Theory of Computer Science
A3. Proof Techniques

Gabriele Röger

University of Basel

March 4, 2024

A3.1 Introduction

What is a Proof?

A mathematical proof is
- a sequence of logical steps
- starting with one set of statements
- that comes to the conclusion 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 conclusion 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 conclusion 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 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.
- Formally, disproofs are proofs of modified ("negated") statements.
- Be careful about how to negate a statement!

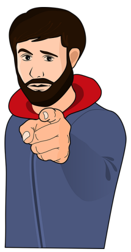
Exercise

You want to disprove the following statement with a counterexample:

If the sun is shining then all kids eat ice cream.

What properties must your counterexample have?

[Discuss with your neighbour; 2 minutes]



Proof Strategies

typical proof/disproof 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

typical proof/disproof 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

typical proof/disproof 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

typical proof/disproof 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

proof techniques we use in this course:

- direct proof
- indirect proof (proof by contradiction)
- structural induction

A3.2 Direct Proof

Direct Proof

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

Direct Proof: Example

Theorem (distributivity)
For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof.
We first show that $x \in A \cap (B \cup C)$ implies $x \in (A \cap B) \cup (A \cap C)$ ($\subseteq$ part):

Let $x \in A \cap (B \cup C)$. Then by the definition of $\cap$ it holds that $x \in A$ and $x \in B \cup C$.

We make a case distinction between $x \in B$ and $x \notin B$:

If $x \in B$ then, because $x \in A$ is true, $x \in A \cap B$ must be true.

Otherwise, because $x \in B \cup C$ we know that $x \in C$ and thus with $x \in A$, that $x \in A \cap C$.

In both cases $x \in A \cap B$ or $x \in A \cap C$, and we conclude $x \in (A \cap B) \cup (A \cap C)$. ...

Direct Proof: Example

Theorem (distributivity)
For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof (continued).
$\supseteq$ part: we must show that $x \in (A \cap B) \cup (A \cap C)$ implies $x \in A \cap (B \cup C)$.

Let $x \in (A \cap B) \cup (A \cap C)$.

We make a case distinction between $x \in A \cap B$ and $x \notin A \cap B$:

If $x \in A \cap B$ then $x \in A$ and $x \in B$.
The latter implies $x \in B \cup C$ and hence $x \in A \cap (B \cup C)$.

If $x \notin A \cap B$ we know $x \in A \cap C$ due to $x \in (A \cap B) \cup (A \cap C)$.
This (analogously) implies $x \in A$ and $x \in C$, and hence $x \in B \cup C$ and thus $x \in A \cap (B \cup C)$.

In both cases we conclude $x \in A \cap (B \cup C)$. ...

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof (continued).

We have shown that every element of $A \cap (B \cup C)$ is an element of $(A \cap B) \cup (A \cap C)$ and vice versa. Thus, both sets are equal. □

Direct Proof: Example

Theorem (distributivity)

For all sets A, B, C: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Proof.

Alternative:

$$\begin{aligned} A \cap (B \cup C) &= \{x \mid x \in A \text{ and } x \in B \cup C\} \\ &= \{x \mid x \in A \text{ and } (x \in B \text{ or } x \in C)\} \\ &= \{x \mid (x \in A \text{ and } x \in B) \text{ or } (x \in A \text{ and } x \in C)\} \\ &= \{x \mid x \in A \cap B \text{ or } x \in A \cap C\} \\ &= (A \cap B) \cup (A \cap C) \end{aligned}$$

□

A3.3 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

Theorem
There are infinitely many prime numbers.

Proof.
Assumption: There are only finitely many prime numbers.

Let $P = \{p_1, \dots, p_n\}$ be the set of all prime numbers.

Define $m = p_1 \cdot \ldots \cdot p_n + 1$.

Since $m \geq 2$, it must have a prime factor.
Let p be such a prime factor.

Since p is a prime number, p has to be in P.

The number m is not divisible without remainder
by any of the numbers in P. Hence p is no factor of m.

$\rightsquigarrow$ Contradiction □

A3.4 Structural Induction

Inductively Defined Sets: Examples

Example (Natural Numbers)
The set $\mathbb{N}_0$ of natural numbers is inductively defined as follows:
- 0 is a natural number.
- If n is a natural number, then $n + 1$ is a natural number.

Example (Binary Tree)
The set $\mathcal{B}$ of binary trees is inductively defined as follows:
- □ is a binary tree (a leaf)
- If L and R are binary trees, then $\langle L, \bigcirc, R\rangle$ is a binary tree (with inner node $\bigcirc$).

Implicit statement: all elements of the set can be constructed by finite application of these rules

Inductive Definition of a Set

Inductive Definition
A set M can be defined inductively by specifying
- basic elements that are contained in M
- construction rules of the form
  "Given some elements of M, another element of M can be constructed like this."

Structural Induction

Structural Induction

Proof of statement for all elements of an inductively defined set

- basis: proof of the statement for the basic elements
- induction hypothesis (IH):
  suppose that the statement is true for some elements M
- inductive step: proof of the statement for elements constructed by applying a construction rule to M
  (one inductive step for each construction rule)

Structural Induction: Example (1)

Definition (Leaves of a Binary Tree)

The number of leaves of a binary tree B, written $\mathit{leaves}(B)$, is defined as follows:

$$\mathit{leaves}(\square) = 1$$
$$\mathit{leaves}(\langle L, \bigcirc, R\rangle) = \mathit{leaves}(L) + \mathit{leaves}(R)$$

Definition (Inner Nodes of a Binary Tree)

The number of inner nodes of a binary tree B, written $\mathit{inner}(B)$, is defined as follows:

$$\mathit{inner}(\square) = 0$$
$$\mathit{inner}(\langle L, \bigcirc, R\rangle) = \mathit{inner}(L) + \mathit{inner}(R) + 1$$

Structural Induction: Example (2)

Theorem

For all binary trees B: $\mathit{inner}(B) = \mathit{leaves}(B) - 1$.

Proof.

induction basis:

$\mathit{inner}(\square) = 0 = 1 - 1 = \mathit{leaves}(\square) - 1$

$\rightsquigarrow$ statement is true for base case ...

Structural Induction: Example (3)

Proof (continued).

induction hypothesis:

to prove that the statement is true for a composite tree $\langle L, \bigcirc, R\rangle$, we may use that it is true for the subtrees L and R.

inductive step for $B = \langle L, \bigcirc, R\rangle$:

$$\begin{aligned}\mathit{inner}(B) &= \mathit{inner}(L) + \mathit{inner}(R) + 1\\ &\overset{\text{IH}}{=} (\mathit{leaves}(L) - 1) + (\mathit{leaves}(R) - 1) + 1\\ &= \mathit{leaves}(L) + \mathit{leaves}(R) - 1 = \mathit{leaves}(B) - 1\end{aligned}$$

□

Structural Induction: Exercise (if time)

Definition (Height of a Binary Tree)

The height of a binary tree B, written $height(B)$,
is defined as follows:

$$height(\Box) = 0$$
$$height(\langle L, \bigcirc, R\rangle) = \max\{height(L), height(R)\} + 1$$

Prove by structural induction:

Theorem

For all binary trees B: $leaves(B) \leq 2^{height(B)}$.

A3.5 Summary

Summary

- A proof is based on axioms and previously proven statements.
- Individual proof steps must be obvious derivations.
- direct proof: sequence of derivations or rewriting
- indirect proof: refute the negated statement
- structural induction: generalization of mathematical induction to arbitrary recursive structures