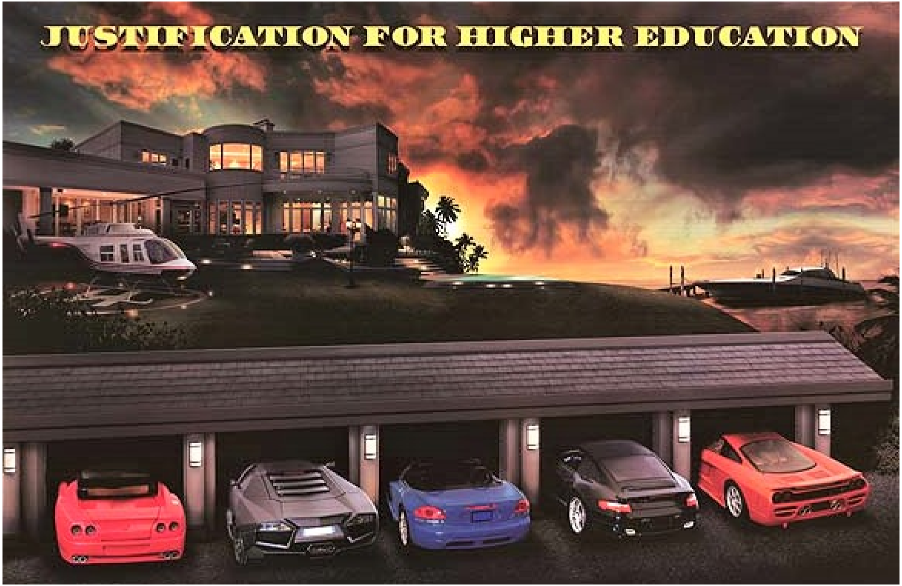
Mathematics for Computer Science

Prof. dr.hab. Viorel Bostan

Technical University of Moldova

viorel.bostan@adm.utm.md

Lecture 3


JUSTIFICATION FOR HIGHER EDUCATION

Previous Lecture

- Cardinality of power set;
- Uncountable sets;
- Uncountability of real numbers;
- What is Mathematical Logic? Proposition.
- What is a proof?

  Method/procedure to ascertain the truth!
- Axioms; ZFC Axioms;

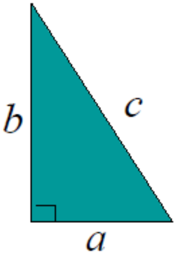
Definition

A formal **proof** of a proposition is a chain of logical deductions leading to the proposition from a base set of axioms.

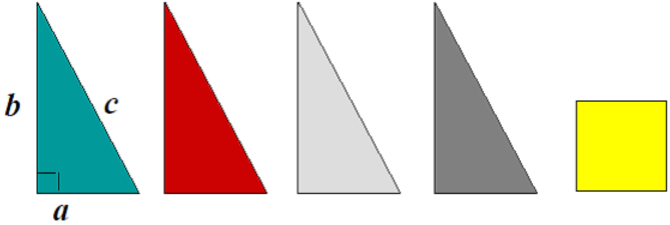
- Consistency and Completeness of Axioms.

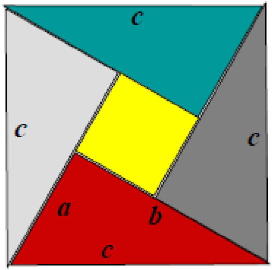
Pythagoras Theorem:

