

# Problem Solving Methodology: Definitions, Theorems, and Proofs<sup>a</sup>

Teodor Rus

rus@cs.uiowa.edu

The University of Iowa, Department of Computer Science

---

<sup>a</sup>These lecture notes have been developed by Teodor Rus. They are copyrighted materials and may not be used in other course settings outside of the University of Iowa in their current form or modified form without the express written permission of one of the copyright holders. During this course, students are prohibited from selling notes to or being paid for taking notes by any person or commercial firm without the express written permission of one of the copyright holders.

# Observations

1. Theorems are the heart of mathematics;
2. Proof are the soul of mathematics;
3. Definitions are the spirit of mathematics.

**Note:** this three entities are central to every mathematical subject, including the theory of computation.

# Definition (informal)

- A definition describes the objects and the notions used by the mathematical subject;
- A definition may be simple, as in the definition of a set, or it can be complex as in the definition of the security in cryptography;
- Precision is essential to any mathematical definition.

**Note:** a definition must make clear what constitutes the defined object and what does not.

# Formally

A definition is a statement that has two parts:

- The first part identifies a class of objects to which the defined object belongs.

**Example:** when defining prime numbers this class is the set on natural numbers

- The second part identifies a property that distinguish the defined object within the class.

**Example:**  $p \in \mathcal{N}$  is prime iff  $\exists!(k, q \in \mathcal{N} \wedge k, q \neq p, 1 \wedge p = kq)$

**Note:** a formal definition implies that both components are formal.

# Mathematical statements

- Typically a mathematical statement expresses that some object has certain property.
- A mathematical statement may or may not be true. However, like a definition it must be precise.
- There must be **no ambiguity about the meaning of mathematical statement.**

**Note:** to make a mathematical statement precise one needs to formalize both the object and the property stated.

# Formally

Formally, a mathematical statement is an expression of a formal language. First order predicate calculus is usually used in Computation Theory.

# Formal system

A formal system is specified by:

1. An alphabet of symbols;
2. A set of well-formed formulas (wf) (words and sentences that define a formal language);
3. A set of well-formed formulas called axioms;
4. A finite set of “deduction rules” which enable one to deduce a wf  $S$  as a “direct consequence” of a set of wf-s  $S_1, \dots, S_n$ .

# Example formal system

The formal system  $L$  of statement calculus is defined as follows:

1. The alphabet is:  $\neg, \rightarrow, (, ), p_1, p_2, p_3, \dots$
2. Set of wfs defined by:
  - (a)  $p_i$  is a wf for each  $i \geq 1$ ;
  - (b) If  $S_1$  and  $S_2$  are wfs then  $(\neg S_1)$  and  $(S_1 \rightarrow S_2)$  are wfs;
  - (c) The set of all wfs is generated by (a) and (b).
3. The axioms are specified by the following axiom schemes:
  - (L1)  $(S_1 \rightarrow (S_2 \rightarrow S_1))$
  - (L2)  $((S_1 \rightarrow (S_2 \rightarrow S_3)) \rightarrow ((S_1 \rightarrow S_2) \rightarrow (S_1 \rightarrow S_3)))$
  - (L3)  $((\neg S_1) \rightarrow (\neg S_2)) \rightarrow (S_2 \rightarrow S_1)$
4. Deduction rules: For  $S_1$  and  $S_2$  wfs,  $S_2$  is a direct consequence of  $S_1$  and  $(S_1 \rightarrow S_2)$ .

**Note:** This is called Modus Ponens, (MP) and is written  $(S_1, S_1 \rightarrow S_2) \rightarrow S_2$  or  $\frac{S_1, S_1 \rightarrow S_2}{S_2}$ .

# First order language

A first order language is a language  $\mathcal{L}$  whose alphabet contain the symbols:

- Variables  $x_1, x_2, \dots$
- Individual constants (possible none)  $a_1, a_2, \dots$
- Predicate letters (possible non)  $\pi_1^{n_1}, \pi_2^{n_2}, \dots$  of arities  $n_1, n_2, \dots$
- Function letters (possible non)  $f_1^{n_1}, f_2^{n_2}, \dots$  of arities  $n_1, n_2, \dots$
- Punctuation symbols  $(, ), ,$
- Connectives (constructors)  $\neg$  and  $\rightarrow$
- The quantifier  $\forall$ .

# Proofs (informal)

- A *proof* is a convincing logical argument that a statement is true.
- A mathematical proof must be convincing in an absolute sense; this is rather different from the notion of proof in everyday life or in law.
- In everyday life or in law a proof is convincing “beyond any reasonable doubt” and is based on compelling evidence.
- However, evidence play no role in a mathematical proof. A mathematician demands “proof beyond any doubt”.

