Prerequisite and Review

Imdad ullah Khan

Prerequisites

You must have "passed" Discrete Mathematics and Algorithms

The course is fast-paced and assume experience with mathematical reasoning and algorithmic thinking

You should be comfortable with

- Propositional Logic
- Predicates and Quantifiers
- Set Theory and Countability
- Functions and Cross Product
- Relations, Equivalence and Partial Order
- Proofs
- Induction
- Algorithm Analysis
- Asymptotic Notation
- Graph Algorithms
- Divide and Conquer Algorithm
- Recursion and Recurrences
- Dynamic Programming
- Complexity and NP-Completeness

Proposition

A statement is a description of something

A proposition is a statement that is either **true** or **false** and not both and not neither

- We can make (compound) propositions from others
- Negation a proposition
- Proposition made by combining two propositions with AND, OR, XOR, IF-THEN, IFF
- $P \rightarrow Q$ is false when P is true and Q is false
- The **converse** of $P \rightarrow Q$ is $Q \rightarrow P$
- The **contrapositive** of $P \rightarrow Q$ is $\neg Q \rightarrow \neg P$
- The **inverse** of $P \rightarrow Q$ is $\neg P \rightarrow \neg Q$

Quantified Expression: Summary

- A predicate is a property that is true or false about the subject(s)
- $P(x)$ is the value of propositional function P at x
- $P(x)$ becomes proposition when specific value are assigned to x
- Quantifiers make it proposition for a range of values

- **Universal Quantifier:** $\forall$
  - $\forall x\ P(x) \quad := \quad P(x)$ (is true) for all values of x in the UoD

Proposition $\forall x\ P(x)$ is **True** iff for every x in UoD, $P(x)$ is **True**

- **Existential Quantifier:** $\exists$
  - $\exists x\ P(x) \quad := \quad P(x)$ (is true) for some value(s) of x in the UoD

Proposition $\exists x\ P(x)$ is **True** iff for at least one x in UoD, $P(x)$ is **True**

Truth Values of Nested Quantified Expressions

Statement	*When True?*	*When False?*
$\forall x \forall y\ P(x,y)$ $\forall y \forall x\ P(x,y)$	$P(x,y)$ is true for every pair x,y	There is a pair x,y for which $P(x,y)$ is false
$\forall x \exists y\ P(x,y)$	For every x, there is a y for which $P(x,y)$ is true	There is an x such that $P(x,y)$ is false for every y
$\exists x \forall y\ P(x,y)$	There is an x for which $P(x,y)$ is true for every y	For every x there is a y for which $P(x,y)$ is false
$\exists x \exists y\ P(x,y)$ $\exists y \exists x\ P(x,y)$	There is a pair x,y for which $P(x,y)$ is true	$P(x,y)$ is false for every pair x,y

Negating Nested Quantified Expressions

Recall $\neg \forall x \, P(x) \equiv \exists x \, \neg P(x)$ $\neg \exists x \, P(x) \equiv \forall x \, \neg P(x)$

Negate nested quantified statements using iterative applications of negating (singly) quantified statements

$$\neg \forall x \, \exists y \, P(x,y) \equiv \exists x \, \neg \exists y \, P(x,y) \equiv \exists x \, \forall y \, \neg P(x,y)$$

$$\neg \exists x \, \forall y \, P(x,y) \equiv \forall x \, \neg \forall y \, P(x,y) \equiv \forall x \, \exists y \, \neg P(x,y)$$

$$\neg \forall x \, \forall y \, P(x,y) \equiv \exists x \, \neg \forall y \, P(x,y) \equiv \exists x \, \exists y \, \neg P(x,y)$$

$$\neg \exists x \, \exists y \, P(x,y) \equiv \forall x \, \neg \exists y \, P(x,y) \equiv \forall x \, \forall y \, \neg P(x,y)$$

