge q) \to r \Leftrightarrow p \to (q \to r)$$

$$\Leftrightarrow q \to (p \to r)$$

Added Premise

p	q	r	$p \wedge q$	r	$(p \wedge q) \rightarrow r$	p	$q \rightarrow r$	$p \rightarrow (q \rightarrow r)$
0	0	0	0	0	1	0	1	1
0	0	1	0	1	1	0	1	1
0	1	0	0	0	1	0	0	1
0	1	1	0	1	1	0	1	1
1	0	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1	1
1	1	0	1	0	0	1	0	0

Tautological Equivalence

Example

Prove the absorption rule $p \wedge (p \vee q) \Leftrightarrow p$.

Proof.

$$\begin{aligned} p \wedge (p \vee q) &\Leftrightarrow (p \vee 0) \wedge (p \vee q) \\ &\Leftrightarrow p \vee (0 \wedge q) \\ &\Leftrightarrow p \vee 0 \\ &\Leftrightarrow p \end{aligned}$$

□

Remark

Consider the saturation function with parameter $a, b \in \mathbb{R}$, $a \leq b$,

$$\mathrm{SAT}_{a,b}(x) := \begin{cases} a, & x < a \\ x, & a \leq x \leq b \\ b, & x > b \end{cases}$$

Note that $\mathrm{SAT}_{a,b}(x) = \min\{b, \max\{a, x\}\} = \max\{a, \min\{b, x\}\}$.

Tautological Equivalence

Remark (Cont.)

Then we can write

$$p \wedge (p \vee q) = \min\{p, \max\{p, q\}\} = \mathrm{SAT}_{p,p}(q) = p$$

or

$$p \wedge (p \vee q) = \min\{p, \max\{q, p\}\} = \mathrm{SAT}_{q,p}(p) = p$$

Remark

Note that

$$\mathrm{SAT}_{a,b}(x) = \mathrm{MEDIAN}(a, b, x)$$

Tautological Equivalence

Example

Show that $(p \to r) \wedge (q \to r) \Leftrightarrow (p \vee q) \to r$.

Proof.

$$\begin{aligned}(p \to r) \wedge (q \to r) &\Leftrightarrow (\neg p \vee r) \wedge (\neg q \vee r) \\ &\Leftrightarrow (\neg p \wedge \neg q) \vee r \\ &\Leftrightarrow (\neg(p \vee q)) \vee r \\ &\Leftrightarrow (p \vee q) \to r\end{aligned}$$

□

Example

Show that $(p \to r) \vee (q \to r) \Leftrightarrow (p \wedge q) \to r$.

Proof.

$$\begin{aligned}(p \to r) \vee (q \to r) &\Leftrightarrow (\neg p) \vee r \vee (\neg q) \vee r \\ &\Leftrightarrow (\neg p) \vee (\neg q) \vee r \\ &\Leftrightarrow (\neg(p \wedge q)) \vee r \\ &\Leftrightarrow (p \wedge q) \to r\end{aligned}$$

□

CNF and DNF

Theorem

For any proposition φ, there is a proposition φ_{dnf} over the same Boolean variables and in DNF such that $\varphi \Leftrightarrow \varphi_{dnf}$.

Example

- $\varphi = p \vee q$ $\quad\quad$ $\varphi_{dnf} = (p) \vee (q)$
- $\varphi = p \wedge q$ $\quad\quad$ $\varphi_{dnf} = (p \wedge q)$
- $\varphi = p \rightarrow q$ $\quad\quad$ $\varphi_{dnf} = (\neg p) \vee (q)$
- $\varphi = p \leftrightarrow q$ $\quad\quad$ $\varphi_{dnf} = (p \wedge q) \vee (\neg q \wedge \neg p)$
- $\varphi = p \oplus q$ $\quad\quad$ $\varphi_{dnf} = (\neg p \wedge q) \vee (p \wedge \neg q)$

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

$\varphi_{dnf} = (\neg p \wedge q) \vee (p \wedge \neg q)$

CNF and DNF

Theorem

For any proposition φ, there is a proposition φ_{cnf} over the same Boolean variables and in CNF such that $\varphi \Leftrightarrow \varphi_{cnf}$.

Example

- $\varphi = p \vee q$ $\quad \varphi_{cnf} = (p \vee q)$
- $\varphi = p \wedge q$ $\quad \varphi_{cnf} = (p) \wedge (q)$
- $\varphi = p \rightarrow q$ $\quad \varphi_{cnf} = (\neg p \vee q)$
- $\varphi = p \leftrightarrow q$ $\quad \varphi_{cnf} = (\neg p \vee q) \wedge (\neg q \vee p)$
- $\varphi = p \oplus q$ $\quad \varphi_{cnf} = (p \vee q) \wedge (\neg q \vee \neg p)$

p	q	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Since

$$\neg(\varphi_{cnf}) = (\neg p \wedge \neg q) \vee (p \wedge q)$$

Then by DeMorgan's law

$$\varphi_{cnf} = (p \vee q) \wedge (\neg q \vee \neg p)$$

Rules of Inference (Implication)

- Detachment (Modus ponens): $(p \to q) \wedge p \Rightarrow q$
- Indirect reasoning (Modus tollens): $(p \to q) \wedge \neg q \Rightarrow \neg p$
- Disjunctive addition: $p \Rightarrow (p \vee q)$
- Conjunctive simplification: $(p \wedge q) \Rightarrow p$
- Disjunctive syllogism: $(p \vee q) \wedge \neg p \Rightarrow q$
- Hypothetical syllogism: $(p \to q) \wedge (q \to r) \Rightarrow p \to r$
- Resolution: $(p \vee q) \wedge (\neg p \vee r) \Rightarrow q \vee r$

Proof by Contrapositive

$$p \to q \Leftrightarrow (\neg q \to \neg p)$$

Proof by Contradiction

$$p \to q \Leftrightarrow (p \wedge \neg q) \to 0$$

Rules of Inference (Implication)

Definition

We say that p implies q if $p \rightarrow q$ is a tautology, denoted by $p \Rightarrow q$.

Example

Disjunctive addition:

$$p \Rightarrow (p \vee q)$$

p	q	$p \vee q$	$p \rightarrow p \vee q$
0	0	0	1
0	1	1	1
1	0	1	1
1	1	1	1

Summary (in terms of truth tables)

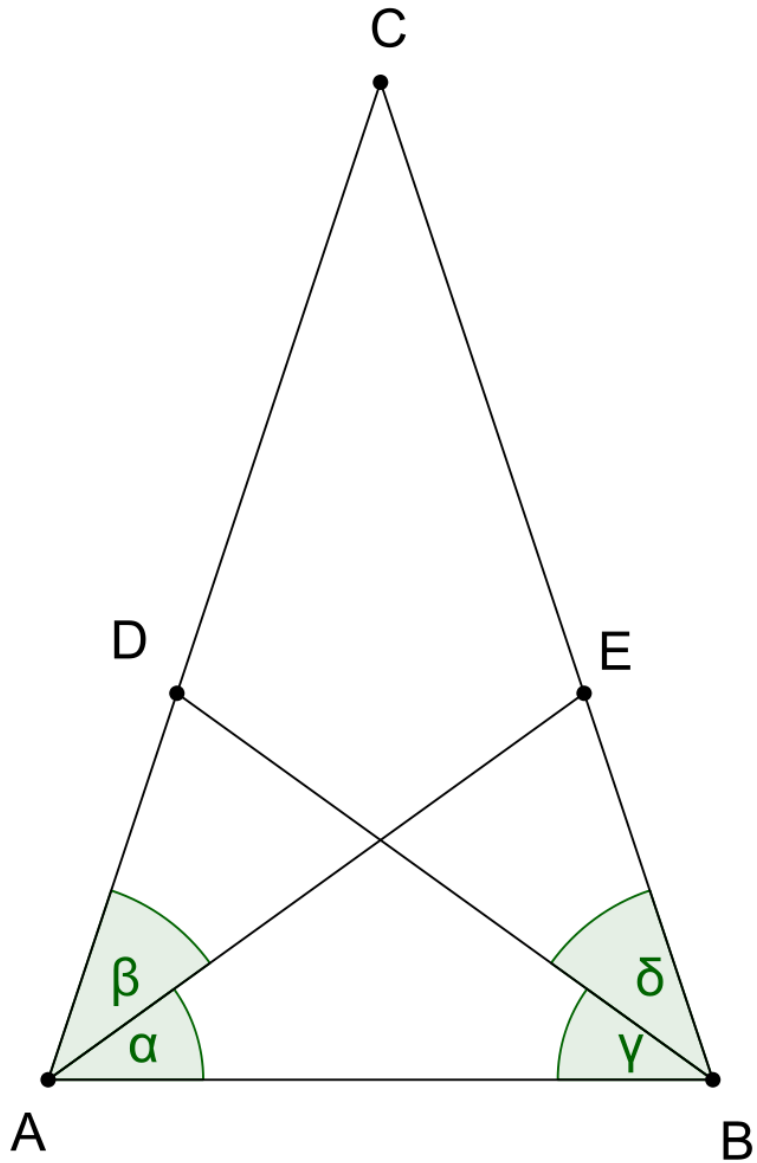
- Tautology: all 1's in the truth table;
- Contradiction: all 0's in the truth table;
- Equivalence $p \Leftrightarrow q$: same value in the truth table;
- Implication $p \Rightarrow q$: if $p = 1$, then $q = 1$.

Direct Proofs Might Be Hard

Theorem (Steiner-Lehmus)

Every triangle with two angle bisectors of equal lengths is isosceles.

$$|AE| = |BD|, \alpha = \beta, \gamma = \delta$$
$$\Rightarrow \triangle ABC \text{ is isosceles.}$$



The Natural Numbers

Definition

Let $m, n \in \mathbb{N}$ be natural numbers.

(i) We say that n is ***greater than or equal to*** m, writing $n \geq m$, if there exists some $k \in \mathbb{N}$ such that $n = m + k$. If we can choose $k \neq 0$, we say n is ***greater than*** m and write $n > m$.

(ii) We say that m ***divides*** n, writing $m \mid n$, if there exists some $k \in \mathbb{N}$ such that $n = m \cdot k$.

(iii) If $2 \mid n$, we say that n is even.

(iv) If there exists some $k \in \mathbb{N}$ such that $n = 2k + 1$, we say that n is odd.

(v) Suppose that $n > 1$. If there does not exist any $k \in \mathbb{N}$ with $1 < k < n$ such that $k \mid n$, we say that n is ***prime***.

Remark

It can be proven that every number is either even or odd and not both (a special property of **equivalence classes**). We also assume this for the purposes of our examples.

Infinitude of Primes

Theorem

There are infinitely many prime numbers.

Proof (NOT due to Euclid).

Assume that there are only finitely many primes, say $\mathbb{P} = \{p_1, \ldots, p_k\}$. consider the integer $N = p_1 p_2 \cdots p_k + 1$, observe that $p_i \nmid N$ for any $i = 1, \ldots, k$, so N must be a prime, but $N \notin \mathbb{P}$, contradiction! □

Proof (by Euclid).

Consider a finite set of primes $\{p_1, \ldots, p_k\}$. Let $N = p_1 p_2 \cdots p_k + 1$, so

- either N is a prime;
- or N is not a prime, so N must admit a prime factor, which is not in $\{p_1, \ldots, p_k\}$. Call this new prime p_{k+1}.

So we can always generate a new prime from a finite set of primes. □

Remark

Euclid's proof of the infinitude of primes is **NOT** a proof by contradiction.

Proof by Contradiction

Recall a proof by contradiction admits the form

$$p \to q \Leftrightarrow (p \wedge \neg q) \to 0$$

Specifically, for some proposition r,

$$\begin{aligned} p \to q &\Leftrightarrow (p \wedge \neg q) \to 0 \\ &\Leftrightarrow (p \wedge \neg q) \to (r \wedge \neg r) \\ &\Leftrightarrow (p \wedge \neg q \to r) \wedge (p \wedge \neg q \to \neg r) \end{aligned}$$

What if $r = q$?

$$\begin{aligned} p \to q &\Leftrightarrow (p \wedge \neg q) \to (q \wedge \neg q) \\ &\Leftrightarrow (p \wedge \neg q \to q) \wedge \underbrace{(p \wedge \neg q \to \neg q)}_{=1} \\ &\Leftrightarrow p \wedge \neg q \to q \\ &\Leftrightarrow \neg q \to (p \to q) \end{aligned}$$

Statements

Examples

- "$3 > 2$" is a ***true statement***.
- "$x^3 > 10$" is not a statement, because we can not decide whether it is true or not.
- "the cube of any natural number is greater than 10" is a ***false statement***.

The last example can be written using a ***statement variable*** n:

- "For any natural number n, $n^3 > 10$"

The first part of the statement is a ***quantifier*** ("for any natural number n"), while the second part is called a ***statement form*** or ***predicate*** ("$n^3 > 10$").

Statements

Definition

A function $P : X \to \{\top, \bot\}$ is called a predicate on its domain X.

Remark

A statement form or predicate becomes a statement (which can then be either true or false) when the variable takes on a specific value.

Example

If $P(x)$ stands for "$x^3 > 10$", then

- $P(10) = \top$, i.e., $10^3 > 10$ is a TRUE statement;
- $P(1) = \bot$, i.e., $1^3 > 10$ is a FALSE statement.

Recall We indicate that an ***element*** x is a member of a ***set*** X by writing $x \in X$. We may characterize the elements of a set X by some predicate P:

$$x \in X \Leftrightarrow P(x).$$

We write $X = \{x \colon P(x)\} = \{x \mid P(x)\}$, which is called the ***set-builder notation***.

Logical Quantifiers

There are two types of quantifiers:

- the ***universal quantifier***, denoted by the symbol $\forall$, read as "for all" and
- the ***existential quantifier***, denoted by $\exists$, read as "there exists."

Definition

Let M be a set and $A(x)$ be a predicate. Then we define the quantifier $\forall$ by

$$(\forall x \in M)A(x) \quad \Leftrightarrow \quad A(x) \text{ is true for all } x \in M$$

We define the quantifier $\exists$ by

$$(\exists x \in M)A(x) \quad \Leftrightarrow \quad A(x) \text{ is true for at least one } x \in M$$

We may also write $\forall x \in M\colon A(x)$ or $\underset{x \in M}{\forall} A(x)$ instead of $(\forall x \in M)A(x)$.

Similarly for $\exists$.

Logical Quantifiers

We may also state the domain before making the statements, as in the following example.

Examples

Let x be a real number. Then

- $\forall x : x > 0 \Rightarrow x^3 > 0$ is a true statement;
- $\forall x : x > 0 \Leftrightarrow x^2 > 0$ is a false statement;
- $\exists x : x > 0 \Leftrightarrow x^2 > 0$ is a true statement.

Sometimes mathematicians put a quantifier at the end of a statement form; this is known as a ***hanging quantifier***. Such a hanging quantifier will be interpreted as being located just before the statement form:

$$\exists y : y + x^2 > 0 \qquad\qquad \forall x$$

is equivalent to $\exists y \forall x : y + x^2 > 0$.

Contraposition and Negation of Quantifiers

We do not actually need the quantifier $\exists$ since

$$\begin{aligned} \exists x \in M : A(x) \quad &\Leftrightarrow \quad A(x) \text{ is true for at least one } x \in M \\ &\Leftrightarrow \quad A(x) \text{ is not false for all } x \in M \\ &\Leftrightarrow \quad \neg \forall x \in M (\neg A(x)) \end{aligned} \tag{1}$$

The equivalence (1) is called ***contraposition of quantifiers***. It implies that the negation of $\exists x \in M \colon A(x)$ is equivalent to $\forall x \in M \colon \neg A(x)$. For example,

$$\neg \left(\exists x \in \mathbb{R} \colon x^2 < 0 \right) \qquad \Leftrightarrow \qquad \forall x \in \mathbb{R} \colon x^2 \not< 0.$$

Conversely,

$$\neg \left(\forall x \in M \colon A(x) \right) \qquad \Leftrightarrow \qquad \exists x \in M \colon \neg A(x).$$

To summarize,

- $\neg \exists \Leftrightarrow \forall \neg$
- $\neg \forall \Leftrightarrow \exists \neg$
- $\neg \forall \neg \Leftrightarrow \exists$
- $\neg \exists \neg \Leftrightarrow \forall$

Equivalence/Implication for Predicate Logic

- $(\forall x \in M)[P(x) \vee \neg P(x)]$
- $\neg[(\forall x \in M)P(x)] \Leftrightarrow [(\exists x \in M)\neg P(x)]$
- $\neg[(\exists x \in M)P(x)] \Leftrightarrow [(\forall x \in M)\neg P(x)]$
- $[(\forall x \in M)P(x)] \Rightarrow [(\exists x \in M)P(x)]$, if $M \neq \varnothing$
- $(\exists x \in M)[P(x) \vee Q(x)] \Leftrightarrow [(\exists x \in M)P(x)] \vee [(\exists x \in M)Q(x)]$
- $(\forall x \in M)[P(x) \wedge Q(x)] \Leftrightarrow [(\forall x \in M)P(x)] \wedge [(\forall x \in M)Q(x)]$
- $(\exists x \in M)[P(x) \wedge Q(x)] \Rightarrow [(\exists x \in M)P(x)] \wedge [(\exists x \in M)Q(x)]$
- $(\forall x \in M)[P(x) \vee Q(x)] \Leftarrow [(\forall x \in M)P(x)] \vee [(\forall x \in M)Q(x)]$
- $[(\forall x \in M)P(x) \rightarrow Q(x)] \wedge [(\forall x \in M)P(x)] \Rightarrow [(\forall x \in M)Q(x)]$
- $[(\forall x \in \{y \in M \mid P(y)\})Q(x)] \Leftrightarrow [(\forall x \in M)P(x) \rightarrow Q(x)]$
- $[(\exists x \in \{y \in M \mid P(y)\})Q(x)] \Leftrightarrow [(\exists x \in M)P(x) \wedge Q(x)]$
- $\varphi \wedge [(\exists x \in M)P(x)] \Leftrightarrow [(\exists x \in M)\varphi \wedge P(x)]$, if no x in φ
- $\varphi \vee [(\forall x \in M)P(x)] \Leftrightarrow [(\forall x \in M)\varphi \vee P(x)]$, if no x in φ

- $(\forall x \in \varnothing)P(x)$
- $\neg(\exists x \in \varnothing)P(x)$

Vacuous Truth

If the domain of the universal quantifier $\forall$ is the empty set $M = \varnothing$, then the statement $\forall x \in M\colon A(x)$ is defined to be true regardless of the predicate $A(x)$. It is then said that $A(x)$ is ***vacuously true***.

Example

Let M be the set of real numbers x such that $x = x + 1$. Then the statement

$$\forall_{x \in M} \; x > x$$

is true.

This convention reflects the philosophy that a universal statement is true unless there is a counterexample to prove it false. While this may seem a strange point of view, it proves useful in practice.

This is similar to saying that "All pink elephants can fly." is a true statement, because it is impossible to find a pink elephant that can't fly.

Nesting Quantifiers

We can also treat predicates with more than one variable as shown in the following example.

Examples

In the following examples, x, y are taken from the real numbers.

- $\forall x \forall y : x^2 + y^2 - 2xy \geq 0$ is equivalent to $\forall y \forall x : x^2 + y^2 - 2xy \geq 0$. Therefore, one often writes $\forall x, y : x^2 + y^2 - 2xy \geq 0$.
- $\exists x \exists y : x + y > 0$ is equivalent to $\exists y \exists x : x + y > 0$, often abbreviated to $\exists x, y : x + y > 0$.
- $\forall x \exists y : x + y > 0$ is a true statement.
- $\exists x \forall y : x + y > 0$ is a false statement.

As is clear from these examples, the order of the quantifiers is important if they are different.

Set Theory Examples

- Extensionality Axiom

$$\forall A, B(\forall x(x \in A \Leftrightarrow x \in B) \Rightarrow A = B)$$

- Empty Set Axiom

$$\exists B \forall x(x \notin B)$$

- Pairing Axiom

$$\forall u, v \exists B \forall x(x \in B \Leftrightarrow x = u \vee x = v)$$

- Union Axiom

$$\forall a, b \exists B \forall x(x \in B \Leftrightarrow x \in a \vee x \in b)$$

- Powerset Axiom

$$\forall a \exists b \forall x(x \in B \Leftrightarrow x \subseteq a)$$

where $x \subseteq a$ is shorthand for $\forall t(t \in x \Rightarrow t \in a)$.

Set-Theoretic Proofs

Basic Facts

$$
\begin{aligned}
x \in A \cup B &\Leftrightarrow (x \in A) \vee (x \in B) \\
x \notin A \cup B &\Leftrightarrow (x \notin A) \wedge (x \notin B) \\
x \in A \cap B &\Leftrightarrow (x \in A) \wedge (x \in B) \\
x \notin A \cap B &\Leftrightarrow (x \notin A) \vee (x \notin B) \\
x \in A - B &\Leftrightarrow (x \in A) \wedge (x \notin B) \\
x \notin A - B &\Leftrightarrow (x \notin A) \vee (x \in B) \\
A \subset B &\Leftrightarrow (x \in A) \rightarrow (x \in B) \\
A = B &\Leftrightarrow (A \subset B) \wedge (B \subset A)
\end{aligned}
$$

Remark

- Prove something exists: sufficient to find an example.
- Prove $P(x)$ for all $x \in A$: Take any $x \in A$ and continue. (or use induction if $A = \mathbb{N}$, more on this later.)

Duality in Propositional Logic

- $\vee$ vs $\wedge$
- 0 vs 1

Basic Law	Property	Dual Law
$p \vee q \Leftrightarrow q \vee p$	Commutativity	$p \wedge q \Leftrightarrow q \wedge p$
$(p \vee q) \vee r \Leftrightarrow p \vee (q \vee r)$	Associativity	$(p \wedge q) \wedge r \Leftrightarrow p \wedge (q \wedge r)$
$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \vee r)$	Distributivity	$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r)$
$p \vee 0 \Leftrightarrow p$	Identity	$p \wedge 1 \Leftrightarrow p$
$p \wedge \neg p \Leftrightarrow 0$	Negation	$p \vee \neg p \Leftrightarrow 1$
$p \vee p \Leftrightarrow p$	Idempotent	$p \wedge p \Leftrightarrow p$
$p \wedge 0 \Leftrightarrow 0$	Null	$p \vee 1 \Leftrightarrow 1$
$p \wedge (p \vee q) \Leftrightarrow p$	Absorption	$p \vee (p \wedge q) \Leftrightarrow p$
$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q$	DeMorgan's	$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Duality in Set Theory

- $\cup$ vs $\cap$
- $\varnothing$ vs U (U is the universe)

Basic Law	Property	Dual Law
$A \cup B = B \cup A$	Commutativity	$A \cap B = B \cap A$
$(A \cup B) \cup C = A \cup (B \cup C)$	Associativity	$(A \cap B) \cap C = A \cap (B \cap C)$
$A \cap (B \cup C) = (A \cap B) \cup (A \cup C)$	Distributivity	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
$A \cup \varnothing = A$	Identity	$A \cap U = A$
$A \cap A^c = \varnothing$	Negation	$A \cup A^c = U$
$A \cup A = A$	Idempotent	$A \cap A = A$
$A \cap \varnothing = \varnothing$	Null	$A \cup U = U$
$A \cap (A \cup B) = A$	Absorption	$A \cup (A \cap B) = A$
$(A \cup B)^c = A^c \cap B^c$	DeMorgan's	$(A \cap B)^c = A^c \cup B^c$

Russell's Paradox

Barber Paradox

The barber is the "one who shaves all those, and those only, who do not shave themselves".

Question: does the barber shave himself?

