Formale Methoden der Informatik

Tutorial: Proof Techniques

Uwe Egly

Knowledge-Based Systems Group
Institute of Information Systems
Vienna University of Technology

Observation

- Many students have problems to prove simple statements
- Possible reasons:
  - Skill was present but has been forgotten during the years
  - Skill has never been achieved (for various reasons)
  - ➥ Goal: Learn it (again)
    - G1 We convey the idea of what is “an acceptable proof”
    - G2 We try to improve your ability to perform proofs

Disclaimer

This is not a full-fledged review course (“repetitorium”) in math! We concentrate on proof strategies and especially on practical aspects like how to get the structure of proofs right.

Resources

The slides are based on the following book:

A. Wohlgemuth:
Introduction to Proof in Abstract Mathematics. Dover 2011.

I detected too late the text

Deductive Mathematics—an introduction to proof and discovery for mathematics education

of the same author. It can be downloaded at

http://andrew-wohlgemuth.com/DMmathed.pdf

Two other books are:

R. Hammack. Book of Proof. It can be downloaded [here]

D. J. Velleman. How to prove it. Cambridge University Press 2006

Outline

What is a Proof?

Simple Proof Techniques

Proof Techniques

- Proving and Using Forall Statements
- Proving and Using Or Statements
- Proving and Using And Statements
- Using Theorems
- Proving and Using Implications
- Handling iff Statements
- Proofs by Contradiction
- Handling Existential Statements

Learning Objectives

Formal vs informal proofs

Formal proofs

Formal proofs [link to Formal Proof, link to Proof Theory]

- Often developed in an interactive theorem prover (like HOL or Isabelle)
- Presented in a calculus like higher-order type theory
- Such proofs can be checked by a machine

More info in the special issue on formal proofs of:
Notices of the American Mathematical Society 55(11), 2008 [link]

Formal vs informal proofs

Formal proofs

- One possibility for a calculus: Natural deduction (ND)

  > *First I wished to construct a formalism that comes as close as possible to actual reasoning. Thus arose a "calculus of natural deduction".*
  >
  > *Gerhard Gentzen (1934)*

- We will use inferences of ND (or combinations thereof) later

Formal vs informal proofs

Informal proofs

Informal proofs

- They have to contain enough detail to be reproducible
- They can be translated into a formal proof by introducing the rules (of the underlying calculus) after an addition of missing "obvious" details
- The level of details in a proof depends on the audience!
- Warning: "An informal proof in the mathematics literature, by contrast, requires weeks of peer review to be checked, and may still contain errors."
  [Link to widely believed results which were later wrong]

Statements

- Statement: a mathematical expression which is either true or false
- Examples: $2 \in \{x \in \mathbb{R} \mid x < 5\}$ (true) or $3^2 + 5^2 = 8^2$ (false)
- Expressions of the form $0 < x < 1$ are used to define a set

$$A = \{x \in \mathbb{R} \mid 0 < x < 1\}$$

- Important: The truth value of the open expression $0 < x < 1$ depends on the chosen x, e.g., true for $x = \frac{1}{2}$ and false for $x = 5$
- Important: The domain
  For $\mathbb{N}$, $0 < x < 1$ is unsatisfiable, for $\mathbb{R}$, it is satisfiable

Formal mathematical proofs

- A formal mathematical proof consists of a numbered sequence of true statements
- Each statement in a proof is an assumption or . . .
- . . . it follows from previous statements by a rule of inference
- The last statement is the one we have proved
- ➥ Open expressions cannot occur in proofs

Example of an inference rule: The set definition rule

If an element is in a set, we may infer that it satisfies the defining property. Conversely, if it satisfies the defining property, then we may infer that it is in the set.

The set definition rule: An example

Define $C = \{x \in \mathbb{R} \mid x < 2\}$ ($x < 2 \land x \in \mathbb{R}$ is the defining property)

Two possibilities for a derivation:

Possibility 1

1. $a \in C$
2. $a < 2 \land a \in \mathbb{R}$ (1; def C)

Possibility 2

1. $b < 2 \land b \in \mathbb{R}$
2. $b \in C$ (1; def C)

- Each statement in a proof has a number
- We justify how we derive a statement, e.g., (1; def C) means we derive the current statement from statement 1 with the definition of C and the definition rule

Remark: $\land\, b \in \mathbb{R}$ is often omitted when it is clear from the context

Macro-steps in proofs

Problem: Consider the following proof attempt:
(ass means assumption and prop means property)

	Assume:	1.	$X = \{x \in \mathbb{R} \mid x < 1\}$
		2.	$a \in X$
	Show:		$a < 2$
1.	$a \in X$		(ass 2)
2.	$a < 1$		(1, ass 1; def X)
3.	$1 < 2$		(prop $\mathbb{R}$)
4.	$a < 2$		$(2, 3$; prop $\mathbb{R}$)

Is this an acceptable proof?

- Acceptance of macro-steps like “prop $\mathbb{R}$” depends on the audience!
  Which properties of $\mathbb{R}$ have been employed?

