CS 5319
Advanced Discrete Structure

Lecture 7:
Methods of Proving

Outline

- Mathematical Induction
- Proof by Contradiction
- Proof by Construction

Mathematical Induction

Mathematical Induction

- Usually, we want to show a general statement $P(n)$ is true for infinite values of n
- One powerful method is called induction
- Idea :
  - Show $P(n)$ is true for some base case $n = k$
  - Show $P(n+1)$ is true if $P(n)$ is true
- The combined effect will be:
  - $P(n)$ is true for all $n = k, k+1, k+2, \ldots$

Mathematical Induction

Ex : Show that for all $n \geq 1$

$$1 + 2 + \ldots + n = n\,(n+1)\,/\,2$$

Ex : Let F_n denote the nth Fibonacci number, where $F_1 = 1$, $F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$.

Show that

$$F_1^{\,2} + F_2^{\,2} + \ldots + F_n^{\,2} = F_n F_{n+1}$$

Mathematical Induction

Ex : In any set of n horses, all horses are of the same color

Proof :

- Base Case: The statement is true for $n = 1$.
- Inductive Case:

  Assume $P(n)$ is true. Then we take any set of $n+1$ horses, and remove one of them.
  The remaining horses are of the same color (because $P(n)$ is true).

Mathematical Induction

- Inductive Case (cont):

  Next, we put back the removed horse into the set, and remove another horse

  In this new set, all horses are of same color (because $P(n)$ is true).

  Therefore, all horses are of the same color.

- What's wrong with the proof ?

Mathematical Induction

- There can be other variations for the induction
- "Strong" Induction :
  - Show $P(n)$ is true for some base case $n = k$
  - Show $P(n+1)$ is true if $P(k)$, $P(k+1)$, …, $P(n)$ are all true
- Backward Induction :
  - Show $P(n)$ is true for infinite # of base cases
  - Show $P(n-1)$ is true if $P(n)$ is true

Mathematical Induction

Ex : The Josephus Problem

We have n people labeled 1 to n around a circle. We eliminate every *second* remaining person until only one survives.

E.g., If $n = 6$, order of people eliminated is :

(2, 4, 6, 3, 1) ➔ person 5 survives.

Let $J(n)$ denote the label of the survivor.

Show that $J(n) = 2k + 1$ where $2^m \leq n = 2^m + k$

Mathematical Induction

Ex : The AM-GM Inequality

Let a_1, a_2, …, a_n be any n non-negative #s

Show that

$$(a_1 + a_2 + \ldots + a_n) / n$$
$$\geq \quad (a_1 a_2 \ldots a_n)^{1/n}$$

with equality holds when all #s are equal

Hint: Show that it is true for all n = powers of 2.

Show that $P(n)$ is true implies $P(n–1)$

Proof by Contradiction

Proof by Contradiction

- In logic, the following two statements are equivalent :

  (1) $P \rightarrow Q$; (2) $\neg Q \rightarrow \neg P$

- This means: the two statements will always have the same truth value
- If we want to show $P \rightarrow Q$ is true, we may try to show $\neg Q \rightarrow \neg P$ is true instead
  - This method is called indirect proof

Proof by Contradiction

- A special type of indirect proof is called proof by contradiction
  - Recall: contradiction = "always false"

    tautology = "always true"
- To show a statement P is true, we instead show

  $$\neg P \rightarrow \text{FALSE} \quad \text{(or, contradiction)}$$

  is true
- This method works because

  $$\neg P \rightarrow \text{FALSE} \quad \Leftrightarrow \quad \text{TRUE} \rightarrow P \quad \Leftrightarrow \quad P$$

Proof by Contradiction

Ex : Show that $\sqrt{2}$ is irrational.