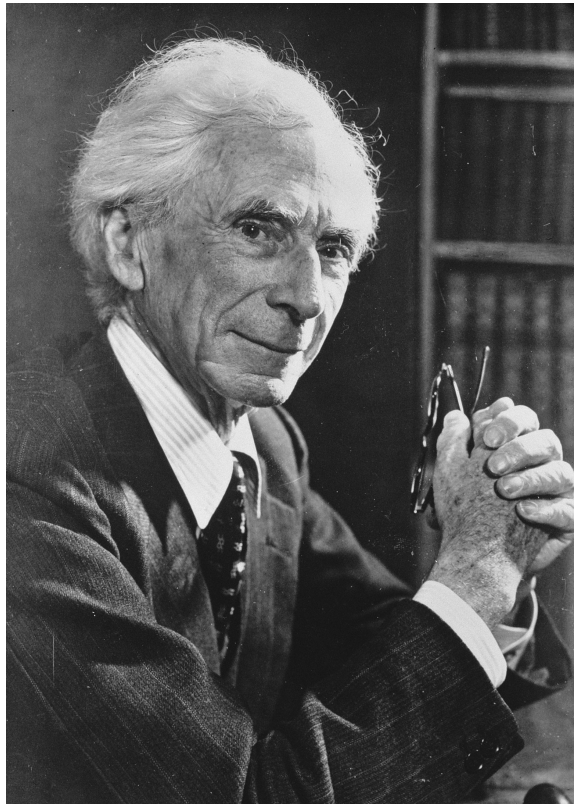
Consider the set of all sets that do not contain themselves:

$$S = \{A \mid A \text{ is a set, and } A \notin A\}$$

If such a set exists, then

- $S \in S \rightarrow S \notin S$
- $S \notin S \rightarrow S \in S$

Contradiction!



Bertrand Russell, Nov. 1957

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Mathematical Induction

Typically one wants to show that some statement frame $P(n)$ is true for all $n \in \mathbb{N}$ with $n \geq n_0$ for some $n_0 \in \mathbb{N}$. Mathematical induction works by establishing two statements:

(I) the **base case**: $P(n_0)$ is true.

(II) the **inductive case**: $P(n+1)$ is true whenever $P(n)$ is true for $n \geq n_0$, i.e.,

$$(\forall n \in \mathbb{N}, n \geq n_0)\big(P(n) \Rightarrow P(n+1)\big)$$

In the inductive case, $P(n)$ is called ***inductive hypothesis***, often abbreviated as ***IH***.

Note that (II) does not make a statement on the situation when $P(n)$ is false; it is permitted for $P(n+1)$ to be true even if $P(n)$ is false.

The principle of mathematical induction now claims that $P(n)$ is true for all $n \geq n_0$ if (I) and (II) are true.

Introductory Example

Example

Consider the statement

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad \text{for all } n \in \mathbb{N}.$$

This is a typical example, in that $P(n)\colon \sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ is a predicate which is to be shown to hold for all natural numbers $n \in \mathbb{N}$.

We first establish that $P(0)$ is true:

$$\sum_{k=0}^{0} k = 0 \qquad \text{and} \qquad \frac{0(0+1)}{2} = 0,$$

so $P(0)\colon 0 = 0$ is true.

Introductory Example

We next show that $P(n) \Rightarrow P(n+1)$ for all $n \in \mathbb{N} \setminus \{0\}$. This means we show that $\sum_{k=0}^{n+1} k = \frac{(n+1)(n+2)}{2}$ if $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. Let n now be any n for which $P(n)$ is true. We then write

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + n + 1$$

If $P(n)$ is true for this specific n, we can replace the sum on the right by $\frac{n(n+1)}{2}$, yielding

$$\sum_{k=0}^{n+1} k = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

But this is just the statement $P(n+1)$. Therefore, if $P(n)$ is true, then $P(n+1)$ will also be true. We have shown that $P(n) \Rightarrow P(n+1)$. □

Application of Induction

We can use induction to prove the ***efficiency*** and ***correctness*** of a recursive algorithm.

Properties of Algorithms

- ***Input.*** An algorithm has input values from a specified set;
- ***Output.*** For given input, the algorithm produces output values from a specified set;
- ***Definiteness.*** The steps of the algorithm are defined precisely;
- ***Correctness.*** For each input, the algorithm produces the correct output values;
- ***Finiteness.*** For given input, the algorithm produces output after a finite number of steps;
- ***Effectiveness.*** Each step of the algorithm can be performed exactly;
- ***Generality.*** The algorithm is generally applicable, not just for certain input values.

Factorial

Input: n, a positive integer
Output: $n!$

```
1 Function fact(n):
2     if n = 1 then
3         return 1
4     else
5         return n · fact(n − 1)
6     end
7 end
```

Remark

Recursion is inefficient. Use iteration/tail recursion/memoization instead (smart compiler can do this automatically).

Correctness of `fact`

Proof.

- **base case ($n = 1$):** Observe that `fact`(1) returns 1 immediately, and $1! = 1$.
- **inductive case ($n \geq 1$):** Assume that `fact`(n) returns $n!$. We want to show that `fact`$(n+1)$ returns $(n+1)!$. Indeed, by induction hypothesis,

$$\texttt{fact}(n+1) = n \cdot \texttt{fact}(n) = (n+1) \cdot n! = (n+1)!$$

Therefore the recursive algorithm `fact` is correct by induction. □

Insertion Sort

Input: $A[1 \dots n] = \langle a_1, \dots, a_n \rangle$, n unsorted elements
Output: all the $a_i, 1 \leq i \leq n$ in increasing order

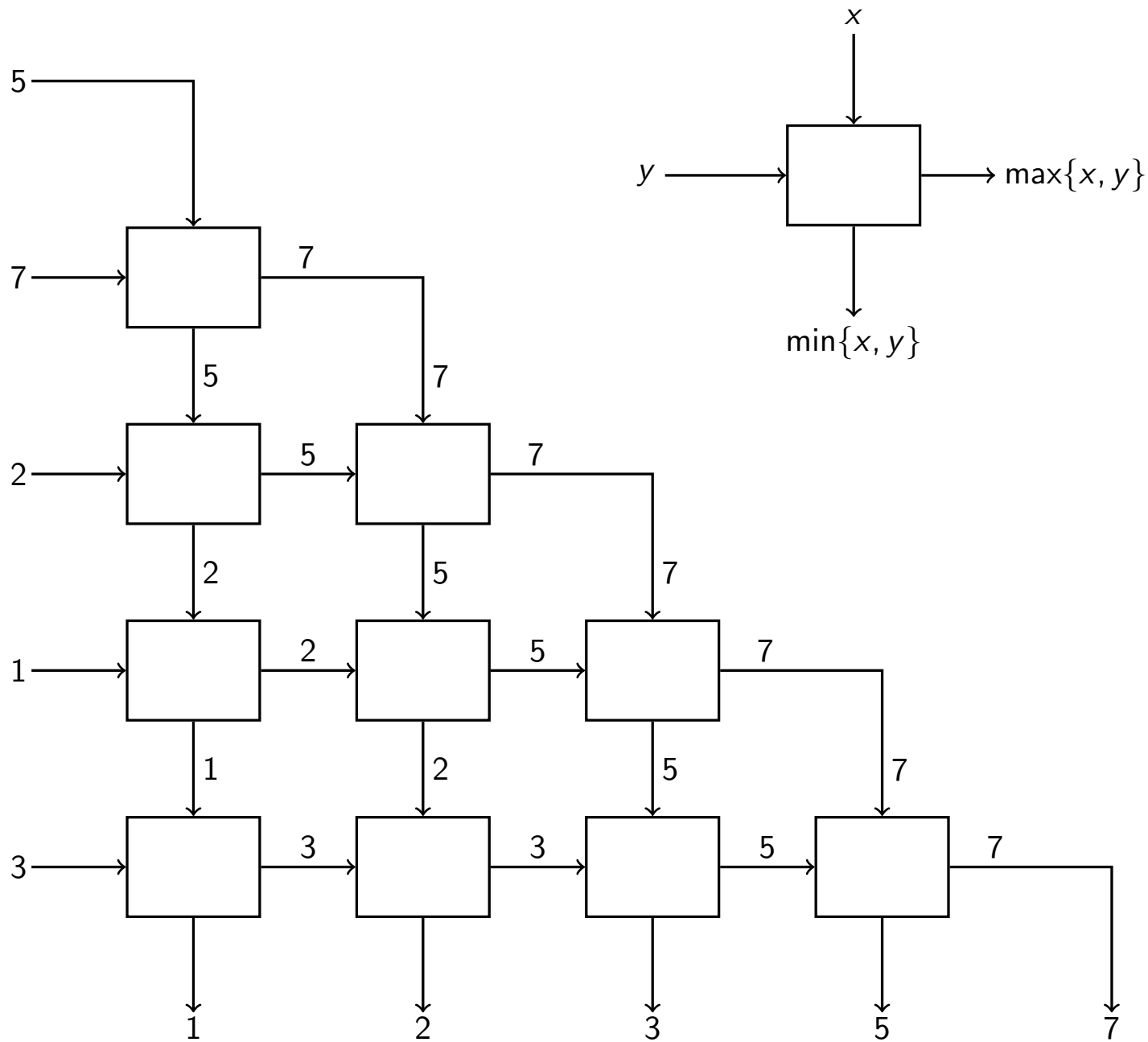
```
1  Function insertionSort(A[1...n], n):
2      if n = 1 then
3          return A[n]
4      else
5          insertionSort(A[1...n-1], n-1);
6          key ← A[n]; i ← n − 1;
7          while i > 0 and A[i] > key do
8              A[i + 1] ← A[i]; i ← i − 1;
9          end
10         A[i + 1] ← key;
11         return A[1 . . . n];
12     end
13 end
```

Selection Sort

Input: $A[1 \dots n] = \langle a_1, \dots, a_n \rangle$, n unsorted elements
Output: all the $a_i, 1 \leq i \leq n$ in increasing order

```
1 Function selectionSort(A[1...n], n):
2     if n = 1 then
3         return A[n]
4     else
5         indmax ←findMaxIndex(A[1...n], n);
6         swap(A[n], A[indmax]);
7         selectionSort(A[1...n − 1], n − 1)
8     end
9 end
```

Insertion Sort vs Selection Sort



Correctness of `insertionSort` and `selectionSort`

Proof. (Correctness of `insertionSort`).

- **base case ($n = 1$):** Trivial since any array of length 1 is sorted.
- **inductive case ($n \geq 1$):** Assume that `insertionSort`$(A[1 \ldots n], n)$ is sorted. We want to show that `insertionSort`$(\langle A[1 \ldots n+1] \rangle, n+1)$ is also sorted, which is true since $A[n+1]$ is inserted into the sorted `insertionSort`$(A[1 \ldots n], n)$ to make this happen. □

Proof. (Correctness of `selectionSort`).

- **base case ($n = 1$):** Trivial since any array of length 1 is sorted.
- **inductive case ($n \geq 1$):** Assume that `selectionSort`$(A[1 \ldots n], n)$ is sorted. We want to show that `selectionSort`$(\langle A[1 \ldots n+1] \rangle, n+1)$ is also sorted. Since $A[\mathit{indexmax}] \geq A[i]$ for all $i < n+1$, then after swap, we have $A[n+1] \geq A[i]$ for all $i < n$. By induction hypothesis, $A[1 \ldots n]$ is already sorted, hence $A[1 \ldots n+1]$ is sorted. □

Fibonacci Numbers

Example

The Fibonacci Numbers is defined by

$$\begin{aligned} f_0 &= 0, \\ f_1 &= 1, \\ f_n &= f_{n-1} + f_{n-2}, \qquad n \geq 2 \end{aligned}$$

Show that

$$f_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right]$$

Strong (Complete) Induction

The method of induction can be strengthened. We can replace

(I) $P(n_0)$ is true.

(II) $P(n+1)$ is true whenever $P(n)$ is true for $n \geq n_0$.

with

(I) $P(n_0)$ is true.

(II') $P(n+1)$ is true whenever all the statements $P(n_0), P(n_0+1), \ldots, P(n)$ are true.

Fibonacci Numbers

Proof.

We prove the formula for Fibonacci Numbers by strong induction on n.
First note that we could let $\varphi = \frac{1+\sqrt{5}}{2}$, then we need to show that

$$f_n = \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}}.$$

- **base case ($n = 0$):**

$$\frac{\varphi^0 - (-\varphi)^0}{\sqrt{5}} = 0 = f_0$$

- **base case ($n = 1$):**

$$\frac{\varphi^1 - (-\varphi)^{-1}}{\sqrt{5}} = \cdots = 1 = f_1$$

Fibonacci Numbers

Proof (Cont.)

- **inductive case ($n \geq 2$):** Assume that the formula holds for all $k < n$, then note that $\varphi^2 = \varphi + 1$,

$$\begin{aligned} f_n &= f_{n-1} + f_{n-2} \\ &= \frac{\varphi^{n-1} - (-\varphi)^{-(n-1)}}{\sqrt{5}} + \frac{\varphi^{n-2} - (-\varphi)^{-(n-2)}}{\sqrt{5}} \\ &= \frac{\varphi^{n-2}(\varphi + 1) - (-\varphi)^{-(n-1)}(1 - \varphi^{-1})}{\sqrt{5}} \\ &= \frac{\varphi^n - (-\varphi)^{-n}}{\sqrt{5}} \end{aligned}$$

□

Prime Factorization

Theorem (Fundamental Theorem of Arithmetic (Existence Part))

Let $n \in \mathbb{N} \setminus \{0\}$, then there exist $k \geq 0$ prime numbers $p_1, p_2, \ldots, p_k$ such that $n = \prod_{i=1}^{k} p_i$. (also unique up to order, more on this later.)

Proof by strong induction on n.

- **base case ($n = 1$):** by convention, 1 is the product of *zero* prime numbers.
- **inductive case ($n \geq 2$):** assume the statement is true for all positive integer n' where $1 \leq n' \leq n - 1$.
  - If n is prime, which is the product of 1 prime number.
  - If n is composite, then by definition there exist positive integers a and b such that $n = a \cdot b$, with $2 \leq a, b \leq n - 1$. By inductive hypotheses, we have $a = q_1 \cdot q_2 \cdots q_\ell$ and $b = r_1 \cdot r_2 \cdots r_m$ for prime numbers $q_1, \ldots, q_\ell$ and $r_1, \ldots, r_\ell$. Therefore $n = a \cdot b = q_1 \cdot q_2 \cdots q_\ell \cdot r_1 \cdot r_2 \cdots r_m$ which is the product of $\ell + m$ prime numbers. □

Prime Factorization

```
1  Function primeFactor(n):
2      if n = 1 then
3          return ⟨⟩
4      else
5          if n is prime then
6              return ⟨n⟩
7          else
8              find factors a, b where 2 ≤ a, b ≤ n − 1 such that
                 n = a · b.
9              ⟨q_1, ..., q_ℓ⟩ ← primeFactor(a);
10             ⟨r_1, ..., r_m⟩ ← primeFactor(b);
11             return ⟨q_1, ..., q_ℓ, r_1, ..., r_m⟩
12         end
13     end
14 end
```

Quick Sort

Input: $A[1 \dots n] = \langle a_1, \dots, a_n \rangle$, n unsorted elements
Output: all the $a_i, 1 \leq i \leq n$ in increasing order

```
1  Function quickSort(A[1...n], n):
2      if n ≤ 1 then
3          return A[n]
4      else
5          choose pivot ∈ {1, ..., n};
6          L := ⟨⟩; R := ⟨⟩;
7          for i ∈ {1, ..., n} with i ≠ pivot do
8              if A[i] < A[pivot] then
9                  L ← L + A[i]
10             else
11                 R ← R + A[i]
12             end
13         end
14         L ← quickSort(L);
15         R ← quickSort(R);
16         return L + ⟨A[pivot]⟩ + R
17     end
18 end
```

Quick Sort

Proof. (Correctness of `quickSort`).

Let $P(n)$ denote the claim that `quickSort`$(A[1 \ldots n])$ returns a sorted array. For simplicity, we assume that the elements in the array are distinct. We will prove $P(n)$ for all $n \geq 0$ by strong induction on n.

- **base case ($n = 0, 1$):** done b/c any array of length 0 or 1 are already sorted.
- **inductive case ($n \geq 2$):** assume $P(0), \ldots, P(n-1)$ that for any array $B[1 \ldots k]$ with distinct elements and $k < n$, `quickSort`$(B[1 \ldots k])$ returns a sorted array. Let $A[1 \ldots n]$ be an arbitrary array with distinct elements. Let *piviot* $\in \{1, \ldots, n\}$ be arbitrary. We need to show that x appears before y in `quicksort`$(A[1 \ldots n])$ iff $x < y$.

Quick Sort

Proof. (Correctness of `quickSort` Cont.)

Inductive case ($n \geq 2$):

- Case 1. $x = A[pivot]$. By $\texttt{quickSort}(A[1 \ldots n])$, $y \in R$ iff $x < y$.
- Case 2. $y = A[pivot]$. Similar to Case 1.
- Case 3. $x, y < A[pivot]$. Now $x, y \in L$. Since $A[pivot] \notin L$, thus L is of at most length $n - 1$. Hence by IH x appears before y in $\texttt{quickSort}(L)$ iff $x < y$. Furthermore x appears before y in $\texttt{quickSort}(A[1 \ldots n])$ iff $x < y$.
- Case 4. $x, y > A[pivot]$. Similar to Case 3.
- Case 5. $x < A[pivot] < y$. Trivial.
- Case 6. $y < A[pivot] < x$. Impossible. □

	L	$pivot$	R
1.		x	
2.		y	
3.	x, y		
4.			x, y
5.	x		y
6.	y		x

$L = A[1 \ldots pivot - 1]$

$R = A[pivot + 1 \ldots n]$

Recursive Definitions and the Factorial

Similar to induction, we could make ***recursive definitions***. For example, we wish to define a function (to be called the ***factorial***)

$$(\,\cdot\,)!\colon \mathbb{N} \to \mathbb{N}$$

having the properties that

$$0! := 1, \qquad n! := n \cdot (n-1)!, \qquad n \in \mathbb{N} \setminus \{0\}.$$

This is an example of a ***recursive definition*** and we may ask whether such a definition "makes sense", i.e., whether such a function exists and is unique.

In the present case, the function is simply

$$n! := \prod_{k=1}^{n} k, \qquad n \in \mathbb{N} \setminus \{0\},$$

This is called a ***closed formula*** for $n!$.

Recursive Definitions

Recursive definitions often occur naturally in the formulation of a problem, and finding a closed formula can be extremely difficult. In some situations, a closed formula is highly desirable, while at other times, important properties are best expressed through recursive expressions.

For example, there exists a continuous extension of the factorial, given by the ***Euler gamma function***, defined for $t > 0$,

$$\Gamma(t) := \int_0^\infty z^{t-1} e^{-z}\, dz, \qquad t > 0.$$

It is possible to show that $\Gamma(1) = 1$ and that

$$\Gamma(t+1) = t\Gamma(t) = t\Gamma\big((t-1)+1\big) \qquad t > 0.$$

we see that $\Gamma(n+1) = n!$ for all $n \in \mathbb{N}$. Furthermore, we can define functions not just based on their preceding value, but on several such values. For example, The ***Fibonacci sequence***.

Recursive Definitions of Sets

In the same manner, we can define subsets of $\mathbb{N}$ recursively. For example, consider the set $S \subset \mathbb{N}$ such that

$$3 \in S \qquad \text{and} \qquad x, y \in S \Rightarrow x + y \in S. \tag{2}$$

We know that $3 \in S$, so $3 + 3 = 6 \in S$, $3 + 6 = 9 \in S$, $6 + 6 = 12 \in S$ and so on. Our goal is to prove that

$$S = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \setminus \{0\} \colon n = 3k\}.$$

However, this requires a little preparation.

Recursively Defined Structures

David Liben-Nowell, Connecting Discrete Mathematics and Computer Science, manuscript at `www.cs.carleton.edu/faculty/dln/book/`

Linked Lists

A ***linked list*** is either;

- $\langle\rangle$, known as the ***empty list***; or
- $\langle x, L\rangle$, where x is an arbitrary element and L is a linked list.

Binary trees

A ***binary tree*** is either:

- the empty tree, denoted by `null`; or
- a root node x, a ***left subtree*** T_ℓ, and a ***right subtree*** T_r, where x is an arbitrary value and T_ℓ and T_r are both binary trees.

Recursively Defined Structures

Arithmetic Expressions

An ***arithmetic expression*** is any of the following:

- any integer n;
- $-E$, where E is an arithmetic expression; or
- $E \odot F$, where E and F are arithmetic expressions and $\odot \in \{+, -, \cdot, /\}$ is an ***operator***.

Sentences of propositional logic

A ***sentence of propositional logic*** (also known as a ***well-formed formula***, or ***wff***) over the propositional variables X is one of the following

- x, for some $x \in \mathrm{X}$;
- $\neg P$, where P is a wff over X; or
- $P \vee Q$, $P \wedge Q$, or $P \rightarrow Q$, where P and Q are wffs over X.

Recursively Defined Structures

Natural numbers, recursively defined

A ***natural numbers*** is either:

- zero, denoted by 0; or
- the successor of a natural number n, denoted by $\mathrm{succ}(n)$ or n^+ for a natural numbers n.

Theorem (Recursion on $\mathbb{N}$)

Let A be a set, $a \in A$, and $F : A \to A$. Then there exists a unique function $h : \mathbb{N} \to A$ such that

- $h(0) = a$,
- $h(n^+) = F(h(n))$, $\forall n \in \mathbb{N}$.

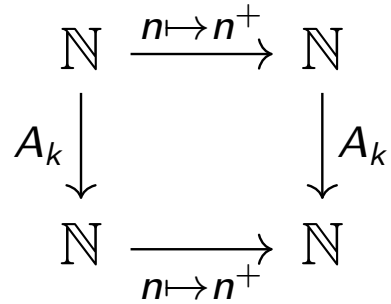
$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{n \mapsto n^+} & \mathbb{N} \\ {\scriptstyle h}\downarrow & & \downarrow{\scriptstyle h} \\ A & \xrightarrow[F]{} & A \end{array}$$

Recursion theorem on $\mathbb{N}$

Example

For fixed $k \in \mathbb{N}$, consider the function $A_k : \mathbb{N} \to \mathbb{N}$ given by

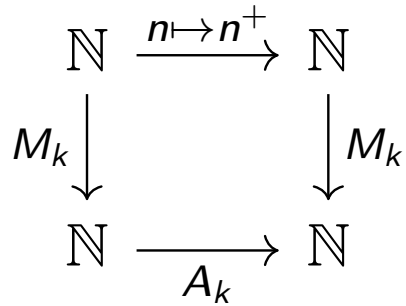
- $A_k(0) := k$
- $A_k(n^+) := A_k(n)^+$



Example

For fixed $k \in \mathbb{N}$, consider the function $M_k : \mathbb{N} \to \mathbb{N}$ given by

- $M_k(0) := 0$
- $M_k(n^+) := A_k(M_k(n))$



Arithmetic and Order on $\mathbb{N}$

Definition

- $n + k := A_k(n)$
- $n \times k := M_k(n)$
- $n < m$ if $n \in m$

Natural Numbers $\mathbb{N}$

A natural number is either

- $0 := \{\} = \varnothing$, or
- $n + 1 = n^+ := n \cup \{n\}$, $n \in \mathbb{N}$.

Usual laws (to be verified)

- Associative law for addition: $(a + b) + c = a + (b + c)$
- Commutative law for addition: $a + b = b + a$
- Distributive law: $a(b + c) = ab + ac$
- Associative law for multiplication: $(ab)c = a(bc)$
- Commutative law for multiplication: $ab = ba$
- Order preserved by addition: $a + c = b + c$
- Order preserved by multiplication: $ac < bc$ if $a < b$ and $c \neq 0$

Structural Induction

Structural induction is a useful variant of induction that allows us to prove properties for recursively defined objects.

