Writing Proofs

Quick Overview of Techniques and Essentials

Ana Cannas

15. October 2025

Mathematical Writing, ETH Zürich

Slides prepared with assistance from ChatGPT 5.

Plan for today

1. Foundations: analysis* and logic ** in the sense of "detailed examination of the elements or structure of something"*
2. Examples of elementary proofs

Based on:

Chapter 7 of the book by F. Vivaldi, *Mathematical Writing*

Part 1: Foundations: analysis and logic

What counts as a proof?

"A **proof** *is formalization of a logic deduction axioms/postulates* $\Longrightarrow$ *theorems."*

"A **proof** *is a series of statements, each of which* **follows** *from those before, starting with things we are assuming to be true, and ending with the thing we are trying to prove."*

How to write it?

- Organize with substatements:
  lemmas, propositions, claims, definitions, instructions.
- Use tags that clarify the flow:
  Assume, *Suppose*, *Then*, *Hence*, *Therefore*, *Q.E.D.*, □

Say what you plan to do; *when you've done it, say so.*

Hierarchy of Statements

Background assumptions

Axioms

General "truths" used across all of mathematics.

Ex: Axiom of Choice.

Postulates

Assumptions specific to a particular branch.

Ex: The Five Postulates of Euclidean Geometry.

Nowadays often used interchangeably.

Quick Lexicon

Term	Description
Theorem	A major, significant mathematical statement that has been proven to be true and is of independent interest.
Lemma	A subsidiary, “helping” statement proved on the way to a more significant theorem or proposition; its importance derives from the larger result it supports.
Proposition	A statement more substantial than a lemma, but typically less central than a theorem. Often used for results with somewhat more independent interest than a lemma.
Corollary	A statement whose proof is a simple and direct consequence of a theorem or proposition that has just been proved; it often follows immediately, sometimes as a special case.

A proof relies on logic

P	Q	$P \vee Q$
T	**T**	**T**
T	**F**	**T**
F	**T**	**T**
F	**F**	**F**

OR

P	Q	$P \wedge Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**F**
F	**F**	**F**

AND

IMPLICATION

P	Q	$P \Rightarrow Q$
T	**T**	**T**
T	**F**	**F**
F	**T**	**T**
F	**F**	**T**

Proof of a conjunction

Claim. P and Q.

or

Claim. (i) P. (ii) Q.

Proof.

(i) We prove P.

(ii) We prove Q.

$\square$

Conjunction in disguise:

Claim. $P \iff Q$.

Proof.

(i) We prove $P \Rightarrow Q$.

(ii) We prove $Q \Rightarrow P$.

$\square$

Direct proof

Claim. $P \Rightarrow Q$.

Often start with a *definition* or an *instruction*.

"Let $\omega \in \Omega$."

"Define $a := \dots$."

"Take the partial fraction decomposition of $\frac{f(x)}{g(x)}$."

☞ Establish good notation.

Good: *"Let p be a prime number greater than 3."*
Good: *"Let X be a compact set, and let C be a subset of X."*
Good: *"Let $x \in \mathbb{R}$."* **Bad**: *"Let $f \in \mathbb{R}$."*

Implications in disguise

Implication because of hidden universal quantifier:

Claim. The set A is a subset of B.

"If $x \in A$, then $x \in B$."

Claim. The determinant of an invertible matrix is non-zero.

"If M is an invertible matrix, then $\det(M) \neq 0$*."*

Contrapositive

- To prove $\boxed{P \Rightarrow Q,}$ it may be easier to prove the equivalent implication $\boxed{\neg Q \Rightarrow \neg P}$, called **contrapositive**.

  $\neg$ represents the operator NOT.

- Choose the easiest route.

Example:

Claim. For any $n \in \mathbb{N}$, if $2^n < n!$, then $n > 3$.

vs.

Claim. For any $n \in \mathbb{N}$, if $n \leq 3$, then $2^n \geq n!$.

Now only need to check the three cases $n = 1$, $n = 2$ and $n = 3$.

