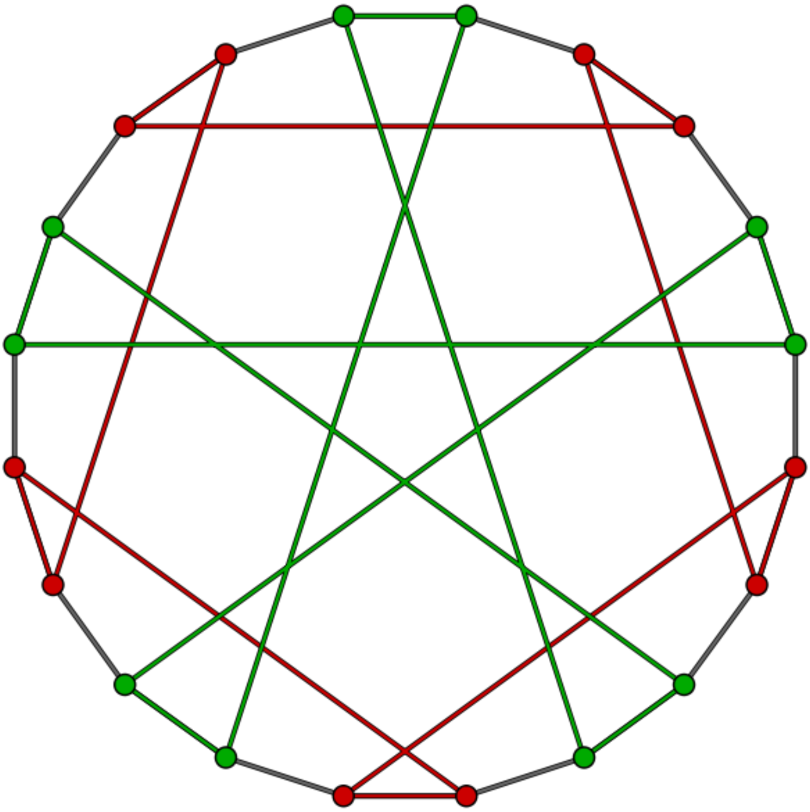
THEORETICAL COMPUTER SCIENCE

DISCRETE STRUCTURES FOR COMPUTER SCIENCE STUDENTS



UP FAMNIT

Spring 2021 – Version 0.1

CIP – Kataložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

123.4(567)(8.901.2)

TEORETIČNE osnove računalništva [Elektronski vir] : Diskretne strukture za računalničarje / avtorji M. Krnc, M. Milanič, R. Požar, N. Prijatelj, P. Škraba; [urednik] M. Krnc. - Version 0.1. - El. knjiga. - Ljubljana : samozal. M. Krnc, 2020.

Način dostopa (URL):
https://github.com/mkrnc/TCS1-course-notes.git

ISBN 978-961-XXX-XXX-X (pdf)
1. Milanič, Martin 2. Krnc, Matjaž, 1987- 123456789

PREFACE

Those are lecture notes for the course Theoretical Computer Science I, given to freshmen students at FAMNIT, University of Primorska. Ever since 2017 when I started teaching this course, those notes have been changing to accommodate the needs of computer science students. Since 2020 I decided to make this TeX project public, so that every student was able to suggest improvements and new exercises (or solutions) to be added to those course notes.

Those notes are supposed to be parsed together with explanations from the lectures. Any questions or found errors should be raised as an issue in our public repository

`https://github.com/mkrnc/TCS1-course-notes.git`.

Those notes are non-trivially based on some notes of my predecessors of this course, most notably

prof. **M. Milanič**, prof. **N. Prijatelj**, and prof. **P. Škraba**.

Theoretical Computer Science
Discrete Structures for Computer Science Students

Avtorji:	M. Krnc, M. Milanič, R. Požar, N. Prijatelj, P. Škraba
Urednik:	Matjaž Krnc
Fotografija na naslovnici:	R. A. Nonenmacher *Desargues Graph*
Samozaložba in oblikovanje:	Matjaž Krnc
ISBN:	978-961-XXX-XXX-X

Ljubljana, Spring 2021

CONTENTS

1 MATHEMATICAL LOGIC

1.1 PROPOSITIONS

A proposition is an affirmative statement that is either true or false.

- We won't be interested in natural language statements that are not affirmative (they are not a subject of logic).

  Examples of statements which are not propositions:

  - Will it rain tomorrow?
  - Good luck with your exam!
  - Do your homework!

- The internal structure of propositions is not important for logic.

  For logic, the following two propositions are the same:

  - "Shakespeare wrote the play Hamlet."
  - "Hamlet is a play written by Shakespeare."

- We assume that the meaning of logical connectives is well defined (which is not always the case in natural language).

- Some propositions are logical consequences of others. **Example:**

  - (P) All children in our kindergarten are boys and some children in our kindergarten are disobedient.
  - (C) Some boys are disobedient.

  If proposition (P) is true, then also proposition (C) is true.

The contribution of logic to the knowledge is the discovery of new propositions that are logical consequences of others.

- The whole theory of numbers can be built from 5 basic propositions called Peano axioms. In fact, using the work "and", all these five propositions can be connected into a single one.
- Hilbert showed that all we need to prove geometric theorems are 20 basic axioms.
- Mathematical structures are typically defined by a handful of axioms from which, using logical inference, theorems are proved and theories are built.

1.2 BASIC LOGICAL CONNECTIVES

We can connect arbitrary propositions with each other, independently of their meaning and internal structure.

Example:
"Paris is the capital of France or 2 *times* 2 *is* 5*."*
"The snow is white or the snow is black."
"If today there is sunny weather, then Paris is the capital of France."

The only restriction is that the correctness (truth value) of the derived proposition must be uniquely determined by the correctness of all the propositions, from which it is composed.

Example of a proposition that is not valid for logic:
"Janez died, because he was a heavy smoker."

We cannot infer the correctness of this proposition solely based on the correctness of its two parts. Even if Janez was a heavy smoker, it is not necessary that he died because of it.

NEGATION: NOT A; IT IS NOT TRUE THAT A

$\neg A$ is a negation of proposition A. Proposition $\neg A$ is true if A is false, and false if A is true.

Example: *It will be raining tomorrow. Negation: It won't be raining tomorrow. (It is not true that it will be raining tomorrow.)*

CONJUNCTION: A AND B

$A \wedge B$ is a conjunction of propositions A and B. This compound proposition is true when both propositions A and B are true, and false otherwise.

Example: *The wind blows. It is snowing. Conjunction: The wind blows and it is snowing.*

DISJUNCTION: A OR B

$A \vee B$ is the disjunction of propositions A and B. This compound proposition is true as soon as one of the propositions A and B is true, and false otherwise.

Example: *Tomorrow Janez will be asked physics. Tomorrow Janez will be asked mathematics. Disjunction: Tomorrow Janez will be asked physics or mathematics.*

Remark (about the differences between the natural and logical language):

1. In the natural language the word "or" often has *exclusive* meaning. Example: *"Janez was born in the year 1959 or in the year 1960."* In logic, we focus on the wider, inclusive meaning.

2. In the natural language we use the disjunction when we are convinced that one of the two propositions is certainly correct, only we do not know which of the two.

Example: Consider the disjunction of the propositions *"Marko has a bike."* and *"Marko has a car."* , that is, the proposition *"Marko has a bike or a car."* If, for example, we know that the first statement is true and the second one false, we would simply say *" Marko has a bike. "* , if we knew that both are true, we would say *" Marko has a bike and a car. "* , but if we knew that both are false, we would say *" Marko has neither a bike nor a car."*

In logic, this is not so. For example, we find the following proposition completely acceptable:

"2 *times* 2 *is* 5 *or* 2 *times* 2 *is* 6."

IMPLICATION: IF A, THEN B

$A \Rightarrow B$ is the implication of propositions A and B. This compound proposition is false if A is true and B is false, and true in all other cases.

A - antecedent, sufficient condition

B - consequent, necessary condition

Example: *If Andrej passes the final exam, I will buy him a bike..*

EQUIVALENCE: *A* **IF AND ONLY IF** *B* $A \Leftrightarrow B$ is the equivalence of propositions A and B. This compound proposition is true if propositions A and B are either both true or both false. In all other cases, it is false.

Read "$A \Leftrightarrow B$" as:

A if and only if B

A when and only when B

Example: *I will buy a bike for Andrej, if and only if he passes the final exam.*

1.3 TRUTH TABLES

The value of each compound proposition is uniquely determined by the values of the propositions that appear in it. For an explicit representation of this dependence we use the so-called *truth tables*.

We will denote the value *true* by 1, and the value *false* by 0. This gives the truth tables described in Table 1 and Table 2.

	A	$\neg A$
1.	1	0
2.	0	1

Table 1: Truth table of negation.

In general, any proposition consisting of basic propositions $A_1, \ldots, A_n$, can be written as the result of successive uses of the 5 basic connectives on the propositions $A_1, \ldots, A_n$ as well as on the already constructed propositions.

EXAMPLE: Let A, B, C be the basic propositions and consider the following sequence of propositions:

	A, B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
1.	1, 1	1	1	1	1
2.	1, 0	0	1	0	0
3.	0, 1	0	1	1	0
4.	0, 0	0	0	1	1

Table 2: Truth table of Conjunction, disjunction, implication and equivalence.

1. $(A \Rightarrow B)$
2. $(B \Rightarrow C)$
3. $(A \Rightarrow B) \wedge (B \Rightarrow C)$
4. $(\neg A)$
5. $((\neg A) \vee C)$
6. $(((A \Rightarrow B) \wedge (B \Rightarrow C)) \wedge ((\neg A) \vee C)))$

Every such finite sequence determines a compound proposition corresponding to the last term of the sequence.

Truth tables can also be written for compound propositions, using an arbitrary sequence of building it. Let us illustrate on the above example.

	A, B, C	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$\neg A$	$\neg A \vee C$	(2)
1.	1, 1, 1	1	1	1	0	1	1
2.	1, 1, 0	1	0	0	0	0	0
3.	1, 0, 1	0	1	0	0	1	0
4.	1, 0, 0	0	1	0	0	0	0
5.	0, 1, 1	1	1	1	1	1	1
6.	0, 1, 0	1	0	0	1	1	0
7.	0, 0, 1	1	1	1	1	1	1
8.	0, 0, 0	1	1	1	1	1	1

Parentheses convention

Doubts about which connective comes earlier and which later can be avoided by using parentheses. Consider again our proposition:

$$(((A \Rightarrow B) \wedge (B \Rightarrow C)) \wedge ((\neg A) \vee C))) \tag{1}$$

The use of parentheses is obvious: without them, we would obtain a confused proposition

$$A \Rightarrow B \wedge B \Rightarrow C \wedge \neg A \vee C\,.$$

We limit as much as possible the use of parentheses using the following convention:

- When a proposition appears on its own, we don't use parentheses:

  e.g.: instead of $(A \wedge B)$ we write $A \wedge B$

- When the same type of connective appears several times in a row, we consider it in order from left to right.

  e.g.: instead of $((A \wedge B) \wedge C) \wedge D$ we write $A \wedge B \wedge C \wedge D$

- We impose the following priority order on the connectives: $\neg$, $\vee$, $\wedge$, $\Rightarrow$, $\Leftrightarrow$ (in every compound proposition we first use negations, then disjunctions, etc.)

  e.g.: instead of $(A \wedge B) \Rightarrow (\neg C)$ we write $A \wedge B \Rightarrow \neg C$

Using the above convention, we can write proposition (1) more clearly as

$$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C) \tag{2}$$

Knights and servants

Using truth tables we can solve problems about knights and servants. Knights are always telling the truth, while servants always lie.

EXAMPLE: Arthur and Bine say the following:

- Arthur: “Bine is a servant."
- Bine: “Neither of us is a servant."

For each of them determine whether they are knights or servants!

Let A be the proposition: “Arthur is a knight," and B the proposition: “Bine is a knight."

Let us determine the validity of propositions A and B with the help of a truth table. From Arthur's statement we can infer that the following proposition is true: $A \Leftrightarrow \neg B$. From Bine's statement we can infer that the following proposition is true: $B \Leftrightarrow A \wedge B$. Hence, the conjunction of these two propositions is true:

$$(A \Leftrightarrow \neg B) \wedge (B \Leftrightarrow A \wedge B)\,.$$

Which truth assignment makes this proposition true?

A	B	$\neg B$	$A \Leftrightarrow \neg B$	$A \wedge B$	$B \Leftrightarrow A \wedge B$	$(A \Leftrightarrow \neg B)$ $\wedge$ $(B \Leftrightarrow A \wedge B)$
1	1	0	0	1	1	0
1	0	1	1	0	1	1
0	1	0	1	0	0	0
0	0	1	0	0	1	0

Arthur is a knight, while Bine is a servant. □

The following conjunction is true:

$$\begin{aligned}&[A \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)] \wedge \\ &\qquad\qquad [B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)]\,. \end{aligned} \tag{3}$$

A	B	$A \wedge \neg B$ $\sim C$	$\neg A \wedge B$ $\sim D$	$C \vee D$ $\sim E$	$B \Leftrightarrow E$	$A \Leftrightarrow E$	(3)
1	1	0	0	0	0	0	0
1	0	1	0	1	1	0	0
0	1	0	1	1	0	1	0
0	0	0	0	0	1	1	1

Both are servants. □

We have seen how to assign a truth table to each compound proposition. Now let us consider the opposite task: Given n independent propositions $A_1, \ldots, A_n$, how can we construct a compound proposition, that will have a given truth value for each of the 2^n truth assignments?

Before we can solve this problem, let us have a look at the so-called *logical equivalences*.

Some special names:

Let A be a proposition, composed of basic propositions $A_1, \ldots, A_n$.

- *Truth assignment of A*: assignment of values 1 / 0 (true / false) to each of the propositions $A_1, \ldots, A_n$
- *Assignment space of A*: all possible truth assignments of A

  If a proposition is composed of n basic propositions then the space of A consists of 2^n truth assignments.
- *Truth subspace of A*: assignments for which the proposition is true.
- Two kinds of propositions deserve special names:
  - *Tautology*: a proposition that is always true (example: $A \lor \neg A$), its truth subspace coincides with the whole assignment space
  - *Contradiction*: a proposition that is always false (example: $A \land \neg A$), its truth subspace is empty

1.4 LOGICAL EQUIVALENCES

Consider two propositions B and C, composed of propositions $A_1, \ldots, A_n$. Clearly, the proposition $B \Leftrightarrow C$ is a tautology if and only if B and C have the same truth subspace. If this is the case, we say that B and C are *logically equivalent*. For logic: $B = C$ (two different forms of the same proposition).

Let us list the most important logical equivalences:

1. The law of double negation:
   $A \Leftrightarrow \neg(\neg A)$,

2. Commutativity of conjunction and disjunction:
   $A \wedge B \Leftrightarrow B \wedge A$,
   $A \vee B \Leftrightarrow B \vee A$,

3. Associativity laws:
   $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$,
   $A \vee (B \vee C) \Leftrightarrow (A \vee B) \vee C$,

4. Distributivity laws:
   $A \vee (B \wedge C) \Leftrightarrow A \vee B \wedge A \vee C$,
   $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$,

5. $A \wedge A \Leftrightarrow A, \quad A \vee A \Leftrightarrow A$

6. De Morgan's laws:
   $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
   $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$,

7. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$

8. $(A \Rightarrow B) \Leftrightarrow \neg A \vee B$

9. $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$

10. $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$

11. Commutativity of equivalence:
    $(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$,

12. $(A \Leftrightarrow B) \Leftrightarrow (\neg A \Leftrightarrow \neg B)$

13. $(A \Leftrightarrow B) \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$

14. $(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$

15. $\neg(A \Leftrightarrow B) \Leftrightarrow (A \Leftrightarrow \neg B)$

As an exercise, let us verify the validity of 16. equivalence using a truth table:

	A, B	$A \Leftrightarrow B$	$\neg(A \Leftrightarrow B)$	$\neg B$	$A \Leftrightarrow \neg B$
1.	1, 1	1	0	0	0
2.	1, 0	0	1	1	1
3.	0, 1	0	1	0	1
4.	0, 0	1	0	1	0

Homework: Using truth tables (or by some other means), verify the valididty of the remaining equivalences.

With the help of the above logical equivalences, we can verify that the 5 basic logical connectives are not mutually independent. In fact, it is possible to express any compound propoisition with only *two (properly chosen) basic connectives*. The following pairs suffice:

(a) negation $\neg$ and disjunction $\vee$

(b) negation $\neg$ and conjunction $\wedge$

(c) negation $\neg$ and implication $\Rightarrow$

This choices are the only possible ones.

Example:
Consider the proposition: "If a thing is beautiful, then it is transient."
($\neg$ and $\vee$) A thing is either not beautiful, or it is transient.
($\neg$ and $\wedge$) It is not true that some thing is beautiful and not transient.
($\neg$ and $\Rightarrow$) If a thing is not transient, then it is not beautiful.

1.5 CANONICAL FORMS OF PROPOSITIONS

We owe the solution to the following task:

From n given propositions $A_1, \ldots, A_n$, construct a compound proposition that will have a given truth value for each of the 2^n truth assignments. We will examine two ways of doing this.

1st approach: To every assignment d for the propositions $A_1, \dots, A_n$, associate the conjunction

$$C_1 \wedge \dots \wedge C_n$$

in the following way: we have $C_i = A_i$, if A_i takes value 1 in d, and $C_i = \neg A_i$, otherwise. The so obtained conjunction is true only for the assignment d, and false for all other assignments. It is called *the basic conjunction of assignment d* (also: minterm).

Now, let us take the basic conjunctions for precisely those assignments for which the sought proposition should be true, and connect them disjunctively!

The so obtained proposition is called the *canonical disjunctive normal form (DNF).*

This approach works always, except in the case of a contradiction! In this case we construct the proposition separately, for example we can take $A_1 \wedge \neg A_1$.

2nd approach: d - assignment

Now let us for the *basic disjunction of assignment d* (maxterm):

$$D_1 \vee \cdots \vee D_n \,,$$

where

$D_i = \neg A_i$, if A_i takes value 1 in d

$D_i = A_i$, if A_i takes value 0 in d.

The so obtained disjunction is false at d, and true for all other assignments.

Let us take the basic disjunctions of precisely those assignemnts, for which the sought proposition should be false, and connect them conjunctively.

The so obtained proposition is called the *canonical conjuctive normal form (CNF).*

This approach works always, except in the case of a tautology! In this case we construct the proposition separately, for example we can take $A_1 \vee \neg A_1$ ("the law of the excluded third", every proposition is either true or false).

Example: We are looking for a proposition D, composed of propositions A, B and C, for which the following holds:

A	B	C	D	basic conjunction	basic disjunction
1	1	1	1	$A \wedge B \wedge C$	
1	1	0	0		$\neg A \vee \neg B \vee C$
1	0	1	0		$\neg A \vee B \vee \neg C$
1	0	0	0		$\neg A \vee B \vee C$
0	1	1	1	$\neg A \wedge B \wedge C$	
0	1	0	0		$A \vee \neg B \vee C$
0	0	1	1	$\neg A \wedge \neg B \wedge C$	
0	0	0	1	$\neg A \wedge \neg B \wedge \neg C$	

The canonical DNF of D is

$$\begin{aligned}(A \wedge B \wedge C) \vee (\neg A \wedge B \wedge C)\\ \vee (\neg A \wedge \neg B \wedge C) \vee (\neg A \wedge \neg B \wedge \neg C).\end{aligned}$$

The canonical CNF of D is

$$\begin{aligned}(\neg A \vee \neg B \vee C) \wedge (\neg A \vee B \vee \neg C)\\ \wedge (\neg A \vee B \vee C) \wedge (A \vee \neg B \vee C).\end{aligned}$$

□

EXAMPLE. Suppose you were caught by cannibals in Africa. Their chief is characterized by an extraordinary sense of humor and a love of logic. Therefore, he puts you in the dungeon with two exits and says: " One exit out of jail leads directly to the cooking pot, and the other into the liberty. Think about it and choose! To make your choice easier, two of my brave warriors will be put next to the exits. You are only allowed to ask a single yes or no question to one of them. But be careful! One of them always speaks the truth, while the other one is constantly lying."

Situation is not easy, but using logic you can avoid the pot. Which question will you ask?

Let A be the proposition: "The first exit leads to freedom."

Let B be the proposition: "You speak the truth."

From these two propositions one must come up with a proposition such that answer "yes" to it will mean that proposition A is true, answer "no" will mean that proposition A is false, and this should hold independently which of the two warriors is asked. Let us denote the sought proposition by C. Then the following should hold:

A	B	C	basic conjunction	basic disjunction
1	1	1	$A \wedge B$	
1	0	0		$\neg A \vee B$
0	1	0		$A \vee \neg B$
0	0	1	$\neg A \wedge \neg B$	

The canonical DNF of C is

$$(A \wedge B) \vee (\neg A \wedge \neg B),$$

and its canonical CNF is:

$$(\neg A \vee B) \wedge (A \vee \neg B).$$

We can ask the question in a simpler form by noticing that both propositions are logically equivalent with the proposition

$$A \Leftrightarrow B.$$

We approach one of the two soldiers and ask him: "Is it true that the first exit leads to freedom if and only if you speak the truth?" §

1.6 SWITCHING CIRCUITS

We can model logical propositions with so-called switching circuits.

A switching circuit is a system of wires and switches connecting two given points, between which there is electric voltage.

Every switch is either "closed" (if electrical current flows through it) or "open" (otherwise).

Suppose that we have such a circuit and we know which switches are open and which ones are closed. We would like to determine whether the

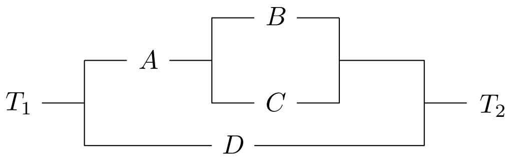
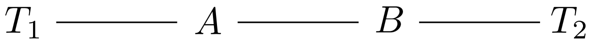


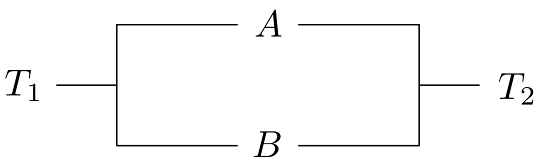
Figure 1: An example of a circuit with four switches

whole circuit is "closed" (that is, admits the flow of current) or "open" (no current).

