Discrete Mathematics in Computer Science
A2. Proofs I

Malte Helmert, Gabriele Röger

University of Basel

September 25, 2023

Discrete Mathematics in Computer Science

A2.1 What is a Proof?

A2.2 Proof Strategies

A2.3 Direct Proof

A2.4 Indirect Proof

A2.5 Proof by Contrapositive

A2.6 Excursus: Computer-assisted Theorem Proving

A2.1 What is a Proof?

What is a Proof?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conlusion
  that some statement must be true.

What is a statement?

Mathematical Statements

> **Mathematical Statement**
> A mathematical statement consists of a set of preconditions
> and a set of conclusions.
>
> The statement is true if the conclusions are true
> whenever the preconditions are true.

Notes:

- ▶ set of preconditions is sometimes empty
- ▶ often, "assumptions" is used instead of "preconditions";
  slightly unfortunate because "assumption"
  is also used with another meaning ($\rightsquigarrow$ cf. indirect proofs)

Examples of Mathematical Statements

Examples (some true, some false):

- ▶ "Let $p \in \mathbb{N}_0$ be a prime number. Then p is odd."
- ▶ "There exists an even prime number."
- ▶ "Let $p \in \mathbb{N}_0$ with $p \geq 3$ be a prime number. Then p is odd."
- ▶ "All prime numbers $p \geq 3$ are odd."
- ▶ "For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$"

What are the preconditions, what are the conclusions?

On what Statements can we Build the Proof?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conlusion
  that some statement must be true.

We can use:

- ▶ axioms: statements that are assumed to always be true
  in the current context
- ▶ theorems and lemmas: statements that were already proven
  - ▶ lemma: an intermediate tool
  - ▶ theorem: itself a relevant result
- ▶ premises: assumptions we make
  to see what consequences they have

What is a Logical Step?

A mathematical proof is

- ▶ a sequence of logical steps
- ▶ starting with one set of statements
- ▶ that comes to the conlusion
  that some statement must be true.

Each step directly follows

- ▶ from the axioms,
- ▶ premises,
- ▶ previously proven statements and
- ▶ the preconditions of the statement we want to prove.

For a formal definition, we would need formal logics.

The Role of Definitions

> **Definition**
>
> A set is an unordered collection of distinct objects.
>
> The objects in a set are called the elements of the set.
>
> We write $x \in S$ to indicate that x is an element of set S, and $x \notin S$ to indicate that S does not contain x.
>
> The set that does not contain any objects is the *empty set* $\emptyset$.

▶ A definition introduces an abbreviation.

▶ Whenever we say "set", we could instead say "an unordered collection of distinct objects" and vice versa.

▶ Definitions can also introduce notation.

Disproofs

▶ A disproof (refutation) shows that a given mathematical statement is false by giving an example where the preconditions are true, but the conclusion is false.

▶ This requires deriving, in a sequence of proof steps, the opposite (negation) of the conclusion.

A Word on Style

A proof should help the reader to see why the result must be true.

▶ A proof should be easy to follow.
▶ Omit unnecessary information.
▶ Move self-contained parts into separate lemmas.
▶ In complicated proofs, reveal the overall structure in advance.
▶ Have a clear line of argument.

$\rightarrow$ Writing a proof is like writing an essay.

Recommended reading (ADAM additional ressources):

▶ "Some Remarks on Writing Mathematical Proofs" (John M. Lee)
▶ "§1. Minicourse on technical writing" of "Mathematical Writing"
   (Donald E. Knuth, Tracy Larrabee, and Paul M. Roberts)

A2.2 Proof Strategies

Common Forms of Statements

Many statements have one of these forms:

1. "All $x \in S$ with the property P also have the property Q."
2. "A is a subset of B."
3. "For all $x \in S$: x has property P iff x has property Q."
4. "$A = B$", where A and B are sets.

In the following, we will discuss some typical proof/disproof strategies for such statements.