$$a^2 + b^2 = c^2$$



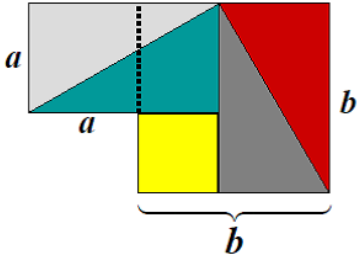
Proofs

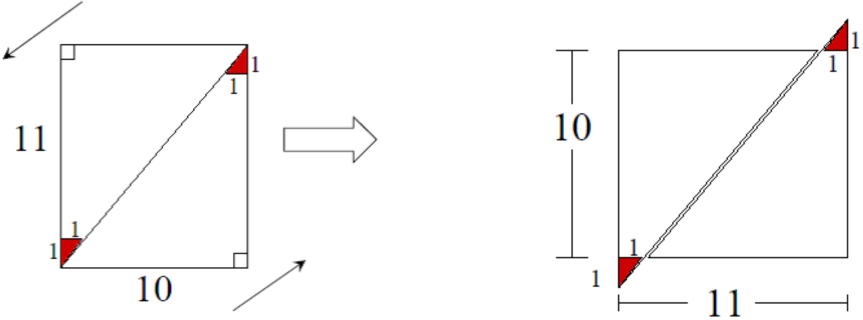


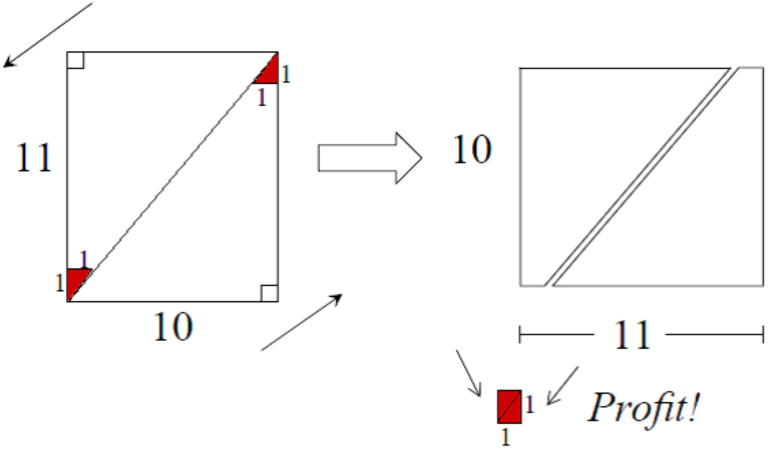


Size of yellow square?

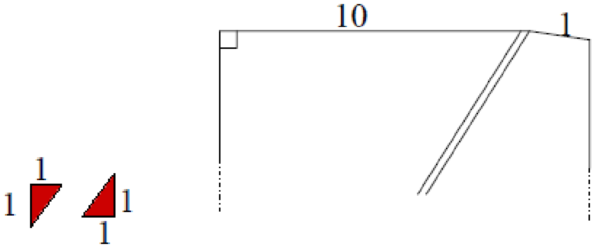
$(b - a) \cdot (b - a)$




11
10
1
1
1
1
10
11
1
1
1
1


11
1
1
1
1
10
10
11
1
1
Profit!

This is a false proof!



Another false proof:

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = \left(\sqrt{-1}\right)^2 = -1$$

Moral: Mindless calculations are not safe.

1. Be sure that right rules are properly applied!
2. Calculation is a risky substitute for understanding!

Consequences of $1 = -1$

$$
\begin{aligned}
1 &= -1 \\
\frac{1}{2} &= -\frac{1}{2} \quad (\text{multiply by } \frac{1}{2}) \\
2 &= 1 \quad \left(\text{add } \frac{3}{2}\right)
\end{aligned}
$$

Bertrand Russel, being asked what is wrong with $2 = 1$, said:

> Since I and the Pope are clearly 2, and $2 = 1$,
> we conclude that I and the Pope are 1.
> That is, I am the Pope.

Erroneous proofs

Approximately $1/3$ of all mathematical papers contain errors. Some famous examples:

- Pierre Fermat in on the margins of Diophantus Arithmetic, carelessly stated the proposition later to became one of the greatest problems in Mathematics.
- For 500 years it was unsolved. Hundreds of attempts have been made to prove the Fermat Theorem! Some of the proofs have been considered correct for few years, until an error was later found.
- In 1993 after working almost in secrecy six years Andrew Wiles announced a proof of Fermat's Last Theorem. It was several hundred pages long.
- It took mathematicians months of hard work to discover it had a fatal flaw, **a bug**. After one year, Wiles produced another proof of several hundred pages; this one seems to be correct.

