Proofs, analysis, and other such things

Matt Hoffman

September 15, 2009

- What's this refresher about?
  - how to prove *something*
  - but every problem's different. . . so we'll get to that
- What am I going to assume?
  - nothing really, other than a little bit of logic
  - we'll go over a few specific examples
- so first: going over general proofs (with boring examples)
- and then just stuff I find cool

What you should already know

- logical operators: $\neg A$, $A \vee B$, $A \wedge B$, $A \Rightarrow B$, etc.
- truth tables for these operators, i.e.

A	B	$A \Rightarrow B$
True	True	True
True	False	**False**
False	True	True
False	False	True

- logical equivalences, i.e. $A \Rightarrow B \equiv \neg A \vee B$

Direct proofs

- Many of things can be stated as an implication
  a. The sum of two rational numbers is rational.
     $a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$
  b. Every odd integer is the difference of two perfect squares.
     $i = 2j + 1$ for $j \in \mathbb{Z} \Rightarrow \exists a, b : \; i = a^2 - b^2$
- If we assume the LHS is true and show the RHS is, then the implication must be true.

Direct proofs

- Many of things can be stated as an implication
  a. The sum of two rational numbers is rational.
     $a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$
  b. Every odd integer is the difference of two perfect squares.
     $i = 2j + 1$ for $j \in \mathbb{Z} \Rightarrow \exists a, b : \; i = a^2 - b^2$

- If we assume the LHS is true and show the RHS is, then the implication must be true.

Proof of b.

Assume $i = 2j + 1$, we can write this as

□

Direct proofs

- Many of things can be stated as an implication
  a. The sum of two rational numbers is rational.
     $a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$
  b. Every odd integer is the difference of two perfect squares.
     $i = 2j + 1$ for $j \in \mathbb{Z} \Rightarrow \exists a, b:\ i = a^2 - b^2$
- If we assume the LHS is true and show the RHS is, then the implication must be true.

Proof of b.

Assume $i = 2j + 1$, we can write this as

$$i = 2j + 1 = j^2 - j^2 + 2j + 1$$

□

Direct proofs

- Many of things can be stated as an implication
  a. The sum of two rational numbers is rational.
     $a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$
  b. Every odd integer is the difference of two perfect squares.
     $i = 2j + 1$ for $j \in \mathbb{Z} \Rightarrow \exists a, b : \ i = a^2 - b^2$

- If we assume the LHS is true and show the RHS is, then the implication must be true.

Proof of b.

Assume $i = 2j + 1$, we can write this as

$$i = 2j + 1 = j^2 - j^2 + 2j + 1 = (j + 1)^2 - j^2.$$

□

Direct proofs

- Many of things can be stated as an implication
  a. The sum of two rational numbers is rational.
     $a, b \in \mathbb{Q} \Rightarrow a + b \in \mathbb{Q}$
  b. Every odd integer is the difference of two perfect squares.
     $i = 2j + 1$ for $j \in \mathbb{Z} \Rightarrow \exists a, b : \; i = a^2 - b^2$
- If we assume the LHS is true and show the RHS is, then the implication must be true.

Proof of b.

Assume $i = 2j + 1$, we can write this as

$$i = 2j + 1 = j^2 - j^2 + 2j + 1 = (j + 1)^2 - j^2.$$

So here we have *constructed* $a = (j + 1)^2$ and $b = j^2$. □

Proof by contrapositive

- We can also use the equivalence: $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Example

Show that if $3n + 2$ is even then n is even.

Proof by contrapositive

- We can also use the equivalence: $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Example

Show that if $3n + 2$ is even then n is even.

Proof.

We will show that if n is odd then $3n + 2$ is odd.

Proof by contrapositive

- We can also use the equivalence: $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Example

Show that if $3n + 2$ is even then n is even.

Proof.

We will show that if n is odd then $3n + 2$ is odd. Assume n is odd, i.e. there exists k s.t. $n = 2k + 1$. which we can plug in to get

$$3n + 2 = 3(2k + 1) + 2$$

□

Proof by contrapositive

- We can also use the equivalence: $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Example

Show that if $3n + 2$ is even then n is even.