Loops of implications

Equivalence $\boxed{P \iff Q}$ may be seen as **loop** $\boxed{P \Rightarrow Q \Rightarrow P.}$

More generally, for n statements $P_1, \ldots, P_n$, the **loop**

$$\boxed{P_1 \Rightarrow P_2 \Rightarrow \cdots \Rightarrow P_n \Rightarrow P_1}$$

establishes

$$\boxed{P_i \iff P_j \text{ for all } i, j = 1, \ldots, n.}$$

Common pitfalls

- Confusing **examples** with **proofs**.
- Circular arguments. *Assuming what we are trying to prove.*
- Proving the converse instead.
- Mishandling functions. *Being outside domain, assuming invertibility.*
- Missing special cases. *Forgetting case of zero, empty set, etc.*
- Redundant assumptions.
- Confusing notation. *BAD: Let X be a set. Call it Y.*

☞ Besides being **correct**, proofs should be **economical**, and **explicit** about plan and closure.

Part 2: Examples of elementary proofs

Proof by cases

- Partition the universe into disjoint cases.
- Prove the claim in each case.

☞ Common when functions/definitions are piecewise.

Example: Absolute value function $|x| = \begin{cases} x & \textit{when } x \geq 0 \\ -x & \textit{when } x < 0 \end{cases}$

☞ Also for different residue classes, types of roots, etc!

Examples: n odd vs. n even; real roots vs. complex roots

Example: inequality solution via cases

Claim. The solution set of $2|x| \leq |x-1|$ is $\left[-1, \frac{1}{3}\right]$.

⚠ *Functions defined by branches*

$$|x| = \begin{cases} x & \text{when } x \geq 0 \\ -x & \text{when } x < 0 \end{cases} \qquad |x-1| = \begin{cases} x-1 & \text{when } x \geq 1 \\ 1-x & \text{when } x < 1 \end{cases}$$

$\Longrightarrow$ *Split into three cases:* $\quad x < 0, \quad 0 \leq x < 1, \quad x \geq 1$

Example: inequality solution via cases, cont.

Claim. The solution set of $2|x| \le |x-1|$ is $[-1, \frac{1}{3}]$.

Announce that you will split into cases;

be careful with strict vs. nonstrict inequalities.

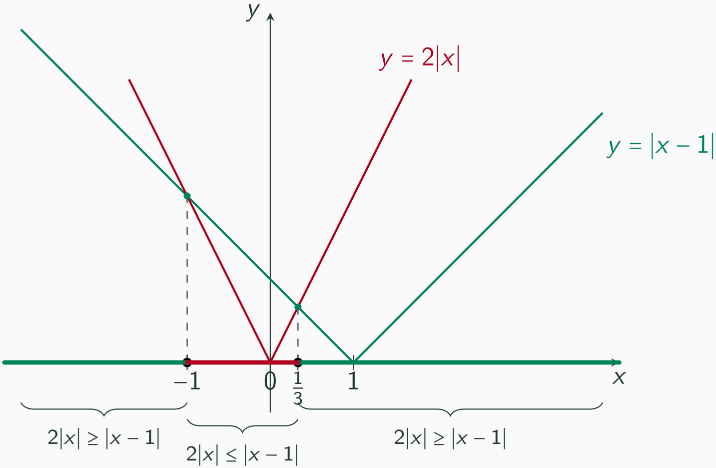
Proof (sketch). Let $x \in \mathbb{R}$. There are three cases:

1. When $x < 0$: inequality becomes $-2x \le 1 - x \;\Rightarrow\; x \ge -1$.
2. When $0 \le x < 1$: inequality becomes $2x \le 1 - x \;\Rightarrow\; x \le \frac{1}{3}$.
3. When $x \ge 1$: inequality becomes $2x \le x - 1 \;\Rightarrow\; x \le -1$, but this is impossible for $x \ge 1$.

Thus we get the solution set $[-1, 0) \cup [0, \frac{1}{3}] \cup \varnothing = [-1, \frac{1}{3}]$. $\square$

Graphic visualization – not a proof!

Claim. The solution set of $2|x| \leq |x-1|$ is $[-1, \frac{1}{3}]$.



Example: divisibility via cases

Claim. For all $n \in \mathbb{Z}$, the integer $n^5 - n$ is divisible by 30.

Proof (outline).

$$30 = 2 \cdot 3 \cdot 5, \qquad n^5 - n = n(n-1)(n+1)(n^2+1).$$

Show divisibility of $n^5 - n$ by 2, 3 and 5 via residue classes:

- mod 2: among n and $n+1$ one is even.
- mod 3: among $n-1$, n and $n+1$ one is divisible by 3.
- mod 5: if $n \equiv 0, \pm 1$, then $5 \mid n(n-1)(n+1)$; if $n \equiv \pm 2$, write $n = 5k \pm 2$, then $n^2 + 1 = 25k^2 \pm 10k + 5 = 5(5k^2 \pm 2k + 1)$.

