1b. Applications of mathematical logic

Grzegorz Kosiorowski

Krakow University of Economics

1. Application: formal proofs
2. Application: definitions and proofs of set theory
3. Application: logic gates and circuits

Motivation

- Rigorous reasoning and proving every claim in line with the laws of logic constitutes the basis of mathematics.
- Most theorems are implications (or equivalences).
- Set of premises: $P_1, P_2, \ldots, P_n$. A **proof** is a reasoning leading (in line with the laws of logic) from premises and other true sentences to the conclusion C.
- What techniques can we use to get from the premises to the conclusion?

Direct proof

The most common type of proof:

Direct proof

A **direct proof** is a sequence of implications from leading from the premises to the conclusion of a claim:

$$P_1 \wedge P_2 \wedge \ldots \wedge P_n \Rightarrow \ldots \Rightarrow C.$$

Direct proof - example

An example of a direct proof:

Claim

If m and n are natural, odd numbers, then their product mn is an odd number.

Proof: m, n are odd (premise). There are $k, l \in \mathbb{N}$ such that $m = 2k + 1$ and $n = 2l + 1$ (by properties of odd numbers). Therefore, $mn = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ (implication by multiplication). $2(2kl + k + l)$ is divisible by 2(arithmetics of integers) and thus even, therefore (another implication) $mn = (2k + 1)(2l + 1) = 2(2kl + k + l) + 1$ is odd (arithmetics of integers). QED.

Indirect proof

However, sometimes we use:

Indirect proof

An **indirect proof** is a proof based on the law of contraposition:

$$\sim C \Rightarrow \ldots \Rightarrow \sim (P_1 \wedge P_2 \wedge \ldots \wedge P_n)$$

where C is a conclusion of the claim that is to be proven and $P_1, P_2, \ldots, P_n$ are its premises.

Indirect proof - example

Claim

Let m and n be natural numbers. If $m + n \geqslant 9$, then either $m \geqslant 5$ or $n \geqslant 5$.

Proof: We prove the contradiction: if it is false that ($m \geqslant 5$ or $n \geqslant 5$), then $m + n \geqslant 9$ is also false. So we assume the negation of ($m \geqslant 5$ or $n \geqslant 5$). By de Morgan's Theorem and the fact that m and n are natural numbers, our new premise is equivalent to a conjunction $m \leqslant 4 \wedge n \leqslant 4$. By arithmetics of natural numbers, we can add both sides of these inequalties to obtain $m + n \leqslant 8$, which in turn implies $\sim (m + n \geqslant 9)$. QED.

A proof by contradiction

There exists an important variant of the indirect proof:

Proof by contradiction

A **proof by contradiction** (or: by reductio ad absurdum) is a proof based on the sentence:

$$(P_1 \wedge P_2 \wedge \ldots \wedge P_n) \wedge (\sim C) \Rightarrow \ldots \Rightarrow 0.$$

where C is a conclusion of the claim that is to be proven and $P_1, P_2, \ldots, P_n$ are its premises.

Namely, we assume that the claim is false, and then we prove that it leads to obviously false consequences.

Example

We will prove the following claim by contradiction:

Claim

If $x^2 = 2$, then x is irrational.

Proof: We assume that $x^2 = 2$ and x is rational. Then, there exist integers p, q $(q \neq 0)$ with no common divisors other than 1 such that $x = \frac{p}{q}$. Therefore, $\left(\frac{p}{q}\right)^2 = 2$, hence $p^2 = 2q^2$. Thus p^2 is even, consequently p is even, so $p = 2k$ for a certain integer k. Thus, $(2k)^2 = 2q^2$, and $2k^2 = q^2$. Therefore, q^2 is even, so also q is even. We assumed that p and q have no common divisors but 1, however it is false as they are both even, so 2 is their common divisor. Thus, the assumption that x is rational leads to contradiction, so x must be irrational. QED.