# Theorems

- A *theorem* is a mathematical statement proved true.
- **Note:** mathematicians reserve the word theorem for statements of special interest.
- *Lemmas:* are mathematical statements proved true, that are interesting only because they assist in the proofs of another, more significant statement.
- *Corollaries:* are true statements that are consequences of theorems or their proofs.

# Finding proofs

The only way to determine the truth or falsity of a mathematical statement is with a mathematical proof!

## Observations

1. Finding proofs is not always simple!
2. Sometimes a proof is simple a set of rules or processes.
3. Other times, it requires inspiration and transpiration.
4. This course requires you to produce proofs!

# Advise

- The author of the textbook advise us:  
**do not despair at the prospect of finding a proof!**
- Even though no one has a recipe for producing proofs, some helpful strategies are available.

# Strategies for finding proofs

- Read carefully the statement you want to prove;
- Be sure that you understand all the notation;
- Rewrite the statement in your own words;
- Break the statement down and consider each part separately; sometimes the parts of a multipart statement are not immediately evident.

# Example multipart statement

*P if and only if Q*, often written *P iff Q*, where both *P* and *Q* are mathematical statements

- The first part is “*P* only if *Q*”, which means:  
*if P is true then Q is true, written  $P \Rightarrow Q$*   
**Proof method:** assume that *P* is true and show that then *Q* is true.
- The second part is “*P* if *Q*”, which means:  
*if Q is true then P is true, written  $P \Leftarrow Q$*   
**Proof method:** assume that *Q* is true and show that then *P* is true.

# Terms used by “iff” proofs

- $P \Rightarrow Q$  is called *forward direction* of the original statement
- $P \Leftarrow Q$  is called *reverse direction* of the original statement
- The original statement can be written  $P \Leftrightarrow Q$

# Proving an *iff* statement

- To prove an iff statement one must prove each of the two implications constituting “iff”.
- Often one of these implications is easier to prove than the other. Always start with the easy one.

# Other multipart statements

Statements stating that two sets  $A$  and  $B$  are equal

- The first part states that “ $A$  is a subset of  $B$ ”
- The second part states that “ $B$  is a subset of  $A$ ”

**Proof:**

1.  $\forall a \in A$  show that  $a \in B$  and
2.  $\forall b \in B$  show that  $b \in A$

# Advise

Try to get an intuitive “gut” feeling of why the statement should be true!

- Experimenting with examples is helpful;
- **Example:**
  - If a statement says that all objects of certain type have a particular property, pick a few objects of that type and observe that they actually do have that property;
  - Then, try to find an object that fails to have the property. This object is called a **counterexample**.

# Using counterexample

- If the statement to prove is true one cannot find counterexamples;
- Seeing where one runs into difficulty when attempting to find counterexamples can help understand why the statement is true.

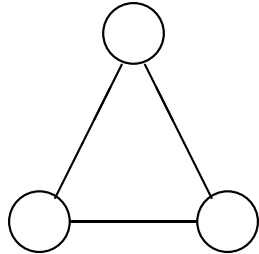
# Example statement and proof

**Statement:** *for every graph  $G$ , the sum of the degrees of all the nodes in  $G$  is an even number.*

# The “gut” feeling

Pick up a few graphs and observe, Figure 1.

$$\text{sum}=2+2+2=6$$



$$\text{sum}=2+3+4+3+2=14$$

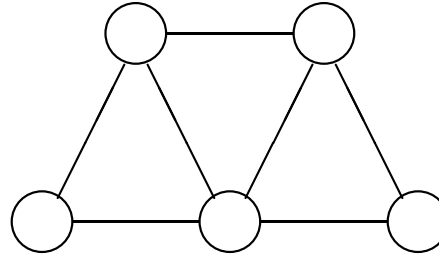


Figure 1: Example graphs and degrees

# Find a counter example

That is, try to find a graph in which the sum of node degrees is an odd number, Figure 2.

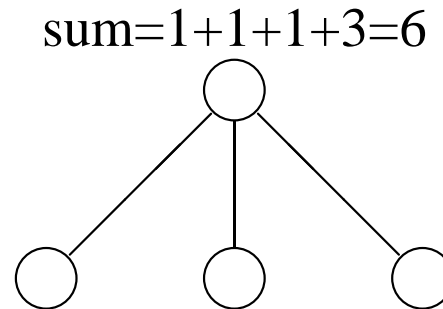


Figure 2: Try a counterexample

# Why is this statement true?

- Every time an edge is added the sum increases by 2;
- The sum of degrees is the sum of edges multiplied by 2.

