CS 441: Proof Methods

PhD. Nils Murrugarra-Llerena
nem177@pitt.edu

University of Pittsburgh

Today's topics

- Proof techniques
  - Proof by exhaustion
  - Proof by cases
  - Existence proofs
  - Uniqueness proofs

- Proof strategies
  - Backward reasoning

Not all theorems are of the form $p \rightarrow q$

Sometimes, we need to prove a theorem of the form:

$$p_1 \vee p_2 \vee \ldots \vee p_n \rightarrow q$$

So, we might need to examine multiple cases!

Prove that $n^2 + 1 \geq 2n$ where n is a positive integer with $1 \leq n \leq 4$

Proof:

Since we have verified each case, we have shown that $n^2 + 1 \geq 2n$ where n is a positive integer with $1 \leq n \leq 4$.
□

With only 4 cases to consider, exhaustive proof was a good choice!

Sometimes, exhaustive proof isn't an option, but we still need to examine multiple possibilities

Example: Prove the triangle inequality. That is, if x and y are real numbers, then $|x| + |y| \geq |x + y|$.

Clearly, we can't use exhaustive proof here since there are infinitely many real numbers to consider.

We also can't use a simple direct proof either, since our proof depends on the signs of x and y.

What should we do?

Example: Prove that if x and y are real numbers, then |x| + |y| ≥ |x + y|.

- Note: If $x \geq 0$, $|x| = x$, otherwise $|x| = -x$
- Cases:

1) $x \geq 0$ and $y \geq 0$
    - $|x| + |y| = x + y$ and $|x + y| = x + y$
    - $x + y \geq x + y$ ✓

2) $x < 0$ and $y < 0$
    - $|x| + |y| = -x - y$ and $|x + y| = -x - y$
    - $-x - y \geq -x - y$ ✓

3) $x \geq 0$ and $y < 0$
    - If $\boxed{x \geq |y|,}$ then $|x + y| = x - |y|$ and $|x| + |y| = x + |y|$
$x + |y| \geq x - |y|$ ✓
    - If $\boxed{x < |y|,}$ then $|x + y| = |y| - x$ and $|x| + |y| = x + |y|$
$|y| + x \geq |y| - x$ ✓

4) Symmetrical to Case 3 □

Making mistakes when using proof by cases is all too easy!

Mistake 1: Proof by "a few cases" is not equivalent to proof by cases.

This is a "there exists" proof, not a "for all" proof!

Example: Prove that all odd numbers are prime.

"Proof:"

- Case (i): The number 1 is both odd and prime
- Case (ii): The number 3 is both odd and prime
- Case (iii): The number 5 is both odd and prime
- Case (iv): The number 7 is both odd and prime

Thus, we have shown that odd numbers are prime. □

Making mistakes when using proof by cases is all too easy!

Mistake 2: Leaving out critical cases.

Example: Prove that $x^2 > 0$ for all integers x

"Proof:"

- Case (i): Assume that $x < 0$. Since the product of two negative numbers is always positive, $x^2 > 0$.
- Case (ii): Assume that $x > 0$. Since the product of two positive numbers is always positive, $x^2 > 0$.

Since we have proven the claim for all cases, we can conclude that $x^2 > 0$ for all integers x. □

What about the case in which x = 0?

Sometimes we need to prove the existence of a given element

There are two ways to do this

The constructive approach

The non-constructive approach

A constructive existence proof

Prove: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.

Proof: $1729 = 10^3 + 9^3 = 12^3 + 1^3$ □

Constructive existence proofs are really just instances of “existential generalization.”

A non-constructive existence proof

Prove: Show that there exist two irrational numbers x and y such that x^y is rational.

Proof:

Note: We don't know whether $\sqrt{2}^{\sqrt{2}}$ is rational or irrational. However, in either case, we can use it to construct a rational number.

Sometimes, existence is not enough, and we need to prove uniqueness

This process has two steps:

1.
2.

Example: Prove that if a and b are real numbers, then there exists a unique real number r such that $ar + b = 0$

Existence

Proof:

- Note that $r = -b/a$ is a solution to this equality since $a(-b/a) + b = -b + b = 0$.
- Assume that $as + b = 0$
- Then $as = -b$, so $s = -b/a = r$, which means s is just r □

