Discrete Mathematics in Computer Science
A1. Organizational Matters

Malte Helmert, Gabriele Röger

University of Basel

September 17, 2025

A1.1 Organizational Matters

A1.2 About this Course

A1.1 Organizational Matters

People

Lecturers

Malte Helmert

- ▶ email: malte.helmert@unibas.ch
- ▶ office: room 06.004, Spiegelgasse 1

Gabi Röger

- ▶ email: gabriele.roeger@unibas.ch
- ▶ office: room 04.005, Spiegelgasse 1

Assistant

David Speck

- ▶ email: davidjakob.speck@unibas.ch
- ▶ office: room 04.003, Spiegelgasse 5

People

Tutors

- ► Maria Desteffani (maria.desteffani@unibas.ch)
- ► Pascal von Fellenberg (pascal.vonfellenberg@unibas.ch)
- ► Carina Schrenk (carina.schrenk@unibas.ch)
- ► Carina Fehr (carina.fehr@unibas.ch)

Target Audience

target audience:

▶ this is an introductory course on the Bachelor's level

▶ we cover mathematical foundations that are
  particularly useful for the computer science curriculum

▶ main target audience: B.Sc. Computer Science,
  1st semester

▶ all other students welcome

Enrolment

▶ https://services.unibas.ch/
▶ official deadline: October 13
▶ better today, so that you get all relevant emails
  and access to the ADAM workspace

Discrete Mathematics Course on ADAM

ADAM

https://adam.unibas.ch/

- ▶ link to website with slides

- ▶ submission of exercise sheets

- ▶ model solutions for exercise sheets

- ▶ link to Discord server (for interaction among participants, but you also get answers from lecturers, assistant and tutors)

- ▶ additional material

Language

- ▶ The course is taught in English.
- ▶ All lecture material is in English.
- ▶ We (lecturers, assistant, tutors) speak German and English.
- ▶ You are also welcome to ask questions in German.
- ▶ Also exercise submissions can be in English or German.

Lectures

- ▶ Mon 16:15–18:00, Hörsaal U1.131, Biozentrum
  Wed 16:15–17:00, Hörsaal 1, Pharmazentrum
- ▶ first half of the course taught by Gabi Röger,
  second half by Malte Helmert
- ▶ on December 17: Q&A session for exam preparation

Exercises

Exercise sheets (homework assignments):

- ▶ mostly theoretical exercises
- ▶ exercise sheets on ADAM every Monday after the lecture
- ▶ must be solved in groups of two or three
  (not alone or in larger groups)
- ▶ due on the following Sunday (23:59)
  (upload to ADAM at https://adam.unibas.ch/)
- ▶ we only accept readable PDFs
  → with a bonus point per sheet created with LATEX
    (template, cheat sheet and intro on ADAM)

  Question: Who has experience with LATEX?

Exercise Sessions With Tutors

Exercise Sessions (starting September 24/25/27)

Wed 17:15–18:00	Alte Universität, Seminarraum −201
	with Carina S.
Wed 17:15–18:00	Spiegelgasse 1, Computer-Labor U1.001
	with Pascal
Thu 17:15–18:00	Spiegelgasse 1, Seminarraum 00.003
	with Maria
Fri 17:15–18:00	Pharmazentrum, Labor U1075
	with Carina F.

▶ common mistakes/misconceptions
  (full model solutions on ADAM)
▶ questions about exercise sheets and the course
▶ as time permits, support while you solve the exercises

important: please fill in the survey on ADAM for the group
allocation until Friday 12:00 (September 19).

Exam

- ▶ Written exam
- ▶ 6 ECTS credits
- ▶ Monday, January 19, 2026, 16:00-18:00
- ▶ Maurice E. Müller Saal, Biozentrum
- ▶ admission to exam: 50% of the exercise marks
- ▶ grade for course determined exclusively by the exam

Required Time

Official calculation

- ▶ 1 CP ≈ 30 hours
- ▶ The course has 6 CP.
- ▶ You need to invest about 180 hours.
- ▶ With 40 hours for exam preparation,
  this leaves 10–11 hours/week during the teaching period.

Alternative calculation

- ▶ A full-time student achieves 30 CP per semester.
- ▶ The course corresponds to 1/5 of 30 CP.
- ▶ With a 42h week, this still corresponds to 8.4 hours/week.

Plagiarism

> **Plagiarism**
> Plagiarism is presenting someone else's work, ideas, or words
> as your own, without proper attribution.

For example:

- ▶ Using someone's text without citation
- ▶ Paraphrasing too closely
- ▶ Using information from a source without attribution
- ▶ Passing off AI-generated content as your own original work

Long-term impact:

- ▶ You undermine your own learning.
- ▶ You start to lose confidence in your ability to think, write, and solve problems independently.
- ▶ Damage to academic reputation and professional consequences in future careers

Plagiarism in Exercises

▶ You may discuss material from the course,
   including the exercise assignments, with your peers.

▶ But: You have to independently write down your exercise
   solutions (in your team).

▶ Help from an LLM is acceptable to the same extent as it is
   acceptable from someone who is not a member of your team.

Immediate consequences of plagiarism:

▶ 0 marks for the exercise sheet (first time)

▶ exclusion from exam (second time)

If in doubt: check with us what is (and isn't) OK before submitting
Exercises too difficult? We are happy to help!

Special Needs?

- ▶ We (and the university) strive for equality of students with disabilities or chronic illnesses.
- ▶ Contact the lecturers for small adaptations.
- ▶ Contact the Students Without Barriers (StoB) service point for general adaptations and disadvantage compensation.

A1.2 About this Course

Content: Discrete Mathematics in Computer Science

▶ mathematical thinking and proof techniques
▶ sets and relations
▶ group theory and permutations
▶ modular arithmetic
▶ graphs and trees
▶ formal logic

Learning Goals

- ▶ proficiency in abstract thinking
- ▶ ability to formalize mathematical ideas and arguments
- ▶ knowledge of common mathematical tools in computer science

Discrete Mathematics in Computer Science
A2. Sets: Foundations

Malte Helmert, Gabriele Röger

University of Basel

September 22, 2025

A2.1 Sets

A2.2 Russell's Paradox

A2.3 Relations on Sets

A2.4 Set Operations

A2.5 Cardinality of Finite Sets

A2.1 Sets

Important Building Blocks of Discrete Mathematics

▶ sets
▶ relations
▶ functions

These topics will mainly be the content of part B of the course.

We cover some foundations on sets already now because we will use them for illustrating proof techniques.

Sets

> ### Definition
> A set is an unordered collection of distinct objects.

