APEC Math Review

Proofs

Natalia Ordaz Reynoso

Summer 2019

Proofs

Theorem: a mathematical statement that is true and can be (and has been) verified as true

A proof of a theorem is a written verification that shows that the theorem is definitely and unequivocally true.

- Understandable
- Convincing
- Unambiguous

Definition: exact, unambiguous explanation of the meaning of a mathematical word or phrase

Theorems

Theorem: Let f be differentiable on an open interval I and let $c \in I$. If $f(c)$ is the maximum or minimum vlue of f on I, then $f'(c) = 0$

Theorem: Every absolutely convergent series converges.

Theorem: Suppose each consumer's preferences are locally non-satiated. Then any allocation (x, y*) that with prices p* forms a competitive equilibrium is Pareto optimal*

Note: all of these are in the conditional form or can be written in it.

Definitions

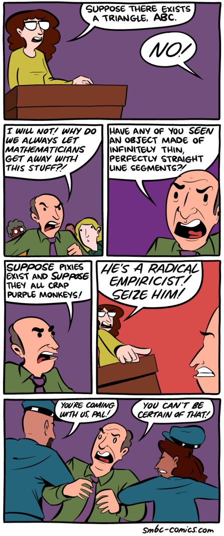
- An integer n is even if $n = 2a$ for some integer $a \in \mathbb{Z}$
- An integer n is odd if $n = 2a + 1$ for some integer $a \in \mathbb{Z}$
- A number $n \in \mathbb{N}$ is prime if it has exactly two positive divisors: 1 and n. If n has more than two positive divisors, it is called a composite (Thus n is composite if and only if $n = ab$ for $1 < a, b < n$.)
- A feasible allocation $(x_1, ..., x_I, y_1, ..., y_J)$ is Pareto Optimal if there is no other feasible allocation $(x'_1, ..., x'_I, y'_1, ..., y'_J)$ such that $u_i(x'_i) \leq u_i(x_i)$ for all i=1,...,I and $u_i(x'_i) > u_i(x_i)$ for some i.

Other types of statements

- Theorems: statements that have been proven to be true
- Proposition, lemma : A statement that is true but not as significant as a theorem
- Corollary: a result that is an immediate consequence of a theorem

Direct Proof

- Let P, Q be statements
- Proposition: $P \Rightarrow Q$
- Direct proofs require us to construct a chain of implications $R_1, R_2, \ldots R_n$ such that: $P \Rightarrow R_1,\ R_1 \Rightarrow R_2,\ \ldots\ R_n \Rightarrow Q$
- Transitivity holds for conditional statements.
- Draw the truth table
- Remember: we only care about those cases when P is true


SUPPOSE THERE EXISTS A TRIANGLE, ABC.
NO!
I WILL NOT! WHY DO WE ALWAYS LET MATHEMATICIANS GET AWAY WITH THIS STUFF?!
HAVE ANY OF YOU SEEN AN OBJECT MADE OF INFINITELY THIN, PERFECTLY STRAIGHT LINE SEGMENTS?!
SUPPOSE PIXIES EXIST AND SUPPOSE THEY ALL CRAP PURPLE MONKEYS!
HE'S A RADICAL EMPIRICIST! SEIZE HIM!
YOU'RE COMING WITH US, PAL!
YOU CAN'T BE CERTAIN OF THAT!
smbc-comics.com

Direct Proof

- We are interested in the logical implications of P
- and statements that imply Q
- The idea is to work forward from P and backwards from Q, and connect the chain of implications
- Sometimes we may have to either strengthen P (add assumptions) or weaken Q
- Example on the board:

Theorem 1: The square of an odd integer is also odd

Direct Proof

- We are interested in the logical implications of P
- and statements that imply Q
- The idea is to work forward from P and backwards from Q, and connect the chain of implications
- Sometimes we may have to either strengthen P (add assumptions) or weaken Q
- Example on the board:

Theorem 1: The square of an odd integer is also odd
Use the definition of odd

Other examples of direct proof

- Proposition: Let x, y be positive real numbers. If $x \leq y$, then $\sqrt{x} \leq \sqrt{y}$
- Proposition: Let x, y be positive real numbers, then $2\sqrt{xy} \leq x + y$
- Proposition: If $n \in \mathbb{N}$, then $1 + (-1)^n(2n - 1)$
- Proposition: Every multiple of 4 equals $1 + (-1)^n(2n - 1)$ for some $n \in \mathbb{N}$
- Proposition: If two integers have opposite parity, their sum is odd

WLOG

Without loss of generality, assume that all masses are eq...
No, you idiot! That DOES lose generality!
quickmeme.com

Indirect Proof

Some propositions are difficult to prove directly. We will study two ways of indirect proofs: Proof by contrapositive and proof by contradiction.

