

Theorems and Proofs

Discrete Mathematics
Evgeny Skvortsov

Previous Lecture

- Equivalent open statements
- Equivalent quantified statements
- Quantifiers and conjunction/disjunction
- Quantifiers and logic connectives
- Equivalence and multiple quantifiers
- Theorems

Proving Theorems

- We know rules of inference to reason about propositional statements. What about predicates and quantified statements?
- The simplest method is the method of exhaustion:
 - To prove that $\forall x P(x)$, just verify that $P(a)$ is true for all values a from the universe.
 - To prove that $\exists x P(x)$, by checking all the values in the universe find a value a such that $P(a)$ is true

“Every car in lot C is red”

“There is a blue car in lot C”

Rule of Universal Specification

- Reconsider the argument

Every man is mortal.
Socrates is a man.

\therefore Socrates is mortal

- In symbolic form it looks like

$$\forall x (P(x) \rightarrow Q(x))$$
$$P(\text{Socrates})$$

$$\therefore Q(\text{Socrates})$$

where

$P(x)$ stands for x is a man, and

$Q(x)$ stands for x is mortal

Rule of Universal Specification (cntd)

- If an open statement becomes true for all values of the universe, then it is true for each specific individual value from that universe

$$\frac{\forall x P(x)}{\therefore P(c)}$$

- Example

Premises: $\forall x (P(x) \rightarrow Q(x)), \quad P(\text{Socrates})$

Step	Reason
1. $\forall x (P(x) \rightarrow Q(x)),$	premise
2. $P(\text{Socrates}) \rightarrow Q(\text{Socrates}),$	rule of universal specification
3. $P(\text{Socrates})$	premise
4. $Q(\text{Socrates}),$	modus ponens

Rule of Universal Generalization

- Let us prove a theorem:

If $2x - 6 = 0$ then $x = 3$.

- Proof

Take any number c such that $2c - 6 = 0$. Then $2c = 6$, and, finally $c = 3$. As c is an arbitrary number this proves the theorem.
Q.E.D

- Look at the first and the last steps.

- In the first step instead of the variable we start to consider its **generic value**, that is a value that does not have any specific property that may not have any other value in the universe
- In the last step having proved the statement for the generic value we conclude that the universal statement is also true

Rule of Universal Generalization (cntd)

- If an open statement $P(x)$ is proved to be true when x is assigned by any arbitrary chosen (generic) value from the universe, then the statement $\forall x P(x)$ is also true.
- Example: “If $2x - 6 = 0$ then $x = 3$.”
- Notation: $P(x)$ - “ $2x - 6 = 0$ ”, $Q(x)$ - “ $2x = 6$ ”, $R(x)$ - “ $x = 3$ ”
- Premises: $\forall x (P(x) \rightarrow Q(x))$, $\forall x (Q(x) \rightarrow R(x))$
- Conclusion: $\forall x (P(x) \rightarrow R(x))$,

Step	Reason
1. $\forall x (P(x) \rightarrow Q(x))$, $\forall x (Q(x) \rightarrow R(x))$	premises
2. $P(c) \rightarrow Q(c)$, $Q(c) \rightarrow R(c)$,	rule of univ. specification
3. $P(c) \rightarrow R(c)$	rule of syllogism
4. $\forall x (P(x) \rightarrow R(x))$	rule of univ. generalization

Existential Rules

- Rule of Existential Specification.

If $\exists x P(x)$ is true in a given universe, then there is value a in this universe with $P(a)$ true.

- Rule of Existential Generalization.

If $P(a)$ is true for some value a in a given universe, then $\exists x P(x)$ is true in this universe.

Methods of Proving – Direct Proofs

- Direct proofs are used when we need to proof statements like

$$\forall x (P(x) \rightarrow Q(x))$$

- Main steps

Our goal is to prove that $P(a) \rightarrow Q(a)$ is a tautology for a generic value a .

1. Assume that $P(a)$ is true
2. Using axioms, previous theorems etc. prove that $Q(a)$ is true
3. Conclude that $P(a) \rightarrow Q(a)$ is a tautology
4. Use the rule of universal generalization to infer

$$\forall x (P(x) \rightarrow Q(x))$$

Example

● Definition: n is **even** if and only if there is k such that $n = 2k$

● Prove that if n is even then n^2 is also even.

● Proof:

Since n is even, there is k such that $n = 2k$.

Therefore

$$n^2 = (2k)^2 = 4k^2$$

Finally

$$n^2 = 2(2k^2)$$

and n^2 is even

$E(n)$ – n is even

Theorem: $\forall x (E(x) \rightarrow E(x^2))$

1. $E(n)$ assume the premise
2. $\forall x (E(x) \leftrightarrow \exists y (x = 2y))$ definition
3. $E(n) \leftrightarrow \exists y (n = 2y)$ rule of un. spec.
4. $\exists y (n = 2y)$ modus ponens
5. $n = 2k$ rule of exist. spec.
6. $n^2 = 2(2k^2)$ arithmetic
7. $\exists y (n^2 = 2y)$ rule of exist. general.
8. $E(n^2)$ modus ponens

Methods of Proving – Proof by Contraposition

- Sometimes direct proofs do not work

- Prove that if $3n + 2$ is even, then n is also even

That is $\forall x (E(3x + 2) \rightarrow E(x))$

- Let us try the direct approach:

As for the generic value n the number $3n + 2$ is even, for some k we have $3n + 2 = 2k$. Therefore $3n = 2(k - 1)$.