Set theory

Logic is also a main tool of the set theory: one of the foundational domains of mathematics. We use logic to define basic operations on sets and also prove theorems about sets. Let us recall the notation for most popular sets of numbers:

- $\mathbb{N}$ - natural numbers (including 0), $\mathbb{N}_+$ - positive natural numbers, $\mathcal{P}$ - prime numbers.
- $\mathbb{Z}$ - integers.
- $\mathbb{R}$ - real numbers.
- $\mathbb{C}$ - complex numbers.
- $\emptyset$ - the empty set.

Throughout this course, unless we directly say otherwise, any number by default is an element of $\mathbb{Z}$.

Relations of sets

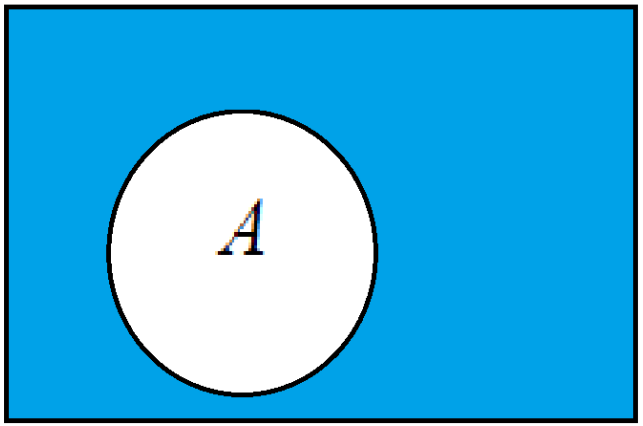
Three basic relations of the set theory are:

- $x \in A$ (x is typically not a set!) - x belongs to A/ x is an element of A. If x does not belong to A we write $x \notin A$.
- $A \subset B$ (A and B are sets!) - A is a subset of B/A is included in B; a logical definition: $x \in A \Rightarrow x \in B$ (set theoretic equivalent of implication).
- $A = B$ - a logical definition: $x \in A \Leftrightarrow x \in B$ (set theoretic equivalent of equivalence).

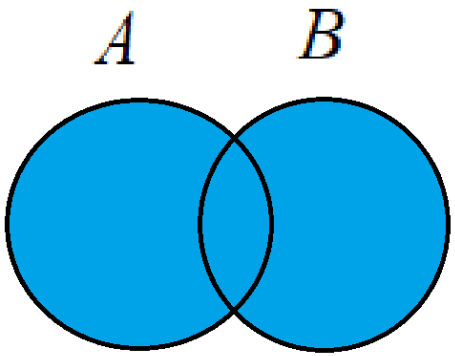
Operations on sets

- If we know that we are operating inside a larger set X (sometimes termed a *universum*), and $A \subset X$, then A^c lub A' is termed a **complement** of A to X and defined as $x \in A^c \Leftrightarrow \sim (x \in A)$ (equivalent of negation).
- A **union** of sets $A \cup B$ is defined as: $x \in A \cup B \Leftrightarrow (x \in A \vee x \in B)$ (equivalent of alternative).
- An **intersection** $A \cap B$ is defined as: $x \in A \cap B \Leftrightarrow (x \in A \wedge x \in B)$ (equivalent of conjunction).
- A **set difference** $A \setminus B$ is defined as: $x \in A \setminus B \Leftrightarrow (x \in A \wedge x \notin B)$.
- By $|X|$ we will denote the *cardinality* of a set X, namely, the number of elements of X.

