

Discrete Mathematics in Computer Science

A4. Proof Techniques I

Malte Helmert, Gabriele Röger

University of Basel

September 24, 2025

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 .”
(“iff”: “if and only if”)
- ④ “ $A = B$ ”, where A and B are sets.

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 .”
(“iff”: “if and only if”)
- 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

Direct Proof

Direct Proof

Direct Proof

Direct derivation of the statement by deducing or rewriting.

German: Direkter Beweis

Direct Proof: Example

Theorem

For all sets A , B and C it holds that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof.

Direct Proof: Example

Theorem

For all sets A , B and C it holds that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof.

Let A , B and C be arbitrary sets.

Direct Proof: Example

Theorem

For all sets A , B and C it holds that

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Proof.

Let A , B and C be arbitrary sets.

We will show separately that

- $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that
- $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

...

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$.

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

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

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

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

Case 1 ($x \in B$): As $x \in A$ is true, it holds in this case that $x \in (A \cap B)$.

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

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

Case 1 ($x \in B$): As $x \in A$ is true, it holds in this case that $x \in (A \cap B)$.

Case 2 ($x \notin B$): From $x \in (B \cup C)$ it follows for this case that $x \in C$. With $x \in A$ we conclude that $x \in (A \cap C)$.

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

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

Case 1 ($x \in B$): As $x \in A$ is true, it holds in this case that $x \in (A \cap B)$.

Case 2 ($x \notin B$): From $x \in (B \cup C)$ it follows for this case that $x \in C$. With $x \in A$ we conclude that $x \in (A \cap C)$.

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

Direct Proof: Example cont.

Proof (continued).

We first show that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:

If $A \cap (B \cup C)$ is empty, the statement is trivially true. Otherwise consider an arbitrary $x \in A \cap (B \cup C)$. By the definition of the intersection it holds that $x \in A$ and that $x \in (B \cup C)$.

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

Case 1 ($x \in B$): As $x \in A$ is true, it holds in this case that $x \in (A \cap B)$.

Case 2 ($x \notin B$): From $x \in (B \cup C)$ it follows for this case that $x \in C$. With $x \in A$ we conclude that $x \in (A \cap C)$.

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

As x was chosen arbitrarily from $A \cap (B \cup C)$, we have shown that every element of $A \cap (B \cup C)$ is an element of $(A \cap B) \cup (A \cap C)$, so it holds that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$

Direct Proof: Example cont.

Proof (continued).

We will now show that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

... **[Homework assignment]** ...

Overall we have shown for arbitrary sets A, B and C that $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and that $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$, which concludes the proof of the theorem. □

Indirect Proof

Indirect Proof

Indirect Proof (Proof by Contradiction)

- Make an **assumption** that the statement is false.
- Use the assumption to derive a **contradiction**.
- This shows that the assumption must be false and hence the original statement must be true.

German: Indirekter Beweis, Beweis durch Widerspruch

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Since $A \not\subseteq B$ there is some $x \in A$ such that $x \notin B$.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Since $A \not\subseteq B$ there is some $x \in A$ such that $x \notin B$.

For this x it holds that $x \in A \setminus B$.

Indirect Proof: Example

Theorem

Let A and B be sets. If $A \setminus B = \emptyset$ then $A \subseteq B$.

Proof.

We prove the theorem by contradiction.

Assume that there are sets A and B with $A \setminus B = \emptyset$ and $A \not\subseteq B$.

Let A and B be such sets.

Since $A \not\subseteq B$ there is some $x \in A$ such that $x \notin B$.

For this x it holds that $x \in A \setminus B$.

This is a contradiction to $A \setminus B = \emptyset$.

We conclude that the assumption was false and thus the theorem is true. □

Proof by Contrapositive

Contrapositive

(Proof by) Contrapositive

Prove “If A , then B ” by proving “If not B , then not A .”

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.”

German: Kontraposition

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.

We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \not\subseteq B$.

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.

We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \not\subseteq B$.

Let A and B be arbitrary sets with $A \setminus B \neq \emptyset$.

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.

We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \not\subseteq B$.

Let A and B be arbitrary sets with $A \setminus B \neq \emptyset$.

As the set difference is not empty, there is at least one x with $x \in A \setminus B$.

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.

We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \not\subseteq B$.

Let A and B be arbitrary sets with $A \setminus B \neq \emptyset$.

As the set difference is not empty, there is at least one x with $x \in A \setminus B$. By the definition of the set difference ($\setminus$), it holds for such x that $x \in A$ and $x \notin B$.

Contrapositive: Example

Theorem

For any sets A and B : If $A \subseteq B$ then $A \setminus B = \emptyset$.

Proof.

We prove the theorem by contrapositive, showing for any sets A and B that if $A \setminus B \neq \emptyset$ then $A \not\subseteq B$.

Let A and B be arbitrary sets with $A \setminus B \neq \emptyset$.

As the set difference is not empty, there is at least one x with $x \in A \setminus B$. By the definition of the set difference ($\setminus$), it holds for such x that $x \in A$ and $x \notin B$.

Hence, not all elements of A are elements of B , so it does not hold that $A \subseteq B$. □

Questions



Questions?

Summary

Summary

- 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.”.