ITB8832 Mathematics for Computer Science

Autumn 2022

Lecture 1 – 29 August 2022

Chapter One

- Propositions and Predicates
- The Axiomatic Method
- Good Proof Guidelines

Last update: 29 August 2022

Contents

Next section

What Is a Proposition?

Definition

A *proposition* is a statement which has a definite *truth value*: either true, or false.

Examples:

- "Tallinn is the capital of Estonia." This is a *true* proposition.
- "Tartu is the capital of Estonia." This is a *false* proposition.
- "For every two real numbers a and b, $|ab| \leq \dfrac{a^2 + b^2}{2}$."
  This is a case of the *arithmetic-geometric inequality*.
- "This statement is true."
  This is a *self-referential* statement, which *might* not have a truth value. This one does: we just don't know which!
- "If two and two are five, then I am the Pope."
  This is actually a *true* proposition! (We will see why in Lecture 2.)

What Is a Proposition?

Definition

A *proposition* is a statement which has a definite *truth value*: either true, or false.

Examples:

- "Tallinn is the capital of Estonia." This is a *true* proposition.
- "Tartu is the capital of Estonia." This is a *false* proposition.
- "For every two real numbers a and b, $|ab| \leq \dfrac{a^2+b^2}{2}$."
  This is a case of the *arithmetic-geometric inequality*.
- "This statement is true."
  This is a *self-referential* statement, which *might* not have a truth value. This one does: we just don't know which!
- "If two and two are five, then I am the Pope."
  This is actually a *true* proposition! (We will see why in Lecture 2.)

What Is a Proposition?

Definition

A *proposition* is a statement which has a definite *truth value*: either true, or false.

Examples:

- "Tallinn is the capital of Estonia." This is a *true* proposition.
- "Tartu is the capital of Estonia." This is a *false* proposition.
- "For every two real numbers a and b, $|ab| \leq \dfrac{a^2 + b^2}{2}$."
  This is a case of the *arithmetic-geometric inequality*.
- "This statement is true."
  This is a *self-referential* statement, which *might* not have a truth value. This one does: we just don't know which!
- "If two and two are five, then I am the Pope."
  This is actually a *true* proposition! (We will see why in Lecture 2.)

What Is a Proposition?

Definition

A *proposition* is a statement which has a definite *truth value*: either true, or false.

Examples:

- "Tallinn is the capital of Estonia." This is a *true* proposition.
- "Tartu is the capital of Estonia." This is a *false* proposition.
- "For every two real numbers a and b, $|ab| \leq \frac{a^2 + b^2}{2}$."
  This is a case of the *arithmetic-geometric inequality*.
- "This statement is true."
  This is a *self-referential* statement, which *might* not have a truth value. This one does: we just don't know which!
- "If two and two are five, then I am the Pope."
  This is actually a *true* proposition! (We will see why in Lecture 2.)

What Is a Proposition?

Definition

A *proposition* is a statement which has a definite *truth value*: either true, or false.

Examples:

- "Tallinn is the capital of Estonia." This is a *true* proposition.
- "Tartu is the capital of Estonia." This is a *false* proposition.
- "For every two real numbers a and b, $|ab| \leq \dfrac{a^2 + b^2}{2}$."
  This is a case of the *arithmetic-geometric inequality*.
- "This statement is true."
  This is a *self-referential* statement, which *might* not have a truth value. This one does: we just don't know which!
- "If two and two are five, then I am the Pope."
  This is actually a *true* proposition! (We will see why in Lecture 2.)

What Is Not a Proposition?

Non-examples:

- "Study the textbook from page 1 to page 30."
  This is a request, not a statement.
- "Is it raining now?"
  This is a question, not a statement.
- "It is raining now."
  This statement may be true or false according to what time and date it is, so it does not have a *definite* truth value.
- "This statement is false."
  Such statement *cannot* have a truth value: if it were true, then it would be false, and if it were false, then it would be true.
- "If this statement is true, then two and two are five."
  This is an instance of *Curry's paradox*.

What Is Not a Proposition?

Non-examples:

- "Study the textbook from page 1 to page 30."
  This is a request, not a statement.
- "Is it raining now?"
  This is a question, not a statement.
- "It is raining now."
  This statement may be true or false according to what time and date it is, so it does not have a *definite* truth value.
- "This statement is false."
  Such statement *cannot* have a truth value: if it were true, then it would be false, and if it were false, then it would be true.
- "If this statement is true, then two and two are five."
  This is an instance of *Curry's paradox*.