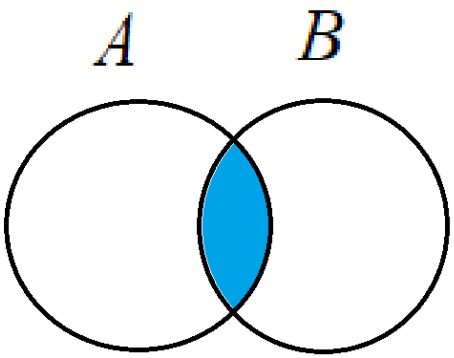
Operations on sets - illustration



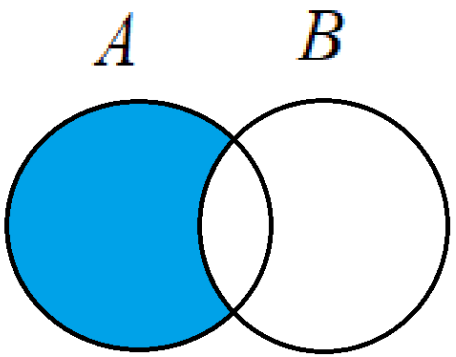
$A' = A^c$



$A \cup B$



$A \cap B$



$A \setminus B$

Operations on sets - a Cartesian product

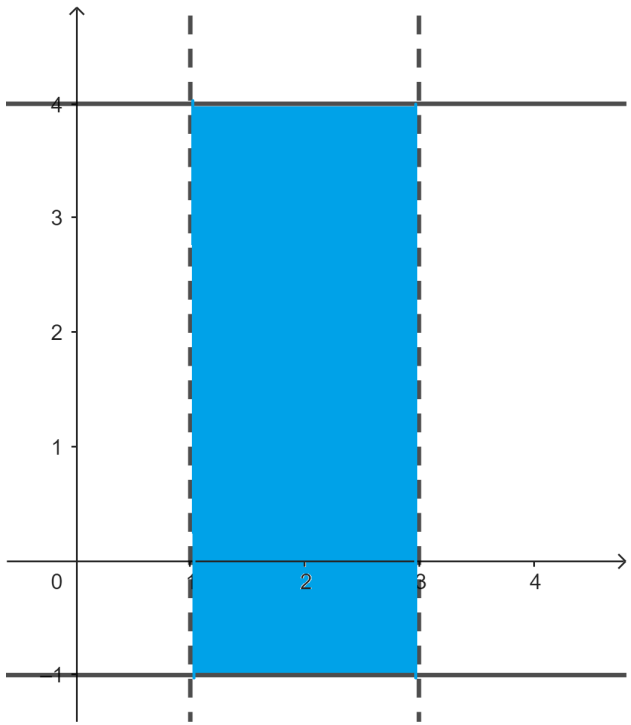
Cartesian product

A **Cartesian product** $A \times B$ of sets A and B is the set whose members are all possible ordered pairs (a, b) such that $a \in A$ and $b \in B$.

$$(a, b) \in A \times B \Leftrightarrow (a \in A \wedge b \in B).$$

Cartesian product - examples

If $A = \{x, y\}$ and $B = \{y, 0, 1\}$, then
$A \times B = \{(x, y),\ (x, 0), (x, 1), (y, y), (y, 0), (y, 1)\}$.
A Cartesian product of subsets of $\mathbb{R}$ are often presented on the plane, here $(1, 3) \times [-1, 4]$:



Laws of logic and theorems of set theory

Laws of logic are the main tool for proving inclusions and equalities of sets:

Task

Let $A, B \subset X$ for some universum X. Prove that $(A \cap B)^c = A^c \cup B^c$.

By definition of equality, we are to prove:

$$x \in (A \cap B)^c \Leftrightarrow x \in (A^c \cup B^c).$$

Logic and sets

$$x \in (A \cap B)^c \Leftrightarrow x \in (A^c \cup B^c)?$$

We assume that the left hand side of equivalence is true and we try to use definitions and laws of logic to equivalently transform it to the right side:

$$x \in (A \cap B)^c \Leftrightarrow \sim (x \in A \cap B) \Leftrightarrow \sim (x \in A \wedge x \in B).$$

We use de Morgan Theorem:

$$\sim (x \in A \wedge x \in B) \Leftrightarrow [\sim (x \in A) \vee \sim (x \in B)] \Leftrightarrow$$

$$\Leftrightarrow (x \in A^c \vee x \in B^c) \Leftrightarrow x \in (A^c \cup B^c).$$

