Mathematical Background Material

Sets

- A *set* : a collection of objects represented as a unit.
- The objects of the collection are called the *members* or *elements*.
- A set is completely determined by its members
- Two sets are equal iff the two sets have the same members.
- Curly braces will be used to define sets. Thus, {Tom, Mary, Paul} refers to the set whose elements are Tom, Mary, and Paul, while $\{x \mid x \text{ is a unicorn}\}$ refers to the set of all unicorns.
- The symbols $\in$ and $\notin$ denote set membership and non-membership.

Sets

- A set that does not have any elements is called the empty set and is denoted $\emptyset$
- Given two sets A and B, we say that A is a subset of B , written $A \subseteq B$, if every member of A is also a member of B.
- We say that A is a proper subset of B, written $A \subset B$ if A is a subset of B and not equal to B.

Sets of Numbers

- The symbol **N** denotes the set of *natural numbers*, which are the "counting numbers" 0, 1, 2, 3, 4, …

- The symbol **Z** denotes the set of integers, which are: {….,-2,-1,0,1,2,…}

Venn Diagrams

- Venn Diagrams are a type of pictures that represent sets as regions enclosed in circular lines

- The elements of the set are listed inside of the diagram

Set-building operations

Given sets A and B, one can construct new sets as follows:

- The *union* of A and B is the set A U B containing all elements of A, all elements of B, and no other elements.
- The *intersection* of A and B is the set $A \cap B$ whose elements are the objects that are simultaneously elements of both A and B.
- Sets are said to be *disjoint* if their intersection is the empty set.
- The *difference* of A and B is the set A-B whose elements are those elements of A that are not elements of B.

Set Building Operations

- The *complement* of A is the set A' of all objects belonging to some predetermined *universal set* that depends on the context, that are not elements of A. So A' is really just U-A, where U is the universal set.
- The *Cartesian product* of A and B is the set

  A x B whose elements are the pairs (a,b), where a ranges over all elements of A and b ranges over all elements of B.
- The *powerset* of a set A is the set of all possible subsets for A.

Set Building operations

- A *partition* of a set S is a collection of subsets that are disjoint from each other and whose union is S
- A *bag* is a collection of elements with no order, but with duplicate-valued elements. To distinguish bags from sets, we use square brackets [ ] around a bag's elements.

DeMorgan's laws

One has the following duality relations for the union and intersection operations:

- $(A \cup B)' = A' \cap B'$
- $(A \cap B)' = A' \cup B'$

Sequences

- **A sequence** is a collection of elements with an order, and which may contain duplicate-value elements.
- We usually designate a sequence by writing the list within parentheses. For example, the sequence 7, 21, 57 is written as (7,21,57)
- As with sets, sequences may be finite or infinite. Finite sequences often are called tuples.
- A sequence with k elements is called a k-tuple. A 2-tuple is called a pair.

- Let s be a sequence, we denote the first element of the sequence as s_1, the second element as s_2, … the nth element as s_n. We call n the index of the sequence.

Increasing sequences:

- A sequence S is increasing or non decreasing if $S_n \leq S_{n+1}$ for all n

- For example, the sequence 2, 4, 6, … is increasing since:

$$S_n = 2n \leq 2(n + 1) = S_{n+1} \quad \text{for all n}$$

Decreasing sequences

- A sequence s is decreasing or nonincreasing if $S_n \geq S_{n+1}$ for all n
- Example: $x_n = (½)^n$ $\quad -1 \leq n \leq 4$
- The elements of x are: 2, 1, ½, ¼, 1/8, 1/16
- The elements of x_n are decreasing since $x_n = (½)^n \geq (½)^{n+1} = x_{n+1}$ for all n.

Sequence Summation

- If $\{a_i\}_{i=m}^{i=n}$ is a sequence, we define the subsequence sum as:
- $$\sum_{i=m}^{i=n} a_i = a_m + a_{m+1} + a_{m+2} \ldots . + a_n$$
- The formalism $\sum_{i=m}^{i=n} a_i$ is called *sum or sigma notation*

Sequence Product

- We also define the subsequence product of a sequence by:

$$\prod_{i=m}^{i=n} a_i = a_m . a_{m+1} . a_{m+2} ..... a_n$$

- The formalism $\prod_{i=m}^{i=n} a_i$ is called the *product notation.*
- i is called the index, m is called the lower limit, and n is called the upper limit.
- The name of the index is irrelevant:

RELATIONS

- A relation can be thought of as a set of ordered pairs.
- We consider the first element of the ordered pair to be related to the second element of the ordered pair.

