# Lecture 3: Foundational Proof Techniques

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

## Introduction to Mathematical Thinking

### September 19th, 2018

Suraj Rampure

# Announcements

- Apply to CubStart, a program by Cal Hacks designed for beginner hackers
- Textbook section on propositional logic has many more examples now, thanks for the feedback!
- Working on a set theory/propositional logic cheat sheet

> **Definition: Proof**
>
> A mathematical proof is a **finite** sequence of valid steps which, when combined in a specific order, indicate the truth of a specific statement.

**Types of Proofs:**

- **Direct Proof**
- **Proof by Contradiction**
- **Proof by Contraposition**
- Vacuous Proofs
- Proof by Cases
- Counterexamples???
- Proof by Induction (next week)

Will learn best by doing examples!

# Direct Proof

In a direct proof, given certain information, we determine the validity of some other information. Direct proofs are often used in mathematical formulas, where simple arithmetic manipulations of given information can get us where we need to be.

As long as each step is valid, we have a valid proof!

## Example 1

$z = bx$ $\qquad$ $y+z = (a+b)x$

*Consider* $x, y, z \in \mathbb{Z}^+$ *. Prove that if* $x|y$ *and* $x|z$*, then* $x|(y+z)$.

"$x$ divides $y$" $\qquad$ $a, b \in \mathbb{Z}^+$

$y = ax$

$$y = ax$$
$$z = bx$$
$$+ \quad y + z = ax + bx = (a+b)x$$
$$\therefore \quad x \mid (y+z)$$

# Proof by Contradiction

assume $S$ is false

To show $S$ is true, we begin by assuming $\neg S$.
After a few steps, we will reach a contradiction, i.e. something that implies $S$ is false. Since our initial assumption was that $S$ was false, we know this cannot be the case, 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. $0 = 1$

## Example 2

*Prove that there is no greatest even integer.*

Assume there exists greatest even int $N$

$M = N + 2$

$\downarrow$

$M$ is even, AND larger than $N$

this contradicts $N$ being greatest even int

$\therefore$ there is no greatest even integer

## Example 3

*Prove that $\sqrt{2}$ is irrational.*

Assume $\sqrt{2} = \dfrac{a}{b}$ $\quad a, b \in \mathbb{Z}$, $\gcd(a,b) = 1$

$$2 = \frac{a^2}{b^2} \rightarrow a^2 = 2b^2$$

$\rightarrow a^2$ is even

$\rightarrow a$ is even

Let $a = 2k$, $k \in \mathbb{Z}^+$

$$a^2 = 2b^2$$

$$\rightarrow (2k)^2 = 2b^2$$

$$2\cancel{4}k^2 = \cancel{2}b^2$$

$$b^2 = 2k^2$$

$\rightarrow b^2$ is even

$\rightarrow b$ is even

$\gcd(a, b) \geq 2$

contradiction!

$\therefore \sqrt{2}$ is irrational!

## Attendance

http://tinyurl.com/KDthesnake

proposition!

# Proof by Contraposition

Usually used when our RTP statement is of the form "if $P$, then $Q$", i.e. $P \to Q$.

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

| $P$ | $Q$ | $P \to Q$ | $\neg Q \to \neg P$ |
|---|---|---|---|
| True | True | True | True |
| True | False | False | False |
| False | True | True | True |
| False | False | True | True |