What Is Not a Proposition?

Non-examples:

- "Study the textbook from page 1 to page 30."
  This is a request, not a statement.
- "Is it raining now?"
  This is a question, not a statement.
- "It is raining now."
  This statement may be true or false according to what time and date it is, so it does not have a *definite* truth value.
- "This statement is false."
  Such statement *cannot* have a truth value: if it were true, then it would be false, and if it were false, then it would be true.
- "If this statement is true, then two and two are five."
  This is an instance of *Curry's paradox*.

What Is Not a Proposition?

Non-examples:

- "Study the textbook from page 1 to page 30."
  This is a request, not a statement.
- "Is it raining now?"
  This is a question, not a statement.
- "It is raining now."
  This statement may be true or false according to what time and date it is, so it does not have a *definite* truth value.
- "This statement is false."
  Such statement *cannot* have a truth value: if it were true, then it would be false, and if it were false, then it would be true.
- "If this statement is true, then two and two are five."
  This is an instance of *Curry's paradox*.

What Is Not a Proposition?

Non-examples:

- "Study the textbook from page 1 to page 30."
  This is a request, not a statement.
- "Is it raining now?"
  This is a question, not a statement.
- "It is raining now."
  This statement may be true or false according to what time and date it is, so it does not have a *definite* truth value.
- "This statement is false."
  Such statement *cannot* have a truth value: if it were true, then it would be false, and if it were false, then it would be true.
- "If this statement is true, then two and two are five."
  This is an instance of *Curry's paradox*.

Predicates

Definition

A *predicate* is a proposition whose truth value may depend on one or more variables.

Examples:

- "n is a perfect square" where n is a positive integer.
  This is true if $n = 1$, but false if $n = 2$.
- "$n^2 + n + 41$ is a prime number" where n is a positive integer.
  This is true for $n = 1, 2, \ldots, 39$, but $40^2 + 40 + 41 = 41^2$.
- "It is raining now."
  This is also a predicate, whose truth value depends on the variable "now".

Predicates

Definition

A *predicate* is a proposition whose truth value may depend on one or more variables.

Examples:

- "n is a perfect square" where n is a positive integer.
  This is true if $n = 1$, but false if $n = 2$.
- "$n^2 + n + 41$ is a prime number" where n is a positive integer.
  This is true for $n = 1, 2, \ldots, 39$, but $40^2 + 40 + 41 = 41^2$.
- "It is raining now."
  This is also a predicate, whose truth value depends on the variable "now".

Predicates

Definition

A *predicate* is a proposition whose truth value may depend on one or more variables.

Examples:

- "n is a perfect square" where n is a positive integer.
  This is true if $n = 1$, but false if $n = 2$.
- "$n^2 + n + 41$ is a prime number" where n is a positive integer.
  This is true for $n = 1, 2, \ldots, 39$, but $40^2 + 40 + 41 = 41^2$.
- "It is raining now."
  This is also a predicate, whose truth value depends on the variable "now".

Predicates

Definition

A *predicate* is a proposition whose truth value may depend on one or more variables.

Examples:

- "n is a perfect square" where n is a positive integer.
  This is true if $n = 1$, but false if $n = 2$.
- "$n^2 + n + 41$ is a prime number" where n is a positive integer.
  This is true for $n = 1, 2, \ldots, 39$, but $40^2 + 40 + 41 = 41^2$.
- "It is raining now."
  This is also a predicate, whose truth value depends on the variable "now".

Next section

Euclidean geometry

The Greek mathematician Euclid (IV–III century BC) based his treatise on plane geometry on the following five *axioms*:
(here we give an equivalent, more modern formulation)

1. Through any two points there is a unique straight line.
2. Every segment can be extended to a straight line.
3. There is always a circle with given center and radius.
4. All right angles are equal to each other.
5. Given a straight line and a point not on it, there exists a unique line parallel to the first and passing through the point.

All other propositions are *deduced* from those five axioms by means of *proofs*.

So, What Is a Proof?

Definition (following the textbook)

A *proof* of a proposition is a sequence of *logical deductions* which, starting from taken-for-granted *axioms* and reusing *previously proved statements*, ends with the proposition itself.

There is a sort of informal nomenclature for propositions which have a proof:

- *Theorem:* a proposition which is "important" somehow.
  Example: Pythagoras' theorem on the side of a right triangle.
- *Lemma:* a proposition which is "useful" somehow.
  Example: Euclid's lemma on divisibility by a prime.
- *Corollary:* a proposition which follows "in few steps" from a theorem or lemma.

