TCS I: DISCRETE STRUCTURES*

CONTENTS

*This is a lecture draft for TCS I – fall 2020, and is supposed to be parsed together with explanations from the lectures. For any questions or found errors in the lecture-notes please write to matjaz.krnc@upr.si.

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.

1.1 *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.)*

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.*

Disjunction: A or B (inclusive)
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."

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.*

1.2 *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:

Negation

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

Conjunction, disjunction, implication and equivalence

	A, B	$A \land B$	$A \lor B$	$A \Rightarrow B$	$A \Leftrightarrow B$
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 $A_1, \dots, A_n$, can be written as the result of successive uses of the 5 basic connectives on the propositions $A_1, \dots, A_n$ 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. $(A \Rightarrow B) \land (B \Rightarrow C)$
4. $(\neg A)$
5. $((\neg A) \lor C)$
6. $(((A \Rightarrow B) \land (B \Rightarrow C)) \land ((\neg A) \lor C)))$

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

$$(((A \Rightarrow B) \land (B \Rightarrow C)) \land ((\neg A) \lor C))) \tag{1}$$

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

$$A \Rightarrow B \land B \Rightarrow C \land \neg A \lor C\,.$$

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.

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:

$$[A \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)] \wedge [B \Leftrightarrow (A \wedge \neg B) \vee (\neg A \wedge B)]. \tag{3}$$

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 $A_1, \dots, A_n$, 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 $A_1, \dots, A_n$.

- *Truth assignment of A*: assignment of values 1 / 0 (true / false) to each of the propositions $A_1, \dots, A_n$
- *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

1.3 *Logical equivalences*

Consider two propositions B and C, composed of propositions $A_1, \dots, A_n$. 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. $A \wedge B \Leftrightarrow B \wedge A$, $\quad A \vee B \Leftrightarrow B \vee A$, 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. $A \vee (B \wedge C) \Leftrightarrow A \vee B \wedge A \vee C, \quad A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C),$ 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.

1.4 *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?" ▲

1.5 *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).

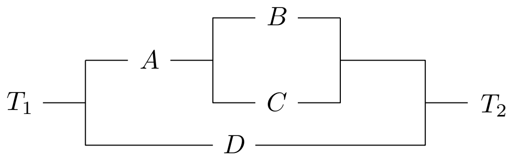
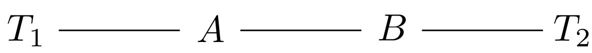


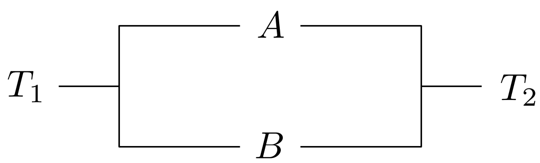
Figure 1: An example of a circuit with four switches

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: **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:

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

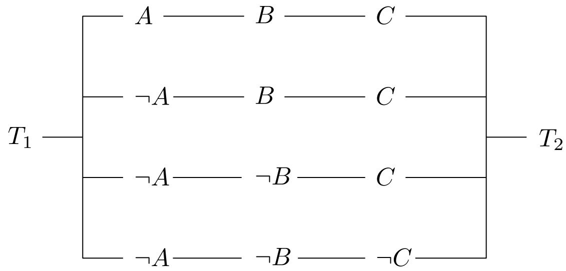
We computed its truth table in Chapter 1.2:

	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:

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

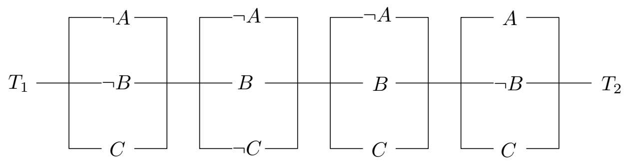
This form corresponds to the following circuit:



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. ▲

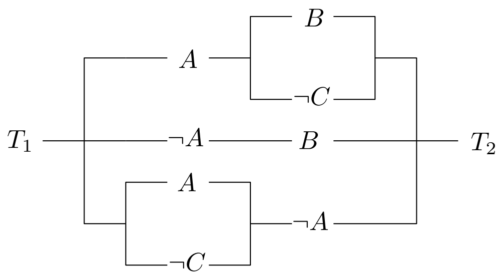
Example: Consider the following switching circuit:

For which switch positions is the circuit closed?

Let us solve the problem with logic.

The corresponding proposition, say D, is:

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

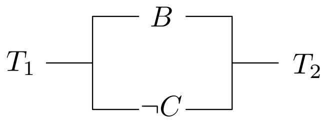


Its truth table is:

	A	B	C	$A \wedge B \vee \neg C$	$\neg A \wedge B$	$A \vee \neg C \wedge \neg A$	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:

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

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 2. ▲

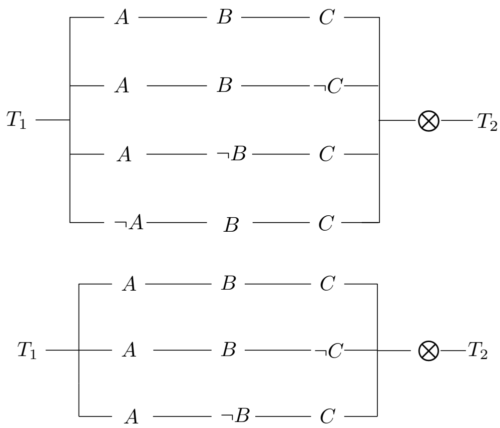


Figure 2: The corresponding circuits for the comittee (a) withouth a veto member (above), and (b) with veto for the member A (below).

1.6 *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. ▲

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.) □

1.7 *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).

1.7.1 *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:

$$\begin{aligned}
&\neg(\exists x)(\frac{1}{1+x^2} > 1)\\
\Leftrightarrow\ &(\forall x)\neg(\frac{1}{1+x^2} > 1)\\
\Leftrightarrow\ &(\forall x)(\frac{1}{1+x^2} \leq 1)\\
\Leftrightarrow\ &(\forall x)(1 \leq 1+x^2)\\
\Leftrightarrow\ &(\forall x)(0 \leq x^2)
\end{aligned}$$

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.