Structural induction establishes a statement on a recursively defined set in two steps. We call those elements specifically included in the set the basis elements of the set.

1. Establish the statement for the basis elements.
2. Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the statement holds for these new elements.

The justification for structural induction lies in ordinary induction, applied to the statement

$P(n)$: The claim is true for all elements of the set generated with n or fewer applications of the recursive rules for the set.

Structural induction first establishes $P(0)$ and then $P(n) \Rightarrow P(n+1)$.

Explicit Representation of Recursively Defined Sets

Example

Define $S \subset \mathbb{N}$ to be the set such that

(i) $3 \in S$,

(ii) $x, y \in S \Rightarrow x + y \in S$.

Let

$$T = \{n \in \mathbb{N} \mid \exists k \in \mathbb{N} \setminus \{0\} \text{ such that } n = 3k\}$$

We want to show that $S = T$.

Proof.

First, we show $S \subset T$ by structural induction: $3 = 3 \cdot 1 \in T$, so the base case is established. Now for $x, y \in S$ suppose that $x, y \in T$ so that $x = 3k$ and $y = 3k'$ for $k, k' \in \mathbb{N} \setminus \{0\}$. Then

$$x + y = 3k + 3k' = 3(k + k')$$

so $x + y \in T$. This shows that $S \subset T$.

Explicit Representation of Recursively Defined Sets

Proof (Cont.)

Next, we show $T \subset S$ by (ordinary) induction. We claim that

$$\forall k \in \mathbb{N} \setminus \{0\} : 3k \in S.$$

For $k = 1$, $3k = 3 \cdot 1 = 3 \in S$, so the base case is established. Now suppose that $3k \in S$. Since $3 \in S$ by definition, we can apply the recursive rule for S to deduce that

$$3(k+1) = 3k + 3 \in S.$$

This shows that $3(k+1) \in S$ if $3k \in S$. By the structural induction principle, $3k \in S$ for all $k \in \mathbb{N} \setminus \{0\}$. This established $T \subset S$.

We finally conclude that $S = T$. □

Propositional Logic Using $\neg$ and $\wedge$

Example

For any logical proposition φ using the connectives $\{\neg, \wedge, \vee, \rightarrow\}$, there exists a proposition using only $\{\neg, \wedge\}$ that is logically equivalent to φ.

Proof by structural induction.

For a logical proposition φ, let $A(\varphi)$ denote the property that there exists a $\{\neg, \wedge\}$-only proposition logically equivalent to φ. We'll prove by structural induction on φ that $A(\varphi)$ holds for any well-formed formula φ.

- **base case: φ is a variable, say $\varphi = x$.** No need for connectives from the set $\{\neg, \wedge\}$, $A(\varphi)$ is vacuously true.
- **inductive case I: φ is a negation, say $\varphi = \neg p$.** Assume the IH $A(p)$, we need to show $A(\neg p)$. By IH, there exists a $\{\neg, \wedge\}$-only proposition $q \Leftrightarrow p$. Since $\neg q \Leftrightarrow \neg p$, and $\neg q$ contains only connectives from $\{\neg, \wedge\}$, therefore $A(\neg p)$ follows.

Propositional Logic Using $\neg$ and $\wedge$

Proof by structural induction, Cont.

- **inductive case II: φ is a conjunction, disjunction, or implication, say $\varphi = p_1 \wedge p_2$, $\varphi = p_1 \vee p_2$, $\varphi = p_1 \to p_2$.** Assume IH $A(p_1)$ and $A(p_2)$, that is, there exist $\{\neg, \wedge\}$-only propositions q_1 and q_2 such that $q_1 \Leftrightarrow p_1$ and $q_2 \Leftrightarrow p_2$. We need to show $A(p_1 \wedge p_2)$, $A(p_1 \vee p_2)$, and $A(p_1 \to p_2)$. Indeed, note that

$$p_1 \wedge p_2 \Leftrightarrow q_1 \wedge q_2$$
$$p_1 \vee p_2 \Leftrightarrow q_1 \vee q_2 \Leftrightarrow \neg(\neg q_1 \wedge \neg q_2)$$
$$p_1 \to p_2 \Leftrightarrow q_1 \to q_2 \Leftrightarrow \neg(q_1 \wedge \neg q_2)$$

  Since q_1 and q_2 are $\{\neg, \wedge\}$-only, $A(p_1 \wedge p_2)$, $A(p_1 \vee p_2)$, and $A(p_1 \to p_2)$ follow. □

Weak Induction as Special Case of Structural Induction

Note that natural numbers $\mathbb{N}$ can be recursively defined, i.e., a natural number is either

- 0, or
- the successor of a natural number n, denoted by $\text{succ}(n)$ or n^+ for a natural numbers n.

Under this definition, a proof of $\forall n \in \mathbb{N} : P(n)$ by structural induction and a proof of $\forall n \in \mathbb{N} : P(n)$ are identical:

- hey have precisely the same **base case**: prove $P(0)$; and
- they have precisely the same **inductive case**: prove $P(n) \Rightarrow P(n^+)$, i.e., prove that $P(n) \Rightarrow P(n+1)$.

Well-Ordering Principle (WOP)

Theorem (Well-Ordering Principle)

Every nonempty collection of natural numbers has a least element.

Proof by induction.

We'll prove the contrapositive, namely, that if a collection of natural numbers has no least element, then it must be empty.
Let T be such a nonempty set of natural numbers. Let $S = \mathbb{N} \setminus T$. We need to show that $n \in S$ for all $n \in \mathbb{N}$.

- **base case ($n = 0$):** If $0 \in T$, then 0 is the least element. So $0 \notin T$, i.e., $0 \in S$.
- **inductive case ($n \geq 1$):** Suppose $n \in S$. If any of the numbers less than n were in T, then one of them would be least (since there are only finitely many such numbers and every finite set has a least element[1]). So none of the numbers $0, 1, \ldots, n$ is in T. If $n+1 \in T$, then $n+1$ would be least. So $n+1 \notin T$, i.e., $n+1 \in S$. □

1. can be proven using induction

Prime Factorization

Recall

Theorem (Fundamental Theorem of Arithmetic)

Let $n \in \mathbb{N} \setminus \{0\}$, then there exist $k \geq 0$ prime numbers $p_1, p_2, \ldots, p_k$ such that $n = \prod_{i=1}^{k} p_i$. (also unique up to order, more on this later.)

Proof by WOP.

Let T be the set of natural numbers greater than 1 which cannot be written as the product of primes. By WOP, T has a least element n. Clearly n cannot be prime, so n is composite. Then we can write $n = ab$, where neither of a and b is 1. So $a < n$ and $b < n$. If both a and b had prime factorizations, then so would n. Therefore at least one of a and b does not have a prime factorization (by relabeling, we can assume it is a). But $a < n$ and $a \in T$, so n was not least in T.
This contradiction establishes that T has no least element, hence by WOP must be empty. So every natural number greater than 1 can be written as the product of primes. □

Back to The Beginning

Recall the claim that $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$ for all $n \in \mathbb{N}$.

Proof by WOP.

Suppose not. Then there exists some $p \in \mathbb{N}$ such that $\sum_{k=0}^{p} k \neq \frac{p(p+1)}{2}$. Consider the set of all such numbers:

$$T = \left\{ k \;\middle|\; 1 + \cdots + k \neq \frac{k(k+1)}{2} \right\}$$

Thus $p \in T$ by assumption; in particular $T \neq \varnothing$.
By WOP, T has a least element N. $N \neq 0$ since $0 = 0(0+1)/2$. Therefore $N > 1$. But then N admits a predecessor, $n = N - 1$. Since $n < N$, then $n \notin T$ (b/c N is ***least*** in T). That is, $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$. Now consider $\sum_{k=0}^{N} k = \left(\sum_{k=0}^{n} k\right) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2} = \frac{N(N+1)}{2}$, which show that $N \notin T$, contradiction! So the initial supposition was incorrect, and thus the claim is true. □

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Motivation

Primitive Models

- equivalence relations ($=$, $\cong$, $\equiv$, $\sim$, etc.)
- partial orders ($\leq$, $\subset$, $\preceq$, $|$, etc.)

Relations

Definition

A subset $R \subset A \times B$ is called a (binary) ***relation*** from A to B. If $A = B$, we say that R is a ***relation on*** A.

Notation

- $(x, y) \in R$,
- xRy,
- via predefined symbols, e.g.,
  - $x \preceq y$, i.e., $(x, y) \in \preceq \subset A \times B$;
  - $x \sim y$, i.e., $(x, y) \in \sim \subset A \times B$.

Definition

- $\text{domain}\,(R) := \{x \mid \exists y(xRy)\}$
- $\text{range}\,(R) := \{y \mid \exists x(xRy)\}$

Relations

Examples

Suppose $R \subset A \times B$.

- $R = \varnothing$, the ***empty relation***, with $\text{domain}(\varnothing) = \text{range}(\varnothing) = \varnothing$.
- When $A = B$, we have the ***identity relation***,

$$\text{id}_A = \{(a, a) \mid a \in A\}$$

  The identity relation relates every element to itself. Note that $\text{domain}(\text{id}_A) = \text{range}(\text{id}_A) = A$.
- The relation $A \times B$ itself. This relation relates every element of A to every element of B. Note that $\text{domain}(A \times B) = A$ and $\text{range}(A \times B) = B$.

Functions

Definition

A ***function*** is a relation F such that

$$(\forall x \in \operatorname{dom} F)(\exists! y(xFy))$$

Remark

- Given function $F : A \to B$, then $(\forall x, y \in A)(x = y \Rightarrow F(x) = F(y))$.
- For a function F and a point $x \in \operatorname{dom}(F)$, the unique y such that xFy is called the ***value*** of F at x and is denoted $F(y)$. Thus $(x, F(x)) \in F$.
- Range/Image of a function is sometimes hard to find.

Remark

- Partial function: not (necessarily) everywhere defined.
- (Total) function: everywhere defined.

Collatz Conjecture ($3n+1$ Problem)

Given $n \in \mathbb{N} \setminus \{0\}$, construct the sequence $c_i(n)$ as follows starting with $i = 1$:

$$c_1(n) = n$$

$$c_{i+1}(n) = \begin{cases} c_i(n)/2, & \text{if } c_i(n) \text{ even} \\ 3c_i(n) + 1, & \text{if } c_i(n) \text{ odd} \end{cases}$$

Observe that for $n = 1$, we get the infinite periodic sequence

$$1 \to 4 \to 2 \to 1 \to 4 \to 2 \to 1 \to \cdots$$

so we may assume that we stop the first time that the sequence $c_i(n)$ reaches the value 1 (if at all). Such an index i is called the stopping time of the sequence.

Conjecture (Collatz)

For any starting integer value $n \geq 1$, the sequence $(c_i(n))$ always reaches 1.

Collatz Conjecture ($3n + 1$ Problem)

- $n = 3$: stops after 7 steps,

$$3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

- $n = 5$: stops after 5 steps,

$$5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

- $n = 6$: stops after 8 steps,

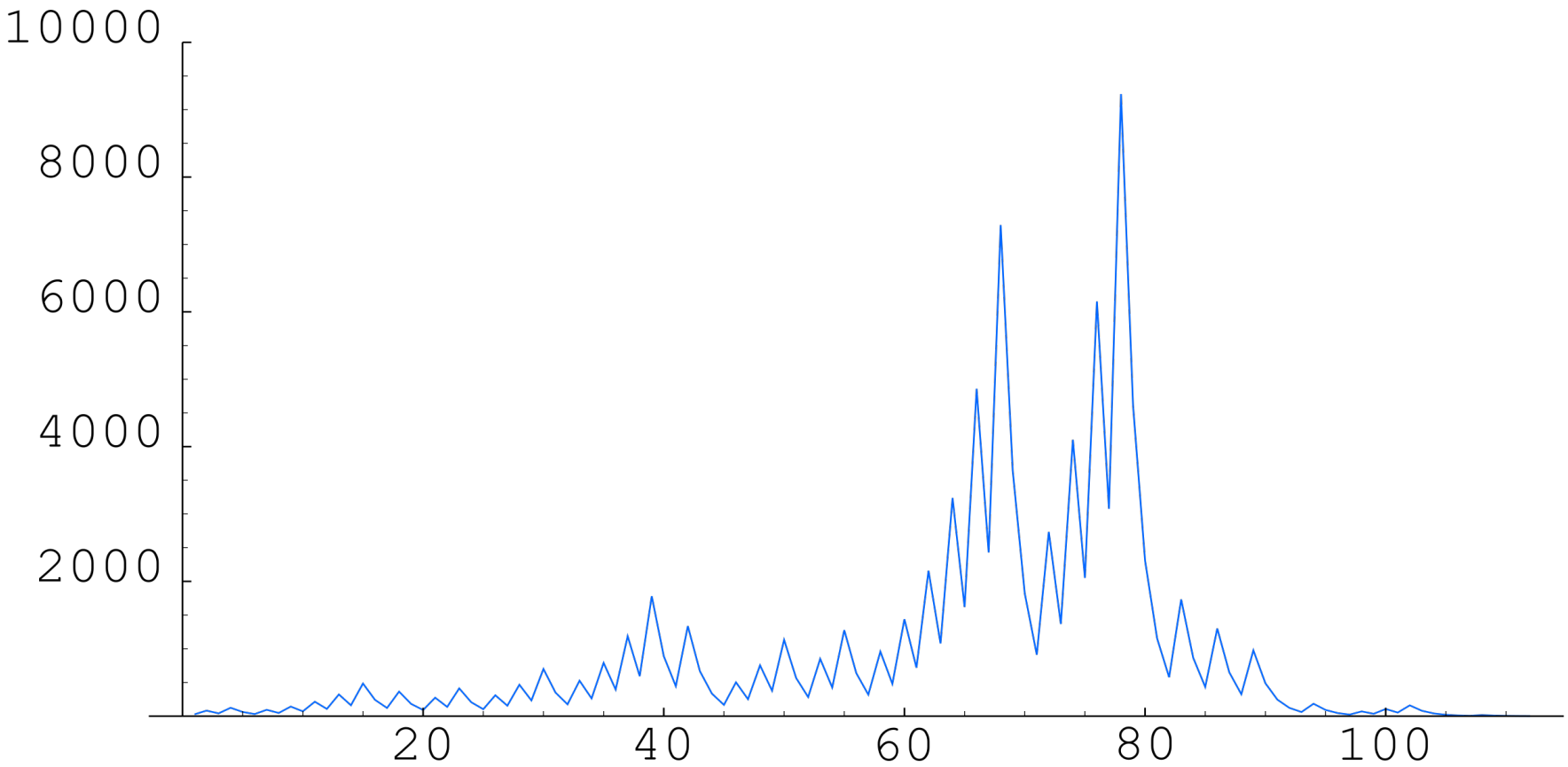
$$6 \to 3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1.$$

- $n = 7$: stops after 16 steps,

$$\begin{aligned} 7 &\to 22 \to 11 \to 34 \to 17 \to 52 \to 26 \\ &\to 13 \to 40 \to 20 \to 10 \to 5 \to 16 \\ &\to 8 \to 4 \to 2 \to 1. \end{aligned}$$

- $n = 27$: stops after 111 steps.
- $n = 97$: stops after 118 steps.

Collatz Conjecture ($3n + 1$ Problem)



$n = 27$

Collatz Conjecture ($3n + 1$ Problem)

We can define the partial function $C : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ as

$$C(n) := \min\{i \in \mathbb{N} \mid c_i(n) = 1\}$$

For example,

n	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$C(n)$	0	1	7	2	5	8	16	3	19	6	14	$\cdots$

The Collatz conjecture is equivalent to asserting that the function C is a (total) function.

Functions

For arbitrary sets/relations/functions A, F, and G,

- The ***inverse*** of F is the set

$$F^{\top} = F^{-1} = \{(y, x) \mid xFy\}$$

- The ***composition*** of F and G is the set (beware of the order)

$$F \circ G = \{(x, z) \mid \exists y(xGy \wedge yFz)\}$$

- The ***restriction*** of F to A is the set

$$F|A = \{(x, y) \mid (xFy) \wedge (x \in A)\}$$

- The ***image*** of A ***under*** F is the set

$$F(A) = \mathrm{ran}(F|A) = \{y \mid (\exists x \in A)(xFy)\}$$

If F is a function, then $F(A) = \{F(x) \mid x \in A\}$.

Injection and Surjection

Definition

Given a function $F : A \to B$, with $\operatorname{dom} F = A$ and $\operatorname{ran}(F) \subset B$, then

- F is ***injective*** or ***one-to-one*** if $\forall x, y \in A(F(x) = F(y) \Rightarrow x = y)$;
- F is ***surjective*** or ***onto*** if $\operatorname{ran}(F) = B$.
- F is ***bijective*** if it is both injective and surjective.

The above function F is also called an injection, surjection, or bijection, respectively.

Example

Given a vector space V over $\mathbb{R}$, and fix $v_1, \ldots, v_n \in V$, define the function $X : \mathbb{R}^n \to V$, $(a_1, a_2, \ldots, a_n) \mapsto a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$, then the set $\{v_1, v_2, \ldots, v_n\} \subset V$

- ***spans/generates*** V iff X is surjective.
- is ***linearly independent*** iff X is injective.
- is a ***basis*** iff X is both injective and surjective.

Injection and Surjection

Theorem/Definition

Given a function $F : A \to B$, $A \neq \varnothing$, then

- There exists a function $G : B \to A$ (a "left inverse") such that $G \circ F = \mathrm{id}_A \Leftrightarrow F$ is one-to-one.
- There exists a function $G : B \to A$ (a "right inverse") such that $F \circ G = \mathrm{id}_B \Leftrightarrow F$ is onto.

Injection and Surjection

Theorem

Let $f : A \to B$, $g : B \to C$

- *If $g \circ f$ is injective, then f is injective.*
- *If $g \circ f$ is surjective, then g is surjective.*

Proof.

- *Given $x, y \in A$, then*

$$f(x) = f(y) \Rightarrow g(f(x)) = g(f(y)) \Rightarrow (g \circ f)(x) = (g \circ f)(y)$$
$$\Rightarrow x = y \text{ (b/c } g \circ f \text{ is injective)}$$

  Therefore f is injective.

- *Since $g \circ f$ is surjective, then $\forall z \in C$, $\exists x \in A$ such that $g \circ f(x) = g(f(x)) = z$. Let $y = f(x) \in B$ (which exists for all $x \in A$ since f is a function), then $\forall z \in C$, $\exists y \in B$ such that $z = f(y)$. Therefore g is surjective.* □

Injection and Surjection

Theorem

Let $f : A \to B$, $g : B \to C$

- *If $g \circ f$ is injective, then f is injective.*
- *If $g \circ f$ is surjective, then g is surjective.*

Proof (Alternative).

- *Since $g \circ f$ is injective, then there exists $h : C \to A$ such that $h \circ (g \circ f) = id_A$, that is, there exists $h \circ g : C \to A$ such that $(h \circ g) \circ f = id_A$. Therefore f is left invertible, hence injective.*
- *Since $g \circ f$ is surjective, then there exists $h : C \to A$ such that $(g \circ f) \circ h = id_C$, that is, there exists $f \circ h : C \to A$ such that $g \circ (f \circ h) = id_C$. Therefore g is right invertible, hence surjective.* □

Relations as Functions

Relation as multivariable boolean functions

Example

- Given a relation $R \subset A \times B$, the associated boolean function is given by

$$\phi_R : A \times B \to \{\top, \bot\}$$
$$(x, y) \mapsto \begin{cases} \top, & xRy \\ \bot, & \text{otherwise} \end{cases}$$

- Given a boolean function $\phi : A \times B \to \{\top, \bot\}$, the associated relation is given by

$$R_\phi = \{(x, y) \in A \times B \mid \phi(x, y) = \top\}$$

Relations as Functions

Relation as set functions

Example

- Given a relation $R \subset A \times B$, the associated set function is given by

$$\begin{aligned} \alpha_R : A &\to \mathcal{P}(B) \\ x &\mapsto \{y \in B \mid xRy\} \end{aligned}$$

- Given a set function $\alpha : A \to \mathcal{P}(B)$, the associated relation is given by

$$R_\alpha = \{(x, y) \in A \times B \mid y \in \alpha(x)\}$$

Relations as Functions

Relation as set functions

Example

- Given a relation $R \subset A \times B$, the associated set function is given by

$$\begin{aligned} \beta_R : B &\to \mathcal{P}(A) \\ x &\mapsto \{y \in A \mid xRy\} \end{aligned}$$

- Given a set function $\beta : B \to \mathcal{P}(A)$, the associated relation is given by

$$R_\beta = \{(x, y) \in A \times B \mid y \in \beta(x)\}$$

Properties of Relations

Definition

A (binary) relation R on A, i.e., $R \subset A \times A$, is

- ***reflexive*** if $aRa \Rightarrow \top$.
- ***irreflexive*** if $aRa \Rightarrow \bot$.
- ***total*** if $aRb \vee bRa \Rightarrow \top$.
- ***transitive*** if $aRb \wedge bRc \Rightarrow aRc$.
- ***symmetric*** if $aRb \Leftrightarrow bRa$.
- ***anti-symmetric*** if $aRb \wedge bRa \Rightarrow a = b$.
- ***asymmetric*** if $aRb \wedge bRa \Rightarrow \bot$.

Properties of Relations

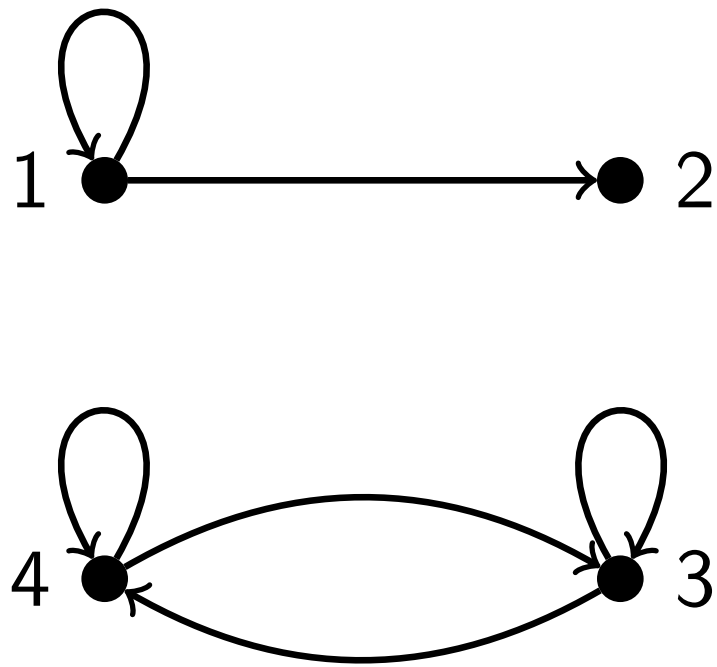
Example

	reflexive	*transitive*	*symmetric*	*antisymmetric*
$\leq$ on $\mathbb{R}$				
$<$ on $\mathbb{R}$				
$\subset$ on 2^S				
$\subsetneq$ on 2^S				
$\equiv_n$ on $\mathbb{Z}$				
$\mid$ on $\mathbb{N} \setminus \{0\}$				
$\mid$ on $\mathbb{N}$				
$\mid$ on $\mathbb{Z}$ $(0 \mid 0)$				
matrix similarity				

Properties of Relations

Example

$R = \{(1,1),(1,2),(3,3),(3,4),(4,3),(4,4)\}$ on $\{1,2,3,4\}$.