Hence, 30 divides $n^5 - n$. □

Proof by contradiction

Claim. Statement P.

- Assume its **negation** $\boxed{\neg P}$ and deduce a false statement.
- Conclude P.

For an implication statement $\boxed{P \Rightarrow Q}$, assume $\boxed{P \land \neg Q}$ (called *"both ends"*) and derive a contradiction.

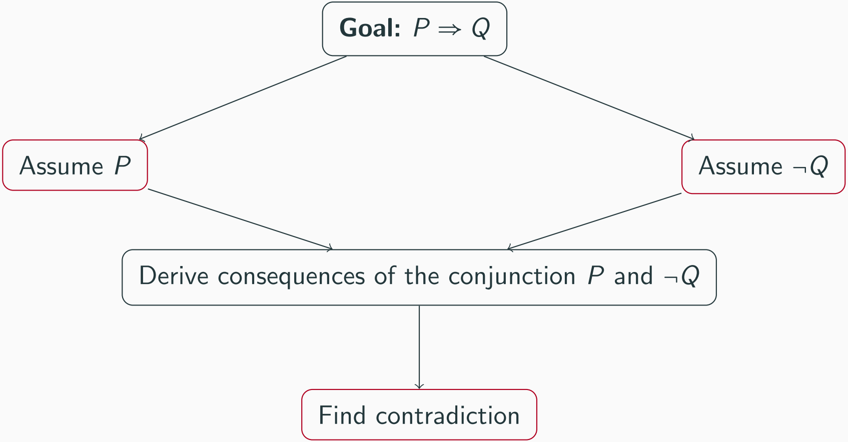
LaTeX symbols for contradiction (*use with caution!*):

$\Rightarrow\!\Leftarrow$ `$\Rightarrow\!\Leftarrow$`

$\rightarrow\!\leftarrow$ `$\rightarrow\!\leftarrow$`

$\bot$ `$\bot$` ↯ `$\mbox{\Lightning}$`

Flow of a proof by contradiction proof (both-ends method)



Conclude $P \Rightarrow Q$

State clearly where the contradiction lies (parity, order, size, etc.).

Example: irrationality of $\sqrt{2}$ by contradiction

Claim. The number $\sqrt{2}$ is irrational.

Proof (skeleton). Assume $\sqrt{2} = \frac{m}{n}$ with $m, n \in \mathbb{N}$ co-prime. Then take the square

$$2 = \frac{m^2}{n^2} \quad \Rightarrow \quad m^2 = 2n^2 \text{ is even}$$

$$\Rightarrow^* \quad m = 2h \text{ is even} \;\Rightarrow\; n^2 = 2h^2 \;\Rightarrow\; n \text{ is also even.}$$

** if a prime divides a product of two integers, then it divides one of the factors.*

This contradicts co-primality between m and n.
Hence, $\sqrt{2}$ is not a rational number. □

Example: Euclid's theorem by contradiction

Claim. The number of primes is infinite.

Proof (skeleton). Assume finitely many primes $p_1, \ldots, p_n$. Consider the integer

$$N = 1 + \prod_{k=1}^{n} p_k.$$

Then N is greater than all the primes and is not divisible by any of the p_k. This contradicts the fact that any integer greater than 1 must have a prime factor. $\square$

Homework due today: Paper 2

Check **guidelines for Paper 2 on course webpage**.

Your paper submission is to take place over Moodle at

`https://moodle-app2.let.ethz.ch/course/view.php?id=25875`

Although the Moodle form includes an *Overall feedback* entry box, please ignore that and *send only the PDF report*, by uploading it at the bottom of the form.

The deadline is Wednesday, 15.10.2025, at 22:00 CET.

- Did you go over the checklist?
- Did you name the file as requested?

Assistance available in the second hour.

Homework for 22/Oct

Paper 3 = Your revised version of your Paper 1
Check guidelines for Paper 3 on course webpage.

- Tomorrow (16/Oct) find on Moodle (at least) one report on your Paper 1.
- Revise your original Paper 1 based on that (those) report(s) and your own updates.
- Respond to the report(s) in up to one page in LaTeX.
- Upload **four files** by 22/Oct 22:00 – see guidelines.
- ⚠ This will use a different system in Moodle.

Guidelines for Paper 4 (due 6/Nov) are on the webpage.