The axiomatic method

1. Start from the axioms.
2. Apply logical deduction.
3. End with the proposition you wanted to prove.

Next subsection

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

meaning:

If all the premises are true,
then the conclusion is true.

- A premise can also be called an *antecedent* or a *hypothesis*.
- The conclusion can also be called the *consequent* or the *thesis*.

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Modus ponens[1]

$$\frac{P\,, \quad P \text{ implies } Q}{Q}$$

Example:

$$\frac{\textit{it is raining}\,, \quad \textit{if it is raining, then I take my umbrella}}{\textit{I take my umbrella}}$$

[1] meaning "way of adding"; pronounced: MAW-doos PAWN-ens

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Contraction of implications

$$\frac{P \text{ implies } Q\,, \quad Q \text{ implies } R}{P \text{ implies } R}$$

Example:

$$\frac{\textit{if Bob is a man, then Bob is an animal}\,, \quad \textit{if Bob is an animal, then Bob is mortal}}{\textit{if Bob is a man, then Bob is mortal}}$$

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Contraposition

$$\frac{P \text{ implies } Q}{\text{not}(Q) \text{ implies not}(P)}$$

Example:

$$\frac{\textit{if it is raining, then I take my umbrella}}{\textit{if I do not take my umbrella, then it is not raining}}$$

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Conjunction

$$\frac{P\,, \quad Q}{P \text{ and } Q}$$

Example:

$$\frac{\textit{the sky is blue}\,, \quad \textit{the rose is red}}{\textit{the sky is blue and the rose is red}}$$

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Disjunction

$$\frac{P}{P \text{ or } Q}, \quad \frac{Q}{P \text{ or } Q}$$

Example:

$$\frac{\textit{the sky is blue}}{\textit{the sky is blue or the rose is green}}$$

Inference rules

These have the form:

$$\frac{\textit{list of premises}}{\textit{conclusion}}$$

Law of Non-Contradiction

$$\frac{}{\text{not}(P \text{ and not}(P))}$$

Example:

$$\frac{}{\textit{it's not the case that it both rains and doesn't rain}}$$

A non-rule

$$\frac{P \text{ implies } Q}{\text{not}(P) \text{ implies } \text{not}(Q)}$$

It *might* be that both “if P, then Q” and “if not-P, then not-Q”.

- But more often than not, this is not the case:
- If I am under the rain, then I get wet; but I can get wet without being under the rain, e.g., by swimming in the lake.
- And we have stated that a logical rule is valid when the conclusion is true *whenever* the premises are all true.

Using this “rule” is a logical fallacy, called *denying the antecedent*.

A non-rule

$$\frac{P \text{ implies } Q}{\text{not}(P) \text{ implies not}(Q)}$$

It *might* be that both "if P, then Q" and "if not-P, then not-Q".

- But more often than not, this is not the case:
- If I am under the rain, then I get wet; but I can get wet without being under the rain, e.g., by swimming in the lake.
- And we have stated that a logical rule is valid when the conclusion is true *whenever* the premises are all true.

Using this "rule" is a logical fallacy, called *denying the antecedent*.

A non-rule

$$\frac{P \text{ implies } Q}{\text{not}(P) \text{ implies not}(Q)}$$

It *might* be that both "if P, then Q" and "if not-P, then not-Q".

- But more often than not, this is not the case:
- If I am under the rain, then I get wet; but I can get wet without being under the rain, e.g., by swimming in the lake.
- And we have stated that a logical rule is valid when the conclusion is true *whenever* the premises are all true.

Using this "rule" is a logical fallacy, called *denying the antecedent*.

Next subsection

How to Prove an Implication

Problem

Provide a proof of "P implies Q".

Method 1: Direct proof

1. Assume P.
2. Show that Q logically follows.

Method 2: Prove the contrapositive

1. State, "We prove the contrapositive".
2. Write down the contrapositive.
3. Write a direct proof of the contrapositive.

Method 1: Example

Claim

If $0 \leq x \leq 2$, then $1 + 4x - x^3 \geq 0$.

- We assume $0 \leq x \leq 2$.
- We isolate the part $4x - x^3$, which contains the variable.
- We observe that we can factorize this as follows:

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

- For x between 0 and 2, each of those factors is nonnegative.
- Then the product is nonnegative too, and we get:

$$1 + 4x - x^3 > 4x - x^3 \geq 0.$$

Method 1: Example

Claim

If $0 \leq x \leq 2$, then $1 + 4x - x^3 \geq 0$.