Important Relations

Definition

A ***partial order*** on a set P is a relation that is

- reflexive
- antisymmetric
- transitive

Example

- On $\mathbb{Z}$ (or $\mathbb{R}$ etc.): $a \leq b$
- On 2^S for a given S: $A \subset B$
- On $\mathbb{N}$: $a \mid b$
- On partitions: refinement

Irreflexive Relations

Recall that a relation R on a set A is irreflexive if $aRa \Rightarrow \bot$ for all $a \in A$.

Remark

- Irreflexive and non-reflexive are different concepts.
  - Irreflexive: zero self-loops.
  - Non-reflexive: missing self-loops.
- Antisymmetric and non-symmetric are different concepts.
  - Antisymmetric: no cycle of length 2.
  - Non-symmetric: exists directed edge of no return.

Terminologies on Partial Orders

Non-strict Partial Order (e.g., $\leq$, $\subseteq$)

A ***reflexive***, ***weak***, or ***non-strict*** partial order is a relation $\preceq$ over a set A that is

- reflexive
- antisymmetric
- transitive

Strict Partial Order (e.g., $<$, $\subsetneq$)

An ***irreflexive***, ***strong***, or ***strict*** partial order is a relation $\prec$ over a set A that is

- irreflexive
- asymmetric
- transitive

Remark

For every strict partial order there is a unique corresponding non-strict partial order, and vice-versa. The two differ by the identity relation on A.

Remark

The term ***partial order*** typically refers to a non-strict partial order relation.

Important Relations

Definition

An ***equivalence relation*** on a set A is a relation that is

- reflexive
- symmetric
- transitive

Example

- On $\mathbb{Z}$ (or $\mathbb{R}$ etc.): $a = b$
- On $\mathbb{Z}$: $a \equiv b \pmod{12}$
- On 2^S for given S: $A \equiv B$ iff $|A| = |B|$
- On square matrices: $A \cong B$ iff $A = PBP^{-1}$

Equivalence Classes

Definition

Given an equivalence relation R on A, the ***equivalence class*** containing x is the set

$$[x]_R := \{t \in A \mid xRt\}$$

Theorem

Given an equivalence relation R on A, then for $x, y \in A$,

$$[x]_R = [y]_R \Leftrightarrow xRy$$

Proof.

($\Rightarrow$) Let $[x]_R = [y]_R$, then $y \in [y]_R$ (b/c yRy) implies $y \in [x]_R$ (b/c $[x]_R = [y]_R$), hence xRy (by definition of $[x]_R$).

Equivalence Classes

Proof.

($\Leftarrow$) Assume xRy, then take any $t \in [y]_R$,

$$\begin{aligned} t \in [y]_R &\Rightarrow yRt \\ &\Rightarrow xRt \qquad (xRy \text{ and transitivity}) \\ &\Rightarrow t \in [x]_R \end{aligned}$$

hence $[y]_R \subset [x]_R$. The other direction is by symmetry of R. $\square$

Partition

Definition

A ***partition*** Π of a set A is a set of nonempty subsets of A that is disjoint and exhaustive, i.e.,

- $(\forall a, b \in \Pi)(a \neq b \Rightarrow a \cap b = \varnothing)$;
- $\bigcup \Pi = A$.

An element of a partition is called a ***fiber***, a ***block***, or an ***equivalence class***. An element of such an equivalence class is called a ***representative*** of the class.

Examples

- $A = \varnothing$: $\Pi = \varnothing$.
- $A \neq \varnothing$: $\Pi = \{\{x\} \mid x \in A\}$, or $\Pi = \{A\}$.
- $A = \mathbb{N}$: $\Pi = \{\{\text{even numbers}\}, \{\text{odd numbers}\}\}$

Partition

Theorem

Given an equivalence relation R on A, then the set $\{[x]_R \mid x \in A\}$ of all equivalence classes is a partition of A.

Proof.

- $[x]_R \neq \varnothing \forall x.$ (b/c $x \in [x]_R$)
- $\bigcup\{[x]_R \mid x \in A\} = A.$ (b/c $x \in [x]_R \subset A$)
- Suppose $t \in [x]_R \cap [y]_R$, then tRx and tRy, hence xRy and $[x]_R = [y]_R$.

□

Quotient set

Definition

Given an equivalence relation R on A, then the ***quotient set*** is given by

$$A/R := \{[x]_R \mid x \in A\}$$

where A/R is read "A modulo R".

Example

Let $\mathbb{N} = \{0, 1, 2, 3, \dots\}$, and define the relation $\sim$ on $\mathbb{N}$ by

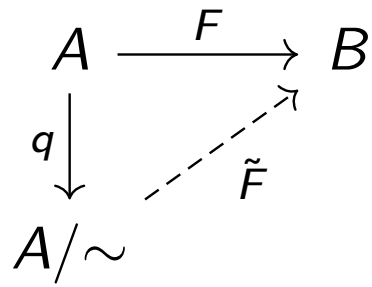
$$m \sim n \quad \Leftrightarrow \quad 6 \mid m - n, \text{i.e., } m - n \text{ divisible by } 6$$

then $\mathbb{N}/\sim = \{[0], [1], [2], [3], [4], [5]\}$

Quotient set

Example

Let $F : A \to B$ and for elements in A define $x \sim y \Leftrightarrow F(x) = F(y)$. The relation $\sim$ is an equivalence relation on A. There is a unique one-to-one function $\tilde{F} : A/\sim \to B$ such that $F = \tilde{F} \circ q$, where $q : A \to A/\sim$, $x \mapsto [x]$, is the natural quotient map. The value of $\tilde{F}$ at a particular equivalence class is the common value at the member of that equivalence class.



- $\tilde{F}$ is well-defined. Pick $[x], [y] \in A/\sim$,

$$[x] = [y] \Rightarrow x \sim y \Rightarrow F(x) = F(y) \Rightarrow F([x]) = F([y])$$

- $\tilde{F}$ one-to-one. $\tilde{F}([x]) = \tilde{F}([y]) \Leftrightarrow F(x) = F(y) \Leftrightarrow x \sim y \Leftrightarrow [x] = [y]$.
- q is surjective. (b/c $x \in [x]$ $\forall x \in A$)
- $\tilde{F}$ is unique. $\tilde{F} \circ q = \tilde{G} \circ q \Rightarrow \tilde{F} = \tilde{G}$.

Note that $\tilde{F} : A/\sim \to \text{ran}(F)$, $[x] \mapsto F(x)$, is bijective.

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Integers

Definition

Let $\sim$ be the following equivalence relation on $\mathbb{N}^2$,

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a +_{\mathbb{N}} d = b +_{\mathbb{N}} c$$

Explicitly, note that $\sim \subset \mathbb{N}^2 \times \mathbb{N}^2$, and

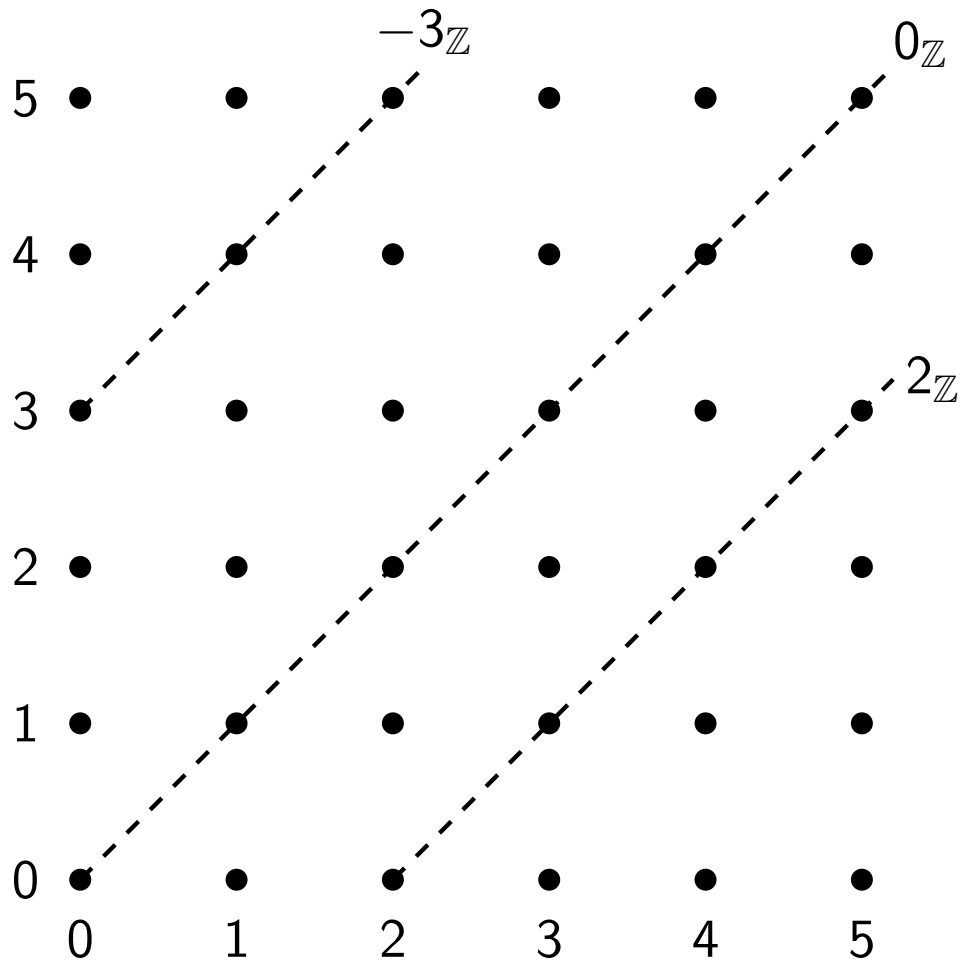
$$\sim = \{((a, b), (c, d)) \in \mathbb{N}^2 \times \mathbb{N}^2 \mid a, b, c, d \in \mathbb{N}, a +_{\mathbb{N}} d = b +_{\mathbb{N}} c\}$$

Define $\mathbb{Z} = \mathbb{N} \times \mathbb{N}/\sim$.

Example

- $0_{\mathbb{Z}} = \{(0_{\mathbb{N}}, 0_{\mathbb{N}}), (1_{\mathbb{N}}, 1_{\mathbb{N}}), \dots\} = [(0_{\mathbb{N}}, 0_{\mathbb{N}})] = [\{\{\varnothing\}\}] = [\{\{\{\}\}\}]$.
- $2_{\mathbb{Z}} = \{(2_{\mathbb{N}}, 0_{\mathbb{N}}), (3_{\mathbb{N}}, 1_{\mathbb{N}}), (4_{\mathbb{N}}, 2_{\mathbb{N}}), \dots\} = [(2_{\mathbb{N}}, 0_{\mathbb{N}})]$.
- $-3_{\mathbb{Z}} = \{(0_{\mathbb{N}}, 3_{\mathbb{N}}), (1_{\mathbb{N}}, 4_{\mathbb{N}}), (2_{\mathbb{N}}, 5_{\mathbb{N}}), \dots\} = [(0_{\mathbb{N}}, 3_{\mathbb{N}})]$.

Integers



Integers

Remark

The relation $\sim$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.

Proof.

Let $(a, b), (a', b'), (a'', b'') \in \mathbb{N} \times \mathbb{N}$.

- Reflexivity. It is clear that $(a, b) \sim (a, b)$, since $a + b = b + a$.
- Symmetry. Let $(a, b) \sim (a', b')$, then

$$\begin{aligned}(a, b) \sim (a', b') &\Rightarrow a + b' = a' + b \\ &\Rightarrow a' + b = a + b' \Rightarrow (a', b') \sim (a, b)\end{aligned}$$

- Transitivity. Let $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$, then we have $a + b' = a' + b$ and $a' + b'' = a'' + b'$. Therefore

$$a + b' + a' + b'' = a' + b + a'' + b'$$

hence $a + b'' = a'' + b$, i.e., $(a, b) \sim (a'', b'')$. $\square$

Integers

Well-defined operations on equivalence classes

- $[(a,b)] +_{\mathbb{Z}} [(c,d)] := [(a+c, b+d)]$.
- $[(a,b)] \times_{\mathbb{Z}} [(c,d)] := [(ac+bd, ad+bc)]$.
- $[(a,b)] <_{\mathbb{Z}} [(c,d)]$ if $a+d <_{\mathbb{N}} b+c$.

Proof.

We want to show that the operations do not depend on the choice of representatives. choose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, which indicates that $a+b' = a'+b$ and $c+d' = c'+d$, then

- We want to show $a+c+b'+d' = a'+b'+c+d$. Since
$$(a+c)+(b'+d') = (a+b')+(c+d')$$
$$= (a'+b)+(c'+d) = (a'+c')+(b+d)$$
Hence $(a+c, b+d) \sim (a'+c', b'+d')$, and $[(a+c, b+d)] = [(a'+c', b'+d')]$, independent of the choice of representatives.

Integers

Proof (Cont.)

- We want to show $ac + bd + a'd' + b'c' = a'c' + b'd' + ad + bc$. Note that $a + b' = a' + b$ and $c + d' = c' + d$, then

$$\begin{aligned} c(a + b') &= c(a' + b) \\ d(a' + b) &= d(a + b') \\ a'(c + d') &= a'(c' + d) \\ b'(c' + d) &= b'(c + d') \end{aligned}$$

which simplifies to

$$\begin{aligned} ac + b'c &= a'c + bc \\ a'd + bd &= ad + b'd \\ a'c + a'd' &= a'c' + a'd \\ b'c' + b'd &= b'c + b'd' \end{aligned}$$

Add all above together and cancel the unwanted terms.

Integers

Proof (Cont.)

- We want to show that $a + d < b + c$ iff $a' + d' < b' + d'$. Recall that $a + b' = a' + b$ and $c + d' = c' + d$, then

$$\begin{aligned} a + d < b + c \quad &\Leftrightarrow \quad a + d + b' + d' < b + c + b' + d' \\ &\Leftrightarrow \quad a' + b + d + d' < b + b' + c' + d \\ &\Leftrightarrow \quad a' + d' < b' + c' \end{aligned}$$

Therefore the ordering $<_{\mathbb{Z}}$ on $\mathbb{Z}$ is well-defined. □

Rational Numbers

Definition

Let $\mathbb{Z}^+ = \{z \in \mathbb{Z} \mid z >_{\mathbb{Z}} 0_{\mathbb{Z}}\}$, and let $\sim$ be the following equivalence relation on $\mathbb{Z} \times \mathbb{Z}^+$,

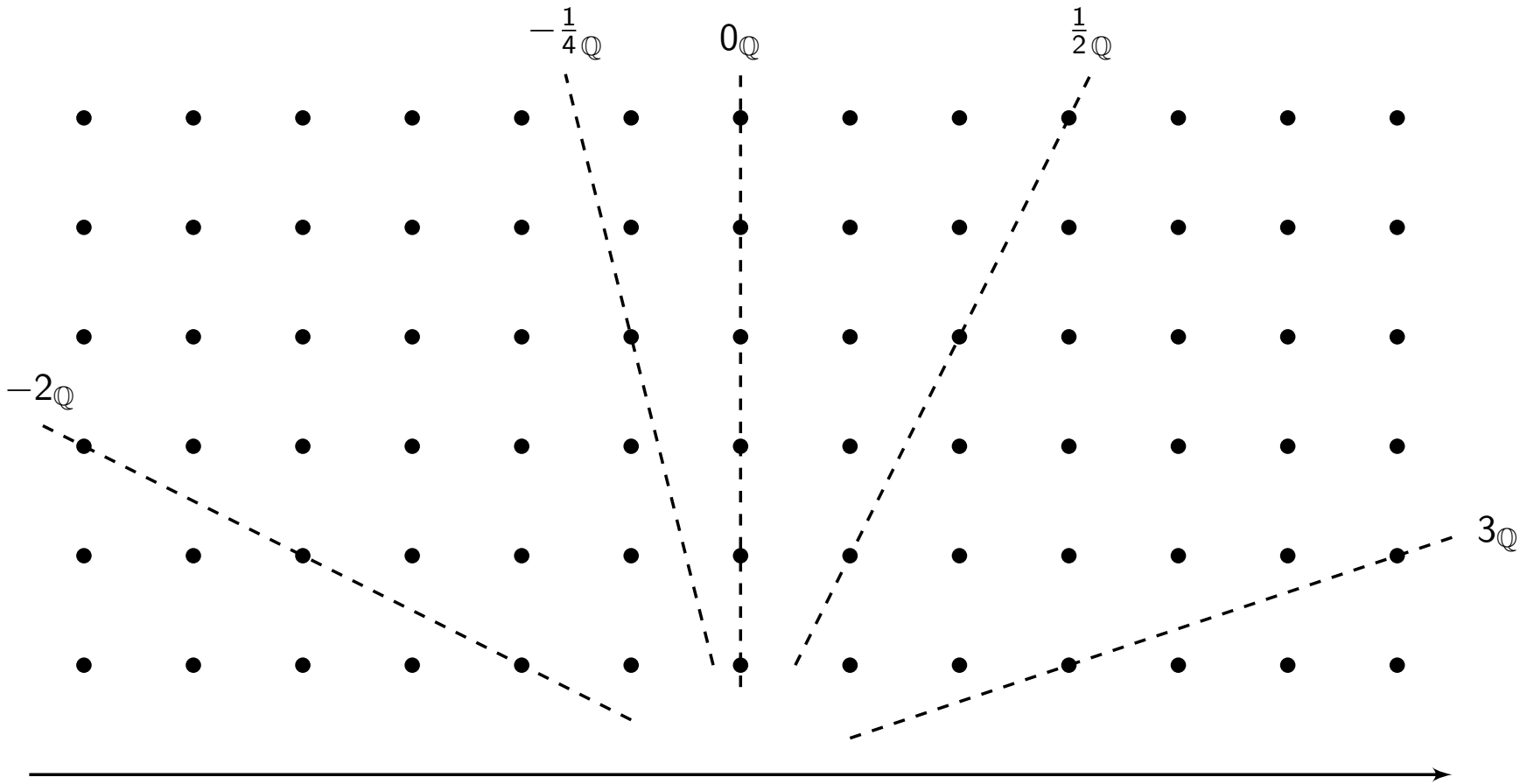
$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a \times_{\mathbb{Z}} d = b \times_{\mathbb{Z}} c$$

Explicitly, note that $\sim \subset (\mathbb{Z} \times \mathbb{Z}^+) \times (\mathbb{Z} \times \mathbb{Z}^+)$, and

$$\sim = \left\{ ((a, b), (c, d)) \in (\mathbb{Z} \times \mathbb{Z}^+)^2 \;\middle|\; \begin{array}{c} a, c \in \mathbb{Z}, b, d \in \mathbb{Z}^+, \\ a \times_{\mathbb{Z}} d = b \times_{\mathbb{Z}} c \end{array} \right\}$$

Define $\mathbb{Q} := \mathbb{Z} \times \mathbb{Z}^+ / \sim$.

Rational Numbers



Rational Numbers

Remark

The relation $\sim$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}^+$.

Proof.

Let $(a, b), (a', b'), (a'', b'') \in \mathbb{Z} \times \mathbb{Z}^+$.

- Reflexivity. Obviously $(a, b) \sim (a, b)$ since $ab = ba$.
- Symmetry. Let $(a, b) \sim (a', b')$, then

$$(a, b) \sim (a', b') \Rightarrow ab' = a'b \Rightarrow a'b = ab' \Rightarrow (a', b') \sim (a, b)$$

- Transitivity. Let $(a, b) \sim (a', b')$ and $(a', b') \sim (a'', b'')$, then we have $ab' = a'b$ and $a'b'' = a''b'$. Thus $ab'a'b'' = a'ba''b'$. Since $b' \neq 0$, then $aa'b'' = a'ba''$.
  - If $a' \neq 0$, then $ab'' = a''b$, i.e., $(a, b) \sim (a'', b'')$.
  - If $a' = 0$, then $ab' = 0$, hence $a = 0$ (b/c $b' \neq 0$). Similarly $a'' = 0$. Therefore $ab'' = 0 = a''b$, i.e., $(a, b) \sim (a'', b'')$. $\square$

Rational Numbers

Well-defined operations on equivalence classes

- $[(a,b)] +_{\mathbb{Q}} [(c,d)] := [(a \times_{\mathbb{Z}} d +_{\mathbb{Z}} b \times_{\mathbb{Z}} c, b \times_{\mathbb{Z}} d)]$.
- $[(a,b)] \times_{\mathbb{Q}} [(c,d)] := [(a \times_{\mathbb{Z}} c, b \times_{\mathbb{Z}} d)]$.
- $[(a,b)] <_{\mathbb{Q}} [(c,d)]$ if $a \times_{\mathbb{Z}} d <_{\mathbb{Z}} b \times_{\mathbb{Z}} c$.

Proof.

Choose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, which indicates that $ab' = a'b$ and $cd' = c'd$, with $b, b', d, d' > 0$.

- We want to show that $(ad+bc, bd) \sim (a'd' + b'c', b'd')$, that is, $(ad+bc)b'd' = bd(a'd' + b'c')$, or $ab'dd' + bb'cd' = a'bdd' + bb'c'd$. Note that this is guranteed by $ab' = a'b$ and $cd' = c'd$.
- Since $ab' = a'b$ and $cd' = c'd$, then $ab'cd' = a'bc'd$, thus $(ac, bd) \sim (a'c', b'd')$.
- $ad < bc \Leftrightarrow adb'd' < bcb'd' \Leftrightarrow a'bdd' < bb'c'd \Leftrightarrow a'd' < b'c'$ (note that $b', d' > 0$). Therefore the ordering $<_{\mathbb{Z}}$ on $\mathbb{Q}$ is well-defined. $\square$

Real Numbers

Definition

A Cauchy sequence is a function $s : \mathbb{N} \to \mathbb{Q}$ such that $|s_m - s_n|$ is arbitrarily small for all sufficiently large m and n; i.e.,

$$(\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0)(\exists k \in \mathbb{N})(\forall m, n > k)(|s_m - s_n| < \varepsilon)$$

Definition

Let C be the set of all Cauchy sequences. For $r, s \in C$, then r and s are ***equivalent*** $(r \sim s)$ if $|r_n - s_n|$ is arbitrarily small for all sufficiently large n; i.e.,

$$(\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0)(\exists k \in \mathbb{N})(\forall n > k)(|r_n - s_n| < \varepsilon)$$

Define $\mathbb{R}$ to be the quotient set $C/\sim$. (This approach to constructing $\mathbb{R}$ is due to Cantor.)

Real Numbers

Definition

A Dedekind cut is a set $x \subset \mathbb{Q}$ such that

- $x \neq \varnothing$ and $x \neq \mathbb{Q}$;
- x is closed downward, i.e., $(\forall p, q \in \mathbb{Q})(p < q \Rightarrow (q \in x \Rightarrow p \in x))$;
- x has no largest element.

Define $\mathbb{R}$ to be the set of all Dedekind cuts.

Definition

Let $x \leq_{\mathbb{R}} y$ if $x \subset y$.

Theorem

Every subset $A \subset \mathbb{R}$ that is bounded above admits a least upper bound.

Proof.

Take $x = \bigcup A$. Claim: x is a Dedekind cut, and $(\forall y \in A)(x \geq y)$. □

Equinumerosity

Definition

A set A is equinumerous to a set B (written $A \approx B$) if there is a bijection from A to B.