Sets Summary

- A set is an ordered collection of objects
- Order and repetition of objects do not matter
- Sets can be described in various ways
- Empty set is a well-defined set with zero objects
- Two sets are equal if and only if they have the same elements
- $\overline{A}$ is the collection of all objects in universal set that are not in A
- Cardinality of A is the number of distinct elements in A

Subsets: Summary

- A is a subset of B if and only if every element of A is an element of B
- $A \subseteq B$, A is subset of B, B is superset of A
- Empty set is a subset of every set
- Every set is a subset of itself
- Power Set of A is the set of all subsets of A
- Cardinality of power set of A with $|A| = n$ is 2^n

Set Operations

- Set Operation (Binary)
  - Union
  - Intersection
  - Difference
  - Symmetric Difference
- Generalized Union
- Generalized Intersection

Set Equality

- Equality of two sets can be proved using
  - Algebraic Rules (Set Identities)
  - Set Membership Tables
  - Logical Equivalence of membership predicates
  - By proving bidirectional subset relationships

Ordered Tuples and Cartesian Product: Summary

- Ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is an ordered collection of n objects
- $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ means $a_i = b_i$ for $1 \leq i \leq n$
- Ordered 2-tuples ($n = 2$) are called ordered pairs
- Cartesian product of sets A and B, $A \times B$ is
  the set of all ordered pairs (x, y), where $x \in A$ and $y \in B$
- Cartesian product can be generalized to that of more than 2 sets
- $\big|A_1 \times A_2 \times \ldots \times A_n\big| \; = \; |A_1| \times |A_2| \times \ldots \times |A_n|$

Functions: Summary

- $f : X \mapsto Y$ maps **each** element of X to **exactly one** element of Y

Let $f : X \mapsto Y$ and let $f(x) = y$

- X is the domain of f
- Y is the codomain of f
- y is the image of x
- x is the pre-image of y
- Range of f: set of images of all elements of X

- Functions can be represented by
  - Listing set of all (pre-image, image) ordered pairs
  - Bipartite Graph
  - Mapping Rule or Algebraic Expression
  - Programming Code

Types of functions: Summary

A function $f : X \mapsto Y$ is **one-to-one** (or **injective**) iff

$$\forall\, x_1, x_2 \in X\ (f(x_1) = f(x_2) \to x_1 = x_2)$$

A function $f : X \mapsto Y$ is **onto** (or **surjective**) iff

for every element $y \in Y$ there is an element $x \in X$ with $f(x) = y$

A function $f : X \mapsto Y$ is **one-to-one correspondence** (or **bijective**) iff

it is **both one-to-one** and **onto**

If $f : X \mapsto Y$ is a bijection and X and Y are finite sets, then $|X| = |Y|$

Relations: Summary

- A (binary) relation from X to Y is a subset of $X \times Y$
- A (binary) relation on a set X is a subset of $X \times X$ (relation from X to X)
- An n-ary relation is a subset of $A_1 \times A_2 \times \ldots \times A_n$
- A binary relation can be represented by listing the ordered pairs, using a bipartite graph, or with a binary matrix

Properties of Relations: Summary

- A relation R on a set X is **reflexive** if $(a, a) \in R$ for every element $a \in X$
- A relation R on a set X is **symmetric** if $(b, a) \in R$ whenever $(a, b) \in R$ for all $a, b \in X$
- A relation R on a set X is **antisymmetric** if $a = b$ whenever $(a, b) \in R$ and $(b, a) \in R$
  - ▷ A relation can be symmetric, antisymmetric, both or none
- A relation R on a set X is transitive if whenever $(a, b) \in R$ and $(b, c) \in R$ then $(a, c) \in R$

Equivalence Relation

Equivalence Relation

A relation R on a set X is an equivalence relation if it is

1. reflexive
2. symmetric, and
3. transitive

- Relates "similar" elements
- Generalize "equality"

Partial Order

Partial Order

A relation R on a set X is a **partial order** if it is

1. reflexive,
2. antisymmetric, and
3. transitive

Partial orders give an order to sets that may not have a natural one.