- Suppose on the contrary that $\sqrt{2}$ is rational
- Then there exists integers p and q such that

$$\sqrt{2} = p / q$$

- Without loss of generality, we may restrict that gcd(p, q) = 1
- Now, the above equation implies that

$$2q^2 = p^2$$

Proof by Contradiction

- This implies that p is an even number
- So we let $p = 2k$, and then we have

$$2q^2 = p^2 = (2k)^2 = 4k^2 \quad \rightarrow \quad q^2 = 2k^2$$

which implies q is also an even number

- At this moment, a contradiction occurs (where?)
- More precisely, the statement

“$\sqrt{2}$ is rational”

leads to a contradiction, so that its negation must be true → The proof completes.

Proof by Contradiction

Ex : Show that there are infinite number of primes.

- Suppose on the contrary that the number of primes are finite (say, there are *k* of them)
- Let $p_1, p_2, \ldots, p_k$ denote all the primes
- Consider the integer $Q = p_1 p_2 \ldots p_k + 1$
- Q is not divisible by any of the *k* primes

  ➔ It has a prime factor not in $\{ p_1, p_2, \ldots, p_k \}$
- Thus a contradiction occurs (where?) and the proof completes

Proof by Contradiction

Ex : (The Pigeonhole Principle)

If $k + 1$ or more objects are placed into k boxes, then at least one box contains two or more objects.

- Suppose no boxes contain two or more objects
- Then the total number of objects is at most k
- Contradiction occurs and the proof completes

Proof by Contradiction

Ex : (The Generalized Pigeonhole Principle)

If N objects are placed into k boxes, then at least one box contains at least $\lceil N/k \rceil$ objects

- Suppose no boxes contain at least $\lceil N/k \rceil$ objects
- Then the total # objects is at most $k\,(\lceil N/k \rceil - 1)$
- Since for any r, $\lceil r \rceil < r + 1$,

$$k\,(\lceil N/k \rceil - 1) \;<\; k\,(N/k + 1 - 1) = N$$

so that the total # objects is less than N

- Contradiction occurs, and the proof completes

Applications of Pigeonhole

Q1: In a group of 6 people where each pair are either friends or strangers, show that we can find 3 mutual friends or 3 mutual strangers.

Q2: Show that there is a number of the form 111…1 which is a multiple of 2009.

Q3: Show that in a sequence of $n^2 + 1$ distinct numbers, we can find an increasing or a decreasing subsequence of length $n + 1$

Applications of Pigeonhole

Q4: Show that in any 51 numbers chosen from {1,2, …, 100}, there must be one number that can divide another.

Q5: Consider a sequence of 30 positive integers whose total sum is at most 45.

Show that we can find a contiguous sequence whose sum is exactly 14.

Applications of Pigeonhole

Q6 : Consider two necklaces that are made with black or white beads.

It is known that one necklace has exactly 50 white beads and 50 black beads.

Show that no matter how the second necklace is, there exists an orientation such that both necklaces agree at 50 or more positions.

Proof by Construction

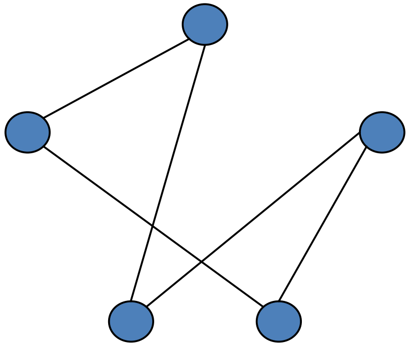
Proof by Construction

- Many theorem states that a particular type of objects exists
- One way to prove is to find a procedure to construct such an object
- Such a method is called proof by construction
- This method is also used in proving many interesting results that arise in geometry