Theorem

For any sets A, B, and C:

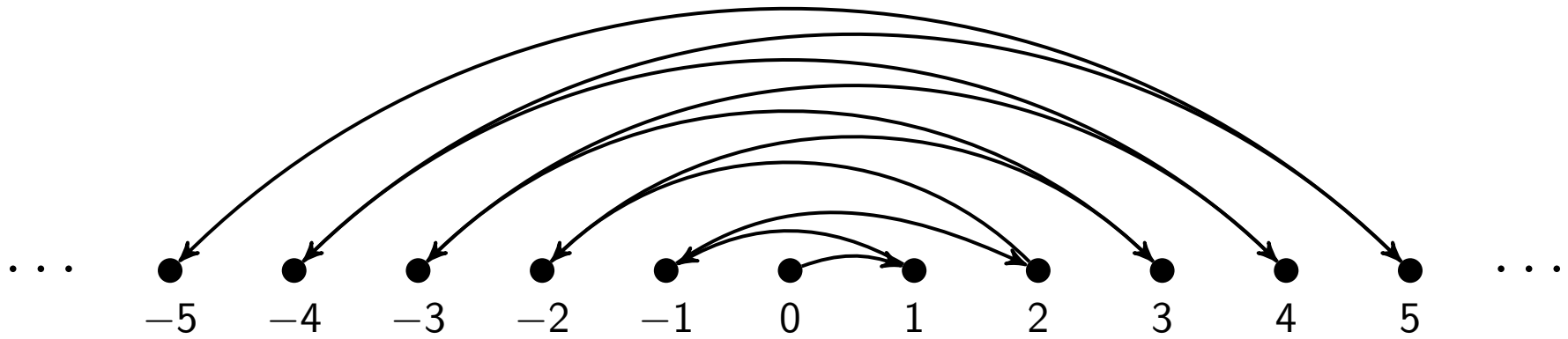
- $A \approx A$.
- $A \approx B \Rightarrow B \approx A$.
- $(A \approx B \wedge B \approx C) \Rightarrow A \approx C$.

Warning

NOT an equivalence relation since the it concerns ***all*** sets.

Equinumerosity

- $\mathbb{Z} \approx \mathbb{N}$.



z	$\cdots$	-5	-4	-3	-2	-1	0	1	2	3	4	5	$\cdots$
$f(z)$	$\cdots$	10	8	6	4	2	0	1	3	5	7	9	$\cdots$

$$f : \mathbb{Z} \to \mathbb{N}$$

$$z \mapsto \begin{cases} 2z - 1, & z > 0 \\ -2z, & z \leq 0 \end{cases}$$

Equinumerosity

- $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$.

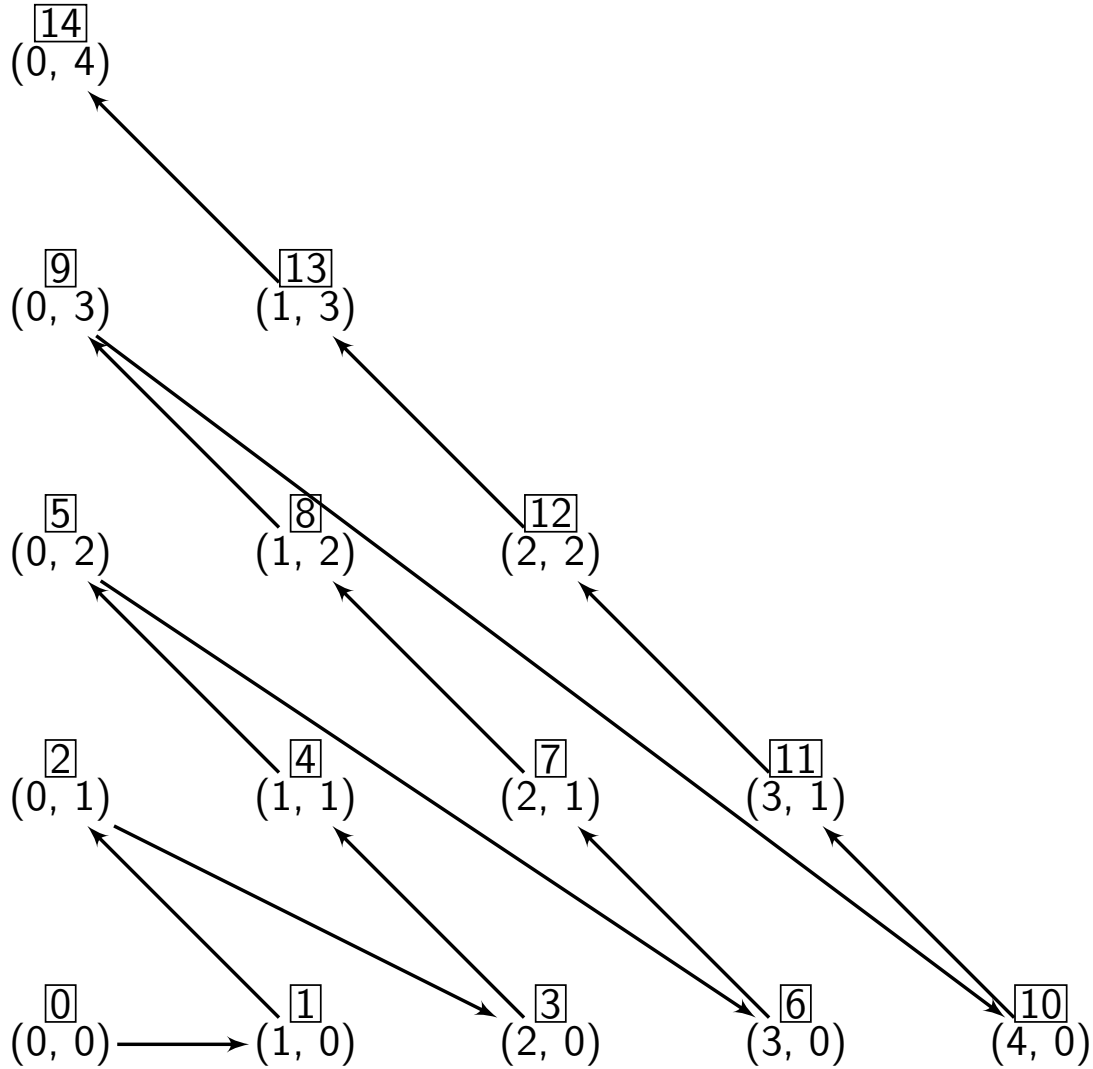
Cantor's Paring Function

$J : \mathbb{N}^2 \to \mathbb{N}$,

$$J(x, y) = \binom{x + y + 1}{2} + y$$

Theorem (Fueter-Pólya)

The only quadratic paring functions are the Cantor polynomials (up to interchanging x and y).



Remark

It is unknown whether this the ***only polynomial*** pairing function.

Pairing Functions Recursively Defined

Consider Cantor's pairing function

$$J(x,y) = \binom{x+y+1}{2} + y, \qquad x,y \in \mathbb{N}$$

We can define it recursively as

$$J(x+1,y) = J(x,y) + x + y + 1$$
$$J(0,y) = \binom{y+1}{2} + y$$

The function $j : \mathbb{N} \to \mathbb{N}^2$ is bijective ($J^{-1} = j$).

A pair $(x,y) \in \mathbb{N}^2$ is either

- $(0,0)$, or
- $(y+1,0)$ as successor of $(0,y)$, or
- $(x-1,y+1)$ as the successor of (x,y) when $x \neq 0$.

Pairing Functions Recursively Defined

Consider another pairing function

$$P(x, y) = 2^x(2y + 1) - 1, \qquad x, y \in \mathbb{N}$$

We can define it recursively as

$$P(x + 1, y) = 2P(x, y) + 1$$
$$P(0, y) = 2y$$

P is bijective

Recall fundamental theorem of arithmetic.

- Surjectivity. For all $z + 1 \in \mathbb{N}$, $z + 1 = 2^x(2y + 1)$ for some $x, y \in \mathbb{N}$.
- Injectivity. Follows from uniqueness of factorization.

Recursively Defined Functions

- When $m \geq 1$, given any two functions $g : \mathbb{N}^m \to \mathbb{N}$ and $h : \mathbb{N} \times \mathbb{N}^m \times \mathbb{N} \to \mathbb{N}$, there exsits a unique function $f : \mathbb{N} \times \mathbb{N}^m \to \mathbb{N}$ defined by

$$f(n+1, x) = h(n, x, f(n, x))$$
$$f(0, x) = g(x)$$

  where $x = (x_1, \ldots, x_m) \in \mathbb{N}^m$.
- When $m = 0$, we have

$$f(n+1) = h(n, f(n))$$
$$f(0) = f_0$$

  for all $n \in \mathbb{N}$, and some fixed $f_0 \in \mathbb{N}$.

Comparing with Differential Equations

- When $m \geq 1$, given any two ***suitable*** functions $g : \mathbb{R}^m \to \mathbb{R}$ and $h : \mathbb{R}^+ \times \mathbb{R}^m \times \mathbb{R} \to \mathbb{R}$, there exists a unique function $u : \mathbb{R}^+ \times \mathbb{R}^m \to \mathbb{R}$ such that

$$\frac{\partial u}{\partial t} = h(t, x, u(t, x))$$
$$u(0, x) = g(x)$$

  where $x = (x_1, \ldots, x_m) \in \mathbb{R}^m$.

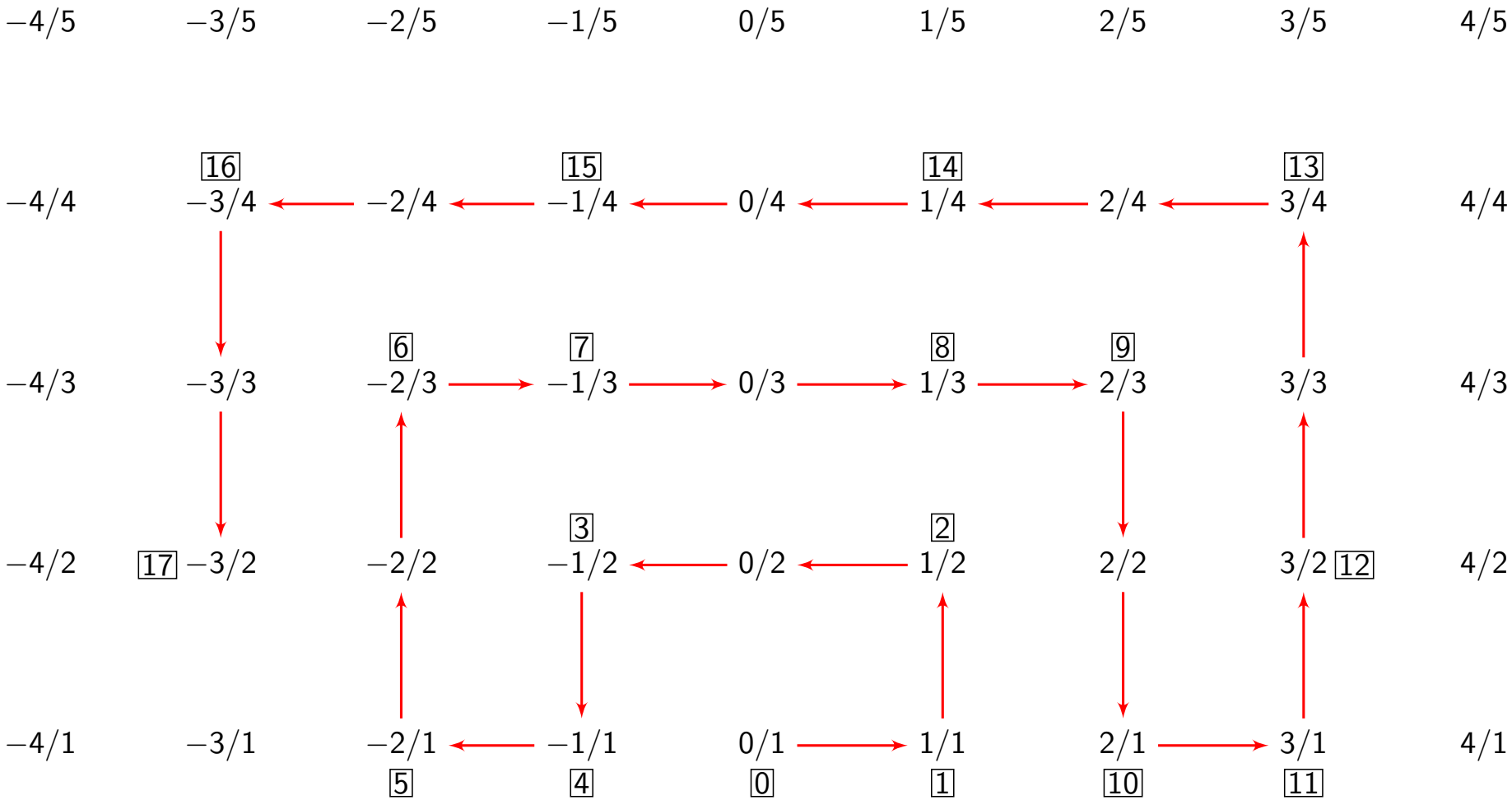
- When $m = 0$, we have

$$\frac{du}{dt} = h(t, u(t))$$
$$u(0) = u_0$$

  for some fixed $u_0 \in \mathbb{R}$.

Equinumerosity

- $\mathbb{Q} \approx \mathbb{N}$.



$\mathbb{Q} \approx \mathbb{N}$

Define $g : \mathbb{N} \to \mathbb{Q}$, such that

$$g(0) = [f(0)]$$
$$g(n+1) = [f(k)] \text{ where } k \text{ is the first such that}$$
$$\forall i \leq n, g(i) \not\sim f(k)$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	$\cdots$
$g(n)$	0	1	2	-2	-1	$-\frac{1}{2}$	$-\frac{3}{2}$	-3	3	$\frac{3}{2}$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{4}{3}$	$\cdots$

Calkin-Wilf-Newman

- $\mathbb{Q}^+ \approx \mathbb{N}$

Moshe Newman successor function

The function

$$x \mapsto \frac{1}{\lfloor x \rfloor + 1 - \{x\}}$$

generates the Calkin-Wilf sequence

$$\frac{1}{1} \to \frac{1}{2} \to \frac{2}{1} \to \frac{1}{3} \to \frac{3}{2} \to \frac{2}{3} \to \frac{3}{1} \to \frac{1}{4} \to \frac{4}{3} \to \cdots$$

which contains every positive rational number exactly once.
(Aigner & Ziegler, p. 131)

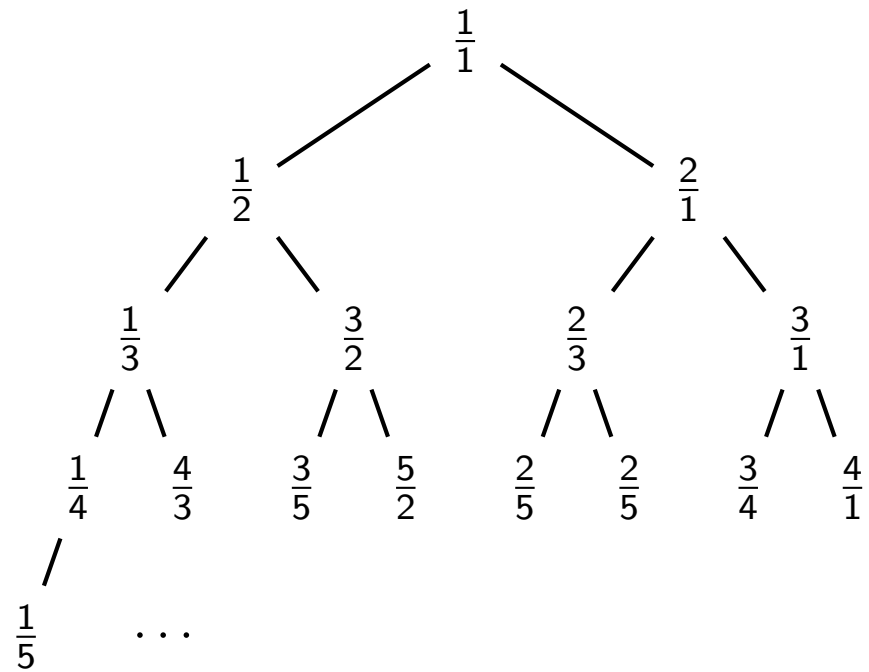
Calkin-Wilf-Newman

Consider the infinite binary tree,

- $\frac{1}{1}$ is the root, and
- every node $\frac{i}{j}$ has a left child $\frac{i}{i+j}$ and a right child $\frac{i+j}{j}$

Properties of the infinite tree:

- All fractions are reduced.
- Every reduced fraction $\frac{r}{s}$ appears in tree.
- Every reduced fraction $\frac{r}{s}$ appears exactly onece.
- The denominator of the n-th fraction in the list equals the numerator of the $(n+1)$-st.



Cantor's Theorem

Theorem

- $\mathbb{R} \not\approx \mathbb{N}$.
- *For every set* A, $A \not\approx \mathcal{P}(A)$.

Proof.

Suppose $\mathbb{R}$ is countable, say

$$
\begin{aligned}
x_1 &= 0.7\,87909\,84732689\cdots \\
x_2 &= 0.2\,34567\,89098765\cdots \\
x_3 &= 0.98\,965\,456756889\cdots \\
x_4 &= 0.237\,89\,237585022\cdots \\
x_5 &= 0.1234\,5\,438765445\cdots \\
&\vdots \\
\text{Consider } x_0 &= 0.84096\cdots?
\end{aligned}
$$

□

Cantor's Theorem

Proof.

Consider $f : A \to \mathcal{P}(A)$, and $B = \{x \in A \mid x \notin f(x)\} \in \mathcal{P}(A)$, e.g.,

$$
\begin{aligned}
f : A &\longrightarrow \mathcal{P}(A) \\
a &\mapsto \{c, d\} \\
b &\mapsto \{e\} \\
c &\mapsto \{b, c, d, e\} \\
d &\mapsto \{\} \\
e &\mapsto A \\
f &\mapsto \{a, c, e, g, \dots\} \\
g &\mapsto \{b, k, m, \dots\} \\
&\vdots \\
B &= \{a, b, d, f, g, \dots\}
\end{aligned}
$$

Cantor's Theorem

Proof.

Claim: f is not onto.

Recall $B = \{x \in A \mid x \notin f(x)\} \in \mathcal{P}(A)$. If f is onto, then $\exists z \in A$ such that $f(z) = B \in \mathcal{P}(A)$, yet

- If $z \in B$, then by definition $z \notin f(z) = B$.
- If $z \notin B$, then by definition $z \in f(z) = B$. □

Also by Cantor

Theorem

The set $\mathbb{R}^2$ of all ordered pairs of real numbers has the same size as $\mathbb{R}$.

Proof. (Julius Kőnig).

It suffices to prove that the set of all pairs (x, y), $0 < x, y \leq 1$, can be mapped bijectively onto $(0, 1]$.
Consider the pair (x, y) and write x, y in their unique non-terminating decimal expansion as in the following example:

$$\begin{array}{lllllllllllllll} x = 0. & 3 & & & 0 & 1 & & 2 & 0 & 0 & 7 & & & 0 & 8 & \cdots \\ y = 0. & 0 & 0 & 9 & & & 2 & & 0 & 5 & & & 1 & & 0 & 0 & 0 & 8 & \cdots \end{array}$$

Now let

$$z = 0.3\ 009\ 01\ 2\ 2\ 05\ 007\ 1\ 08\ 0008\cdots$$

□

(Aigner & Ziegler, p. 133)

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Cardinals

Cardinal Number

For any set A, we will define a set $\operatorname{card} A$ such that

- For any sets A and B,

$$\operatorname{card} A = \operatorname{card} B \Leftrightarrow A \approx B$$

- For a finite set A, $\operatorname{card} A$ is the natural number for which $A \approx n$.

Example

- Each $n \in \mathbb{N}$ is a cardinal, e.g., $\operatorname{card}\{a, b, c, d\} = 4$ since $\operatorname{card}\{a, b, c, d\} \approx 4$.

Cardinality

Cardinality

For every A, there is a unique cardinal κ with $A \approx \kappa$. We call that κ the ***cardinality*** of A, denoted by $\operatorname{card} A = \kappa$.

Example

- $\operatorname{card} n = n$.
- $\operatorname{card} \mathbb{N} = \aleph_0$ (by Cantor).
- $\operatorname{card} \mathbb{R} = 2^{\aleph_0}$.

Caution

$\{X \mid \operatorname{card} X = \kappa\}$ is NOT a set, excpet for $\kappa = 0$.

Ordering Cardinals

Definition

A set A is ***dominated*** by a set B (written $A \preceq B$) if there is an injection from A to B.

Examples

- $A \preceq A$.
- $A \preceq B$ if $A \subset B$. (Consider the inclusion map $\iota : A \hookrightarrow B$.)
- $A \preceq B$ iff A is equinumerous to some subset of B. (Consider a bijection between A and $f(A) \subset B$.)
- $\mathbb{N} \preceq \mathbb{Z} \preceq \mathbb{Q} \preceq \mathbb{R} \preceq \mathbb{C}$.
- $\mathbb{R} \approx (0,1) \preceq [0,1] \preceq \mathcal{P}(\mathbb{N}) \approx 2^{\mathbb{N}} \preceq \mathbb{R}$.

Ordering Cardinals

Definition

We write $\operatorname{card} A \leq \operatorname{card} B$ if $A \preceq B$.

Claim: This ordering is is well-defined.

We need to verify that the definition is independent of the chosen representatives.
Suppose for sets A' and B' with $\operatorname{card} A = \operatorname{card} A'$ and $\operatorname{card} B = \operatorname{card} B'$, then $A \approx A'$ and $B \approx B'$. Now if $A \preceq B$, then there exist

- $\alpha : A' \to A$ bijective;
- $\beta : A \to B$ injective;
- $\gamma : B \to B'$ bijective.

Thus the overall composition $\gamma \circ \beta \circ \alpha : A' \to B'$ is injective, hence $A' \preceq B'$.

Ordering Cardinals

Definition

We write $\operatorname{card} A < \operatorname{card} B$ if $A \preceq B$ and $A \not\approx B$.

Examples

- If $A \subset B$, then $\operatorname{card} A \leq \operatorname{card} B$.
- For all cardinal κ, $0 \leq \kappa$.
- For all finite cardinal n, $n < \aleph_0$.
- If m and n are finite cardinals, then $m \subset n \Rightarrow m \leq n$.
- For all cardinal κ, $\kappa < 2^\kappa$. (There is no largest cardinal number.)

Countable Sets

Definition

A set A is ***countable*** if $A \preceq \mathbb{N}$, i.e., $\operatorname{card} A \leq \aleph_0$. Otherwise, it is called ***uncountable***.

Examples

- $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are countable; $\mathbb{R}$ is uncountable.
- A subset of a countable set is countable.
- The Cartesian product of two countable sets is countable.
- A countable union of countable sets is countable.
- If X is countable and $f : X \to Y$ is onto, then Y is countable.
- For all infinite set A, $\mathcal{P}(A)$ is uncountable.

Cantor-Schröder-Bernstein Theorem

Q: Does the ordering on the cardinals induce a "partial ordering"?
For sets A, B, and C,

- reflexivity: $\operatorname{card} A \leq \operatorname{card} A$, i.e., $A \preceq A$.
- transitivity: $(\operatorname{card} A \leq \operatorname{card} B) \wedge (\operatorname{card} B \leq \operatorname{card} C) \Rightarrow \operatorname{card} A \leq \operatorname{card} C$, i.e.,
  $(A \preceq B) \wedge (B \preceq C) \Rightarrow A \preceq C$.
- antisymmetry:
  $(\operatorname{card} A \leq \operatorname{card} B) \wedge (\operatorname{card} B \leq \operatorname{card} A) \Rightarrow ? \operatorname{card} A = \operatorname{card} B$, i.e.,
  $(A \preceq B) \wedge (B \preceq A) \Rightarrow ? A \approx B$.