## Example 4

$x^3$ is non-negative if and only if $x$ is non-negative

$A \longleftrightarrow B$

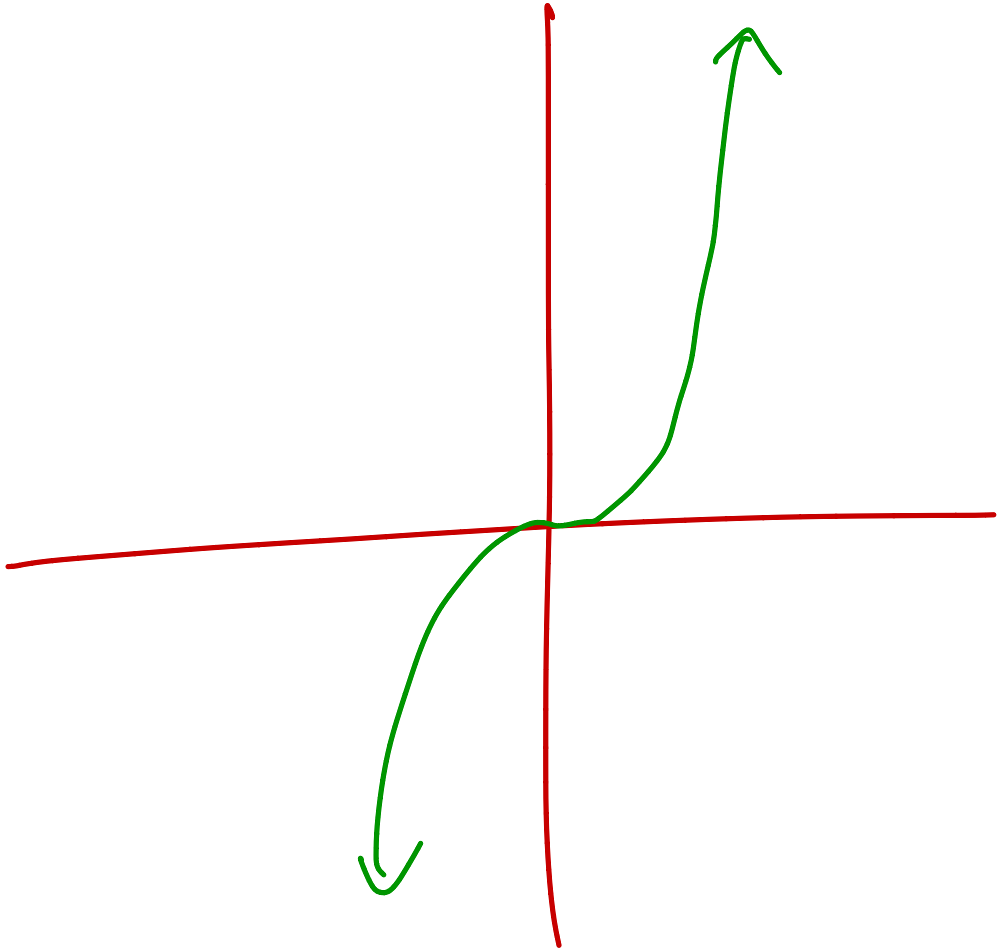
$P: x^3 \geq 0$

$Q: x \geq 0$

*Prove that if $x^3$ is non-negative, then $x$ is non-negative.*

$\neg Q : x < 0$

$\rightarrow x^3 < 0 : \neg P$



since $\neg Q \rightarrow \neg P$,

$P \rightarrow Q$

$\therefore$ if $x^3 \geq 0$, $x \geq 0$

$P \to Q \equiv \neg P \vee Q$

## Contradictions with Implications

Can also do the previous problem as a proof by contradiction!

How do we find the negation of this proposition?

*Prove that if $x^3$ is non-negative, then $x$ is non-negative.*

$(x^3 \geq 0) \to (x \geq 0)$

$\equiv \neg(x^3 \geq 0) \vee (x \geq 0)$

$\equiv (x^3 < 0) \vee (x \geq 0)$

$S$

$(A \cap B)^c = A^c \cup B^c$

$\neg S : \neg\left(\underbrace{(x^3 < 0) \vee (x \geq 0)}\right)$

$\equiv (x^3 \geq 0) \wedge (x < 0)$ i.e. $\boxed{P \wedge \neg Q}$

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

$\equiv \exists x\ \neg P(x)$

negation of original statement

never true : if $x < 0$, then $x^3 < 0$ : $P$ and $\neg Q$

CONTRADICTION! never true @ same time

# Vacuous Proofs

*won't spend too much time on these, more of an interesting idea

$P \to Q$ 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 P is false, Q could be anything

$P \to Q$ : true

*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; $P \to Q$ is true.

## Example 5

*Prove that if* $\overbrace{(x-2)^2 - 4 < -6}^{P}$*, then* $\overbrace{4 \text{ is prime}}^{Q}$*.*

$$(x-2)^2 - 4 < -6$$

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

we know $(x-2)^2 \geq 0$

$\therefore$ : therefore

$\therefore$ $P$ is false

$\therefore$ $P \to Q$ is true

# 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.

## Example 6

Three cases for $x$

*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.*

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

these cover all integers $x$

1) $x^3 = (3k)^3 = 27k^3 = 9(3k^3)$ ✓

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

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

$= 9\square + 1$ ✓

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

$= 9\square - 1$

binomial thm

# 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:

$(a, b, c) \rightarrow a^2 + b^2 = c^2$

### Example 7

*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

RTP $1 = 2$.

Assume $1 = 2$.

$0 \times 1 = 0 \times 2$

$0 = 0$

not a proof!!!

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

$\neg Q \to \neg P \equiv P \to Q$ $\qquad$ $Q \to P \not\equiv P \to Q$

# Example 8

*Prove* $1 = 2$.

Proof: Let $x = y$. Then:

$$x^2 = xy$$

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

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

$$x + y = y$$

$$2y = y$$

$$2 = 1$$

x-y is 0
can't
divide by it

have to rearrange
for y,
can't divide by
it

Where did we go wrong?

- Direct, Contradiction and Contraposition are the most commonly seen proof techniques of what we've covered
- This HW will give you much more practice in each of these, and also extend what we've covered here
- Next week: Mathematical Induction. Read 2.2 if interested (still a work in progress)