EECS 1028 M: Discrete Mathematics for Engineers

Suprakash Datta
Office: LAS 3043

Course page: `http://www.eecs.yorku.ca/course/1028`
Also on Moodle

Proofs

Sec 1.7-1.8, 5.1-5.2

Key questions:

- Why are proofs necessary?
- What is a (valid) proof?
- What can we assume? In what level of detail and rigour do we prove things?

Caveat: In order to prove a statement, it MUST be True!

Assertion Types

Domain: e.g., $\mathbb{R}$

- Axioms
- Proposition, Lemma, Theorem
- Corollary
- Conjecture

Types of proofs

- Direct proofs (including Proof by cases)
- Proof by contraposition
- Proof by contradiction
- Proof by construction
- Proof by Induction (Ch 5.1-5.2)
- Other techniques

Direct proofs

Simplest technique. Two examples:

- The average of any two primes greater than 2 is an integer
- Every prime number greater than 2 can be written as the difference of two squares, i.e. $a^2 - b^2$.

Direct Proofs: Example 1

Proposition: The average of any two primes greater than 2 is an integer

- All primes greater than 2 must be odd, because otherwise they would be divisible by 2 and therefore not prime

- The average of 2 odd numbers is an integer because the sum of two odd integers is an even number and thus divisible by 2.

Direct Proofs: Example 2

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 (last slide) 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: Logical Basis

Prove q is true by cases.

Case 1: p is true.
Prove q

Case 2: p is false (i.e., $\neg p$ is true).
Prove q

So we have $p \to q$ and $\neg p \to q$.

Rationale 1: Simplify $(p \to q) \wedge (\neg p \to q)$. You will get q
Rationale 2: Apply resolution on $p \to q$ and $\neg p \to q$. You can infer q

Proofs by Contrapositive

Logical Basis: Any statement is logically equivalent to its contrapositive

- 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
    $\sqrt{pq} = \sqrt{pp} = \sqrt{p^2} = p = (p+p)/2 = (p+q)/2$.

Proofs by Contradiction

Prove: $\sqrt{2}$ 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 (a 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.
- Recall: for any proposition p, $p \wedge \neg p$ must be false.
- Difference between proofs by contradiction, contrapositives: Former proves a statement, latter proves a conditional However we can view proof by contradiction as proving a conditional: to prove p, we show that $\neg p \rightarrow p$. This is logically equivalent to $p \vee p \equiv p$

Proofs by Contradiction: More Examples

- 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

Proofs by Construction

aka Existence proofs

- Prove: There exists integers x, y, z satisfying $x^2 + y^2 = z^2$
  Proof: $x = 3, y = 4, z = 5$.

- There exists irrational b, c, such that b^c is rational (page 97).
  (Nonconstructive) Proof: Consider $\sqrt{2}^{\sqrt{2}}$. Two cases are possible:
  $\sqrt{2}^{\sqrt{2}}$ is rational: DONE ($b = c = \sqrt{2}$).
  $\sqrt{2}^{\sqrt{2}}$ is irrational: Let $b = \sqrt{2}^{\sqrt{2}}, c = \sqrt{2}$.
  Then $b^c = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = (\sqrt{2})^{\sqrt{2} * \sqrt{2}} = (\sqrt{2})^2 = 2$.

Proofs of Uniqueness

- the equation $ax + b = 0$, $a, b \in \mathbb{R}$, $a \neq 0$ has a unique solution.

- Show that if n is an odd integer, there is a unique integer k such that n is the sum of k-2 and k+3.

The Use of Counterexamples

- All prime numbers are odd

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

Examples

- Prove that there are no solutions in positive integers x and y to the equation $2x^2 + 5y^2 = 14$.
- If x^3 is irrational then x is irrational.
- Prove or disprove: if x, y are irrational, $x + y$ is irrational.

Alternative problem statements

- “show A is true if and only if B is true”
- “show that the statements A,B,C are equivalent”
- Try: Q8, 10, 26, 28 on page 91

The role of conjectures

- Not to be used frivolously

- Example: $3x + 1$ conjecture.
  Game: Start from a given integer n. If n is even, replace n by $n/2$. If n is odd, replace n with $3n + 1$. Keep doing this until you hit 1.
  e.g. $n = 5 \Rightarrow 16 \Rightarrow 8 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1$
  Q: Does this game terminate for all n?
  $3x + 1$ conjecture: Yes!

Elegance in proofs

Example: Prove that the only pair of positive integers satisfying $ab = a + b$ is $(2, 2)$.

- Many different proofs exist. What is the simplest one you can think of?