First, let us consider two very simple circuits:
(1) *two switches connected in series:*



A series circuit is closed if and only if both switches are closed: **conjunction**.
(2) *two switches connected in parallel:*



A parallel circuit is closed if and only if at least one of the two switches is closed: **disjunction**.

To every such circuit we can associate a logical proposition, composed of propositions corresponding to switches.

And conversely: by means of *identical* and *opposite* switches we can represent every compound proposition with a circuit!
A pair of switches are said to be identical if they are either simultaneously both open or both closed.
A pair of switches are said to be opposite if exactly one of them is open.

The following connection between propositions and switches holds: *a circuit is closed if and only if the corresponding proposition is true, and open otherwise.*

EXAMPLE. Consider the following proposition:

$$(A \Rightarrow B) \land (B \Rightarrow C) \land (\neg A \lor C)$$

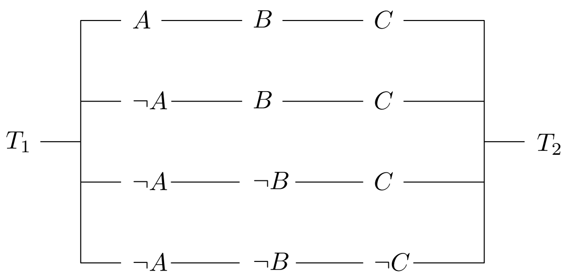
We computed its truth table in Chapter 1.2:

	A	B	C	$(A \Rightarrow B) \land (B \Rightarrow C) \land (\neg A \lor C)$
1.	1	1	1	1
2.	1	1	0	0
3.	1	0	1	0
4.	1	0	0	0
5.	0	1	1	1
6.	0	1	0	0
7.	0	0	1	1
8.	0	0	0	1

In the previous chapter we wrote this proposition in its canonical DNF as:

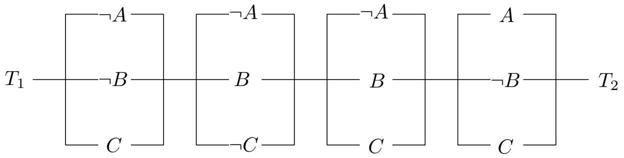
$$(A \land B \land C) \lor (\neg A \land B \land C) \lor (\neg A \land \neg B \land C) \lor (\neg A \land \neg B \land \neg C).$$

This form corresponds to the following circuit:



On the other hand, the canonical CNF

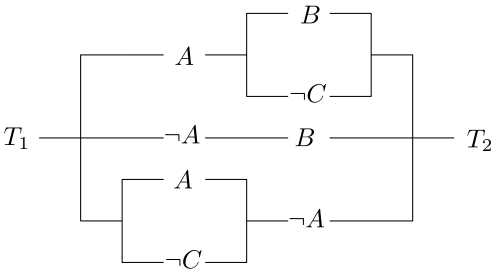
$$(\neg A \lor \neg B \lor C) \land (\neg A \lor B \lor \neg C) \land (\neg A \lor B \lor C) \land (A \lor \neg B \lor C)$$



corresponds to circuit

Therefore, a single proposition can be represented by more than one switching circuit. It is therefore reasonable to require that, in the actual physical construction of circuits simulating a given proposition, our goal is to find a circuit as simple as possible. Perhaps the circuit should also satisfy certain other requirements (depending on the application). We will not consider these issues here. §

EXAMPLE. Consider the following switching circuit:



For which switch positions is the circuit closed?

Let us solve the problem with logic.

The corresponding proposition, say D, is:

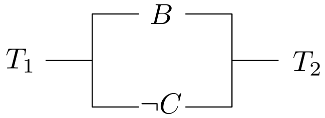
$$(A \wedge B \vee \neg C) \vee (\neg A \wedge B) \vee (A \vee \neg C \wedge \neg A).$$

Its truth table is:

	A	B	C	$A \land B \lor \neg C$	$\neg A \land B$	$A \lor \neg C \land \neg A$	D
1.	1	1	1	1	0	0	1
2.	1	1	0	1	0	0	1
3.	1	0	1	0	0	0	0
4.	1	0	0	1	0	0	1
5.	0	1	1	0	1	0	1
6.	0	1	0	0	1	1	1
7.	0	0	1	0	0	0	0
8.	0	0	0	0	0	1	1

We see that the circuit is open if and only if switch B is open and switch C is closed, and closed in all other cases.

Hence, we could replace the circuit with the following simpler one:



The same result could be derived in a purely logical way:

From the truth table, we read off the canonical CNF of D:

$$(\neg A \lor B \lor \neg C) \land (A \lor B \lor \neg C)\,.$$

Using distributivity, we see that this proposition is equivalent to the following one:

$$(\neg A \lor \quad \land A) \lor (B \lor \neg C)\,,$$

however, since the conjunction $\neg A \lor \quad \land A$ is always false, the above proposition is equivalent to the proposition

$$B \lor \neg C\,.$$

§

We conclude this chapter with a more practical example.

EXAMPLE. Consider a committee of 3 members voting about individual motions according to a certain voting rule. The task is to construct a switching circuit that would tell immediately whether the motion is accepted or not.

Let us consider the following two voting rules:

(a) the principle of simple majority

(b) the principle of simple majority, where member A has a right to veto

The truth table says:

A	B	C	(a)	(b)
1	1	1	1	1
1	1	0	1	1
1	0	1	1	1
1	0	0	0	0
0	1	1	1	0
0	1	0	0	0
0	0	1	0	0
0	0	0	0	0

The canonical DNF of the sought proposition in case (a) reads

$$(A \land B \land C) \lor (A \land B \land \neg C) \lor (A \land \neg B \land C) \lor (\neg A \land B \land C)$$

and in case (b)

$$(A \land B \land C) \lor (A \land B \land \neg C) \lor (A \land \neg B \land C).$$

The corresponding circuits are depicted on Figure 2. §

1.7 LOGICAL IMPLICATIONS

A *logical implication* is a tautology such that the main connective is an implication. It $B \Rightarrow C$ is a tautology, then the truth subspace of the antecedent (that is, proposition B) is contained in the truth subspace of the consequent (that is, proposition C). And conversely, if the truth subspace of the antecedent is contained in the truth subspace of the consequent, then $B \Rightarrow C$ is a tautology.

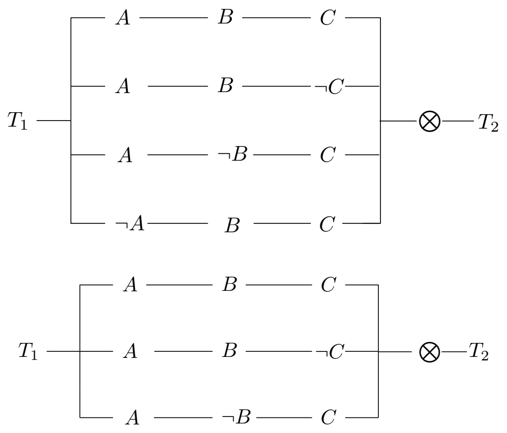


Figure 2: The corresponding circuits for the comittee (a) withouth a veto member (above), and (b) with veto for the member A (below).

Homework: Prove the statement that $B \Rightarrow C$ is a tautology if and only if the truth subspace of the antecedent is contained in the truth subspace of the consequent.

The following basic facts about logical implications hold:

1. If the antecedent is a tautology, then also the consequent is a tautology.
2. If the consequent is a contradiction, then also the antecedent is a contradiction.
3. If the consequent is a tautology, then the antecedent can be any proposition.
4. If the antecedent is a contradiction, then the consequent can be any proposition.
5. Every proposition logically implies itself.
6. Every proposition that logically implies both some proposition A and its negation $\neg A$, must be a contradiction.

7. Every proposition that logically implies its own negation, is a contradiction.

Some comments to the implications:

(1.) From the truthfulness of the antecedent and the truth of the implication we can infer the truth of the consequent.

- In classical logic this inference rule was called *mixed hypothetical syllogism*, namely *modus ponendo ponens* (lat. the way that affirmes by affirming).

EXAMPLE.

- If today is Monday, I will go to the lectures.
- Today is Monday.
- ○ **Conclusion:** I will go to the lectures. §

(2.) *mixed hypothetical syllogism modus tollendo tollens* (lat. the way that denies by denying)

Examples:

1. Where there is smoke, there is also fire.
Here there is no fire.
Conclusion: Here there is no smoke.
2. A person that is happy with little lives well.
A greedy person does not live well.
Conclusion: A greedy person is not happy with little.

(3.) *disjunctive syllogism modus tollendo ponens* (lat. the way that affirms by denying)

Example:

Koper is a country or it is a town.
Koper is not a country.
Conclusion: Koper is a town.

(4.) Simplification.

(5.) Addition.

(6.) From a contradiction an arbitrary proposition can be derived.

(7.) Transitivity of implication (so called *pure hypothetical syllogism*).

(12.) Transitivity of equivalence.
(19.) The rule of absurd.

Some important logical implications

1. $A \wedge (A \Rightarrow B) \Rightarrow B$
2. $\neg B \wedge (A \Rightarrow B) \Rightarrow \neg A$
3. $\neg A \wedge (A \vee B) \Rightarrow B$
4. $A \wedge B \Rightarrow A$
5. $A \Rightarrow A \vee B$
6. $A \wedge \neg A \Rightarrow B$
7. $(A \Rightarrow B) \wedge (B \Rightarrow C) \Rightarrow (A \Rightarrow C)$
8. $(A \Rightarrow B) \Rightarrow (C \Rightarrow A \Rightarrow (C \Rightarrow B))$
9. $(A \Rightarrow B) \Rightarrow (B \Rightarrow C \Rightarrow (A \Rightarrow C))$
10. $(A \Rightarrow B) \Rightarrow (A \wedge C \Rightarrow B \wedge C)$
11. $(A \Rightarrow B) \Rightarrow (A \vee C \Rightarrow B \vee C)$
12. $(A \Leftrightarrow B) \wedge (B \Leftrightarrow C) \Rightarrow (A \Leftrightarrow C)$
13. $(A \Leftrightarrow B) \Rightarrow (A \Rightarrow B)$
14. $(A \Leftrightarrow B) \Rightarrow (B \Rightarrow A)$
15. $A \wedge (A \Leftrightarrow B) \Rightarrow B$
16. $\neg A \wedge (A \Leftrightarrow B) \Rightarrow \neg B$
17. $B \Rightarrow (A \Leftrightarrow A \wedge B)$
18. $\neg B \Rightarrow (A \Leftrightarrow A \vee B)$
19. $(A \Rightarrow (B \wedge \neg B)) \Rightarrow \neg A$

As an exercise, convince yourself in the validity of these logical implications. Instead of truth tables, you may use the following method: *Starting from the definition of a logical implication, try to construct such a truth assignment for which the implication is false. Of course, it then has to turn out that such a truth assignment does not exist.*

EXAMPLE. Let us prove the 10th implication from the list:

$$A \Rightarrow B \Rightarrow (A \wedge C \Rightarrow B \wedge C)$$

This implication would only be false for a truth assignment for which the proposition $A \Rightarrow B$ would be true, while the proposition $A \wedge C \Rightarrow B \wedge C$ would be false. However, according to the definition of the implication, this is true only if the propositions A and C are true, while proposition B is false. In this case the implication $A \Rightarrow B$ is false, which contradicts the assumption that it is true. Therefore, an assignment for which the proposition $A \Rightarrow B$ would be true and the proposition $A \wedge C \Rightarrow B \wedge C$ false, does not exist. Implication 10 is indeed a tautology. §

1.8 PROOFS

Here we describe several types of proofs.

1.8.1 Direct proof

We would like to prove the truthfulness of logical implication $A \Rightarrow B$. We assume that proposition A is true, and directly derive the truthfulness of proposition B.

Example: If n is an odd natural number, then also n^2 is odd.

Proof: Let n be an odd natural number. Then we can write it as $n = 2k - 1$ for some natural number k. Therefore $n^2 = (2k-1)^2 = 4k^2 - 4k + 1 = 2(2k^2 - 2k) + 1$, hence n^2 is odd. □

1.8.2 Indirect proof.

We would like to prove the truthfulness of logical implication $A \Rightarrow B$. It is sometimes more convenient to prove instead equivalent implication $\neg B \Rightarrow \neg A$.

Example : If n^2 is even, then n is also even.

Proof: The proposition is equivalent to the implication:

If n is a number that is not even, then also n^2 is a number that is not even.

Equivalently: If n is odd, then also n^2 is odd.

But this we just proved. □

1.8.3 Proof by contradiction.

We would like to prove the truthfulness of proposition A. We assume that A is false and show that this assumption leads to a contradiction (which we denote by $\perp$). This way, we showed the truthfulness of the proposition $\neg A \Rightarrow \perp$. But this proposition is only true if proposition $\neg A$ is false. Hence A is true.

Example: $\sqrt{2}$ is not rational.

Proof: Suppose that $\sqrt{2}$ is a rational number. Then we can write it as $\sqrt{2} = p/q$, where p and q are two relatively prime natural numbers.

It follows that

$2 = p^2/q^2$.

$p^2 = 2q^2$.

Hence p^2 is even. Therefore (according to what we proved above) p is even.

Let us write $p = 2m$, where m is a natural number.

We obtain

$4m^2 = 2q^2$.

Thus $2m^2 = q^2$.

Hence, also q is even. This, however, is a contradiction. (We assumed that p and q are relatively prime numbers and showed that they are both divisible by 2.) □

1.8.4 Propositions with quantifiers

Quantifiers tell, for how many objects of some kind a given proposition is true. We will use the following notation:

- $(\forall x)A(x)$ ... for every x proposition $A(x)$ is true.
- $(\exists x)A(x)$ ... there exists an x such that proposition $A(x)$ is true.
- $(\exists! x)A(x)$ ... there exists a unique (that is, one and only one) x such that proposition $A(x)$ is true.

Examples:

- $(\forall$ natural numbers $n)$ $(n$ is divisible by 2).
- $(\exists n)$ $(n$ is a natural number and n is divisible by 2).
- $(\exists! n)$ $(n$ is the smallest natural number).

Negation of propositions with quantifiers

Negation $\forall$

$$\neg(\forall x)A(x) \;\Leftrightarrow\; (\exists x)(\neg A(x))$$

EXAMPLE. B: Every citizen of Slovenia is dark haired.

$\neg B$: It is not true that every citizen of Slovenia is dark haired.

Equivalently: There exists at least one citizen of Slovenia that is not dark haired. §

Negation $\exists$

$$\neg(\exists x)A(x) \;\Leftrightarrow\; (\forall x)\neg A(x)$$

EXAMPLE. B: There is a red ball in the box.

$\neg B$: It is not true that there is a red ball in the box.

Equivalently: For every ball in the box, it holds that it is not red. §

Negation $\exists!$

$$\neg(\exists! x)A(x) \;\Leftrightarrow\; (\forall x)(\neg A(x)) \;\vee\; (\exists x)(\exists y)(x \neq y \;\wedge\; A(x) \;\wedge\; A(y))$$

EXAMPLE. B: There exists a unique prime number.

$\neg B$: It is not true that there exists a unique prime number.

Equivalently: Either no number is prime, or there exists at least two different prime numbers. §

EXAMPLE. Is the following proposition correct?

There exists a real number x such that $\frac{1}{1+x^2} > 1$.

$$(\exists x)(\frac{1}{1+x^2} > 1)$$

No, the proposition is not true. We can check that its negation is true:

$$\neg(\exists x)(\frac{1}{1+x^2} > 1)$$

$$\Leftrightarrow \ (\forall x)\neg(\frac{1}{1+x^2} > 1)$$

$$\Leftrightarrow \ (\forall x)(\frac{1}{1+x^2} \leq 1)$$

$$\Leftrightarrow \ (\forall x)(1 \leq 1 + x^2)$$

$$\Leftrightarrow \ (\forall x)(0 \leq x^2)$$

Hence:

$$\neg \left(\exists \,\text{real number}\, x : \frac{1}{x^2+1} > 1 \right)$$

§

EXAMPLE. Let $P(x)$ denote the proposition "x is prime".

For every natural number x there exists a natural number y, bigger than x, that is a prime number: $(\forall x)(\exists y)(y > x \ \wedge \ P(y))$.

Negation:

$$\neg(\forall x)(\exists y)(y > x \ \wedge \ P(y)) \ \Leftrightarrow \ (\exists x)\neg(\exists y)(y > x \ \wedge \ P(y))$$

$$\Leftrightarrow \ (\exists x)(\forall y)\neg(y > x \ \wedge \ P(y)) \ \Leftrightarrow \ (\exists x)(\forall y)(y \leq x \ \vee \ \neg P(y))\,.$$

EXAMPLE. Let us write the negation of the proposition

$$(\forall x)(\exists y)(y < x)\,.$$

$$\neg(\forall x)(\exists y)(y < x)$$

$$\Leftrightarrow$$

$$(\exists x)(\neg(\exists y)(y < x))$$

$$\Leftrightarrow$$

$$(\exists x)(\forall y)\neg(y < x)$$

$$\Leftrightarrow$$

$$(\exists x)(\forall y)(y \geq x)$$

§

- Is the following proposition true in real numbers?

  $$(\forall x)(\exists y)(y < x)$$

  Yes, the proposition is true!

- Is it true in natural numbers?

  $$(\forall x)(\exists y)(y < x)$$

  No, its negation is true:

  $$(\exists x)(\forall y)(y \geq x)\,,$$

  since there exists a smallest natural number.

Inference of Propositions

name	assumption(s)	conclusion
modus ponens	$A, A \Rightarrow B$	B
modus tollens	$A \Rightarrow B, \neg B$	$\neg A$
hipotetični silogizem	$A \Rightarrow B, B \Rightarrow C$	$A \Rightarrow C$
disjunktivni silogizem	$A \vee B, \neg A$	B
združitev	A, B	$A \wedge B$
poenostavitev	$A \wedge B$	A
pridružitev	A	$A \vee B$

Example 1:

- I will go to the match.
- In the evening, I will do the homework.
- If I go to the match and then to the cinema, I will not have the time to do the homework.

Can I infer that I will not be able to go to the cinema?

Solution:
Let us define the following propositions:
A_1: I will go to the match.
A_2: In the evening, I will do the homework.
A_3: I will go to the cinema.
C_1: A_1
C_2: A_2
C_3: $A_1 \;\wedge\; A_3 \;\Rightarrow\; \neg A_2$.
We have to determine whether the implication

$$C_1 \;\wedge\; C_2 \;\wedge\; C_3 \;\Rightarrow\; \neg A_3$$

is a tautology.

Example 2
The following facts are given:

- This animal is not a bird, or it has wings.

- If this animal is a bird, then it lays eggs.

Is the following inference correct? *If this animal does not have wings, then it does not lay eggs.*

Solution:

Let us define the following propositions:
A_1: This animal is a bird.
A_2: This animal has wings.
A_3: This animal lays eggs.
C_1: $\neg A_1 \lor A_2$
C_2: $A_1 \Rightarrow A_3$
B: $\neg A_2 \Rightarrow \neg A_3$.
We have to determine whether the implication

$$C_1 \land C_2 \Rightarrow B$$

is a tautology.

1.8.5 Sets of propositions

We are given atomic propositions $A_1, \ldots, A_n$ (that is, propositions without any logical connectives).

How many different propositions can we built out of them?

It seems that infinitely many! However, for logic, two propositions are the same if they are logically equivalent.

There are only finitely many propositions that are pairwise logically non-equivalent!

The assignment space of every proposition composed of $A_1, \ldots, A_n$, consists of exactly 2^n different truth assignments. A proposition is uniquely defined (up to logical equivalence), as soon as we define its values for each of these 2^n truth assignments.

Every truth assignment takes one of the two values 0 and 1, independently of the others. Consequently, the number of possible propositions is $2^{(2^n)}$.

Let us examine the construction of all possible propositions for $n = 1$ and $n = 2$.

n = 1

We have only one atomic proposition A. From it, we can build $2^{(2^1)} = 4$ propositions, $C_1, \ldots, C_4$.

A	C_1	C_2	C_3	C_4
1	1	1	0	0
0	1	0	1	0

C_1 is the tautology, e.g. $A \lor \neg A$.

C_4 is the contradiction, e.g. $A \land \neg A$.

For C_2 we can take just A.

For C_3 we can take $\neg A$.

n = 2

We have two propositions, A and B. From them, we can build $2^{(2^2)} = 16$ propositions, $C_1, \ldots, C_{16}$.

A	B	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}	C_{16}
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

Of course, C_1 is the tautology, e.g., $A \lor \neg A$, and C_{16} is the contradiction $A \land \neg A$.

Propositions C_2, C_3, C_5 and C_9 are only false for one truth assignment, hence we can express them with the canonical CNF:

- $C_2 = A \lor B$
- $C_3 = A \lor \neg B$
- $C_5 = \neg A \lor B$
- $C_8 = \neg A \lor \neg B$

Similarly, the propositions C_8, C_{12}, C_{14} and C_{15} can be expressed with their canonical DNF:

- $C_8 = A \ \wedge \ B$
- $C_{12} = A \ \wedge \ \neg B$
- $C_{14} = \neg A \ \wedge \ B$
- $C_{15} = \neg A \ \wedge \ \neg B$

Each of the remaining propositions is true for two truth assignments, and also false for two truth assignments.

For C_4 we can take

$$(A \ \wedge \ B) \ \vee \ (A \ \wedge \ \neg B)\,,$$

which is equivalent to

$$A \ \wedge \ B \ \vee \ \neg B$$

and since the disjunction $B \ \vee \ \neg B$ is always true, proposition C_4 is equivalent to proposition A.

Similarly, we can verify that:

- proposition C_6 is equivalent to proposition B,
- proposition C_{11} is equivalent to proposition $\neg B$,
- proposition C_{13} is equivalent to proposition $\neg A$.

