Lecture 2

Proof techniques

Basic schemes of proof

In this lecture we will discuss basic proof techniques:

- Direct proof
- Proof by contraposition
- Proof by contradiction
- Proof by exhaustion (proof by cases)

Direct proof (to prove $P \implies Q$)

Idea: If P is true and $P \implies Q$, then Q is also true.

Logical justification: $(P \wedge (P \implies Q)) \implies Q$ is a tautology.

This rule of logical deduction is called **modus ponens**.

It allows to eliminate a conditional statement from a proof.

Method: Assume (let) P. Then ... Then ... Therefore, Q.

Example 1. Prove that if an integer n is odd, then n^2 is odd.

Proof. We have to prove that $\forall\, n \in \mathbb{Z}\, (n \text{ is odd} \implies n^2 \text{ is odd})$ $\forall\, n \in \mathbb{Z}\, (\underbrace{n \text{ is odd}}_{P} \implies \underbrace{n^2 \text{ is odd}}_{Q})$

(given) (to prove)

Let n be odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. Therefore,

$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd, as required.

qed

(quod erat demonstrandum)

Modern replacement: $\square$

Arithmetic mean and geometric mean

Example 2. Show that $\dfrac{a+b}{2} \ge \sqrt{ab}$ for any non-negative real numbers a, b.

Remark. $\dfrac{a+b}{2}$ is called the **arithmetic mean** (AM) of numbers a, b.

$\sqrt{ab}$ is called the **geometric mean** (GM) of numbers a, b.

Discussion. We have to prove that $\forall\, a, b \in \mathbb{R}\ (a, b \ge 0 \implies \dfrac{a+b}{2} \ge \sqrt{ab})$.

It's difficult to get $\dfrac{a+b}{2} \ge \sqrt{ab}$ directly from $a, b \ge 0$, though.

Let us work "backwards":

$$\frac{a+b}{2} \ge \sqrt{ab} \implies a+b \ge 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\ge 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \ge 0 \implies (\sqrt{a}-\sqrt{b})^2 \ge 0.$$

Is this a proof? NO ! Can we reverse the implications? Yes!

AM-GM inequality

Recall backwards arguments:

$$\frac{a+b}{2} \ge \sqrt{ab} \implies a+b \ge 2\sqrt{ab} \underset{\substack{\uparrow \\ a,b\ge 0}}{\implies} (\sqrt{a})^2 + (\sqrt{b})^2 - 2\sqrt{a}\sqrt{b} \ge 0 \implies (\sqrt{a}-\sqrt{b})^2 \ge 0.$$

Theorem. *The arithmetic mean of two non-negative numbers is greater than or equal to their geometric mean.*

Proof. Take any non-negative real numbers a and b. Then

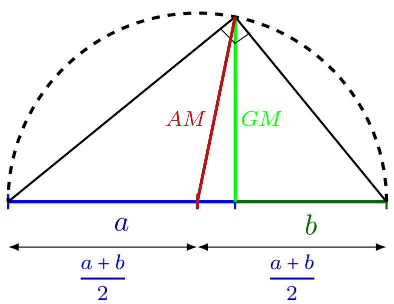
$$(\sqrt{a}-\sqrt{b})^2 \ge 0 \implies a - 2\sqrt{a}\sqrt{b} + b \ge 0 \implies a+b \ge 2\sqrt{ab} \implies \frac{a+b}{2} \ge \sqrt{ab},$$

as required. □

Corollary. $AM(a,b) = GM(a,b)$ iff $a = b$.

Proof. Let $a, b \ge 0$. Then $a = b \iff (\sqrt{a}-\sqrt{b})^2 = 0 \iff a - 2\sqrt{a}\sqrt{b} + b = 0$
$\iff \dfrac{a+b}{2} = \sqrt{ab} \iff AM(a,b) = GM(a,b)$, as required. □

Geometric interpretation of AM-GM inequality



$$AM = \frac{a+b}{2}$$

$$GM = \sqrt{ab}$$

$$AM \geq GM$$

$$AM = GM \iff a = b$$

Differentiability implies continuity

Example 3. Prove that if a function is differentiable at a point, then it is continuous at this point.