- **Definition:**
- A relation R from a set X to a set Y is a subset of the Cartesian Product X x Y,
- if $(x, y) \in R$, we write x R y and say that x is *related to* y.
- In case X = Y, we call R a binary relation on X.

Domain and Range of a relation

- The set $\{x \in X \mid (x, y)$ for some $y \in Y\}$ is called the domain of R.
- The set $\{y \in Y \mid (x, y)$ for some $x \in X\}$ is called the range of R.
- If a relation is given as a table, the domain consists of the first column and the range consists of the second column.

Digraph

- An informative way to picture a relation on a set is to draw its digraph.
- To draw the digraph of a relation on a set X:
- First, draw dots or **vertices** to represent the elements of X.
- Next, if the ordered pair $(x, y) \in R$, draw an arrow, called a **directed edge** from x to y.
- An element of the form (x, x) is in relation with itself and corresponds to a directed edge from x to x called a **loop.**

Properties of Relations

Reflexive:

- A relation R on a set X is called *reflexive*

if $(x, x) \in R$ **<u>for every</u>** $x \in X$.

- The digraph of a reflexive relation has a loop on every vertex.

Properties of Relations

Symmetric:

- A relation R on a set X is called *symmetric* if :

for all $x, y \in X$, if $(x, y) \in R$ then $(y, x) \in R$.

- The digraph of a symmetric relation has the property that whenever there is a directed edge from any vertex *v* to a vertex *w*, then there is a directed edge from *w* to *v.*

Properties of Relations

Antisymmetric:

- A relation R on a set X is called antisymmetric if for all x, y $\in$ X ,

if ((x, y) $\in$ R and x $\neq$ y) then (y, x) $\notin$ R.

The digraph of an antisymmetric relation has the property that between any two vertices there is at most one directed edge.

Properties of Relations

Transitive:

- A relation R on a set X is called transitive if:
- for all $x, y, z \in X$,

if $((x, y) \in R$ and $(y, z) \in R$ then $(x, z) \in R$

The digraph of a transitive relation has the property that whenever there are directed edges from x to y and from y to z, there is also a directed edge from x to z.

Partial Orders

- A relation R on a set X is called a

partial order if R is reflexive, antisymmetric and transitive.

- For example, the relation R defined on the set of integers by: $(x, y) \in R$ if $x \leq y$

  is a partial order, it orders the integers.

Inverse of a relation

- Let R be a relation from X to Y. The inverse of R, denoted R^{-1} is the relation from Y to X defined by
- $R^{-1} = \{(y, x) \mid (x, y) \in R\}$

Composition of Relations

- Let R1 be a relation from X to Y and R2 be a relation from Y to Z.
- The composition of R1 and R2, written as R2 o R1 is the relation from X to Z defined by: R2 o R1= {(x, z) | (x, y) $\in$ R1 and (y, z) $\in$ R2 for some y in Y}

Equivalence Relation

- A relation that is reflexive, symmetric and transitive on a set X is called an ***equivalence relation on X.***

Functions

- A *function* f: B -> A from a set B to another set A is an object that sets up an input-output relationship.
- A function takes an input and produces an output.
- In every function, the same input always produces the same output.

Function Domain and Range

- If f is a function whose output value is b when the input value is a, we write: $f(a)=b$.
- A function is also called a mapping and if $f(a)=b$, we say that f maps a to b.
- The set of possible inputs to the function is called its domain. The outputs of a function come from a set called its range. The notation for saying that f is a function within domain D and range R is: $f: D \rightarrow R$

Recurrence Relation

- A recurrence relation defines a function by means of an expression that includes one or more (smaller) instances of itself. A classical example of recursive definition for the factorial function is:
- $n! = (n-1)!.n$ for $n>1$;
- $1!= 0!=1$.

Recursion and induction

- *Recursion* is a method of defining countable sets, relations, or functions in a step-by-step fashion.

- *Induction* is a method of reasoning which may be used to show that every element of an inductive set has a certain property.

Example of recursion

- Find a formula for the sum S_n of the first n natural numbers: $S_n = 1 + 2 + 3 + ... + n$.
- You try some small values of n and find: $S_0=0$, $S_1=1$, $S_2=3$, $S_3=6$, $S_4=10$.
- Assume that Sn= n(n+1)/2

How does induction work?