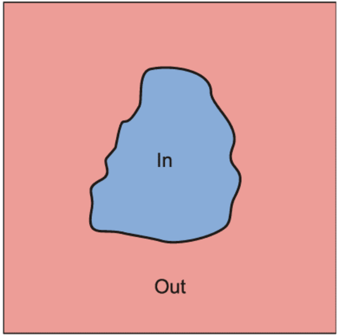
Even great minds can be wrong

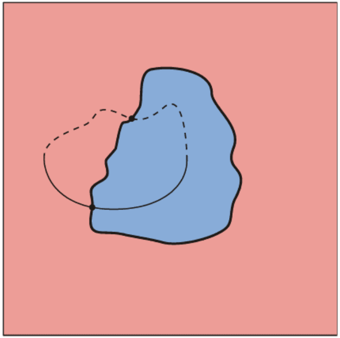
Carl Friedrich Gauss, one of the greatest mathematicians of all times. Gauss's 1799 PhD thesis is usually referred to as being the first rigorous proof of the Fundamental Theorem of Algebra (every polynomial has a zero over the complex numbers). But it contains quotes like:

Gauss mistake

> *"If a branch of an algebraic curve enters a bounded region, it must necessarily leave it again. ... Nobody, to my knowledge, has ever doubted [this fact]. But if anybody desires it, then on another occasion I intend to give a demonstration which will leave no doubt."*

It was an "immense gap" in the proof that was not filled in until 1920, more than a hundred years later, by Jordan Curve Theorem.





A **proof** of a proposition is a sequence of logical deductions from axioms and previously proved statements that concludes with the proposition in question.

How to start a proof? Many proofs follow one of a handful of standard templates.

An enormous number of mathematical propositions have the form:

$$\text{“If} \quad P, \quad \text{then} \quad Q\text{''}$$

or, equivalently, “P implies Q” or ”$P \Rightarrow Q$”.

- If $ax^2 + bx + c = 0$ and $a \neq 0$, then $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$.
- If n is an even integer greater than 2, then n is a sum of two primes.
- If $0 \leqslant x \leqslant 2$, then $-x^3 + 4x + 1 > 0$.

In order to prove that P implies Q:

1. Write, "Assume P." (meaning that we assume P is a true proposition).
2. Show that Q **logically** follows. In other words, show that Q is also true.

Theorem

If $0 \leqslant x \leqslant 2$, *then* $-x^3 + 4x + 1 > 0$.

Proof.

Suppose $0 \leqslant x \leqslant 2$. Then, factor expression

$$-x^3 + 4x = x(2 - x)(2 + x).$$

Then, observe that x, $2 - x$, and $2 + x$ are all nonnegative.

Thus, the product of these terms is also nonnegative.

Clearly, $-x^3 + 4x \geqslant 0$.

Therefore, $-x^3 + 4x + 1 > 0$. $\square$

Method nr. 2: prove the contrapositive

An implication ("P implies Q") is logically equivalent to its **contrapositive**, which means: "not Q implies not P". Often proving the contrapositive is easier.

Theorem

If r is irrational, then $\sqrt{r}$ is also irrational.

Proof.

Prove the contrapositive: if $\sqrt{r}$ is rational, then r is rational.
Assume that $\sqrt{r}$ is rational. Then, there exists integers a and b such that:

$$\begin{aligned} \sqrt{r} &= \tfrac{a}{b}, \\ \left(\sqrt{r}\right)^2 &= \left(\tfrac{a}{b}\right)^2, \\ r &= \tfrac{a^2}{b^2}. \end{aligned}$$

Since a^2 and b^2 are integers, then r is rational. $\square$

Method nr.3: prove by contradiction

In order to prove a proposition P by contradiction:

1. Write, "Proof by contradiction."
2. Write, "Suppose P is false."
3. Deduce a logical contradiction.
4. Write, "This is a contradiction. Therefore, P must be true."

Theorem

$\sqrt{2}$ *is irrational.*

Proving by contradiction

Proof.

Proof by contradiction. Suppose the claim is false; that is, $\sqrt{2}$ is rational.
Then, there exist integers a and b such that

$$\sqrt{2} = \frac{a}{b}$$

and this fraction is irreducible.
Squaring both sides, gives $2 = \frac{a^2}{b^2}$ and so, $2b^2 = a^2$.
This implies that a^2 is even;
So, a is also even, that is, $a = 2p$, for some integer p.
Therefore, $a^2 = 4p^2$ must be a multiple of 4.
Because of equality $2b^2 = a^2 = 4p^2$, we conclude that $2b^2$ must also be a multiple of 4.
This implies that $b^2 = 2p^2$ is even and so b must be also even.
But, since a and b are both even, the fraction $\frac{a}{b}$ is not irreducible.
This is a **contradiction**. Therefore, $\sqrt{2}$ must be irrational. $\square$

Method nr.4: prove by cases

Breaking a complicated proof into cases and proving each case separately.