Outline

What is a Proof?

Simple Proof Techniques

Proof Techniques

- Proving and Using Forall Statements
- Proving and Using Or Statements
- Proving and Using And Statements
- Using Theorems
- Proving and Using Implications
- Handling iff Statements
- Proofs by Contradiction
- Handling Existential Statements

Learning Objectives

Simple proof techniques

Proof by example

Example

Prove that there is a prime number between 80 and 90.

Idea

Just give a witness for the prime number (say p) in the statement (i.e., present p for which the statement holds)

Proof: Choose $p = 83$.

Is this sufficient?

Simple proof techniques

Proof by example

Example

Prove that there is a prime number between 80 and 90.

Idea

Just give a witness for the prime number (say p) in the statement (i.e., present p for which the statement holds)

Proof: Choose $p = 83$.

Is this sufficient?

Strictly speaking, NO. We have to show that 83 is indeed prime.

This can be done by checking all possible divisors exhaustively.

Simple proof techniques

Proof by exhaustive enumeration

Example

Prove that $p = 83$ is a prime number.

Idea

Check all possible divisors q of p.

If we are informed then we know that it is sufficient to check all natural numbers q for which $q \leq \lceil \sqrt{p} \rceil$ holds.

NB: Such a statement could require a proof or at least a reference to one.

Proof: Let $p = 83$.

We check and obtain that $2, 3, 4, 5, 6, 7, 8, 9, 10$ do not divide 83.

Simple proof techniques

Disproving conjectures

Conjecture

Suppose n is an integer larger than 1 and n is prime. Then $2^n - 1$ is prime.

Can you prove the conjecture? Try hard ...

If you can't, you should think to disprove it. A single n, which is prime, but $2^n - 1$ is not, is sufficient to disprove the conjecture!

The counterexample is $n = 11$ because 11 is prime, but

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

is not!

Outline

What is a Proof?

Simple Proof Techniques

Proof Techniques

- Proving and Using Forall Statements
- Proving and Using Or Statements
- Proving and Using And Statements
- Using Theorems
- Proving and Using Implications
- Handling iff Statements
- Proofs by Contradiction
- Handling Existential Statements

Learning Objectives

Proving ∀ statements

Inference rule for defined relations

The definition rule

Suppose some relationship has been defined. If the relationship holds (in some proof step or some assumption), then the defining condition may be inferred. Conversely, if the defining condition holds, then the relationship may be inferred.

Example

For sets A and B, A is a subset of B, $A \subseteq B$, provided that for all x such that (s.t.) $x \in A : x \in B$. In other word:

$$A \subseteq B \quad \text{if and only if (iff)} \quad \forall x\,((x \in A) \rightarrow (x \in B)) \text{ is valid}$$

Possibility 1:

1. $A \subseteq B$

Proving $\forall$ statements

Inference rule for defined relations

The definition rule

Suppose some relationship has been defined. If the relationship holds (in some proof step or some assumption), then the defining condition may be inferred. Conversely, if the defining condition holds, then the relationship may be inferred.

Example

For sets A and B, A is a subset of B, $A \subseteq B$, provided that for all x such that (s.t.) $x \in A : x \in B$. In other word:

$$A \subseteq B \quad \text{if and only if (iff)} \quad \forall x \left((x \in A) \to (x \in B) \right) \text{ is valid}$$

Possibility 1:

1. $A \subseteq B$
2. for all x s.t. $x \in A : x \in B$ (1; def $\subseteq$)

Proving ∀ statements

Inference rule for defined relations

The definition rule

Suppose some relationship has been defined. If the relationship holds (in some proof step or some assumption), then the defining condition may be inferred. Conversely, if the defining condition holds, then the relationship may be inferred.

Example

For sets A and B, A is a subset of B, $A \subseteq B$, provided that for all x such that (s.t.) $x \in A : x \in B$. In other word:

$$A \subseteq B \quad \text{if and only if (iff)} \quad \forall x \left((x \in A) \to (x \in B)\right) \text{ is valid}$$

Possibility 2:

1. for all x s.t. $x \in A : x \in B$

Proving ∀ statements

Inference rule for defined relations

The definition rule

Suppose some relationship has been defined. If the relationship holds (in some proof step or some assumption), then the defining condition may be inferred. Conversely, if the defining condition holds, then the relationship may be inferred.

Example

For sets A and B, A is a subset of B, $A \subseteq B$, provided that for all x such that (s.t.) $x \in A : x \in B$. In other word:

$$A \subseteq B \quad \text{if and only if (iff)} \quad \forall x\,((x \in A) \to (x \in B)) \text{ is valid}$$

Possibility 2:

1. for all x s.t. $x \in A : x \in B$
2. $A \subseteq B$ (1; def $\subseteq$)

Proving $\forall$ statements

Inference rule for $\forall$

- Let $\mathcal{P}(x)$ denote an expression (with the only free variable x)
- Example: $\mathcal{P}(x)$ denotes $x \in A$ and $\mathcal{Q}(x)$ denotes $x \in B$
- Then "for all x s.t. $x \in A : x \in B$" can be denoted as "for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$"

The rule for proving $\forall$ statements (pr $\forall$)

In order to prove a statement of the form "for all x s.t. $\mathcal{P}(x)$: $\mathcal{Q}(x)$", assume that x is an arbitrarily chosen element (eigenvariable) s.t. $\mathcal{P}(x)$ is true. Then establish that $\mathcal{Q}(x)$ is true.