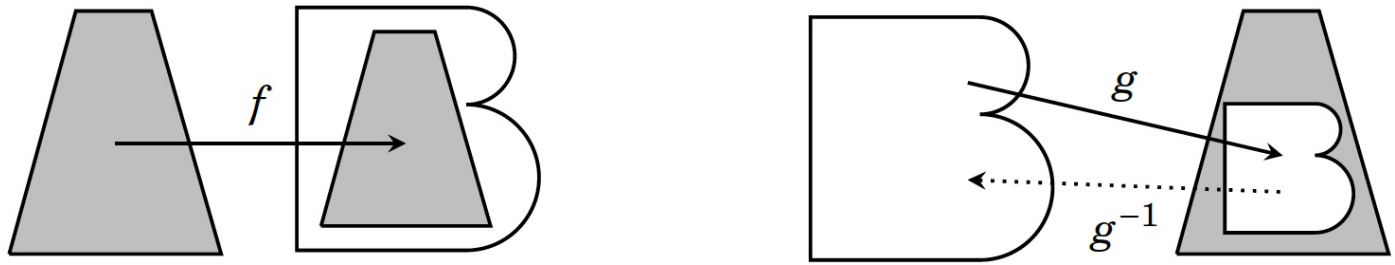
A: Yes.

Theorem (Cantor-Schröder-Bernstein)

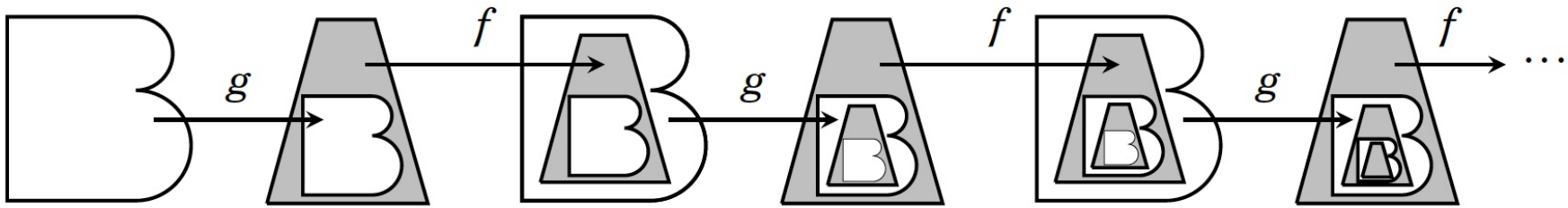
$(\operatorname{card} A \leq \operatorname{card} B) \wedge (\operatorname{card} B \leq \operatorname{card} A) \Rightarrow \operatorname{card} A = \operatorname{card} B$, *i.e.*,
$(A \preceq B) \wedge (B \preceq A) \Rightarrow A \approx B$.

Cantor-Schröder-Bernstein Theorem

Let $f : A \to B$ and $g : B \to A$ be injective.

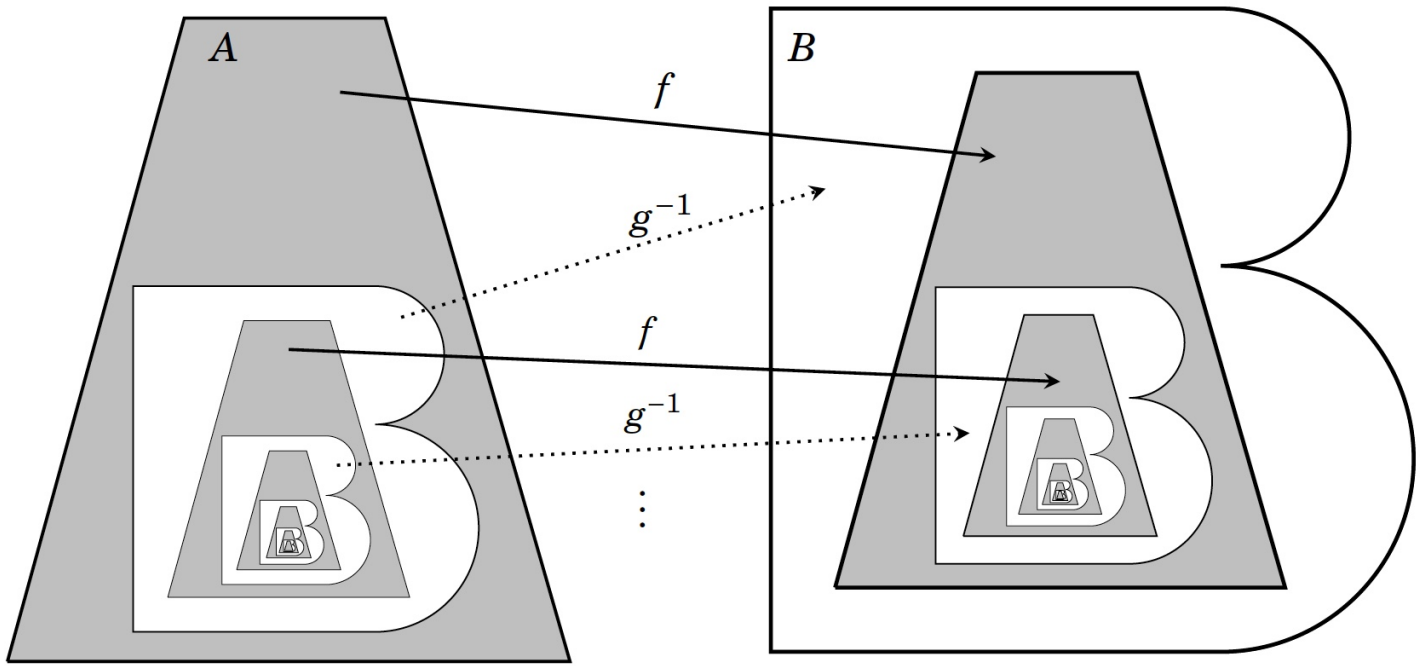


Alternating f and g, we get a chain of injections.



Cantor-Schröder-Bernstein Theorem

Iterate to get a bijection $h : A \to B$.



$$h(x) := \begin{cases} f(x), & x \in \bigcup_{k\in\mathbb{N}} (g \circ f)^k (A - g(B)) \\ g^{-1}(x), & \text{otherwise} \end{cases}$$

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

Finite Sets

For any $n \in \mathbb{N}$, let $[n] \coloneqq \{1, \ldots, n\}$, with $[0] = \varnothing$.

Definition

A set A is ***finite*** if it is equinumerous to $[n]$ for some n. A set is ***infinite*** iff it is not finite.

Example

Any natural number is itself a finite set. Recall that for any $n \in \mathbb{N}$

$$n = \{0, \ldots, n-1\}$$

Theorem (Pigeonhole Principle)

No set of the form $[n]$ *is equinumerous to a proper subset of itself, where* $n \in \mathbb{N}$.

Pigeonhole Principle

Pigeonhole Principle (that we know)

If there are $n + 1$ pigeons in n holes, then some hole contains at least 2 pigeons.

Pigeonhole Principle

Theorem (Pigeonhole Principle)

No set of the form $[n]$ *is equinumerous to a proper subset of itself, where* $n \in \mathbb{N}$.

Proof (Take 1).

Note that any function F is a surjection onto its image $\operatorname{im} F$, we need to show that

$$\nexists f : [n] \to [n](f \text{ injective} \wedge \overbrace{\underbrace{f([n])}_{\operatorname{im} f} \subsetneq [n]}^{f \text{ not surjective}})$$

$$\Leftrightarrow \quad \forall f : [n] \to [n](\neg(f \text{ injective} \wedge \neg(f \text{ surjective})))$$

$$\Leftrightarrow \quad \forall f : [n] \to [n](\neg f \text{ injective} \vee f \text{ surjective})$$

$$\Leftrightarrow \quad \forall f : [n] \to [n](f \text{ injective} \to f \text{ surjective})$$

See (Gallier, p. 133) for the rest of the proof (by induction). □

Pigeonhole Principle

Proof (by induction).

We want to show that for all $m, n \in \mathbb{N}$,

$$m > n \Rightarrow \nexists f : [m] \to [n] \text{ bijective}$$

It suffices to show that for all $m, n \in \mathbb{N}$,

$$m > n \Rightarrow \nexists f : [m] \to [n] \text{ injective}$$

or, for all $m, n \in \mathbb{N}$,

$$m > n \Rightarrow \neg(\exists f : [m] \to [n] \text{ injective})$$

or equivalently, by considering the contrapositive, for all $m, n \in \mathbb{N}$,

$$(\exists f : [m] \to [n] \text{ injective}) \Rightarrow (m \leq n)$$

Pigeonhole Principle

Proof by Induction.

We proceed by induction on n.

- **base case. ($n = 0$):** If $n = 0$, $[0] = \varnothing$. If $f : [m] \to [n]$ is injective, then the only possibility is that $[m] = \varnothing$, hence $m = 0$.
- **inductive case. ($n \geq 1$):** Assume the IH that for all $m \in \mathbb{N}$

$$\exists f : [m] \to [n-1] \text{ injective} \Rightarrow m \leq n-1$$

We want to show that for all $m \in \mathbb{N}$

$$\exists f : [m] \to [n] \text{ injective} \Rightarrow m \leq n$$

Suppose that for all $m \in \mathbb{N}$, there exists an injective $f : [m] \to [n]$,

- If $f(i) < n$ for all $i \in [m]$, then consider $g : [m] \to [n-1], i \mapsto f(i)$, which is also injective. Hence by IH $m \leq n-1 \leq n$.

Pigeonhole Principle

Proof by Induction (Cont.)

- If $n \in f([m])$, say, $f(i_0) = n$ for some $i_0 \in [m]$, $m \neq 0$, then $n \notin f([m] \setminus \{i_0\})$ (since f is injective). Define

$$g : [m-1] \to [n-1]$$
$$i \mapsto \begin{cases} f(i), & i < i_0 \\ f(i+1), & i \geq i_0 \end{cases}$$

  which is also injective, since for $i, j \in [m-1]$,
  - $i, j < i_0$. $g(i) = g(j) \Rightarrow f(i) = f(j) \Rightarrow i = j$;
  - $i, j \geq i_0$. $g(i) = g(j) \Rightarrow f(i+1) = f(j+1) \Rightarrow i = j$;
  - $i < i_0 \leq j$. $g(i) = g(j) \Rightarrow f(i) = f(j+1) \Rightarrow i = j+1 \Rightarrow i > j$. Impossible!
  - $j < i_0 \leq i$. Also impossible.

  Therefore by IH $m - 1 \leq n - 1$, hence $m \leq n$. □

Pigeonhole Principle

Proof by Induction.

We proceed by induction on m.

- **base case. ($m = 0$):** If $m = 0$, $[0] = \varnothing$. Since $f : \varnothing \to [n]$ is injective for all $n \in \mathbb{N}$, then trivially $m \leq n$.
- **inductive case. ($m \geq 1$):** Assume the IH that for all $n \in \mathbb{N}$,

$$\exists f : [m-1] \to [n] \text{ injective} \Rightarrow m - 1 \leq n$$

We want to show that for all $n \in \mathbb{N}$

$$\exists f : [m] \to [n] \text{ injective} \Rightarrow m \leq n$$

Suppose that for all $m \in \mathbb{N}$, there exists an injective $f : [m] \to [n]$,

- If $f(i) < n$ for all $i \in [m]$, define $g : [m-1] \to [n-1]$ as $g = f|[m-1]$. Then g is also injective, hence $m - 1 \leq n - 1$, and $m \leq n$.

Pigeonhole Principle

Proof by Induction (Cont.)

- If $f(i_0) = n$ for some $i_0 \in [m]$, thus $f([m] \setminus \{i_0\}) \subset [n-1]$ (since for any other $i \neq i_0$, $f(i) \neq f(i_0) = k$). Define

$$g : [m-1] \to [n-1]$$
$$i \mapsto \begin{cases} f(i), & i \neq i_0 \\ f(m), & i = i_0 \end{cases}$$

  then g is also injective, since
  - If $i, j \neq i_0$, then $g(i) = g(j) \Rightarrow f(i) = f(j) \Rightarrow i = j$.
  - If $i \neq i_0$, then $g(i) = f(i) \neq f(m) = g(i_0)$ (since $i < m \Rightarrow f(i) \neq f(m)$).

  Therefore by IH $m - 1 \leq n - 1$, hence $m \leq n$. □

Finite Sets

Caveat

Given function $f : A \to B$,

- If $A = \varnothing$, then any function, $f : \varnothing \to B$ is (trivially) injective.
- If $B = \varnothing$, then f is the ***empty function*** from $\varnothing$ to itself, and is (trivially) surjective, hence also bijective.

Corollary

- *No finite set is equinumerous to a proper subset of itself.*
- $\mathbb{N}$ *is infinite.*
- *Every finite set is equinumerous to a unique natural number.*
- *Any subset of a finite subset is finite.*

Finite Sets

Corollary (Pigeonhole Principle for Finite Sets)

No finite set is equinumerous to a proper subset of itself.

Proof.

Since A is finite, then there exists a bijection $g : A \to [n]$ for some $n \in \mathbb{N}$. Assume that there exists a bijection f between A and some proper subset of A. Then, consider the function $g \circ f \circ g^{-1}$, from $[n]$ to itself.

$$\begin{array}{ccc} A & \xleftarrow{g^{-1}} & [n] \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle g\circ f\circ g^{-1}} \\ A & \xrightarrow[g]{} & [n] \end{array}$$

Then, note that $g(a) \in [n] \setminus \operatorname{ran} g \circ f \circ g^{-1}$ for some $a \in A \setminus \operatorname{ran} f$, therefore $g \circ f \circ g^{-1}$ is a bijection from $[n]$ to some proper subset of itself, which is a contradiction. $\square$

Finite Sets

Corollary

Given non-empty finite sets A, B, if there exists an injection $f : A \to B$, then $|A| \leq |B|$

Corollary

Suppose that $f : A \to [n]$ is an injection, then A is a finite set and $|A| \leq n$.

Corollary

Given a finite set A and a surjective function $f : A \to B$, then $|B| \leq |A|$.

Corollary

Given a finite set A and a function $f : A \to B$, then $|f(A)| \leq |A|$.

Pigeonhole Principle

Other versions of pigeonhole principle

Let $r, s \in \mathbb{N} - \{0\}$, if a set containing at least $rs + 1$ elements is partitioned into r subsets, then some subsets contains at least $s + 1$ elements.

Example

- In any group of $12 \cdot 2 + 1 = 25$ people, at least three were born in the same month.
- At least two people in London have the same number of hairs on their heads.

Application of Pigeonhole Principle

Example

Let $S \subset \{1, 2, \ldots, 200\}$ with $|S| = 101$, then S contains two consecutive integers.

Proof.

Consider the following sets,

$$\begin{aligned} S_1 &= \{1, 2\} \\ S_2 &= \{3, 4\} \\ &\vdots \\ S_{99} &= \{197, 198\} \\ S_{100} &= \{199, 200\} \end{aligned}$$

The rest follows by applying the Pigeonhole principle. □

Application of Pigeonhole Principle

Example

Let $S \subset \{1, 2, \ldots, 200\}$ with $|S| = 101$, then S contains two integers that one divides the other.

Proof.

Consider the following sets,

$$
\begin{aligned}
S_1 &= \{1, 2, 4, 8, \ldots, 64, 128\} = \{1, 2, 2^2, 2^3, \ldots, 2^7\} \\
S_3 &= \{3, 6, 12, 24, \ldots, 96, 192\} = \{3, 3 \cdot 2, 3 \cdot 2^2, 3 \cdot 2^3, \ldots, 3 \cdot 2^6\} \\
S_5 &= \{5, 10, 20, 40, 80, 160\} = \{5, 5 \cdot 2, 5 \cdot 2^2, 5 \cdot 2^3, 5 \cdot 2^4, 5 \cdot 2^5\} \\
&\vdots \\
S_{49} &= \{49, 98, 196\} = \{49, 49 \cdot 2, 49 \cdot 2^2\} \\
&\vdots \\
S_{99} &= \{99, 198\} = \{99, 99 \cdot 2\} \\
S_{101} &= \{101\}, \ldots, S_{199} = \{199\}
\end{aligned}
$$

The rest follows by applying the Pigeonhole principle. □

Erdős–Szekeres Theorem

Theorem (Erdős–Szekeres, 1935)

Let $A = (a_1, ..., a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of $s + 1$ terms or a decreasing subsequence of $r + 1$ terms (or both).

"The slickest and most systematic" proof (Seidenberg 1959).

Proof.

Define a function $f : \mathbb{R} \to \{1, \ldots, n\}^2$, $a_i \mapsto (x_i, y_i)$, where

- x_i is the number of terms in the longest increasing subsequence ending at a_i,
- y_i is the number of terms in the longest decreasing subsequence starting at a_i.

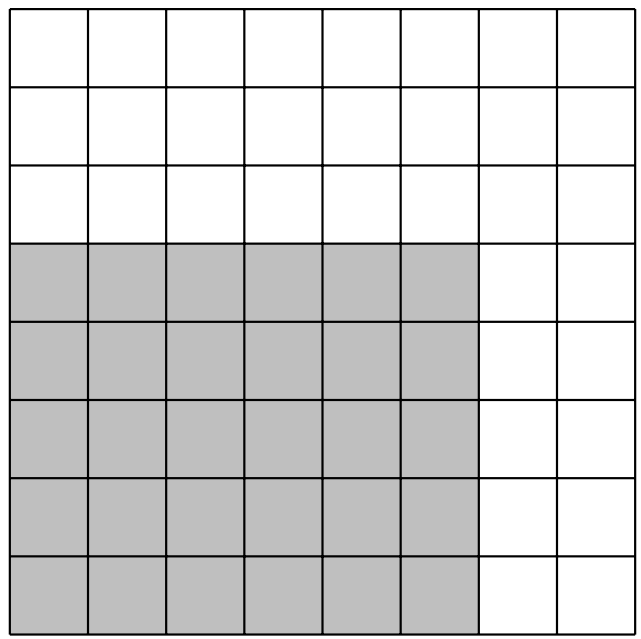
Erdős–Szekeres Theorem

Proof. (Cont.)

Claim: The mapping $a_i \mapsto (x_i, y_i)$ is injective, i.e., $\forall i, j \in \{1, \ldots, n\}$, $a_i \neq a_j \Rightarrow (x_i, y_i) \neq (x_j, y_j)$.
Indeed, for a subsequence $\cdots a_i \cdots a_j \cdots$, either

- $a_i < a_j \Rightarrow x_i < x_j$, or
- $a_i > a_j \Rightarrow y_i > y_j$,

The rest follows by Pigeonhole principle. □



300. Longest Increasing Subsequence[2]

Given an integer array `nums`, return the length of the longest strictly increasing subsequence.
A subsequence is a sequence that can be derived from an array by deleting some or no elements without changing the order of the remaining elements. For example, $[3, 6, 2, 7]$ is a subsequence of the array $[0, 3, 1, 6, 2, 2, 7]$.

Example 1

- **Input:** nums $= [10, 9, 2, 5, 3, 7, 101, 18]$
- **Output:** 4
- **Explanation:** The longest increasing subsequence is $[2, 3, 7, 101]$, therefore the length is 4.

Example 2

- **Input:** nums $= [0,1,0,3,2,3]$
- **Output:** 4

Example 3

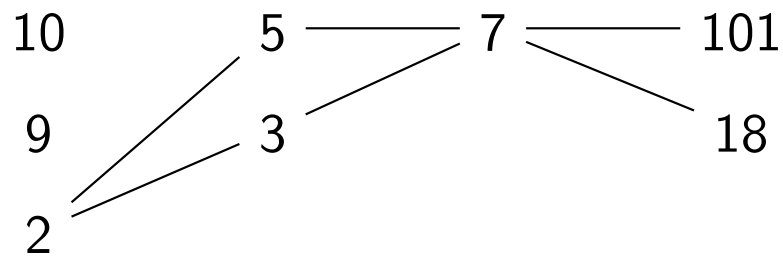
- **Input:** nums $= [7,7,7,7,7,7,7]$
- **Output:** 1

2. `https://leetcode.com/problems/longest-increasing-subsequence/`

300. Longest Increasing Subsequence

Example 1 (Patience Sort)

- **Input:** nums $= [10, 9, 2, 5, 3, 7, 101, 18]$
- **Output:** 4
- **Explanation:** A longest increasing subsequence is $[2, 3, 7, 101]$, therefore the length is 4.



Observation

- Each column is a decreasing subsequence.
- The length of any increasing subsequence is at most the number of columns (pigeonhole principle).

Table of Contents

1. Sets (Naive)

2. Logic

3. Induction

4. Relations and Functions

5. Numbers and Equinumerosity

6. Cardinality

7. Finite Sets and Pigeonhole Principle

8. Partial Order

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 $\prec$)

Definition

If $(P, \leq)$ is a poset, and for all $x, y \in P$, either $x \leq y$ or $y \leq x$, then it is a ***total order*** or ***linear order***.

Example of linear/total order

- $\mathbb{Z}$
- $\mathbb{Q}$
- $\mathbb{N}$
- $\mathbb{R}$

Partial Order

Pre-order/Quasi-order

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

Partial Order

- antisymmetric: $a \leq b \wedge b \leq a \Rightarrow a = b$

Total Order

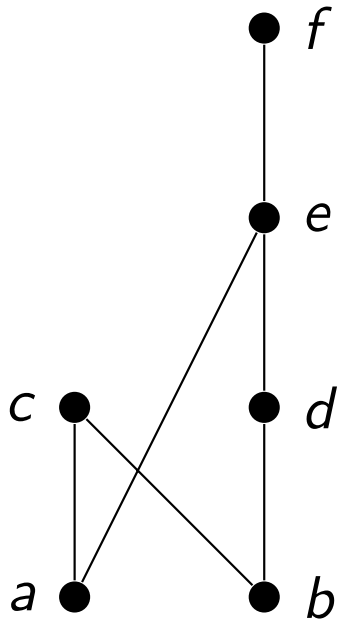
- total: $a \leq b \vee b \leq a \Rightarrow \top$

Hasse Diagram

Hasse/Order Diagram (Idea: keep the most essential component.)

- 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.

