# Lecture 3 — Proof Techniques

A proof is a convincing demonstration (within the accepted standards of the field) that some mathematical statement is necessarily true. Proofs are obtained from deductive reasoning, rather than from inductive or empirical arguments. That is, a proof must demonstrate that a statement is true in all cases, without a single exception.

In this chapter we will take a look at the most common and expedient proof techniques and give examples to illustrate them.

## 3.1 Direct proof

*A direct proof [direkter Beweis] is straightforward. The conclusion is established by logically combining the axioms, definitions, and earlier theorems. Thus, you start out with the assumptions $A$ and try to directly conclude proposition $B$. I.e., we want to show $A \implies B$.*

**Example 3.1.1.**

- The sum of two even integers is even.
- If $a$ divides $b$ and $a$ divides $c$ then $a$ divides $b+c$.

## 3.2 Proof by contradiction

*A proof by contradiction [Beweis durch Widerspruch] (also known as reductio ad absurdum) uses the fact that a proposition can only be either true or false.*

*It is shown that if some statement (namely, the negation of what we aim to prove) were true, then a logical contradiction would have to occur.*

**Example 3.2.1.**

- $\sqrt{3}$ is irrational.
- There is no smallest positive (*i.e.*, $> 0$) rational number.

## 3.3 Proof by contraposition

*A proof by contraposition [Beweis durch Kontraposition] uses*

$$(A \implies B) \iff (\neg B \implies \neg A).$$

*In other words, it establishes the conclusion "if $A$ then $B$" by proving the equivalent contrapositive statement "if not $B$ then not $A$".*

**Example 3.3.1.** If $n^2$ is even, then $n$ is even.

## 3.4 Proof by induction

*A proof by induction [Beweis durch vollständige Induktion] is a useful tool to prove a proposition $B(n)$ which is stated for all natural numbers $n$ (or for all natural numbers greater than a given number $k \in \mathbb{N}$).*

*A proof by induction consists of two parts:*

(i) *Induction beginning [Induktionsanfang]: Prove $B(1)$ (or $B(k)$).*

(ii) *Induction step [Induktionsschritt]: Assume that $B(n)$ is true and show that $B(n+1)$ is true (making use of the fact that $B(n)$ is true).*

*Imagine a domino chain. The induction step assures that a domino (here $n+1$) falls if domino $n$ falls.*

*Look at this example:*

**Example 3.4.1.** A typical example for a proof by induction is the following:

**Proposition:** $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

*Proof.* We do a proof by induction.

**Induction beginning:** For $n = 1$, the claim is

$$\sum_{k=1}^{1} k = 1 = \frac{1 \cdot 2}{2},$$

which is quite obviously true.

**Induction step:** Now we assume that the proposition is true for $n$. That means

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$$

is true. With the help of this assumption we try to prove the proposition

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2},$$

which is the proposition for $n+1$. We get

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\
&\overset{\text{assumption}}{=} \frac{n(n+1)}{2} + (n+1) \\
&= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&= \frac{n(n+1) + 2(n+1)}{2} \\
&= \frac{(n+1)(n+2)}{2}.
\end{aligned}$$

□

*To see that both steps (beginning and induction) are essentiall for the proof to be valid, consider the following:*

**Example 3.4.2.** Consider the proposition: $1+n > 2+n$ for all $n \in \mathbb{N}$.
This is obviously wrong, but still it is easy to do the induction step:
Assume that the proposition is true for $n$. So

$$\begin{aligned} & n+1 > n+2 \\ \Longleftrightarrow\ & n+1+1 > n+2+1 \\ \Longleftrightarrow\ & (n+1)+1 > (n+1)+2. \end{aligned}$$

But we cannot do the induction beginning because there is no smallest natural number satisfying $n+1 > n+2$.