Generalizations like "for all x, y s.t. $\mathcal{P}(x, y) : \mathcal{Q}(x, y)$" possible

Proving $\forall$ statements

Inference rule for $\forall$: An example

Let $C = \{x \in \mathbb{R} \mid x < 1\}$ and $D = \{x \in \mathbb{R} \mid x < 2\}$. Show $C \subseteq D$!

Assume: 1. $C = \{x \in \mathbb{R} \mid x < 1\}$

2. $D = \{x \in \mathbb{R} \mid x < 2\}$

Show: $C \subseteq D$

1.	Let $x \in C$ be arbitrary	
2	$x < 1$	(1, ass 1; def C)
3.	$x < 2$	(2; prop $\mathbb{R}$)
4.	$x \in D$	(3; def D)
5.	for all $x \in C : x \in D$	($1-4$; pr $\forall$)
6.	$C \subseteq D$	(5; def $\subseteq$)

How can we disprove "for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$"?

Proving ∀ statements

Inference rule for ∀: Some remarks

- By indentation, we indicate a subproof depending on an assumption like "Let $x \in C$ be arbitrary" above
- An assumption has no justification
- The subproof 2–4 is based on the assumption in 1
- Steps from 1–4 cannot occur in justifications once the subproof is finished (i.e, after pr ∀ in 5)
- We often write "for all $x \in C : x \in D$" instead of

  "for all x s.t. $x \in C : x \in D$"

Using $\forall$ statements

Inference rule for using $\forall$ statements

The rule for using $\forall$ statements in proofs (us $\forall$)

If we know that a statement "for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$" is true and if we have $\mathcal{P}(t)$ as a step already in the proof for any variable t, then we may infer $\mathcal{Q}(t)$.

Examples

1. $t \in A$
2. for all x s.t. $x \in A : x \in B$
3. ? (1,2; us $\forall$)

Using ∀ statements

Inference rule for using ∀ statements

The rule for using ∀ statements in proofs (us ∀)

If we know that a statement "for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$" is true and if we have $\mathcal{P}(t)$ as a step already in the proof for any variable t, then we may infer $\mathcal{Q}(t)$.

Examples

1. $t \in A$
2. for all x s.t. $x \in A : x \in B$
3. $t \in B$ (1,2; us ∀)

Using ∀ statements

Inference rule for using ∀ statements

The rule for using ∀ statements in proofs (us ∀)

If we know that a statement “for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$” is true and if we have $\mathcal{P}(t)$ as a step already in the proof for any variable t, then we may infer $\mathcal{Q}(t)$.

Examples

1. for all x, y s.t. $|x| < |y| : x^2 < y^2$
2. $|a| < |b|$
3. ? (1,2; us ∀)

Using $\forall$ statements

Inference rule for using $\forall$ statements

The rule for using $\forall$ statements in proofs (us $\forall$)

If we know that a statement “for all x s.t. $\mathcal{P}(x) : \mathcal{Q}(x)$” is true and if we have $\mathcal{P}(t)$ as a step already in the proof for any variable t, then we may infer $\mathcal{Q}(t)$.

Examples

1.	for all x, y s.t. $\lvert x\rvert < \lvert y\rvert : x^2 < y^2$	
2.	$\lvert a\rvert < \lvert b\rvert$	
3.	$a^2 < b^2$	(1,2; us $\forall$)

Using ∀ statements

Inference rule for using ∀ statements: An example

Let A, B, C be sets. Show that $\subseteq$ is transitive, i.e., show that if $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.

Assume:		A, B, C sets
	1.	$A \subseteq B$
	2.	$B \subseteq C$
Show:		$A \subseteq C$

1.	Let $x \in A$ be arbitrary	
2.	for all $t \in A : t \in B$	(ass 1; def $\subseteq$)
3.	$x \in B$	(1,2; us $\forall$)
4.	for all $t \in B : t \in C$	(ass 2; def $\subseteq$)
5.	$x \in C$	($3, 4$; us $\forall$)
6.	for all $x \in A : x \in C$	($1 - 5$; pr $\forall$)
7.	$A \subseteq C$	(6; def $\subseteq$)

Using $\vee$ statements

Inference rule for using $\vee$ statements

The rule for using $\vee$ statements in proofs (us $\vee$), preliminary

If we know that "$\mathcal{P}$ or $\mathcal{Q}$" is true and if we can show that $\mathcal{R}$ is true assuming $\mathcal{P}$ and also that $\mathcal{R}$ is true assuming $\mathcal{Q}$, then we may infer that $\mathcal{R}$ is true.