By transitivity of equivalences we obtained the conclusion. Q.E.D

Operations on multiple sets

Analogously, we define operations on more than 2 sets:
A union of sets $A_1, A_2, \ldots, A_k$:

$$\bigcup_{i=1}^{k} A_i = A_1 \cup A_2 \cup \ldots \cup A_k$$

An intersection of sets $A_1, A_2, \ldots, A_k$:

$$\bigcap_{i=1}^{k} A_i = A_1 \cap A_2 \cap \ldots \cap A_k$$

Operations on multiple sets

A Cartesian product of $A_1, A_2, \ldots, A_k$ is a set of k-tuples (k-element sequences) whose subsequent elements belong to subsequent sets of the list:

$$\prod_{i=1}^{k} A_i = A_1 \times A_2 \times \ldots \times A_k.$$

In particular:

$$A^n = A \times A \times \ldots \times A,$$

where we use the $\times$ sign $(n-1)$ times.
This is why $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is a standard notation for a Cartesian plane, namely a set of pairs of real numbers.

Some useful notation

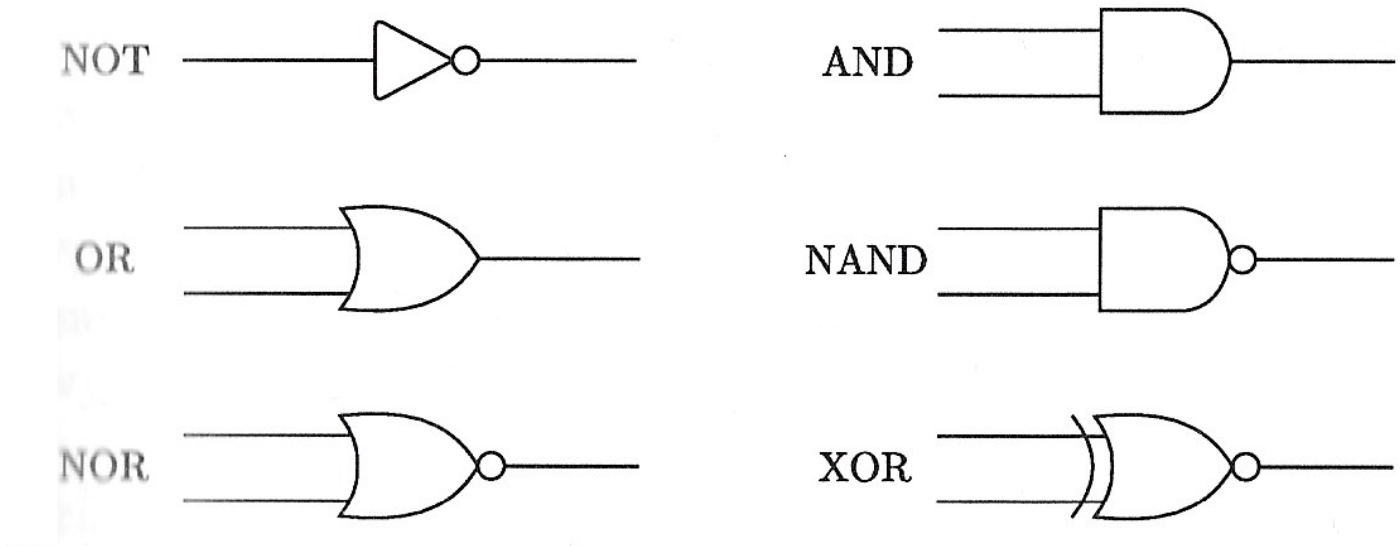
Some extra notation of set theory will become useful throughout the course:

- Set of all subsets of A (including A and $\emptyset$): $P(A)$ or 2^A.
- Set of all functions of domain A and codomain B: B^A.