Proof.

We will show that if n is odd then $3n + 2$ is odd. Assume n is odd, i.e. there exists k s.t. $n = 2k + 1$. which we can plug in to get

$$3n + 2 = 3(2k + 1) + 2 = 6k + 5$$

□

Proof by contrapositive

- We can also use the equivalence: $A \Rightarrow B \equiv \neg B \Rightarrow \neg A$

Example

Show that if $3n + 2$ is even then n is even.

Proof.

We will show that if n is odd then $3n + 2$ is odd. Assume n is odd, i.e. there exists k s.t. $n = 2k + 1$. which we can plug in to get

$$3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1.$$

and hence is $3n + 2$ odd. □

Proof by contradiction

- Let's say we want to prove A
  - Instead we'll assume $\neg A$ and arrive at some contradiction
  - Everything however **must** be logically consistent if only A were false.

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$.

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$. Substitute this in and rearrange to arrive at

$$ap^2 + bpq + cq^2 = 0.$$

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$. Substitute this in and rearrange to arrive at

$$ap^2 + bpq + cq^2 = 0.$$

We assumed p/q was fully reduced, so both cannot be even. Consider:

- only p is odd: odd + even + even = odd;

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$. Substitute this in and rearrange to arrive at

$$ap^2 + bpq + cq^2 = 0.$$

We assumed p/q was fully reduced, so both cannot be even. Consider:

- only p is odd: odd + even + even = odd;
- only q is odd: even + even + odd = odd;

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$. Substitute this in and rearrange to arrive at

$$ap^2 + bpq + cq^2 = 0.$$

We assumed p/q was fully reduced, so both cannot be even. Consider:

- only p is odd: odd + even + even = odd;
- only q is odd: even + even + odd = odd;
- both odd: odd + odd + odd = odd.

Example

Show that if a, b, c are odd integers, then $ax^2 + bx + c = 0$ has no solution in the set of rational numbers.

Proof.

Assume a solution $x = p/q$ does exist, in lowest form, $q \neq 0$. Substitute this in and rearrange to arrive at

$$ap^2 + bpq + cq^2 = 0.$$

We assumed p/q was fully reduced, so both cannot be even. Consider:

- only p is odd: odd + even + even = odd;
- only q is odd: even + even + odd = odd;
- both odd: odd + odd + odd = odd.

But 0 is even, so this cannot be equal to 0. Therefore our assumption that a solution exists must be false. □

Proof by induction

- Say we want to prove an infinite number of statements $A_0, A_1, A_2, \ldots$
  - Idea: prove that $A_n \Rightarrow A_{n+1}$ for any n. Then prove A_0.
  - Like dominoes, $A_0 \Rightarrow A_1 \Rightarrow A_2 \Rightarrow \ldots$

Example

Show that $\sum_{k=1}^{n}(k \cdot k!) = (n+1)! - 1$ for all natural numbers.

Proof.

Base case: $1 \cdot 1! = (1+1)! - 1 = 1$.
Now we'll prove the inductive case directly. We'll assume that what we're trying to prove holds for **a specific** n. If this is true then

$$\sum_{k=1}^{n+1}(k \cdot k!) = \sum_{k=1}^{n}(k \cdot k!) + (n+1)(n+1)!$$
$$\vdots$$
$$= ((n+1)+1)! - 1.$$

□

Playing with sets

- Sets are just logical statements in disguise
  - $A \cup B = \{x|(x \in A) \vee (x \in B)\}$
  - $A \cap B = \{x|(x \in A) \wedge (x \in B)\}$
  - $A \setminus B = A \cap \overline{B}$
  - $A \subseteq B$ can be translated as "if x is in A, then x is in B."

Example

Show that $(A \setminus B \subseteq C) \Rightarrow (A \setminus C \subseteq B)$.

Proof.