- We assume $0 \leq x \leq 2$.
- We isolate the part $4x - x^3$, which contains the variable.
- We observe that we can factorize this as follows:

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

- For x between 0 and 2, each of those factors is nonnegative.
- Then the product is nonnegative too, and we get:

$$1 + 4x - x^3 > 4x - x^3 \geq 0.$$

Method 1: Example

Claim

If $0 \le x \le 2$, then $1 + 4x - x^3 \ge 0$.

- We assume $0 \le x \le 2$.
- We isolate the part $4x - x^3$, which contains the variable.
- We observe that we can factorize this as follows:

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

- For x between 0 and 2, each of those factors is nonnegative.
- Then the product is nonnegative too, and we get:

$$1 + 4x - x^3 > 4x - x^3 \ge 0.$$

Method 1: Example

Claim

If $0 \leq x \leq 2$, then $1 + 4x - x^3 \geq 0$.

- We assume $0 \leq x \leq 2$.
- We isolate the part $4x - x^3$, which contains the variable.
- We observe that we can factorize this as follows:

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

- For x between 0 and 2, each of those factors is nonnegative.
- Then the product is nonnegative too, and we get:

$$1 + 4x - x^3 > 4x - x^3 \geq 0.$$

Method 2: Example

Claim

If $r \geq 0$ is irrational, then $\sqrt{r}$ is irrational.

- We prove the contrapositive:
  If $\sqrt{r}$ is rational, then r is rational.
- Assume there exist integers m, n such that $\sqrt{r} = \dfrac{m}{n}$.
- By squaring both sides, as $r \geq 0$, we get $r = \dfrac{m^2}{n^2}$
- As m^2 and n^2 are also integers, r is rational.

Method 2: Example

Claim

If $r \geq 0$ is irrational, then $\sqrt{r}$ is irrational.

- We prove the contrapositive:
  If $\sqrt{r}$ is rational, then r is rational.
- Assume there exist integers m, n such that $\sqrt{r} = \frac{m}{n}$.
- By squaring both sides, as $r \geq 0$, we get $r = \frac{m^2}{n^2}$
- As m^2 and n^2 are also integers, r is rational.

Method 2: Example

Claim

If $r \geq 0$ is irrational, then $\sqrt{r}$ is irrational.

- We prove the contrapositive:
  If $\sqrt{r}$ is rational, then r is rational.
- Assume there exist integers m, n such that $\sqrt{r} = \dfrac{m}{n}$.
- By squaring both sides, as $r \geq 0$, we get $r = \dfrac{m^2}{n^2}$
- As m^2 and n^2 are also integers, r is rational.

Method 2: Example

Claim

If $r \geq 0$ is irrational, then $\sqrt{r}$ is irrational.

- We prove the contrapositive:
  If $\sqrt{r}$ is rational, then r is rational.
- Assume there exist integers m, n such that $\sqrt{r} = \dfrac{m}{n}$.
- By squaring both sides, as $r \geq 0$, we get $r = \dfrac{m^2}{n^2}$
- As m^2 and n^2 are also integers, r is rational.

The Law of Excluded Middle

The technique of proof by contraposition works because of:

Law of Excluded Middle

Given any proposition P, one between P and not(P) is true.

Expressed as a logical rule: (" iff " is a shortcut for 'if and only if")

$$\frac{}{P \text{ or } \mathrm{not}(P)}, \quad \text{or equivalently}, \quad \frac{}{P \text{ iff } \mathrm{not}(\mathrm{not}(P))}$$

- Technically, if we iterate the rule of contraposition, we get:

$$\frac{\mathrm{not}(Q) \text{ implies } \mathrm{not}(P)}{\mathrm{not}(\mathrm{not}(P)) \text{ implies } \mathrm{not}(\mathrm{not}(Q))}$$

- We then need the Law of Excluded Middle to substitute not(not(P)) and not(not(Q)) with P and Q, respectively.
- There are some logics in which the Law of Excluded Middle is not valid.

Next subsection

How to Prove an "If and Only If"

Problem

Provide a proof of "P iff Q".

Method 1: Prove each implication separately

1. First, prove P implies Q.
2. Then, prove Q implies P.

Method 2: Construct a chain of iff 's

1. Write down a sequence $P_1, \ldots, P_n$ of propositions such that $P_1 = P$ and $P_n = Q$.
2. For every i from 1 to $n-1$, prove: P_i iff P_{i+1}.

