Monash University
Faculty of Information Technology

FIT2014 Theory of Computation

Lecture 4
Proofs

slides by Graham Farr

Overview

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

Proof (recap)

- A step-by-step argument t[illegible]lishes, logically and with certainty, that something is true.
- Should be verifiable.
- Must be finite.
- Every statement must be:
  - something you already know at the start
    - a definition
    - an axiom
    - a previously-proved theorem

  or
  - a logical consequence of some conjunction of previous statements.

Proof (recap)

If you've previously established
and also that $P \Rightarrow Q$
then you can deduce Q.
(modus ponens)

Exercise in Boolean algebra: Prove that $(P \wedge (P \Rightarrow Q)) \Rightarrow Q$ is a tautology.

If you've previously established all of $P_1, P_2, \ldots, P_n$
and also that $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow Q$
then you can deduce Q.

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

Finding proofs: general advice

To prove subset relations, $A \subseteq$ A and B are sets):

1. Take a general member of ive it a name. e.g., "Let $x \in A$"
2. Use the definition of A to say something about x.
3. Follow through the logical consequences of that,
4. . . . aiming to prove that x also satisfies the definition of B.

See, e.g., Lecture 1, slide 30, proof that DOUBLEWORD $\subseteq$ EVEN-EVEN.
See also: Tutorial 1, exercise 1.

Finding proofs: general advice

To prove set equality, $A = B$ A and B are sets):

1. Prove $A \subseteq B$
2. Prove $A \supseteq B$

To prove numerical equality, $A = B$ (where A and B represent numbers):
If algebra can transform A to B, then that's good;
but if not:

1. Prove $A \leq B$
2. Prove $A \geq B$

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 [illegible]uctio 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 [illegible] 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. □

Proof by contradiction

> “Every positive integer was one of his personal friends.”
>
> — J. E. Littlewood on Srinivasa Ramanujan, quoted by G. H. Hardy, *Srinivasa Ramanujan* (obituary), *Proceedings of the London Mathematica*[illegible]921) xl–lviii. See p. lvii.

Theorem.
Every natural number is interesting.

Proof.
Assume that not every natural number is interesting.
So, there exists at least one uninteresting number.
Therefore there exists a *smallest* uninteresting number.
But that number must be interesting, by virtue of having
this special property of being the smallest of its type.
This is a contradiction, as this number is uninteresting.
Therefore our original assumption was wrong.
Therefore every natural number is interesting. □

Srinivasa Ramanujan
(1887–1920)
`https://mathshistory.st-andrews.ac.uk/Biographies/Ramanujan/`

See, e.g., Ch. 14 (Fallacies), in: Martin Gardner, *The Scientific American Book of Mathematical Puzzles and Diversions*, Simon & Schuster, New York, 1959.

Proof by contradiction

Comments:

That “theorem” and “proof” is really just an informal argument, as the meaning of “interesting” is imprecise and subjective.
But it illustrates the structure of proof by contradiction.

It also illustrates the point that, if you know a set of objects is nonempty, then you can choose an element of *smallest* size in the set.
Often, the smallest object in a set may have special properties that can help you go further in the proof.

Can you always choose an object of *largest* size in a nonempty set?

Is every integer interesting?
Would the above proof still work, if applied to the set of all integers?

More proofs

Recall De Morgan's Laws:

$$
\begin{aligned}
\neg(P \lor Q) &= \neg P \land \neg Q \\
\neg(P \land Q) &= \neg P \lor \neg Q
\end{aligned}
$$

We proved these using truth tables.

But, how to prove its extended form? . . .

For all n:

$$\neg(P_1 \lor \cdots \lor P_n) = \neg P_1 \land \cdots \land \neg P_n$$

More proofs

Theorem.
For all n:

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

First proof:
Left-Hand Side is True
if and only if $P_1 \vee \cdots \vee P_n$ 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. □

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

More proofs

Theorem.

For all n:

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

Second proof *(attempt):*

$$\begin{aligned} & \neg(P_1 \vee \cdots \vee P_n) \\ = \quad & \neg((P_1 \vee \cdots \vee P_{n-1}) \vee P_n) && \text{(just grouping \dots)} \\ = \quad & \neg(P_1 \vee \cdots \vee P_{n-1}) \wedge \neg P_n && \text{(by De Morgan's Law)} \\ = \quad & \dots \text{ and so on and so on } \dots \\ = \quad & \neg P_1 \wedge \cdots \wedge \neg P_n && \text{Q.E.D.??} \end{aligned}$$

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 $\forall k:$ **if** $\underbrace{S(k) \text{ is true}}_{\textit{inductive hypothesis}}$, **then** $S(k+1)$ is true *(inductive step)*

THEN

$\forall n: \quad S(n)$ is true.

$$S(1), \ldots\ldots, S(n), S(n+1), \ldots\ldots$$

Proof by mathematical induction

Theorem.