We'll assume $A \setminus B \subseteq C$. We want to prove the consequent, which can be translated into

$$x \in A \setminus C \Rightarrow x \in B.$$

We can do this by assuming $x \in A \setminus C$ and showing that

$$\begin{aligned} x \in (A \setminus C) &\Rightarrow x \notin C \\ &\Rightarrow x \notin (A \setminus B) \\ &\Rightarrow x \notin A \wedge x \notin \overline{B} \Rightarrow x \in B. \end{aligned}$$

□

And now something completely different. . .

Diagonalization and uncountable sets

Example

The real numbers are uncountable, i.e. $\mathbb{R}$ cannot be put into one-to-one correspondence with $\mathbb{N}$.

Proof.

We'll assume $[0, 1]$ is countable, and thus we can construct an infinite table containing all the reals in this range

0	0.0
1	0.14159...
2	0.3
⋮	

Let k_n to be the nth digit of the nth number. We'll construct a number i such that the nth digit of i is $k_n + 1 \mod 10$. This number does not exist on our list because it differs from every number on the list by at least one digit. Therefore the reals are not countable. □

Density of $\mathbb{Q}$ in $\mathbb{R}$

Theorem

For any $a, b \in \mathbb{R}$ s.t. $a < b$ there is a $q \in \mathbb{Q}$ such that $a < q < b$.

Proof.

There exists an n such that $nb - na > 1$ due to the Archimedian property of $\mathbb{R}$. Let m be the largest integer such that $m < na$. It must hold that $na < m + 1 < nb$:

- $m + 1 < na$ cannot hold since m is the largest integer less than na
- $m + 1 > nb$ cannot hold since $nb - na > 1$

As a result $a < \frac{m+1}{n} < b$. □

inf, sup, and ordering

- Consider an ordered set T with a relation $\leq$ and a subset $S \subseteq T$.
- The *infimum* is the greatest lower bound.
- The *supremum* is the least upper bound.

- These are the tightest bounds on the set S, but need not be in S
- hence differ from the greatest/least elements

- Consider $S = \{\exp(-x) : x \in [0, \inf)\}$ where $T = \mathbb{R}$.
- $\sup S = 1$ and $\inf S = 0$, but $0 \notin S$.
- $\max(S) = 1$ but $\min(S)$ does not exist.

limits

Definition

The limit of a function $\lim_{x \to x_0} f(x) = L$ holds if for every $\epsilon > 0$ there exists $\delta > 0$ such that

$$|f(x) - L| < \epsilon \quad \text{if} \quad |x - x_0| < \delta.$$

Definition

For limits tending to infinity $\lim_{x \to \infty} f(x) = L$ if for every $\epsilon > 0$ there exists a bound $M > 0$ such that

$$|f(x) - L| < \epsilon \quad \text{if} \quad M < x.$$

Example

Show that $\lim_{x\to\infty} \frac{2x-1}{x-3} = 2$.

Proof.

Using the definition we can write

$$|f(x) - L| = \frac{2x-1}{x-3} - 2 = \frac{5}{x-3} < \epsilon.$$

We can see that this holds if $x > M = 3 + \frac{5}{\epsilon}$ so long as $x > 3$. □

Continuity

Definition

$f(x)$ is continuous at x_0 if $\lim_{x \to x_0} f(x) = f(x_0)$. $f(x)$ is continuous on $[a, b]$ if this holds for every point in the range.

Theorem (Intermediate-value theorem)

If $f(x)$ is continuous on $[a, b]$ then f takes on every value between $f(a)$ and $f(b)$.

Differentiable

Definition

A function $f(x)$ is differentiable at x_0 so long as the limit

$$f'(x_0) = \lim_{x \longrightarrow x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

exists.

Integration

- For *smooth enough* functions the standard Riemannian integral is fine (i.e. use subintervals, take limit)
- Otherwise we need the Lebesgue integral (divide up the *range*)
- Here we need measure theory to *measure* the resulting interval
- Why in continuous probabilities a specific point has probability 0
- $\int_0^1 \mathbb{I}_{\mathbb{Q}}(x)\, dx$