EECS 2001A : Introduction to the Theory of Computation

Suprakash Datta

Course page: `http://www.eecs.yorku.ca/course/2001`
Also on Moodle

Proofs

- What is a proof?
- Does a proof need mathematical symbols?
- What makes a proof incorrect?
- How does one come up with a proof?

Proof techniques

- Direct Proofs
- Proof by cases
- Proof by contrapositive
- Proof by contradiction
- Proof by induction
- Others ...

Direct Proofs: Example

Proposition: Every prime number greater than 2 can be written as the difference of two squares, i.e. $a^2 - b^2$.

- Question: where do we start?
- We know how $a^2 - b^2$ factors. Let us start there.
- $a^2 - b^2 = (a+b)(a-b)$. We have to assume $a > b$ because $a^2 - b^2$ must be positive. A prime $p > 2$ only factors as $p * 1$.
- Equating factors, $a - b = 1$, $a + b = p$. Solving, $a = \frac{p+1}{2}, b = \frac{p-1}{2}$. Since all primes $p > 2$ are odd, a, b are integers.

Proof by Cases

Prove: If n is an integer, then $\frac{n(n+1)}{2}$ is an integer

Case 1: n is even. or $n = 2a$, 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. So $n+1$ is even, or $n+1 = 2a$, for an integer a So $n(n+1)/2 = n * 2a/2 = n * a$, which is an integer.

Alternative argument: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. The sum of the first n integers must be an integer itself.

Proof by Cases: Caution

What is being proved must be true in ALL cases, not some!

Proof by contrapositive

Logical Basis: Any implication $p \to q$ is logically equivalent to its contrapositive $\neg q \to \neg p$

Claim: If $\sqrt{pq} \neq (p+q)/2$, then $p \neq q$

- Direct proof involves some algebraic manipulation

- Contrapositive: If $p = q$, then $\sqrt{pq} = (p+q)/2$.
  Easy: Assuming $p = q$, we see that
  $\sqrt{pq} = \sqrt{pp} = \sqrt{p^2} = p = (p+p)/2 = (p+q)/2$.

Exercise: prove that for all $a \in \mathbb{Z}$, if a^2 is even, then a is even

Proof by contradiction

Claim: $\sqrt{2}$ is irrational
Proof: Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = p/q$, $p, q \in \mathbb{Z}, q \neq 0$, such that p, q have no common factors.
Squaring and transposing,
$p^2 = 2q^2$ (so p^2 is an even number)
So, p is even (previous slide)
Or $p = 2x$ for some integer x
So $4x^2 = 2q^2$ or $q^2 = 2x^2$
So, q is even (a previous slide)
So, p, q are both even i.e., they have a common factor of 2.
CONTRADICTION.
So $\sqrt{2}$ is NOT rational.

Proofs by Contradiction: Rationale

- In general, start with an assumption that statement A is true. Then, using standard inference procedures infer that A is false. This is the contradiction.

- This A may or not be what you are trying to prove (e.g. in the example, the contradiction was on the fact that the numerator and denominator had no common factors)

- Recall: for any proposition p, $p \wedge \neg p$ must be false.

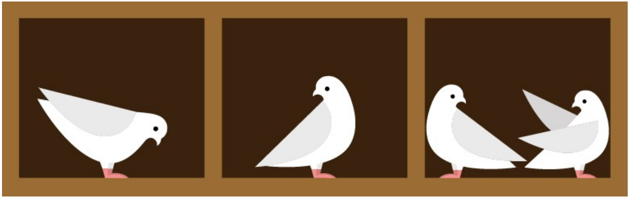
More Complex Proof Techniques

Proof by using special results, e.g.,

- Using the Pigeonhole Principle

- Proof by Induction

Pigeonhole Principle



https://www.ethz.ch/en/news-and-events/eth-news/news/2016/05/creative-proofs-with-pigeons-and-boxes.html

Two statements:

- Pigeonhole Principle: If $n+1$ balls are distributed among n bins then at least one bin has more than 1 ball
- Generalized Pigeonhole Principle: If n balls are distributed among k bins then at least one bin has at least $\lceil n/k \rceil$ balls

Lots of interesting (and difficult) problems!

Examples

Pigeonhole Principle

- In any group of 367 people, at least 2 people must share a birthday
- In any group of 27 English words, at least 2 must start with the same letter
- In a class of 22 people, at least 2 must get the same score on a test out of 20, assuming all scores are integers

Generalized Pigeonhole Principle

- If there are 16 people and 5 possible grades, 4 people must have the same grade.
- There are 50 baskets of apples. Each basket contains no more than 24 apples. So there are at least 3 baskets containing the same number of apples.

Proofs by Induction

Mathematical Induction:

- Very simple

- Very powerful proof technique

- “Guess and verify” strategy

Induction: Steps

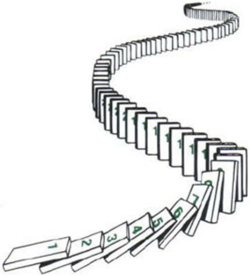
Hypothesis: $P(n)$ is true for all $n \in \mathbb{N}$

- Base case/basis step (starting value):
  Show $P(1)$ is true.
- Inductive step:
  Show that $\forall k \in \mathbb{N}(P(k) \to P(k+1))$ is true.