Logic gates and circuits - motivation

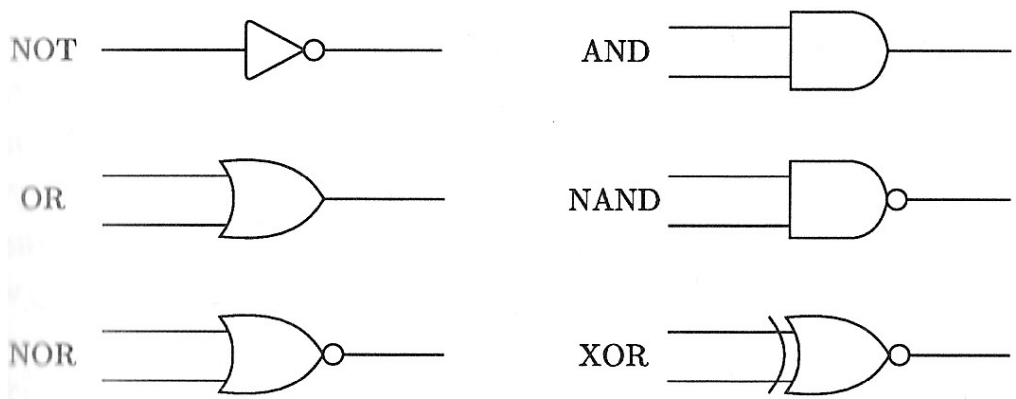
- Hardware level computer science: constructing physical devices providing proper results for given inputs.
- Both inputs and outputs may be presented as zeroes and ones (e.g. by manipulating electric currents), thus they can be modeled in the language of mathematical logic.
- Such systems, known as *logic circuits*, are built of simple units called logic gates that realize different truth functions. Physical devices constructed to represent such gates are available on the market.
- We will analyze the standard notation of diagrams for logic circuits.

Logic gates - notation



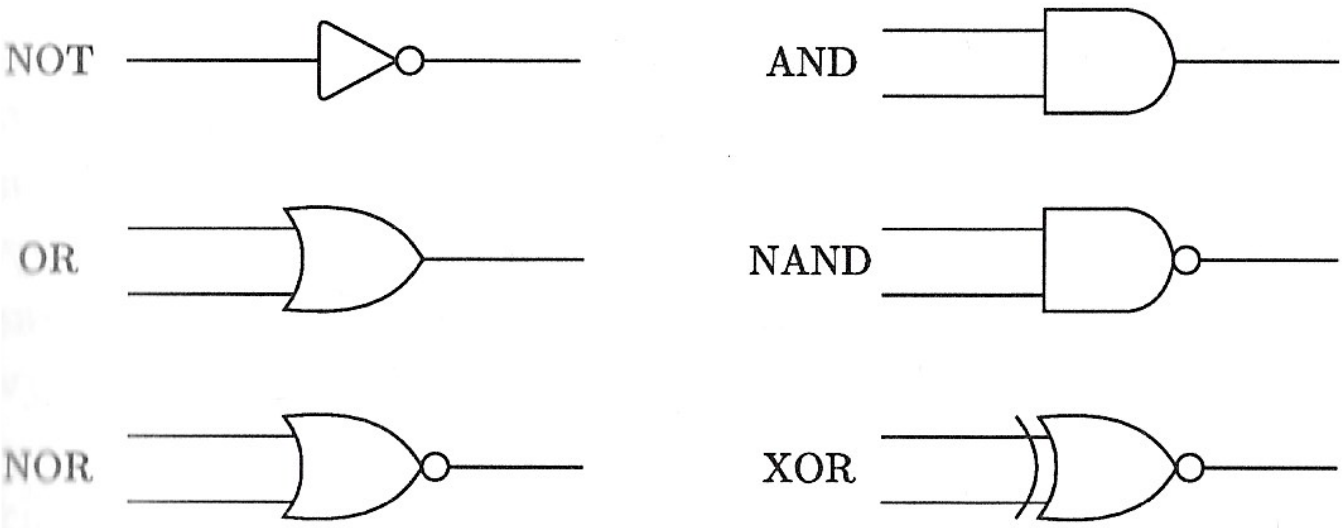
The figure above presents the notation for the most common logic gates (in line with ANSI/IEEE standard). Lines coming into the symbol from the left are inputs (providing arguments of values 0 or 1 to truth functions represented by a gate) while lines on the left contain output of a relevant function (again, 0 or 1).