For C_7 let us write

$$(A \ \wedge \ B) \ \vee \ (\neg A \ \vee \ \neg B)\,,$$

which is equivalent to

$$A \ \Leftrightarrow \ B\,.$$

Similarly, for C_{10} we can take the equivalence

$$A \ \Leftrightarrow \ \neg B\,.$$

□

1.9 EXERCISES

1. The following two propositions are given: A: "Andrej speaks French." and B: "Andrej speaks Danish." Write the following compound propositions in natural language:

(a) $A \lor B$
(b) $A \land B$
(c) $A \land \neg B$
(d) $\neg A \lor \neg B$
(e) $\neg\neg A$
(f) $\neg(\neg A \land \neg B)$

2. The following two propositions are given: A: "Janez is rich." and B: "Janez is happy."

Write the following propositions symbolically:
(a) If Janez is rich, then he is unhappy.
(b) Janez is neither happy nor rich.
(c) Janez is happy only if he is poor.
(d) Janez is poor if and only if he is unhappy.

Exercise: Solve the following exercises about knights and servants:

- Arthur: "It is not true that Bine is a servant." Bine: "We are not both of the same kind."

- Arthur: "It is not true that Cene is servant." Bine: "Cene is a knight or I am a knight." Cene: "Bine is a servant."

A similar exercise: Now Arthur and Bine say the following:

- Arthur: "Me and Bine are not of the same kind."

- Bine: "Exactly one of us is a knight."

2 SET THEORY

2.1 SETS

Elements (objects): $a, b, \ldots, x, y, z$ (+ indices: a_6, x_1, z_λ)

Sets: $A, B, \ldots, X, Y, Z$ (+ indices)

$a \in F$: element a belongs to set F, a is an element of set F.

$\in$: symbol of containment

$a \notin F$: a is not an element of (does not belong to) set F.

Example: If G is the set of all even numbers, then $16 \in G$ and $3 \notin G$.

Equality of sets: Sets A and B are equal if and only if they have exactly the same objects as elements:

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

This definition is necessary, since it describes an important property that the containment relation must satisfy!

Example: Suppose that the objects under consideration are people, and let us write $x \in A$ if and only if x is an ancestor of A. Can we use this definition to define people as sets? The above equivalence says:

- *If two people are the same then they have the same ancestors.* This is true.
- *If two people have the same ancestors, then they are the same.* This however is not true!

A set can be given by a list of all its elements:

$$A = \left\{1, \frac{1}{2}, \frac{\pi}{3}, 2i + 8\right\} .$$

The order *is irrelevant!*

Sometimes such a description is impractical:

- If the set is infinite (e.g., the set of all prime numbers).
- If the set is finite but too large (e.g., the set of all books that were printed on Planet Earth until the year 2011),

A set can also be given by a description of it. The description must be unambiguous: for every object, it must hold that it either belongs to the set, or that it does not belong to the set.

Example: Let A be the set of all complex numbers x that are a solution of some equation of the form

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0\,,$$

where $n \in \mathbb{N}$ and $a_i \in \mathbb{Z}$ for all $i = 0, 1, \ldots, n$.

A - the set of all algebraic numbers.
Is $2^{\pi} \in A$? We do not know (contemporary mathematics cannot yet give an answer this question). □

In general, we can write:

$$A = \{x; P(x)\}\,,$$

set A is the set of all elements x such that proposition $P(x)$ is true. Or, if we have several propositions $P_1, \ldots, P_n$:

$$A = \{x; P_1(x) \ \wedge \ \cdots \ \wedge \ P_n(x)\}$$

$$A = \{x; P_1(x) \ \vee \ \cdots \ \vee \ P_n(x)\}$$

As we will see soon, we can build such sets only with elements of the sets that we already know (or for which we know that they exist).

Example: Let L be the set of all people. Propositions 'x is married" and "x is at least 20 years old" are meaningful for elements of the set L. Hence, we can construct sets

$$\{x \in L; x \text{ is married}\}$$

$$\{x \in L; x \text{ is married } \wedge \ x \text{ is at least 20 years old}\}$$

as well as (by negating the above conjunction)

$$\{x \in L; x \text{ is not married } \vee \ x \text{ is not at least 20 years old}\}$$

The set

$$\{x \in L; x \text{ is the current president of Republic of Slovenia}\}$$

contains only Borut Pahor and nothing else.

Be careful: a box that contains a hat is not the same thing as the hat. Similarly, the set $\{a\}$ is not the same thing as a. For every object a, it holds that $a \in \{a\}$.

2.2 EMPTY SET

We denote the set that has no elements with symbol $\emptyset$ — *empty set*.

$$X = \emptyset \iff (\forall x)(x \notin X)$$

Of course it holds that:

$$(\forall X)(\emptyset \subseteq X)$$

2.3 SUBSETS

We are given two sets A and B.

We say that A is a *subset* of B if and only if every element of A is also an element of B.

Notation: $A \subseteq B$

$$A \subseteq B \iff (\forall x)(x \in A \implies x \in B)$$

Of course, every set is a subset of itself:

$$(\forall A)(A \subseteq A)\,.$$

If $A \subseteq B$ and $A \neq B$, then A is a *proper subset* of set B: $A \subset B$.

$$A \subset B \iff (A \subseteq B \land A \neq B)$$

Clearly, it holds that:

- $A \subseteq B \ \wedge \ B \subseteq A \ \Leftrightarrow \ A = B$.

  This equivalence is extremely important for proving equality of two sets!

- $A \subseteq B \ \wedge \ B \subseteq C \ \Rightarrow \ A \subseteq C$ (transitivity of inclusion)

For our proof of equivalence $A \subseteq B \ \wedge \ B \subseteq A \ \Leftrightarrow \ A = B$, we will need the following equivalence:

$$(\forall x)(P(x) \ \wedge \ Q(x)) \ \Leftrightarrow \ (\forall x)P(x) \ \wedge \ (\forall x)Q(x)\,.$$

Proof:
($\Rightarrow$):
Proof by contradiction. Suppose that $(\forall x)(P(x) \ \wedge \ Q(x))$, while
$\neg((\forall x)P(x) \ \wedge \ (\forall x)Q(x))$.
Then: $\neg(\forall x)P(x) \ \vee \ \neg(\forall x)Q(x)$.
$(\exists x)\neg P(x) \ \vee \ (\exists x)\neg Q(x)$.
Independently of which of the propositions $(\exists x)\neg P(x)$ and $(\exists x)\neg Q(x)$ is true, we have a contradiction with proposition $(\forall x)(P(x) \ \wedge \ Q(x))$.
($\Leftarrow$):
Proof by contradiction. Suppose that $(\forall x)P(x) \ \wedge \ (\forall x)Q(x)$, while
$\neg(\forall x)(P(x) \ \wedge \ Q(x))$.
Then: $(\exists x)\neg(P(x) \ \wedge \ Q(x))$.
$(\exists x)(\neg P(x) \ \vee \ \neg Q(x))$.
Choose x such that $\neg P(x) \ \vee \ \neg Q(x)$.
Independently of which of the propositions $\neg P(x)$ and $\neg Q(x)$ is true, we have a contradiction with proposition $(\forall x)P(x) \ \wedge \ (\forall x)Q(x)$. □

Let us now prove the equivalence

$$A \subseteq B \ \wedge \ B \subseteq A \ \Leftrightarrow \ A = B \ :$$

$$A \subseteq B \ \wedge \ B \subseteq A$$

$$\Leftrightarrow$$

$$(\forall x)(x \in A \ \Rightarrow \ x \in B) \ \wedge \ (\forall x)(x \in B \ \Rightarrow \ x \in A)$$

$$\Leftrightarrow$$

$$(\forall x)((x \in A \;\Rightarrow\; x \in B) \;\wedge\; (x \in B \;\Rightarrow\; x \in A))$$

$$\Leftrightarrow$$

$$(\forall x)(x \in A \;\Leftrightarrow\; x \in B)$$

$$\Leftrightarrow$$

$$A = B\,.$$

□

Homework: prove the above implication (transitivity of inclusion).

A question: Do there exist two sets A and B such that $A \subset B$ and $B \subset A$?

Be careful: relation of inclusion $\subseteq$ and relation of containment $\in$ are two completely different notions!
$1 \in \{1, 2, 3\}$, but 1 is not a subset of the set $\{1, 2, 3\}$. Set $\{1\}$ is a subset of the set $\{1, 2, 3\}$, but $\{1\}$ is not an element of the set $\{1, 2, 3\}$.

Some questions: Let $X = \{1, 2, \{1\}, \{2\}\}$. Is 1 an element of X? Is 1 a subset of X? Is $\{1\}$ an element of X? Is $\{1\}$ a subset of X?

2.4 UNION

We are given two sets A and B. The *union* of these two sets is the set $A \cup B$, that has for elements precisely those objects that are elements of the set A or of the set B:

$$A \cup B = \{x; x \in A \;\vee\; x \in B\}\,.$$

Example: $A = \{1, 3, 5, 7\}$, $B = \{1, 2, 4, 8\}$.
$A \cup B = \{1, 3, 5, 7, 2, 4, 8\}$.

Union of several sets:
$\mathcal{A} = \{A_\lambda; \lambda \in J\}$ - union of sets with index set J
The index set can be an arbitrary set!
We define the union of an arbitrary family of sets as

$$\cup\mathcal{A} = \cup_{\lambda \in J} A_\lambda = \{x; (\exists\lambda)(\lambda \in J \;\wedge\; x \in A_\lambda)\}$$

Example: $J = \{1, 2\}$

$\cup_{\lambda \in \{1,2\}} A_\lambda = \{x; (\exists \lambda)(\lambda \in \{1,2\} \ \wedge \ x \in A_\lambda)\} = \{x; x \in A_1 \ \vee \ x \in A_2\} = A_1 \cup A_2 \,.$

If J is finite, we usually take $J = \{1, 2, \ldots, n\}$ and write

$$\cup \mathcal{A} = \cup_{j=1}^{n} A_j = A_1 \cup \cdots \cup A_n \,.$$

Basic properties of the union:

- $A \cup B = B \cup A$, commutativity
- $(A \cup B) \cup C = A \cup (B \cup C)$, associativity
- $A \cup A = A$, idempotency
- $A \cup \emptyset = A$
- $A \subseteq A \cup B$, $B \subseteq A \cup B$
- $A \subseteq B \ \Leftrightarrow \ A \cup B = B$
- $A \subseteq C \ \wedge \ B \subseteq C \ \Rightarrow \ A \cup B \subseteq C$

Let us prove the property

$$A \subseteq B \ \Leftrightarrow \ A \cup B = B \ :$$

We will show the equivalence by proving the converse equivalence $\neg(A \subseteq B) \ \Leftrightarrow \ \neg(A \cup B = B)$:

$$\neg(A \subseteq B)$$

$$\Leftrightarrow$$

$$\neg(\forall x)(x \in A \ \Rightarrow \ x \in B)$$

$$\Leftrightarrow$$

$$(\exists x)(x \in A \ \wedge \ x \notin B)$$

$$\Leftrightarrow$$

$$(\exists x)((x \in A \ \wedge \ x \notin B) \ \vee \ (x \in B \ \wedge \ x \notin B))$$

$$\Leftrightarrow$$

$$(\exists x)((x \in A \ \vee \ x \in B) \ \wedge \ x \notin B)$$

$$\Leftrightarrow$$

$$(\exists x)(x \in A \cup B \ \wedge \ x \notin B)$$

$$\Leftrightarrow$$

$$\neg(A \cup B \subseteq B)$$

$$\Leftrightarrow$$

$$\neg(A \cup B \subseteq B) \ \vee \ \neg(B \subseteq A \cup B)$$

$$\Leftrightarrow$$

$$\neg((A \cup B \subseteq B) \ \wedge \ (B \subseteq A \cup B))$$

$$\Leftrightarrow$$

$$\neg(A \cup B = B)$$

□

Homework: Prove the remaining properties.

2.5 INTERSECTION

We are given two sets, A and B. The *intersection* of these two sets is the set $A \cap B$, that contains as elements precisely those objects that are elements of set A and of set B:

$$A \cap B = \{x; x \in A \ \wedge \ x \in B\} .$$

Example: $A = \{1, 3, 5, 7\}$, $B = \{1, 2, 4, 8\}$.
$A \cap B = \{1\}$.

Intersection of several sets:
$\mathcal{A} = \{A_\lambda; \lambda \in J\}$ - a family of sets with index set J, $J \neq \emptyset$!

The index set is an arbitrary nonempty set!

We can define the intersection of an arbitrary nonempty family of sets as

$$\cap\mathcal{A} = \cap_{\lambda\in J}A_\lambda = \{x; (\forall\lambda)(\lambda \in J \;\Rightarrow\; x \in A_\lambda)\}$$

(If $J = \emptyset$, we would have $\cap\mathcal{A}$ = everything. But such a set does not exist.)

If J is finite, we usually take $J = \{1, 2, \ldots, n\}$ and write

$$\cap\mathcal{A} = \cap_{j=1}^{n} A_j = A_1 \cap \cdots \cap A_n\,.$$

If $A \cap B = \emptyset$, we say that the sets A and B are *disjoint*.

Basic properties of intersection:

- $A \cap B = B \cap A$, commutativity
- $(A \cap B) \cap C = A \cap (B \cap C)$, associativity
- $A \cap A = A$, idempotency
- $A \cap \emptyset = \emptyset$
- $A \cap B \subseteq A$, $A \cap B \subseteq B$,
- $A \subseteq B \;\Leftrightarrow\; A \cap B = A$
- $A \subseteq B \;\wedge\; A \subseteq C \;\Rightarrow\; A \subseteq B \cap C$

Homework: Prove the above properties. (Proofs are similar to the proofs of analogous properties of the union.)

The union and the intersection are related via the distributivity laws:

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

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

Let us prove the first distributivity law: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

How do we show equality of two sets, $X = Y$? There are several possibilities:

1. *We show the correctness of the proposition* $(\forall x)(x \in X \;\Leftrightarrow\; x \in Y)$

   OR:

2. *a) We show $X \subseteq Y$, that is, the correctness of the proposition $(\forall x)(x \in X \Rightarrow x \in Y)$.*

   b) We also show $Y \subseteq X$, that is, the correctness of the proposition $(\forall x)(x \in Y \Rightarrow x \in X)$.

Let's have a look at the first approach:

$$x \in (A \cup B) \cap C$$

$$\Leftrightarrow$$

$$(x \in A \cup B) \ \wedge \ (x \in C)$$

$$\Leftrightarrow$$

$$(x \in A \ \vee \ x \in B) \ \wedge \ (x \in C)$$

$$\Leftrightarrow$$

$$(x \in A \ \wedge \ x \in C) \ \vee \ (x \in B \ \wedge \ x \in C)$$

$$\Leftrightarrow$$

$$(x \in A \cap C) \ \vee \ (x \in B \cap C)$$

$$\Leftrightarrow$$

$$x \in (A \cap C) \cup (B \cap C)\,.$$

Since the above chain of equivalences holds for an arbitrary x, the proposition

$$(\forall x)(x \in (A \cup B) \cap C \ \Leftrightarrow \ x \in (A \cap C) \cup (B \cap C))$$

is correct. Hence, the sets are equal. □

The distributivity laws also hold more generally, for nonempty set families:

$$(\bigcup_{\lambda \in J} A_\lambda) \cap (\bigcup_{\mu \in K} B_\mu) = \bigcup_{\lambda \in J, \mu \in K} (A_\lambda \cap B_\mu)\,.$$

$$(\bigcap_{\lambda \in J} A_\lambda) \cup (\bigcap_{\mu \in K} B_\mu) = \bigcap_{\lambda \in J, \mu \in K} (A_\lambda \cup B_\mu)\,.$$

Homework: Prove that for arbitrary three sets A, B, C it holds that:

$$(A \cap B) \cup C = A \cap (B \cup C) \ \Leftrightarrow \ C \subseteq A\,.$$

(The condition on the right does not depend on B!)

Homework solution.

Let us prove transitivity of inclusion: $A \subseteq B \land B \subseteq C \Rightarrow A \subseteq C$

Direct proof:

Assume that $A \subseteq B$ and $B \subseteq C$. We need to show: $(\forall x)(x \in A \Rightarrow x \in C)$.

Consider an arbitrary $x \in A$.

- Since $x \in A$ and $A \subseteq B$, it follows $x \in B$.
- Since $x \in B$ and $B \subseteq C$, it follows $x \in C$.

Since x was arbitrary, we proved $(\forall x)(x \in A \Rightarrow x \in C)$, that is, $A \subseteq C$.

2.6 SET DIFFERENCE

We are given two sets A and B.

The *difference* of sets A and B is the set that contains as elements precisely those objects that are elements of set A but they are not elements of set B.

$$A \setminus B = \{x; x \in A \land x \notin B\}.$$

Example: Let A be the set of all prime numbers, and B the set of all positive odd numbers. Then

$A \setminus B = \{2\}$ (2 is the only even prime)

$B \setminus A = \{1, 9, 15, 21, 25, \ldots\}$ (the set of all odd numbers that are not primes)

Basic properties:

- $A \setminus A = \emptyset$
- $A \setminus (A \cap B) = A \setminus B$
- $A \cap (A \setminus B) = A \setminus B$
- $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

- $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
- $(A \setminus B) \cup B = A \cup B$
- $(A \cup B) \setminus B = A \setminus B$
- $(A \cap B) \setminus B = \emptyset$
- $(A \setminus B) \cap B = \emptyset$

Let us prove the equality $(A \setminus B) \cup B = A \cup B$:

$$x \in (A \setminus B) \cup B$$

$$\Leftrightarrow$$

$$x \in A \setminus B \ \vee \ x \in B$$

$$\Leftrightarrow$$

$$(x \in A \ \wedge \ x \notin B) \ \vee \ x \in B$$

$$\Leftrightarrow$$

$$(x \in A \ \vee \ x \in B) \ \wedge \ (x \notin B \ \vee \ x \in B)$$

$$\Leftrightarrow$$

$$(x \in A \ \vee \ x \in B)$$

$$\Leftrightarrow$$

$$x \in A \cup B$$

□

Homework: Prove the remaining properties.

2.7 COMPLEMENT

Very frequently in mathemathics, we are in the following situation: we are given some *universal set* S, and only care about the elements and subsets of S.

Let $A \subseteq S$. Then we can define the *complement of set A (relative to S)* as:

$$C_S A = \overline{A} = S \setminus A\,.$$

If the set S is not defined, we cannot talk about the complemet: $\overline{\emptyset}$ = set of all sets — which does not exist (Russell's antinomy)!

EXAMPLE. Let $S = \{0, 1, 2, 3, \ldots\}$ be the set of all natural numbers, and let A be the set of all prime numbers. Then $\overline{A} = \{0, 1, 4, 6, 8, 9, 10, 12, \ldots\}$. §

Properties of the complement:

- $\overline{S} = \emptyset, \quad \overline{\emptyset} = S$
- $\overline{\overline{A}} = A, \quad A \cup \overline{A} = S, \quad A \cap \overline{A} = \emptyset$
- $A \setminus B = A \cap \overline{B}$
- $A \subseteq B \;\Leftrightarrow\; \overline{B} \subseteq \overline{A}$
- $A = B \;\Leftrightarrow\; \overline{A} = \overline{B}$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B}$ (De Morgan's laws)

De Morgan's laws also hold for an arbitrary family of sets $\mathcal{A} = \{A_\lambda\,;\, \lambda \in J\}$:

$$\overline{\cup_{\lambda \in J} A_\lambda} = \cap_{\lambda \in J} \overline{A_\lambda}$$
$$\overline{\cap_{\lambda \in J} A_\lambda} = \cup_{\lambda \in J} \overline{A_\lambda}$$

Because of De Morgan's laws, theorems about sets often come in pairs. If in a given inclusion, equality or equivalence about unions, intersections and complements of subsets of a certain set we replace each set with its complement, we interchange all union and intersections, and reverse all inclusions, the result is again a valid inclusion, equality or equivalence. This principle is called **principle of duality**.

EXAMPLE. The proposition

$$(A \cap B) \cup C = A \cap (B \cup C) \ \Leftrightarrow\ C \subseteq A\,.$$

becomes

$$(\overline{A} \cup \overline{B}) \cap \overline{C} = \overline{A} \cup (\overline{B} \cap \overline{C}) \ \Leftrightarrow\ \overline{A} \subseteq \overline{C}\,,$$

which is equivalent to

$$(A \cup B) \cap C = A \cup (B \cap C) \ \Leftrightarrow\ A \subseteq C$$

(after interchanging the roles of sets and their complements). §

2.8 POWER SET

The *power set* of a given set A is the family of sets that contains as elements precisely all the subsets of the set A:

$$\mathcal{P}(A) = \{X; X \subseteq A\}$$

Example:

- $\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$
- $\mathcal{P}(\emptyset) = \{\emptyset\}$.
- $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

If a set A has n elements, then its power set $\mathcal{P}(A)$ has 2^n elementov.[1]

Properties:

- $A \subseteq B \ \Rightarrow\ \mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
- $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$.

[1] For each of the n elements of A we need to decide, independently of the other elements, whether to include it in $X \subseteq A$ or not. Thus, altogether we have n independent choices of one out of two possibilities, which, for all subsets $X \subseteq A$, gives us exactly 2^n possobilities.

The first property follows from transitivity of inclusion:
$X \in \mathcal{P}(A) \wedge A \subseteq B \Leftrightarrow X \subseteq A \subseteq B \Rightarrow X \subseteq B \Leftrightarrow X \in \mathcal{P}(B)$.
Proof of the second property:
$X \in \mathcal{P}(A) \cup \mathcal{P}(B) \Leftrightarrow X \subseteq A \vee X \subseteq B \Rightarrow X \subseteq A \cup B \Leftrightarrow X \in \mathcal{P}(A \cup B)$.
Proof of the third property:
$X \in \mathcal{P}(A) \cap \mathcal{P}(B) \Leftrightarrow X \in \mathcal{P}(A) \wedge A \in \mathcal{P}(B) \Leftrightarrow X \subseteq A \wedge X \subseteq B \Leftrightarrow X \subseteq A \cap B \Leftrightarrow X \in \mathcal{P}(A \cap B)$
A question: Why in the second property we don't have equality?