➥ This is reasoning by cases!

Definition

Given sets A and B, the union of A and B, $A \cup B$, is defined by $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$.

Using $\vee$ statements

Inference rule for using $\vee$ statements: An example

Prove: For sets A, B, C, if $A \subseteq C$ and $B \subseteq C$, then $(A \cup B) \subseteq C$.

Assume: A, B, C sets
1. $A \subseteq C$
2. $B \subseteq C$

Show: $(A \cup B) \subseteq C$

1.	Let $x \in A \cup B$ be arbitrary	
2.	$x \in A$ or $x \in B$	$(1;$ def $\cup)$
3.	Case 1: Assume $x \in A$	
4.	for all $t \in A : t \in C$	(ass 1; def $\subseteq$)
5.	$x \in C$	$(3, 4;$ us $\forall)$
6.	Case 2: Assume $x \in B$	
7.	for all $t \in B : t \in C$	(ass 2; def $\subseteq$)
8.	$x \in C$	$(6, 7;$ us $\forall)$
9.	$x \in C$	$(2, 3-8;$ us $\vee)$
10.	for all $x \in A \cup B : x \in C$	$(1-9;$ pr $\forall)$
11.	$(A \cup B) \subseteq C$	$(10;$ def $\subseteq)$

Using and proving $\vee$ statements

Inference rule for using $\vee$ statements

Extended definition rule (def^2)

When the statement $\mathcal{P}$ is the defining property of some definition, it is permissible to either use $\mathcal{P}$ or prove $\mathcal{P}$ (according to appropriate rules) without writing $\mathcal{P}$ itself as a step. For justification of the step inferred, give the definition and not the rule for using of proving $\mathcal{P}$.

➥ This results in shorter proofs (with some details omitted)

Examples

1.	$a \in M$	
2.	$M \subseteq N$	
3.	?	(1,2; def^2 $\subseteq$)

Warning: Later we will use def and def^2 synonymously!

Using and proving $\vee$ statements

Inference rule for using $\vee$ statements

Extended definition rule (def^2)

When the statement $\mathcal{P}$ is the defining property of some definition, it is permissible to either use $\mathcal{P}$ or prove $\mathcal{P}$ (according to appropriate rules) without writing $\mathcal{P}$ itself as a step. For justification of the step inferred, give the definition and not the rule for using of proving $\mathcal{P}$.

➥ This results in shorter proofs (with some details omitted)

Examples

1. $a \in M$
2. $M \subseteq N$
3. $a \in N$ (1,2; def^2 $\subseteq$)

Warning: Later we will use def and def^2 synonymously!

Using and proving $\vee$ statements

Inference rule for proving $\vee$ statements: An example

Prove rule for $\vee$ (pr $\vee$)

If $\mathcal{P}$ has been established as a line in a proof, then "$\mathcal{P}$ or $\mathcal{Q}$" may be written as a new line. Symmetrically, if $\mathcal{Q}$ has been established as a line in a proof, then "$\mathcal{P}$ or $\mathcal{Q}$" may be written as a new line.

Show: For sets A, B, C: if $A \subseteq B$ or $A \subseteq C$, then $A \subseteq B \cup C$

Using and proving $\vee$ statements

Inference rule for proving $\vee$ statements: An example proof

Show: For sets A, B, C: if $A \subseteq B$ or $A \subseteq C$, then $A \subseteq B \cup C$

Assume: A, B, C sets

1. $A \subseteq B$ or $A \subseteq C$

Show: $A \subseteq (B \cup C)$

1.	Let $x \in A$ be arbitrary	
2.	$A \subseteq B$ or $A \subseteq C$	(ass 1)
3.	Case 1: Assume $A \subseteq B$	
4.	$x \in B$	$(1, 3;$ def^2 $\subseteq)$
5.	$x \in B$ or $x \in C$	(4; pr $\vee$)
6.	Case 2: Assume $A \subseteq C$	
7.	$x \in C$	$(1, 6;$ def^2 $\subseteq)$
8.	$x \in B$ or $x \in C$	(7; pr $\vee$)
9.	$x \in B$ or $x \in C$	$(2, 3 - 8;$ us $\vee)$
10.	$x \in (B \cup C)$	(9; def $\cup$)
11.	for all $x \in A : x \in (B \cup C)$	$(1 - 10;$ pr $\forall)$
12.	$A \subseteq (B \cup C)$	(11; def $\subseteq$)

Using and proving $\vee$ statements

General versions of the $\vee$ inference rules

The following two rules generalize the corresponding ones from before

The rule for using $\vee$ statements in proofs (us $\vee$), final

If we know that "$\mathcal{P}_1$ or $\mathcal{P}_2$ or $\cdots$ or $\mathcal{P}_n$" is true and if we prove $\mathcal{R}$ in all cases that do not lead to a contradiction, then we infer that $\mathcal{R}$ is true. If all cases lead to a contradiction, then we infer the negation of the most recently assumed statement.

