Proof Methods and Strategies

Jing Yang
September 27, 2010

Review

- A proof is a step-by-step demonstration that a conclusion follows from some hypotheses.
  - □ In each step use hypotheses, definitions, axioms, previously proven theorems, rules of inference, and logical equivalences
- Types of proofs
  - □ Direct proof, proof by contraposition, proof by contradiction
  - □ … …

Proof by Cases

$$(p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q \equiv (p_1 \rightarrow q) \land (p_2 \rightarrow q) \land \ldots \land (p_n \rightarrow q))$$

- Break the hypothesis into an equivalent disjunction of the form $p_1 \lor p_2 \lor \ldots \lor p_n$, prove $p_i \rightarrow q$ is true for every p_i
- How to prove $(p_1 \lor p_2 \lor \ldots \lor p_n) \rightarrow q$?
  - For each p_i,
    - Assume p_i is true

      ____

      ____

      ____

      ____
    - q must be true
  - Q.E.D.

These steps are constructed using:

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems
- ...

Proof by Cases (example)

If n is an integer, then n(n+1)/2 is an integer

Proof (by cases):

- Case 1: n is even.

  n = 2a, for some integer a

  So n(n+1)/2=2a(n+1)/2=a(n+1), which is an integer

- Case 2: n is odd.

  n = 2a+1, for some integer a

  So n(n+1)/2=n(2a+1+1)/2=n(2a+2)/2=n(a+1), which is an integer

Proof by Cases (example) -2

Let ⊗ be the ‘max’ on the set of integers: if $a \geq b$ then $a \otimes b = \max\{a,b\} = a = b \otimes a$

Prove: for all a,b,c, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$

Proof (by cases): Let a,b,c be arbitrary integers, then one of the following six cases must hold

- $a \geq b \geq c$
- $a \geq c \geq b$
- $b \geq a \geq c$
- $b \geq c \geq a$
- $c \geq a \geq b$
- $c \geq b \geq a$

Proof by Exhaustion

- Check a relatively small number of cases
- A special type of proof by cases

Proof by Exhaustion (example)

Prove $(n+1)^2 \geq 3^n$ if n is a positive integer with $n \leq 4$

Proof (by exhaustion):

- $n=1$
- $n=2$
- $n=3$
- $n=4$

Proof of Equivalences

$$\boxed{p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)}$$

- How to prove $p \leftrightarrow q$ is true?
  - We need to prove $p \rightarrow q$ and $q \rightarrow p$
  - Recall: to prove the logical equivalence of two formulas we can also use truth tables and developing a series of logical equivalences.

Proof of Equivalences (example)

Prove $(\neg p \wedge \neg q) \leftrightarrow \neg(p \vee q)$ is true

- Part 1: prove $(\neg p \wedge \neg q) \rightarrow \neg(p \vee q)$ is true
    - Assume $(\neg p \wedge \neg q)$ is true.
    - Then $\neg p$ is true and $\neg q$ is true, i.e. p is false and q is false
    - Therefore $p \vee q$ is false, i.e. $\neg(p \vee q)$ is true
- Part 2: prove if $\neg(p \vee q)$ is true then $\neg p \wedge \neg q$ is true
    - ...

Proof of Equivalences (example)

Prove n is odd if and only if n^2 is odd.

- Part 1: prove if n is odd then n^2 is odd
  - (We have proved it in last lecture
- Part 2: prove if n^2 is odd then n is odd (by contraposition)
  - Assume n is even. Then n=2k for some integer k
  - $n^2=(2k)^2=4k^2=2(2k^2)=2m$ for some integer m
  - Therefore n^2 is even
- Q.E.D

Proof of Existence

- How to prove $\exists x P(x)$?
  - □ Constructive existence proof: Find an element c such that P(c) is true
  - □ Nonconstructive existence proof (do not find an element c such that P(c) is true):
    - Prove $\exists x P(x)$ is true in some other way
    - Assume no c exists which makes P(c) true and derive a contradiction

Constructive Existence Proof (example)

Prove: there exists integers x, y, z satisfying $x^2+y^2=z^2$.

Proof (by construction):

Find an example: x=3, y=4, z=5

Nonconstructive Existence Proof (example)

Prove: there exists irrational numbers x and y such that x^y is rational.

Proof (by non-construction):

By previous example: $\sqrt{2}$ is irrational

For $(\sqrt{2})^{\sqrt{2}}$

- Case 1: If $(\sqrt{2})^{\sqrt{2}}$ is rational, then the theorem is proved
- Case 2: If $(\sqrt{2})^{\sqrt{2}}$ is irrational
    - $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 =2$ is rational

Q.E.D.

Nonconstructive Existence Proof (example)

Prove: there exists irrational numbers x and y such that x^y is rational.

Proof (by contradiction):

Assume there exists no irrational numbers x and y such that x^y is rational, i.e. for all irrational numbers x and y, x^y is irrational.

By previous example: $\sqrt{2}$ is irrational

Then $(\sqrt{2})^{\sqrt{2}}$ is irrational.

Then is $((\sqrt{2})^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^2 = 2$ is irrational. Contradiction!

Q.E.D.

Disproof by Counterexample

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

- How to prove $\forall x P(x)$ is not true?
  - Find a counterexample c such that P(c) is false

Disproof by Counterexample (example)

Prove not every positive integer is the sum of the squares of three integers.

Proof (by counterexample):

- Try to find a counterexample

  $1 = 0^2 + 0^2 + 1^2$

  $2 = 0^2 + 1^2 + 1^2$

  $3 = 1^2 + 1^2 + 1^2$

  $4 = 0^2 + 0^2 + 2^2$

  $5 = 0^2 + 1^2 + 2^2$

  $6 = 1^2 + 1^2 + 2^2$

  $7 = ?$

- 7 is a counterexample. Since squares less than 7 are 0, 1, and 4, 7 cannot be written as a sum of three of these numbers.

Proof Strategies

- Finding proofs can be challenging
  - □ Replace terms by their definitions
  - □ Carefully analyze hypotheses and conclusion
  - □ Choose a proof method
  - □ Attempt to prove the theorem
  - □ If it fails try different proof methods

Readings and Notes

- Learning how to construct proofs is probably one of the most difficult things you will face in life. Few of us are gifted enough to do it with ease. One only learns how to do it by practicing.
- Recommended exercises: 1.7: 5,21,37,41
- Recommended book: “How to read and do proofs” by Daniel Solow