# Another suggestion

If you are stuck trying to prove a statement, try something easier!

- Attempt to prove a special case of the statement.  
**Example:** if you try to prove that some property is true for every  $k > 0$ , first try to prove it for  $k = 1$ .
- If you succeed with a special case, try one a little more complicated.  
**Example:** if you succeeded with  $k = 1$  try  $k = 2$ .
- Repeat this procedure until you can get the general proof!

# Write proofs properly

When you have found a proof, write it up properly!

- A well-written proof is a sequence of statements, wherein each one follows by simple reasoning from previous statements in the sequence;
- Carefully writing a proof is important, both to enable a reader to understand it and for the prover to be sure that it is free from errors.

# Tips for producing proofs

- **Be patient.**
  - Finding proofs takes time;
  - If you don't see how to do it right away, don't worry;
  - One can work for weeks, or even years, to find a proof!
- **Come back to it.**
  - Look over the statement you want to prove, think about it a bit, leave it, and return a few minutes or hours later;
  - Give the unconscious (intuitive part of your mind) a chance to work.

# More tips

- **Be neat.**
  - Use simple and clear pictures and text to build your intuition;
  - Neatness of your writing will help you (and others) to understand your proof.
- **Be concise.**
  - Brevity helps you express high-level ideas without getting lost in details;
  - Good mathematical notation is useful for expressing ideas concisely;
  - However, do not forget Einstein's suggestion:  
**simple, as simple as possible, but not simpler!**

# Example: DeMorgan's Laws

**Theorem 0.1:** for any two sets  $A$  and  $B$ ,  
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$ .

## Understanding the statement

- Is the meaning of this theorem clear? Do you understand the meaning of  $\cup$ ,  $\cap$ ,  $\overline{A}$ ?
- Here we must show that two sets are equal. Do you remember how this can be done?
- Can you consider a few examples before trying the proof?

# The proof

Prove the assertion  $\overline{A \cup B} = \overline{A} \cap \overline{B}$  by showing

1.  $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ :

Suppose  $x \in \overline{A \cup B}$ . Then, from the definition of the complement of a set it follows that  $x \notin A \cup B$ . Hence,  $x \notin A$  and  $x \notin B$ . Then  $x \in \overline{A}$  and  $x \in \overline{B}$ . That is,  $x \in \overline{A} \cap \overline{B}$

2.  $\overline{A} \cap \overline{B} \subseteq \overline{A \cup B}$ :

Suppose  $x \in \overline{A} \cap \overline{B}$ . By the definition of  $\cap$ ,  $x \in \overline{A}$  and  $x \in \overline{B}$ . Hence,  $x \notin A$  and  $x \notin B$ . That is,  $x \notin A \cup B$ . Hence,  $x \in \overline{A \cup B}$

# Another theorem

**Theorem 0.2:** In a graph  $G = (V, E)$  the sum of the degrees of the nodes in  $V$  is an even number.

## **Proof:**

1. Every edge in  $E$  is connected to two nodes;
2. Each edge contributes 1 to each node to which it is connected;
3. Therefore, each edge contributes 2 to the sum of the degrees of all nodes;
4. Hence, if  $E$  contains  $e$  edges, the sum of the degrees of all nodes of  $G$  is  $2e$ , which is an even number.

# Types of proofs

Several types of arguments arise frequently in mathematical proofs. The few that often occurs in the theory of computation are:

- Proof by construction;
- Proof by contradiction;
- Proof by induction.

# Proof structure

- A proof may contain more than one type of argument;
- This is because the proof may contain within it several different subproofs of several components of the main statement.

# Proof by construction

- Many theorems state that a particular type of object exists.
- One way to prove such a theorem is by demonstrating how to construct that object.

**Note:** this technique is called a **proof by construction**.

# Example proof by construction

**Theorem 0.3** For each even number  $n > 2$  there exists a 3 – *regular* graph with  $n$  nodes.

**Note:** a 3 – *regular* graph is a graph where every node has the degree 3.

# Proof of Theorem 0.3

**Method:** by construction.

**Proof:** Construct  $G = (V, E)$ ,  $V = \{0, 1, 2, \dots, n - 1\}$ , and  $E = \{\{i, i+1\} | 0 \leq i \leq n-2\} \cup \{\{n-1, 0\}\} \cup \{\{i, i+n/2\} | 0 \leq i \leq n/2-1\}$

1. Take a particular value of  $n$  and picture the nodes of this graph written consecutively around the circumference of a circle.
2. The edges described by  $0 \leq i \leq n - 2$  and  $\{n - 1, 0\}$  go between adjacent pairs around the circle.
3. The edges described by  $0 \leq i \leq n/2 - 1$  go between nodes opposite sides of the circle.