- ▶ unorderd: no notion of a "first" or "second" object,
  e. g. {Alice, Bob, Charly} = {Charly, Bob, Alice}
- ▶ distinct: each object contained at most once,
  e. g. {Alice, Bob, Charly} = {Alice, Charly, Bob, Alice}

German: Menge

Notation

- ▶ Specification of sets
    - ▶ explicit, listing all elements, e. g. $A = \{1, 2, 3\}$
    - ▶ implicit with set-builder notation,
      specifying a property characterizing all elements,
      e. g. $A = \{x \mid x \in \mathbb{N}_0 \text{ and } 1 \le x \le 3\}$,
          $B = \{n^2 \mid n \in \mathbb{N}_0\}$
    - ▶ implicit, as a sequence with dots,
      e. g. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
    - ▶ implicit with an inductive definition
- ▶ $e \in M$: e is in set M (an element of the set)
- ▶ $e \notin M$: e is not in set M
- ▶ empty set $\emptyset = \{\}$

Question: Is it true that $1 \in \{\{1, 2\}, 3\}$?

German: Element, leere Menge

Special Sets

- Natural numbers $\mathbb{N}_0 = \{0, 1, 2, \dots\}$
- Integers $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- Positive integers $\mathbb{Z}_+ = \mathbb{N}_1 = \{1, 2, \dots\}$
- Rational numbers $\mathbb{Q} = \{n/d \mid n \in \mathbb{Z}, d \in \mathbb{N}_1\}$
- Real numbers $\mathbb{R} = (-\infty, \infty)$
  Why do we use interval notation?
  Why didn't we introduce it before?

German: Natürliche ($\mathbb{N}_0$), ganze ($\mathbb{Z}$), rationale ($\mathbb{Q}$), reelle ($\mathbb{R}$) Zahlen

A2.2 Russell's Paradox

Excursus: Barber Paradox

Barber Paradox

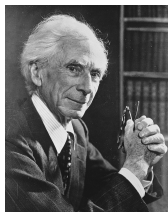In a town there is only one barber, who is male.

The barber shaves all men in the town,
and only those, who do not shave themselves.

Who shaves the barber?

We can exploit the self-reference to derive a contradiction.

Russell's Paradox

Bertrand Russell

> ### Question
> Is the collection of all sets that do not contain themselves as a member a set?

Is $S = \{M \mid M \text{ is a set and } M \notin M\}$ a set?

Assume that S is a set.
If $S \notin S$ then $S \in S \rightsquigarrow$ Contradiction
If $S \in S$ then $S \notin S \rightsquigarrow$ Contradiction
Hence, there is no such set S.

$\rightarrow$ Not every property used in set-builder notation defines a set.

A2.3 Relations on Sets

Equality

> **Definition (Axiom of Extensionality)**
> Two sets A and B are equal (written $A = B$)
> if every element of A is an element of B and vice versa.

Two sets are equal if they contain the same elements.

We write $A \neq B$ to indicate that A and B are not equal.

Subsets and Supersets

▶ $A \subseteq B$: A is a subset of B,
   i.e., every element of A is an element of B

▶ $A \subset B$: A is a strict subset of B,
   i.e., $A \subseteq B$ and $A \neq B$.

▶ $A \supseteq B$: A is a superset of B if $B \subseteq A$.

▶ $A \supset B$: A is a strict superset of B if $B \subset A$.

We write $A \nsubseteq B$ to indicate that A is not a subset of B.

Analogously: $\not\subset$, $\nsupseteq$, $\not\supset$

German: Teilmenge, echte Teilmenge, Obermenge, echte Obermenge

Power Set

> **Definition (Power Set)**
>
> The power set $\mathcal{P}(S)$ of a set S is the set of all subsets of S.
> That is,
> $$\mathcal{P}(S) = \{M \mid M \subseteq S\}.$$

Example: $\mathcal{P}(\{a, b\}) =$

German: Potenzmenge

A2.4 Set Operations

Set Operations

Set operations allow us to express sets in terms of other sets

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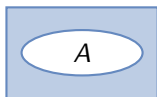

If $A \cap B = \emptyset$ then A and B are disjoint.

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

▶ set difference $A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$

▶ complement $\overline{A} = B \setminus A$, where $A \subseteq B$ and
   B is the set of all considered objects (in a given context)

German: Schnitt, disjunkt, Vereinigung, Differenz, Komplement

Properties of Set Operations: Commutativity

Theorem (Commutativity of ∪ and ∩)

For all sets A and B it holds that

▶ $A \cup B = B \cup A$ *and*

▶ $A \cap B = B \cap A$.

Question: Is the set difference also commutative,
                  i. e. is $A \setminus B = B \setminus A$ for all sets A and B?

German: Kommutativität

Properties of Set Operations: Associativity

Theorem (Associativity of ∪ and ∩)

For all sets A, B and C it holds that

▶ $(A \cup B) \cup C = A \cup (B \cup C)$ *and*

▶ $(A \cap B) \cap C = A \cap (B \cap C)$.

German: Assoziativität

Properties of Set Operations: Distributivity

Theorem (Union distributes over intersection and vice versa)

For all sets A, B and C it holds that

- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ *and*
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

German: Distributivität

Properties of Set Operations: De Morgan's Law

Augustus De Morgan
British mathematician (1806-1871)

Theorem (De Morgan's Law)

For all sets A and B it holds that

- $\overline{A \cup B} = \overline{A} \cap \overline{B}$ *and*
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

A2.5 Cardinality of Finite Sets

Cardinality of Sets

The cardinality $|S|$ measures the size of set S.

A set is finite if it has a finite number of elements.

> ### Definition (Cardinality)
> The cardinality of a finite set is the number of elements it contains.

- $|\emptyset| =$
- $|\{x \mid x \in \mathbb{N}_0 \text{ and } 2 \leq x < 5\}| =$
- $|\{3, 0, \{1, 3\}\}| =$
- $|\mathcal{P}(\{1, 2\})| =$

German: Kardinalität oder Mächtigkeit

Cardinality of the Union of Sets

Theorem
For finite sets A and B it holds that $|A \cup B| = |A| + |B| - |A \cap B|$.

Corollary
If finite sets A and B are disjoint then $|A \cup B| = |A| + |B|$.

Cardinality of the Power Set

Theorem

Let S be a finite set. Then $|\mathcal{P}(S)| = 2^{|S|}$.

Proof sketch.

We can construct a subset S' by iterating over all elements e of S and deciding whether e becomes a member of S' or not.

We make $|S|$ independent decisions, each between two options. Hence, there are $2^{|S|}$ possible outcomes.

Every subset of S can be constructed this way and different choices lead to different sets. Thus, $|\mathcal{P}(S)| = 2^{|S|}$.   □

Summary

- ▶ **Sets** are **unordered collections** of **distinct** objects.
- ▶ Important **set relations**: **equality** ($=$), **subset** ($\subseteq$), **superset** ($\supseteq$) and strict variants ($\subset$ and $\supset$)
- ▶ The **power set** of a set S is the set of all subsets of S.
- ▶ Important **set operations** are **intersection**, **union**, **set difference** and **complement**.
  - ▶ Union and intersection are **commutative and associative**.
  - ▶ Union distributes over intersection and vice versa.
  - ▶ **De Morgan's law** for complement of union or intersection.
- ▶ The number of elements in a finite set is called its **cardinality**.