The rule for proving $\vee$ statements in proofs (pr $\vee$), final

We may write "$\mathcal{P}_1$ or $\mathcal{P}_2$ or $\cdots$ or $\mathcal{P}_n$" if we have established one of $\mathcal{P}_1$ through $\mathcal{P}_n$.

Using and proving $\wedge$ statements

Inference rule for using $\wedge$ statements

Rule for using conjunctions (us $\wedge$)

If "$\mathcal{P}$ and $\mathcal{Q}$" is a step in a proof, then $\mathcal{P}$ can be written as a step and $\mathcal{Q}$ can be written as a step.

Example

1. $a < 1$ and $a \in A$
2. ? (1; us $\wedge$)

Using and proving $\wedge$ statements

Inference rule for using $\wedge$ statements

Rule for using conjunctions (us $\wedge$)

If "$\mathcal{P}$ and $\mathcal{Q}$" is a step in a proof, then $\mathcal{P}$ can be written as a step and $\mathcal{Q}$ can be written as a step.

Example

1. $a < 1$ and $a \in A$
2. $a < 1$ (or 2. $a \in A$) (1; us $\wedge$)

Using and proving $\wedge$ statements

Inference rule for proving $\wedge$ statements

Rule for proving conjunctions (pr $\wedge$)

In order to show "$\mathcal{P}$ and $\mathcal{Q}$" in a proof, show $\mathcal{P}$ and also show $\mathcal{Q}$.

Example

$i.$	$\mathcal{P}$	
	$\vdots$	
$j.$	$\mathcal{Q}$	
	$\vdots$	
$k.$	?	?

Using and proving $\wedge$ statements

Inference rule for proving $\wedge$ statements

Rule for proving conjunctions (pr $\wedge$)

In order to show "$\mathcal{P}$ and $\mathcal{Q}$" in a proof, show $\mathcal{P}$ and also show $\mathcal{Q}$.

Example

$$\begin{array}{lll}
i. & \mathcal{P} & \\
 & \vdots & \\
j. & \mathcal{Q} & \\
 & \vdots & \\
k. & \mathcal{P} \text{ and } \mathcal{Q} & \qquad (i, j;\ \text{pr } \wedge)
\end{array}$$

Using and proving $\wedge$ statements

An example: Show for sets A, B that $A \cap B = B \cap A$ holds

Assume: A, B sets
Show: $A \cap B = B \cap A$

1.	Let $x \in A \cap B$ be arbitrary	
2.	$x \in A$ and $x \in B$	$(1;$ def $\cap)$
3.	$x \in A$	$(2;$ us $\wedge)$
4.	$x \in B$	$(2;$ us $\wedge)$
5.	$x \in B$ and $x \in A$	$(4, 3;$ pr $\wedge)$
6.	$x \in B \cap A$	$(5;$ def $\cap)$
7.	for all $x \in A \cap B : x \in B \cap A$	$(1 - 6;$ pr $\forall)$
8.	$A \cap B \subseteq B \cap A$	$(7;$ def $\subseteq)$
9.	$B \cap A \subseteq A \cap B$	$(1 - 8;$ symmetry$)$
10.	$A \cap B \subseteq B \cap A$ and $B \cap A \subseteq A \cap B$	$(8, 9;$ pr $\wedge)$
11.	$A \cap B = B \cap A$	$(10;$ def $=)$

In 11, we use the definition of $=$, i.e., $A = B$ iff $A \subseteq B \wedge B \subseteq A$

The rule of symmetry

Rule of symmetry

If $\mathcal{P}(A_1, B_1, \ldots)$ is any statement that has been proved for arbitrary $A_1, B_1, \ldots$ in the assumptions and hypothesis, and if $A_2, B_2, \ldots$ is any rearrangement of $A_1, B_1, \ldots$, then $\mathcal{P}(A_2, B_2, \ldots)$ is true. The foregoing also applies to universal variables inside a for all statement; that is, if for all $A_1, B_1, \ldots : \mathcal{P}(A_1, B_1, \ldots)$ is true, then for all $A_1, B_1, \ldots : \mathcal{P}(A_2, B_2, \ldots)$ is true.

Example from above:

$$\begin{array}{ccccccc} A & \cap & B & \subseteq & B & \cap & A \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ B & \cap & A & \subseteq & A & \cap & B \end{array}$$

Change A by B and B by A, i.e., apply the permutation (AB)

Using theorems

Applying substitutions

Rule for substitution (subs)

Any name or representation of a mathematical object can be replaced by another name/representation of the same object. It is necessary to avoid using the same name for different objects.

Two examples

1. $A \cap B = C$
2. $A = D$
3. $D \cap B = C$ (1,2; subs)

1. $x^2 + 3 = x$
2. $x = y + 1$
3. $(y + 1)^2 + 3 =$ y+1 (1,2; subs)

Using theorems

Theorem rule (thm)

In order to apply a theorem to steps in a proof, find a statement $\mathcal{P}$ equivalent to the statement in the theorem. Then $\mathcal{P}$ may be written as a new proof step or used, by subs, to change a step.

