Lecture 7: Foundational Proof Techniques, Cont'd

http://book.imt-decal.org, Ch. 2.0, 2.1

Introduction to Mathematical Thinking

February 19th, 2018

Suraj Rampure

$q1 + q2 + \max(q3, q4)$

Announcements

- Quiz grades are out!
    - Raw score is out of 34 ~~3~~2, but it should really be out of 25
    - Q4B was graded incorrectly and was recently fixed, so your score may have changed within the last two hours.
    - Overall, the class did very well.
    - Solutions and a blank copy are linked on the website.
- Quiz 2 is in a week from Thursday!

Last Time: Types of Proofs

- Direct Proofs
- Proof by Contradiction
- Proof by Contraposition
- Proof by Cases
- Proof by Induction (Thursday)

Will learn best by doing examples!

Review: Proof by Contradiction

In a proof by contradiction, to show S is true, we begin by assuming $\neg S$, i.e. that S is false.

After a few steps, we will reach a contradiction, i.e. something that implies $\neg S$ is false. Since our initial assumption was that S was false, we know this cannot be the case (since S and $\neg S$ can never be equal), thus S must be true, proving our statement.

- S could be a single proposition, e.g. "13 is prime", or even an implication!
  e.g. x^2 is even $\Rightarrow x$ is even (how would we negate this?)
- Issue with proofs by contradiction: the goal isn't immediately clear. We don't know what the contradiction is going to be when we begin.
  - Could show that two things that are not equal are equal, i.e. $0 = 1$
- Often, we use contradictions to prove the non-existence of something

Review: Proof by Contraposition

Suppose we want to prove $P \Rightarrow Q$.

Remember, $P \Rightarrow Q$ is nothing but a proposition with a truth value. Our job is to show that $P \Rightarrow Q$ is true. Often we can do this directly, but sometimes it's easier to show the contrapositive $\neg Q \Rightarrow \neg P$ has a true value.

P	Q	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$
True	True	True	True
True	False	False	False
False	True	True	True
False	False	True	True

Example

Prove that if a, b and c are odd integers, then there are no ~~integer~~ rational solutions to $\underbrace{ax^2 + bx + c = 0}_{Q}$.

P (over "if a, b and c are odd integers")

negation of $P \Rightarrow Q$ is $P \wedge \neg Q$

Proof by Contradiction

Assume there exist rational solutions:

$ax^2 + bx + c = (Ax + B)(Cx + D) = 0$

$= ACx^2 + (AD + BC)x + BD$

$a = AC$

$b = AD + BC$

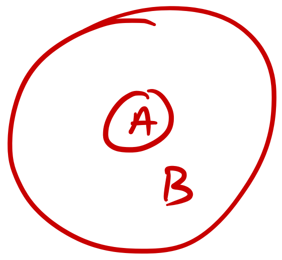
$c = BD$

1) consider $a = AC$
since a is odd, A and C are also odd

2) consider $c = BD$
since c is odd, B and D are also odd

$\rightarrow$ consider $b = \underbrace{AD}_{\text{odd}} + \underbrace{BC}_{\text{odd}} =$ even BUT we assumed b odd
$\rightarrow$ contradiction!

Example



Prove that if $A \subseteq B$, then for any set C, $A \cap C \subseteq B \cap C$.

Given : $x \in A \Rightarrow x \in B$

only assuming this

$A \cap C$

$\rightarrow$ $x \in A$ and $x \in C$

$x \in A \cap C$

This means $x \in A$ and $x \in C$

But if $x \in A$, then $x \in B$

$\therefore$ $x \in B$ and $x \in C$

$\therefore$ $x \in B \cap C$

$a \mid b \iff \exists c \in \mathbb{Z}: b = ac$

e.g. $8 \mid 24$ but $5 \nmid 24$

Proving If and Only If

When the statement we're proving is of the form "P if and only if Q", we essentially have to perform two separate proofs. We need to independently prove that $P \Rightarrow Q$, and $Q \Rightarrow P$. (For each of these separate proofs, we can use whatever method we want: direct, contradiction, contrapositive, etc.)