Discrete Mathematics in Computer Science
A3. Proofs: Introduction

Malte Helmert, Gabriele Röger

University of Basel

September 22, 2025

Discrete Mathematics in Computer Science

A3.1 What is a Proof?

A3.1 What is a Proof?

What is a Proof?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conlusion
  that some statement must be true.

What is a statement?

Mathematical Statements

> ### Mathematical Statement
> A mathematical statement is a declarative sentence that is either
> true or false (but not both).

Examples (some true, some false):

▶ Let $p \in \mathbb{N}_0$ be a prime number. Then p is odd.

▶ There exists an even prime number.

▶ The equation $a^k + b^k = c^k$ has infinitely many solutions
with $a, b, c, k \in \mathbb{N}_1$ and $k \geq 2$.

German: Mathematische Aussage

Mathematical Statements: Quantification

Statements often use quantification.

> ▶ Universal quantification:
>   "For all x in set S it holds that $\langle$sub-statement on $x\rangle$."
>
>   This is true if the sub-statement is true for every x in S.
>
> ▶ Existential quantification:
>   "There is an x in set S such that $\langle$sub-statement on $x\rangle$."
>
>   This is true if there exists at least one x in S for which the
>   sub-statement is true.

Examples (some true, some false):

▶ For all $x \in \mathbb{N}_1$ it holds that $x + 1$ is in $\mathbb{N}_1$.

▶ For all $x \in \mathbb{N}_1$ it holds that $x - 1$ is in $\mathbb{N}_1$.

▶ There is an $x \in \mathbb{N}_1$ such that $x = \sqrt{x}$.

Mathematical Statements: Preconditions and Conclusions

We can identify preconditions and conclusions.

> "If ⟨preconditions⟩ then ⟨conclusions⟩."
>
> The statement is true if the conclusions are true
> whenever the preconditions are true.

Not every statement has preconditions. Preconditions are often
used in universally quantified sub-statements.

Examples (some true, some false):

- ▶ If 4 is a prime number then $2 \cdot 3 = 4$.
- ▶ If n is a prime number with $n > 2$ then n is odd.
- ▶ For all $p \in \mathbb{N}_1$ it holds that if p is a prime number then p is
  odd.

Different Statements with the same Meaning

The following statements have the same meaning, we just move preconditions into the quantification, make some aspects implicit, and change the structure.

- For all $p \in \mathbb{N}_1$ it holds that if p is a prime number with $p > 2$ then p is odd.

- For all prime numbers p it holds that if $p > 2$ then p is odd.

- Let p be a natural number with $p > 2$.
  Then p is prime if p is odd.

- If p is a prime number with $p > 2$ then p is odd.

- All prime numbers $p > 2$ are odd.

A single mathematical statement can be expressed in different ways, as long as the meaning stays the same.

Like paraphrasing a sentence in everyday language.

On what Statements can we Build the Proof?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conlusion
  that some statement must be true.

We can use:

- ▶ axioms: statements that are assumed to always be true
  in the current context
- ▶ theorems and lemmas: statements that were already proven
    - ▶ lemma: an intermediate tool
    - ▶ theorem: itself a relevant result
- ▶ premises: assumptions we make
  to see what consequences they have

German: Axiom, Theorem/Satz, Lemma, Prämisse/Annahme

What is a Logical Step?

A mathematical proof is

▶ a sequence of logical steps

▶ starting with one set of statements

▶ that comes to the conlusion
   that some statement must be true.

Each step directly follows

▶ from the axioms,

▶ premises,

▶ previously proven statements and

▶ the preconditions of the statement we want to prove.

For a formal definition, we would need formal logics.

The Role of Definitions

> **Definition**
>
> A set is an unordered collection of distinct objects.
>
> The objects in a set are called the elements of the set. A set is said to contain its elements.
>
> We write $x \in S$ to indicate that x is an element of set S, and $x \notin S$ to indicate that S does not contain x.
>
> The set that does not contain any objects is the *empty set* $\emptyset$.

- ▶ A definition introduces an abbreviation.
- ▶ Whenever we say "set", we could instead say "an unordered collection of distinct objects" and vice versa.
- ▶ Definitions can also introduce notation.

German: Definition

Disproofs

▶ A disproof (refutation) shows that a given mathematical statement is false by giving an example where the preconditions are true, but the conclusion is false.

▶ This requires deriving, in a sequence of proof steps, the opposite (negation) of the conclusion.

Example (False statement)

"If $p \in \mathbb{N}_0$ is a prime number then p is odd."

Refutation.

Consider natural number 2 as a counter example. It is prime because it has exactly 2 divisors, 1 and itself. It is not odd, because it is divisible by 2. □

German: Widerlegung

A Word on Style

A proof should help the reader to see why the result must be true.

▶ A proof should be easy to follow.
▶ Omit unnecessary information.
▶ Move self-contained parts into separate lemmas.
▶ In complicated proofs, reveal the overall structure in advance.
▶ Have a clear line of argument.

$\rightarrow$ Writing a proof is like writing an essay.

Recommended reading (ADAM additional ressources):

▶ "Some Remarks on Writing Mathematical Proofs" (John M. Lee)
▶ "§1. Minicourse on technical writing" of "Mathematical Writing"
   (Donald E. Knuth, Tracy Larrabee, and Paul M. Roberts)

Summary

A proof should convince the reader by logical steps of the truth of some mathematical statement.

Discrete Mathematics in Computer Science
A4. Proof Techniques I

Malte Helmert, Gabriele Röger

University of Basel

September 24, 2025

A4.1 Proof Strategies

A4.2 Direct Proof

A4.3 Indirect Proof

A4.4 Proof by Contrapositive

A4.1 Proof Strategies

Common Forms of Statements

Many statements have one of these forms:

1. "All $x \in S$ with the property P also have the property Q."
2. "A is a subset of B."
3. "For all $x \in S$: x has property P iff x has property Q." ("iff": "if and only if")
4. "$A = B$", where A and B are sets.

In the following, we will discuss some typical proof/disproof strategies for such statements.

Proof Strategies

1. "All $x \in S$ with the property P also have the property Q."
   "For all $x \in S$: if x has property P, then x has property Q."

   ▶ To prove, assume you are given an arbitrary $x \in S$
   that has the property P.
   Give a sequence of proof steps showing that x
   must have the property Q.

   ▶ To disprove, find a counterexample, i. e., find an $x \in S$
   that has property P but not Q and prove this.

Proof Strategies

2. "A is a subset of B."

   ▶ To prove, assume you have an arbitrary element $x \in A$
     and prove that $x \in B$.
   ▶ To disprove, find an element in $x \in A \setminus B$
     and prove that $x \in A \setminus B$.