Example

Suppose that that given any two people, either they have met or not.
If every pair of people in a group has met, we'll call the group a club.
If every pair of people in a group has not met, we'll call it a group of strangers.

Theorem

Every collection of 6 *people includes a club of* 3 *people or a group of* 3 *strangers.*

Method nr.4: prove by cases

Theorem

Every collection of 6 people includes a club of 3 people or a group of 3 strangers.

Proof.

The proof is by case analysis.
Let x denote one of the 6 people. There are 2 cases:

1. Among 5 other people besides x, at least 3 have met x.
2. Among 5 other people, at least 3 have not met x.

Have to be sure that at least one of these two cases must hold.

Indeed: split the 5 people into two groups:
– those who have shaken hands with x and
– those who have not shaken hands with x.

So, one of the groups must have at least half the people (i.e. 3).

Method nr.4: prove by cases

Proof.

Case 1: Suppose that at least 3 people did meet x.
This case splits into two subcases:

Case 1.1: No pair among those people met each other. Then these people are a group of at least 3 strangers.
The theorem holds in this subcase.

Case 1.2: Some pair among those people have met each other. Then that pair, together with x, form a club of 3 people.
So the theorem holds in this subcase.

This implies that the theorem holds in Case 1.

Method nr.4: prove by cases

Proof.

Case 2: Suppose that at least 3 people did not meet x.
This case also splits into two subcases:

Case 2.1: Every pair among those people met each other. Then these people are a club of at least 3 people.
The theorem holds in this subcase.

Case 2.2: Some pair among those people have not met each other. Then that pair, together with x, form a group of at least 3 strangers.
So the theorem holds in this subcase.

This implies that the theorem holds in Case 2 as well.
In conclusion, it holds for all cases. $\square$

Method nr.1

The statement P if and only if Q or $P \iff Q$ is equivalent to the two statements P implies Q and Q implies P .

So you can prove an **if and only if** by proving 2 implications:

1. Write: Prove P implies Q and vice versa.
2. Write: Show P implies Q.
3. Write: Show Q implies P.

Method nr.2 (Construct a Chain of Iffs)

In order to prove that P is true if and only if Q is true:

1. Write: Construct a chain of if and only if implications.
2. Prove P is equivalent to a second statement, which is equivalent to a third statement, and so forth, until you reach Q.

$$P \iff S_1 \iff S_2 \iff \ldots \iff S_n \iff Q$$

Generally more difficult than the first, but the result can be a short, elegant proof.

Question: If x and y are two irrational numbers, can x^y be rational?

Theorem

There exists numbers $x, y \notin \mathbb{Q}$ such that $x^y \in \mathbb{Q}$.

Proof.

Consider number $\sqrt{2}^{\sqrt{2}}$. If $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$, then theorem is proved.

Suppose $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$. Then,

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^{2} = 2 \in \mathbb{Q}.$$

$\square$

Observe, that we proved the above theorem, without finding numbers x and y.
Such proofs are called **non-constructive proofs**.

Moreover, we didn't even prove whether $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ or $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$.

A Wrong Method: Reasoning Backwards

Theorem (Arithmetic-Geometric Mean Inequality)

$$\forall a,\ b \in \mathbb{R}^+, \qquad \frac{a+b}{2} \geqslant \sqrt{ab}.$$

Proof.

$$\frac{a+b}{2} \overset{?}{\geqslant} \sqrt{ab}$$

$$a + b \overset{?}{\geqslant} 2\sqrt{ab}$$

$$(a+b)^2 \overset{?}{\geqslant} \left(2\sqrt{ab}\right)^2$$

$$a^2 + 2ab + b^2 \overset{?}{\geqslant} 4ab$$

$$a^2 - 2ab + b^2 \overset{?}{\geqslant} 0$$

$$(a-b)^2 \overset{?}{\geqslant} 0.$$

Why Reasoning Backward Is Bad

In reasoning backward, we began with a proposition P, and reasoned to a true conclusion. Thus, what we actually proved was: $P \implies \mathit{true}$.
But, this implication is trivially true, regardless of whether P is true or false! Therefore, by reasoning backward we can **prove** not only true statements, but also every false statement!