Example

Given $a, b, x, y \in \mathbb{N}$ such that $A = a + \frac{1}{x}$ and $B = b + \frac{1}{y}$, and $y|a$ and $x|b$, prove that $A \cdot B$ is an integer if and only if $x = y = 1$.

1) if $x = y = 1$, then $A \cdot B \in \mathbb{Z}$
2) if $A \cdot B \in \mathbb{Z}$, then $x = y = 1$

1) substitute $x = y = 1$

$$A \cdot B = \left(a + \frac{1}{x}\right)\left(b + \frac{1}{y}\right)$$
$$= (a+1)(b+1)$$
$$= ab + a + b + 1$$

$\rightarrow$ since $a, b \in \mathbb{Z}$,
$ab + a + b + 1 \in \mathbb{Z}$ ✓

2) RTP if $AB \in \mathbb{Z}$, then $x = y = 1$

Given:

$y \mid a$ and $x \mid b$

$$A \cdot B = \left(a + \frac{1}{x}\right)\left(b + \frac{1}{y}\right)$$

$$= ab + \frac{a}{y} + \frac{b}{x} + \frac{1}{xy}$$

int

int, since $y \mid a$

int, since $x \mid b$

Need to show $\frac{1}{xy} \in \mathbb{Z}$

this is only possible when

$xy = 1$

but $xy = 1 \Rightarrow x = 1$ and $y = 1$

$\therefore$ if $A \cdot B \in \mathbb{Z}$, then $x = y = 1$.

we showed both directions,

$\therefore$ statement holds.

Contradictions with Implications

Just because a statement is of the form "if P, then Q" doesn't mean we have to resort to a direct or contrapositive proof. We can also do a proof by contradiction!

Recall, the negation of $P \Rightarrow Q$ is $P \wedge \neg Q$.

Example

Prove that if $\underbrace{x^2 \text{ is even}}_{P}$, then $\underbrace{x \text{ is even}}_{Q}$.

$P \wedge \neg Q$: x^2 is even $\wedge$ x is odd

Proof by Cases

In many instances, we may find it easier to view a statement as the combination of many sub-cases. By proving each possible sub-case, we can prove the validity of the full statement.

When doing a proof by cases, we need to ensure that all possibilities are accounted for.

This works, because we split our proposition P into sub-propositions, e.g. P_1, P_2:

$$(P_1 \vee P_2) \Rightarrow Q \equiv (P_1 \Rightarrow Q) \wedge (P_2 \Rightarrow Q)$$

we can show this using a truth table

1) $x = 2k$

2) $x = 2k+1$

Example

Prove that the cube of any integer is either a multiple of 9, 1 more than a multiple of 9, or one less than a multiple of 9.

since we've accounted for all cases, we've shown the statement holds in general.

Question: What are the cases?

Every integer has remainder 0, 1, or 2 when divided by 3.

1) $x = 3k$
2) $x = 3k+1$
3) $x = 3k+2$

$k \in \mathbb{Z}$

Case 1 $\quad x = 3k, \ k \in \mathbb{Z}$

$$x^3 = (3k)^3 = 27k^3$$
$$= 9(3k^3)$$

$\therefore x$ is a multiple of 9

Case 2 $\quad x = 3k+1, \ k \in \mathbb{Z}$

$$x^3 = (3k+1)^3$$
$$= 27k^3 + 27k^2 + 9k + 1$$
$$= 9(3k^3 + 3k^2 + k) + 1$$

$\therefore x$ is 1 greater than a multiple of 9

Case 3 $\quad x = 3k+2, \ k \in \mathbb{Z}$

$$x^3 = (3k+2)^3$$
$$= 27k^3 + 18k + \ldots + 8$$
$$= 9\square + 8 = 9\square + 9 - 1$$
$$= 9(\square + 1) - 1$$

Example

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

Prove that $\left|\frac{a}{b}\right| = \frac{|a|}{|b|}, \forall a, b \in \mathbb{R}, b \neq 0.$

4 cases to consider!