Proof Strategies

③ "For all $x \in S$: x has property P iff x has property Q."
   ("iff": "if and only if")
   ▶ To prove, separately prove "if P then Q" and "if Q then P".
   ▶ To disprove, disprove "if P then Q" or disprove "if Q then P".

Proof Strategies

4. "$A = B$", where A and B are sets.
   - To prove, separately prove "$A \subseteq B$" and "$B \subseteq A$".
   - To disprove, disprove "$A \subseteq B$" or disprove "$B \subseteq A$".

Proof Techniques

most common proof techniques:

- ▶ direct proof
- ▶ indirect proof (proof by contradiction)
- ▶ contrapositive
- ▶ mathematical induction
- ▶ structural induction

A4.2 Direct Proof

Direct Proof

Direct Proof
Direct derivation of the statement by deducing or rewriting.

German: Direkter Beweis

Direct Proof: Example

Theorem
For all sets A, B and C it holds that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof.
Let A, B and C be arbitrary sets.

We will show separately that

▶ $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that
▶ $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

. . .

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

We make a case distinction between $x \in B$ and $x \notin B$:

Case 1 ($x \in B$): As $x \in A$ is true, it holds in this case that $x \in (A \cap B)$.

Case 2 ($x \notin B$): From $x \in (B \cup C)$ it follows for this case that $x \in C$. With $x \in A$ we conclude that $x \in (A \cap C)$.

In both cases it holds that $x \in A \cap B$ or $x \in A \cap C$, and we conclude that $x \in (A \cap B) \cup (A \cap C)$.

As x was chosen arbitrarily from $A \cap (B \cup C)$, we have shown that every element of $A \cap (B \cup C)$ is an element of $(A \cap B) \cup (A \cap C)$, so it holds that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.   . . .

Direct Proof: Example cont.

> Proof (continued).
> We will now show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.
>
> ... **[Homework assignment]** ...
>
> Overall we have shown for arbitrary sets A, B and C that
> $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that
> $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, which concludes the proof of the
> theorem.   □

A4.3 Indirect Proof

Indirect Proof

> ### Indirect Proof (Proof by Contradiction)
>
> ▶ Make an assumption that the statement is false.
>
> ▶ Use the assumption to derive a contradiction.
>
> ▶ This shows that the assumption must be false
>   and hence the original statement must be true.

German: Indirekter Beweis, Beweis durch Widerspruch

Indirect Proof: Example

Theorem
Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.
We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Since $A \not\subseteq B$ there is some $x \in A$ such that $x \notin B$.

For this x it holds that $x \in A \setminus B$.

This is a contradiction to $A \setminus B = \emptyset$.

We conclude that the assumption was false and thus the theorem is true. $\qquad\square$

A4.4 Proof by Contrapositive

Contrapositive

> (Proof by) Contrapositive
> Prove "If A, then B" by proving "If not B, then not A."

Examples:

- ▶ Prove "For all $n \in \mathbb{N}_0$: if n^2 is odd, then n is odd"
  by proving "For all $n \in \mathbb{N}_0$, if n is even, then n^2 is even."

- ▶ Prove "For all $n \in \mathbb{N}_0$: if n is not a square number,
  then $\sqrt{n}$ is irrational" by proving "For all $n \in \mathbb{N}_0$:
  if $\sqrt{n}$ is rational, then n is a square number."

German: Kontraposition

Contrapositive: Example

Theorem
For any sets A and B: If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.
We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \nsubseteq B$.

Let A and B be arbitrary sets with $A \setminus B \neq \emptyset$.

As the set difference is not empty, there is at least one x with $x \in A \setminus B$. By the definition of the set difference $(\setminus)$, it holds for such x that $x \in A$ and $x \notin B$.

Hence, not all elements of A are elements of B, so it does not hold that $A \subseteq B$. $\qquad\square$

Summary

- There are standard strategies for proving some common forms of statements, e.g. some property of all elements of a set.
- Direct proof: derive statement by deducing or rewriting.
- Indirect proof: derive contradiction from the assumption that the statement is false.
- Proof by contrapositive: Prove "If A, then B" by proving "If not B, then not A.".

Discrete Mathematics in Computer Science
A5. Proof Techniques II

Malte Helmert, Gabriele Röger

University of Basel

September 29, 2025

A5.1 Mathematical Induction

A5.2 Structural Induction

A5.3 Excursus: Computer-assisted Theorem Proving

A5.1 Mathematical Induction

Proof Techniques

most common proof techniques:

- ▶ direct proof
- ▶ indirect proof (proof by contradiction)
- ▶ contrapositive
- ▶ mathematical induction
- ▶ structural induction

Mathematical Induction

Concrete Mathematics by Graham, Knuth and Patashnik (p. 3)

Mathematical induction proves that

we can climb as high as we like on a ladder,

by proving that we can climb onto the bottom rung (the basis)

and that

from each rung we can climb up to the next one (the step).

Propositions

Consider a statement on all natural numbers n with $n \geq m$.

▶ E.g. "Every natural number $n \geq 2$ can be written as a product of prime numbers."

  ▶ $P(2)$: "2 can be written as a product of prime numbers."
  ▶ $P(3)$: "3 can be written as a product of prime numbers."
  ▶ $P(4)$: "4 can be written as a product of prime numbers."
  ▶ ...
  ▶ $P(n)$: "n can be written as a product of prime numbers."
  ▶ For every natural number $n \geq 2$ proposition $P(n)$ is true.

Proposition $P(n)$ is a mathematical statement that is defined in terms of natural number n.

Mathematical Induction

> ## Mathematical Induction
> Proof (of the truth) of proposition $P(n)$
> for all natural numbers n with $n \geq m$:
>
> - ▶ basis: proof of $P(m)$
> - ▶ induction hypothesis (IH):
>   suppose that $P(k)$ is true for all k with $m \leq k \leq n$
> - ▶ inductive step: proof of $P(n+1)$
>   using the induction hypothesis

German: Vollständige Induktion, Induktionsanfang,
Induktionsannahme oder Induktionsvoraussetzung,
Induktionsschritt

Mathematical Induction: Example I

Theorem
Every natural number $n \geq 2$ can be written as a product of prime numbers, i. e. $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$ with prime numbers $p_1, \ldots, p_m$.

Proof.
Mathematical Induction over n:

basis $n = 2$: trivially satisfied, since 2 is prime

IH: Every natural number k with $2 \leq k \leq n$
     can be written as a product of prime numbers.   . . .

Mathematical Induction: Example I

Theorem
Every natural number $n \geq 2$ can be written as a product of prime numbers, i.e. $n = p_1 \cdot p_2 \cdot \ldots \cdot p_m$ with prime numbers $p_1, \ldots, p_m$.