- Proof by contrapositive: instead of proving $P \Rightarrow Q$, we prove its logical equivalent: $\neg Q \Rightarrow \neg P$
- Proof by contradiction: instead of proving $P \Rightarrow Q$, we show that $(P \wedge \neg Q)$ implies a contradiction.

Prove by Contrapositive

- Draw the truth table that verifies that a statement is logically equivalent to its contrapositive
- The outline of proofs by contrapositive is:
  1. Suppose $\neg Q$
  2. ...
  3. Therefore $\neg P$
- Compare to the outline of a direct proof.
- An example: Proposition: if n is an integer, and n^2 is even, then n is also even
- Proofs by contrapositive are convenient when the universal quantifier is present, because the contrapositive will include the existence quantifier.

Proof by Contrapositive: Examples

- Suppose $x \in \mathbb{Z}$. If $7x + 9$ is even, then x is odd (prove both ways)
- Suppose $x \in \mathbb{Z}$. If $x^2 - 6x + 5$ is even, then x is odd (try both)
-
- Let $a \geq 0, \in \mathbb{R}$. If $\forall \epsilon > 0$ it is true that $0 \leq a < \epsilon$ then $a = 0$
- If m, n are natural numbers such that $m + n \geq 20$ then either $m \geq 10$ or $n \geq 10$

Mathematical Writing

Hammack's style guidelines for mathematical writing

1. Never begin a sentence with a mathematical symbol (capitalization)
2. End each sentence with a period
3. Separate mathematical symbols and expressions with words (to avoid confusion)
4. Avoid misuse of symbols (!!)
5. Avoid unnecessary symbols
6. Use the first person plural (in math)
7. Use the active voice
8. Explain each new symbol
9. Watch out for "it" (!!)
10. Since, because, as for, so
11. Thus, hence, therefore, consequently

Suggested Exercises

Either odd or even exercises for Chapters 4 and 5 of Hammack

Proof by Contradiction

- We can use this to prove all kinds of statements, not just conditional ones.
- Idea: assume not, and get to nonsense
- Sometimes called reduction to absurdity
- A contradiction is a statement that cannot be true
- We will use the fact that if C is a contradiction, then $P \wedge \neg Q \Rightarrow C$, and $P \Rightarrow Q$ are logically equivalent

Proof by Contradiction

- You begin by saying "suppose P but not Q"
- You make sound logical steps
- if you arrive to a contradiction, then your initial assumption* must be wrong.
- Small detail: we do not necessarily know what the contradiction will be
- Example: The number $\sqrt{2}$ is irrational
- Example: Euclid's Theorem: There are infinitely many prime numbers
- Let $a > 0$, a real number. Then $1/a > 0$

Combining techniques

- Every non-zero rational number can be expressed as the product of two irrational numbers.
- (By contradiction and then by contrapositive) Suppose $a \in \mathbb{Z}$. if $a^2 - 2a + 7$is even then a is odd

Suggested Exercises

Either even or odd exercises from Chapter 6 of Hammack

More on Proofs: Biconditional statements

- If and only if
- Prove a conditional statement and its converse
- Example: an integer n is odd if and only if n^2 is odd
- That's it!

Equivalent statements

Theorem Suppose A is an *nxn* matrix. The following statements are equivalent

1. The matrix A is invertible
2. The equation $A\boldsymbol{x} = \boldsymbol{b}$ has a unique solution for every $\boldsymbol{b} \in \mathbb{R}^n$
3. $det(A) \neq 0$
4. The matrix A does not have 0 as an eigenvector

The theorem says that these are all either true or all false. How do we prove these?

Existence, Uniqueness

- We have been proving conditional statements, which are universally quantified statements
- How would you prove an existensially quantified statement?

Existence, Uniqueness

- We have been proving conditional statements, which are universally quantified statements
- How would you prove an existensially quantified statement?
- all we need is an example, as we saw last time
- Example: There exists an even prime number
- Example: There is an integer that can be expressed as the sum of two perfect cubes in two different ways
- Uniqueness statements assert that there is exactly one example x for which P(x) is true.
- It exists and it is unique

Uniqueness Example

To show uniqueness, an example is not enough, you must show that there are no others

- Given a, b, c be real numbers. There is only one real number x that satisfies $a + bx = c$

Uniqueness Example

To show uniqueness, an example is not enough, you must show that there are no others

- Given a, b, c be real numbers. There is only one real number x that satisfies $a + bx = c$
- We need something else here. What is it?
- Show existence for the example above

Constructive vs non constructive proofs

Existence proofs are either constructive or non-constructive

- Constructive proofs display an explicit example
- Non-constructive proofs prove an example exists without providing it
- There exist irrational numbers x and y for which x^y is rational

Suggested Exercises

Hammack Section 7 (either even or odd)

Proofs Involving Sets

- Show $a \in A$, when $A = \{x \in S : P(x)\}$
- Then show that $a \in S$ and P(a) holds
- Show $A \subseteq B$
- The you must show that $\forall a \in A, a \in B$
- directly, by contrapositive, contradiction, ...

