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)

should be up around 4pm
Linked on website

What is a proof?

$P \Rightarrow K \Rightarrow S \Rightarrow T, \ldots \Rightarrow Q$

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 guarantee the truth of a statement with *infinitely* many cases.

Do it during lecture

Advice: 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
$P \wedge Q$	Prove P and Prove Q
$(P \Rightarrow Q)$	Assume P is true, then show the Q follow (also true)
P iff Q $P \Leftrightarrow Q$	Proving $P \Rightarrow Q$ and Proving $Q \Rightarrow P$
$(\exists x \in S)\ P(x)$	Provide some $x \in S$ and prove $P(x)$
$(\forall x \in S)\ P(x)$	Let x be <u>arbitrary</u> in S and prove $P(x)$

You can also replace the proposition to be proved with something logically equivalent that has a different structure.
Example: $P \Rightarrow Q$, $\neg P \vee Q$ $\neg Q \Rightarrow \neg P$
Contrapositive

Direct Proof (Example 1)

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

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

Let n be an arbitrary natural number.
Observe that $n+1$ is also a natural number.
Since, $n+1 > n$ we have found a natural number greater than n. Since, n was arbitrary the statement holds $\forall n \in \mathbb{N}$.

Goal: $P \Rightarrow Q$

Method: Assume P

⋮ step

Conclude Q

<u>things we assumed</u>

1) $n+1$ is natural

2) $n+1 > n$

Direct Proof (Example 2)

$a | b$ if no remainder

$P \Rightarrow Q$

divides

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:

Let $a, b, c \in \mathbb{Z}$ be arbitrary and assume $a|b$ and $a|c$. So, by definition $b = aq_1$ and $c = aq_2$ for some $q_1, q_2 \in \mathbb{Z}$. Then, $b - c = aq_1 - aq_2 = a(q_1 - q_2)$. Since $q_1 - q_2 \in \mathbb{Z}$ it follows by definition that $a | (b-c)$

Scratch work

$a | b$ $\quad a | c$

$b = aq_1 \quad c = aq_2$

$b - c = aq_1 - aq_2$

$= a\underbrace{(q_1 - q_2)}_{\in \mathbb{Z}}$

$\cancel{b - c} = aq_3$

$\therefore$

$a | (b-c)$

Lesson: Use your definitions!

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 $\underbrace{\text{is even}}_{P}$, then so is $\underbrace{n.\ \text{is ev}}_{Q}$
Proof:

Let n be an integer. We will proceed by contraposition and show that if n is odd then n^2 is odd. By definition, $n = 2k+1$ $\forall k \in \mathbb{Z}$
then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
Since, $2k^2 + 2k \in \mathbb{Z}$ by definition n^2 is odd. $\square$

Useful

$\forall x\ P(x) \Rightarrow \forall y\ P(y)$

$\neg(\forall y\ P(y)) \Rightarrow \neg(\forall x\ P(x))$

$\exists y\ \neg P(y) \Rightarrow \exists x\ \neg P(x)$

Lets try directly

$n^2 = 2k \qquad n = \sqrt{2k}$???

Contrapositive

Goal: $P \Rightarrow Q$
Method: prove $\neg Q \Rightarrow \neg P$

Contrapositive:
if n is odd, then n^2 is odd

$n = 2k+1$

$n^2 = 4k^2 + 4k + 1$

$n^2 = 2(\underbrace{2k^2 + 2k}_{\in \mathbb{Z}}) + 1$

Proof by Cases (Example 1)

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

Proof:

Goal: P

Method: $R_1 \vee \ldots \vee R_n$ true

Show $R_1 \Rightarrow P$

⋮

Show $R_n \Rightarrow P$

Let $n \in \mathbb{N}$

Case 1: $n = 3k$ $\quad k \in \mathbb{N}$

$n^3 - n = (n)(n-1)(n+1)$

$= 3\underbrace{k(3k-1)(3k+1)}_{\in \mathbb{N}}$

thus $3 | n^3 - n$

Case 2: $n = 3k-1$

$n^3 - n = (3k-1)(3k-1-1)(3k-\cancel{1+1})$

$\hookrightarrow 3 | n^3 - n$

Case 3: $n = 3k+1$

$n^3 - n = (3k+1)(3k+\cancel{1-1})(3k+1+1)$

$\hookrightarrow 3 | n^3 - n$

Scratch Work

$n^3 - n = 3q$

$n(n^2-1) = 3q$

$n(n-1)(n+1) = 3q$

$2^3 - 2 = 8 - 2 = 6$

$3^3 - 3 = 27 - 3 = 24$

$2(2-1)(2+1) = 6 = 3(2)$

$3(3-1)(3+1) = 24 = 3(8)$

$4(4-1)(4+1) = \ldots$

$5(5-1)(5+1) =$

$6(6-1)(6+1)$:

$7(7-1)(7+1)$

Proof by Cases (Example 2)

$r \in \mathbb{Q}$ iff $r = \frac{p}{q}$

~~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:

Case 1: $\sqrt{2}^{\sqrt{2}}$ is rational. Then, we are done, $x = y = \sqrt{2}$

Case 2: $\sqrt{2}^{\sqrt{2}}$ is irrational. Let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$

$x^y = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$

Since 2 is rational for $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$ we've found an example that satisfies the claim.

Assumed $\sqrt{2}$ is irrational

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?

Goal: P

Method: Assume $\neg P$

⋮

R is true

⋮

$\neg R$ is true

$$\neg P \Rightarrow R \land \neg R \equiv F$$

P	$\neg P$	F	$\neg P \Rightarrow F$
T	F	F	T
F	T	F	F

$$\neg P \Rightarrow F \equiv P$$

$$\Downarrow$$

$$T \Rightarrow P$$

T	P	$T \Rightarrow P$
T	T	T

always true

what must go here.

this from proof

Proof by Contradiction (Example 1)

$\frac{1}{2}$

$\frac{p}{q} = \sqrt{2}$

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: $\sqrt{2}$ is irrational

Proof:

p,q share no common factors

Assume for contradiction that $\sqrt{2}$ is rational. Then, by definition $\sqrt{2} = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$. $2 = \frac{p^2}{q^2} \Rightarrow p^2 = 2q^2$. So, by def. p^2 is even. From an earlier thm, if p^2 is even, then p is even. So, $p = 2k$ for some $k \in \mathbb{Z}$ $(2k)^2 = 4k^2 = 2q^2 \Rightarrow q^2 = 2k^2$. q^2 is then even, so q is even. This is a contradiction since p and q share a common factor of 2. Thus, $\sqrt{2}$ must be irrational.

$q = 2j$ $j \in \mathbb{Z}$

Proof by Contradiction (Example 2)

NOT COVERED DURING LECTURE

Theorem: There's infinite prime numbers

Proof:

Every non-prime number has a prime divisor (ask students)

Assume for contradiction there are finite prime numbers. That is $p_1, p_2, \dots, p_n$ are all the prime numbers. Let $q = p_1 \cdot p_2 \cdot \ldots \cdot p_n$

Consider $q+1$. Clearly $q+1 > p_n$, where p_n is the largest prime number. So $q+1$ is not prime, thus it has a prime divisor. That is, there exists some prime $x \mid q+1$. Since x is prime, $x \in \{p_1, \dots, p_n\}$ and $x \mid q$. By previous Lemma 1, if $x \mid q$ and $x \mid q+1$, then $x \mid (q+1-q)$. That is, $x \mid 1$ but only $1 \mid 1$ and $x \neq 1$. This is a contradiction, so there must be infinitely many prime numbers.

Incorrect Proof

Theorem: $1 = 2$

Proof: For $\underline{x = y}$ we have

$$x^2 - xy = x^2 - y^2$$

$$x\cancel{(x-y)} = \cancel{(x-y)}(x+y)$$

divide by zero since $x=0$

$$x = x+y$$

$$x = 2x$$

$$1 = 2$$

Summary

NOT COVERED DURING LECTURE

Proof Technique	General Procedure
Direct Proof	Goal : $P \Rightarrow Q$ Method: Assume P ⋮ steps Conclude Q
Proof by contraposition	Goal : $P \Rightarrow Q$ Method : prove $\neg Q \Rightarrow \neg P$
Proof by contradiction	Goal : P Method : Assume $\neg P$ ⋮ Prove R ⋮ Prove $\neg R$
Proof by cases	Goal : P Method : Show $R_1 \vee \ldots \vee R_n$ is true; Show $R_1 \Rightarrow P$ ⋮ Show $R_n \Rightarrow P$

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?