For example pre-requisite order to courses

Notation: $a \preccurlyeq b \leftrightarrow (a, b) \in R$ and $a \prec b \leftrightarrow (a, b) \in R, a \neq b$

Pronounced as a **preceeds** b

Do not confuse $\preccurlyeq$ with $\leq$ $\quad$ $\preccurlyeq$ denotes partial ordering

Proofs

An argument that convincingly demonstrates the truth of a statement

In mathematics,

A proof is a chain of logical deductions that demonstrates the truth of a proposition assuming the truth of some known axioms

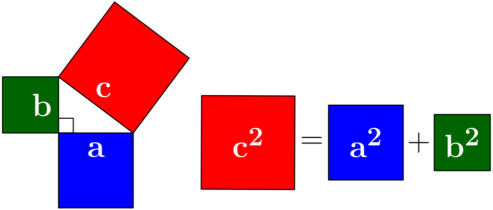
Terminology

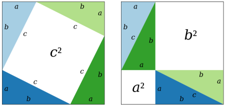
- **Axiom:** A basic assumption about mathematical structure that is accepted to be true. e.g.
  - *There is a straight line between any two points*
  - $2 > 1$
- **Theorem:** Important proposition that has a proof
- **Lemma:** Proposition that serves as an intermediate step in proof of a theorem
- **Corollary:** Proposition that follows directly (easily) from a theorem
  - Essentially a special case of the general statement of the theorem
- **Rules of Inference:** The justification for the steps in the chain of deductions in a proof
- **Fallacy:** An incorrect reasoning or deduction

Proving Statements

Pythagoras's Theorem ($\sim$ 500 BC)

$a^2 + b^2 = c^2$ has solutions where a, b, and c are positive integers





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

This statement is TRUE,

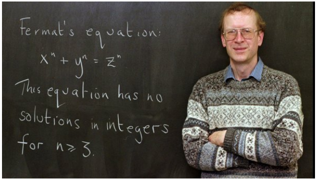
e.g. $a = 3$, $b = 4$, and $c = 5$

Proving Statements

Fermat's Last Theorem (1637)

$a^3 + b^3 = c^3$ has no solution where a, b, c are positive integers

Andrew Wiles (1994) proved this statement to be TRUE



- Wiles announced "proof" on 23 June 1993
- In September 1993, error was found in the proof
- On 19 September 1994, Wiles corrected the proof
- The corrected proof was published in 1995

Proving Statements

Euler Conjecture (1769)

$a^4 + b^4 + c^4 = d^4$ has no solutions where a, b, c, d are positive integers

Noam Elkies (1987) proved this statement FALSE

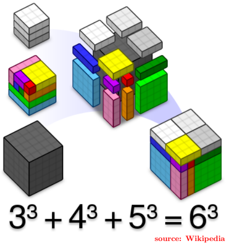
$a = 2682440$,

$b = 15365639$,

$c = 18796760$,

$d = 20615673$,

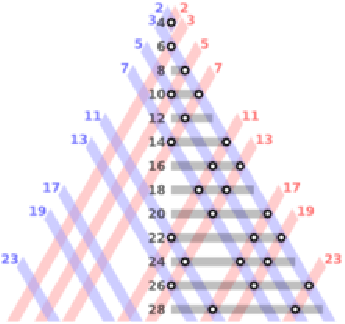
is a solution



Proving Statements

Goldbach Conjecture (1742)

Every even integer > 2 is the sum of two primes



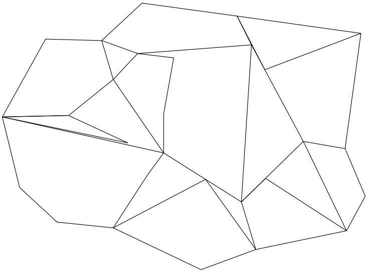
Sum of two primes at intersection of two lines. (source: Wikipedia)

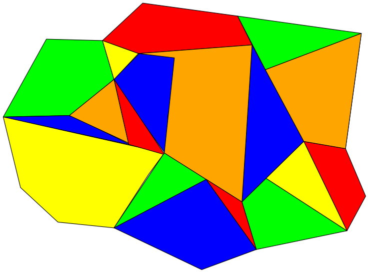
- No one yet knows the truth value of this statement
- Every even integer ever checked is a sum of two primes
- Just one counter-example will disprove the claim
- Homework!

