Lecture 6: Foundational Proof Techniques

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

Introduction to Mathematical Thinking

February 14th, 2018

Suraj Rampure

Announcements

- Homework 2 due tomorrow!
    - If you use CamScanner, use the feature that allows you to convert your image to black and white. It makes it easier for us to grade.
    - Please submit as a PDF. Sometimes with images things get wonky.
- Quiz solutions will be out tonight, and (hopefully) grades will be out before Tuesday.

Proofs

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

Less formally (but just as valid), a proof is an argument that convinces a reader that something is true.

Often times, we are given some information that we are allowed to assume. We will use this information to make a series of implications, that will eventually imply the condition we want to prove.

$$P \Rightarrow S_1 \Rightarrow S_2 \Rightarrow ... \Rightarrow Q$$

Types of Proofs

- Direct Proofs
- Proof by Contradiction
- Proof by Contraposition
- Proof by Cases
- Proof by Induction (next week)

Will learn best by doing examples!

Today: Direct proofs, contradiction, contraposition. Tuesday: a few more examples, and proof by cases. Next Thursday and Tuesday: induction.

Quick Primer: "divides" notation

$8 \mid 24$

$5 \nmid 24$

$a \mid b$, read "a divides b", states that there exists some $c \in \mathbb{Z}$ such that $b = ac$. This is another way of stating that b is an integer multiple of a.

Another key idea: We often use $2k$ (with $k \in \mathbb{Z}$) to represent an arbitrary even number, and $2k + 1$ to represent an arbitrary odd number. To show that some quantity is even or odd, we need to show that it can be written as $2 \cdot (\text{some integer})$ or $2 \cdot (\text{some integer} + 1)$.

We'll talk significantly more about divisibility in coming weeks, after we lay down the foundations of proof techniques. However, knowing this notation will allow us to look at significantly more examples, so we'll introduce it now.

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!

Often times, direct proofs read "if A, then B". We are allowed to assume that A is true, and using this information we need to show that B is true. Sometimes, we aren't explicitly given what A is, but we can infer properties that are universally known to be true.

Example

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

$y = cx$, $c \in \mathbb{Z}$

$z = dx$, $d \in \mathbb{Z}$

$\Updownarrow$

$y + z = (\text{some int})\, x$

$\therefore$ therefore

$\therefore$ because

$+$

$y + z = cx + dx$

$y + z = (c+d)x$

$\therefore$ since $c+d \in \mathbb{Z}$, $x \mid (y+z)$.

Example

Prove that for any $n \in \mathbb{N}, 3|(n^3 - n)$.

RTP $n^3 - n = 3k$, $k \in \mathbb{Z}$

required to prove

$$n^3 - n = n(n^2 - 1)$$
$$= n(n-1)(n+1)$$
$$= (n-1)(n)(n+1)$$
$$= 3k, \quad k \in \mathbb{Z}$$

$\therefore$, $3|(n^3 - n)$

Diff. of Squares

$x^2 - y^2 = (x-y)(x+y)$

consider any 3 consecutive ints.

one must be a multiple of 3

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

Example

Prove that there is no greatest even integer.

Proof by Contradiction

Assume N is the greatest even integer.

Since N is even, $N = 2k$, $k \in \mathbb{Z}$.

Consider $M = N + 2$

$= 2k + 2$

$= 2(k+1)$

$\rightarrow$ M is even AND greater than N.

Contradiction!

$\therefore$, there is no greatest even integer.

Example

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

Proof by Cont.

Assume $\sqrt{2}$ is rational.

$\rightarrow \sqrt{2} = \frac{a}{b}$, a, b in reduced form

$a, b \in \mathbb{Z}$

SBS ↓

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

↓

$2b^2 = a^2$

$\therefore a^2$ is even

$\rightarrow$ a is even

$\rightarrow$ we can say $a = 2k$, $k \in \mathbb{Z}$.

$a^2 = 2b^2$

substitute $a = 2k$

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

$4k^2 = 2b^2$

$2k^2 = b^2$

$\rightarrow b^2$ is even

$\rightarrow$ b is even

$\rightarrow$ we can say $b = 2c$, $c \in \mathbb{Z}$

CONTRADICTION!

we assumed $\gcd(a, b) = 1$

but showed they share a factor of 2. $\therefore \sqrt{2}$ is irrational

Example

Prove that in any set of n numbers, there is at least one number that is less than or equal to the mean.

Assume all are greater than mean

$S = \{x_1, x_2, \cdots x_n\}$

$x_1 > \dfrac{x_1 + x_2 + \cdots + x_n}{n}$

$x_2 > \dfrac{x_1 + x_2 + \cdots + x_n}{n}$

$\vdots$

$x_n > \dfrac{x_1 + \cdots + x_n}{n}$

$+$

$x_1 + x_2 + \cdots + x_n > x_1 + x_2 + \cdots + x_n$

contradiction!

Proof by Contraposition

$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$

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

$(x-1)(x-5)$

x^2-6x+5 odd $\Rightarrow$ x even

P $\quad$ Q

$\neg Q \Rightarrow \neg P$

Example

Prove that if $x^2 - 6x + 5$ is odd, then x is even, using (a) a direct proof and (b) a proof by contraposition.

b) RTP x odd $\Rightarrow$ x^2-6x+5 even

if x odd, $x = 2k+1$, $k \in \mathbb{Z}$

x^2-6x+5

$= (2k+1)^2 - 6(2k+1) + 5$

$= 4k^2+4k+1-12k-6+5$

$= 4k^2 - 8k = 2(2k^2-4k)$

some int

$\therefore$ if x is odd, x^2-6x+5 is even

$\therefore$ original statement holds by contraposition.