Now what?

- What if instead of $\forall x (E(3x + 2) \rightarrow E(x))$ we prove the contrapositive, $\forall x (\neg E(x) \rightarrow \neg E(3x + 2))$?

Methods of Proving – Proof by Contraposition (cntd)

- So assume that n is **odd**, that is there is k such that $n = 2k + 1$.
- Then $3n + 2 = 3 \cdot (2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1$.
That is $3n + 2$ is odd.
- We have proved that $\neg E(3n + 2)$ is true, and therefore the contraposition $\forall x (\neg E(x) \rightarrow \neg E(3x + 2))$ is true.
Finally, we conclude that the theorem $\forall x (E(3x + 2) \rightarrow E(x))$ is also true.

Methods of Proving – Proof by Contraposition (cntd)

● Main steps

Our goal is to prove that $P(a) \rightarrow Q(a)$ is a tautology for a generic value a .

Instead we prove the contrapositive $\neg Q(a) \rightarrow \neg P(a)$

1. Assume that $\neg Q(a)$ is true
2. Using axioms, previous theorems etc. prove that $\neg P(a)$ is true
3. Conclude that $\neg Q(a) \rightarrow \neg P(a)$ is a tautology
4. Conclude that $P(a) \rightarrow Q(a)$ is a tautology
5. Use the rule of universal generalization to infer

$$\forall x (P(x) \rightarrow Q(x))$$

Methods of Proving – Proof by Contradiction

- Proofs by contradiction use the Rule of Contradiction

$$\frac{\neg p \rightarrow F}{\therefore p}$$

- Can be used to prove statements of any form
- Main steps
 1. Assume $\neg p$.
 2. Using axioms, previous theorems etc. infer a contradiction
 3. Conclude p .
- Usually the contradiction has the form $\exists x (P(x) \wedge \neg P(x))$

Example

● Definition: a real number is said to be rational if it can be represented as a fraction $\frac{a}{b}$ where a, b are integers

● Prove that $\sqrt{2}$ is irrational

● Proof

Suppose that $\sqrt{2}$ is rational, that is there are integers a, b such that $\sqrt{2} = \frac{a}{b}$.

We may assume that a, b have no common factor.

Squaring we obtain $a^2 = 2b^2$.

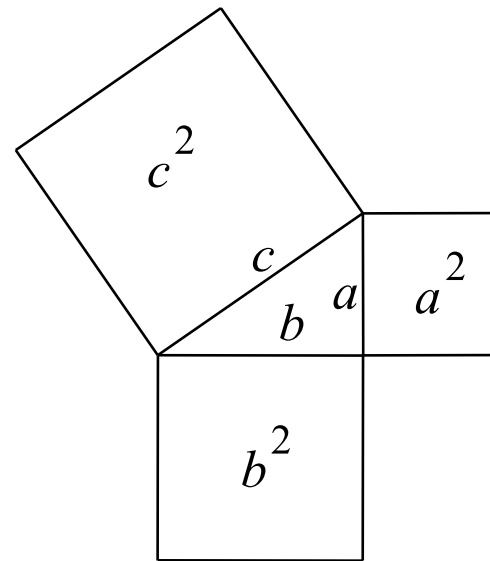
Since a^2 is even, a is also even, hence $a = 2c$ for some c .

Therefore $2b^2 = 4c^2$, and so $b^2 = 2c^2$.

Hence b is even.

We get that a and b have a common factor – 2. A contradiction.

Pythagoras

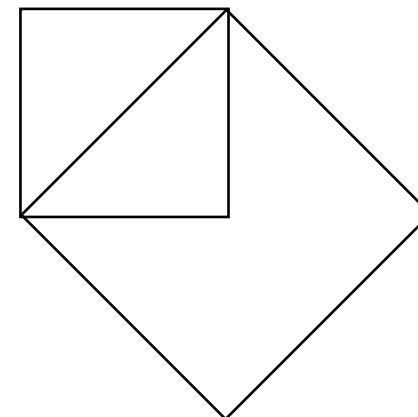


$$c^2 = a^2 + b^2$$

“Number is the ruler of forms and ideas, and the cause of gods and demons”

numbers = rational numbers

$\sqrt{2}$ does not belong to this world



Proving Existential Statements

- How to prove $\exists x P(x)$.
- Constructive proofs: find or construct a value a such that $P(a)$ is true.
Prove that there is a grey car...
My car is grey!
- Pure proofs of existence:
Assume that $\forall x \neg P(x)$.
Using axioms, previous theorems etc. infer a contradiction
Thus, this is a proof by contradiction.

Homework

Exercises from the Book:

No. 5, 9, 11, 13, 15, 17 (page 116-117)