Logic gates - notation



A gate NOT represents negation (changes a value into its "complement"). A gate AND represents conjunction (two arguments are changed into a value of their conjunction), OR - alternative, NAND and NOR are negations of conjunction and alternative, respectively (the "bubbles" at the end generally denote negation), and XOR is an exclusive alternative. The next slide is a recollection of their outputs for given inputs x and y.

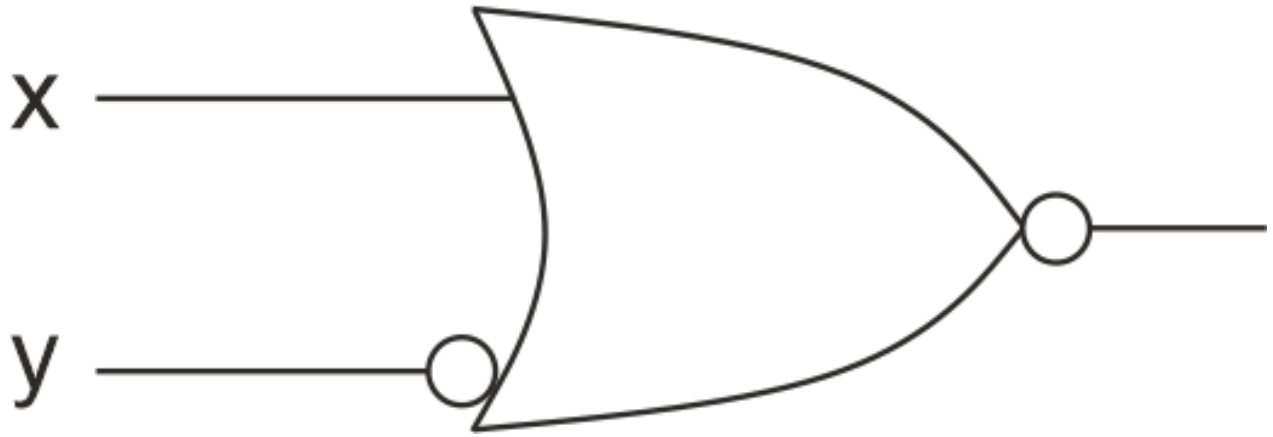
Logic gates - notation



x	y	$NOT(x)$	OR	NOR	AND	NAND	XOR
1	1	0	1	0	1	0	0
1	0	0	1	0	0	1	1
0	1	1	1	0	0	1	1
0	0	1	0	1	0	1	0

Logic gates - notation

A bubble at the end of a gate represents a simplified negation gate (technical name: an inverter) changing 0 into 1 and 1 into 0.

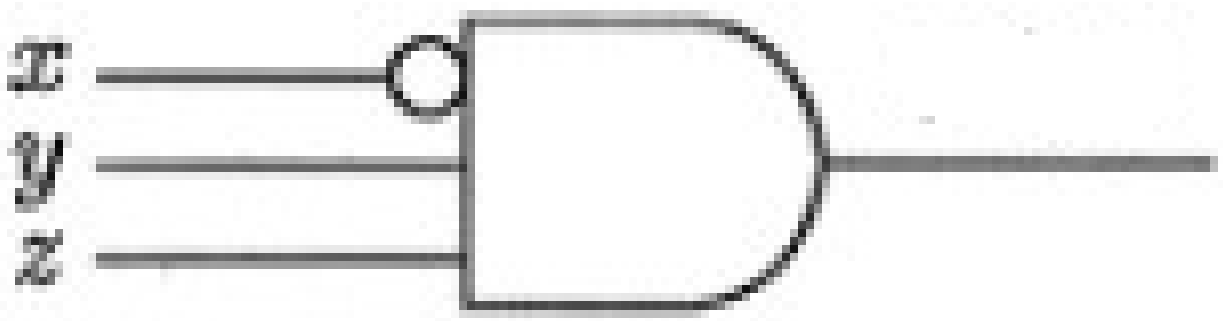


The gate above represents:

$$\sim (x \vee \sim y).$$

Logic gates - notation

In the same way as for truth functors, it is possible to generalize logic gates so that they may be provided with more than 2 inputs:



