Discrete Math

Dhruva Karkada

Fall 2017

Contents

1 Propositional Logic

Proposition

A statement that is either true or false. Often represented by lowercase letters such as p and q.

Example: Austin is the capital of Texas.

Logical connective

A logical operation defined by truth tables. The 5 main connectives are:

Connective	Symbol	Plain English
Negation	$\neg$	not
Conjunction	$\wedge$	and
Disjunction	$\vee$	or
Implication	$\rightarrow$	implies
Biconditional	$\leftrightarrow$	if and only if (iff)

The exclusive or ($\oplus$) is a less well-known connective.

Implication $p \rightarrow q$ has related statements: converse ($q \rightarrow p$), inverse ($\neg p \rightarrow \neg q$), and contrapositive ($\neg q \rightarrow \neg p$). Of these, only the contrapositive is guaranteed to hold if the implication holds.

Formula

A syntactically valid series of propositions, connected by connectives.

Example: $(p \rightarrow q) \wedge p$

Interpretation of a formula

A mapping of all propositional variables in a formula F to their truth values. Necessary for determining the truth value of F.

Example: For the formula $p \wedge q$, a possible interpretation is $p = \mathrm{T},\ q = \mathrm{F}$.

Entailment

An interpretation I entails formula F (written $I \models F$) iff F evaluates to true under I. $I \models F$ iff $I \not\models \neg F$.

Example: From the previous definition, F is false, since $\mathrm{T} \wedge \mathrm{F} = \mathrm{F}$. Therefore, $I \not\models F$.

Validity
F is valid iff for all interpretations I, $I \models F$.

Satisfiability
F is satisfiable iff there exists an interpretation I such that $I \models F$.

Unsatisfiability
F is unsatisfiable iff for all interpretations I, $I \not\models F$.

Contingency
F is contingent if it is satisfiable, but not valid.

Importantly, validity is the opposite of unsatisfiability. There is an important duality between the two.

Duality between Valid and Unsat:

F is valid iff $\neg F$ is unsat.

To prove that a formula is valid, we can use a truth table to show that all interpretations result in true. Similarly, to prove unsat, show that all rows in the table result in false. To prove satisfiable, just have to give an example of a satisfying interpretation; to prove contingent, also give an example of a falsifying interpretation.

Equivalence
$F_1 \equiv F_2$ iff $F_1 \leftrightarrow F_2$ is valid.

Some common equivalences are listed on the next page.

Equivalence Name	Formula
Contrapositive	$p \to q \equiv \neg q \to \neg p$
Remove implication	$p \to q \equiv \neg p \vee q$
Absorption	$p \vee (p \wedge q) \equiv p \wedge (p \vee q) \equiv p$
Identity	$p \wedge T \equiv p$
	$p \vee F \equiv p$
Domination	$p \vee T \equiv T$
	$p \wedge F \equiv F$
Idempotent	$p \wedge p \equiv p \vee p \equiv p$
Negation	$p \wedge \neg p \equiv F$
	$p \vee \neg p \equiv T$
Distribution	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
DeMorgan's Law	$\neg(p \wedge q) \equiv \neg p \vee \neg q$
	$\neg(p \vee q) \equiv \neg p \wedge \neg q$
Negate implication	$\neg(p \to q) \equiv p \wedge \neg q$

Rules of inference are a related concept. Rules of inference take some number of hypotheses, which are assumed to be true, and deduces a conclusion which must be true. In other words, the conjunction of all the hypotheses implies the conclusion.

Inference Rule	Hypotheses	Conclusion
Modus Ponens	$(p \to q) \wedge p$	q
Modus Tollens	$(p \to q) \wedge \neg q$	$\neg p$
Hypothetical Syllogism	$(p \to q) \wedge (q \to r)$	$p \to r$
And elimination	$p \wedge q$	p
And introduction	$(p) \wedge (q)$	$p \wedge q$
Or elimination	$(p \vee q) \wedge \neg q$	p
Or introduction	p	$p \vee q$
Resolution	$(p \vee q) \wedge (\neg p \vee r)$	$q \vee r$

2 First Order Logic

Similar to propositional logic, but adds semantics for dealing with predicates and quantification.

Universe of discourse
The set of all possible elements to consider for any statements.
Example: Positive integers.

Variable
An arbitrary element in the universe of discourse.
Example: x

Predicate
A statement about a variable which evaluates to either true or false, depending on the identity of the variable.
Example: x is even. Written $even(x)$.

Clearly, predicates are more powerful than propositions because they can be applied to any element in the universe. Formulae are analogous to the propositional logic formulae; an interpretation specifies both a universe and a definition for all predicates.

Quantifier
A modification to a predicate/formula which quantifies the elements for which it holds.

Universal quantifier
Refers to all objects in the universe.
Example: $\forall x.P(x)$ means that $P(x)$ holds for all x in the universe.