Theorem (Obviously false)

$$0 = 1.$$

Proof.

$$\begin{aligned} 0 &\stackrel{?}{=} 1, \\ 0 \cdot 0 &\stackrel{?}{=} 1 \cdot 0, \\ 0 &\stackrel{?}{=} 0. \end{aligned}$$

$\square$

Propositional logic formalizes the reasoning that can be done with **connectives** such as **not** , **and**, **or**, and **if . . . then**.

Define the formal language of propositional logic, $\mathcal{L}_P$ by specifying its symbols (alphabet) and rules for assembling these symbols into the formulas of the language.

Definition

The symbols of $\mathcal{L}_P$ are:

1. Parentheses: (and);
2. Connectives: $\neg$ and $\rightarrow$;
3. Atomic formulas: $A_0, A_1, A_2, \ldots, A_n, \ldots$

Use lower-case Greek letters (such as α, β, φ) to represent formulas, and upper-case Greek letters (such as Σ, Φ) to represent sets of formulas.

Definition

The **formulas** of $\mathcal{L}_P$ are those finite sequences or strings of the symbols given in previous definition which satisfy the following rules:

1. Every atomic formula is a formula;
2. If α is a formula, then $(\neg\alpha)$ is a formula;
3. If α and β are formulas, then $(\alpha \to \beta)$ is a formula;
4. No other sequence of symbols is a formula.

These are formulas:
A_{2013}, $(A_{100} \to A_1)$, $(A_0 \to A_0)$, $((\neg A_1) \to (A_2 \to A_{231}))$

These are NOT formulas:
X_2, (A_3), $(A_0 \to (\neg A_1)$, $(A_7 \neg A_1)$, $A_2 \to A_0$

Logic Formulas Examples

Consider atomic formulas:

$A_0 =$ "The moon is red."

$A_1 =$ "The moon is made of cheese."

Then, $(A_0 \to (\neg A_1))$ means: **If the moon is red, then it is not made of cheese!**

In what follows, use the symbols $\wedge$, $\vee$, and $\leftrightarrow$ to represent **and**, **or**, and **if and only if**.

Since they are not among the symbols of $\mathcal{L}_P$, use them as abbreviations for certain constructions involving symbols $\neg$ and $\to$:

- $(\alpha \wedge \beta)$ is short for $(\neg(\alpha \to (\neg\beta)))$ and it is called **conjunction** or logic textbfand.
- $(\alpha \vee \beta)$ is short for $((\neg\alpha) \to \beta)$ and it is called **disjunction** or logic **or**.
- $(\alpha \leftrightarrow \beta)$ is short for $((\alpha \to \beta) \wedge (\beta \to \alpha))$ and it is called **equivalence**.

"The moon is red and made of cheese" is written as $(A_0 \wedge A_1)$.

Or actually is $(\neg(A_0 \to (\neg A_1)))$.

Precedence Rules

Adapt informal conventions (allow to use fewer parentheses):

- Drop the outermost parentheses in a formula, writing $\alpha \to \beta$ instead of $(\alpha \to \beta)$ and $\neg\alpha$ instead of $(\neg\alpha)$;
- Let $\neg$ take precedence over $\to$ when parentheses are missing, so $\neg\alpha \to \beta$ is short for $((\neg\alpha) \to \beta)$, and fit the informal connectives into this scheme by letting the order of precedence be:

$$\neg, \quad \wedge, \quad \vee, \quad \to, \quad \leftrightarrow;$$

- Group repetitions of $\to$, $\wedge$, $\vee$, or $\leftrightarrow$ to the right when parentheses are missing, so $\alpha \to \beta \to \gamma$ is short for $((\alpha \to \beta) \to \gamma)$.