A gate presented above represents:

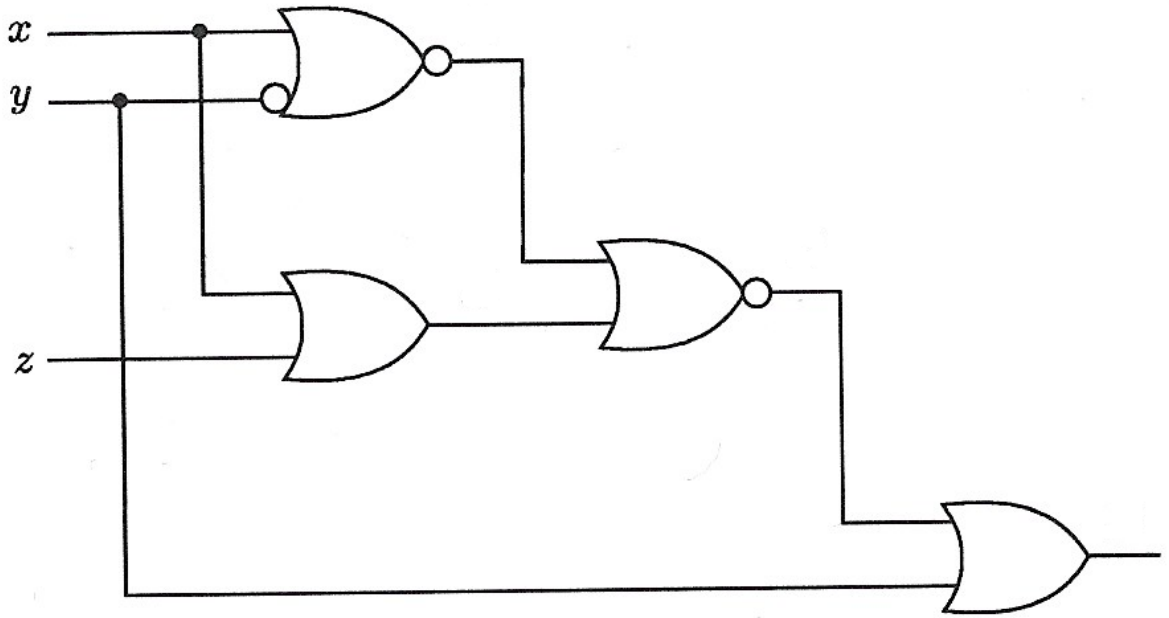
$$(\sim x) \wedge y \wedge z.$$

Logic applied to circuits

Devices based on logic circuits (such as microprocessors) usually operate on a giant number of inputs and gates. There are usually multiple ways to build a circuit representing a desired outcome. However, it is important to optimize such circuits for example with respect to:

- minimal number of logic gates;
- minimal length of the longest sequence of gates;
- other factors, depending on a problem.

Optimizing a circuit - example



This circuit correctly represents the following formula:

$$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y.$$

But it is unnecessarily complicated.

Optimizing a circuit - example

Building a truth table for this formula (intermediate steps are left as an exercise) we obtain:

$$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y.$$

x	y	z	$\sim [\sim (x \vee \sim y) \vee (x \vee z)] \vee y$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	1

Optimizing a circuit - example

We can obtain the same result by much simpler formula:

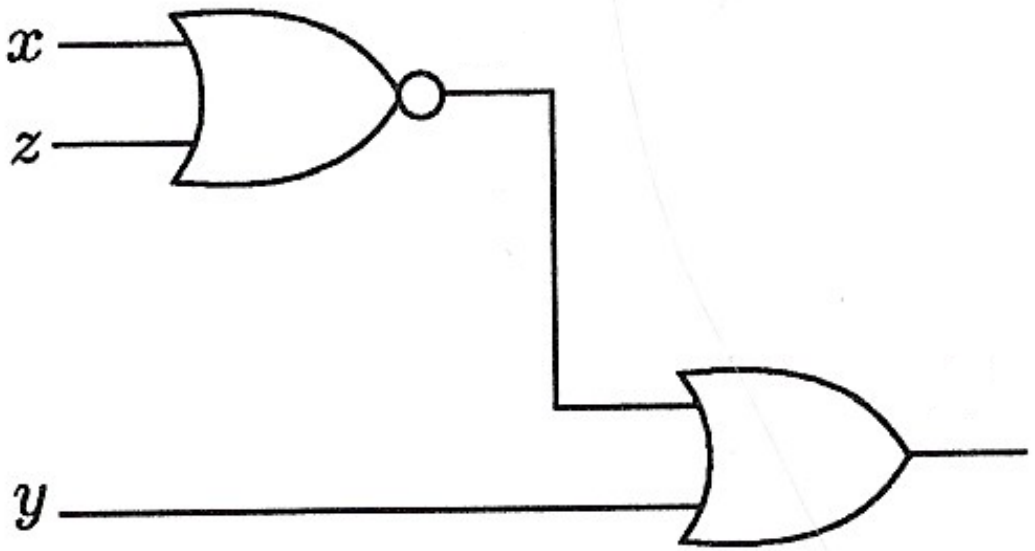
$$\sim (x \vee z) \vee y.$$

x	y	z	$\sim (x \vee z) \vee y$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	1

Optimizing a circuit - example

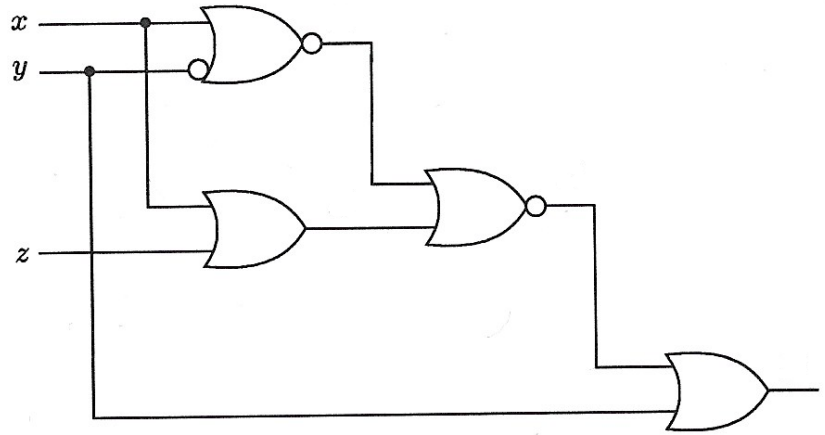
$$\sim (x \vee z) \vee y.$$

This formula is represented by a more optimal (with respect to both the number of gates and the longest sequence of gates) logic circuit:

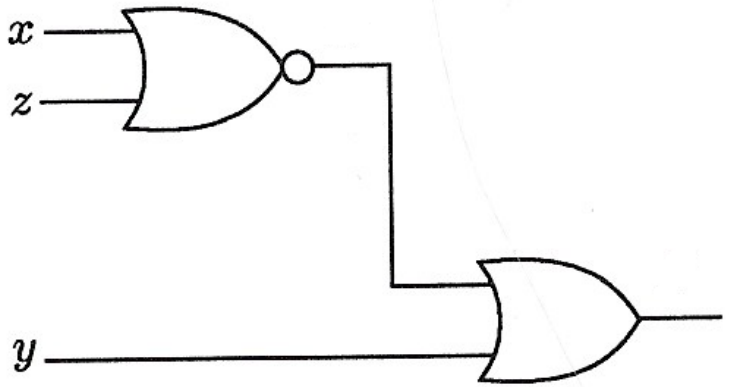


Optimizing a circuit - example

Summarizing, this circuit:



can be replaced by a simpler one:



Optimizing a circuit - general approach

Generally, optimizing circuits is an intresting but difficult issue that may be formalized (to some extent) into an algorithmic approach. This falls beyond the scope of our lecture. If anyone is interested in delving into this topic, I suggest looking for information about:

- Karnough maps;
- Quine-McCluskey algorithm.