Solution of one of the homeworks:
Let us show that for every three subsets A, B, C, it holds that:

$$(A \cap B) \cup C = A \cap (B \cup C) \Leftrightarrow C \subseteq A\,.$$

$(\Rightarrow)$: Suppose that $(A \cap B) \cup C = A \cap (B \cup C)$.
$C \subseteq (A \cap B) \cup C = A \cap (B \cup C) \subseteq A$. We use transitivity of inclusion.

$(\Leftarrow)$: Suppose that $C \subseteq A$. Then $A \cup C = A$.
Consequently $(A \cap B) \cup C = (A \cup C) \cap (B \cup C) = A \cap (B \cup C)$. §

Let us prove one of De Morgan's laws for an arbitrary set family $\mathcal{A} = \{A_\lambda\ ;\ \lambda \in J\}$:

$$\overline{\cup_{\lambda \in J} A_\lambda} = \cap_{\lambda \in J} \overline{A}_\lambda$$

$$\begin{aligned} x \in \overline{\cup_{\lambda \in J} A_\lambda} &\Leftrightarrow x \notin \cup_{\lambda \in J} A_\lambda \Leftrightarrow \neg(\exists\lambda)(\lambda \in J \wedge x \in A_\lambda) \Leftrightarrow \\ &\Leftrightarrow (\forall\lambda)(\lambda \in J \Rightarrow \neg(x \in A_\lambda)) \Leftrightarrow \\ &\Leftrightarrow (\forall\lambda)(\lambda \in J \Rightarrow x \in \overline{A_\lambda}) \Leftrightarrow x \in \cap_{\lambda \in J} \overline{A}_\lambda\,. \end{aligned}$$

2.9 ORDERED PAIRS AND TUPLES

Consider two objects a and b, $a \neq b$. For the set $\{a, b\}$ the order is irrelevant, $\{a, b\} = \{b, a\}$. When the order of elements is important, we speak about an *ordered pairs*:
(a, b) - ordered pair, $(a, b) \neq (b, a)$

- a - first coordinate
- b - second coordinate

When are two ordered pairs the same?

$$(a,b) = (u,v) \;\Leftrightarrow\; a = u \;\wedge\; b = v\,.$$

Remark: Ordered pairs (a,b) or ordered structures of length k (called ordered k-tupkes can also be defined as follows.

Definition: The ordered k-tuple is an ordered sequence of elements denoted by normal brackets, i.e. $(a_1, a_2, \ldots, a_k)$. Formally we may encode the ordered k-tuple $(a_1, a_2, \ldots, a_k)$ as an ordinary set

$$(a_1, a_2, \ldots, a_k) = \{A_1, A_2, \ldots, A_k\},$$

where $A_i = a_i, a_{i+1}, \ldots, a_k$ for any $1 \le i \le k$. Usually we use only ordered 2-tuples, which are also called ordered pairs.

Homework: Prove that

$$\{\{a\},\{a,b\}\} = \{\{u\},\{u,v\}\} \;\Leftrightarrow\; a = u \;\wedge\; b = v\,.$$

2.10 CARTESIAN PRODUCT

The *Cartesian product* of sets A and B is the set that contains as elements precisely all the ordered pairs (x,y) such that the first coordinate is from A and the second coordinate is from B:

$$A \times B = \{(x,y)\ ;\ x \in A \;\wedge\; y \in B\}$$

Example: $\{1\} \times \{2,3\} = \{(1,2),(1,3)\}$,
$\{2,3\} \times \{1\} = \{(2,1),(3,1)\}$.

Properties of the Cartesian product:

- $A \times B \neq B \times A$ (unless $A = B$)
- $A \times B = \emptyset \;\Leftrightarrow\; A = \emptyset \;\vee\; B = \emptyset$.

- $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
- $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
- $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

The Cartesian product of three sets can be defined as:

$$A \times B \times C = (A \times B) \times C = \{((x,y),z) \; ; \; x \in A \ \wedge \ y \in B \ \wedge \ z \in C\} \, .$$

Usually, we write just: $((x,y),z) = (x,y,z)$ (ordered triple).

The Cartesian product of sets $A_1, \ldots, A_n$ is defined as the set of all ordered n-tuples:

$$A_1 \times A_2 \times \cdots \times A_n = \prod_{i=1}^{n} A_i = \{(x_1, \ldots, x_n) \, ; \, x_1 \in A_1 \ \wedge \ x_2 \in A_2 \ \wedge \ \cdots \ \wedge \ x_n \in A_n\} \, .$$

A SHORT DISCUSSION ABOUT AXIOMS

Every mathematical theory is based on a set of axioms — basic propositions that we em assume to be correct. These axioms define the basic properties that objects of a certain theory should satisfy (e.g. integers, real numbers, groups, vector spaces, graphs, manifolds, ...). From the axioms new truths (claims, consequences, theorems ...) are derived by logical reasoning.

In Set Theory, the situation is the same! There are several families of axioms, but the most established are seven particular axioms, called *axioms of ZFC* (Zermelo - Fraenkel - (Axiom of) Choice), see Appendix.

These axioms ensure the existence of sets and ways of forming new sets from existing ones. Except for the Axiom of Choice, which is of special interest, we will not discuss other axioms here in detail.

3 RELATIONS

Within every mathematical theory $\mathcal{T}$ with universal set S we can represent every meaningful property $P(x)$ with the set

$$\{x\ ;\ x \in S\ \wedge\ P(x)\}\,.$$

Similarly, we can also represent *relations* with sets.

Examples of binary relations: $\in$, $\subseteq$, $=$, $\leq$, $>$, parallel, congruent

- Example: 3 and 5 are in relation “smaller".

Ternary relations: sum, difference, product

“Family” relations: father, son, mother, husband, mother-in-law, ...

parents – ternary relation (x, y, z are in the relation if and only if x and y are parents of z)

3.1 BASIC NOTIONS FOR BINARY RELATIONS

Let R be a meaningful binary relation for some mathematical theory $\mathcal{T}$ with universal set S.

R will be presented with the set of exactly those ordered pairs of elements of S whose first coordinate is in relation R with the second coordinate.

x is in relation R with y: xRy or $R(x, y)$.

$$R = \{(x, y)\ ;\ x, y \in S\ \wedge\ xRy\}$$

or simply (if the universal set S is clear from the context):

$$R = \{(x, y)\ ;\ xRy\}\,.$$

If R is n-ary, we use n-tuples:

$$R = \{(x_1, \ldots, x_n) \; ; \; R(x_1, \ldots, x_n)\}$$

A binary relation is therefore **a subset of the Cartesian product** $S \times S =: S^2$.

An n-ary relation is a subset of the n-fold Cartesian product of set S with itself, $S \times \cdots \times S = \Pi_{i=1}^{n} S =: S^n$.

EXAMPLE: $S = \{1,2,3,4\}$,
Binary relation "smaller", $< (x,y) \;\Leftrightarrow\; x < y$:

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

Ternary relation "sum", $+(x,y,z) \;\Leftrightarrow\; x + y = z$:

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

§

EXAMPLE: $S = \{1,2,3,4,5,6\}$,
Binary relation R "multiple", $R(x,y) \;\Leftrightarrow\; x$ is a multiple of y, that is, $(\exists k)(k$ is a positive integer and $x = k \cdot y)$:

$$R = \{(1,1),(2,1),(2,2),(3,1),(3,3),(4,1),(4,2),(4,4),(5,1),(5,5),(6,1),(6,2),(6,3),(6,$$

Ternary relation "product", $\cdot(x,y,z) \;\Leftrightarrow\; z = x \cdot y$:

$$\cdot = \{(1,1,1),(1,2,2),(1,3,3),(1,4,4),(1,5,5),(1,6,6),(2,1,2),$$

$$(2,2,4),(2,3,6),(3,1,3),(3,2,6),(4,1,4),(5,1,5),(6,1,6)\}\,.$$

"Unary" relation "prime", $P(x) \;\Leftrightarrow\; x$ is a prime:
$P = \{2,3,5\}$. §

Since we represented relations with sets, we can also speak about relations $R \cup T$, $R \cap T$, $R \setminus T$.

EXAMPLE: Let us denote by $R_{\leq}$, $R_{<}$, $R_{=}$, $R_{\geq}$, $R_{>}$ and $R_{\neq}$ respectively the relations "smaller or equal", "smaller", "equal", "greater or equal", "greater" and "non-equal" (e.g., on the set of positive integers). Then:

$$R_{\leq} = R_{<} \cup R_{=}$$

$$R_{>} = R_{\geq} \setminus R_{=} = R_{\geq} \cap R_{\neq}$$

§

Let us now focus on **binary relations** (these are of particular interest, as we shall see in the chapter on order structures).

Let R be a binary relation on a universal set S:

$$R = \{(x,y)\ ;\ xRy\}\,.$$

The set of all first coordinates of elements of R is said to be the *domain of relation R.*

The set of all second coordinates of elements of R is said to be the *range (codomain) of relation R.*

Domain:

$$\mathcal{D}R = \{x\ ;\ (\exists y)(xRy)\}$$

Range:

$$\mathcal{R}R = \{y\ ;\ (\exists x)(xRy)\}$$

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

$\mathcal{D}R = \{1,2\}$,

$\mathcal{R}R = \{2,3,4\}$

§

—

Inverse relation:

$$R^{-1} = \{(y,x)\ ;\ xRy\}$$

Clearly:

- $yR^{-1}x \;\Leftrightarrow\; xRy\,.$
- $\mathcal{D}R^{-1} = \mathcal{R}R$ and $\mathcal{R}R^{-1} = \mathcal{D}R$.
- $(R^{-1})^{-1} = R$.

EXAMPLE: $R_{\leq}^{-1} = R_{\geq}$,
$R_{<}^{-1} = R_{>}$,
$R_{=}^{-1} = R_{=}$,
$R_{\neq}^{-1} = R_{\neq}$. §

3.1.1 Composition of relations

Let R and T be two binary relations.
$T \circ R$: composition of relation R with relation T

$$xT \circ Ry \;\Leftrightarrow\; (\exists u)(xRu \;\wedge\; uTy)$$

$$T \circ R = \{(x,y) \;;\; (\exists u)(xRu \;\wedge\; uTy)$$

EXAMPLE: $R = \{(1,3),(2,3)\}$, $T = \{(3,1)\}$
$T \circ R = \{(1,1),(2,1)\}$, $R \circ T = \{(3,3)\}$.

brother ∘ father ⊆ father
father ∘ brother ⊆ uncle
(father ∘ brother)∪(mother ∘ brother) = uncle
sister ∘ mother ⊆ mother
(wife ∘ mother) ∪ (husband ∘ mother) = mother-in-law §

In general $T \circ R \neq R \circ T$. On the other hand, associativity holds.

Proposition. *Let V, T, R be binary relations on universal set S. Then*

$$V \circ (T \circ R) = (V \circ T) \circ R\,.$$

Proof.

$$(x,y) \in V \circ (T \circ R) \;\Leftrightarrow\; xV \circ (T \circ R)y \;\Leftrightarrow$$

$$(\exists u)(x(T \circ R)u \;\wedge\; uVy) \;\Leftrightarrow\; (\exists u)(\exists v)(xRv \;\wedge\; vTu \;\wedge\; uVy) \;\Leftrightarrow$$

$$(\exists v)(xRv \;\wedge\; (\exists u)(vTu \;\wedge\; uVy)) \;\Leftrightarrow\; (\exists v)(xRv \;\wedge\; v(V \circ T)y) \;\Leftrightarrow$$

$$x((V \circ T) \circ R)y \;\Leftrightarrow\; (x,y) \in (V \circ T) \circ R\,.$$

□

Inverse of a composition is equal to the composition of inverses in reverse order:

Proposition. *Let T and R be binary relations on universal set S. Then*

$$(T \circ R)^{-1} = R^{-1} \circ T^{-1} .$$

Proof.

$$(x,y) \in (T \circ R)^{-1} \;\Leftrightarrow\; (y,x) \in T \circ R \;\Leftrightarrow$$
$$(\exists u)(yRu \;\wedge\; uTx) \;\Leftrightarrow\; (\exists u)(uR^{-1}y \;\wedge\; xT^{-1}u) \;\Leftrightarrow$$
$$(\exists u)(xT^{-1}u \;\wedge\; uR^{-1}y) \;\Leftrightarrow\; x(R^{-1} \circ T^{-1})y \;\Leftrightarrow\; (x,y) \in R^{-1} \circ T^{-1} .$$

□

EXAMPLE: Let $a, b \in \mathbb{R}$.

Define the following relations
$R = \{(x,y) \;;\; x + y = a\}$,
$T = \{(x,y) \;;\; x + y = b\}$.

Then $T \circ R = \{(x,y) \;;\; (\exists u)(x + u = a \;\wedge\; u + y = b)\} = \{(x,y) \;;\; x - y = a - b\}$.

$R \circ T = \{(x,y) \;;\; x - y = b - a\}$.

$R^{-1} = R$, $T^{-1} = T$.

In this case, equality in the above claim becomes $(T \circ R)^{-1} = R \circ T$. §

3.1.2 Universal, null and identity relations

Every set S asmits three special relations:
$S \times S$ – the universal relation
$\emptyset$ – the null relation
$I = \{(x,x) \;;\; x \in S\}$ – the identity relation

Proposition. *Let R be a binary relation on universal set S.*
Then $I \circ R = R \circ I = R$.

Proof. $xI \circ Ry \;\Leftrightarrow\; (\exists u)(xRu \;\wedge\; uIy) \;\Leftrightarrow\; xRy.$
$xR \circ Iy \;\Leftrightarrow\; (\exists u)(xIu \;\wedge\; uRy) \;\Leftrightarrow\; xRy.$ □

It also holds:

- $\emptyset \circ R = R \circ \emptyset = \emptyset$
- $(S \times S) \circ R = (\mathcal{D}R) \times S$ and $R \circ (S \times S) = S \times \mathcal{R}R$.

Homework: Prove the above properties.

3.2 PROPERTIES OF BINARY RELATIONS

Some properties of binary relations are particularly important:

R is *reflexive* $\Leftrightarrow (\forall x)(x \in S \Rightarrow xRx)$
Example: relation $\leq$ in real numbers

R is *irreflexive* $\Leftrightarrow (\forall x)(x \in S \Rightarrow \neg(xRx))$
Example: relation $<$ in real numbers

R is *symmetric* $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \Rightarrow yRx)$
Example: relation "being parallel" on lines in the plane

R is *asymmetric* $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \Rightarrow \neg(yRx))$
Example: relation $<$ in real numbers

R is *antisymmetric* $\Leftrightarrow (\forall x)(\forall y)(x \in S \wedge y \in S \wedge xRy \wedge yRx \Rightarrow x = y)$
Example: relation $\leq$ in real numbers
relation $\subseteq$ in sets

R is *transitive* $\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow xRz)$
Example: relation $<$ in real numbers
relation $\subset$ in sets

R is *intransitive* $\Leftrightarrow (\forall x)(\forall y)(\forall z)(x \in S \wedge y \in S \wedge z \in S \wedge xRy \wedge yRz \Rightarrow \neg(xRz)$
Example: relation R in real numbers, defined by the rule $xRy \Leftrightarrow x = y + 1$

R is *strict total* $\Leftrightarrow$ $(\forall x)(\forall y)(x \in S \ \wedge \ y \in S \ \wedge \ x \neq y \ \Rightarrow \ (xRy) \ \vee \ (yRx))$
Example: relation $<$ in real numbers

R is *total* $\Leftrightarrow$ $(\forall x)(\forall y)(x \in S \ \wedge \ y \in S \ \Rightarrow \ (xRy) \ \vee \ (yRx))$
Example:
relation $\leq$ in real numbers

Homework: Choose some family relations and for each of them verify which of the above properties hold.

Some of the above properties imply others:

- R is total $\Rightarrow$ R is strict total.
- R is asymmetric $\Rightarrow$ R is irreflexive.
- R is symmetric and transitive, and $\mathcal{D}R = S$ $\Rightarrow$ R is reflexive

3.3 EQUIVALENCE RELATION

R is *equivalence* $\Leftrightarrow$ R is reflexive, symmetric and transitive.
Example: the identity relation

Proposition. *R is equivalence $\Leftrightarrow$ $\mathcal{D}R = S$ and $R^{-1} \circ R = R$.*

Proof. The condition is necessary:
$xRx \ \Rightarrow \ \mathcal{D}R = S$

$$xR^{-1} \circ Ry \ \Rightarrow \ (\exists z)(xRz \ \wedge \ zR^{-1}y) \ \Rightarrow \ (\exists z)(xRz \ \wedge \ yRz) \ \Rightarrow \ (\exists z)(xRz \ \wedge \ zRy) \ \Rightarrow \ xR$$

$$xRy \ \Rightarrow \ (xRy \ \wedge \ yRy) \ \Rightarrow \ (xRy \ \wedge \ yR^{-1}y) \ \Rightarrow \ xR^{-1} \circ Ry\,.$$

Hence $R^{-1} \circ R = R$.

The condition is also sufficient:
Let $\mathcal{D}R = S$ and $R^{-1} \circ R = R$.
Reflexivity: we need to show $(\forall x)(x \in S \ \Rightarrow \ xRx)$.
Let $x \in S$. Since $\mathcal{D}R = S$, it follows $x \in \mathcal{D}R \ \Rightarrow \ (\exists y)(y \in S \ \wedge \ xRy)$.

$$xRy \ \Rightarrow \ xRy \ \wedge \ yR^{-1}x \ \Rightarrow \ xR^{-1} \circ Rx \ \Rightarrow \ xRx\,.$$

Symmetry: we need to show $(\forall x)(\forall y)(x \in S \ \wedge \ y \in S \ \wedge \ xRy \ \Rightarrow \ yRx)$. Let $x \in S \ \wedge \ y \in S \ \wedge \ xRy$. Then

$$xRy \ \Rightarrow \ (xRy \ \wedge \ yRy) \ \Rightarrow \ (yRy \ \wedge \ yR^{-1}x) \ \Rightarrow \ yR^{-1} \circ Rx \ \Rightarrow \ yRx\,.$$

Transitivity: we need to show $(\forall x)(\forall y)(\forall z)(x \in S \ \wedge \ y \in S \ \wedge \ z \in S \ \wedge \ xRy \ \wedge \ yRz \ \Rightarrow \ xRz)$.
Let $x \in S \ \wedge \ y \in S \ \wedge \ z \in S \ \wedge \ xRy \ \wedge \ yRz$. Then

$$xRy \ \wedge \ yRz \ \Rightarrow \ xRy \ \wedge \ zRy \ \Rightarrow \ xRy \ \wedge \ yR^{-1}z \ \Rightarrow \ xR^{-1} \circ Rz \ \Rightarrow \ xRz\,.$$

□

Every equivalence relation has the nice property that it divides set S on which it is defined into *non-empty and pairwise disjoint sets the union of which is exactly set* S.

Equivalence classes.
Let R be an equivalence relation defined on a set S. Let $x \in S$. The *equivalence class of element x with respect to the equivalence relation R* is the set of all elements that are in relation with x:

$$R[x] = \{y\,; y \in S \ \wedge \ yRx\}\,.$$

Equivalence classes enjoy the following properties:

- Since R is a reflexive relation, it holds $x \in R[x]$. Consequently $R[x] \neq \emptyset$.

- $y \in R[x] \ \Rightarrow \ R[y] = R[x]$.

  Indeed: Let $y \in R[x]$.

  $z \in R[y] \ \Rightarrow \ zRy \ \wedge \ yRx \ \Rightarrow \ zRx \ \Rightarrow \ z \in R[x]$.

  $z \in R[x] \ \Rightarrow \ zRx \ \wedge \ yRx \ \Rightarrow \ zRx \ \wedge \ xRy \ \Rightarrow \ zRy \ \Rightarrow \ z \in R[y]$.

- $y \notin R[x] \ \Rightarrow \ R[x] \cap R[y] = \emptyset$.

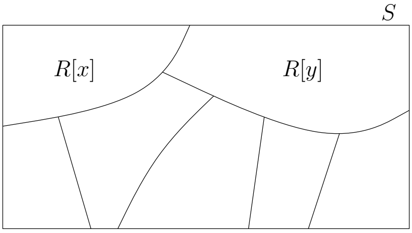
  Indeed: $(\exists z)(z \in R[x] \cap R[y]) \ \Rightarrow \ (\exists z)(R[z] = R[x] \ \wedge \ R[z] = R[y]) \ \Rightarrow \ y \in R[y] = R[x]$. Contradiction with assumption $y \notin R[x]$.

It follows that:

1. Every element of S is in exactly one equivalence class. Namely in the one containing all elements of S that are in relation R with it.

2. Every equivalence class is completely determined with an arbitrary element of it. We say that an arbitrary element of a class is a *representative* of the class.

3. The equivalence classes of a given equivalence relation R divide the set S into nonempty and pairwise disjoint sets the union of which is the set S.



Such divisions are called partitions. *Partition of a set S* = a set of nonempty and pairwise disjoint sets the union of which is S.

Hence, to every equivalence relation there corresponds a partition of set S. The converse holds as well. Every partition $\mathcal{A}$ of set S determines a unique equivalence relation R such that the sets in the partition are exactly the equivalence classes of relation R.

- Two elements x and y are in relation R if and only if they belong to the same set of the partition:

$$xRy \Leftrightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X)\,.$$

Let us verify that the so defined relation is an equivalence relation:

- reflexivity: $x \in S \Rightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X) \Rightarrow xRx\,.$

- symmetry: $xRy \Rightarrow (\exists X)(X \in \mathcal{A} \wedge x \in X \wedge y \in X) \Rightarrow (\exists X)(X \in \mathcal{A} \wedge y \in X \wedge x \in X) \Rightarrow yRx\,.$

- transitivity: $xRy \;\wedge\; yRz \;\Rightarrow\; (\exists X)(X \in \mathcal{A} \;\wedge\; x \in X \;\wedge\; y \in X) \;\wedge\; (\exists Y)(Y \in \mathcal{A} \;\wedge\; y \in Y \;\wedge\; z \in Y)$.