Subformulas

Definition

Suppose φ is a formula of $\mathcal{L}_P$. The **set of subformulas** of φ, $S(\varphi)$, is defined as follows:

1. If φ is an atomic formula, then $S(\varphi) = \{\varphi\}$;
2. If φ is $(\neg\alpha)$, then $S(\varphi) = S(\alpha) \cup \{\neg\alpha\}$;
3. If φ is $(\alpha \to \beta)$, then $S(\varphi) = S(\alpha) \cup S(\beta) \cup \{(\alpha \to \beta)\}$.

For example, let φ be the formula

$$(((\neg A_0) \to A_1) \to (A_2 \to (\neg A_1)))$$

Then the set of subformulas of φ is:

$$S(\varphi) = \{A_0,\, A_1,\, A_2,\, (\neg A_0)\,,\, ((\neg A_0) \to A_1)\,,\, (\neg A_1),\, (A_2 \to (\neg A_1)),\, \varphi\}$$

Subformulas

Observe that, dropping parentheses convention, allow us to rewrite formula

$$(((\neg A_0) \to A_1) \to (A_2 \to (\neg A_1)))$$

in

$$(\neg A_0 \to A_1) \to (A_2 \to \neg A_1)$$

and

$$S(\varphi) = \{A_0,\, A_1,\, A_2,\, (\neg A_0)\,,\, ((\neg A_0) \to A_1)\,,\, (\neg A_1),\, (A_2 \to (\neg A_1)),\, \varphi\}$$

can be rewritten as

$$S(\varphi) = \{A_0,\ A_1,\ A_2,\ \neg A_0,\ \neg A_0 \to A_1,\ \neg A_1,\ A_2 \to \neg A_1,\ \varphi\}$$

$$\neg A_0 \wedge \neg A_1 \leftrightarrow \neg(A_0 \vee A_1)$$

Using parentheses it should be

$$(((\neg A_0) \wedge (\neg A_1)) \leftrightarrow (\neg(A_0 \vee A_1)))$$

Truth Assignment

Whether a given formula φ of $\mathcal{L}_P$ is true or false usually depends on how we interpret the atomic formulas which appear in φ.

If $\varphi = \{A_2\}$ and $A_2 =$ "$2 + 2 = 4$", then φ is **True**,
but if $A_2 =$ "The moon is made of cheese", it is **False**.

Not any statement can be assigned true or false value. Consider atomic formula:

$$A_0 = \text{"This statement is false"}$$

Can we assign it the value true or value false?

At this stage logical relationships are important.
Let's define how any assignment of truth values T ("true") and F ("false") to atomic formulas of $\mathcal{L}_P$ can be extended to all other formulas.

We will also get a reasonable definition of what it means for a formula of $\mathcal{L}_P$ to follow logically from other formulas (logical deductions).

Truth Assignment

Definition

A truth assignment is a function $v : \mathcal{L}_P \to \{T; F\}$, such that:

1. $v(A_n)$ is defined for every atomic formula A_n.
2. For any formula α,

$$v(\neg\alpha) = \begin{cases} T, & \text{if } v(\alpha) = F, \\ F, & \text{if } v(\alpha) = T, \end{cases}$$

3. For any formulas α and β,

$$v(\alpha \to \beta) = \begin{cases} F, & \text{if } v(\alpha) = T \text{ and } v(\beta) = F \\ T, & \text{otherwise,} \end{cases}$$

Truth assignment of implication $\to$, means that $T \to F$ is **false**.

Truth Assignment Example

Example

Suppose v is a truth assignment such that $v(A_0) = T$ and $v(A_1) = F$.
Want to know the truth assignment: $v\big((\neg A_1) \to (A_0 \to A_1)\big)$

A_0	A_1	$\neg A_1$	$A_0 \to A_1$	$(\neg A_1) \to (A_0 \to A_1)$
T	F	T	F	F

Have shown that if $v(A_0) = T$ and $v(A_1) = F$, then

$$v\big(((\neg A_1) \to (A_0 \to A_1))\big) = F.$$

What if another truth assignment is given? Say, $v(A_0) = F$ and $v(A_1) = F$. Then:

A_0	A_1	$\neg A_1$	$A_0 \to A_1$	$(\neg A_1) \to (A_0 \to A_1)$
F	F	T	T	T

Construct the **truth table** with all possible truth assignments:

A_0	A_1	, $(\neg A_1)$	$(A_0 \rightarrow A_1)$	$((\neg A_1) \rightarrow (A_0 \rightarrow A_1))$
T	T	F	T	T
T	F	T	F	F
F	T	F	T	T
F	F	T	T	T

Clearly, if there are three atomic formulas present, then will have 8 possible different truth assignments.