- (*Basis step*) Check the first value of n: n=0. Yes, $S_0=0=0(0+1)/2$.
- Assume that the formula is correct for n
- (*Induction step*) Assume that you've checked all the values up to and including some n, and show that the next value, n+1 also checks:
  $S_{n+1} = S_n + (n+1) = n(n+1)/2 + (n+1)$
  $= (n+1)(n/2 + 1) = (n+1)(n+2)/2$

Inductive Set

- A set A constructed by recursion according to the above procedure is called an *inductive set*

Recursive function

- Using recursion, one proceeds as follows:
- Define the "first value" f(0) of the function.
- Assuming that the values f(0) ... f(n) have been defined for some value of n, define the "next value" f(n+1), possibly in terms of one or more of the "previous values" f(0) ... f(n).
- More generally, a definition by recursion constructs a set A in three steps:
- *Basis step*: Define a starting set A0.
- *Recursion step*: Assume that sets A0, ... An have been defined. Then define the "next" set An+1 in terms of A0, ... An.

Summations and Recurrences

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2} \qquad (1)$$

$$\sum_{i=1}^{n} i^2 = \frac{2n^3 + 3n^2 + n}{6} \qquad (2)$$

$$\sum_{i=1}^{\log n} i = n \log n \qquad (3)$$

$$\sum_{i=0}^{\infty} a^i = \frac{1}{1-a} \ \mathit{for}\ 0 < a < 1 \qquad (4)$$

$$\sum_{i=1}^{n} \frac{i}{2i} = 2 - \frac{n+2}{2^n} \qquad (5)$$

$$\sum_{i=0}^{n} a^i = \frac{a^{n+1} - 1}{a-1} \ \mathit{for}\ a \neq 1 \qquad (6)$$

Graphs

- An undirected graph, or simply a graph, is a set of points with lines connecting some of the points.
- The points in a graph are called nodes or vertices, and the lines are called edges
- The degree of a node is the number of edges at a particular node.
- In a graph G that contains nodes i and j, the pair (i,j) represents the edge that connects i and j.
-

- In undirected graphs, the pairs (i,j) and (j,i) are equivalent and can be represented with sets as in {i,j}.
- If V is the set of nodes of G and E is the set of edges, we say G=(V,E). A graph can then be described with a diagram or more formally by specifying V and E.
- A labeled graph has nodes and edges labeled.

- G is a subgraph of graph H if the nodes of G are a subset of the nodes of H and the edges of G are the edges of H on the corresponding nodes.
- A path in a graph is a sequence of nodes connected by edges.
- A simple path is a path that does not repeat any nodes.
- A graph is connected if every two nodes have a path between them.

Graphs

- A path is a cycle if it starts and ends in the same node.
- A simple path is one that contains at least three nodes and repeats only the first and last node.
- A tree is a graph if it is connected and has no simple cycles.
- A tree may contain a specially designated node called the root.
- The nodes of degree 1 in a tree, other than the root, are called the leaves of the tree.
- A directed graph has arrows instead of lines.

Graphs

- The number of arrows pointing from a particular node is the outdegree of that node.
- The number of arrows pointing to a particular node is the indegree of that node.
- In a directed graph, we represent an edge from i to j as a pair (i,j).
- A path which all the arrows point in the same direction as its steps is called a directed path.
- A directed graph is strongly connected if a directed path connects every two nodes.

Strings and Languages

- Strings of characters are fundamental building blocks in CS. The alphabet over which the strings are defined may vary with the application.
- An alphabet is defined as a nonempty finite set. The members of the alphabet are the symbols of the alphabet.
- Σ and Γ are used to designate alphabets.

Strings and Languages

- A string over an alphabet is a finite sequence of symbols from that alphabet, usually written next to one another and not separated by commas.
- If $\sum = \{0,1\}$ then 001101 is a string over $\sum$.
- If w is a string over $\sum$, the length of w, written $|w|$, is the number of symbols that it contains.
- The string of length of zero is called the empty string and is written ε

Boolean Algebra

Definition of a Proposition:

- A proposition is a sentence that is either true or false but not both.
- Boolean Logic is a mathematical system built around the notion of proposition and two values TRUE and FALSE.
- The values TRUE and FALSE are called the Boolean values and are represented as 1 and 0

Boolean Operators: **Negation**

- Let's have the proposition " Logic is confusing"
- The negation of p, denoted $\neg p$ is the proposition:

"***not*** p" or "***it is not the case that*** *p".*

- It has the opposite truth value from p:
- if p is true, $\neg p$ is false*;* if p is false, $\neg p$ is true

Negation Truth Table

The truth-value of the proposition $\neg p$ is defined by the truth table:

p	$\neg p$
T	F
F	T

Boolean Operators: Conjunction

- Let *p* and *q* be propositions.
- The conjunction of *p* and *q*, denoted: $p \wedge q$ is the proposition *p and q.*
- It is **True** when and only when <u>both p and q are true.</u>
- If <u>p is false or q is false or both are false</u>, then $p \wedge q$ is **false**

Conjunction Truth Table

p	q	***p*** $\wedge$ ***q***
T	T	T
T	F	F
F	T	F
F	F	F

Boolean Operators: Disjunction:

Let p and q are propositions, the disjunction of p and q is “p or q” denoted $p \vee q$.