1) $a \geq 0, b > 0$

$|a| = a, \quad |b| = b$

$\frac{a}{b} \geq 0$

$\Downarrow$

$\left|\frac{a}{b}\right| = \frac{a}{b} = \frac{|a|}{|b|}$ ✓

2) $a \geq 0, b < 0$

$\frac{a}{b} < 0 \Rightarrow \left|\frac{a}{b}\right| = -\frac{a}{b}$

$|a| = a \quad |b| = -b$

$\left|\frac{a}{b}\right| = -\frac{a}{b} = \frac{a}{-b} = \frac{|a|}{|b|}$

3) $a < 0, b > 0$

4) $a < 0, b < 0$

$|a| = -a, \quad |-b| = -b$

$\therefore$ the statement holds in general.

We've now covered the main styles of proof techniques, save for induction. We'll now look at the following oddities:

- Vacuous "Proofs"
- Counterexamples
- Faulty Proofs and Logic

Vacuous Proofs

$P \Rightarrow Q$ has a true value when both P is true and Q is true. But it also has a true value whenever P is false!

If the earth is flat, then all dogs can fly.

This is an implication that holds a true value. Since P is false, Q could be anything; $P \Rightarrow Q$ is true.

Example

$x \in \mathbb{R}$

Prove that if $(x-2)^2 - 4 < -6$, then 4 is prime.

$(x-2)^2 < -2$

$\square^2 \geq 0$

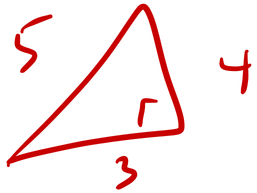
$\therefore P$ is false $\Rightarrow$ $P \Rightarrow Q$ is true.

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

Proof by... Counterexample?

NOT a proof technique! (more of a disproof technique)

We can't prove things to be true by using a counterexample. We can prove that things are not true, though:



Example

Prove or disprove: All Pythagorean triplets are of the form $(3k, 4k, 5k)$ for $k \in \mathbb{R}^+$.

- $8^2 + 15^2 = 17^2$, but $(8, 15, 17) \neq (3k, 4k, 5k)$ for any positive real k
- Counterexample! Disproof.

Faulty Proofs and Logic

We want you to be able to read a proof and point out flaws in it.

Watch out for some common mistakes:

- **Assuming the statement we are trying to prove to be true to begin with**
- Dividing by something which could be 0
- Not switching inequalities when working with negative numbers
- Using an example as a proof for a statement which applies to multiple cases
- Introducing a variable twice with two different values
- confusing contrapositive w/ converse

Example

Prove $1 = 2$.

Proof: Let $x = y$. Then:

$x, y \in \mathbb{R}$

$$x^2 = xy$$

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

$$(x+y)(x-y) = y(x-y)$$

$$x + y = y$$

can't divide by $x-y$, since $x-y=0$

$$2y = y$$

$$2 = 1$$

What is the flaw in logic with this proof?

Example

Prove that if n is an integer and $\underbrace{\overset{2(n+1)}{2n+2} \text{ is even}}_{P}$, then $\underbrace{n \text{ is odd}}_{Q}$.

Proof: Proceed by contraposition. Assume that $\boxed{n \text{ is odd.}}$ We will now prove that $2n+2$ is even. Clearly, $2n$ must be an even number, since it is divisible by 2. Furthermore, 2 is an even number, so $2n+2$ must be even. This concludes the proof.

What is the flaw in logic with this proof?

This proof tries to use the converse instead of the contrapositive

P : $2n+2$ is even

Q : n is odd

$\neg Q$: n is even

$\neg P$: $2n+2$ is odd

Example

Prove that 1 is the greatest whole number.

Proof: Let $n \in \mathbb{N}_0$ be the greatest ~~natural~~ whole number. Since it is the largest, its square n^2 must be less than or equal to it.

$$n^2 \leq n$$

Equivalently,

$$n(n-1) \leq 0$$

Which has two integer solutions, $n = 0$ and $n = 1$. Since $1 > 0$, we have that $\cancel{n}$ 1 is the greatest ~~natural~~ whole number.

What is the flaw in logic with this proof?

We assumed there exists a greatest whole number.

Prove there is no greatest even int.

Pf. by contradiction: Assume M is the greatest even int

$$N = M + 2$$

$N \in \mathbb{Z}$, N even

$\to$ contradiction!