For all n:

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

Second proof: We prove it by induction on the # of propositions.

Inductive basis:

It is trivially true when we have just one proposition:

$$\neg P_1 = \neg P_1 \ldots !$$

Inductive step:

Suppose it's true for k propositions:

$$\neg(P_1 \vee \cdots \vee P_k) = \neg P_1 \wedge \cdots \wedge \neg P_k$$

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

Proof by mathematical induction

(continued)

We have:

$$
\begin{aligned}
&\neg(P_1 \vee \cdots \vee P_{k+1}) \\
&\quad = \quad \neg((P_1 \vee \cdots \vee P_k) \vee P_{k+1}) && \text{(just grouping \ldots)} \\
&\quad = \quad \neg(P_1 \vee \cdots \vee P_k) \wedge \neg P_{k+1} && \text{(by De Morgan's Law)} \\
&\quad = \quad \neg P_1 \wedge \cdots \wedge \neg P_k \wedge \neg P_{k+1} && \text{(by Inductive Hypothesis)}
\end{aligned}
$$

Conclusion:
So, by the Principle of Mathematical Induction, it's true for any number of propositions.

□

Proof by mathematical induction

Theorem.

For all n:

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

Proof: We prove it by inducti

Inductive basis:

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

Inductive step:

Suppose it's true for $n = k$:

$$1 + \cdots + k = k(k+1)/2$$

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

$1 + \cdots + (k+1) = (1 + \cdots + k) + (k+1)$ (preparing to use the inductive hypothesis)

Proof by mathematical induction

$$
\begin{aligned}
1 + \cdots + {\color{blue}(k+1)} &= {\color{green}(1 + \cdots + k)} + (k+1) && \text{(preparing to use the inductive hypothesis)} \\
&= {\color{green}k(k+1)/2} + (k+1) && \text{(by the {\color{green}Inductive Hypothesis})} \\
&= (k+1)k/2 + (k+1) && \text{(algebra \ldots)} \\
&= (k+1)(k/2+1) \\
&= (k+1)(k+2)/2 \\
&= {\color{blue}(k+1)}({\color{blue}(k+1)}+1)/2
\end{aligned}
$$

This is just the equation in the Theorem, for $n = k+1$ instead of k.
So the inductive step is now complete. ✓

Conclusion:

Therefore, by the Principle of Mathematical Induction, the equation holds for all n. □

Proof by mathematical induction

Alternatively, we could make the inductive step go from $n = k - 1$ to $n = k$, instead of from $n = k$ to $n = k + 1$.

Slightly different proof: W[illegible]t 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 $n = k - 1$, where $k \geq 2$:

$$1 + \cdots + (k-1) = (k-1)k/2$$

We will deduce that it's true for $n = k$.

$$1 + \cdots + k = (1 + \cdots + (k-1)) + k \qquad \text{(preparing to use the inductive hypothesis)}$$

Proof by mathematical induction

$$
\begin{aligned}
1 + \cdots + k &= (1 + \cdots + (k-1)) + k && \text{(preparing to use the inductive hypothesis)} \\
&= (k-1)k/2 + && \text{the Inductive Hypothesis)} \\
&= k(k-1)/2 + && \text{ebra \ldots)} \\
&= k((k-1)/2 + 1) \\
&= k(k+1)/2
\end{aligned}
$$

This is just the equation in the Theorem, for $n = k$ instead of $k - 1$.
So the inductive step is now complete. ✓

Conclusion:
Therefore, by the Principle of Mathematical Induction, the equation holds for all n. □

Proof by mathematical induction

Exercise:

Prove by induction that, for a

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

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.

Revision

Practise doing proofs!

- tutorial sheets, textbooks,

Sipser, pp. 22–25.

For more about Srinivasa Ramanujan, see:

- `https://mathshistory.st-andrews.ac.uk/Biographies/Ramanujan/`
- R Kanigel, *The Man Who Knew Infinity: A Life of the Genius Ramanujan*, Washington Square Press, New York, 1991.
- *The Man Who Knew Infinity*, feature film, 2015.
- film review: G Farr, The Man Who Knew Infinity: inspiration, rigour and the art of mathematics, *The Conversation*, 24 May 2016.

`https://theconversation.com/the-man-who-knew-infinity-inspiration-rigour-and-the-art-of-mathematics-59520`