Proof (continued).
inductive step $n \rightarrow n + 1$:

▶ Case 1: $n + 1$ is a prime number $\rightsquigarrow$ trivial

▶ Case 2: $n + 1$ is not a prime number.
  There are natural numbers $2 \leq q, r \leq n$ with $n + 1 = q \cdot r$.
  Using the IH shows that there are prime numbers
  $q_1, \ldots, q_s$ with $q = q_1 \cdot \ldots \cdot q_s$ and
  $r_1, \ldots, r_t$ with $r = r_1 \cdot \ldots \cdot r_t$.
  Together this means $n + 1 = q_1 \cdot \ldots \cdot q_s \cdot r_1 \cdot \ldots \cdot r_t$.

Mathematical Induction: Example II

> **Theorem**
>
> *Let S be a finite set. Then $|\mathcal{P}(S)| = 2^{|S|}$.*

What proposition can we use to prove this
with mathematical induction?

Proof by Induction

Proof.

By induction over $|S|$.

Basis ($|S| = 0$): Then $S = \emptyset$ and $|\mathcal{P}(S)| = |\{\emptyset\}| = 1 = 2^0$.

IH: For all sets S with $|S| \leq n$, it holds that $|\mathcal{P}(S)| = 2^{|S|}$.

Inductive Step ($n \rightarrow n + 1$):

Let S' be an arbitrary set with $|S'| = n + 1$ and
let e be an arbitrary member of S'.

Let further $S = S' \setminus \{e\}$ and $X = \{S'' \cup \{e\} \mid S'' \in \mathcal{P}(S)\}$.

Then $\mathcal{P}(S') = \mathcal{P}(S) \cup X$. As $\mathcal{P}(S)$ and X are disjoint and
$|X| = |\mathcal{P}(S)|$, it holds that $|\mathcal{P}(S')| = 2|\mathcal{P}(S)|$.

Since $|S| = n$, we can use the IH and get

$$|\mathcal{P}(S')| = 2 \cdot 2^{|S|} = 2 \cdot 2^n = 2^{n+1} = 2^{|S'|}.$$

$\square$

Weak vs. Strong Induction

▶ **Weak induction:** Induction hypothesis only supposes
  that $P(k)$ is true for $k = n$

▶ **Strong induction:** Induction hypothesis supposes
  that $P(k)$ is true for all $k \in \mathbb{N}_0$ with $m \leq k \leq n$
  ▶ also: complete induction

Our previous definition corresponds to strong induction.

Which of the examples had also worked with weak induction?

Is Strong Induction More Powerful than Weak Induction?

Are there statements that we can prove with strong induction
but not with weak induction?

We can always use a stronger proposition:

▶ "Every $n \in \mathbb{N}_0$ with $n \geq 2$ can be written as a product of
   prime numbers."

▶ $P(n)$: "n can be written as a product of prime numbers."

▶ $P'(n)$: "all $k \in \mathbb{N}_0$ with $2 \leq k \leq n$ can be written
   as a product of prime numbers."

A5.2 Structural Induction

Inductively Defined Sets: Examples

Example (Natural Numbers)

The set $\mathbb{N}_0$ of natural numbers is inductively defined as follows:

- ▶ 0 is a natural number.
- ▶ If n is a natural number, then $n + 1$ is a natural number.

Example (Binary Tree)

The set $\mathcal{B}$ of binary trees is inductively defined as follows:

- ▶ $\square$ is a binary tree (a leaf)
- ▶ If L and R are binary trees, then $\langle L, \bigcirc, R \rangle$ is a binary tree (with inner node $\bigcirc$).

Implicit statement: all elements of the set can be constructed
                         by finite application of these rules

German: Binärbaum, Blatt, innerer Knoten

Inductive Definition of a Set

> ### Inductive Definition
> A set M can be defined inductively by specifying
>
> ▶ basic elements that are contained in M
>
> ▶ construction rules of the form
>   "Given some elements of M, another element of M
>   can be constructed like this."

German: Induktive Definition, Basiselemente, Konstruktionsregeln

Structural Induction

> ## Structural Induction
> Proof of statement for all elements of an inductively defined set
>
> ► **basis**: proof of the statement for the basic elements
>
> ► **induction hypothesis** (IH):
>   suppose that the statement is true for some elements M
>
> ► **inductive step**: proof of the statement for elements
>   constructed by applying a construction rule to M
>   (one inductive step for each construction rule)

German: Strukturelle Induktion

Structural Induction: Example (1)

Definition (Leaves of a Binary Tree)

The number of leaves of a binary tree B, written $leaves(B)$, is defined as follows:

$$leaves(\square) = 1$$
$$leaves(\langle L, \bigcirc, R \rangle) = leaves(L) + leaves(R)$$

Definition (Inner Nodes of a Binary Tree)

The number of inner nodes of a binary tree B, written $inner(B)$, is defined as follows:

$$inner(\square) = 0$$
$$inner(\langle L, \bigcirc, R \rangle) = inner(L) + inner(R) + 1$$

Structural Induction: Example (2)

Theorem
For all binary trees B: inner(B) = leaves(B) − 1.

Proof.
induction basis:
$inner(\square) = 0 = 1 - 1 = leaves(\square) - 1$
⤳ statement is true for base case   . . .

Structural Induction: Example (3)

Proof (continued).

induction hypothesis:

to prove that the statement is true for a composite tree $\langle L, \bigcirc, R \rangle$, we may use that it is true for the subtrees L and R.

inductive step for $B = \langle L, \bigcirc, R \rangle$:

$$
\begin{aligned}
inner(B) &= inner(L) + inner(R) + 1 \\
&\overset{IH}{=} (leaves(L) - 1) + (leaves(R) - 1) + 1 \\
&= leaves(L) + leaves(R) - 1 = leaves(B) - 1
\end{aligned}
$$

$\square$

Example: Tarradiddles

Example (Tarradiddles)

The set of tarradiddles is inductively defined as follows:

- ► ✈ is a tarradiddle.
- ► ♥ is a tarradiddle.
- ► If x and y are tarradiddles, then x❀❀y is a tarradiddle.
- ► If x and y are tarradiddles, then ❀x✈y❀ is a tarradiddle.

How do you prove with structural induction that every tarradiddle contains an even number of flowers?

A5.3 Excursus: Computer-assisted Theorem Proving

Computer-assisted Proofs

▶ Computers can help proving theorems.
▶ Computer-aided proofs have for example been used for proving theorems by exhaustion.
▶ Example: Four color theorem

Interactive Theorem Proving

- ▶ On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.
- ▶ On this level, proofs can be automatically verified by computers.
- ▶ Nobody wants to write or read proofs on this level of detail.
- ▶ In Interactive Theorem Proving a human guides the proof and the computer tries to fill in the details.
- ▶ If it succeeds, we can be very confident that the proof is valid.
- ▶ Example theorem provers: Isabelle/HOL, Lean

Example

⇝ Demo

Summary

- **Mathematical induction** is used to prove a proposition P for all natural numbers $\geq m$.
  - Prove $P(m)$.
  - Make hypothesis that $P(k)$ is true for $m \leq k \leq n$.
  - Establish $P(n+1)$ using the hypothesis.
- **Structural induction** applies the same general concept to prove a proposition P for all elements of an inductively defined set.