Proving Statements

Conjecture (1852)

Regions of any 2-d map can be colored with 4 colors so that no neighboring regions have the same color





4-Coloring Theorem

- Kempe (1879) announced a proof
- Tait (1880) announced an alternative proof
- Heawood (1890) found a flaw in Kempe's proof
- Petersen (1881) found a flaw in Tait's proof
- Heesch (1969) reduced the statement to checking a large number of cases
- Appel & Haken (1976) gave a "proof", that involved a computer program to check 1936 cases (1200 hours of computer time)
- Robertson et.al. (1997) gave another simpler "proof" but still involved computer program

UIUC stamp in honor of the 4-Color theorem

- No human can check all the cases
- What if the program has a bug
- What if the compiler/system hardware has a bug

Direct Proofs

Direct Proof: used to prove statement of the form $P \rightarrow Q$

1. Assume that P is true
2. With a chain of logical deductions conclude that Q is true

P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

When P is false, $P \rightarrow Q$ is already true irrespective of value of Q

The only case when $P \rightarrow Q$ is false, is when $P = T$ and $Q = F$

Hence our goal is to rule out that possibility

Proof by Contrapositive

Recall that an implication is equivalent to it's contrapositive

$$P \to Q \;\equiv\; \neg Q \to \neg P$$

Direct Proof to show $P \to Q$

- Assume P is true, logically deduce that Q is also true

Proof by Contrapositive to show $P \to Q$

- apply the direct proof method to it's contrapositive ($\neg Q \to \neg P$)

Just a restatement of the given statement rather than a proof method

Proof by Contradiction

Suppose we want to prove some statement P to be true

In proof by contradiction we argue that

if P is not true, then some contradiction must occur

1. Assume that P is false
2. Show that from this ($\neg P$) we can logically deduce some contradiction

The contradiction can be to

- the assumption $\neg P$
  - implying both P and $\neg P$ are simultaneously true, a contradiction
- or to some known true statement S
  - implying S is false, meaning both S and $\neg S$ are simultaneously true

Function: List Representation

Let X and Y be two sets. A function f maps **each** element of X to **exactly one** element of Y

Let X be the domain with its **elements ordered** $x_1, x_2 \ldots,$

$f : X \mapsto Y$ can be represented as a list $\quad f(x_1), f(x_2), f(x_3), \ldots$

- Images of $x_1, x_2, \ldots$ listed in the order of X

Properties of functions as lists

Let $f : X \mapsto Y$ be represented as list

$f : X \mapsto Y$ is **one-to-one** if every $y \in Y$ appears at most once in the list

$f : X \mapsto Y$ is **onto** if every $y \in Y$ appears at least once in the list

$f : X \mapsto Y$ is **bijection** if every $y \in Y$ appears exactly once in the list

If $f : X \mapsto Y$ is a bijection and X and Y are finite sets, then $|X| = |Y|$

For finite sets X and Y, $|X| = |Y|$ iff there is a bijection $f : X \mapsto Y$

Cardinality of infinite sets

We showed that

- $|\text{integer powers of 2 and other integers}| = |\mathbb{N}|$
- $|\text{powers of all integers}| = |\mathbb{N}|$
- $|\mathbb{Z}| = |\mathbb{N}|$

"$\textit{size}/2 = \textit{size}$". Surprised!