- This is one possibility to use lemmas in proofs
- Other possibilities will be discussed later when we consider equivalences and iff (if and only if) statements

Using theorems

An example: Show for sets A, B, C that $A \cup (B \cup C) = (A \cup B) \cup C$ holds

1.	Let $x \in (A \cup B) \cup C$ be arbitrary	
2.	$x \in (A \cup B)$ or $x \in C$	(1; def $\cup$)
3.	Case 1: $x \in A \cup B$	
4.	$x \in A$ or $x \in B$	(3; def $\cup$)
5.	Case 1a: $x \in A$	
6.	$x \in A \cup (B \cup C)$	(5; def $\cup$)
7.	Case 1b: $x \in B$	
8.	$x \in B \cup C$	(7; def $\cup$)
9.	$x \in A \cup (B \cup C)$	(8; def $\cup$)
10.	$x \in A \cup (B \cup C)$	(4, 5–9; us $\vee$)
11.	Case 2: $x \in C$	
12.	$x \in B \cup C$	(11; def $\cup$)
13.	$x \in A \cup (B \cup C)$	(12; def $\cup$)
14.	$x \in A \cup (B \cup C)$	(2, 3–13; us $\vee$)
15.	$(A \cup B) \cup C \subseteq A \cup (B \cup C)$	(1, 2–14; def $\subseteq$)
16.	$C \cup (B \cup A) \subseteq (C \cup B) \cup A$	(15; Thm $X \cup Y = Y \cup X$)
17.	$A \cup (B \cup C) \subseteq (A \cup B) \cup C$	(16; symmetry (AC))
18.	$A \cup (B \cup C) = (A \cup B) \cup C$	(15, 17; def $=$)

Proving and using if-then statements

Inference rule for proving if-then statements

Rule for proving implications (pr $\rightarrow$)

In order to prove a statement of the form “if $\mathcal{P}$, then $\mathcal{Q}$”, assume that $\mathcal{P}$ is true and show that $\mathcal{Q}$ is true.

$i-1.$	$\dots$	
$i.$	Assume $\mathcal{P}$	
	$\vdots$	
$j.$	$\mathcal{Q}$	
$k.$	If $\mathcal{P}$, then $\mathcal{Q}$	($i-j$; pr $\rightarrow$)

Proving and using if-then statements

Proving if-then statements: An example

Let A, B, C be sets. Prove: If $A \subseteq B$, then $A \cap C \subseteq B \cap C$.

Assume: A, B, C sets

Show: If $A \subseteq B$, then $A \cap C \subseteq B \cap C$

1.	Assume $A \subseteq B$	
2.	Let $x \in A \cap C$ be arbitrary	
3.	$x \in A$	(2; def $\cap$)
4.	$x \in C$	(2; def $\cap$)
5.	$x \in B$	(1, 3; def $\subseteq$)
6.	$x \in B \cap C$	(5, 4; def $\cap$)
7.	$A \cap C \subseteq B \cap C$	(2, 3 – 6; def $\subseteq$)
8.	If $A \subseteq B$, then $A \cap C \subseteq B \cap C$	(1 – 7; pr $\rightarrow$)

Proving and using if-then statements

Inference rule for using if-then statements

Rule for using implications (us $\rightarrow$) (or modus ponens (MP))

If $\mathcal{P}$ and "if $\mathcal{P}$, then $\mathcal{Q}$" are steps in a proof, then we may infer that $\mathcal{Q}$ is a step.

$i.$	$\mathcal{P}$	
	$\vdots$	
$j.$	If $\mathcal{P}$, then $\mathcal{Q}$	
$j+1.$	$\mathcal{Q}$	$(i, j;$ us $\rightarrow)$

Example

1.	if $x < 2$, then $x \in A$	
2.	$x < 2$	
3.	$x \in A$	(1,2; us $\rightarrow$)

Proving and using if-then statements

The inference rule for $\mathcal{P}$ or $\neg\mathcal{P}$ (lem)

Rule for $\mathcal{P}$ or $\neg\mathcal{P}$ (lem (= law of excluded middle))

For any $\mathcal{P}$, $\mathcal{P} \vee \neg\mathcal{P}$ is true (in classical logic).

➥ lem is usually used to allow reasoning by cases

For a real number x, the absolute value of x, $|x|$, is defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

The two cases are of the form $(x \geq 0) \vee \neg(x \geq 0)$

Prove: For all $x \in \mathbb{R}$, $|x|^2 = x^2$.