Discrete Mathematics in Computer Science

B1. Tuples & Cartesian Product

Malte Helmert, Gabriele Röger

University of Basel

October 1, 2025

Discrete Mathematics in Computer Science
October 1, 2025 — B1. Tuples & Cartesian Product

B1.1 Tuples and the Cartesian Product

B1.1 Tuples and the Cartesian Product

Motivation

- A set is an unordered collection of distinct objects.
- We often need a more structured way of representation.
  - A person is associated with a name, address, phone number.
  - A set of persons makes sense in many contexts.
  - Representing the associated data as a set rather not.
- We could for example want to
  - directly access the name of a person, or
  - have a separate billing and delivery address for some order, but in general, these can be the same.
- Tuples are mathematical building blocks that support this.

Sets vs. Tuples

▶ A set is an unordered collection of distinct objects.
▶ A tuple is an ordered sequence of objects.

Tuples

- ▶ k-tuple: ordered sequence of k objects ($k \in \mathbb{N}_0$)
- ▶ written $(o_1, \ldots, o_k)$ or $\langle o_1, \ldots, o_k \rangle$
- ▶ unlike sets, order matters ($\langle 1, 2 \rangle \neq \langle 2, 1 \rangle$)
- ▶ objects may occur multiple times in a tuple
- ▶ objects contained in tuples are called components
- ▶ terminology:
  - ▶ $k = 2$: (ordered) pair
  - ▶ $k = 3$: triple
  - ▶ more rarely: quadruple, quintuple, sextuple, septuple, . . .
- ▶ if k is clear from context (or does not matter),
  often just called tuple

German: k-Tupel, Komponente, (geordnetes) Paar, Tripel, Quadrupel

Equality of Tuples

> **Definition (Equality of Tuples)**
>
> Two n-tuples $t = \langle o_1, \ldots, o_n \rangle$ and $t' = \langle o'_1, \ldots, o'_n \rangle$
> are equal ($t = t'$) if for $i \in \{1, \ldots, n\}$ it holds that $o_i = o'_i$.

Cartesian Product

Definition (Cartesian Product and Cartesian Power)

Let $S_1, \ldots, S_n$ be sets. The Cartesian product $S_1 \times \cdots \times S_n$ is the following set of n-tuples:

$$S_1 \times \cdots \times S_n = \{\langle x_1, \ldots, x_n \rangle \mid x_1 \in S_1, x_2 \in S_2, \ldots, x_n \in S_n\}.$$

The k-ary Cartesian power of a set S (with $k \in \mathbb{N}_1$) is the set
$S^k = \{\langle o_1, \ldots, o_k \rangle \mid o_i \in S \text{ for all } i \in \{1, \ldots, k\}\} = \underbrace{S \times \cdots \times S}_{k \text{ times}}$.

René Descartes: French mathematician and philosopher (1596–1650)

Example: $A = \{a, b\}$, $B = \{1, 2, 3\}$

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$$
$$A^2 = \{(a, a), (a, b), (b, a), (b, b)\}$$

German: Kartesisches Produkt

(Non-)properties of the Cartesian Product

The Cartesian product is

▶ not commutative, in most cases $A \times B \neq B \times A$.

▶ not associative, in most cases $(A \times B) \times C \neq A \times (B \times C)$

Why? Exceptions?

Summary

▶ A k-tuple is an ordered sequence of k objects, called the components of the tuple.

▶ 2-tuples are also called pairs and 3-tuples triples.

▶ The Cartesian Product $S_1 \times \cdots \times S_n$ of set $S_1, \ldots, S_n$ is the set of all tuples $\langle o_1, \ldots, o_n \rangle$, where for all $i \in \{1, \ldots, n\}$ component o_i is an element of S_i.

Discrete Mathematics in Computer Science

B2. Relations

Malte Helmert, Gabriele Röger

University of Basel

October 6, 2025

Discrete Mathematics in Computer Science
October 6, 2025 — B2. Relations

B2.1 Relations

B2.2 Properties of Binary Relations

B2.1 Relations

Relations: Informally

- Intuitively, a mathematical relation connects elements from several (possibly different) sets by specifying related groupings.
- We already know some relations, e. g.
  - $\subseteq$ relation for sets
  - $\leq$ relation for natural numbers
- These are examples of binary relations, considering pairs of objects.
- There are also relations of higher arity, e. g.
  - "$x + y = z$" for integers x, y, z.
  - "The name, address and office number belong to the same person."
- Relations are for example important for relational databases, semantic networks or knowledge representation and reasoning.

Relations

> ### Definition (Relation)
> Let $S_1, \ldots, S_n$ be sets.
>
> A relation over $S_1, \ldots, S_n$ is a set $R \subseteq S_1 \times \cdots \times S_n$.
>
> The arity of R is n.

A relation of arity n is a set of n-tuples.

German: Relation, Stelligkeit

Relations: Examples

- $\subseteq = \{(S, S') \mid S$ and S' are sets and
  for every $x \in S$ it holds that $x \in S'\}$
- $\leq = \{(x, y) \mid x, y \in \mathbb{N}_0$ and $x < y$ or $x = y\}$
- $R = \{(x, y, z) \mid x, y, z \in \mathbb{Z}$ and $x + y = z\}$
- $R' = \{($Gabi Röger, Spiegelgasse 1, 04.005$),$
  $($Malte Helmert, Spiegelgasse 1, 06.004$),$
  $($David Speck, Spiegelgasse 5, 04.003$)\}$

B2.2 Properties of Binary Relations

Binary Relation

A binary relation is a relation of arity 2:

> **Definition (binary relation)**
> A binary relation is a relation over two sets A and B.

- Instead of $(x, y) \in R$, we also write xRy, e.g.
  $x \le y$ instead of $(x, y) \in \le$
- If the sets are equal, we say "R is a binary relation over A"
  instead of "R is a binary relation over A and A".
- Such a relation over a set is also called
  a homogeneous relation or an endorelation.

German: zweistellige Relation, homogene Relation

Reflexivity

A reflexive relation relates every object to itself.

> **Definition (reflexive)**
> A binary relation R over set A is reflexive
> if for all $a \in A$ it holds that $(a, a) \in R$.

Which of these relations are reflexive?

- $R = \{(a, a), (a, b), (a, c), (b, a), (b, c), (c, c)\}$ over $\{a, b, c\}$
- $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$
- equality relation $=$ on natural numbers
- less-than relation $\leq$ on natural numbers
- strictly-less-than relation $<$ on natural numbers

German: reflexiv

Irreflexivity

A irreflexive relation never relates an object to itself.

> **Definition (irreflexive)**
> A binary relation R over set A is irreflexive
> if for all $a \in A$ it holds that $(a, a) \notin R$.