**Note:** use a circle to picture this figure and thus increase intuition.

# Proof by contradiction

- Assume that the theorem is false.
- Show that this assumption leads to an obviously false consequence called a contradiction.

**Note:** this kind of reasoning is often used in everyday life.

# Examples from everyday life

- Jacks sees Jill, who just come from outdoors.
- On observing that she is completely dry, he knows that it is not raining.
- His “proof” that it is not raining:
  1. **the assumption:** it is raining;
  2. **the conclusion:** Jill is wet (obviously false);
  3. Therefore it must not be raining.

# A mathematical proof

**Theorem 0.4**  $\sqrt{2}$  is irrational.

**Proof:** by contradiction.

Assume that  $\sqrt{2} = m/n$ , where  $m, n$  are integers, and have no common divisors.

**Note:**  $m, n$  having a common divisor  $k$  means  $m = km_1, n = kn_1$  and we may simplify the fraction  $m/n$  by  $k$  thus getting  $m_1/n_1$  where  $m_1, n_1$  have no common divisors.

# Proof, continuation

1. Multiply both sides of the equality  $\sqrt{2} = m/n$  by  $n$ , obtaining  $n\sqrt{2} = m$ ;
2. Square both sides of the equality, obtaining  $2n^2 = m^2$ ;
3. Because  $m^2$  is  $2n^2$  it result that  $m^2$  is even, hence  $m$  is also even, i.e.,  $m = 2k$ , (square of an odd number is always odd);
4. Replacing  $m$  with  $2k$  in the above equality we get:  $2n^2 = (2k)^2 = 4k^2$ ;
5. Dividing both sides by 2 we obtain  $n^2 = 2k^2$ , i.e.  $n$  is even;
6. We have thus established that both  $m$  and  $n$  are even, i.e., they have a common divisor, what is a contradiction.

# Proof by induction

- This is an advanced proof-method used to show that all elements of a set have a specified property.
- **Examples:**
  1. We may use the proof by induction to show that an arithmetic expression computes a desired quantity for every assignment to its variables, such as  $\sum_{i=1}^{i=n} i = n(n + 1)/2$ .
  2. We may proof by induction that a program works correctly at all steps for all inputs!

# Illustration

Let us take the infinite set to be  $\mathcal{N} = \{1, 2, \dots\}$  and say that we want to show that a property  $\mathbf{P}$  is true for all natural numbers, i.e.,  $\mathbf{P}(k)$  is true for all  $k \in \mathcal{N}$ .

- **Induction basis:** show that  $\mathbf{P}(1)$  is true;
- **Induction step:** show that for each  $i \geq 1$ , if  $\mathbf{P}(i)$  (called *induction hypothesis*) is true then so is  $\mathbf{P}(i + 1)$ .

When both of these parts are proved, it result that  $\mathbf{P}(i)$  is true for every  $i \in \mathcal{N}$ .

# Question

Why can we conclude that  $\mathbf{P}(i)$  is true for all  $i \in \mathcal{N}$ ?

# Formal rationale

The mathematical foundation resides in the structure of  $\mathcal{N}$ , which is an inductive set:

**Definition:**  $A$  is inductive if: (1)  $\emptyset \in A$  and  
(2)  $\forall a \in A \Rightarrow succ(a) = \{a \cup \{a\}\} \in A$

**Construction:**  $\mathcal{N}$  was constructed by the rules:

$$0 = \emptyset$$

$$1 = \{\emptyset\} = \{0\}$$

$$2 = \{\emptyset, \{\emptyset\}\} = \{0, 1\}$$

$$3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\}$$

...

That is,  $\mathcal{N}$  is inductive and  $\forall n \in \mathcal{N}$ ,  $succ(n)$  is actually the  $P(i + 1)$  in the induction principle.

# Intuitive rationale

1.  $P(1)$  is true in virtue of **Induction basis**.
2. If  $P(1)$  is true then  $P(2)$  is true in virtue of **Induction step**.
3. If  $P(2)$  is true then  $P(3)$  is true in virtue of **Induction step**.
4. The process can continue for all natural numbers.

