Lecture 1B: Proofs

UC Berkeley EECS 70
Summer 2022
Tarang Srivastava

Announcements!

- Join Piazza. Read the Welcome Post
- Lecture is posted under "Media Gallery" in bCourses
- Evelyn's 6-7 pm discussion is now hybrid
- Signup and attend discussion
- **HW 1** and **Vitamin 1** have been released, due Thu (grace period Friday)

What is a proof?

A **proof** is a finite list of statements, each of which is logically implied by the previous statement, to establish the truth of some proposition.

The power here is that using *finite* statements, we can <u>guarantee</u> the truth of a statement with *infinitely* many cases.

<u>Advice</u>: When writing proofs, imagine a very skeptical friend is reading over your proof who questions every statement you make.

Since you're learning, try to be more formal in your proof writing

How to prove things?

Structure	How to generally prove it

You can also replace the proposition to be proved with something logically equivalent that has a different structure. Example:

Direct Proof (Example 1)

Theorem: For every natural number there is a natural number greater than it

Proof:

$$\forall n \in \mathbb{N}, \exists m \in \mathbb{N}(m > n)$$

Direct Proof (Example 2)

Definition: For $a, b \in \mathbb{Z}$ we say $a|b$ iff $\exists q \in Z$ such that $b = aq$
Theorem: For any $a, b, c \in \mathbb{Z}$ if $a|b$ and $a|c$ then $a|(b-c)$
Proof:

Lesson:

Proof by Contraposition

Definition: $n \in \mathbb{Z}$ is even if $\exists k \in \mathbb{Z}$ such that $n = 2k$
Definition: $n \in \mathbb{Z}$ is odd if $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$
Theorem: For every $n \in \mathbb{Z}$ if n^2 is even, then so is n.
Proof:

Proof by Cases (Example 1)

Theorem: For all $n \in \mathbb{N}$, $3|(n^3 - n)$
Proof:

Proof by Cases (Example 2)

Definition: A real number r is **rational** if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{p}{q}$. Otherwise, r is **irrational**.

Theorem: There exist irrational x and y such that x^y is rational.

Proof:

Proof by Contradiction

A ***proof by contradiction*** proves a proposition "P" by first assuming "*not* P" is true. That is, the opposite of P is true.

Then, it follows logical steps to arrive at a contradiction by proving both some proposition "R" and "*not* R".

Why does this work?

Proof by Contradiction (Example 1)

Definition: A real number r is **rational** if there are $p, q \in \mathbb{Z}$ such that $q \neq 0$ and $r = \frac{p}{q}$. Otherwise, r is **irrational**.

Theorem: $\sqrt{2}$ is irrational

Proof:

Proof by Contradiction (Example 2)

Theorem: There's infinite prime numbers

Proof:

Proof

Theorem:

Proof:

Summary

Proof Technique	General Procedure
Direct Proof	
Proof by contraposition	
Proof by contradiction	
Proof by cases	

Few notes about what we did today

Write full proofs in your homework like we did today, but on discussion you can just write an outline/sketch of the proof.

No one gets the complete proof immediately, there's a lot of scratch work and thinking before you can write the proof.

Remember! Every step in your proof must be justified and follow from previous steps.

Usually how things go:

1. Think about problem
2. Do some scratch work
3. Come up with solution
4. Try to write a proof
5. Realize solution is wrong

FAQ

How do I get started?

Think about the definitions that may be relevant. Maybe a theorem or lemma that was in the notes.

I’m stuck?

Try doing a bit of scratch work to see if you missed some pattern. Read over what you currently have in the proof. Try proving an easier statement or an intermediary statement.

Is my proof correct?

Question every statement. Does it follow from a definition or previous statement?