Example

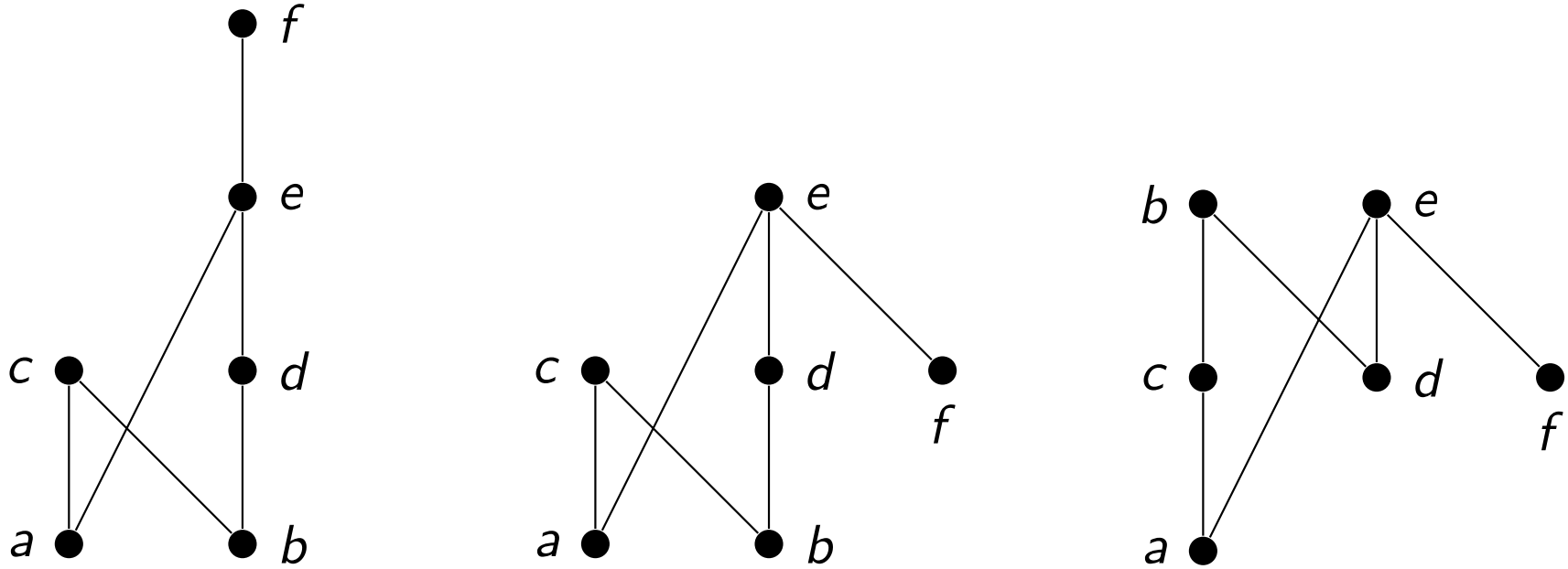


What relation does the Hasse diagram on the left corresponds to?

$$\begin{aligned}\leq = \{&(a,a),(b,b),(c,c),(d,d),(e,e),(f,f),\\ &(a,e),(a,f),(b,d),(b,e),(b,f),(b,c),\\ &(d,e),(d,f),(a,c),(e,f)\}\end{aligned}$$

Hasse Diagrams of Three Different Posets

Example

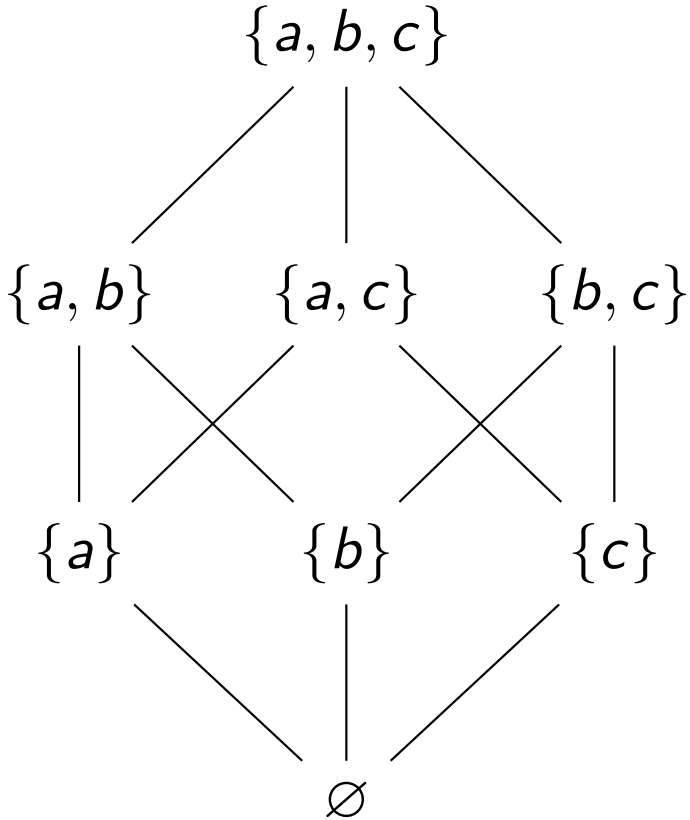


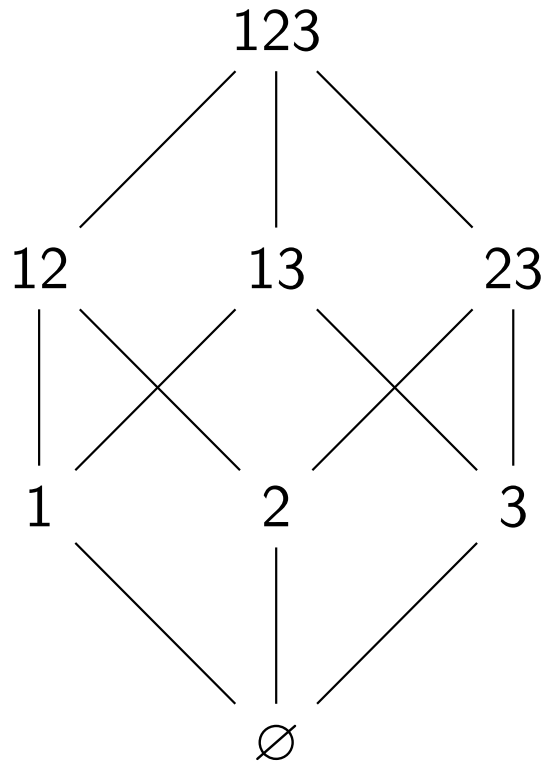
Note that all three are the same as graphs, but not as posets.

Partial Order

Examples

- Power set/Boolean lattice $(\mathbf{2}^{[n]}, \subseteq)$. $[n] = \{1, \ldots, n\}$, subsets of $[n]$ ordered by inclusion.

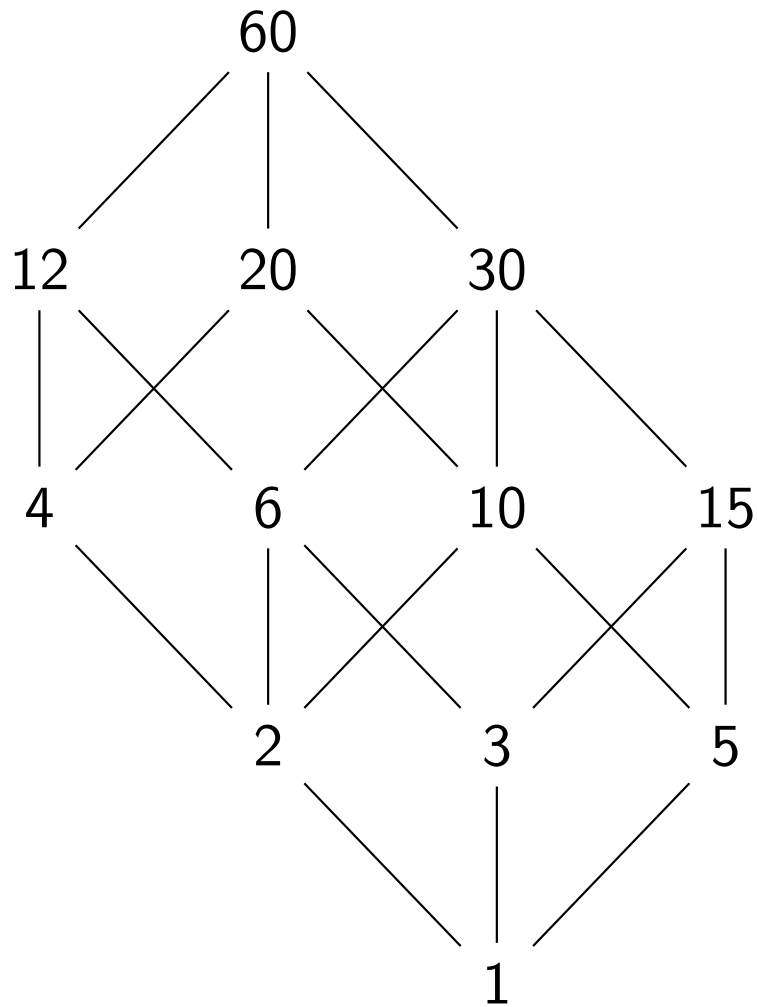




Partial Order

Examples

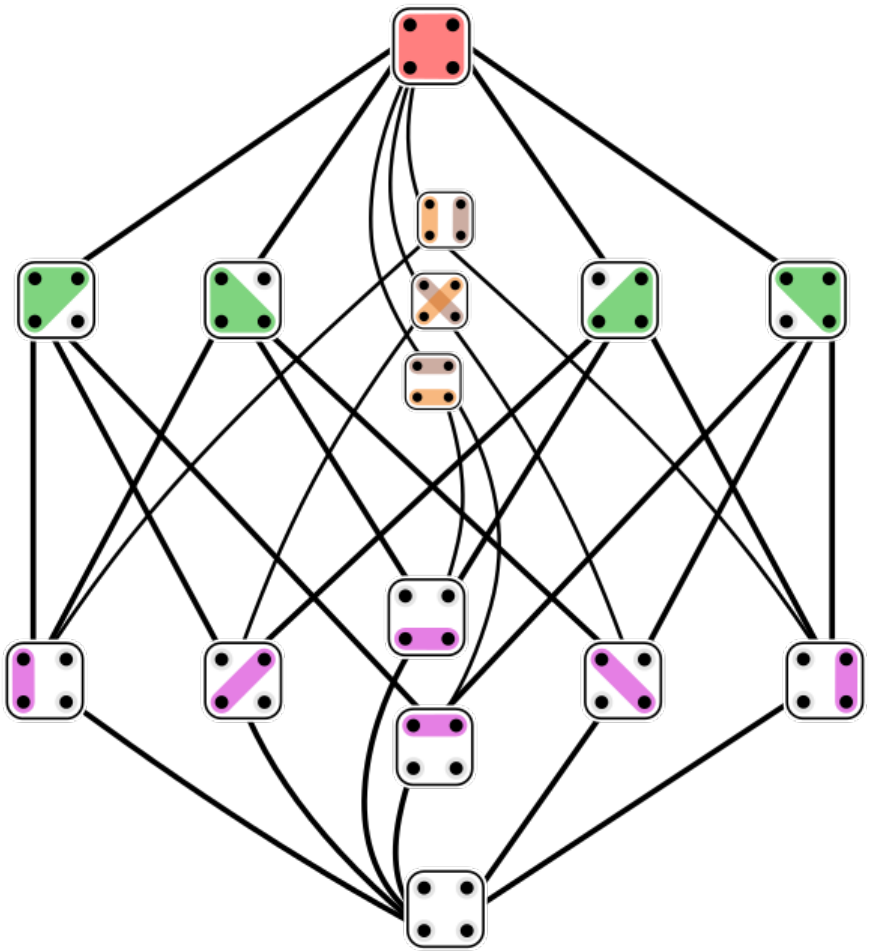
- Divisors of $n \in \mathbb{N}$. $(\mathbb{N}, |)$. Ordered by divisibility. $n = 60$.



Partial Order

Examples

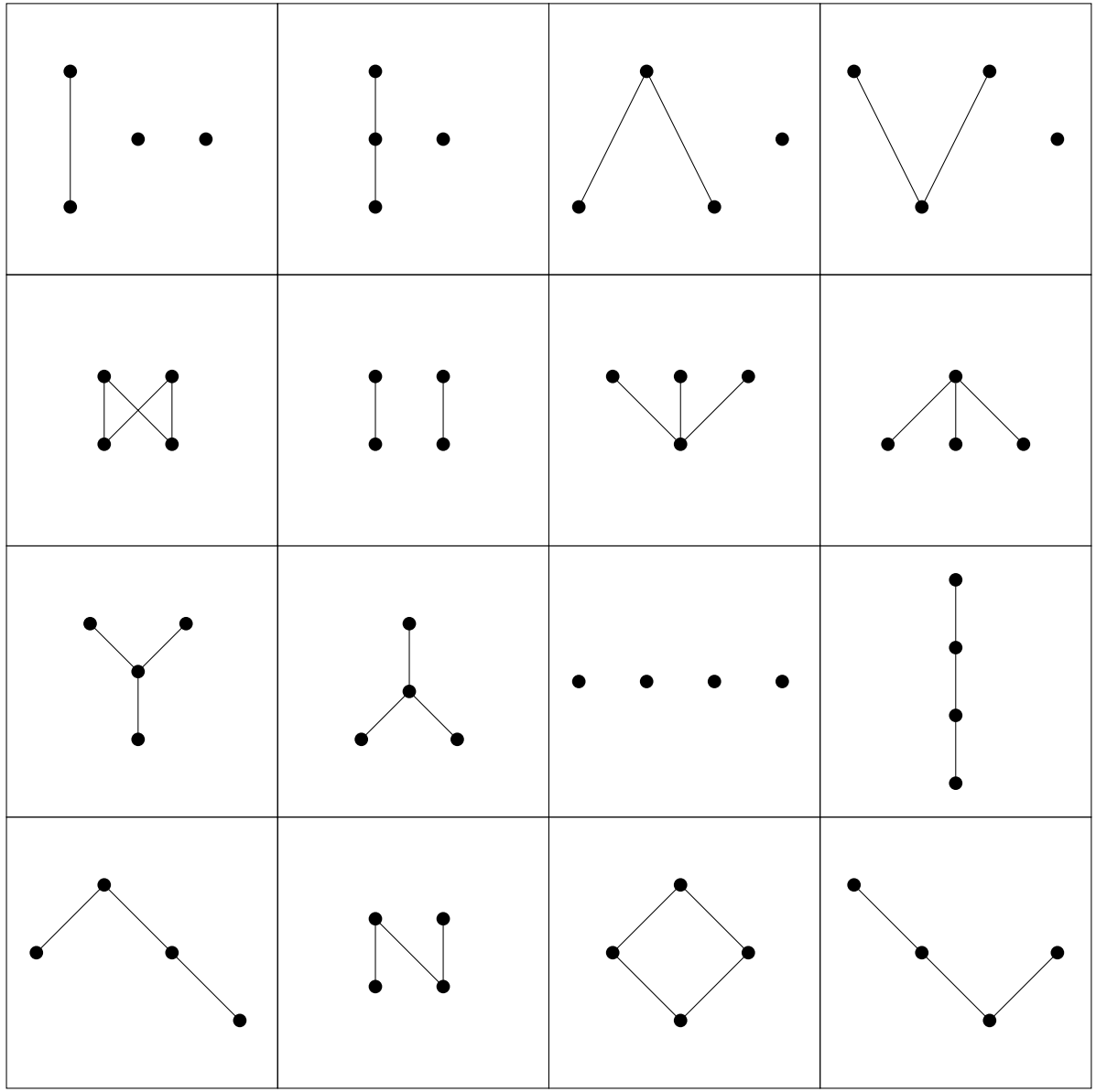
- Partition of $[n] = \{1, \ldots, n\}$, ordered by refinement.



Partial Order

Examples

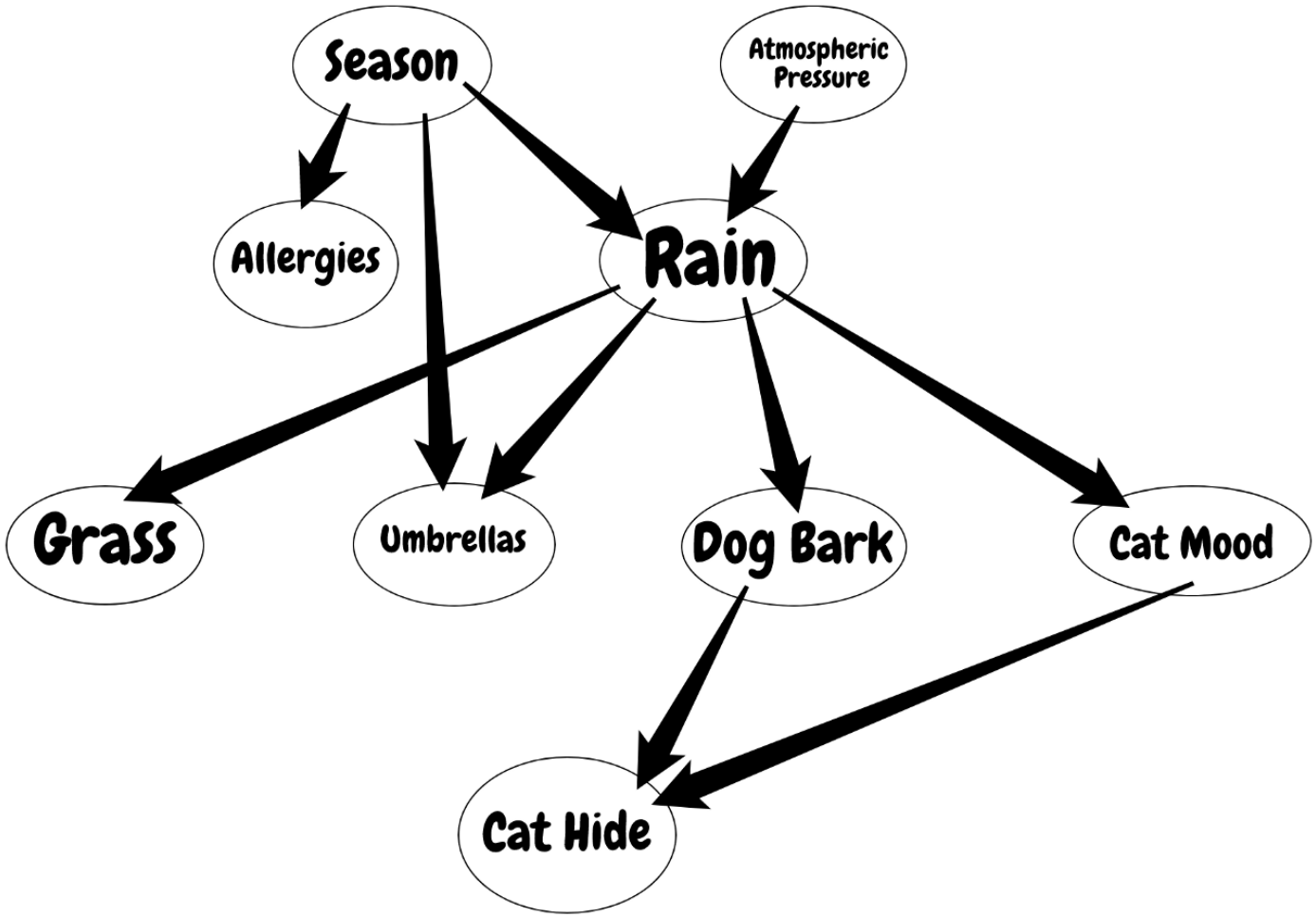
- All posets on a set with 4 elements (up to relabeling of the points).



Partial Order

Examples

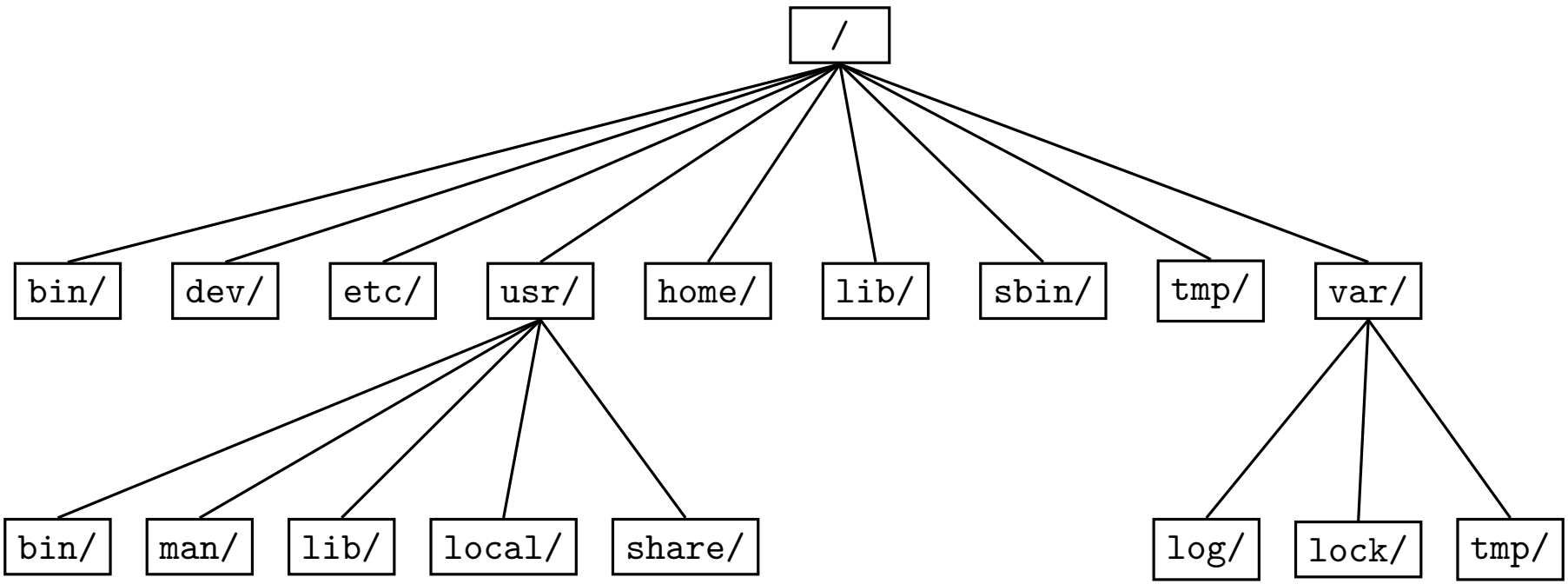
- Any directed acyclic graph (DAG), e.g., Bayesian network.



Partial Order

Examples

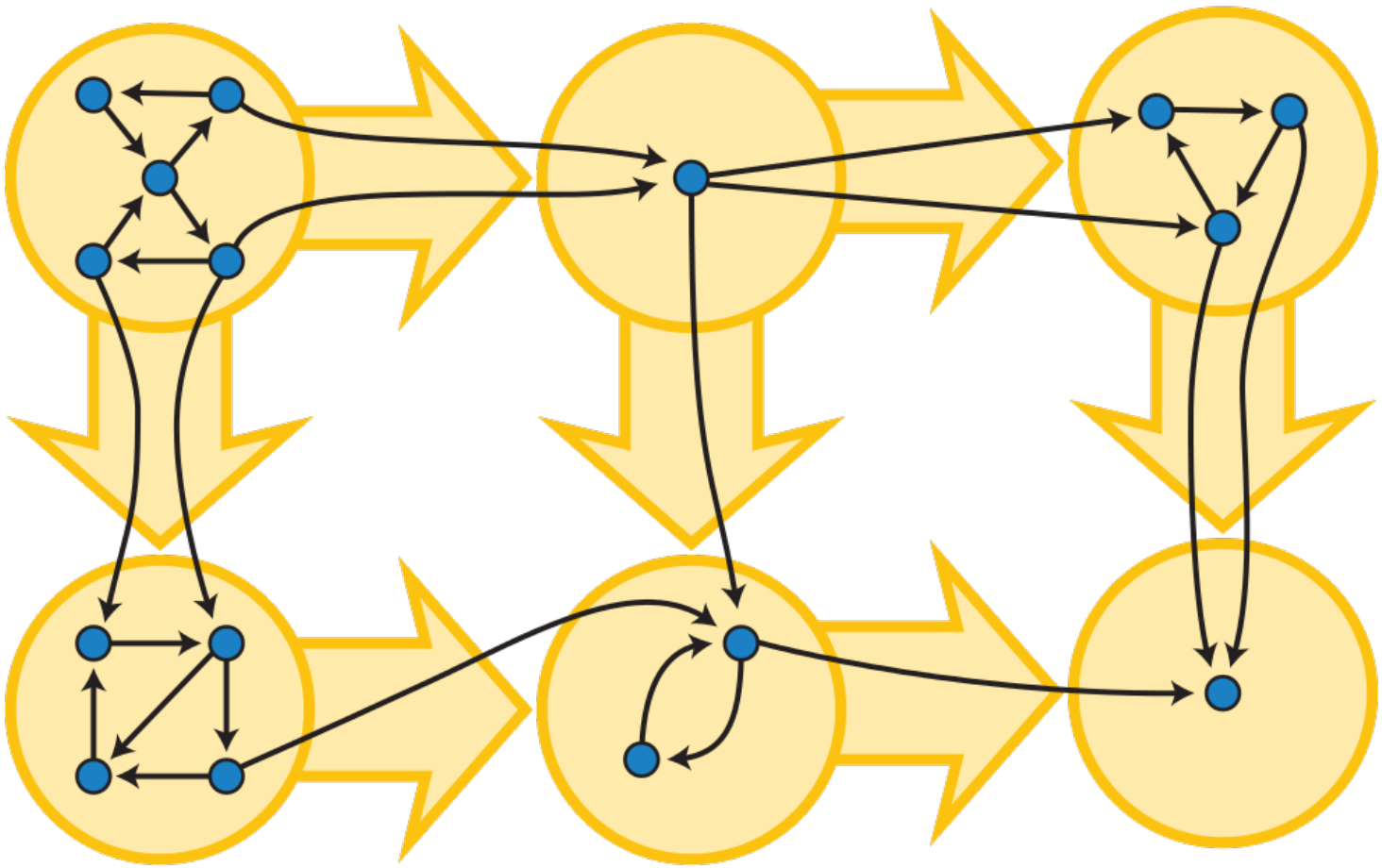
- Vertices in a rooted tree (e.g., computer directory structure, family tree).