Which of these relations are irreflexive?

- $R = \{(a, a), (a, b), (a, c), (b, a), (b, c), (c, c)\}$ over $\{a, b, c\}$
- $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$
- equality relation $=$ on natural numbers
- less-than relation $\leq$ on natural numbers
- strictly-less-than relation $<$ on natural numbers

German: irreflexiv

Symmetry

> **Definition (symmetric)**
>
> A binary relation R over set A is symmetric
> if for all $a, b \in A$ it holds that $(a, b) \in R$ iff $(b, a) \in R$.

Which of these relations are symmetric?

- $R = \{(a, a), (a, b), (a, c), (b, a), (c, a), (c, c)\}$ over $\{a, b, c\}$
- $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$
- equality relation $=$ on natural numbers
- less-than relation $\leq$ on natural numbers
- strictly-less-than relation $<$ on natural numbers

German: symmetrisch

Asymmetry and Antisymmetry

How do these properties relate to irreflexivity?

> **Definition (asymmetric and antisymmetric)**
>
> Let R be a binary relation over set A.
>
> Relation R is asymmetric if
> for all $a, b \in A$ it holds that if $(a, b) \in R$ then $(b, a) \notin R$.
>
> Relation R is antisymmetric if for all $a, b \in A$ with $a \neq b$ it holds that if $(a, b) \in R$ then $(b, a) \notin R$.

Which of these relations are asymmetric/antisymmetric?

- $R = \{(a, a), (a, b), (a, c), (b, a), (c, a), (c, c)\}$ over $\{a, b, c\}$
- $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$
- equality relation $=$ on natural numbers
- less-than relation $\leq$ on natural numbers
- strictly-less-than relation $<$ on natural numbers

German: asymmetrisch, antisymmetrisch

Transitivity

> **Definition**
> A binary relation R over set A is transitive
> if it holds for all $a, b, c \in A$ that
> if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$.

Which of these relations are transitive?

- $R = \{(a, a), (a, b), (a, c), (b, a), (c, a), (c, c)\}$ over $\{a, b, c\}$
- $R = \{(a, a), (a, b), (a, c), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$
- equality relation $=$ on natural numbers
- less-than relation $\leq$ on natural numbers
- strictly-less-than relation $<$ on natural numbers

German: transitiv

Summary

- A relation over sets $S_1, \ldots, S_n$ is a set $R \subseteq S_1 \times \cdots \times S_n$.
- A binary relation is a relation over two sets.
- A binary relation over set S is a relation $R \subseteq S \times S$ and also called a homogeneous relation.
- A binary relation R over A is
  - reflexive if $(a, a) \in R$ for all $a \in A$,
  - irreflexive if $(a, a) \notin R$ for all $a \in A$,
  - symmetric if for all $a, b \in A$ it holds that $(a, b) \in R$ iff $(b, a) \in R$,
  - asymmetric if for all $a, b \in A$ it holds that if $(a, b) \in R$ then $(b, a) \notin R$,
  - antisymmetric if for all $a, b \in A$ with $a \neq b$ it holds that if $(a, b) \in R$ then $(b, a) \notin R$,
  - transitive if for all $a, b, c \in A$ it holds that if $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$.

Special Classes of Relations

▶ Some important classes of relations are defined in terms of these properties.

  ▶ Equivalence relation: reflexive, symmetric, transitive
  ▶ Partial order: reflexive, antisymmetric, transitive
  ▶ Strict order: irreflexive, asymmetric, transitive
  ▶ . . .

▶ We will consider these and other classes in detail.

Discrete Mathematics in Computer Science
B3. Equivalence and Order Relations

Malte Helmert, Gabriele Röger

University of Basel

October 6/8, 2025

B3.1 Equivalence Relations

B3.2 Order Relations

B3.1 Equivalence Relations

Motivation

▶ Think of any attribute that two objects can have in common,
  e. g. their color.

▶ We could place the objects into distinct "buckets",
  e. g. one bucket for each color.

▶ We also can define a relation $\sim$ such that $x \sim y$ iff
  x and y share the attribute, e. g.have the same color.

▶ Would this relation be
  ▶ reflexive?
  ▶ irreflexive?
  ▶ symmetric?
  ▶ asymmetric?
  ▶ antisymmetric?
  ▶ transitive?

Equivalence Relation

Definition (Equivalence Relation)
A binary relation $\sim$ over set S is an equivalence relation
if $\sim$ is reflexive, symmetric and transitive.

Examples:

- $\{(x, y) \mid x \text{ and } y \text{ have the same place of origin}\}$
  over the set of all Swiss citizens

- $\{(x, y) \mid x \text{ and } y \text{ have the same parity}\}$ over $\mathbb{N}_0$

- $\{(1, 1), (1, 4), (1, 5), (4, 1), (4, 4), (4, 5), (5, 1), (5, 4), (5, 5),$
  $(2, 2), (2, 3), (3, 2), (3, 3)\}$ over $\{1, 2, \ldots, 5\}$

Is this definition indeed what we want?
Does it allow us to partition the objects into buckets
(e. g. one "bucket" for all objects that share a specific color)?

German: Äquivalenzrelation

Equivalence Classes

> ### Definition (Equivalence Class)
> Let $\sim$ be an equivalence relation over set S.
>
> For any $x \in S$, the equivalence class of x is the set
>
> $$[x]_\sim = \{y \in S \mid x \sim y\}.$$

Consider
$$\sim = \{(1, 1), (1, 4), (1, 5), (4, 1), (4, 4), (4, 5), (5, 1), (5, 4), (5, 5),$$
$$(2, 2), (2, 3), (3, 2), (3, 3)\}$$
over set $\{1, 2, \ldots, 5\}$.

$[4]_\sim =$

German: Äquivalenzklasse

Equivalence Classes: Properties

Let $\sim$ be an equivalence relation over set S and
$E = \{[x]_\sim \mid x \in S\}$ the set of all equivalence classes.

- ▶ Every element of S is in some equivalence class in E.
- ▶ Every element of S is in at most one equivalence class in E.
  $\rightsquigarrow$ homework assignment

$\Rightarrow$ Equivalence relations induce partitions
(not covered in this course).

B3.2 Order Relations

Order Relations

▶ We now consider other combinations of properties,
  that allow us to describe a consistent order of the objects.

▶ "Number x is not larger than number y."
  "Set S is a subset of set T."
  "Jerry runs at least as fast as Tom."
  "Pasta tastes better than Potatoes."

German: Ordnungsrelation

Partial Orders

- ▶ We begin with partial orders.
- ▶ Example partial order relations are $\leq$ over $\mathbb{N}_0$ or $\subseteq$ for sets.
- ▶ Are these relations
  - ▶ reflexive?
  - ▶ irreflexive?
  - ▶ symmetric?
  - ▶ asymmetric?
  - ▶ antisymmetric?
  - ▶ transitive?