- It is **true** when either p is true or q is true or both p and q are true;
- it is **false** only when both p and q are false.

Disjunction Truth Table

p	q	p V q
T	T	T
T	F	T
F	T	T
F	F	F

Logical Propositions

- **Tautology**
- We say that a compound proposition C is a **tautology** if C is True for any truth-value of its propositions ($p \lor \neg p$)
- For example let p : it is raining
- The compound proposition $p \lor \neg p$ (it is raining or it is not raining) is a tautology.
- **Contradiction:**
- We say that a compound proposition C is a **contradiction** if C is false for any combination of truth-values of its components ($p \land$ not p)
- For example let p : it is raining
- The compound proposition $p \land \neg p$ (it is raining and it is not raining) is a contradiction.

Logical Operators : Conditional

- If p and q are propositions, the compound proposition: **if p then q**

is called a conditional proposition and is denoted: $\mathbf{p \rightarrow q}$

- The proposition **p** is called the **hypothesis** (or antecedent) and the proposition **q** is called the **conclusion** (or consequent)

Conditional Truth Table

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

Converse of a proposition

Let p and q be propositions, such that $p \rightarrow q$,

we call the proposition $q \rightarrow p$ the converse of the proposition $p \rightarrow q$

Biconditional Proposition:

- If p and q are propositions, the compound proposition: q if and only if p

is a called a biconditional proposition and is denoted: $q \leftrightarrow p$

- p if and only if q is the same as saying that p is a necessary and sufficient condition for q, it is written as “p iff q”

Truth table for iff

p	q	$p\rightarrow q$	$q\rightarrow p$	$p\rightarrow q \wedge q\rightarrow p$	$p\leftrightarrow q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	T	F	F	F
F	F	T	T	T	T

Precedence of Logical operators

Operator	Precedence
( )	0
$\neg$	1
$\wedge$	2
$\vee$	3
$\rightarrow$	4
$\leftrightarrow$	5

Propositional function

- **Definition:**
- Let P(x) be a statement involving the variable x and let D be a set. We call P a propositional function (with respect to D) if for each x in D, P(x) is a proposition.
- We call D *the domain of discourse* or domain of P.
- Example: p(n): $n^2 + 2n$ is an odd integer, (D= set of positive integers)

Universally quantified statements

- <u>**Definition:**</u>
- Let P be a propositional function with domain of discourse D, the statement:

  for every x, P(x) is said to be a *universally quantified statement.*
- This statement may be written $\forall$ x, p(x)
- The symbol $\forall$ is called a universal quantifier.
- $\forall$ means and reads **for all**

Truth-value of universally quantified statement

- The statement: $\forall$ x, p(x) is true

  if p(x) is true **for every** x in D.

- The statement $\forall$ x, p(x) is false

if p(x) is false **for at least one** x in D.

Existentially Quantified Statements

<u>**Definition:**</u>

- Let P be a propositional function with domain of discourse D, the statement:
- **For some** x, p(x) is said to be an **existentially quantified** statement.
- This statement may be written: **$\exists$x, p(x)**
- The symbol $\exists$ is called ***existential quantifier.***
- The symbol $\exists$ means and reads *for some*, or *there exists*

Mathematical Proof Techniques

- A mathematical system consists of axioms, definitions and undefined terms.
- An axiom is assumed ***true***.
- Definitions are used to create new concepts in terms of existing ones.
- Undefined terms are only defined implicitly by the axioms.
- Within a mathematical system, we can derive theorems.
- A theorem is a proposition that has been proved true.
- A lemma is a special kind of theorem that is not usually interesting.
- A corollary is a theorem that follows quickly from another theorem.

Theorems

- Theorems are often of the form:

Theorem 1:

- for all $x_1, x_2, \ldots, x_n$,

  if $p(x_1, x_2, \ldots, x_n)$ then $q(x_1, x_2, \ldots, x_n)$
- This universally quantified statement is true provided that the conditional statement:

if $p(x_1, x_2, \ldots, x_n)$ then $q(x_1, x_2, \ldots, x_n)$ is true for all $x_1, x_2, \ldots, x_n$.