Partial Order

Examples

- Strongly connected components in a directed graph. (cf., preorder)



Partial Order

Examples

- sub-trees/graphs/groups/vector spaces of a trees/graphs/groups/vector spaces.

Non-example

- $(\mathbb{Z}, |)$. $-1|1$ and $1|-1$, but $1 \neq -1$.

Covers in a Poset

Definition

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***.

Examples

- In $(\mathcal{P}([6]), \subseteq)$, $\{1, 3\}$ is covered by $\{1, 3, 5\}$, but not covered by $\{1, 2, 3, 4\}$.
- In $\mathbb{Z}$, each $k \in \mathbb{Z}$ is covered by $k + 1$, and covers $k - 1$.
- In $(\mathbb{N}, |)$, 15 is covered by 105, 14 is not covered by 84.
- In $\mathbb{R}$ and $\mathbb{Q}$, no two elements are covers of each other.

More Definitions

Definition

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***.

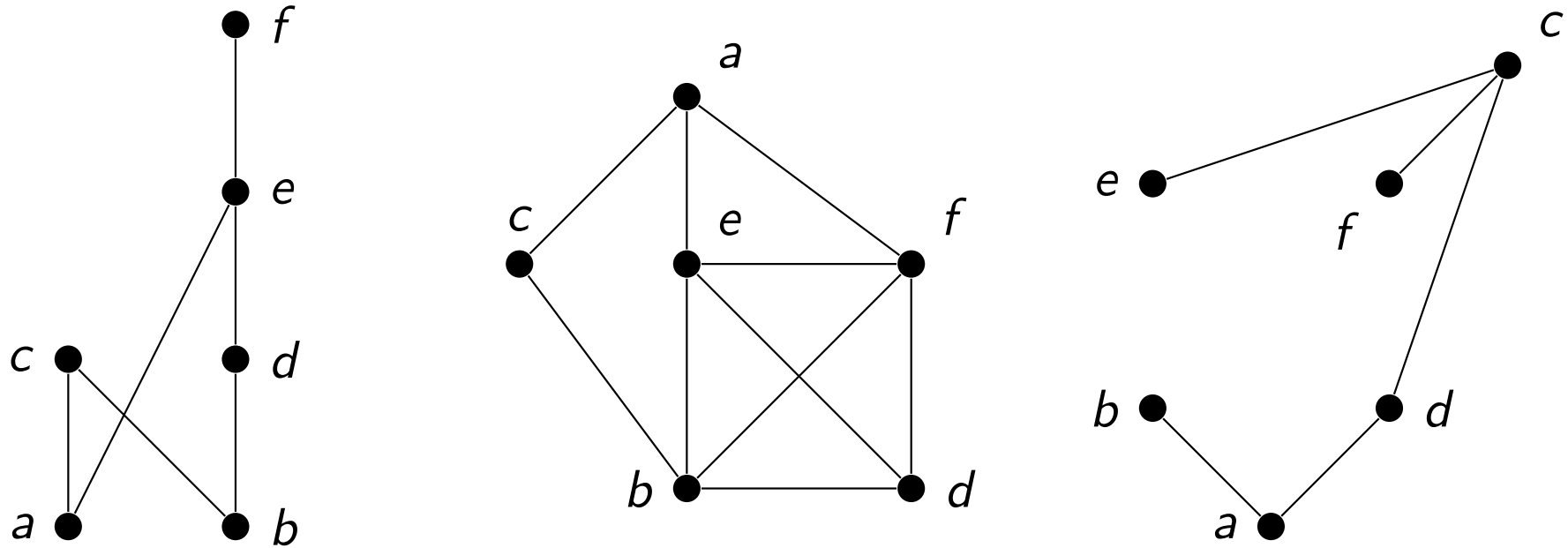
Definition

Given a poset $(P, \leq_P)$ and $Q \subset P$, then the (binary) relation $\leq_Q = \leq_P|_{Q \times Q}$ is a partial order on Q. The induced poset $(Q, \leq_Q)$ is called ***subposet*** of $(P, \leq_P)$.

Comparability and Incomparability Graphs

With a poset $(P, \leq)$, we associate a ***comparability graph*** $G_1 = (P, E_1)$ and an ***incomparability graph*** $G_2 = (P, E_2)$, where
$E_1 = \{\{x, y\} \in \binom{P}{2} \mid x, y \text{ comparable}\}$ and
$E_2 = \{\{x, y\} \in \binom{P}{2} \mid x, y \text{ incomparable}\}$.

Example

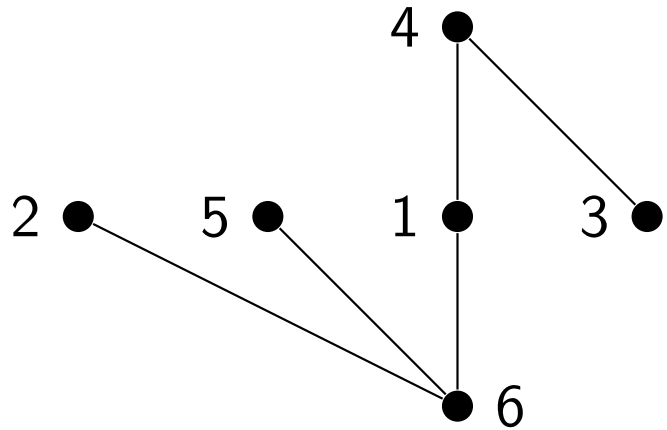


Note that a comparability graph and an incomparability graph are complement graph of each other. The ***complement*** of graph $G = (V, E)$ is $\overline{G} = \left(V, \binom{V}{2} - E\right)$.

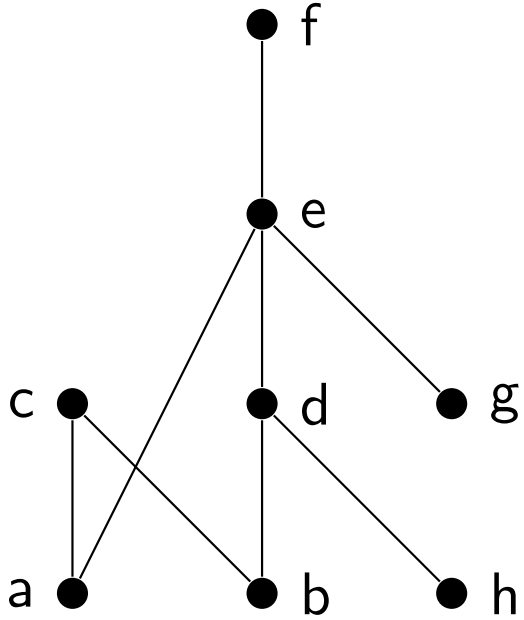
An Example

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.



Another Example



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

Chains and Antichains

Definition

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.

Definition

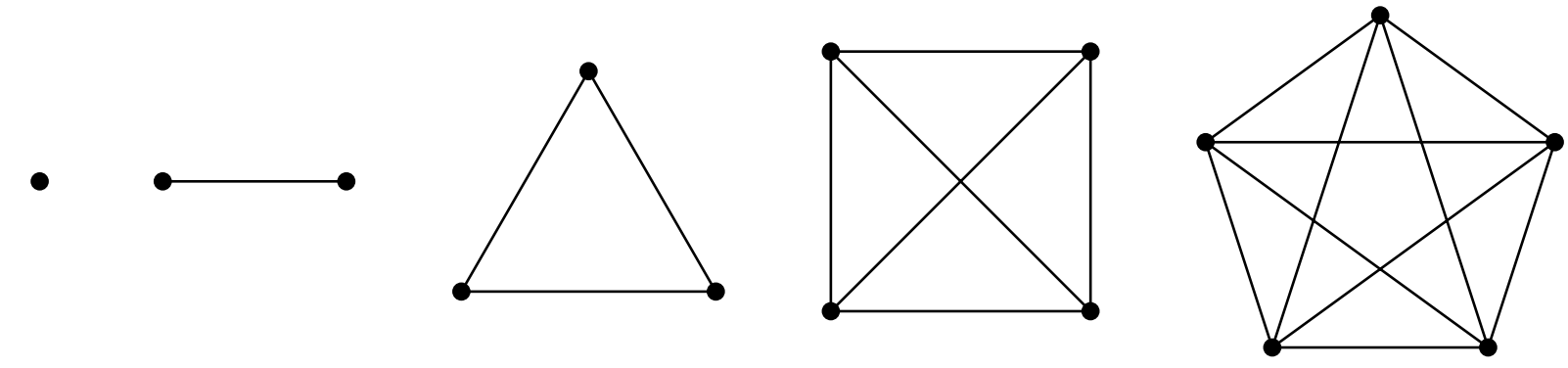
A graph $G = (V, E)$ is called a ***clique*** or ***complete graph*** if $E = \binom{V}{2}$.
Conversely, the complement graph of $G = (V, \binom{V}{2})$, given by $\overline{G} = (V, \varnothing)$, is called an ***independent graph*** or ***independent set***.

Remark

- The comparability graph of a chain is a complete graph.
- The comparability graph of an antichain is an independent graph.

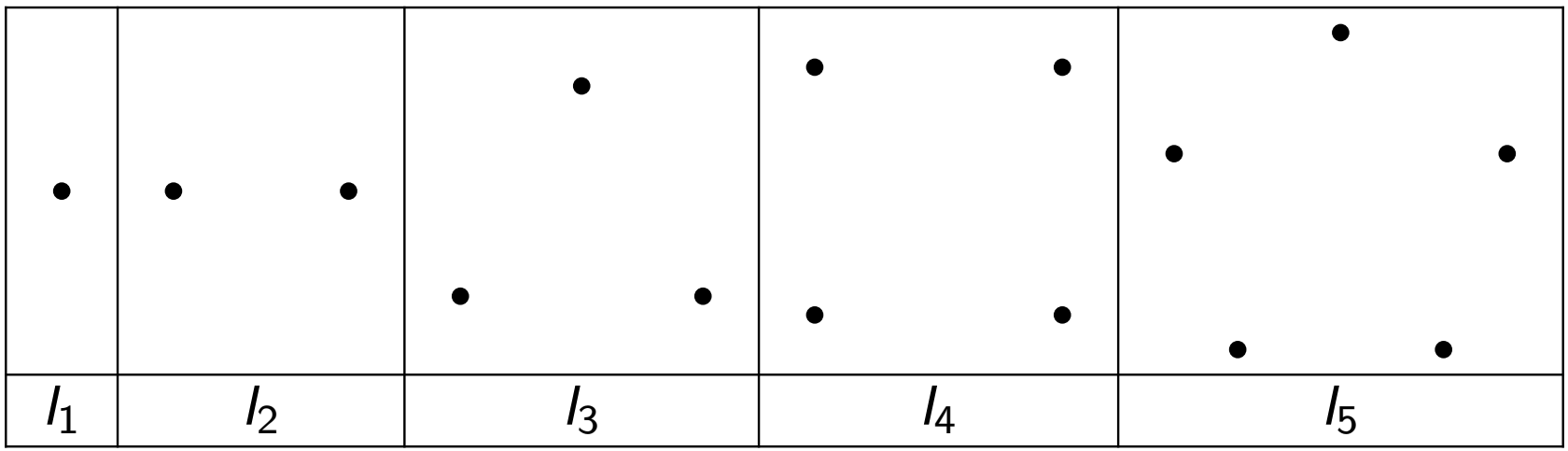
Complete Graphs and Independent Graphs

Complete Graphs K_n



K_1 K_2 K_3 K_4 K_5

Independent Graphs I_n



I_1 I_2 I_3 I_4 I_5

Chains and Antichains

Lemma

Given a chain C and an antichain A of a poset, $|A \cap C| \leq 1$.

Proof.

If $|A \cap C| \geq 2$, then we can find two elements that are both comparable and incomparable. Contradiction. $\square$

Chains and Antichains

Definition

A chain C in P is

- ***maximal*** if there exists no chain C' such that $C \subsetneq C'$.
- ***maximum*** if for all chain C', $|C| \not< |C'|$.

The ***height*** (not *length*) of a poset P, denoted by $h(P)$, is the maximum size of a chain in P.

Definition

An antichain A in P is

- ***maximal*** if there exists no antichain A' such that $A \subsetneq A'$.
- ***maximum*** if for all chain A', $|A| \not< |A'|$.

The ***width*** of a poset P, denoted by $w(P)$, is the maximum size of an antichain in P.

Remark

A maximal chain or maximal antichain CANNOT be prolonged by adding a new element.

Chains and Antichains

Observation

By pigeonhole principle,

- If P can be partitioned into t antichains, then the height of P is at most t.
- If P can be partitioned into s chains, then the width of P is at most s.

Observation

The set of maximal (or minimal) elements is an antichain.

Theorem (Mirsky's Theorem, 1971)

A poset of height h can be partitioned into h antichains.

Proof.

Recursively remove the set of maximal (or minimal) elements. □

Mirsky's Theorem (dual Dilworth)

Proof. (a little more detail).

Denote the set of minimal elements of $(P, \leq)$ by $\mathrm{Min}(P)$. Similarly for $\mathrm{Max}(P)$. Thus we have a partition of P into antichains $A_1, \ldots, A_k$, $k \in \mathbb{N}$. Since $|A_i \cap C| \leq 1$ for any chain $C \subset P$, then (recall observation)

$$\begin{aligned} k &\geq \max\{|C| : C \text{ is a chain in } P\} \\ &= h(P) \end{aligned}$$

Input: A partition order $(P, \leq)$
Output: An antichain partition of $(P, \leq)$

```
1 i ← 1
2 while P ≠ ∅ do
3 |   A_i ← Min(P)
4 |   P ← P − A_i
5 |   i ← i + 1
6 end
7 return {A_1, ..., A_{i−1}}
```

Claim: a chain of length k can be traced back from A_k.
Indeed, choose $x_k \in A_k$, then $\exists x_{k-1} \in A_{k-1}$ such that $x_{k-1} < x_k$, and so on. Eventually, we have $x_1 < x_2 < \cdots < x_{k-1} < x_k$. Therefore $h(P) = k$. □

Dilworth's Theorem

Theorem (Dilworth's Theorem, 1950)

A poset of width w can be partitioned into w chains.

Remark

Dilworth theorem holds if the size of the poset is infinite, however, the width w needs to be finite, i.e., $w \in \mathbb{N}$.

Dilworth's Theorem

Proof. (Perles, 1963).

We use induction on the size of the poset P.

- True when $|P| = 1$.
- Assume the theorem is true when $|P| \leq k$, then consider a poset P with $|P| = k + 1$, then for each maximal antichain A, define the downset of A

$$D(A) := \{x \mid x < a \text{ for some } a \in A\}$$

and the upset of A

$$U(A) := \{x \mid x > a \text{ for some } a \in A\}$$

Dilworth's Theorem

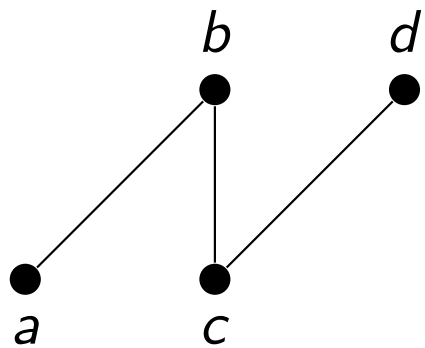
Proof (Cont.)

Case I. Assume there exists a maximum antichain A with $D(A) \neq \varnothing$ and $U(A) \neq \varnothing$.
Claim: $\{A, D(A), U(A)\}$ form a partition of P.
It suffices to show that $D(A) \cap U(A) = \varnothing$. Indeed, otherwise let $x \in D(A) \cap U(A)$, then $\exists y \in A$ with $x < y$, and $\exists z \in A$ with $z < x$, resulting $y, z \in A$ comparable, contradiction.
Let $A = \{a_1, \ldots, a_w\}$, note that $|A \cup D(A)| \leq k$ and $|A \cup U(A)| \leq k$, thus by induction hypothesis, we obtain a chain partition $\{D_1, \ldots, D_w\}$ of $A \cup D(A)$ with maximal elements $a_1, \ldots, a_w$.
Similarly we can obtain a chain partition $\{U_1, \ldots, U_w\}$ of $A \cup U(A)$ with minimal elements $a_1, \ldots, a_w$.
Glue the chains resepctively, we have a chain partition $\{D_1 \cup U_1, \ldots, D_w \cup U_w\}$ of P.

Dilworth's Theorem

Proof (Cont.)

Case II. Otherwise for every maximum antichain A, either $D(A)$ or $U(A)$ is empty. (Or equivalently, either $D(A) \cup A = P$ or $U(A) \cup A = P$ for every maximum antichain A). Hence each maximum antichain is either the set of minimal or maximal elements of P.
Choose $x \in \text{Min}(P)$ and $y \in \text{Max}(P)$ with $x \leq y$ (Possibly $x = y$), then $\{x, y\}$ is a chain.
Now $|P - \{x, y\}| \leq k$ and $P - \{x, y\}$ is of width $w - 1$ (since each antichain of size k contains x or y), hence by induction hypothesis, $P - \{x, y\}$ can be partitioned into $w - 1$ chains. Add chain $\{x, y\}$ to obtained the w-chain partition of P. □



An Application of Dilworth's Theorem

Theorem (Erdős–Szekeres, 1935)

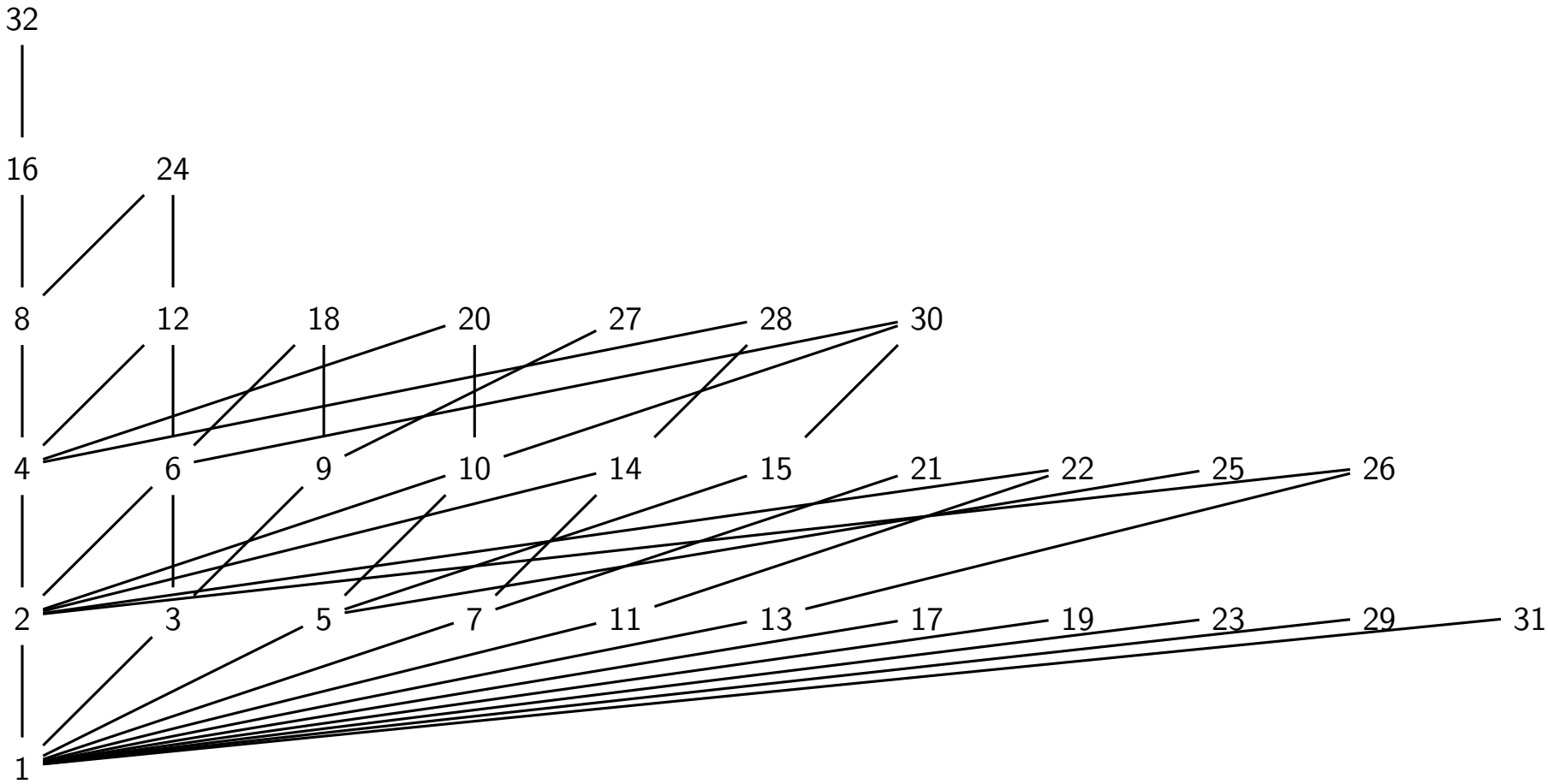
Let $A = (a_1, ..., a_n)$ be a sequence of n ***different*** *real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of $s + 1$ terms or a decreasing subsequence of $r + 1$ terms (or both).*

Proof by Dilworth's Theorem.

Define the partial order $\preceq$ on A by $a_i \preceq a_j$ iff $a_i \leq a_j$ and $i \leq j$. (Check it!)
Then we can observe that an increasing subsequence of A corresponds to a chain in $(A, \preceq)$, and an decreasing subsequence in A corresponds to an antichain in $(A, \preceq)$.
Assume that there is no decreasing subsequence of length $r + 1$, then by Dilworth's Theorem, the poset $(A, \preceq)$ can be ***partitioned*** into k chains $C_1, \ldots, C_k$, with $k \leq r$. Therefore $|C_1| + \cdots + |C_k| = n \geq sr + 1$.
By pigeonhole principle, there exsits a chain C_j with $|C_j| \geq s + 1$, which corresponds to an increasing subsequence of length at least $s + 1$. □

Divisibility Revisited

Consider the set $[32] = \{1, 2, \ldots, 31, 32\}$, ordered by divisibility.



Several Equivalent Major Theorems in Combinatorics

- König's Theorem
- Menger's Theorem (1929)
- Max-Flow Min-Cut theorem
- König-Egerváry theorem (1931)
- Birkhoff-Von Neumann Theorem (1946)
- ***Hall's Theorem***
- ***Dilworth's Theorem***

and duality in linear programming.