Discussion. Given: function f,
point a in its domain,
differentiability of f at a. What does it mean exactly?

Definition. A function f is **differentiable** at point a if there exists $f'(a)$,
that is, there exists the limit $\lim\limits_{h\to 0} \frac{f(a+h)-f(a)}{h}$.

Have to prove: f is continuous at a. What does it mean exactly?

Definition. A function f is **continuous** at point a if $\lim\limits_{x\to a} f(x) = f(a)$.

What does the phrase $\lim\limits_{x\to a} f(x) = f(a)$ say exactly?

1. $\exists \lim\limits_{x\to a} f(x)$

2. $f(x)$ is defined at $x = a$

3. $\lim\limits_{x\to a} f(x) = f(a)$.

Differentiability implies continuity

We have to prove the implication

$$\exists \lim_{h\to 0}\frac{f(a+h)-f(a)}{h} \implies \lim_{x\to a} f(x) = f(a) \quad \underbrace{\exists \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}}_{\text{given}} \implies \underbrace{\lim_{x\to a} f(x) = f(a)}_{\text{to prove}}$$

Let us prove that $\lim_{x\to a} f(x) - f(a) = 0$:

$$\lim_{x\to a} f(x) - f(a) = \lim_{x\to a} f(x) - \underbrace{f(a)}_{\text{constant}} = \lim_{x\to a}(f(x)-f(a)) \underbrace{=}_{\substack{x\neq a \\ \text{by def. of lim}}} \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right)$$

$$\underbrace{=}_{\text{let } h=x-a} \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) \underbrace{=}_{\substack{\text{since both} \\ \text{lims exist}}} \lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot\lim_{h\to 0} h$$

$= f'(a)\cdot 0 = 0$, as required.

Differentiability implies continuity

Let us clear our work off unnecessary "educational" bells and whistles:

Theorem. *Let f be a function defined in a neighborhood of a point a.*

If f is differentiable at a, then f is continuous at a.

Proof. $\lim_{x\to a} f(x) - f(a) = \lim_{x\to a}(f(x)-f(a)) = \lim_{x\to a}\left(\frac{f(x)-f(a)}{x-a}\cdot(x-a)\right) = \lim_{h\to 0}\left(\frac{f(a+h)-f(a)}{h}\cdot h\right) =$
$\lim_{h\to 0}\frac{f(a+h)-f(a)}{h}\cdot\lim_{h\to 0} h = f'(a)\cdot 0 = 0$.

Therefore, $\lim_{x\to a} f(x) = f(a)$, and, by this, f is continuous at a, as required.

Proof by contraposition

Idea: To prove $P \implies Q$, we prove $\neg Q \implies \neg P$.

Logical justification: $P \implies Q$ is equivalent to $\neg Q \implies \neg P$.

This rule of logical deduction $((P \implies Q) \wedge \neg Q) \implies \neg P$ is called **modus tollens**.
Method: Assume (let) $\neg Q$. Then ... Then ... Therefore, $\neg P$.

So $\neg Q \implies \neg P$. By contraposition, $P \implies Q$.

Example 1. Let n be an integer. Prove that if n^2 is odd then n is odd.

Discussion. We have to prove that

$$\forall n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

Why not to prove like this: n^2 is odd $\implies$ $\sqrt{n^2} = n$ is odd?

What to choose: direct proof or proof by contraposition?

For a **direct** proof of

$$\forall n \in \mathbb{Z} \quad \underbrace{\boxed{n^2 \text{ is odd}}}_{P} \implies \underbrace{\boxed{n \text{ is odd}}}_{Q}$$

we have to start with P. But Q seems to be simpler than P.

This suggests a proof by **contraposition**:

Let $\neg Q$, that is, let n be even, that is, $n = 2k$ for some integer k.