  Hence y is both in X and Y. Since the sets are pairwise disjoint, it follows that $X = Y$. But then z is also in set X. Consequently xRz.

Exercise: Justify that partition $\mathcal{A}$ coincides with the set of equivalence classes of relation R.

To every set S on which some equivalence relation R is defined, we can associate some new set, the elements of which are the equivalence classes of relation R:

Quotient set of S with respect to relation R:

$$S/R = \{R[x]\;;\; x \in S\} = \{X\;;\; (\exists x)(x \in S \;\wedge\; X = R[x])\}$$

- The notion of quotient set represents a mathematical formulation of the logical notion of *abstraction*: By moving from a given set S to the quotient set, we ignore all differences between objects belonging to the same equivalence class!

EXAMPLE: Let $S = \{1,2,3\}$ and $R = \{(1,1),(1,3),(2,2),(3,1),(3,3)\}$.
Relation R is an equivalence relation.
$R[1] = R[3] = \{1,3\}$, $R[2] = \{2\}$.
$S/R = \{R[1], R[2], R[3]\} = \{R[1], R[2]\} = \{\{1,3\},\{2\}\}$.
If we define a partition $\mathcal{A} = \{\{1,2\},\{3\}\}$ of set S, then we can define a relation R' by the rule $xR'y \;\Leftrightarrow\; (\exists X)(X \in \mathcal{A} \;\wedge\; x \in X \;\wedge\; y \in Y)$. It holds $R' = \{(1,1),(1,2),(2,1),(2,2),(3,3)\} = R$ and $S/R' = \{\{1,2\},\{3\}\} = \mathcal{A}$. §

Examples of equivalence relations

1. **Fractions.**

   In the set of fractions a/b, where a and b be arbitrary integers and $b \neq 0$, the definition of equality of two fractions $a/b = c/d \;\Leftrightarrow\; ad = bc$ is an equivalence relation. Each equivalence class with respect to this relation collects together all pairwise equal fractions and then represents the corresponding *rational number*. The corresponding quotient set is the *set of rational numbers*.

2. **Congruences.**

   In the set of *integers* the relation *congruence modulo m*, where $m > 0$ is a positive integer,

   $$a \equiv b \pmod{m} \;\Leftrightarrow\; m \text{ divides } a - b\,,$$

   is an equivalence relation.

   In this case, the equivalence classes are the *residue classes modulo m*. Each equivalence class contains all those numbers that give the same remainder (residue) when divided by m.

   Obviously there are exactly m of these classes. These classes are called *integers modulo m*. The quotient set is the set of integers modulo m.

3. **Parallelism of lines.**

   In the set of *all lines*, the relation "parallel" is an equivalence relation. Each equivalence class therefore contains all the lines that are parallel to each other, and therefore represent a certain *direction*. In this case, the quotient set is *the set of all directions*.

3.4 FUNCTIONS

Function is a central notion of classical and modern mathematics. From 18*th century on, the notion of a function was becoming increasingly more precise and general. The definition of a function as we know it today was given by Cauchy and Riemann:*

For two sets A and B, a *function from A to B* is a rule that assigns to every element of A a unique element of B. Notation: $f : A \to B$.

To avoid any doubt what is meant with the word "rule", we can define functions as special relations.

A binary relation R is *unique* if:

$$(x, y) \in R \;\wedge\; (x, z) \in R \;\Rightarrow\; y = z$$

A *function* (also *mapping, map, transformation*) is a unique binary relation. We usually denote functions with letters $f, g, h, \dots$

We say that f is a function from A to B, and write $f : A \to B$ if $\mathcal{D}f = A$ and the following holds: $(x, y) \in f \;\Rightarrow\; x \in A \;\wedge\; y \in B$.

The set of all functions from A to B is denoted by B^A.

We write

$$y = f(x) \;\Leftrightarrow\; (x, y) \in f\,.$$

$$f = \{(x, y)\ ;\ x \in A \;\wedge\; y = f(x) \in B\}\,.$$

$x \in A$: independent variable, original, argument
$y (= f(x))$: dependent variable, image of element x.

The following notation is also in use:
$x \mapsto f(x)$ "x maps to $f(x)$",
$A \xrightarrow{f} B$ "f is a function from A to B".

Examples of functions:

- $A = \{1, 2, 3\}$, $B = \{2, 4, 6\}$

  $f = \{(1, 2), (2, 4), (3, 4)\}$

- $A = \{$points at the surface of planet Earth$\}$, $B = \mathbb{R}$,

  $f(x) =$ temperature in °C at point x on December 2, 2012, at 6:00 local time

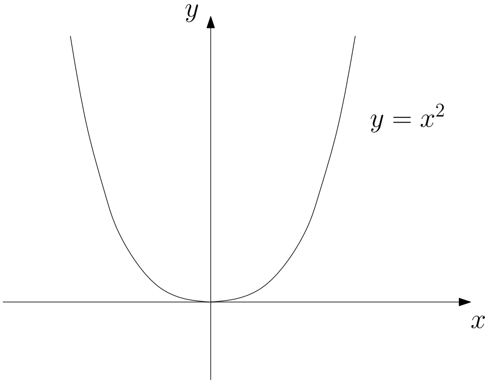
- $A = \{$people living on Earth at a certain time $T\}$, $B = \mathbb{N}$,

  $f(x) =$ age (in seconds) of person x at time T.

The set $\{(x, y)\ ;\ x \in A \;\wedge\; y = f(x)\}$ is sometimes referred to as the *graph of a function.*

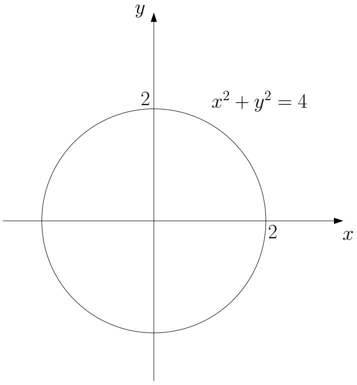
Depictions of functions. If $A \subseteq \mathbb{R}$ and $B = \mathbb{R}$, the graph of a function can also be depicted as a set of points in the plane.

Example: $f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^2\,.$



In a asimilar way, we can also depict *binary relations* on the set $S = \mathbb{R}$:

Let $xRy \;\Leftrightarrow\; x^2 + y^2 = 4$. Then, relation R is represented by a circle of radius 2 and center in the origin.



Let $f : A \to B$. The domain of function f:

$$\mathcal{D}f = \{x \;,\; (\exists y)((x,y) \in f)\} = A$$

Range of function f:

$$\mathrm{Im}f = \{y \;,\; y \in B \;\wedge\; (\exists x)(x \in A \;\wedge\; (x,y) \in f)\} \subseteq B$$

Example: $f = \{(1,2),(2,4),(3,4)\}$, $A = \{1,2,3\}$, $B = \{2,4,6\}$. $\mathcal{D}f = \{1,2,3\}$, $\mathrm{Im}(f) = \{2,4\}$.

In general $\mathrm{Im} f \subseteq B$. If equality holds, $\mathrm{Im} f = B$, then we say that f is a *surjective* function. In this case we say that f maps A *onto* B.

Example: $A = \{1, 2, 3\}$, $B = \{2, 4, 6\}$. $f = \{(1, 2), (2, 4), (3, 4)\}$ is not surjective. $g : A \to B$, $g = \{(1, 2), (2, 6), (3, 4)\}$, is surjective.

The definition of a function allows that several originals have the same f-image. In the extreme case, f maps all elements of A into the same element of B. Such a function is called a *constant (function)*.

The other extreme occurs when two different originals always have different images:

$$\begin{aligned} f \text{ is } \textit{injective} \quad &\Leftrightarrow \quad (\forall y)(y \in \mathrm{Im} f \ \Rightarrow \ (\exists! x)(x \in A \ \wedge \ f(x) = y)) \\ &\Leftrightarrow \quad (\forall x)(\forall y)(f(x) = f(y) \ \Rightarrow \ x = y) \end{aligned}$$

Example: $f = \{(1, 2), (2, 4), (3, 4)\}$ is not injective. $g = \{(1, 2), (2, 6), (3, 4)\}$ is injective.

Let $U \subseteq A$. We write:

$$f(U) = \{y \ ; \ y \in B \ \wedge \ (\exists x)(x \in U \ \wedge \ f(x) = y)\}$$

$f(U)$ – image of subset U under mapping f

Example: $f = \{(1, 2), (2, 4), (3, 4)\}$. $U = \{2, 3\}$. $f(U) = \{f(2), f(3)\} = \{4\}$.

Clearly:

- $f(A) = \mathrm{Im} f$.
- $U \subseteq V \ \Rightarrow \ f(U) \subseteq f(V)$.

The images behave in the following way with respect to unions and intersections:

- $f(U \cup V) = f(U) \cup f(V)$,
- $f(U \cap V) \subseteq f(U) \cap f(V)$.

Homework: Prove the above properties.

3.4.1 Inverse relation, preimages

Inverse relation:

$$f^{-1} = \{(y,x)\ ;\ f(x) = y\}\,.$$

f^{-1} is not necessarily a function!

Example: $f = \{(1,2),(2,4),(3,4)\}$. $f^{-1} = \{(2,1),(4,2),(4,3)\}$ - is not a function.

Preimage of element y:

$$f^{-1}(y) = \{x\ ;\ x \in A\ \wedge\ f(x) = y\}\,.$$

Let $E \subseteq B$. *Preimage of* E (under mapping f):

$$f^{-1}(E) = \{x\ ;\ x \in A\ \wedge\ f(x) \in E\}$$

Example: $f = \{(1,2),(2,4),(3,4)\}$. $f^{-1}(2) = \{1\}$, $f^{-1}(4) = \{2,3\}$, $f^{-1}(\{2,4\}) = \{1,2,3\}$

Clearly:

- $f^{-1}(\mathrm{Im} f) = A$

It also holds:

- $E \subseteq F\ \Rightarrow\ f^{-1}(E) \subseteq f^{-1}(F)$

Preimages are in good relations with unions, intersections, and differences:

- $f^{-1}(E \cup F) = f^{-1}(E) \cup f^{-1}(F)$
- $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$
- $f^{-1}(E \setminus F) = f^{-1}(E) \setminus f^{-1}(F)$

Proof of the property $f^{-1}(E \cap F) = f^{-1}(E) \cap f^{-1}(F)$:

$$x \in f^{-1}(E \cap F) \;\Leftrightarrow\; f(x) \in E \cap F \;\Leftrightarrow\; f(x) \in E \;\wedge\; f(x) \in F \;\Leftrightarrow$$

$$\Leftrightarrow\; x \in f^{-1}(E) \;\wedge\; x \in f^{-1}(F) \;\Leftrightarrow\; x \in f^{-1}(E) \cap f^{-1}(F)$$

□

Homework: Prove the other two properties.

Similarly we can check that:

- for all $U \subseteq A$, it holds that

$$U \subseteq f^{-1}(f(U))$$

- for all $E \subseteq B$, it holds that

$$f(f^{-1}(E)) \subseteq E$$

Let $f : A \to B$. When is the inverse relation f^{-1} a function?
f^{-1} is a function from $\text{Im} f$ to $A \quad\Leftrightarrow\quad f$ is injective.
Therefore, if f^{-1} is a function, then for every element $y \in \text{Im} f$ there exists a unique $x \in \mathcal{D} f$ such that $f^{-1}(y) = x$. It holds that

$$f^{-1}(y) = x \;\Leftrightarrow\; f(x) = y\,.$$

Hence:

$$f^{-1}(f(x)) = x$$

and

$$f(f^{-1}(y)) = y\,.$$

A particularly interesting case is given if function f is not only injective, but also surjective. In this case, we say that function f is *bijective*.

If f is bijective, then $\text{Im} f = B$ and f^{-1} is a function from B to A.

3.4.2 Composition of functions

$$\begin{aligned} g \circ f &= \{(x,z) \; ; \; (\exists y)((x,y) \in f \;\wedge\; (y,z) \in g)\} \\ &= \{(x,z) \; ; \; (\exists y)(f(x) = y \;\wedge\; g(y) = z)\} \,. \end{aligned}$$

Hence, if $\mathrm{Im} f \cap \mathcal{D}g = \emptyset$, then $g \circ f = \emptyset$. This example is not particularly interesting, so we usually require: $\mathrm{Im} f \subseteq \mathcal{D}g$, therefore $A \xrightarrow{f} B \xrightarrow{g} C$. Under this condition:

$$g \circ f = \{(x,z) \; ; \; z = g(f(x))\}$$

relation $g \circ f$ is also a function (from A to C): $(g \circ f)(x) = g(f(x))$.

Example: $f = \{(1,2),(2,4),(3,4)\}$, $g = \{(2,3),(4,5)\}$ (Notice that $\mathcal{D}g = \mathrm{Im} f$.) $g \circ f = \{(1,3),(2,5),(3,5)\}$

Just like compositions of binary relations, compositions of functions also enjoy

Associativity:

If

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \,,$$

then

$$h \circ (g \circ f) = (h \circ g) \circ f \,.$$

3.4.3 Restrictions and extensions

When are two functions f and g the same?

According to the definition of equality of sets, $f = g$ only if they have the same ordered pairs as elements. This is true precisely when the following two conditions are satisfied:

- $\mathcal{D}f = \mathcal{D}g$
- for every element x of this common domain, it holds $f(x) = g(x)$.

Two particular ways of modifying a given function are particularly important:

Restriction: Let $f : A \to B$ and $U \subseteq A$.

The *restriction* of f on U is the function g that has set U as its domain and such that for all $x \in U$, it holds $g(x) = f(x)$. Notation:

$$g = f_{|U}$$

Example: $f = \{(1,2),(2,4),(3,4)\}$, $A = \{1,2,3\}$, $U = \{1,2\}$. $f_{|U} = \{(1,2),(2,4)\}$

If function g is a restriction of function f, we say that f is an *extension* of function g.

3.4.4 Canonical decomposition of a function

Consider the function $f : A \rightarrow B$. Let us define the following relation R on set A:

$$xRy \;\Leftrightarrow\; f(x) = f(y)\,.$$

Clearly, R is an equivalence relation:

- for all $x \in A$ it holds xRx,
- $xRy \;\Rightarrow\; f(x) = f(y) \;\Rightarrow\; f(y) = f(x) \;\Rightarrow\; yRx$,
- $xRy \,\wedge\, yRz \;\Rightarrow\; f(x) = f(y) \,\wedge\, f(y) = f(z) \;\Rightarrow\; f(x) = f(z) \;\Rightarrow\; xRz$.

Now, let us compute the quotient set A/R (the set of all equivalence classes).

Let us first map set A *onto* set A/R:

$$p : A \rightarrow A/R$$

$$p(a) = R[a]$$

Mapping p is surjective. It is called a *natural mapping*.

Now, let us define a mapping g from the quotient set A/R to set B so that function f will be the composition of functions p and g, $f = g \circ p$:

$$g : A/R \rightarrow B$$

$$g(u) = f(x)\,,$$

where x is an arbitrary representative of equivalence class u (that is, $x \in u$).

- Mapping g is well defined (the value of $g(u)$ is independent of the choice of representative of class u):

$$x \in u \ \wedge \ y \in u \ \Rightarrow \ xRy \ \Rightarrow \ f(x) = f(y)\,.$$

- Mapping g is injective:

$$g(u) = g(v) \ \wedge \ g(u) = f(x) \ \wedge \ g(v) = f(y) \ \Rightarrow \ f(x) = f(y) \ \Rightarrow \ xRy \ \Rightarrow \ u = v\,.$$

- It follows from the definitions of functions g and p that $f = g \circ p$:

  Let $x \in A$. Then:

$$(g \circ p)(x) = g(p(x)) = g(R[x]) = f(x)\,.$$

We can decompose f as follows:

$$\begin{tikzcd} A \arrow[r, "p", "\text{surj.}"'] \arrow[rr, bend right, "f"'] & A/R \arrow[r, "g", "\text{inj.}"'] & B \end{tikzcd}$$

This decomposition can be further refined by introducing a mapping h, given by the same rule as g, but that maps to the set $\mathrm{Im}g = \mathrm{Im}f$. Mapping h is then bijective:

$$h : A/R \to \mathrm{Im}f$$

$$h(u) = g(u)\,.$$

Finally, we map set $\mathrm{Im}f$ to set B with the *identity mapping* i, which fixes all elements:

$$i : \mathrm{Im}f \to B$$

$$i(y) = y\,.$$

It is clear that for all $x \in A$, it holds

$$i(h(p(x))) = h(p(x)) = g(p(x)) = f(x)\,.$$

Therefore

$$f = i \circ h \circ p\,.$$

This way, we obtain *canonical decomposition* of function f:

$$\begin{tikzcd}
A \arrow[r, "p", "\text{surj.}"'] \arrow[rrr, bend right, "f"'] & A/R \arrow[r, "h", "\text{bij.}"'] & \mathrm{Im} f \arrow[r, "i", "\text{inj. (identity)}"'] & B
\end{tikzcd}$$

Example: $A = \{1,2,3\}, B = \{2,4,6\}, f = \{(1,2),(2,4),(3,4)\}$
(that is, $f(1) = 2$, $f(2) = f(3) = 4$)
Equivalence relation: $R = \{(1,1),(2,2),(3,3),(2,3),(3,2)\}$
Quotient set: $A/R = \{\{1\},\{2,3\}\}$
$\mathrm{Im} f = \{2,4\}$
Natural mapping p: $p(1) = \{1\}$, $p(2) = p(3) = \{2,3\}$.
Mapping $g : \{\{1\},\{2,3\}\} \to \{2,4,6\}$:
$g(\{1\}) = f(1) = 2$, $g(\{2,3\}) = f(2) = f(3) = 4$.
Mapping $h : \{\{1\},\{2,3\}\} \to \{2,4\}$: $h(\{1\}) = g(\{1\}) = 2$, $h(\{2,3\}) = g(\{2,3\}) = 4$.
Identity mapping $i : \{2,4\} \to \{2,4,6\}$: $i(2) = 2$, $i(4) = 4$.

$$\begin{tikzcd}
\{1,2,3\} \arrow[r, "p", "\text{surj.}"'] \arrow[rrr, bend right, "f"'] & \{\{1\},\{2,3\}\} \arrow[r, "h", "\text{bij.}"'] & \{2,4\} \arrow[r, "i", "\text{inj. (identity)}"'] & \{2,4,6\}
\end{tikzcd}$$

3.5 ORDER STRUCTURES

Besides equivalence relations and functions, relations that generate a certain order *among the elements of a given set are of particular importance in mathematics. The order can be more or less strict, so we deal with different order structures. As we shall see, these structures form a hierarchy and are thus ordered on their own.*

Let us start with the most general structures.

Let S be a universal set and R a relation on S.
We obtain the most general structure if we only require transitivity.
This is not a particularly interesting structure: the null relation, the identity relation and the universal relation are all transitive!

R virtually orders S $\Leftrightarrow$ R is transitive and reflexive.
The word "virtually" relates to our intuitive notion of order, since the universal relation $S \times S$ is a virtual order on S, even though it does not order anything!

R partially orders S $\Leftrightarrow$ R is transitive, reflexive and antisymmetric.

Let R be a partial order on S. Then, a pair (S, R) is called a partially ordered set or, shortly, a *poset*.
xRy:
"x is smaller than or equal to y" or
"y is greater than or equal to x".

Example of a partial order: relation of set inclusion "$\subseteq$", defined on an arbitrary family of subsets of a given universal set $\mathcal{U}$.
Two sets A and B might not be comparable with respect to relation of inclusion!
This holds also in general. This is where the name "partial order" comes from.

Example: relation of divisibility on the set of positive integers.
This is also a partial order. Two numbers might be incomparable with respect to this relation (e.g., 5 and 7, or 12 and 16).

The relation "$\leq$" on the set of real numbers also satisfies all conditions of a partial order.

Even more: this relation is also total, since every two real numbers x and y satisfy $x \leq y$ or $y \leq x$.

R totally or *linearly orders S* $\Leftrightarrow$ R is transitive, reflexive, antisymmetric and total.

However: R is total $\Rightarrow$ R is reflexive!
(if in the condition $(\forall x)(\forall y)(xRy \vee yRx)$ we take $y = x$, we get $(\forall x)(xRx)$).
Hence:
R totally (linearly) orders S $\Leftrightarrow$ R is transitive, antisymmetric and total.

Relations of strict inclusion "$\subset$" and strict inequality "$<$":

- they are both transitive and irreflexive
- both are asymmetric
- relation of strict inclusion determines only a "*partial*" order (since there exist pairs of incomparable sets)
- on the other hand, relation of strict inequality stroge determines a "total" order: it is *strict total*, any two *different* real numbers are pairwise comparable with respect to $<$.

Every asymmetric relation is also irreflexive. Hence we can define
R strictly partially orders S $\Leftrightarrow$ R is transitive and asymmetric.

Analogously:

R strictly linearly orders S $\Leftrightarrow$ R is transitive, asymmetric and strict total.

Let R be a strict partial order on S.
xRy: "x is below y" or
"x is smaller than y" or
"y is above x" or

"y is greater than x".
(The same terminology is also used if R is a partial order and $x \neq y$.

Let us consider one more relation of order: **preorder** (or: quasiorder).

A model for preorder is for example the relation "is at least as tall as" on the set of all people. It is transitive and total (therefore also reflexive).

But it is not antisymmetric! If x "is at least as tall as" y and y "is at least as tall as" x, we can only infer that x and y are equally tall, and not that $x = y$.

R is a *preorder* on $S \quad \Leftrightarrow \quad R$ is transitive and total.

So far we have seen 7 different order structures. Let us define on the set that contains as elements these 7 structures, relation "is a special case of".

x is a special case of y if every relation R_x that determines structure x also has all the properties of structure y.