Example: The standard deviation

Recall that the *mean* of the values $x_1, x_2, \ldots, x_n$ is the quantity:

$$\mu = \frac{x_1 + x_2 + \ldots + x_n}{n}$$

Theorem

However given values x_1, ..., x_n, their *standard deviation*

$$\sigma = \sqrt{\frac{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \ldots + (x_n - \mu)^2}{n}}$$

is zero if and only if all the x_i's are equal.

Example: The standard deviation

Theorem

However given values $x_1, \ldots, x_n$, their *standard deviation*

$$\sigma = \sqrt{\frac{(x_1-\mu)^2+(x_2-\mu)^2+\ldots+(x_n-\mu)^2}{n}}$$

is zero if and only if all the x_i's are equal.

We construct the following chain of propositions:

1. $\sigma = 0$.
2. $(x_1-\mu)^2+(x_2-\mu)^2+\ldots+(x_n-\mu)^2 = 0$.
3. $x_1-\mu = x_2-\mu = \ldots = x_n-\mu = 0$.
4. $x_1 = x_2 = \ldots = x_n = \mu$.

Example: The standard deviation

Theorem

However given values $x_1, \ldots, x_n$, their *standard deviation*

$$\sigma = \sqrt{\frac{(x_1 - \mu)^2 + (x_2 - \mu)^2 + \ldots + (x_n - \mu)^2}{n}}$$

is zero if and only if all the x_i's are equal.

Then:

- P_1 iff P_2, because a square root is 0 iff its argument is 0.
- P_2 iff P_3, because a sum of squares is 0 iff each square is 0.
- P_3 iff P_4 in an *obvious*[1] way.

[1] Use this word ***VERY*** carefully!

Next subsection

Proof by Cases

Suppose we have a predicate $P(x)$ depending on a variable x.

1. Identify a *finite* number of cases such that, for *each* value k of the variable x, the proposition $P(\mathrm{k})$ belongs to *some* case (maybe more than one, but at least one).
2. Construct a proof for each of those cases.

This works because, if $C_1, C_2, \ldots, C_n$ are all the possible cases, then $P(x)$ is equivalent to:

$$(C_1 \text{ and } P(x)) \text{ or } (C_2 \text{ and } P(x)) \text{ or } \ldots \text{ or } (C_n \text{ and } P(x))$$

Example: Ramsey's Theorem for (3,3)

Statement

Among any six people there is

1. either a *club* of three people who all know each other,
2. or a group of three *strangers* none of whom knows any of the others.

Example: Ramsey's Theorem for (3,3)

Statement

Among any six people there is

1. either a *club* of three people who all know each other,
2. or a group of three *strangers* none of whom knows any of the others.

Part 1: Identify the Cases

Call A, B, C, D, E, F the six people. Exactly one of the following happens:

a. At least three between B, C, D, E, and F know A.

b. At most two between B, C, D, E, and F know A.

Example: Ramsey's Theorem for (3,3)

Statement

Among any six people there is

1. either a *club* of three people who all know each other,
2. or a group of three *strangers* none of whom knows any of the others.

Part 2a: Prove the First Case

Call R, S, and T three people who *know* A.

- If *none of R, S, and T* know each other, then *they* form a group of strangers.
- If *two of them know each other*, call them U and V: then *A, U, and V* form a club.

Note that we used a proof by cases inside a proof by cases.

Example: Ramsey's Theorem for (3,3)

Statement

Among any six people there is

1. either a *club* of three people who all know each other,
2. or a group of three *strangers* none of whom knows any of the others.

Part 2b: Prove the Next Case

Call R, S, and T three people who *don't know* A.

- If *R, S, and T know each other*, then *they* form a club.
- If *two of them don't know each other*, call them U and V: then *A, U, and V* form a group of three strangers.

Again, we used a proof by cases inside a proof by cases.

Example: Ramsey's Theorem for (3,3)

Statement

Among any six people there is

1. either a *club* of three people who all know each other,
2. or a group of three *strangers* none of whom knows any of the others.

Note that the options in the thesis are not mutually exclusive:

- It might be that A, B, and C form a club, while D, E, and F form a group of three strangers.

Next section

Good proof guidelines

- State your plan.
- Keep a linear flow.
- A proof is an essay, rather than a calculation.
- Use notation consistently and sparingly.
- Structure a long proof as you would do with a long program.
- Make multiple revisions.
- "Obvious" is a relative concept.
- Write down conclusions explicitly.