Examples: proofs involving sets

- Prove that if A and B are sets, then $\wp(A) \cup (B) \subseteq \wp(A \cup B)$
- Let A and B be sets, show that if $\wp(A) \subseteq \wp(B)$ then $A \subseteq B$
- Let A, B, C be sets, and $C \neq \emptyset$. Show that if A x C = B x C then A=B

Disproof: universal statements

$\rightarrow$ proving that something is not true.

- How do you disproof? You cannot just say "there is no proof"
- Statements={ Are known to be true , truth unknown, known to be false }
- $\neg P$
- Disproving universal statements: counterexamples
- $\forall x \in S, P(x)$ can be disproved by proving $\exists x \in S : \neg P(x)$
- Conjecture: for every integer n, $f(n) = n^2 - n + 11$ is prime

Disproof: universal statements

$\rightarrow$ proving that something is not true.

- How do you disproof? You cannot just say "there is no proof"
- Statements=$\{$ Are known to be true , truth unknown, known to be false $\}$
- $\neg P$
- Disproving universal statements: counterexamples
- $\forall x \in S, P(x)$ can be disproved by proving $\exists x \in S : \neg P(x)$
- Conjecture: for every integer n, $f(n) = n^2 - n + 11$ is prime
- Consider n=11
- Conjecture: If A, B, C are sets then $A - (B \cap C) = (A - B) \cap (A - C)$

Disproof: existence statements

- $\exists x \in S, P(x)$
- To prove, an example is enough. To disprove it is not.
- The negation of the above statement is universally quantified
- Conjecture: There is a real number x for which $x^4 < x < x^2$

Disproof: existence statements

- $\exists x \in S, P(x)$
- To prove, an example is enough. To disprove it is not.
- The negation of the above statement is universally quantified
- Conjecture: There is a real number x for which $x^4 < x < x^2$
- Prove the negation by contradiction

Disproof: existence statements

- $\exists x \in S, P(x)$
- To prove, an example is enough. To disprove it is not.
- The negation of the above statement is universally quantified
- Conjecture: There is a real number x for which $x^4 < x < x^2$
- Prove the negation by contradiction
- Conjecture: There exist three different integers x, y, z greater than 1 such that $x^y = y^z$

Disproof by contradiction

- Disprove P
- equivalent to proving $\neg P$
- to prove that by contradiction, I begin assuming $\neg\neg P$
- so assume P, work, get to a contradiction, done!

Finally: Induction

- Induction: from particular to general
- Useful for statements that involve natural numbers.
- We use the property of good order of natural numbers.
- Any nonempty set of the natural numbers has a smallest element

Induction

- Conjecture: the sum of the first n odd natural numbers equals n^2 (table)
- From the table: sequential statements S_n
- Outline:
  1. Show that it holds for n=1 (basis)
  2. Show that if it holds for $n > 1$ (inductive hypothesis), it holds for n+1 (inductive)
- Convinced? Want to see the proof? B&S pg 15
- note: n=1 does not have to be the first statement.
- note: does not work for n in integers (why?)
- Prove the above conjecture using mathematical induction.

- If n is a non negative integer, then 5 is a factor of $(n^5 - n)$ (notation: $5|(n^5 - n)$)
- If $n \in \mathbb{Z}$ and $n \geq 0$, then $\Sigma_{i=0}^{n} i \cdot i! = (n+1)! - 1$
- For each $n \in \mathbb{N}, 2^n \leq 2^{n+1} - 2^{n-1} - 1$

Strong Induction

- Sometimes, it is not easy to show s_{k+1} from S_k
- strong induction has a different inductive step:
- Given any integer $k \geq 1$, prove $(S_1 \wedge S_2 \wedge S_3 \wedge ... \wedge S_k) \Rightarrow S_{K+1}$
- Is strong induction equivalent to induction?

Proof by Smallest Counterexample

- Hybrid of induction and counterexample
  1. Check that S_1 is true
  2. For the sake of contradiction, suppose not every S_n is true
  3. Let $k > 1$ be the smallest integer for which S_k is false
  4. Then S_{k-1} is true and S_k is false
  5. find a contradiction
- Example in page 165 of The Book of Proof
- Fibonacci example
- Suggested induction exercises in section 10 of Hammack and Section 1.2 of Bartle and Sherbert