Elegance in proofs

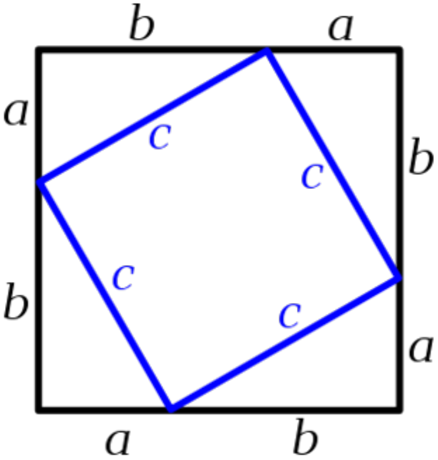
Example: Prove that the only pair of positive integers satisfying $ab = a + b$ is $(2, 2)$.

- Many different proofs exist. What is the simplest one you can think of?
-

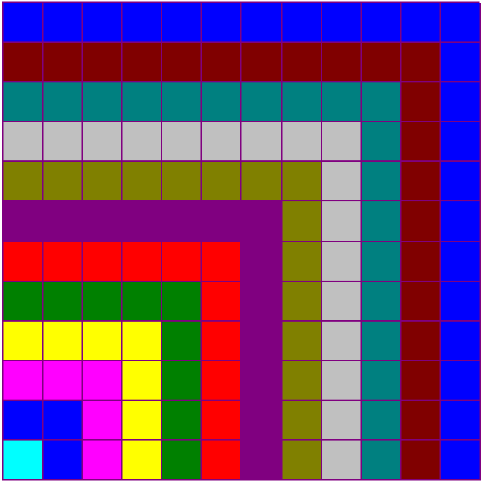
$$\begin{aligned} ab &= a + b \\ ab - a - b &= 0 \\ ab - a - b + 1 &= 1 \text{ adding 1 to both sides} \\ (a-1)(b-1) &= 1 \text{ factoring} \end{aligned}$$

Since the only ways to factorize 1 are $1 * 1$ and $(-1) * (-1)$, the only solutions are $(0, 0), (2, 2)$.

Meaningful Diagrams - 1

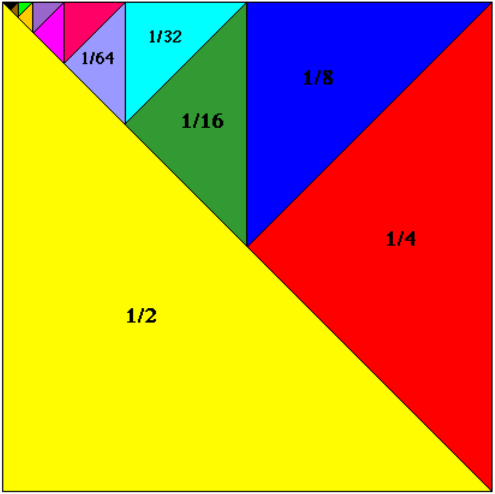


Meaningful Diagrams - 2



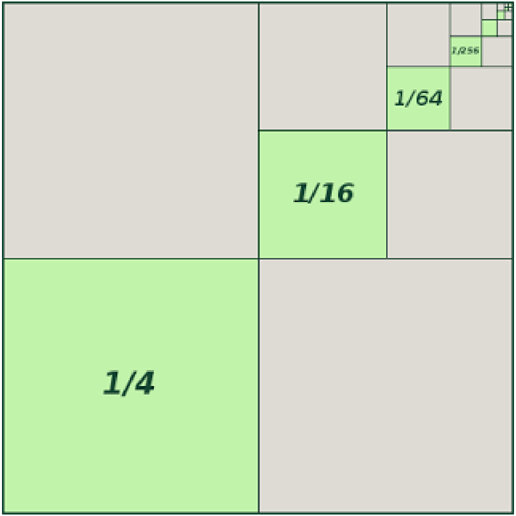
from https://www.math.upenn.edu/~deturck/probsolv/LP1ans.html

Meaningful Diagrams - 3



from http://math.rice.edu/~lanius/Lessons/Series/one.gif

Meaningful Diagrams - 3



from http://www.billthelizard.com/2009/07/six-visual-proofs_25.html

Proofs by Induction (Ch 5.1)

Mathematical Induction:

- Very simple
- Very powerful proof technique
- "Guess and verify" strategy

Induction: Steps

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

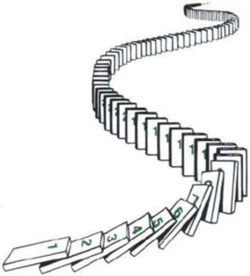
- Base case/basis step (starting value):
  Show $P(1)$ is true.

- Inductive step:
  Show that $\forall k \in \mathbb{N}(P(k) \rightarrow P(k+1))$ 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)

- Proof is beyond the scope of this course

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?

- 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.

Strong Induction (Ch 5.2)

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

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

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`