Uniqueness

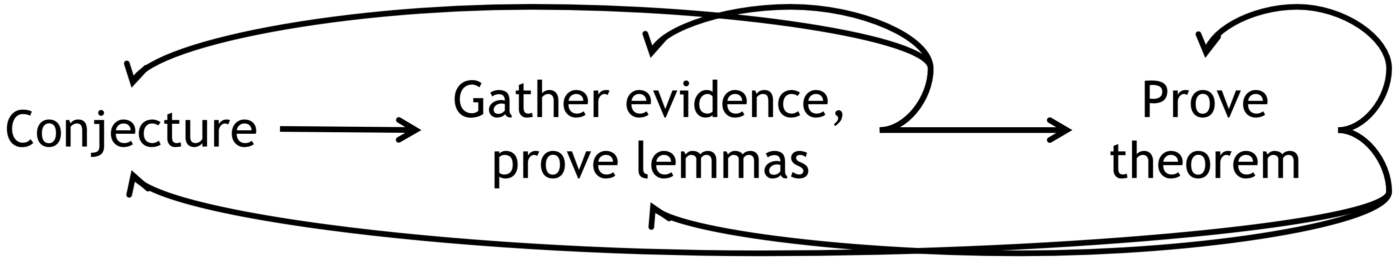
In-class exercises

Problem 1: Prove that there exists a positive integer that is equal to the sum of all positive integers less than it. Is your proof constructive or non-constructive?

Problem 2: Prove that there is no positive integer n such that $n^2 + n^3 = 100$.

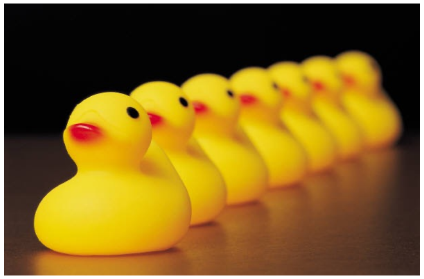
Top Hat

The scientific process is not always straightforward…



Proof strategies can help preserve your sanity

Proof strategies help us…



Organize our problem solving approach

Effectively use all of the tools at our disposal

Develop a coherent plan of attack

Types of proof strategy

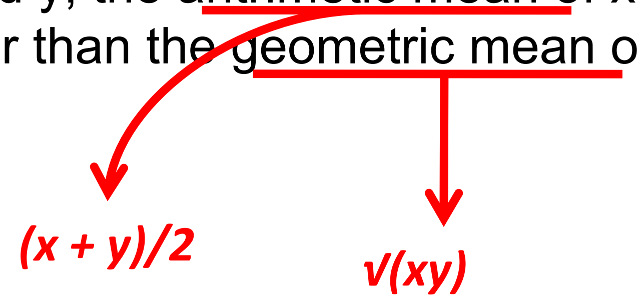
Today we’ll discuss four types of strategy:

1. Forward reasoning
2. Backward reasoning
3. Searching for counterexamples
4. Adapting existing proofs

Sometimes forward reasoning doesn't work

In these cases, it is often helpful to reason backwards, starting with the goal that we want to prove.

Example: Prove that given two distinct positive real numbers x and y, the arithmetic mean of x and y is always greater than the geometric mean of x and y.



$(x + y)/2$

$\sqrt{(xy)}$

Sanity check: Let x=8 and y=4. $(8+4)/2 = 6$. $\sqrt{(8 \times 4)} = \sqrt{(32)} \cong 5.66$. $6 > 5.66$ ✓

Prove that $(x+y)/2 > \sqrt{(xy)}$ for all distinct pairs of positive real numbers x and y.

Proof:

$(x + y)/2 > \sqrt{(xy)}$

$(x + y)^2/4 > xy$

$(x + y)^2 > 4xy$

$x^2 + 2xy + y^2 > 4xy$

$x^2 - 2xy + y^2 > 0$

$(x – y)^2 > 0$

$(x-y) > 0$

$x > y$

Since $(x – y)^2 > 0$ whenever $x \neq y$, the final inequality is true. Since all of these inequalities are equivalent, it follows that $(x + y)/2 > \sqrt{(xy)}$. □

Other times, searching for a counterexample is helpful

Proof by counterexample is helpful if:

- Proof attempts repeatedly fail
- The conjecture to be proven looks “funny”

Example: Prove that every positive integer is the sum of two squares.

This seems suspicious to me, since other factorizations (e.g., prime factorizations) can be complex.

Counterexample:

3 is not the sum of two squares, so the claim is false. □

These four proof strategies are just a start!

A great tool for programmers AND logicians!

When trying to prove a new conjecture, a good "meta strategy" is to:

1. If possible, try to reuse an existing proof (analogy!)
2. If the conjecture looks fishy, check for a counterexample
3. Attempt a "real" proof
   a) Apply the forward reasoning strategy
   b) Or, apply the backward reasoning strategy
   c) Possibly alternate between forward and backward reasoning

Unfortunately, not every proof can be solved using this nice little meta strategy…

In fact, there are many, many proof strategies out there, and NONE of them can be guaranteed to find a proof!

Final Thoughts

- Proving theorems is not always straightforward
- Having several proof strategies at your disposal will make a huge difference in your success rate!
- We are “done” with our intro to logic and proofs
- Next lecture:
  - Intro to set theory
  - Please read sections 2.1 and 2.2