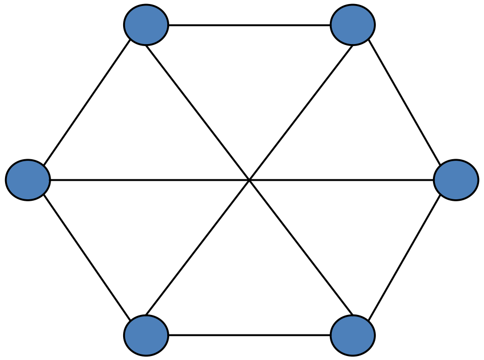
Proof by Construction

- A graph is k-regular if every vertex has degree k

  E.g.,



2-regular



3-regular

Ex: Show that for each even $n \geq 4$, there exists a graph with n vertices which is 3-regular

Proof by Construction

Ex : There exists a rational number *p* which can be expressed as q^r such that *q* and *r* are both irrational

Hint: What is the following value?

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}}$$

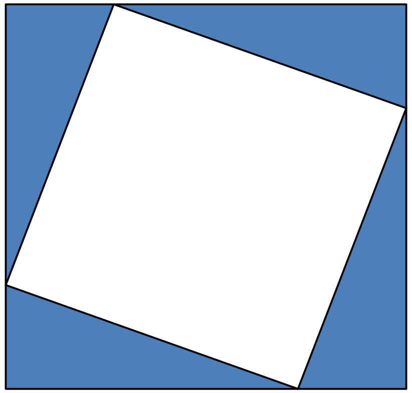
Proof by Construction

Ex : Pythagoras's Theorem

For any right-angled triangle with sides of lengths a, b, and c (where c is the length of the hypotenuse), we have

$$a^2 + b^2 = c^2.$$

Ans :



Area of "big" square

$= (a + b)^2$

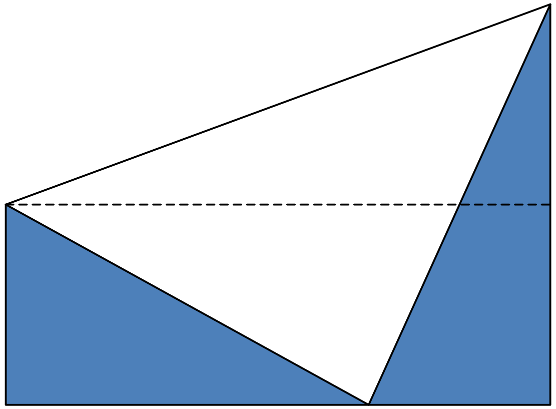
$= c^2 + 4\,(ab/2)$

Proof by Construction

Ex : Show that

$$\tan^{-1}(1/3) + \tan^{-1}(1/2) = \pi / 4$$

Ans :



Proof by Construction

Ex : A set S is called countable if its size is finite, or if there exists a one-to-one correspondence between the items in S and the numbers in the natural number set $\mathcal{N} = \{ 1, 2, 3, \dots \}$

Show that the following sets are countable.

1. $\mathcal{E} = \{$ all even numbers $\}$
2. $\mathcal{P} = \{$ all prime numbers $\}$
3. A subset of a countable set
4. $\mathcal{Q} = \{$ all rational numbers $\}$

A Mixture of Proof Techniques

Ex : Show that the set $\mathcal{R}$ of all real numbers is not countable.

A : It is sufficient to show that the set $\mathcal{R}$' of all real numbers in (0,1) is not countable (why?).

Suppose on the contrary that it is countable.

Then there is a one-to-onecorrespondence between $\mathcal{R}$' and $\mathcal{N}$. We list the real numbers according to their correspondence in $\mathcal{N}$.

Let $x_k = k$ th real number in the list

A Mixture of Proof Techniques

- Construct x whose kth digit is equal to “the kth digit of x_k” (mod 2) + 1

E.g.	x_1	0.7182818284590452354…
	x_2	0.4426950408889634074…
	x_3	0.14159265358979323846…
	x_4	0.41421356237309504880…
	x_5	0.5000000000000000000…
		⋮
	$x =$	0.21211…

- x is in (0,1) but without any correspondence

➔ contradiction occurs and the proof completes