### A fake induction proof

*Some proofs look good at the first glance, but sometimes a subtle error is inside. Look at this "proof":*

***Theorem:** All sheep have the same colour.*

*Proof.* We proof inductively that any set of sheep consists of only sheep of a single colour, *i.e.*, is equicolored.
Induction start: A set containing one sheep is obviously equicolored.
Induction step: Assume that any set of $n$ sheep is equicolored. Now consider a set of $n+1$ sheep. The set formed by the first $n$ sheep is equicolored. But so is the set formed by the last $n$ sheep. Hence the whole set must be equicolored. □

*What is wrong here?*

## 3.5 Proof strategies

*In mathematics, you often state the existence of a certain object. For example:*

**Theorem 3.5.1.** *Any two natural numbers $a$ and $b$ have a* greatest common divisor *[größter gemeinsamer Teiler].*

*We will first consider two different proofs of Theorem 3.5.1.*

### Existence proof

*Like the name promises, an* existence proof *[Existenzbeweis] proves the existence of something. Let's look at Theorem 3.5.1:*

*Proof.* A divisor of a natural number has to be less or equal to the number. Since there are only finitely many natural numbers which are less than or equal to $a$ and $b$, respectively, only finitely many divisors can exist.

Take 1: it is a natural number and divides both $a$ and $b$. So 1 is a common divisor. Since there are only finitely many other divisors, a greatest common divisor exists. □

*At the end of the proof, we know that the theorem holds but we cannot say what the greatest common divisor is.*

## Constructive proof

*A constructive proof [konstruktiver Beweis] is a proof which also delivers a solution. Again we look at Theorem 3.5.1:*

*Proof.* For each prime number $p$ denote by $e_a(p), e_b(p)$ its exponent in the (unique!) prime factor decompositions of $a$, respectively $b$. (Note that in either case only finitely many of the $e_a(p), e_b(p)$ are larger than zero.)

Then

$$d := \prod_{p \text{ prime}} p^{\min(e_a(p), e_b(p))}$$

is the greatest common divisor of $a$ and $b$. □

## Uniqueness proof

*Once we know about the existence of a solution, we might be interested in its uniqueness. Then we have to maintain a uniqueness proof [Eindeutigkeitsbeweis].*

*Consider the following theorem, which is stronger than Theorem 3.5.1.*

**Theorem 3.5.2.** *Any two natural numbers $a$ and $b$ have a* unique *greatest common divisor.*

*Proof.* Assume that there are two different greatest common divisors $c$ and $d$ of $a$ and $b$. Since $c$ and $d$ are common divisors and $c$ is the greatest common divisor, this leads to $c \geq d$. The same is true for $d$ leading to $d \geq c$ and so $c = d$. □

# 3.6 The pigeon hole principle

*The following – surprisingly simple – theorem can very often be applied in proofs:*

**Theorem 3.6.1** (The *pigeon hole principle [Schubfachprinzip]*)**.** *Assume we are given $n+1$ balls and $n$ boxes and are asked to distribute the balls among the boxes. Then there exists one box which contains more than one ball.*

*There is nothing to prove.*

*Now let us apply the pigeon hole principle to prove the following:*

**Proposition 3.6.2.** *Let $n \in \mathbb{N}$ with $2 \not| n$, $5 \not| n$. Then there is a number $N \in \mathbb{N}$ whose decimal representation is $N = 111\ldots111$ such that $n|N$.*

*Proof.* Denote by $N_1, N_2, \ldots, N_{n+1}$ the first $n+1$ numbers of the form $111\ldots111$, *i.e.*,

$$N_i = \underbrace{111\ldots111}_{i \text{ ones}}.$$

Moreover, denote by $R_i$ the remainder of $N_i$ on division by $n$. Then $0 \leq R_i \leq n-1$. Thus, there are only $n$ different possible values for $R_i$ and by the pigeon hole principle (Theorem 3.6.1) there are $i \neq j$ such that $R_i = R_j$. Without loss of generality assume that $i > j$. Then $n|(N_i - N_j)$ and

$$N_i - N_j = \underbrace{111\ldots111}_{i-j \text{ many}}\underbrace{000\ldots000}_{j \text{ many}} = \underbrace{111\ldots111}_{i-j \text{ many}} \cdot 10^j = N_{i-j} \cdot 10^j.$$

Since $n$ is relatively prime to $10^j$, we must have $n|N_{i-j}$. □