Theoretical Computer Science I

Discrete Structures for Computer Science

FAMNIT, Fall 2020

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 may suggest 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 for this course, most notably

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

CONTENTS

1

MATHEMATICAL LOGIC

PROPOSITIONS.

What is a proposition? 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).

  For example: 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.

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

Notation: $\neg A$.

$\neg A$ 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.)*

1.0.1 *Conjunction:* A *and* B

Notation: $A \wedge B$

$A \wedge B$ 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.*

1.0.2 *Disjunction:* A *or* B

Notation: $A \vee B$

$A \vee B$ 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*."*

1.0.3 *Implication: If* A*, then* B

Notation: $A \Rightarrow B$

$A \Rightarrow B$ 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

Notation: $A \Leftrightarrow B$

$A \Leftrightarrow B$ 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.*

Some 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) $A \vee B$

(b) $A \wedge B$
(c) $A \wedge \neg B$
(d) $\neg A \vee \neg B$
(e) $\neg\neg A$
(f) $\neg(\neg A \wedge \neg B)$

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.

1.1 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 following truth tables:

Truth table of negation

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

Truth table of Conjunction, disjunction, implication and equivalence

	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

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:

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	$A \Rightarrow B$	$B \Rightarrow C$	$(A \Rightarrow B) \wedge (B \Rightarrow C)$	$\neg A$	$\neg A \vee C$	(**??**)
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 (**??**) 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.

Exercise: 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:

$$[A \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)] \wedge [B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)]\,. \quad (3)$$

A	B	$A \wedge \neg B$	$\neg A \wedge B$	$(A \wedge \neg B) \vee (\neg A \wedge B)$ $(*)$	$B \Leftrightarrow (*)$	$A \Leftrightarrow (*)$	**(??)**
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. □

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."

□

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: $A \vee \neg A$), its truth subspace coincides with the whole assignment space
  - *Contradiction*: a proposition that is always false (example: $A \wedge \neg A$), its truth subspace is empty

1.1.1 *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. $A \Leftrightarrow \neg(\neg A)$, the law of double negation
2. $A \wedge B \Leftrightarrow B \wedge A$, $A \vee B \Leftrightarrow B \vee A$, commutativity of conjunction and disjunction
3. $A \wedge (B \wedge C) \Leftrightarrow (A \wedge B) \wedge C$, $A \wedge (B \vee C) \Leftrightarrow (A \vee B) \vee C$, associativity laws
4. $A \vee (B \wedge C) \Leftrightarrow A \vee B \wedge A \vee C$, $A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge$ distributivity laws

5. $A \wedge A \Leftrightarrow A, \quad A \vee A \Leftrightarrow A$
6. $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
7. $\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$, De Morgan's laws (6. and 7.)
8. $(A \Rightarrow B) \Leftrightarrow (\neg B \Rightarrow \neg A)$
9. $(A \Rightarrow B) \Leftrightarrow \neg A \vee B$
10. $(A \Rightarrow B) \Leftrightarrow \neg(A \wedge \neg B)$
11. $(A \Leftrightarrow B) \Leftrightarrow (A \Rightarrow B) \wedge (B \Rightarrow A)$
12. $(A \Leftrightarrow B) \Leftrightarrow (B \Leftrightarrow A)$, commutativity of equivalence
13. $(A \Leftrightarrow B) \Leftrightarrow (\neg A \Leftrightarrow \neg B)$
14. $(A \Leftrightarrow B) \Leftrightarrow (\neg A \vee B) \wedge (A \vee \neg B)$
15. $(A \Leftrightarrow B) \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$
16. $\neg(A \Leftrightarrow B) \Leftrightarrow (A \Leftrightarrow \neg B)$

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.

1.1.2 *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 $A_1, \ldots, A_n$, associate the conjunction

$$C_1 \wedge \ldots \wedge C_n$$

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 sre 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

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

The canonical CNF of D is

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

□

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?" §

1.1.3 *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).

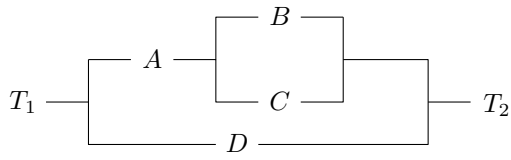
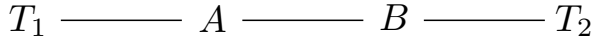


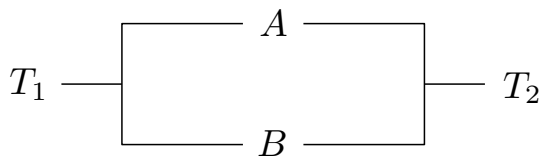
Figure 1: An example of a circuit with four switches

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 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: **c**onjunction.
(2) *two switches connected in parallel:*



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

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:

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

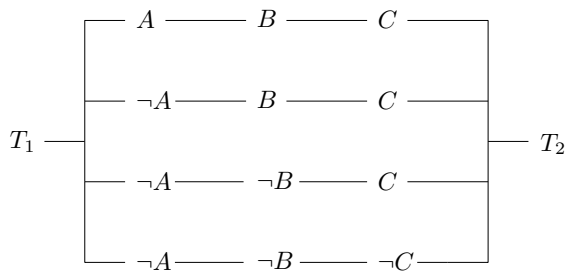
We computed its truth table in Chapter 1.2:

	A	B	C	$(A \Rightarrow B) \wedge (B \Rightarrow C) \wedge (\neg A \vee C)$
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:

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

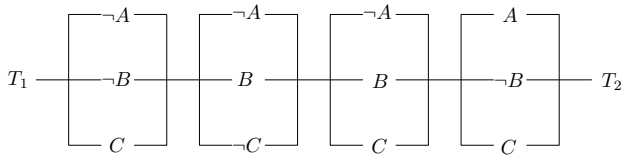
This form corresponds to the following circuit:



On the other hand, the canonical CNF

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

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. §

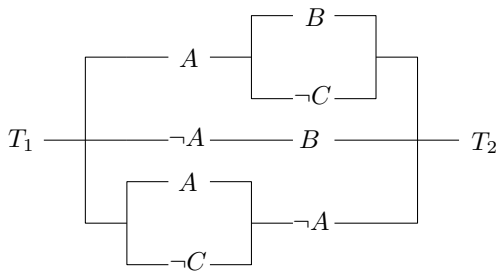
EXAMPLE. Consider the following switching circuit:

For which switch positions is the circuit closed?

Let us solve the problem with logic.

The corresponding proposition, say D, is:

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

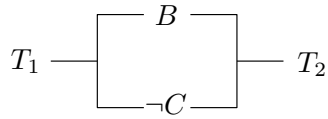


Its truth table is:

	A	B	C	A ∧ B ∨ ¬C	¬A ∧ B	A ∨ ¬C ∧ ¬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:

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

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

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

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

$$B \vee \neg C.$$

§

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

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

and in case (b)

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

The corresponding circuits are depicted on Figure **??**. §

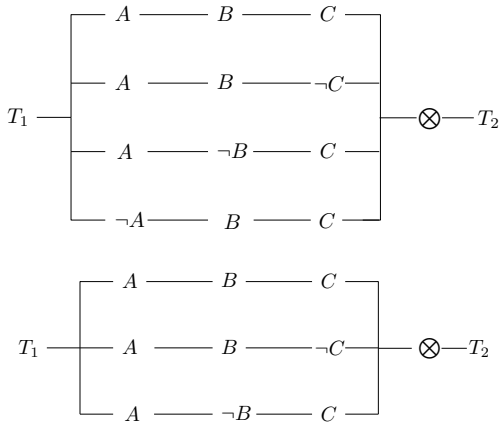


Figure 2: The corresponding circuits for the comittee (a) withouth a veto member (above), and (b) with veto for the member A (below).

1.1.4 *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.

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. §

1.2 PROOFS

Here we describe several types of proofs. **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. □

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. □

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.) □

1.2.1 *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:

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

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

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

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

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

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".

*F*or 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:

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

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

EXAMPLE. Let us write the negation of the proposition

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

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

$$\Leftrightarrow$$

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

$$\Leftrightarrow$$

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

$$\Leftrightarrow$$

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

§

- 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:

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

  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: $\neg A_1 \vee A_2$
C_2: $A_1 \Rightarrow A_3$
B: $\neg A_2 \Rightarrow \neg A_3$.
We have to determine whether the implication

$$C_1 \wedge C_2 \Rightarrow B$$

is a tautology.

1.2.2 *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. $A \vee \neg A$.

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

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}
1	1	1	1	1	1	1	1	1	1	0	0	0	0	0	0
1	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0
0	1	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

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

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:

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

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

$$A \Leftrightarrow \neg B.$$

□

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 $a \in \{a\}$.

2.1.1 *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: $A \subseteq B$

$$A \subseteq B \ \Leftrightarrow \ (\forall x)(x \in A \ \Rightarrow \ x \in B)$$

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: $A \subset B$.

$$A \subset B \ \Leftrightarrow \ (A \subseteq B \ \wedge \ A \neq B)$$

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?

2.1.2 *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.

2.1.3 *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: $A \subseteq B \ \wedge \ B \subseteq C \ \Rightarrow \ A \subseteq C$
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, $A \subseteq C$.

2.1.4 *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.

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

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.

2.1.5 *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 **p**rinciple 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). §

2.1.6 *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 $\mathcal{A} = \{A_\lambda\,;\,\lambda \in J\}$:

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

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

Ordered tuples

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 $1 \leqslant i \leqslant k$. Usually we use only ordered 2-tuples, which are also called ordered pairs.

2.1.7 *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:

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

Empty set

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

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

Of course it holds that:

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

Ordered pair

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 pair*:
(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 pair (a, b) can also be defined as the set $\{\{a\}, \{a, b\}\}$.

Homework: Prove that

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

Appendix

A

ADDITIONAL TOPICS FROM SET THEORY

A.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:

$$0,5 = \left\{ \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \cdots \right\}$$

(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).

A.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: *T*here is an empty set.

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

3. Axiom of pairing: *A*ny 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: *T*he 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: *F*or 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: *T*he 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. (For $k = 1$):

   $\forall a\, \forall c\, \exists B\, \forall x\, (x \in B \;\Leftrightarrow\; x \in c \;\wedge\; x \in a)$

   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. $\{x \in \mathbb{R}; x \geqslant 0\}$.

7. Axiom of infinity: *T*here exists an infinite set.

$$\exists A\, (\emptyset \in A \;\wedge\; (\forall a \in A)\, (a \cup \{a\} \in A))$$

8. Axiom schema of replacement: *T*he 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 $\{x \in \mathbb{R}; x \geqslant 0\}$.

9. Axion of regularity: *E*very 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: *E*ach 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.