Monash University
Faculty of Information Technology

Lecture 4
Proofs

Slides by Graham Farr (2013-2014).

FIT2014 Theory of Computation

Overview

- Finding proofs
- Proof by construction
- Proof by cases
- Proof by contradiction
- Proof by induction
  - base case
  - inductive step
  - conclusion

Proof (recap)

- A step-by-step argument that establishes, logically and with certainty, that something is true.
- Should be verifiable.

Every statement must be a logical consequence of some conjunction of previous statements.

If you've previously established P,

and also that $P \Rightarrow Q$

then you can deduce Q.

(modus ponens)

Finding proofs

There is no systematic method for finding proofs for theorems.

- There are deep theoretical reasons for this.

  (Gödel, 1931; Church, 1936; Turing, 1936)

Discovering proofs is an art as well as a science.

It requires

- skill at logical thinking and reasoning
- understanding the objects you're working with
- practice, experience
- play, exploration
- creativity and imagination
- perseverence

Types of proofs

Proof by construction

Proof by cases

Proof by contradiction

Proof by induction

This list is not exhaustive. Proofs can be quite individual in character and hard to classify, although many will follow one of the above patterns.

Many proofs are a mix of these types.

Proof by construction

- also known as:

Proof by example

- can be used where the theorem asserts the existence of some object with a specific property
  - just give the example, show it has the property.
- BUT: an ***illustration*** is NOT a ***proof***.
- So, if your example merely illustrates the *idea* of a proof, then it is not, itself, a proof (although it might still be useful in illustrating a proof).
- Recall Lecture 1: ***English has a palindrome.***

Proof by cases

- also known as:

Proof by exhaustion

or (if lots of cases) brute force

- identify a number of different cases which cover all possibilities
- Prove the theorem for each of these cases.

- Recall Lecture 1:

Every English word has a vowel or a "y".

Proof by contradiction

(also known as: "*reductio ad absurdum*")

- Start by assuming the ***negation*** of the statement you want to prove.
- Deduce a ***contradiction***.
- Therefore, the statement must be true.

Proof by contradiction

Theorem

The statement "This statement is false" is not a proposition.

Proof.

Assume that it is a proposition.

Then it must be either true or false.

If it is true, then it is false.

If it is false, then it is true.

So, it is false if and only if it is true.

This is a contradiction. So our assumption, that the statement is a proposition, must be false. Q.E.D.

More proofs

Recall De Morgan's Laws:

$$\neg(P \vee Q) = \neg P \wedge \neg Q$$

$$\neg(P \wedge Q) = \neg P \vee \neg Q$$

- We proved these using *truth tables*.

- But, how to prove its extended form? …

For all n:

$$\neg(P_1 \vee \ldots \vee P_n) = \neg P_1 \wedge \ldots \wedge \neg P_n$$

More proofs

Theorem

For all n:

$\neg(P_1 \vee \ldots \vee P_n) \;=\; \neg P_1 \wedge \ldots \wedge \neg P_n$

First proof:

Left-Hand Side is True

if and only if $P_1 \vee \ldots \vee P_n$ is False

if and only if $P_1, \ldots, P_n$ are all False

if and only if $\neg P_1, \ldots, \neg P_n$ are all True

if and only if Right-Hand Side is True. Q.E.D.

Let's try for a different proof, using De Morgan's Law.

More proofs

Theorem: For all n:

$\neg(P_1 \vee \ldots \vee P_n) \;=\; \neg P_1 \wedge \ldots \wedge \neg P_n$

Second proof (attempt):

$\neg(P_1 \vee \ldots \vee P_n)$

$= \neg((P_1 \vee \ldots \vee P_{n-1}) \vee P_n)$ (just grouping …)

$= \neg(P_1 \vee \ldots \vee P_{n-1}) \wedge \neg P_n$ (by De Morgan's Law)

= … ***and so on and so on*** …

$= \neg P_1 \wedge \ldots \wedge \neg P_n$ Q.E.D.??

Good try, but reader has to infer how to fill the gap.

It's shorthand for a "proof" whose length depends on n.

But we can turn its main *idea* into a proper proof.

Proof by mathematical induction

Suppose you want to prove that a statement S(n) holds for every natural number n.

Principle of Mathematical Induction

IF S(1) is true *(inductive basis)*

AND ∀n: **if** S(n) is true, then S(n+1) is true *(inductive step)*

THEN

∀n: S(n) is true.

inductive hypothesis

S(1), S(2), …., S(n), S(n+1), S(n+2), …….

Proof by mathematical induction

Theorem: For all n:

$\neg(P_1 \vee \ldots \vee P_n) = \neg P_1 \wedge \ldots \wedge \neg P_n$

Second proof:

We prove it by ***induction*** on the # of propositions.

Inductive basis:

It is trivially true when we have just one proposition:

$\neg P_1 = \neg P_1$!

Inductive step:

Suppose it's true for n-1 propositions:

$\neg(P_1 \vee \ldots \vee P_{n-1}) = \neg P_1 \wedge \ldots \wedge \neg P_{n-1}$

(This our *Inductive Hypothesis*. We will use it later.)

Proof by mathematical induction

(continued)

We have:

$\neg(P_1 \vee \ldots \vee P_n)$

$= \neg((P_1 \vee \ldots \vee P_{n-1}) \vee P_n)$ (just grouping …)

$= \mathbf{\neg(P_1 \vee \ldots \vee P_{n-1})} \wedge \neg P_n$ (by De Morgan's Law)

$= \mathbf{\neg P_1 \wedge \ldots \wedge \neg P_{n-1}} \wedge \neg P_n$

(***by Inductive Hypothesis***)

So, by the ***Principle of Mathematical Induction***, it's true for any number of propositions. Q.E.D.

Proof by mathematical induction

Theorem: For all *n*:

$$1+\cdots+n=\frac{n(n+1)}{2}$$

Proof:

We prove it by ***induction*** on *n*.

Inductive basis:

When n = 1, LHS = 1 and RHS = 1(1+1)/2 = 1. ✓

Inductive step:

Suppose it's true for n.

We will deduce that it's true for n+1.

1+…+(n+1) = (1+…+n) + (n+1)

(preparing to use the inductive hypothesis)

Proof by mathematical induction

$1+\ldots+(n+1) = (1+\ldots+n) + (n+1)$

(preparing to use the inductive hypothesis)

$= n(n+1)/2 + (n+1)$ *(by the inductive hypothesis)*

$= (n+1)n/2 + (n+1)$ *(algebra …)*

$= (n+1)(n/2 + 1)$

$= (n+1)(n+2)/2$

$= (n+1)((n+1)+1)/2$

This is just the equation in the Theorem, for $n+1$ instead of n.

So the inductive step is now complete. ✓

Therefore, by the Principle of Mathematical Induction, the equation holds for all n. Q.E.D.

Proof by mathematical induction

Exercise: Prove by induction that, for all *n*:

$$1^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

Something to think about:

the relationship between **induction** and **recursion**

Proof by mathematical induction

Contrast with "induction" in statistics, which is the process of drawing general conclusions from data.

Statistical induction is typically used in situations where there is some randomness in the data.

Statistical induction cannot be used as a step in a mathematical proof.

Mathematical induction is a rigorous and very powerful tool for proofs in mathematics and computer science.