How about n atomic formulas? **Answer:** 2^n possible truth assignments.

Truth Table

A_0	A_1	A_2	$\dots$	A_{n-2}	A_{n-1}	A_n	Subformulas
T	T	T	$\cdots$	T	T	T	
T	T	T	$\cdots$	T	T	F	
T	T	T	$\cdots$	T	F	T	
T	T	T	$\cdots$	T	F	F	
T	T	T	$\cdots$	F	T	T	
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	
F	F	F	$\cdots$	F	F	T	
F	F	F	$\cdots$	F	F	F	

Proposition

Suppose u and v are truth assignments such that $u(A_i) = v(A_i)$ for every atomic formula A_i. Then $u = v$, i.e. $u(\varphi) = v(\varphi)$ for every formula φ.

Truth Table

α	$\neg\alpha$
T	F
F	T

α	β	$\alpha \to \beta$
T	T	T
T	F	F
F	T	T
F	F	T

α	β	$\alpha \vee \beta$	$(\neg\alpha) \to \beta$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	F

α	β	$\alpha \wedge \beta$	$\neg(\alpha \to (\neg\beta))$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	F	F

α	β	$\alpha \leftrightarrow \beta$	$(\alpha \to \beta) \wedge (\beta \to \alpha)$
T	T	T	T
T	F	F	F
F	T	F	F
F	F	T	T

Definition

If v is a truth assignment and φ is a formula, we say that truth assignment v **satisfies** φ, if $v(\varphi) = T$. Similarly, if is a set Σ of formulas, we say that v satisfies Σ, if $v(\varphi) = T$ for every $\varphi \in \Sigma$. We say that φ (respectively, Σ) is **satisfiable**, if there is at least one truth assignment, which satisfies it.

Definition

A formula φ is called a **tautology**, if it is satisfied by every truth assignment.

These are tautologies: $\alpha \to \alpha, \quad \alpha \vee \neg\alpha.$

Definition

A formula φ is called a **contradiction**, if there is no truth assignment which satisfies it.

Examples of contradictions: $\alpha \to \neg\alpha, \quad \alpha \wedge \neg\alpha.$

Example

Show that $A_3 \to (A_4 \to A_3)$ is a tautology.

Construct the truth table:

A_3	A_4	$A_4 \to A_3$	$A_3 \to (A_4 \to A_3)$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	T	T

According to the above truth table, the formula is satisfied by any truth assignment, therefore it is a tautology.

Tautology and Contradiction

Proposition

If α is any formula, then $((\neg\alpha) \vee \alpha)$ is a tautology and $((\neg\alpha) \wedge \alpha)$ is a contradiction.

Proof.

Proof follows from the truth tables for each formula:

α	$\neg\alpha$	$(\neg\alpha) \vee \alpha$
T	F	T
F	T	T

α	$\neg\alpha$	$(\neg\alpha) \wedge \alpha$
T	F	F
F	T	F

$\square$

Lecture 3 Summary

- Proving implications $P \Rightarrow Q$:
  - directly;
  - by contrapositive;
  - by contradiction;
  - by cases.
- Proving Iff, $P \Leftrightarrow Q$.
- Do not reason backwards!
- Formalizing propositional logic:
  - Language $\mathcal{L}_P$;
  - Logic formula;
  - Set of sub-formulas;
  - Precedence rules;
- Truth assignment and Truth tables;
- Tautology and Contradiction.

$$\text{study} = \text{not fail}. \tag{1}$$

$$\text{not study} = \text{fail}. \tag{2}$$

Adding equations (1) and (2) gets:

$$\text{study} + \text{not study} = \text{fail} + \text{not fail},$$

and by distribution law:

$$\text{study} \cdot (1 + \text{not}) = \text{fail} \cdot (1 + \text{not}).$$

Thus, by cancellation

$$\text{study} = \text{fail}.$$

Then, why should we study??