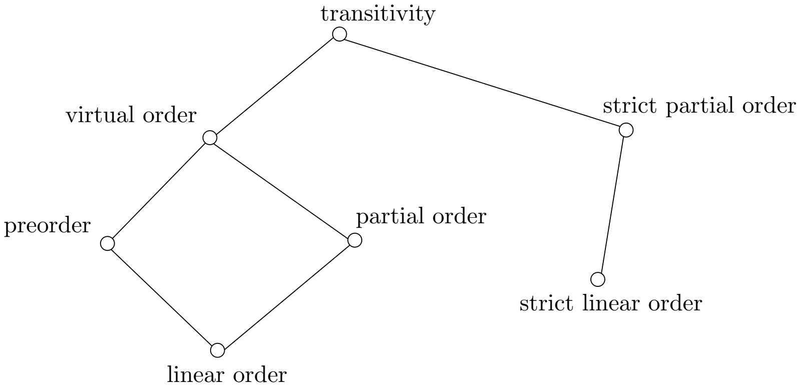
- Example:

  linear order is a special case of partial order

  strict linear order is a special case of strict partial order

relation "is a special case of" is transitive, reflexive and antisymmetric, hence it determines a partial order among these structures.

Partial orders can be represented with so called *Hasse diagrams:*



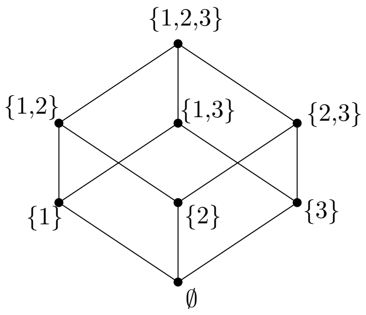
Hasse diagram

R - relation that partially or strictly partially orders S

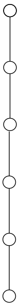
$xRy \;\Leftrightarrow\;$ we can get from x to y in the diagram moving only upwards

---

Example: $A = \{1, 2, 3\}$, $S = \mathcal{P}(A)$, R: strict inclusion



Example: Hasse diagram of a totally or strictly totally ordered set:



3.5.1 Lattice

A *lattice* structure is a partial order with particularly nice features. In order to define it, we need some definitions.

Let a set S be partially ordered with relation R and let $U \subseteq S$.
If there exists $a \in S$ such that for all $x \in U$ it holds aRx, we say that a is an *R-lower bound* for U.

If there exists $b \in S$ such that for all $x \in U$ it holds xRb, we say that b is an *R-upper bound* for U.

If U has an R-lower bound, we say that U is *R-bounded from below*.

If U has an R-upper bound, we say that U is *R-bounded from above*.

If U has an R-upper bound as well as an R-lower bound, we say that U is *R-bounded*.

$a \in S$ is an *R-greatest lower bound (R-infimum)* of a subset $U \quad \Leftrightarrow \quad a$ is an R-lower bound for U and for every R-lower bound x for U it holds xRa.
Notation: $a = R\text{-}\inf U$.

$b \in S$ is an *R-least upper bound (R-supremum)* of a subset $U \quad \Leftrightarrow \quad b$ is an R-upper bound for U and for every R-upper bound x for U it holds bRx.
Notation: $b = R\text{-}\sup U$.

Because of antisymmetry, every subset $U \subseteq S$ has at most one R-sup and at most one R-inf.
But some subsets might have neither of them!

Example:
$S = \mathbb{Q}$, $R = \leq$

$$U = \{x \; ; \; x \in \mathbb{Q} \; \wedge \; 0 \leq x \; \wedge \; x^2 \leq 2\}$$

Set U is bounded from above and from below.
$\inf U = 0$, $\sup U$ does not exist!

$$V = \{x\ ;\ x \in \mathbb{Q}\ \wedge\ 0 \leq x\ \wedge\ 2 \leq x^2 \leq 5\}$$

Set V is bounded, but neither $\inf V$ nor $\sup V$ exist.

Definition. Set S has the structure of a *lattice* with respect to relation R $\Leftrightarrow$ R partially orders S and every *two-element* subset $X \subseteq S$ has an R-supremum and an R-infimum.

Remark: the structure of a lattice can be defined purely algebraically.

Examples of lattices

1. A - set

   $\mathcal{P}(A)$ – power set

   $\mathcal{P}(A)$ is a lattice with respect to $R = \subseteq$:

   - partial order ✓
   - $E, F \subseteq A$, $E \neq F$:

     $\inf\{E, F\} = E \cap F$

     $\sup\{E, F\} = E \cup F$

2. Let R linearly order S.

   $a, b \in S, a \neq b \ \Rightarrow\ aRb$ or bRa

   $aRb \ \Rightarrow\ R\text{-}\inf\{a, b\} = a,\ R\text{-}\sup\{a, b\} = b.$

   $bRa \ \Rightarrow\ R\text{-}\inf\{a, b\} = b,\ R\text{-}\sup\{a, b\} = a.$

3. $S = \mathbb{N}\backslash\{0\}$, $R = |$ (relation of divisibility).

   - partial order ✓
   - $x, y \in \mathbb{N}$, $x \neq y$

     $\inf\{x, y\} =$ greatest common divisor of x and y

     $\sup\{x, y\} =$ least common multiple of x and y

In every lattice, every finite non empty subset of set S has an infimum and a supremum!

Proposition. *Let S have the structure of a lattice with respect to R. Then for every three elements $a_1, a_2, a_3 \in S$, it holds that*

$$R\text{-}\inf\{a_1, a_2, a_3\} = R\text{-}\inf\{R\text{-}\inf\{a_1, a_2\}, a_3\}\,.$$

Proof. Let $a = R\text{-}\inf\{R\text{-}\inf\{a_1, a_2\}, a_3\}$.

a is a lower bound of the set $\{a_1, a_2, a_3\}$:

aRa_3, since a is a lower bound of the set $\{R\text{-}\inf\{a_1, a_2\}, a_3\}$.

Similarly $aR(R\text{-}\inf\{a_1, a_2\})$, but since $(R\text{-}\inf\{a_1, a_2\})Ra_1$ and R is transitive, we get aRa_1. Similarly we also get aRa_2.

a is the greatest lower bound of the set $\{a_1, a_2, a_3\}$:

Let x be an arbitrary lower bound of the set $\{a_1, a_2, a_3\}$. Therefore xRa_1, xRa_2 and xRa_3.

$xRa_1, xRa_2 \;\Rightarrow\; xR(R\text{-}\inf\{a_1, a_2\})$.

$xR(R\text{-}\inf\{a_1, a_2\}) \;\wedge\; xRa_3 \;\Rightarrow\; xRa$. □

Similarly for supremum. We can repeat the procedure and show the existence of infimum and supremum for arbitrary finite nonempty sets.

Corollary. If S is a lattice with respect to R, then every finite nonempty set has both R-inf and R-sup.

We may require the existence of infimum and supremum for *all* nonempty subsets (not only for finite ones):

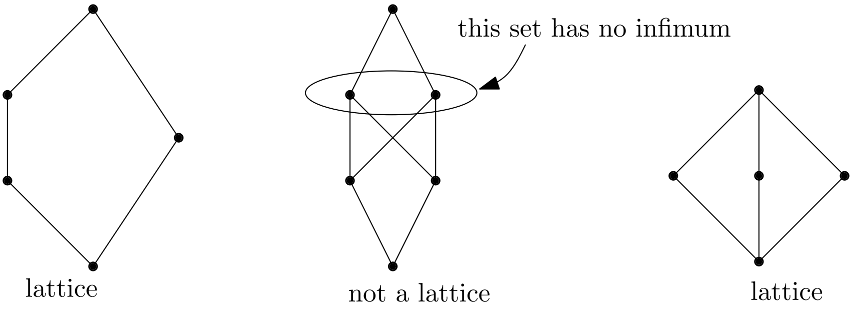


Figure 3: Some further examples with Hasse diagrams.

Definition. Set S has the structure of a *complete lattice* with respect to relation $R \quad \Leftrightarrow \quad R$ partially orders set S and every nonempty subset X of set S has R-inf and R-sup.

Clearly, every complete lattice is also a lattice with respect to the same relation R. Every finite lattice is a complete lattice.

Example:

A – arbitrary set

$\mathcal{P}(A)$ is a complete lattice for $\subseteq$:

If $\mathcal{A}$ is a nonempty family of subsets of set A, then

$$(\subseteq)\text{-}\inf \mathcal{A} = \cap \mathcal{A}$$

and

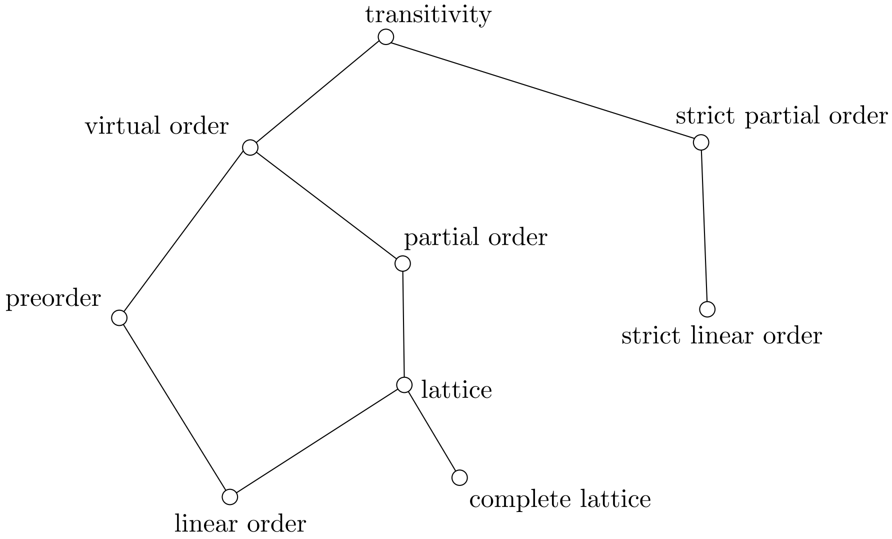
$$(\subseteq)\text{-}\sup \mathcal{A} = \cup \mathcal{A} .$$

Question: Is the set $\mathbb{R}$ of real numbers a complete lattice with respect to relation "$\leq$"?

$\mathbb{R}$ is not a complete lattice with respect to $\leq$: the whole set $\mathbb{R}$ is not bounded! (it has neither a supremum nor an infimum)

We can extend the set of real numbers to a complete lattice by adding to it elements ∞ and $-\infty$, and require $x \leq \infty$ for all $x \in \mathbb{R}$ and $-\infty \leq x$ for all $x \in \mathbb{R}$.

Hasse diagram of the 9 order structures that we have seen:



x is below $y \quad \Leftrightarrow \quad x$ is a special case of y.

3.5.2 Well ordering

Just like the set of real numbers $\mathbb{R}$, the set of natural numbers $\mathbb{N}$ is also strictly linearly oredered with relation "$<$".

But it also has the following additional property:

Every nonempty subset of natural numbers has a smallest element!

Example:

- In the set of all natural numbers such an element is 0.
- In the set of all prime numbers the smallest element is 2.

The set of real numbers does not have this property!

- set $\mathbb{R}$ does not have any smallest element
- the set $\{x \ ; \ x \in \mathbb{R} \ \wedge \ x > 0\}$ also not

The property that every nonempty subset has a smallest element is referred to *well ordering*.

R – relation on set S (typically partial or strict partial order)

- $a \in S$ is a *minimal element* of set S with respect to relation R (or R-*minimal element* of set S) $\Leftrightarrow$ $(\forall y)(y \in S \ \wedge \ y \neq a \ \Rightarrow \ \neg(yRa))$
- $b \in S$ is a *least element* of set S with respect to relation R (or R-*least element* of set S) $\Leftrightarrow$ $(\forall y)(y \in S \ \wedge \ y \neq b \ \Rightarrow \ bRy)$

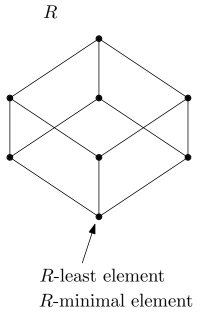
xRy: "x is below y"

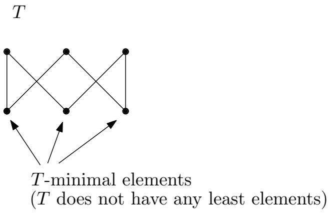
No element of S is below a minimal element.
A least element is below every other element.

- Every element that is incomparable with every other element is a minimal element.

Example:

Partial orders R and T are given with the following Hasse diagrams:





Proposition. *Let R be antisymmetric. Then every R-least element is also R-minimal.*

Proof. By contradiction. Suppose that there exists an R-least element b that is not R-minimal.

b is not R-minimal:

$\neg(\forall y)(y \in S \;\wedge\; y \neq b \;\Rightarrow\; \neg(yRb))$

$\;\Rightarrow\; (\exists y)(y \in S \;\wedge\; y \neq b \;\wedge\; yRb)$

Since b is R-least, it holds bRy. But since R is antisymmetric, from $bRy \;\wedge\; yRb$ it follows that $y = b$. This is in contradiction with $y \neq b$. □

R well orders S $\Leftrightarrow$ R is strict total, irreflexive and
$(\forall X)(X \subseteq S \;\wedge\; X \neq \emptyset \;\Rightarrow\; X$ has an R-minimal element$)$

Proposition. *R well orders S $\Rightarrow$ R is a strict linear order of S.*

Proof. We need to show that R is transitive, asymmetric and strict total.

Strict totality follows from the definition of a well order.

Asymmetry: Suppose that xRy and yRx. Since R is irreflexive, we have $y \neq x$. But then, the set $\{x, y\}$ does not have any R-minimal element:

- $xRy \;\Rightarrow\; y$ is not R-minimal
- $yRx \;\Rightarrow\; x$ is not R-minimal

Therefore, R is asymmetric.

Transitivity can be shown similarly: Suppose that

$$xRy \ \wedge \ yRz \ \wedge \ \neg(xRz)\,.$$

Since R is irreflexive, we have $x \neq y$ and $y \neq z$. Since it is strict total, we have zRx and consequently $z \neq x$. The set $\{x, y, z\}$ has an R-minimal element, however:

- this element is not y, since $xRy \ \wedge \ x \neq y$,
- this element is not z, since $yRz \ \wedge \ y \neq z$.
- this element is not x, since $zRx \ \wedge \ z \neq x$.

This contradiction shows that R is transitive. □

Proposition. *Let R be a well ordering on S. Then every R-minimal element is also R-least.*

Proof. x is R-minimal for $S \ \Rightarrow \ (\forall y)(y \in S \ \wedge \ y \neq x \ \Rightarrow \ \neg(yRx))$
Strict totality: $y \neq x \ \wedge \ \neg(yRx) \ \Rightarrow \ xRy$
Consequently: $(\forall y)(y \in S \ \wedge \ y \neq x \ \Rightarrow \ xRy)$
Therefore x is an R-least element. □

Corollary. Let R be a well ordering on S. Then for all $x \in S$ it holds:

$$x \text{ is } R\text{-least} \ \Leftrightarrow \ x \text{ is } R\text{-minimal}\,.$$

Proposition. *Let R be a well ordering on a nonempty set X. Then X has* a unique *R-least (or R-minimal) element.*

Proof. Suppose that there exist two different R-least elements x and y. Then xRy and yRx. But this is a contradiction with asymmetry. □

One can also define well ordering by means of R-least elements, but then we also need to require asymmetry.

Proposition. *R well orders S if and only if R is strict total, asymmetric and the following condition holds:*
$(\forall X)(X \subseteq S \ \wedge \ X \neq \emptyset \ \Rightarrow \ X \text{ has an } R\text{-least element}).$

Proof. **Homework.** □

Remark: The notion of well ordering is important because it generalizes the ordering $<$ on the set of natural numbers. The principle of induction can also be generalized to well ordered sets (this is the so called *transfinite induction*).

Immediate successor. Greatest element.

In the set of natural numbers, ordered with respect to relation "$<$", every number has its (uniquely determined) immediate successor. What characterizes an immediate successor y of a number x?

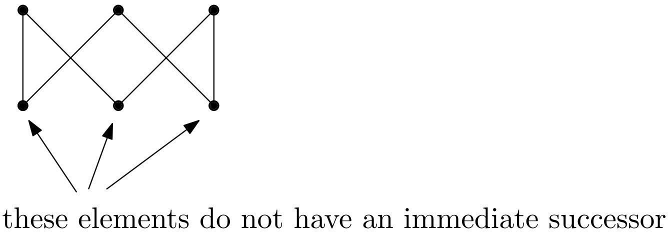
- $x < y$
- for every other number z such that $x < z$, it also holds $y < z$.

Let R be a well ordering on a set S. Element y is an *immediate successor* of element $x \iff xRy$ and $(\forall z)(z \in S \ \wedge \ z \neq y \ \wedge \ xRz \ \Rightarrow \ yRz)$.

Every finite subset of natural numbers has not only the least but also the *greatest element*. This is such a number x from the set with which every other number y is in relation $y < x$.

We can generalize the definition:
Let R be a well ordering of S and let $X \subseteq S$. Element $x \in X$ is an *R-greatest element* of set $X \iff (\forall y)(y \in X \ \wedge \ y \neq x \ \Rightarrow \ yRx)$.

Remark: The definitions of immediate successor and R-greatest element can also be introduced for general partially ordered sets. But they are particularly interesting for well ordered sets, since the R-greatest elements are the only elements without an immediate successor (as we will see below). In general partially ordered sets this may not be the case:



Proposition. *Let R be a well ordering on S and let $x \in S$. If x is not the R-greatest element of the set S, then x has a unique immediate successor.*

Proof. Consider the set

$$X = \{z\, ; z \in S \ \wedge \ xRz\}\,.$$

Since x is not R-last, the set X is nonempty.

Therefore, set X has a unique R-least element y.

Let us show that y is an immediate successor of x:

- Since $y \in X$, we have xRy.
- If $z \in S$ is an element such that xRz and $z \neq y$, then yRz (since $z \in X$ and is y R-least element of set X).

y is also unique immediate successor of element x:

Suppose that there exists $z \neq y$ that is an immediate successor of x. Since xRz, we have $z \in X$.

Since y is R-least element of X, $z \in X \ \wedge \ z \neq y$, it also holds yRz.

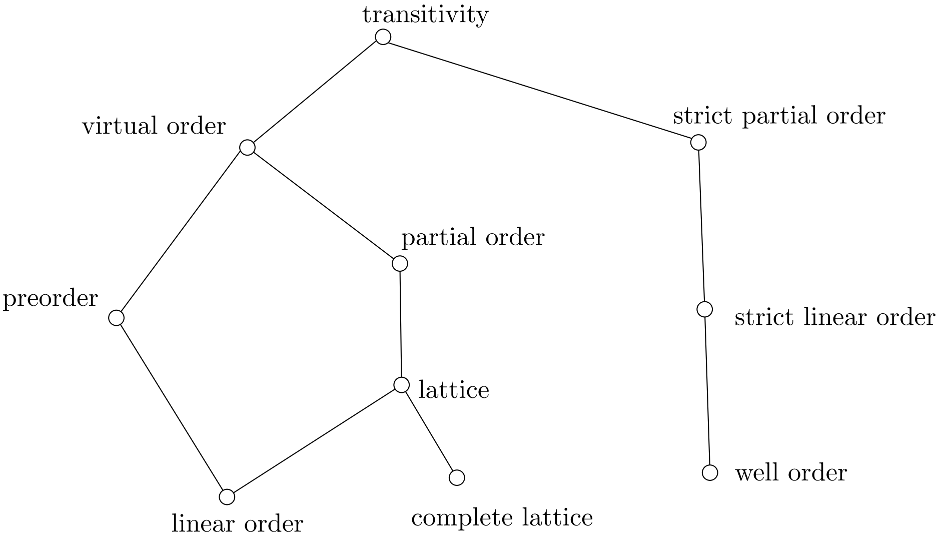
But this is a contradiction with the definition of immediate successor of x. □

The notion of immediate predecessor is defined similarly as the notion of immediate successor.

However the analogous claim for a well order R, saying that every element x that is not R-least has (a unique) immediate successor, does not hold!

Example: Let $S = \mathbb{N} \cup \{\infty\}$. For R take the usual ordering $<$ on $\mathbb{N}$, extended by the rule $n < \infty$ for all $n \in \mathbb{N}$. Then R well orders S. However, element ∞ does not have any immediate predecessors.

Let us close this chapter on order structures with the Hasse diagram of the 10 order structures that we have studied:



x is below y $\Leftrightarrow$ x is a special case of y.

4 CARDINALITY OF SETS

When do two finite sets have the same number of elements?

We remove one element from each of the sets and repeat the procedure. The two sets have the same number of elements if and only if they become empty simultaneously with the above procedure. This way, we found a bijective mapping between the two sets.

4.1 EQUIPOLLENT SETS

A set A is *equipollent* to a set B if there exists at least one bijective mapping from A onto B.

Notation:

$$A \sim B\,.$$

We also say that A and B *have the same cardinality*.

— —

Example:

$\mathbb{N} = \{0, 1, 2, \ldots\}, \quad 2\mathbb{N} = \{0, 2, 4, \ldots\}$

$f : 2\mathbb{N} \to \mathbb{N}$, $f(2n) = 2n$ is not a bijective mapping

$g : 2\mathbb{N} \to \mathbb{N}$, $g(2n) = n$ is a bijective mapping! Hence the sets are equipollent.

— —

Example:

Let X be a set. Let $C(X)$ be the set of all functions of the form $f : X \to \{0, 1\}$. Then $C(X) \sim \mathcal{P}(X)$.

Indeed: Consider the mapping $F : C(X) \to \mathcal{P}(X)$ defined with the rule

$$F(f) = f^{-1}(1) = \{x \in X \,:\, f(x) = 1\}$$

for all $f \in C(X)$. Mapping F is a bijective mapping from the set $C(X)$ onto the set $\mathcal{P}(X)$. There are several ways to verify this, for example by finding a mapping $G : \mathcal{P}(X) \to C(X)$ that is inverse to F, that is, that $F \circ G = \mathrm{id}_{\mathcal{P}(X)}$ and $G \circ F = \mathrm{id}_{C(X)}$. Function G with these properties can be defined with the rule

$$G(S) = \chi_S$$

for all $S \subseteq X$, where $\chi_S : X \to \{0, 1\}$ is the **characteristic function** of set S, defined by

$$\chi_S(x) = \begin{cases} 1, & \text{if } x \in S; \\ 0, & \text{if } x \notin S. \end{cases}$$

4.1.1 Properties of the equipollence relation

- $A \sim A$ *(reflexivity)*

  (identity: $i : A \to A$ is bijective)

- $A \sim B \;\Rightarrow\; B \sim A$ *(symmetry)*

  (the inverse of a bijective mapping is a bijective mapping!