Induction: Rationale

Formally: $(P(1) \wedge \forall k \in \mathbb{N} P(k) \rightarrow P(k+1)) \rightarrow \forall n \in \mathbb{N} P(n)$

- Intuition: Iterative modus ponens:
  $P(k) \wedge (P(k) \rightarrow P(k+1)) \rightarrow P(k+1)$
  Need a starting point (Base case)



Induction: Example 1

$P(n): 1 + 2 + \ldots + n = n(n+1)/2$

- Base case: $P(1)$.
  LHS $= 1$. RHS $= 1(1+1)/2 =$ LHS
- Inductive step:
  Assume $P(n)$ is true. Show $P(n+1)$ is true.
  Note:

$$\begin{aligned} 1 + 2 + \ldots + n + (n+1) &= n(n+1)/2 + (n+1) \\ &= (n+1)(n+2)/2 \end{aligned}$$

So, by the principle of mathematical induction, $\forall n \in \mathbb{N}, P(n)$.

Induction: Example 2

$P(n) : 1^2 + 2^2 + \ldots + n^2 = n(n+1)(2n+1)/6$

- Base case: $P(1)$.
  LHS $= 1$. RHS $= 1(1+1)(2+1)/6 = 1 =$ LHS
- Inductive step:
  Assume $P(n)$ is true. Show $P(n+1)$ is true.
  Note:

$$\begin{aligned} 1^2 + 2^2 + \ldots + n^2 + (n+1)^2 &= n(n+1)(2n+1)/6 + (n+1)^2 \\ &= (n+1)(n+2)(2n+3)/6 \end{aligned}$$

So, by the principle of mathematical induction, $\forall n \in \mathbb{N}, P(n)$.

Induction: Proving Inequalities

$P(n) : n < 4^n$

- Base case: $P(1)$.
  $P(1)$ holds since $1 < 4$.
- Inductive step:
  Assume $P(n)$ is true, show $P(n+1)$ is true, i.e.,
  show that $n + 1 < 4^{n+1}$:

$$\begin{aligned} n+1 &< 4^n + 1 \\ &< 4^n + 4^n \\ &< 4.4^n \\ &= 4^{n+1} \end{aligned}$$

So, by the principle of mathematical induction, $\forall n \in \mathbb{N}, P(n)$.

Induction: More Examples

- Sum of odd integers
- $n^3 - n$ is divisible by 3
- Number of subsets of a finite set

Induction: Facts to Remember

- Base case does not have to be $n = 1$
- Most common mistakes are in not verifying that the base case holds
- Usually guessing the solution is done first

How can you guess a solution?

Depends on the problem.

- Try simple tricks: e.g. for sums with similar terms: n times the average or n times the maximum; for sums with fast increasing/decreasing terms, some multiple of the maximum term
- Often proving upper and lower bounds separately helps
- If nothing else works, make educated guesses

Strong Induction

Sometimes we need more than $P(n)$ to prove $P(n+1)$; in these cases STRONG induction is used.
Formally:

$$[P(1) \land \forall k(P(1) \land \ldots \land P(k-1) \land P(k)) \rightarrow P(k+1))] \rightarrow \forall n P(n)$$

Note: Strong Induction is:

- Equivalent to induction – use whichever is convenient
- Often useful for proving facts about algorithms

Strong Induction: Examples

- Fundamental Theorem of Arithmetic: every positive integer n, $n > 1$, can be expressed as the product of one or more prime numbers.
- every amount of postage of 12 cents or more can be formed using just 4-cent and 5-cent stamps.

Fallacies/caveats: "Proof" that all Canadians are of the same age!
http://www.math.toronto.edu/mathnet/falseProofs/sameAge.html

A Graph Example

Claim: A tree with n nodes has exactly $n-1$ edges

- Consider any node a in the tree, connected by edges to $k \geq 1$ nodes, each of which is part of a tree. Remove the node and these k edges
- Let the size of the k trees be $n_1, \ldots, n_k$
- By the inductive hypothesis the total number of edges in these trees are $n_1 - 1 + \ldots + n_k - 1 = n_1 + \ldots + n_k - k$
- Now add the removed node and the k edges. So the number of nodes $n = n_1 + \ldots + n_k + 1$ and the number of edges is $n_1 + \ldots + n_k - k + k = n - 1$

Proofs vs Counterexamples

To prove quantified statements of the form

- $\forall x P(x)$: an example (or 10) x for which $P(x)$ is true is/are NOT enough; a proof is needed
- $\exists x P(x)$: an example x for which $P(x)$ is true is enough.

To DISPROVE quantified statements of the form

- $\forall x P(x)$: a COUNTERexample x for which $P(x)$ is false is enough
- $\exists x P(x)$: an example x for which $P(x)$ is false is NOT enough; a proof is needed

Intuition:

Disproving $(\forall x)P(x)$ means proving $\neg(\forall x)P(x) \equiv (\exists x)\neg P(x)$

Proofs vs Counterexamples - 2

If you try to prove universally quantified statements of the form $\forall x P(x)$ with an example

- You will likely see a comment "proof by example!" on your answer, and

- get little or no credit