Proof Strategies

1. "All $x \in S$ with the property P also have the property Q."
   "For all $x \in S$: if x has property P, then x has property Q."

   ▶ To prove, assume you are given an arbitrary $x \in S$
     that has the property P.
     Give a sequence of proof steps showing that x
     must have the property Q.

   ▶ To disprove, find a counterexample, i.e., find an $x \in S$
     that has property P but not Q and prove this.

Proof Strategies

2. "A is a subset of B."
   - ▶ To prove, assume you have an arbitrary element $x \in A$
     and prove that $x \in B$.
   - ▶ To disprove, find an element in $x \in A \setminus B$
     and prove that $x \in A \setminus B$.

Proof Strategies

3. "For all $x \in S$: x has property P iff x has property Q."
   ("iff": "if and only if")
   - To prove, separately prove "if P then Q" and "if Q then P".
   - To disprove, disprove "if P then Q" or disprove "if Q then P".

Proof Strategies

4. "$A = B$", where A and B are sets.
   - ▶ To prove, separately prove "$A \subseteq B$" and "$B \subseteq A$".
   - ▶ To disprove, disprove "$A \subseteq B$" or disprove "$B \subseteq A$".

Proof Techniques

most common proof techniques:

- ▶ direct proof
- ▶ indirect proof (proof by contradiction)
- ▶ contrapositive
- ▶ mathematical induction
- ▶ structural induction

A2.3 Direct Proof

Direct Proof

Direct Proof
Direct derivation of the statement by deducing or rewriting.

Direct Proof: Example

$\rightarrow$ Separate file proof_examples_1.pdf

A2.4 Indirect Proof

Indirect Proof

Indirect Proof (Proof by Contradiction)

▶ Make an **assumption** that the statement is false.

▶ Derive a **contradiction** from the assumption together with the preconditions of the statement.

▶ This shows that the assumption must be false given the preconditions of the statement, and hence the original statement must be true.

Indirect Proof: Example

$\rightarrow$ Separate file proof_examples_1.pdf

A2.5 Proof by Contrapositive

Contrapositive

(Proof by) Contrapositive
Prove "If A, then B" by proving "If not B, then not A."

Examples:

▶ Prove "For all $n \in \mathbb{N}_0$: if n^2 is odd, then n is odd"
  by proving "For all $n \in \mathbb{N}_0$, if n is even, then n^2 is even."

▶ Prove "For all $n \in \mathbb{N}_0$: if n is not a square number,
  then $\sqrt{n}$ is irrational" by proving "For all $n \in \mathbb{N}_0$:
  if $\sqrt{n}$ is rational, then n is a square number."

Contrapositive: Example

$\rightarrow$ Separate file proof_examples_1.pdf

A2.6 Excursus: Computer-assisted Theorem Proving
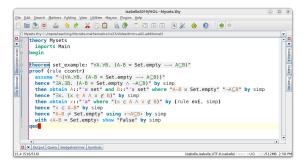
Computer-assisted Proofs

▶ Computers can help proving theorems.
▶ Computer-aided proofs have for example been used for proving theorems by exhaustion.
▶ Example: Four color theorem

Interactive Theorem Proving

▶ On the lowest abstraction level, rigorous mathematical proofs rely on formal logic.

▶ On this level, proofs can be automatically verified by computers.

▶ Nobody wants to write or read proofs on this level of detail.

▶ In Interactive Theorem Proving a human guides the proof and the computer tries to fill in the details.

▶ If it succeeds, we can be very confident that the proof is valid.

▶ Example theorem provers: Isabelle/HOL, Lean

Example

⤳ Demo

Summary

- ▶ A proof should convince the reader by logical steps of the truth of some mathematical statement.

- ▶ There are standard strategies for proving some common forms of statements, e.g. some property of all elements of a set.

- ▶ Direct proof: derive statement by deducing or rewriting.

- ▶ Indirect proof: derive contradiction from the assumption that the statement is false.

- ▶ Proof by contrapositive: Prove "If A, then B" by proving "If not B, then not A.".