Partial Orders – Definition

> **Definition (Partial order)**
>
> A binary relation $\preceq$ over set S is a partial order
> if $\preceq$ is reflexive, antisymmetric and transitive.

Which of these relations are partial orders?

- strict subset relation $\subset$ for sets
- not-less-than relation $\geq$ over $\mathbb{N}_0$
- $R = \{(a, a), (a, b), (b, b), (b, c), (c, c)\}$ over $\{a, b, c\}$

German: Halbordnung oder partielle Ordnung

Least and Greatest Element

> **Definition (Least and greatest element)**
>
> Let $\preceq$ be a partial order over set S.
>
> An element $x \in S$ is the least element of S
> if for all $y \in S$ it holds that $x \preceq y$.
>
> It is the greatest element of S if for all $y \in S$, $y \preceq x$.

- ▶ Is there a least/greatest element? Which one?
    - ▶ $S = \{1, 2, 3\}$ and $\preceq = \{(x, y) \mid x, y \in S \text{ and } x \leq y\}$
    - ▶ relation $\leq$ over $\mathbb{N}_0$
    - ▶ relation $\leq$ over $\mathbb{Z}$
- ▶ Why can we say the least element instead of a least element?

German: kleinstes/grösstes Element

Uniqueness of Least Element

Theorem
Let $\preceq$ be a partial order over set S.
If S contains a least element, it contains exactly one least element.

Proof.
By contradiction: Assume x, y are least elements of S with $x \neq y$.
Since x is a least element, $x \preceq y$ is true.
Since y is a least element, $y \preceq x$ is true.
As a partial order is antisymmetric, this implies that $x = y$. $\notlightning$ $\quad\square$

Analogously: If there is a greatest element then is unique.

Minimal and Maximal Elements

> **Definition (Minimal/Maximal element of a set)**
>
> Let $\preceq$ be a partial order over set S.
> An element $x \in S$ is a minimal element of S
> if there is no $y \in S$ with $y \preceq x$ and $x \neq y$.
>
> An element $x \in S$ is a maximal element of S
> if there is no $y \in S$ with $x \preceq y$ and $x \neq y$.

A set can have several minimal elements and no least element.
Example?

German: minimales/maximales Element

Total Orders

- Relations $\leq$ over $\mathbb{N}_0$ and $\subseteq$ for sets are partial orders.
- Can we compare every object against every object?
    - For all $x, y \in \mathbb{N}_0$ it holds that $x \leq y$ or that $y \leq x$ (or both).
    - $\{1, 2\} \nsubseteq \{2, 3\}$ and $\{2, 3\} \nsubseteq \{1, 2\}$
- Relation $\leq$ is a total order, relation $\subseteq$ is not.

Total Order – Definition

Definition (Total relation)
A binary relation R over set S is total
if for all $x, y \in S$ at least one of xRy or yRx is true.

Definition (Total order)
A binary relation is a total order if it is total and a partial order.

German: totale Relation, (schwache) Totalordnung oder totale Ordnung

Strict Orders

▶ A partial order is reflexive, antisymmetric and transitive.
▶ We now consider strict orders.
▶ Example strict order relations are $<$ over $\mathbb{N}_0$ or $\subset$ for sets.
▶ Are these relations
  ▶ reflexive?
  ▶ irreflexive?
  ▶ symmetric?
  ▶ asymmetric?
  ▶ antisymmetric?
  ▶ transitive?

Strict Orders – Definition

> **Definition (Strict (partial) order)**
>
> A binary relation $\prec$ over set S is a **strict (partial) order**
> if $\prec$ is **irreflexive, asymmetric and transitive**.

Which of these relations are strict orders?

- ▶ subset relation $\subseteq$ for sets
- ▶ strict superset relation $\supset$ for sets

Can a relation be both, a partial order and a strict (partial) order?

We can omit irreflexivity or asymmetry from the definition
(but not both). Why?

German: strenge (Halb-)ordnung

Strict Total Orders

▶ As partial orders, a strict order does not automatically
   allow us to rank arbitrary two objects against each other.

▶ Example 1 (personal preferences):
   ▶ "Pasta tastes better than potato."
   ▶ "Rice tastes better than bread."
   ▶ "Bread tastes better than potato."
   ▶ "Rice tastes better than potato."

   ▶ This definition of "tastes better than" is a strict order.
   ▶ No ranking of pasta against rice or of pasta against bread.
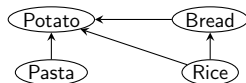
▶ Example 2: ⊂ relation for sets

▶ It doesn't work to simply require that the strict order is total.
   Why?

Strict Total Orders – Definition

> **Definition (Trichotomy)**
> A binary relation R over set S is trichotomous if for all $x, y \in S$ exactly one of xRy, yRx or $x = y$ is true.

> **Definition (Strict total order)**
> A binary relation $\prec$ over S is a strict total order if $\prec$ is trichotomous and a strict order.

A strict total order completely ranks the elements of set S.

Example: $<$ relation over $\mathbb{N}_0$ gives the standard ordering
$0, 1, 2, 3, \ldots$ of natural numbers.

Attention: a non-empty strict total order is never a total order.

German: trichotom, strenge Totalordnung

Special Elements

Special elements are defined almost as for partial orders:

Definition (Least/greatest/minimal/maximal element of a set)

Let $\prec$ be a strict order over set S.

An element $x \in S$ is the least element of S
if for all $y \in S$ where $y \neq x$ it holds that $x \prec y$.

It is the greatest element of S if for all $y \in S$ where $y \neq x$, $y \prec x$.

Element $x \in S$ is a minimal element of S
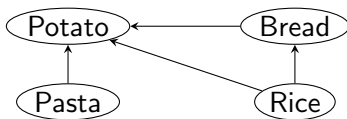if there is no $y \in S$ with $y \prec x$.

It is a maximal element of S
if there is no $y \in S$ with $x \prec y$.

Special Elements – Example

Consider again the previous example:

$S = \{\text{Pasta}, \text{Potato}, \text{Bread}, \text{Rice}\}$
$\prec = \{(\text{Pasta}, \text{Potato}), (\text{Bread}, \text{Potato}),$
$\qquad (\text{Rice}, \text{Potato}), (\text{Rice}, \text{Bread})\}$

Is there a least and a greatest element?
Which elements are maximal or minimal?

Summary

- An equivalence relation is reflexive, symmetric and transitive.
- A partial order $x \preceq y$ is reflexive, antisymmetric and transitive.
  - If x is the greatest element of a set S, it is greater than every element: for all $y \in S$ it holds that $y \preceq x$.
  - If x is a maximal element of set S then it is not smaller than any other element y: there is no $y \in S$ with $x \preceq y$ and $x \neq y$.
  - A total order is a partial order without incomparable objects.
- A strict order is irreflexive, asymmetric and transitive.
  - Strict total orders and special elements are analogously defined as for partial orders but with a special treatment of equal elements.