> *I see it, but I don't believe it!*
>
> George Cantor (in a letter to Dedekind, 1877)

This notion of cardinality enables us to reason about infinity

Countability

A set S is countable if it is either finite or has the same cardinality as $\mathbb{N}$

S is countable if it can be placed in a **one-to-one correspondence** with $\mathbb{N}$

S is countable in the following sense

If we count (write, print, list) one element of S per 'second', *then any particular element of S will be counted after a finite time*

This means we can list element of S like

$$a_1, a_2, a_3, a_4, a_5, \cdots$$

Note: We do not say that the whole set will be printed

Countability

A set S is **countable** if it is either finite or has the same cardinality as $\mathbb{N}$

The following sets are countable

- $\mathbb{Z}$
- $\mathbb{O}$ and $\mathbb{E}$, odd and even integers
- Integer powers of 2
- Integer powers of other integers
- Squares, cubes and any power of integers
- $\mathbb{Q}^+$, the set of $+$ve rational numbers

Countability

Are all infinite sets of the same size (countable)?

No

Cantor invented a very important technique,

DIAGNOLIZATION

to show how to find bigger infinity

The set $\mathbb{I}$ of real numbers between 0 and 1 is not countable

Proof by Induction

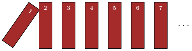
A proposition about non-negative integers, $\forall\ n\ P(n)$ is a sequence of propositions (dominoes)

$$P(0), P(1), P(2), \dots, P(n), P(n+1), \dots$$

Establish two facts

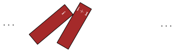
- Prove $P(0)$

  the first domino falls



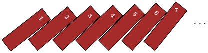
- Prove $\forall k \geq 0, P(k) \rightarrow P(k+1)$

  if a domino falls, then the next domino also falls



Conclude that $P(n)$ is true for all n

all dominoes fall



Principle of Mathematical Induction

$$\Big[\, P(0) \wedge \forall k \geq 0 \,\big[P(k) \rightarrow P(k+1)\big] \,\Big] \longrightarrow \forall n \geq 0\, P(n)$$

Strong Induction

Principle of Mathematical Induction

$$\Big[\, P(0) \,\wedge\, \forall k \geq 0 \,\big[P(k) \rightarrow P(k+1) \big] \,\Big] \;\longrightarrow\; \forall n \geq 0 \, P(n)$$

Proof using Induction

- *Basis Step:* Prove $P(0)$ is true
- *IH:* Assume $P(n)$
- *Inductive Step:* Using $P(n)$, prove $P(n+1)$

Principle of Strong Mathematical Induction

$$\Big[\, P(0) \,\wedge\, \forall k \geq 0 \,\big[\forall\, 0 \leq i \leq k \;\, P(i) \rightarrow P(k+1) \big] \,\Big] \;\longrightarrow\; \forall n \geq 0 \, P(n)$$

Proof using Strong Induction

- *Basis Step:* Prove $P(0)$ is true
- *IH:* Assume $P(k)$ is true for all $1 \leq k \leq n$
- *IS:* Using $\forall\, k \leq n \; P(k)$, prove $P(n+1)$

How to write proofs

Do not worry about your difficulties in Mathematics. I can assure you mine are still greater.

Albert Einstein

I don't have any magical ability...I look at the problem, and it looks like one I've already done. When nothing's working out, then I think of a small trick that makes it a little better. I play with the problem, and after a while, I figure out what's going on.

Terry Tao

How to write proofs

Understand the problem

- List what is given to you
- Write down what you need to derive
- Unpack definitions

How to write proofs

Figure out some meaningful special cases

- $n = 1$, $n = 0$,
- empty set
- Boundary cases, extreme cases, easy case
- Put yourself in the mind of the adversary, worst-case examples/scenarios?

How to write proofs

Simplify the problem

- Develop good notation, Rephrase the problem
- Focus on simple version/cases at first
- Use paper, draw pictures, Draw picture

How to write proofs

Try Different Techniques

- Direct, Contrapositive, Contradiction, Case Analysis, Induction
- Focus on simple version/cases at first
- Use paper, draw pictures, make tables