Then $n^2 = 4k^2$, which is even ($\neg P$).

Therefore, $\neg Q \implies \neg P$, or, equivalently, $P \implies Q$.
Cast off crutches:

Proposition. *For any integer n, if n^2 is odd then n is odd.*

Proof. Let n be even. Then $n = 2k$ for some integer k. So $n^2 = 4k^2$, which is even. Therefore, by contraposition, if n^2 is odd then n is odd, as required. □

Parity

Let us collect our results about the parity.

Theorem. *Any integer has the same parity as its square.*

Proof. We have to prove that n and n^2 have the same parity, that is, both are even or both are odd. For this, it's enough to prove that

n is even $\iff$ n^2 is even.

Indeed, if n is even, then $n = 2k$ for some $k \in \mathbb{Z}$. In this case, $n^2 = 4k^2$, which is even. So if n is even, then n^2 is also even.

To prove the converse (if n^2 is even, then n is even), we use contaposition.

Let n be odd, that is $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then $n^2 = 4k^2 + 4k + 1$, which is odd. By contraposition, if n^2 is even, then n is even.

qed

13 / 26

Divisibility

Example 2. Prove that if $n^2 - 1$ is not divisible by 8, then n is even.

Proof. Have to prove: $8 \nmid (n^2 - 1) \implies 2 | n$ $\underbrace{8 \nmid (n^2 - 1)}_{P} \implies \underbrace{2 | n}_{Q}$

Which one is simpler, P or Q? Q is simpler, so we'll do contraposition:

Assume that $2 \nmid n$ $(\neg Q)$. Then $n = 2k + 1$ for some integer k.

Calculate $n^2 - 1$:

$n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4\ k(k + 1) = 4\ \underbrace{k(k + 1)}_{\text{divisible by } 2}$ is divisible by 8 $(\neg P)$.

We have proved that $2 \nmid n \implies 8 | (n^2 - 1)$.

By contraposition, $8 \nmid (n^2 - 1) \implies 2 | n$, as required.

14 / 26

Non-zero integral

Example 3. Let f be integrable on $[0,1]$. Prove that

$$\text{if } \int_0^1 f(x)\,dx \neq 0, \text{ then } f(x) \neq 0 \text{ for some } x \in [0,1].$$

Proof. Have to prove:

$$\int_0^1 f(x)\,dx \neq 0 \implies \exists\, x \in [0,1]\;\; f(x) \neq 0.$$

Assume that $f(x) = 0$ for **all** $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$.

Therefore, by contraposition,

if $\int_0^1 f(x)\,dx \neq 0$, then $f(x) \neq 0$ for some $x \in [0,1]$, as required.

Proof by contradiction (indirect proof)

Idea: To prove P, we assume $\neg P$ and get two mutually exclusive statements, Q and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... Q. Then ... $\neg Q$. Therefore, P.

Example 1. Prove that $\sqrt{2}$ is irrational.

Proof. The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\underbrace{\boxed{\sqrt{2} \text{ is rational}}}_{\neg P}$.

Then $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z},\; q \neq 0$.

$\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underset{Q}{\gcd(p,q) = 1}$ .that $\boxed{\gcd(p,q) = 1}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that p^2 is even. Since p has the same parity as p^2

(see Theorem about the same parity of an integer and its square),

we conclude that p should be even, that is, $p = 2k$ for some integer k.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, q^2 is even, and, therefore, q is even too: $2 | q$.

But p is also even, that is $2 | p$. We have got that $2 | p$ and $2 | q$.

Therefore, $\underset{\neg Q}{\gcd(p,q) \neq 1}$ Therefore $\boxed{\gcd(p,q) \neq 1}$, which contradicts to the fact that $\gcd(p,q) = 1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous,
and $\sqrt{2}$ is actually irrational, as required.

Euclid's theorem

Theorem (Euclid). *There are infinitely many prime numbers.*

Proof. Assume, to the contrary, that there are only finitely many prime numbers:

$p_1, p_2, \ldots, p_n$.