  If $f : A \overset{bij.}{\to} B$, then $f^{-1} : B \overset{bij.}{\to} A$)

- $A \sim B$ and $B \sim C \;\Rightarrow\; A \sim C$ *(transitivity)*

  (Composition of bijective mappings is a bijective mapping!

  If $f : A \overset{bij.}{\to} B$ and $g : B \overset{bij.}{\to} C$, then $g \circ f : A \overset{bij.}{\to} C$)

The relation of equipollence $\sim$ is an *equivalence relation*!

$$\boxed{A \sim B \text{ and } C \sim D \text{ and } A \cap C = \emptyset \text{ and } B \cap D = \emptyset \;\Rightarrow\; A \cup C \sim B \cup D}$$

Proof. Let $f : A \overset{bij.}{\to} B$ and $g : C \overset{bij.}{\to} D$.

Define $h : A \cup C \to B \cup D$ with the rule

$$h(x) = \begin{cases} f(x), & \text{if } x \in A; \\ g(x), & \text{if } x \in C. \end{cases}$$

Mapping h is a bijective mapping from the set $A \cup C$ onto the set $B \cup D$, since every element of the set $B \cup D$ is the image of exactly one element from the set $A \cup C$. □

$\boxed{A \sim B \text{ and } C \sim D \quad \Rightarrow \quad A \times C \sim B \times D}$

Proof. Let $f : A \overset{bij.}{\to} B$ and $g : C \overset{bij.}{\to} D$.
Define $h : A \times C \to B \times D$ with the rule

$$h(x,y) = (f(x), g(y))\,.$$

Mapping h is a bijective mapping of the set $A \times C$ onto the set $B \times D$:

- injectivity:

  $h(x,y) = h(x',y') \;\Rightarrow\; (f(x),g(y)) = (f(x'),g(y')) \;\Rightarrow\; f(x) = f(x')$ and $g(y) = g(y')$

  $\Rightarrow\; x = x'$ and $y = y' \;\Rightarrow\; (x,y) = (x',y')$

- surjectivity:

  Let $(b,d) \in B \times D$. Since f and g are surjective, there exist elements $a \in A$ and $c \in C$ such that $f(a) = b$ and $g(c) = d$. Therefore $(b,d) = (f(a),g(c)) = h(a,c)$.

□

$\boxed{A \times B \sim B \times A}$

Proof. Define $f : A \times B \to B \times A$ with the rule

$$f(x,y) = (y,x)\,.$$

Mapping f is bijective:

- injectivity:

  $f(x,y) = f(x',y') \;\Rightarrow\; (y,x) = (y',x') \;\Rightarrow\; y = y'$ and $x = x' \;\Rightarrow\; (x,y) = (x',y')$.

- surjectivity: $(b,a) \in B \times A$ is the image of element (a,b).

□

Let us mention some more properties without proof:

1. $(A \times B) \times C \sim A \times (B \times C)$.

2. $A \times \{a\} \sim A$.

3. To every two sets X and Y we can associate two *disjoint* sets U and V such that $X \sim U$ and $Y \sim V$.

   Indeed: $U = X \times \{\emptyset\}$, $V = Y \times \{\{\emptyset\}\}$.

4. Recall that the symbol A^B denote the set of all functions from set B to set A.

   $A \sim C$ and $B \sim D \quad \Rightarrow \quad A^B \sim C^D$.

Homework: Prove properties 1. and 2.
Question for thougth: How would you prove property 4.?

4.2 COMPARABILITY OF SETS

Is it possible to define relations similar to $\leq, <, \geq, >$ on sets? Is it possible to reasonably compare sets to each other regarding the quantities of their elements?

Let A and B be arbitrary sets. There are four logical possibilities:

(1) Set A has at least one subset A_1 that is equipollent to set B, while set B does not have any subset that would be equipollent to set A.

(2) Set B has at least one subset B_1 that is equipollent to set A, while set A does not have any subset that would be equipollent to set B.

(3) Set A has at least one subset A_1 that is equipollent to set B, and set B has at least one subset B_1 that is equipollent to set A.

(4) Set A does not have any subset that would be equipollent to set B, and set B does not have any subset that would be equipollent to set A.

(1): We say that set A *is of bigger cardinality than* set B.
(2): Set B *is of bigger cardinality than* set A.
(1): $A > B$, (2): $B > A$

It follows immediately from definition that relation $>$ is irreflexive, asymmetric and transitive (therefore, it is a strict partial order)!

- $A \not> A$
- $A > B \;\Rightarrow\; B \not> A$
- $A > B$ and $B > C \;\Rightarrow\; A > C$

If $B > A$, then we also write $A < B$ and say that set A *is of smaller cardinality than* set B.

$$A < B \;\Leftrightarrow\; B > A\,.$$

Case (3) is considered by the following theorem.

Schröder-Bernstein theorem:

$$(3) \;\Rightarrow\; A \sim B\,.$$

(Proof later.)

Remark: Clearly, the implication $A \sim B \;\Rightarrow\;$ (3) holds. (We can take $A_1 = A$, $B_1 = B$.) Schröder-Bernstein theorem states that also the converse implication holds.

The most “problematic” is case (4):
(4): “A and B are incomparable neither with respect to the relation of equipollence $\sim$ nor with respect to the relation “is of bigger cardinality than” $>$"
As soon as we assume the axiom of choice, case (4) never occurs!
Axiom of choice $\Rightarrow$ Given any two sets A and B, at least one of them is equipollent to a subset of the other one.
(For a proof, see A.A. Fraenkel: Abstract Set Theory, North-Holland Publishing Company, Amsterdam 1953, p. 319–321.)

Law of trichotomy:

Arbitrary two sets A and B are comparable with respect to their cardinality. Exactly one of the following conditions holds:

$$A > B, \;\; B > A \quad \textit{or}\; A \sim B\,.$$

It holds:

Axiom of choice $\Leftrightarrow$ law of trichotomy.

Questions for thought:
Relation $>$ is a strict partial order.

- Let $\gtrsim$ be the relation on sets, defined by the rule $A \gtrsim B \;\Leftrightarrow\; (A > B$ or $A \sim B)$. Is this relation total (assuming the law of trichotomy)? Is it a partial order (assuming the law of trichotomy)?
- Let $\geq$ be the relation on sets, defined by the rule $A \gtrsim B \;\Leftrightarrow\; (A > B$ or $A = B)$. Is this relation total (assuming the law of trichotomy)? Is it a partial order (assuming the law of trichotomy)?

Theorem (Schröder-Bernstein theorem)**.** *Let A and B be two sets. Suppose that set A has has at least one subset A_1 that is equipollent to set B, and set B has at least one subset B_1 that is equipollent to set A. Then*

$$A \sim B\,.$$

Proof. There exists a set $A_1 \subseteq A$ such that $A_1 \sim B$.

There exists a set $B_1 \subseteq B$ such that $B_1 \sim A$.

Fix two bijections $f : A \to B_1$ and $g : B \to A_1$.

We will find two subsets $A_0 \subseteq A$ and $B_0 \subseteq B$ such that mappings $f|_{A_0} : A_0 \to B_0$ and $g|_{B \setminus B_0} : B \setminus B_0 \to A \setminus A_0$ will be bijections.

Then, it will follow:

$$A = A_0 \cup (A \setminus A_0) \sim B_0 \cup (B \setminus B_0) = B\,,$$

since $A_0 \cap (A \setminus A_0) = \emptyset$ and $B_0 \cap (B \setminus B_0) = \emptyset$.

First, let us assign to every proper subset X of set A some subset X' of set A, as follows:

$$X' = A \setminus g(B \setminus f(X)) \,.$$

It holds that:

$$X_1 \subseteq X_2 \;\Rightarrow\; X_1' \subseteq X_2' \,.$$

Indeed:

$X_1 \subseteq X_2 \;\Rightarrow\; Y_1 = f(X_1) \subseteq f(X_2) = Y_2 \;\Rightarrow$
$\;\Rightarrow\; B \setminus Y_2 \subseteq B \setminus Y_1 \;\Rightarrow\; g(B \setminus Y_2) \subseteq g(B \setminus Y_1) \;\Rightarrow$
$\;\Rightarrow\; X_1' = A \setminus g(B \setminus Y_2) \subseteq A \setminus g(B \setminus Y_1) = X_2'.$

$- - -$

A subset $Z \subseteq A$ is a *particular subset* if

$$Z \subseteq Z' \,.$$

$\emptyset$ is a particular subset of set A!

Let A_0 be *the union of all particular subsets of set A*!

If Z is a particular subset, then $Z \subseteq A_0 \;\Rightarrow\; Z' \subseteq A_0' \;\Rightarrow$

$$Z \subseteq Z' \subseteq A_0' \,.$$

Therefore, also A_0 is contained in A_0':

$$A_0 \subseteq A_0'$$

Hence, A_0 is a particular subset!

$A_0 \subseteq A_0' \;\Rightarrow\; A_0' \subseteq (A_0')' \;\Rightarrow\; A_0'$ is a particular subset $\;\Rightarrow\; A_0' \subseteq A_0$.

We have

$$A_0 = A_0' \,.$$

This way, we found the subset A_0 we were looking for, a subset that f bijectively maps onto set B_0:

$$B_0 = f(A_0) \subseteq B \,.$$

Moreover, function g bijectively maps the set $B \setminus B_0$ onto the set $A \setminus A_0$:

$$g(B \setminus B_0) = g(B \setminus f(A_0)) = A \setminus A_0 \,,$$

since $A_0 = A \setminus g(B \setminus f(A_0))$. □

5 FINITE AND INFINITE SETS

One can define (in)finite sets in several ways. Assuming the axiom of choice, all these ways are equivalent.

(BY MEANS OF NATURAL NUMBERS.) A given set S is finite if and only if there exists a natural number n such that set S has exactly n elements.

Weaknesses:

– The definition relies on the notion of natural number.

– For some sets we can certainly say that they are finite even though we do not know the precise number of their elements. For instance, the set of all books printed an planet Earth until year 2012, is surely finite.

(PEIRCE AND DEDEKIND.) A given set S is infinite if and only if it has at least one proper subset that is equipollent to it.

This definition is nicely exempplified with the so-called *Hilbert's Great Hotel:*

In a hotel with infinitely many rooms (numbered with $1, 2, 3, \ldots$) there is a quest in every room. A number of new guests come to the hotel. Can we find room for them?

Let's consider two cases.

- Finitely many guests arrive. Suppose that 10 new guests arrive.

  We ask the guest in room j to move to room $j + 10$, for all $j = 1, 2, 3, \ldots$

  The new 10 guests are placed into rooms $1, 2, \ldots, 10$, that became free.

- Infinitely many guests arrive, $g_1, g_2, g_3, \ldots$

We ask the guest in room j to move to room $2j$, for all $j = 1, 2, 3, \ldots$

The new guests are placed in the following way:

$g_1 \mapsto 1$

$g_2 \mapsto 3$

$g_3 \mapsto 5$

$\ldots$

$g_j \mapsto 2j - 1$

When rearranging the "old" guests we used the facts that

$\{1, 2, 3, \ldots\} \sim \{1, 2, 3, \ldots\} \setminus \{1, \ldots, 10\}$ and

$\{1, 2, 3, \ldots\} \sim \{2, 4, 6, \ldots\}$.

In addition, when rearranging the infinitely many new guests we used the fact that

$\{1, 2, 3, \ldots\} \sim \{1, 3, 5, \ldots\}$.

(TARSKI.) Recall: a is a minimal element in S with respect to relation R if for no other element y if this set, it holds yRa.

If S is an arbitrary set, then every family of its subsets is partially ordered with respect to the relation of inclusion $\subseteq$. With respect to this relation, this family either has a minimal element, or it does not have one. In this case, a minimal element is a subset that has no other set from this family as its subset!

Example: $A = \{1, 2, 3\}$.

Family $\mathcal{D}_1 = \{\{1\}, \{1, 2\}, \{1, 2, 3\}\}$ has one minimal element: set $\{1\}$.

Family $\mathcal{D}_2 = \{\{1\}, \{2\}, \{1, 2\}, \{2, 3\}\}$ has two minimal elements: set $\{1\}$ and set $\{2\}$.

Every nonempty family of subsets of set A has at least one minimal element with respect to relation $\subseteq$.

Example: $\mathbb{N}^+ = \{1, 2, 3, \ldots\}$.

For $k \geq 1$ let

$$\mathbb{N}_k = \mathbb{N}^+ \setminus \{1, 2, \ldots, k\} = \{k+1, k+2, \ldots\} .$$

Consider the following nonempty family of subsets

$$\mathcal{D} = \{\mathbb{N}_1, \mathbb{N}_2, \mathbb{N}_3, \ldots\} .$$

Notice that for all $k \geq 1$ it holds $\mathbb{N}_{k+1} \subseteq \mathbb{N}_k$. Therefore $\mathcal{D}$ does not have any minimal element with respect to $\subseteq$.

The definition of Tarski: A given set S is finite if and only if every nonempty family of subsets of set S has at least one minimal element with respect to the relation of inclusion "$\subseteq$". If the set is not finite, it is infinite.

Appendix

A ADDITIONAL TOPICS FROM SET THEORY

A.1 LOGICAL CONSEQUENCES

We are given propositions $C_1, \ldots, C_m$, composed of propositions $A_1, \ldots, A_n$. Let us determine all propositions B for which

$$C_1 \;\wedge\; \cdots \;\wedge\; C_m \;\Rightarrow\; B$$

is a tautology. Such a proposition B is called *logical consequence* of propositions $C_1, \ldots, C_m$.

Special cases:

- $C_1 \;\wedge\; \cdots \;\wedge\; C_m$ tautology $\;\Rightarrow\;$ B tautology
- $C_1 \;\wedge\; \cdots \;\wedge\; C_m$ contradiction $\;\Rightarrow\;$ B any proposition

Otherwise, we take the following approach:

We express the proposition $C_1 \;\wedge\; \cdots \;\wedge\; C_m$ in its canonical CNF. $C_1 \;\wedge\; \cdots \;\wedge\; C_m$ is the conjunction of a number of basic disjunctions (maxterms), composed of propositions $A_1, \ldots, A_n$:

$$(\;\vee\;\;\vee\;\;\vee\;)\wedge(\;\vee\;\;\vee\;\;\vee\;)\wedge\;\cdots\;\wedge(\;\vee\;\;\vee\;\;\vee\;)$$

The following holds:

1. If B is the conjunction of any number of these maxterms, then

$$C_1 \;\wedge\; \cdots \;\wedge\; C_m \;\Rightarrow\; B$$

is a tautology!

(Indeed: if proposition $C_1 \;\wedge\; \cdots \;\wedge\; C_m$ is true, then all the maxterms appearing in the canonical CNF of it are true. Therefore also the conjunction of any number of these maxterms is true.)

2. If $C_1 \;\wedge\; \cdots \;\wedge\; C_m \;\Rightarrow\; B$ is a tautology, then the canonical CNF of B can only contain those maxterms that also appear in the canonical CNF of $C_1 \;\wedge\; \cdots \;\wedge\; C_m$.

(Indeed: if, in the canonical CNF of B we have a maxterm corresponding to a truth assignment d, which does not appear in the canonical CNF for $C_1 \wedge \cdots \wedge C_m$, then proposition B is false at d, while proposition $C_1 \wedge \cdots \wedge C_m$ is true at d. This is a contradiction with the assumption that $C_1 \wedge \cdots \wedge C_m \Rightarrow B$ is a tautology.)

Example:

C_1: A man speaks the truth or is not brave.
C_2: If a man is free, he is brave.

A_1: A man speaks the truth.
A_2: A man is brave.
A_3: A man is free.

$C_1 : A_1 \vee \neg A_2$
$C_2 : A_3 \Rightarrow A_2$
$C_1 \wedge C_2 : (A_1 \vee \neg A_2) \wedge (A_3 \Rightarrow A_2)$

Truth table:

	A_1	A_2	A_3	$A_1 \vee \neg A_2$	$A_3 \Rightarrow A_2$	$C_1 \wedge C_2$
1.	1	1	1	1	1	1
2.	1	1	0	1	1	1
3.	1	0	1	1	0	0
4.	1	0	0	1	1	1
5.	0	1	1	0	1	0
6.	0	1	0	0	1	0
7.	0	0	1	1	0	0
8.	0	0	0	1	1	1

Canonical CNF:

$$\begin{aligned}(\neg A_1 \vee A_2 \vee \neg A_3) &\wedge (A_1 \vee \neg A_2 \vee \neg A_3)\\ &\wedge (A_1 \vee \neg A_2 \vee A_3)\\ &\wedge (A_1 \vee A_2 \vee \neg A_3)\end{aligned}$$

We can obtain all logical consequences that are not tautologies by choosing one or more maxterms and connecting them conjunctively. The number of such consequences is

$$\binom{4}{1}+\binom{4}{2}+\binom{4}{3}+\binom{4}{4}=4+6+4+1=15\,.$$

Let us analyze one of them:

$$\begin{gathered}
(A_1 \lor \neg A_2 \lor \neg A_3) \land (A_1 \lor A_2 \lor \neg A_3)\\
\Leftrightarrow\\
(A_1 \lor \neg A_3 \lor \neg A_2) \land (A_1 \lor \neg A_3 \lor A_2)\\
\Leftrightarrow\\
((A_1 \lor \neg A_3) \lor \neg A_2) \land ((A_1 \lor \neg A_3) \lor A_2)\\
\Leftrightarrow\\
(A_1 \lor \neg A_3) \lor (\neg A_2 \land A_2)\\
\Leftrightarrow\\
A_1 \lor \neg A_3
\end{gathered}$$

The proposition reads: *A man speaks the truth or is not free.*

Suppose also that somebody asks us: Is proposition A_1 a tautological consequence of propositions C_1 and C_2?

In this case, we express proposition A_1 in its canonical CNF with respect to the atomic propositions A_1, A_2, A_3:

Applying implication (18) twice, we can write A_1 as

$$A_1 \lor (A_2 \land \neg A_2) \lor (A_3 \land \neg A_3)\,.$$

Applying distributivity, we obtain the canonical CNF of A_1:

$$\begin{aligned}
&(A_1 \lor A_2 \lor A_3) \land (A_1 \lor A_2 \lor \neg A_3)\\
&\qquad\qquad \land (A_1 \lor \neg A_2 \lor A_3) \land (A_1 \lor \neg A_2 \lor \neg A_3)\,.
\end{aligned}$$

We notice that disjunction $A_1 \lor A_2 \lor A_3$ does not appear in the canonical CNF of proposition $C_1 \land C_2$. Therefore, the answer to the above question is: no. □

A.2 INFERENCE

Facts:

- I will go to the match.
- In the evening, I will do the homework.
- If I go to the match and then to the cinema, I will not have the time to do the homework.

Can I infer that I will not be able to go to the cinema?

Solution:

Let us define the following propositions:
A_1: I will go to the match.
A_2: In the evening, I will do the homework.
A_3: I will go to the cinema.
C_1: A_1
C_2: A_2
C_3: $A_1 \wedge A_3 \Rightarrow \neg A_2$.
We have to determine whether the implication

$$C_1 \wedge C_2 \wedge C_3 \Rightarrow \neg A_3$$

is a tautology.

Suppose this is not the case: let d be a truth assignment for which the antecedent $C_1 \wedge C_2 \wedge C_3$ is true, while the consequent $\neg A_3$ is false. Since the consequent $\neg A_3(d)$ is false, the proposition $A_3(d)$ is true.

Since the antecedent $C_1 \wedge C_2 \wedge C_3$ is true, both propositions $C_1 = A_1$ and $C_2 = A_2$ are true for assignment d. What is the value of C_3, that is, $A_1 \wedge A_3 \Rightarrow \neg A_2$? Proposition $A_1 \wedge A_3$ is true at assignment d, while proposition $\neg A_2$ is false. Therefore, also proposition C_3 is false. However this is a contradiction with the assumption that the conjunction $C_1 \wedge C_2 \wedge C_3$ (antecedent) is true.

This contradiction shows that the implication

$$C_1 \wedge C_2 \wedge C_3 \Rightarrow \neg A_3$$

is indeed a tautology, hence the above inference is correct. (I will not make it to the cinema.) □

The following facts are given:

- This bird is not a bird, or it has wings.
- If this animal is a bird, then it lays eggs.

Is the following inference correct? *If this animal does not have wings, then it does not lay eggs.*

Solution:

Let us define the following propositions:
A_1: This animal is a bird.
A_2: This animal has wings.
A_3: This animal lays eggs.
C_1: $\neg A_1 \lor A_2$
C_2: $A_1 \Rightarrow A_3$
B: $\neg A_2 \Rightarrow \neg A_3$.
We have to determine whether the implication

$$C_1 \land C_2 \Rightarrow B$$

is a tautology.

So let us suppose that it is not: let d be a truth assignment at which the antecedens $C_1 \land C_2$ is true and the consequent B is false. Since the consequent $B(d)$ is false, the proposition $\neg A_2(d)$ is true, and the proposition $\neg A_3(d)$ is false. It follows that the proposition $A_2(d)$ is false, and the proposition $A_3(d)$ is true.

Since the antecedens $C_1 \land C_2$ is true at the truth assignment d, also the proposition C_1 is true at d: $\neg A_1 \lor A_2$. However since the proposition $A_2(d)$ is false, the proposition $\neg A_1(d)$ must be correct. Equivalently: proposition A_1 is false at truth assignemnt d.

The truth assignment is already completely determined with this: $A_1(d)$ and $A_2(d)$ are false propositions, and $A_3(d)$ is true. We can check that also the proposition C_2 is correct at this truth assignment.