Proving and using if-then statements

The proof for the statement

```
1.      Let $x \in \mathbb{R}$ be arbitrary
2.      $x \geq 0$ or $\neg(x \geq 0)$                    $(\text{lem})$
3.          Case 1: $x \geq 0$
4.          $|x| = x$                                 $(3; \text{def } |\cdot|)$
5.          $|x|^2 = x^2$                             $(4; \text{prop } \mathbb{R})$
6.          Case 2: $\neg(x \geq 0)$
7.          $x < 0$                                   $(6; \text{prop } \mathbb{R}))$
8.          $|x| = -x$                                $(7; \text{def } |\cdot|)$
9.          $|x|^2 = (-x)^2$                          $(8; \text{prop } \mathbb{R})$
10.         $(-x)^2 = x^2$                            $(9; \text{prop } \mathbb{R})$
11.         $|x|^2 = x^2$                             $(9, 10; \text{subs})$
12.     $|x|^2 = x^2$                                 $(2, 3 - 11; \text{us } \vee)$
13. for all $x \in \mathbb{R} : |x|^2 = x^2$          $(1 - 12; \text{pr } \forall)$
```

Proving and using if-then statements

Equivalences

Proving equivalences (pr $\leftrightarrow$)

In order to show that "$\mathcal{P}$ is equivalent to $\mathcal{Q}$", first assume $\mathcal{P}$ and show $\mathcal{Q}$, and then assume $\mathcal{Q}$ and show $\mathcal{P}$.

Using equivalences (us $\leftrightarrow$)

Any statement may be substituted for an equivalent statement

- This is an application of the equivalent replacement theorem
- We implicitly used this rule before, e.g., for definitions

Handling iff statements

- Recall: $\mathcal{P}$ iff $\mathcal{Q}$ holds iff $\mathcal{P} \leftrightarrow \mathcal{Q}$ is valid
- Prove $\mathcal{P}$ iff $\mathcal{Q}$ by proving "if $\mathcal{P}$, then $\mathcal{Q}$" and "if $\mathcal{Q}$, then $\mathcal{P}$"
- "If $\mathcal{P}$, then $\mathcal{Q}$" is proved by assuming $\mathcal{P}$ and deriving $\mathcal{Q}$
- Alternatively, "if $\mathcal{P}$, then $\mathcal{Q}$" can be proved by contraposition

  Prove "if $\mathcal{P}$, then $\mathcal{Q}$" by assuming $\neg\mathcal{Q}$ and deriving $\neg\mathcal{P}$

Justify this procedure!

Proofs by contradiction

The inference scheme

Idea: Assume the negation of some $\mathcal{P}$ and derive a contradiction!

$\vdots$

$i.$ $\mathcal{Q}$

$\vdots$

$j.$ Assume $\neg\mathcal{P}$ (to get a contradiction)

$\vdots$

$k.$ $\neg\mathcal{Q}$ (which contradicts $\mathcal{Q}$ at some i.)

$k+1.$ $\mathcal{P}$ ($j-k$; contradiction)

Proofs by contradiction

An example

Show: For every $x \in \mathbb{R}$ with $x \in [0, \pi/2]$: $\sin x + \cos x \geq 1$

1. Let $x \in \mathbb{R} \wedge x \in [0, \pi/2]$ be arbitrary
2. $\sin x \geq 0$ and $\cos x \geq 0$ (1; prop $\sin, \cos$)
3. Assume $\neg(\sin x + \cos x \geq 1)$, i.e., $\sin x + \cos x < 1$
4. $0 \leq \sin x + \cos x < 1$ ($2, 3$; prop $\mathbb{R}$)
5. $0^2 \leq (\sin x + \cos x)^2 < 1^2$ (4; prop $\mathbb{R}$)
6. $0^2 \leq \sin^2 x + 2 \sin x \cos x + \cos^2 x < 1^2$ (5; prop $\mathbb{R}$)
7. $0^2 \leq 1 + 2 \sin x \cos x < 1^2$ (6; $\sin^2 + \cos^2 = 1$)
8. $\sin x \cos x < 0$ (7; prop $\mathbb{R}$)
9. either $\sin x < 0$ or $\cos x < 0$ (8; prop $\mathbb{R}$)
   contradicts 2.
10. $\sin x + \cos x \geq 1$ ($3 - 9$; contradiction)
11. $\forall x \in \mathbb{R} \wedge x \in [0, \pi/2] : \sin x + \cos x \geq 1$ ($1 - 10$; pr $\forall$)

Handling existential statements

Using existential statements

Using existential statements (us $\exists$)

To use the statement “$\mathcal{P}(j)$ for some $1 \leq j \leq n$” in a proof, immediately follow it with the step

“Pick $1 \leq j_0 \leq n$ such that $\mathcal{P}(j_0)$”.

This defines the symbol j_0. The truth of both $1 \leq j_0 \leq n$ and $\mathcal{P}(j_0)$ may be used in the remainder of the proof.

Example: For each $i = 1, 2, \ldots, 10$, define $A_i = \{t \in \mathbb{R} \mid 0 < t < \frac{1}{i}\}$

1.	$x \in A_i$ for some $1 \leq i \leq 10$	
2.	pick $1 \leq j \leq 10$ such that $x \in A_j$	(1; us $\exists$)
3.	$1 \leq j \leq 10$	(from step 2.)
4.	$x \in A_j$	(from step 2.)

Handling existential statements

Using existential statements: An example

Prove: Let $B, A_1, \ldots, A_n$ be sets. Suppose that $A_i \subseteq B$ holds for all $1 \leq i \leq n$. Then $\left(\bigcup_{i=1}^{n} A_i\right) \subseteq B$.