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

N is not divisible by any of p_1, p_2, $\ldots$, p_n.

Indeed, N has a remainder of 1 when divided by any of them.

As any natural number greater than 1, N is divisible by some prime number.

By this, N should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.
This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

and there are infinitely many primes, as required.

For source and comments see
Euclid's Elements, Book IX, Proposition 20.
http://aleph0.clarku.edu/ djoyce/java/elements/bookIX/propIX20.html

Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

Inscribed Angle Theorem. *An angle inscribed in a circle is half of the central angle subtending the same arc.*

Proof. How an inscribed angle may be positioned with respect to the center of the circle?

Listen to the proof and try to write it down...

The triangle inequality

Theorem (triangle inequality). $|a+b| \le |a|+|b|$ *for any real numbers* a, b.

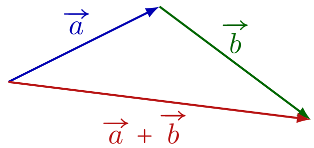
Proof (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \le |a|+|b|$.
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \le |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \le a-b = |a|+|b|$, so $|a+b| \le |a|+|b|$.
- Case 3. $a < 0$ and $b \ge 0$ is similar to Case 2, just swap a and b.
- Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a|+|b|$, and, by this $|a+b| \le |a|+|b|$.

Therefore, $|a+b| \le |a|+|b|$ for all real numbers a and b, as required.

The triangle inequality

Why the inequality $|a+b| \le |a|+|b|$ is called the triangle inequality?



$|\vec{a}+\vec{b}| < |\vec{a}|+|\vec{b}|$

Corollary 1. $|a-b| \le |a|+|b|$ for all $a, b \in \mathbb{R}$.

Proof. Apply the triangle inequality to a and $-b$:
$|a+(-b)| \le |a|+|-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \le |a|+|b|$, as required.

Corollary 2. $||a|-|b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

Proof. $|a| = |(a-b)+b| \le |a-b|+|b| \implies |a|-|b| \le |a-b|$.
$|b| = |(b-a)+a| \le |b-a|+|a| \implies |a|-|b| \ge -|a-b|$.
Therefore, $-|a-b| \le |a|-|b| \le |a-b|$. Hence $||a|-|b|| \le |a-b|$, as required.

The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers a and b, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\le}_{ab\le|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \le (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \le \sqrt{(|a|+|b|)^2}$, which implies
$|a+b| \le ||a|+|b||$.

Since $||a|+|b|| = |a|+|b|$, we get $|a+b| \le |a|+|b|$.

How to prove an equivalence

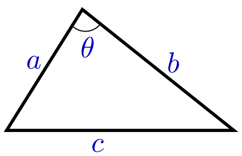
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

Example 1. Let a, b, c be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

Proof. What is the law of cosines?



$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides a, b, c is right $\underset{?}{\iff}$ $\theta = 90°$ $\underset{?}{\iff}$ $\cos\theta = 0$

$\underset{?}{\iff}$ $c^2 = a^2 + b^2$.

An integer and its cube have the same parity

Example 2. Let n be an integer. Prove that n is even iff n^3 is even.

Proof. Let us prove first that

n is even $\implies$ n^3 is even.

Let n be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

n^3 is even $\implies$ n is even.

Assume that n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd.
We have got that n is odd $\implies$ n^3 is odd. Therefore, by contraposition,

n^3 is even $\implies$ n is even.

qed

How to prove uniqueness

In order to prove that an object is unique, one assumes that there are two such objects and come to a conclusion that they have to be equal.

Example. Prove that in any ring, the additive identity is unique.

Proof. Assume that there are two additive identities, 0 and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element a in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any a in the ring.

Therefore, $0' = 0$.

qed

Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given) and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \dots$
  2. **Denying the antecedent**
     Prove $P \implies Q$.
     "Proof." Let $\neg P \dots$
  3. **Guilt by assumption** (proof by example)
     $\exists x\, P(x) \implies \forall x\, P(x)$