# Variations and generalizations

- The **Induction basis** doesn't necessarily need to start with 1; it may start with any value  $b$ . In this case **Induction step** must show that  $\mathbf{P}(k)$  implies  $\mathbf{P}(k + 1)$ , for  $k \geq b$ .
- Sometimes a stronger induction hypothesis is useful, such as  $\mathbf{P}(j)$  for all  $j \leq i$ .
- One can use instead of  $\mathcal{N}$  a set isomorphic with  $\mathcal{N}$ ; one can also generalize  $\mathcal{N}$  to a transitive set  $A$ .

**Transitive set:**  $A$  is transitive if  $\forall a \in A \wedge \forall x \in a \Rightarrow x \in A$ .

# Application

We will prove by induction the correctness of the formula used to calculate the size of the monthly payments of mortgages.

(See textbook)

# Observations

- For investment reasons people borrow money (called loan) and repay the loan over a certain number of years;
- The terms of such repayments stipulate that a fixed amount of money is payed each month to cover the interest as well as the part of the original sum so that total is re-payd in say 30 years;
- Formula for calculating monthly payments is shrouded in mystery. But it is actually quite simple. We will show by induction that it is correct.

# Notations

- Let  $P$  be the principal, i.e., the amount of the original loan.
- Let  $I$  be the yearly interest rate of the loan. The value  $I = 0.06$  indicates a 6% interest rate.
- Let  $Y$  be the monthly payment.
- Denote by  $M$  the rate at which the loan changes each month because of the interest in it, i.e.,  $M = 1 + I/12$ , is called *monthly multiplier*.

# Things happening each month

1. The amount of loan tends to increase because of the monthly multiplier;
2. The amount of loan tends to decrease because of the monthly payment;
3. Let  $P_t$  be the amount of the loan outstanding after the  $t$ -th month.

# Relationships

1.  $P_0 = P$ , i.e., no loan has been payed;
2.  $P_1 = MP_0 - Y$ , is the amount of loan after one month;
3.  $P_2 = MP_1 - Y$   
 $= M(MP_0 - Y) - Y$   
 $= M^2 P_0 - MY - Y$   
 $= M^2 P_0 - Y(M + 1)$

is the amount of loan after 2 months;

4.  $P_3 = MP_2 - Y$   
 $= M(M^2 P_0 - Y(M + 1)) - Y$   
 $= M^3 P_0 - Y(M^2 + M) - Y$   
 $= M^3 P_0 - Y(M^2 + M + 1)$

is the amount of loan after 3 months;

5.  $P_{k+1} = MP_k - Y = \dots$   
 $= M^{k+1} P_0 - Y(M^k + M^{k-1} + \dots + 1)$

is the amount of loan after  $k + 1$  months.

# Facts

1. The following algebraic identity holds:

$$M^{k+1} - 1 = (M^k + M^{k-1} + \dots + M + 1)(M - 1).$$

(Check it directly by polynomial multiplication)

2. That is, for  $M \neq 1$  we have the identity:

$$M^k + M^{k-1} + \dots + M + 1 = \frac{M^{k+1} - 1}{M - 1}$$

# Putting all together

**Theorem 0.5** For each  $t \geq 0$ ,

$$P_t = PM^t - Y \frac{M^t - 1}{M - 1}$$

**Proof:** By induction

- **Induction basis:** Prove that formula is true for  $t = 0$ .

**Proof:** replacing  $t = 0$  in the formula and observing that  $M^0 = 1$  we obtain  $P_0 = P$

# Proof, continuation

- **Induction step:** For each  $k \geq 0$ , assume that the formula is true for  $t = k$  and show that then it is true for  $t = k + 1$ .

The induction hypothesis states that:

$$P_k = PM^k - Y \frac{M^k - 1}{M-1} \text{ implies } P_{k+1} = PM^{k+1} - Y \frac{M^{k+1} - 1}{M-1}.$$

1. From the definition we have:  $P_{k+1} = P_k M - Y$ ;
2. Using the induction hypothesis to calculate  $P_k$  we get  
$$P_{k+1} = [PM^k - Y \frac{M^k - 1}{M-1}]M - Y$$
;
3. Evaluating the bracket  $[\dots]$  and replacing  $Y$  by  $Y \frac{M-1}{M-1}$  we obtain:

$$P_{k+1} = PM^{k+1} - Y \left( \frac{M^{k+1} - M}{M-1} \right) - Y \left( \frac{M-1}{M-1} \right);$$

4. Factoring  $-Y$  we obtain

$$P_{k+1} = PM^{k+1} - Y \left( \frac{M^{k+1} - M}{M-1} + \frac{M-1}{M-1} \right) = PM^{k+1} - Y \frac{M^{k+1} - 1}{M-1}.$$

Thus, the formula is correct for  $t = k + 1$ , which proves the theorem.