We have not reached a contradiction, we constructed a truth assignment, for which the proposition

$$C_1 \land C_2 \Rightarrow B$$

is flase. (This happens only in the case when *this animal is not a bird, it has no wings, and lays eggs.*) □

The above examples nicely illustrate that the process of proving that a particular proposition is a tautology is the same as the process of proving that the a certain proposition is not a tautology. In both cases, we are trying to construct a truth assignment d, for which the proposition is false. If we do that, then we have a proof that the proposition is not a tautology. If we get a contradiction, we have thus proved that the proposition is a tautology!

Homework: Found out whether the following inference is correct.
Facts:
Duke was killed by one of his staff: the cook, the servant or the driver.
If the killer was the cook, she poisoned the food.
If the killer was the driver, he put a bomb in the car.
The food was not poisoned and the servant is not a murderer.
Conclusion: The killer was the driver. content...

B ADDITIONAL TOPICS FROM SET THEORY

B.1 ON AXIOMS

Every mathematical theory is based on a set of axioms — basic propositions that we em assume to be correct. These axioms define the basic properties that objects of a certain theory should satisfy (e.g. integers, real numbers, groups, vector spaces, graphs, manifolds, ...). From the axioms new truths (claims, consequences, theorems ...) are derived by logical reasoning.

In Set Theory, the situation is the same! There are several families of axioms, but the most established are seven particular axioms, called *axioms of ZFC* (Zermelo - Fraenkel - (Axiom of) Choice).

These axioms ensure the existence of sets and ways of forming new sets from existing ones. Except for the Axiom of Choice, which is of special interest, we will not discuss other axioms here in detail.

To understand why we need the axioms, let's see why the set of all sets does not exist!

Russell's Antinomy

We can form very big sets of sets (or families of sets), see the example below

EXAMPLE. Q: The set of rational numbers is a set of sets:

$$0,5 = \left\{ \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \dots \right\}$$

(Fraction is understood as an ordered pair of integers. Ordered pair (a, b) can be defined as the set $\{\{a\}, \{a, b\}\}$.)

This gives the following question:

Is there a *set of all sets?*

We will prove, by contradiction that there is no such set!

So suppose there is. Let A be the set of all sets. For each set, we can ask whether it contains itself as an element. $\mathbb{N}$ is not an element of itself! The set of all abstract notions has itself as an element.

Let $B \subseteq A$ be that subset of A that has for elements precisely those sets from A that do not contain themselves as elements. Does the set B contain itself as an element?

If yes, then it does not contain itself as an element!

What if B does not contain itself as an element? Then, by definition, $B \in B$, a contradiction.

The set of all sets does not exist!

Nothing contains everything.

(mathematical) space does not exist.

So, in forming new sets we should not trust too much our intuition ... Axioms are needed to ensure the existence of certain sets (e.g. the axiom of pairs, the axiom of subsets).

B.2 AXIOMS OF ZERMELO-FRAENKEL SET THEORY

1. Axiom of extensionality (set equality)

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

2. Axiom of an empty set: *There is an empty set.*

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

3. Axiom of pairing: *Any couple of elements from universe may form a 2-set.*

$$\forall u\, \forall v\, \exists B\, \forall x\, (x \in B \;\Leftrightarrow\; x = u \text{ ali } x = v)$$

4. Axiom of union: *The union over the elements of a set exists.*

$$\forall A\, \exists B\, \forall x\, (x \in B \;\Leftrightarrow\; (\exists b \in A) x \in b)$$

5. Axiom of power set: *For each set, the set of all its subsets exists.*

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

6. Axiom schema of specification: *The set builder notation makes sense!*

   For each logical predicate φ which include variables $t_1, \ldots, t_k$, but not B, we have:

$$\forall t_1 \cdots \forall t_k\, \forall c\, \exists B\, \forall x\, (x \in B \;\Leftrightarrow\; x \in c \;\wedge\; \varphi)$$

   EXAMPLE. (Fpr $k = 1$):

   $\forall a\, \forall c\, \exists B\, \forall x\, (x \in B \;\Leftrightarrow\; x \in c \;\wedge\; x \in a)$

   This means in particular that for each sets a and c there is a set $B = a \cap c$, i.e. their intersection.

   As a result of this axiom, the set builder notation is always well-defined, i.e. we may define sets as

$$\{x \in A; P(x)\}\,.$$

   EXAMPLE. $\{x \in \mathbb{R}; x \geq 0\}$.

7. Axiom of infinity: *There exists an infinite set.*

$$\exists A\, (\emptyset \in A \;\wedge\; (\forall a \in A)\, (a \cup \{a\} \in A))$$

8. Axiom schema of replacement: *The image of a set under any definable function will also fall inside a set.*

   This schema allows us to describe functions in a form

$$\{f(x); x \in A\}\,,$$

   where f is any function with a domain which contains A.

EXAMPLE. We may write a set $\{x^2; x \in \mathbb{R}\}$. This is equal to $\{x \in \mathbb{R}; x \geq 0\}$.

9. Axion of regularity: *Every non-empty set x contains a member y such that x and y are disjoint sets.*

$$(\forall A \neq \emptyset)\,(\exists m \in A)\,(m \cap A = \emptyset)$$

   This implies, for example, that for any A and B, niether $A \in B$ or $B \in A$.

10. Axiom of choice: *Each relation admits a function with the same domain.*

$$(\forall \text{ relacijo } R)(\exists \text{ funkcija } F)(F \subseteq R \ \wedge \ \mathcal{D}(F) = \mathcal{D}(R))$$

   We will cover this axiom in detail later, at the end of the Relations chapter.

Some of above axioms maybe derived from the remaining ones, in particular 2., 3. and 6.

C AXIOM OF CHOICE

C.1 AXIOM OF CHOICE

A_1, A_2: sets

$A_1 \times A_2 = \{(x,y)\ ;\ x \in A_1,\ y \in A_2\}$

Every ordered pair is determined so that the first element is chosen from set A_1, and the second one from A_2. Such a choice corresponds to a function

$$f : \{1,2\} \to A_1 \cup A_2$$

such that

$$f(1) \in A_1 \text{ and } f(2) \in A_2\,.$$

Hence

$$A_1 \times A_2 = \{f : \{1,2\} \to A_1 \cup A_2, f(1) \in A_1, f(2) \in A_2\}\,.$$

We can write a similar expression for Cartesian products of finitely many factors:

$$A_1 \times \cdots \times A_n = \{f : \{1,\ldots,n\} \to A_1 \cup \cdots \cup A_n, f(1) \in A_1, \ldots, f(n) \in A_n\}\,.$$

This way, we can generalize the definition of the Cartesian product to products of an arbitrary set family:

Let

$$\mathcal{A} = \{A_\lambda\ ;\ \lambda \in I\}$$

be an arbitrary (nonempty) set family. The *Cartesian product* of family $\mathcal{A}$ is defined as

$$\prod \mathcal{A} = \prod_{\lambda \in I} A_\lambda = \{f : I \to \cup_{\lambda \in I} A_\lambda,\ (\forall \lambda)(\lambda \in I\ \Rightarrow\ f(\lambda) \in A_\lambda)\}\,.$$

An element $f \in \prod_{\lambda \in I} A_\lambda$ is called a *choice function*.

If at least one of the sets A_λ is empty, then also the product $\prod_{\lambda \in I} A_\lambda$ is empty (since if $A_\lambda = \emptyset$ then the condition $f(\lambda) \in A_\lambda$ can certainly not be satisfied)!

- $(\exists \lambda)(\lambda \in I \ \wedge \ A_\lambda = \emptyset) \ \Rightarrow \ \prod_{\lambda \in I} A_\lambda = \emptyset$.

In the finite case also the converse holds:

$$(\forall \lambda)(\lambda \in I \ \Rightarrow \ A_\lambda \neq \emptyset) \ \Rightarrow \ \prod_{\lambda \in I} A_\lambda \neq \emptyset\,.$$

What about the infinite case??
"If $A_\lambda \neq \emptyset$ for all $\lambda \in I$ then there exists at least one choice function."
Can we prove this?
Cohen (1963): this proposition is unprovable from the remaining axioms of Set Theory.

The Cartesian product axiom:
If $\mathcal{A}$ is an arbitrary family of nonempty sets, then $\prod \mathcal{A}$ is a nonempty set.

The Axiom of Choice (AC):
If $\mathcal{A} = \{A_\lambda \ ; \ \lambda \in I\}$ is an arbitrary family of nonempty sets, then there exists at least one funcion $f : I \to \cup_{\lambda \in I} A_\lambda$ such that $f(\lambda) \in A_\lambda$ for all $\lambda \in I$.
Zermelo, 1904 – used AC when proving the Well ordering theorem
(Zermelo Axiom)

Gödel's Theorem (1940): The Axiom of Choice is consistent with the remaining axioms of Set Theory:[1]

- *If we can derive a contradiction in a system, where, besides other axioms we also assume the Axiom of Choice, then a contradiction can also be derived in the system that only relies on the remaining axioms and has no Axiom of Choice.*

[1] Together with the consistency of the Axiom of Choice, Kurt Gödel also demonstrated the consistency of the continuum hypothesis with the other axioms of Set Theory. This way he solved the first of its famous 23 problems, that German mathematician David Hilbert posed to the mathematical community in 1900.

Using the Axiom of Choice one can prove many important theorems in various areas of mathematics (algebra, analysis, topology, ...), as well as some less intuitive theorems, e.g. the **Banach–Tarski paradox:** A three-dimensional unit ball can be the cut into finitely many pairwise disjoint parts such that translations and rotations of them can be composed into *two* identical copies of the original ball!

The Axiom of Choice is equivalent to many other propositions, for example to the following two:

- Every binary relation contains a function with the same domain.
- If $\mathcal{A}$ is a family of pairwise disjoint nonempty sets, then there exists a set X such that for every $A \in \mathcal{A}$, set $X \cap A$ contains exactly one element.

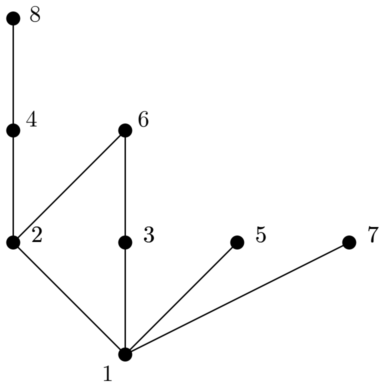
C.1.1 Maximality principles

We will give four maximality principles and show that they are logically equivalent. They are also equivalent to the Axiom of Choice.

First, two definitions:
Let R be a partial order on S.

- If S contains an element m such that for every other element $x \in S$ *it does not hold* mRx, then we say that m is an *R-maximal element* of set S.
- A *chain* in set S is a subset X of S that is linearly ordered by R.

Example: Let $S = \{1, 2, \ldots, 8\}$ and let R be the divisibility relation on S (xRy if and only if x divides y). This poset is represented with the following Hasse diagram:

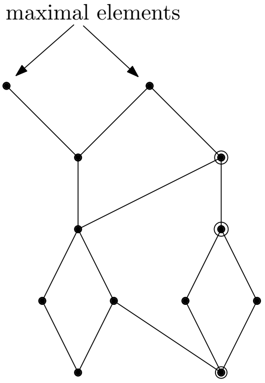


The poset has 4 maximal elements (5, 6, 7, 8) and contains the following chains:

- $\emptyset$ (1 chain without elements)
- $\{1\}, \{2\}, \ldots, \{8\}$ (8 1-element chains)
- $\{1,2\}, \{1,3\}, \ldots, \{1,8\}, \{2,4\}, \{2,6\}, \{2,8\}, \{3,6\}, \{4,8\}$ (12 2-element chains)
- $\{1,2,4\}, \{1,2,8\}, \{1,3,6\}, \{1,4,8\}, \{2,4,8\}$ (5 3-element chains)
- $\{1,2,4,8\}$ (1 4-element chain)

Example:

The following partial order has two maximal elements. The circled elements form a chain:



1. Hausdorff maximality principle.

Let S be a set partially ordered with relation R. Let $\mathcal{V}$ be the family of all chains:

$$\mathcal{V} = \{X \subseteq S\ ;\ X \text{ is a chain}\}\,.$$

The set $\mathcal{V}$ is partially ordered with respect to relation $\subseteq$.

When is X a maximal element of $\mathcal{V}$?

When for every other $Y \in \mathcal{V}$ it holds that X is not a subset of Y: $X \nsubseteq Y$. Such an element is called a *maximal chain*.

Hausdorff maximality principle:

Set $\mathcal{V}$ has at least one maximal element with respect to $\subseteq$.

Every poset has a maximal chain.

2. Zorn's lemma.

Zorn's lemma says that the condition that every chain in a poset is bounded from above is a sufficient condition for the existence of a maximal element in the given poset.

Zorn's lemma: *Let S be a set partially ordered with respect to relation R and suppose that every chain in S has an R-upper bound. Then the set S has at least one R-maximal element.*

3. Tukey's maximality principle.

Let S be an arbitrary set and let $\mathcal{D}$ be an arbitrary (nonempty) family of subsets of set S (hence $\mathcal{D} \subseteq \mathcal{P}(S)$).

Definition. $\mathcal{D}$ is *of finite character* $\Leftrightarrow$ an arbitrary subset $X \subseteq S$ is in $\mathcal{D}$ if and only if every *finite* subset of set X is in $\mathcal{D}$.

Tukey's maximality principle:

If $\mathcal{D}$ is of finite character, then $\mathcal{D}$ has at least one maximal element with respect to relation "$\subseteq$" (which partially orders $\mathcal{D}$).

4. Kuratowski's lemma.

Let S be a set partially ordered with relation R. Let $V \subseteq S$ be a chain in S.

$$\mathcal{U}_V = \{X \subseteq S\ ;\ X \text{ is a chain in } S \text{ and } V \subseteq X\}\,.$$

$\mathcal{U}_V$ is partially ordered with relation "$\subseteq$".

Kuratowski's lemma: *$\mathcal{U}_V$ has at least one maximal element with respect to inclusion $\subseteq$.*

Every chain is contained in a maximal chain.

All these maximality principles are pairwise logically equivalent. We will show:

(Hausdorff) $\Rightarrow$ (Zorn) $\Rightarrow$ (Tukey) $\Rightarrow$ (Kuratowski) $\Rightarrow$ (Hausdorff)

Step 1: (Hausdorff) $\Rightarrow$ (Zorn)

Let R partially order S and let every chain in S have R-upper bound.

By Hausdorff, S contains at least one maximal chain V.

The hypothesis of Zorn's lemma says that V has an R-upper bound u.

We claim that u is an R-maximal element.

Suppose this is not the case. Then there exists an element $x \in S$ such that $x \neq u$ and uRx.

Let $y \in V$. Since u is an upper bound for chain V, we have yRu and also uRx and therefore, by transitivity, yRx. Consequently $y \neq x$, since $y = x$ would imply uRx and xRu and also $x = u$.

Therefore the chain V is a proper subset of the set $V \cup \{x\}$. But the set $V \cup \{x\}$ is linearly ordered with relation R, hence it is a chain. This is in contradiction with the condition that V is a maximal chain.

We thus showed that set S has an R-maximal element. □

Step 2: (Zorn) $\Rightarrow$ (Tukey)

Let $\mathcal{D}$ be a nonempty family of subsets of a given set X and let $\mathcal{D}$ be of finite character.

The family $\mathcal{D}$ is partially ordered with respect to relation "$\subseteq$".

Let us check that every chain in this family has an upper bound!

Let V be an arbitrary chain in family $\mathcal{D}$. The elements of set V are subsets of set X, which are linearly ordered with relation $\subseteq$ (since V is a chain). Let us take the union of all the elements of this chain, $W = \cup V$.

Clearly, W is an upper bound for V (for every element $X \in V$ it holds $X \subseteq \cup V = W$).

Let us show that $W \in \mathcal{D}$. Since $\mathcal{D}$ is of finite character, it suffice to show that every finite subset of W belongs to $\mathcal{D}$. Let $A = \{a_1, \dots, a_n\} \subseteq W$. There exist sets $A_1, \dots, A_n \in V$ such that $a_i \in A_i$ for all i. But since these sets are linearly ordered, one of these n sets, say A_j, contains all others. It follows that A_j also contains A. Since $A \subseteq A_j \in V$ and therefore also $A_j \in \mathcal{D}$, it follows that also $A \in \mathcal{D}$, since A is a finite subset of V, which is an element of $\mathcal{D}$, and family $\mathcal{D}$ is of finite character.

We have showed that every chain has an upper bound with respect to relation of inclusion. It follows from Zorn's lemma that family $\mathcal{D}$ has at least one maximal element. □

Step 3: (Tukey) $\Rightarrow$ (Kuratowski)

Let a relation R partially order set S and let V be an arbitrary chain in S.

Let $\mathcal{D}$ be the family of all the subsets X of set S such that $X \cup V$ is a chain in set S.

Let us verify that $\mathcal{D}$ is of finite character!

Let $X \in \mathcal{D}$. Then also every finite subset X' of set X is in $\mathcal{D}$: namely, $V \cup X$ is a chain, therefore $V \cup X'$ is also a chain.

And conversely: let X be a subset of set S such that $\mathcal{D}$ contains all finite subsets of X. This means that for every two elements $x, y \in X$ it holds that $\{x, y\} \cup V$ is a chain. It is evident that then also the set $X \cup V$ is a chain. Therefore $X \in \mathcal{D}$.

By Tukey, set $\mathcal{D}$ contains a maximal element M with respect to relation of inclusion $\subseteq$.

By the definition of family $\mathcal{D}$, the set $M \cup V$ is a maximal chain in set S containing chain V. But this is exactly the statement of Kuratowski's lemma. □

Step 4: (Kuratowski) $\Rightarrow$ (Hausdorff)

Let a relation R partially order a set S. Consider the empty set. This is certainly a chain in S; the condition about linear ordering of its elements is vacuously satisfied.

But the empty set is a subset of every chain in S. According to Kuratowski's lemma, a maximal chain exists and at the same time is also a maximal element of the family $\mathcal{V}$ of all chains with respect to relation of inclusion $\subseteq$. But this is precisely the content of Hausdorff maximality principle. $\square$

Maximality principles are also equivalent to the axiom of choice:
(Tukey) $\Rightarrow$ (axiom of choice) $\Rightarrow$ (Hausdorff)

(Tukey) $\Rightarrow$ (axiom of choice)
Let $\mathcal{A} = \{A_\lambda \ ; \ \lambda \in I\}$ be an arbitrary family of nonempty sets.

Let $\mathcal{F}$ be the set of all functions the domain $\mathcal{D}f$ of which is a subset of I and that assign to each $\lambda \in \mathcal{D}f$ an element $f(\lambda) \in A_\lambda$.

Every such function is a set of ordered pairs, that is,

$$f \subseteq I \times \cup\mathcal{A}\,.$$

Set $\mathcal{F}$ is a family of subsets of the Cartesian product $I \times \cup\mathcal{A}$.

Claim: $\mathcal{F}$ is of finite character.

Proof of claim: Let $f \in \mathcal{F}$. Clearly, every finite subset of function f is an element of $\mathcal{F}$.

Now, take an arbitrary subset g of the Cartesian product $I \times \cup\mathcal{A}$ with the property that every finite subset of g is an element of $\mathcal{F}$.

In this case, g is also a function and an element of family $\mathcal{F}$. Indeed, if in the set g there existed two different pairs (λ, a) and (λ, b) with the same first coordinate, then the two-element subset $\{(\lambda, a), (\lambda, b)\}$ would not be a function, which is in contradiction with the assumption.

Similarly we conclude that $g \in \mathcal{F}$, since for every $(\lambda, a) \in g$, it holds that $\{(\lambda, a)\} \in \mathcal{F}$, therefore $\lambda \in I$ and $a \in A_\lambda$.

We proved that $\mathcal{F}$ is of finite character. Tukey's maximality principle implies that $\mathcal{F}$ has at least one maximal element F with respect to relation "$\subseteq$".

Let us verify that this F is a choice function!

Since $F \in \mathcal{F}$, F is a function. Hence, it is enough to show that the domain of F is equal to I. Suppose this is not the case. Then, there exists an index $\lambda \in I \backslash \mathcal{D}f$. Let a be an arbitrary element of the non-empty set A_λ and let us make the ordered pair (λ, a) and the union $F \cup \{(\lambda, a)\}$. This union is an element of family $\mathcal{F}$ that contains function F as a proper subset. This, however, is in contradiction with the fact that F is a maximal element of family $\mathcal{F}$.

Therefore $\mathcal{D}F = I$ and F is indeed a choice function. □

It is possible to show that **(axiom of choice)** $\Rightarrow$ **(Hausdorff)**.
See *Niko Prijatelj: Matematične strukture I, p. 135–142.*
For the proof of implication **(axiom of choice)** $\Rightarrow$ **(Zorn's lemma)**, see *Paul Halmos: Naive Set Theory, p. 63–65.*

C.2 WELL ORDERING THEOREM

Perhaps the deepest reason why the axiom of choice seems problematic to many mathematicians stems from the fact that the axiom of choice implies the well ordering theorem, that states that every set can be well ordered.

Well ordering theorem: For every set S there exists a relation R that well orders S.

Well ordering theorem $\Leftrightarrow$ axiom of choice.

Let us show the easier of both implications.
Well ordering theorem $\Rightarrow$ axiom of choice.
Let $\mathcal{A} = \{A_\lambda\ ;\ \lambda \in I\}$ be an arbitrary family of nonempty sets. According to the well ordering theorem, there exists a relation R that well orders *the union of family* $\mathcal{A}$, $\cup\mathcal{A}$.
Since every subset A_λ of family $\mathcal{A}$ is a nonempty subset of the union $\cup\mathcal{A}$, it has an R-least element. Hence, we can define the choice function f by assigning to each element $\lambda \in I$ the R-least element of set A_λ:

$$f(\lambda) = R\text{-least element in } A_\lambda\,.$$

The axiom of choice is thus verified. □
It is also possible to show the implication **(axiom of choice)** $\Rightarrow$ **(well-ordering theorem)**. See *Niko Prijatelj: Matematične strukture I, p. 143–151.*
For a proof of implication of **(Zorn's lemma)** $\Rightarrow$ **(well-ordering theorem)** see *Paul Halmos: Naive Set Theory, p. 68.*