Assume:	$A_i \subseteq B$ for all $1 \leq i \leq n$	
Show:	$\left(\bigcup_{i=1}^{n} A_i\right) \subseteq B$	
1.	Let $x \in \bigcup_{i=1}^{n} A_i$ be arbitrary	
2.	$x \in A_i$ for some $1 \leq i \leq n$	$(1;$ def $\cup)$
3.	pick $1 \leq j \leq n$ such that $x \in A_j$	$(2;$ us $\exists)$
4.	$A_j \subseteq B$	$(3,$ ass; us $\forall)$
5.	$x \in B$	$(3, 4;$ def $\subseteq)$
6.	$\left(\bigcup_{i=1}^{n} A_i\right) \subseteq B$	$(1 - 5;$ def $\subseteq)$

Remark: Our proof presentations will become more high level!

Handling existential statements

Proving existential statements

Proving existential statements (pr $\exists$)

If $1 \leq i \leq n$ and $\mathcal{P}(i)$ are steps in a proof, then “for some $1 \leq j \leq n : \mathcal{P}(j)$” can be written as a proof step.

Examples

1. ?
2. $1 \leq 3 \leq 10$
3. for some $1 \leq i \leq 10\colon x \in A_i$ $\qquad$ $(1, 2;$ pr $\exists)$

Handling existential statements

Proving existential statements

Proving existential statements (pr $\exists$)

If $1 \leq i \leq n$ and $\mathcal{P}(i)$ are steps in a proof, then "for some $1 \leq j \leq n : \mathcal{P}(j)$" can be written as a proof step.

Examples

1. $x \in A_3$
2. $1 \leq 3 \leq 10$
3. for some $1 \leq i \leq 10\colon x \in A_i$ $\qquad$ $(1, 2;$ pr $\exists)$

Handling existential statements

Proving existential statements

Proving existential statements (pr $\exists$)

If $1 \leq i \leq n$ and $\mathcal{P}(i)$ are steps in a proof, then "for some $1 \leq j \leq n : \mathcal{P}(j)$" can be written as a proof step.

Examples

1. $x \in A_3$
2. $1 \leq 3 \leq 10$
3. for some $1 \leq i \leq 10 \colon x \in A_i$ $(1, 2;$ pr $\exists)$

---

1. $x \in A_j$
2. $1 \leq j \leq n$
3. ?

Handling existential statements

Proving existential statements

Proving existential statements (pr $\exists$)

If $1 \leq i \leq n$ and $\mathcal{P}(i)$ are steps in a proof, then "for some $1 \leq j \leq n : \mathcal{P}(j)$" can be written as a proof step.

Examples

1. $x \in A_3$
2. $1 \leq 3 \leq 10$
3. for some $1 \leq i \leq 10 \colon x \in A_i$ $\qquad$ $(1, 2;$ pr $\exists)$

1. $x \in A_j$
2. $1 \leq j \leq n$
3. for some $1 \leq i \leq n \colon x \in A_i$ $\qquad$ $(1, 2;$ pr $\exists)$

Handling existential statements

Proving existential statements

Proving existential statements (pr $\exists$)

To prove the statement "for some $1 \leq j \leq n : \mathcal{P}(j)$", define j in your proof (in terms of previously defined symbols) and show that $\mathcal{P}(j)$ and $1 \leq j \leq n$ hold for j.

Let $A_1, \ldots, A_n$ be sets. Show: For all $1 \leq j \leq n : A_j \subseteq \bigcup_{i=1}^{n} A_i$

```
1.      Let $1 \leq j \leq n$
2.          Let $x \in A_j$ be arbitrary
3.          for some $1 \leq i \leq n : x \in A_i$                    $(1, 2;$ pr $\exists)$
4.          $x \in \bigcup_{i=1}^{n} A_i$                              $(3;$ def $\cup)$
5.      $A_j \subseteq \bigcup_{i=1}^{n} A_i$                          $(2 - 4;$ def $\subseteq)$
6.  for all $1 \leq j \leq n : A_j \subseteq \bigcup_{i=1}^{n} A_i$    $(1 - 5;$ pr $\forall)$
```

Negations

Negation rule ($\neg$)

The negation of “for all $1 \leq i \leq n : \mathcal{P}(i)$” is “for some $1 \leq i \leq n : \neg\mathcal{P}(i)$”. The negation of “for some $1 \leq i \leq n : \mathcal{P}(i)$” is “for all $1 \leq i \leq n : \neg\mathcal{P}(i)$”.

- ➥ This is the application of “quantifier de Morgan rules”
- ➥ Further negation rules (exploiting de Morgan’s laws) can be defined!

Learning objectives

- Ability to discuss the notions of formal and informal proofs
- Ability to employ the discussed simple proof techniques
- Ability to discuss the general structure of proofs, to apply the different proof techniques and to produce proofs of theorems
- Ability to disprove simple false conjectures