Direct proof

To prove that Theorem is true, we assume that:

1. $x_1, x_2, \ldots, x_n$ are arbitrary members of the domain of discourse.
2. We also assume that $p(x_1, x_2, \ldots, x_n)$ is true
3. then , using $p(x_1, x_2, \ldots, x_n)$ as well as other axioms, definitions and previously derived theorems, we show directly that $q(x_1, x_2, \ldots, x_n)$ is true

Proof by Contrapositive

Since the implication:

$p \rightarrow q$ is equivalent to its contrapositive $\neg q \rightarrow \neg p$

the implication $p \rightarrow q$ can be shown by proving its contrapositive

$\neg q \rightarrow \neg p$ is true.

Deductive reasoning:

- Definition of a valid argument:
- Any argument of the form:
- **If p1 and p2 and …pn then q** can be written as a sequence of propositions:

p1

p2

.

.

pn

$\therefore$ q

Truth Value for an existentially quantified statement:

- The statement **: $\exists$x, p(x)** is true

if p(x) is true for ***at least one*** x in D

- The statement **$\exists$x, p(x)** is false if p(x) is false ***for every*** x in D.

- The propositions p_1 p_2 …p_n are called the premises or the hypotheses
- q is called the conclusion.

- The argument is valid provided that: if p_1 and p_2 … and p_n are all true, then q must also be true . Otherwise, the argument is invalid or a fallacy.

Rules of Inference

- Modus Ponens:

$p \rightarrow q$

p

$\therefore q$

- Modus Tollens:

$p \rightarrow q$

$\neg q$

$\therefore \neg p$

- Addition

p

$\therefore p \vee q$

- Simplification
- $p \wedge q$

- $\therefore p$

Deductive Reasoning

- **Conjunction**

p

q

$\therefore$ p $\wedge$ q

- **Disjunctive syllogism**

p $\vee$ q

$\neg$p

$\therefore$ q

- **Hypothetical syllogism**

$p \rightarrow q$

$q \rightarrow r$

$\therefore p \rightarrow r$

Rules of Inference for Universally Quantified Statements

Let x be a universally quantified variable in the domain of discourse D, such that p(x) is true.

Universal instantiation: $\forall\, x \in D\; P(x)$

$\therefore\; P(d)$ if $d \in D$

Universal generalization: $P(d)$ for any $d \in D$

$\therefore\; \forall\, x \in D\; P(x)$

Rules of inference for Existentially Quantified Statements

- **Existential instantiation:**

  $\exists\, x \in D\ P(x)$

  $\therefore\ P(d)$ for some $d \in D$

Existential generalization:

$P(d)$ for some $d \in D$

$\therefore\ \exists\, x \in D\ P(x)$

Quantifiers and Logical Operators

- $\forall x\,[p(x) \wedge q(x)] \Leftrightarrow [\forall x\, p(x) \wedge \forall x\, q(x)]$
- $\forall x\,[p(x) \vee q(x)] \Leftrightarrow [\forall x\, p(x) \vee \forall x\, q(x)]$
- $\exists x\,[p(x) \wedge q(x)] \Leftrightarrow [\exists x\, p(x) \wedge \exists x\, q(x)]$
- $\exists x\,[p(x) \vee q(x)] \Leftrightarrow [\exists x\, p(x) \vee \exists x\, q(x)]$

Proof by counterexample:

- The simplest way to disprove a theorem or statement is to find a counterexample to the theorem.
- No number of examples supporting a theorem is sufficient to prove that the theorem is correct.
- However if we find an example that does not support the theorem, then we have proved that theorem is false.

<u>Proof by Mathematical induction</u>:

- Mathematical induction states that Thrm is true for any value of parameter n (n > c where c is some constant) if the following two conditions are true:
- *Base Case:* Show that Thrm holds for n=c, and
- Assume that Thrm holds for n-1
- *Induction step:* If Thrm holds for n-1, then prove that Thrm holds for n.

Example: Geometric Sum

- *Base Case:* Show that Thrm holds for n=c, and Assume that Thrm holds for n-1
- *Induction step:* If Thrm holds for n-1, then prove that Thrm holds for n.
- Use induction to show that if r $\neq$ 1,

$$a + ar^1 + ar^2 + ... + ar^n = \frac{a(r^{n+1} - 1)}{r - 1} \quad for \ n = 0,1,..., n$$