Existential quantifier
Refers to some object in the universe.
Example: $\exists x.P(x)$ means that there exists an x for which $P(x)$ holds.

The universal quantifier is analogous to the conjunction, and the existential quantifier is analogous to the disjunction. Negating a quantified formula switches the quantifier, in a way analogous to DeMorgan's law:

$$\neg\forall x.P(x) \equiv \exists x.\neg P(x).$$

For nested quantifiers, the order is very important if the quantifiers are different. The statement $\forall y\exists x.P(x,\ y)$ is very different from $\exists x\forall y.P(x,\ y)$.

The definitions of validity, satisfiability, unsatisfiability, and equivalence are the same as from propositional logic. However, since an interpretation now specifies the universe, of which there are infinite, it is not possible to use a truth table to determine validity. Equivalence is shown by using known equivalences to roowrite one formula as the other.

We can also use the rules of inference to help with proofs. Additional inference rules are known for quantifiers:

Inference Rule	Hypotheses	Conclusion
Universal Instantiations	$\forall x.P(x)$	$P(c)$ for any c
Universal Generalization	$P(c)$ for arbitrary c	$\forall x.P(x)$
Existential Instantiation	$\exists x.P(x)$	$P(c)$ for fresh c
Existential Generalization	$P(c)$	$\exists x.P(x)$

Note that $\forall$-gen. and $\exists$-inst. have caveats: the c must be truly arbitrary for $\forall$-gen., and the c must be a fresh variable for $\exists$-inst. These caveats are why a $\forall$-gen cannot follow a $\exists$-inst. in a proof; not heeding the caveats can lead a bogus proof, as Işil would say.

3 Proof Techniques

3.1 Proving validity of formulae

To prove a formula F valid, we must show that $\neg F$ implies false. If we derive false from $\neg F$, then $\neg F$ must be false, since true never implies false. Then, F must be true. We can't try to show that F implies true, because it doesn't guarantee that F is true. Anything implies true.

3.2 Proving theorems

Theorem
Important, provable mathematical statement.

Lemma
An auxiliary theorem that helps with a larger proof.

Conjecture
Suspected to be true, but unproven.

Theorems often take the form of $p \to q$. There are several ways to go about proving such theorems.

Direct proof
Assume p. Show that q must follow.

Proof by contraposition
Show that $\neg q \to \neg p$.

Proof by contradiction
Prove that the negation of the theorem yields a contradiction. Since $\neg(p \to q) \equiv p \wedge \neg q$, assume p and $\neg q$ and show that they are incompatible.

Proof by cases
Enumerate all possibilites and prove theorem for each case.

Common math proofs involve showing existence and uniqueness of certain objects. Existence proofs require showing that the object with the desired properties exist; uniqueness proofs show that no other object has the property. In an existence proof, we can have two types of proofs: constructive (where we provide an example) and non-constructive (indirect proof, i.e. by contradiction).

Invalid proof techniques, courtesy of Işil:

Proof by obviousness
"The proof is so clear it need not be mentioned!"

Proof by intimidation
"Don't be stupid – of course it's true!'

Proof by mumbo-jumbo
$\forall \alpha \in \theta \exists \beta \in \alpha \odot \beta \approx \gamma$

Proof by intuition
"By eyeballing, I'm pretty sure"

Proof by resource limits
"Due to lack of space, we omit this part of the proof."

Proof by illegibility
"sdjikfhiugyhjlaks??fskl; QED."

4 Sets and Functions

4.1 Set Theory

Set
Unordered, distinct objects. Important mathematical sets:

$\emptyset$: empty set	$\mathbb{Z}$: integers	$\mathbb{Z}^+$: positive ints
$\mathbb{N} : \{0, 1, 2, \dots\}$	$\mathbb{R}$: reals	$\mathbb{Q}$: rationals

Cardinality
$|S|$ = number of elements

Universal Set
Equivalent to universe of discourse

Singleton Set
Set with cardinality = 1

Subset
$A \subseteq B \quad \equiv \quad \forall x.(x \in A \rightarrow x \in B)$

Set equality
$A = B \quad \equiv \quad (A \subseteq B) \wedge (B \subseteq A)$

Power Set
$\mathcal{P}(S)$ is the set of all subsets of S. If $|S| = n$, then $|\mathcal{P}(S)| = 2^n$.

Cartesian Product
$A \times B = \{(a, b) \mid (a \in A) \wedge (b \in B)\}$
In general, $A \times B \neq B \times A$. Also, $|A \times B| = |A||B|$.

Union
$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}$

Intersection
$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}$
If $A \cap B = \emptyset$, then A and B are *disjoint*.

Difference
$A - B = \{x \mid (x \in A) \wedge (x \notin B)\}$

Complement
$\overline{A} = \{x \mid x \notin A\}$

Russell's Paradox

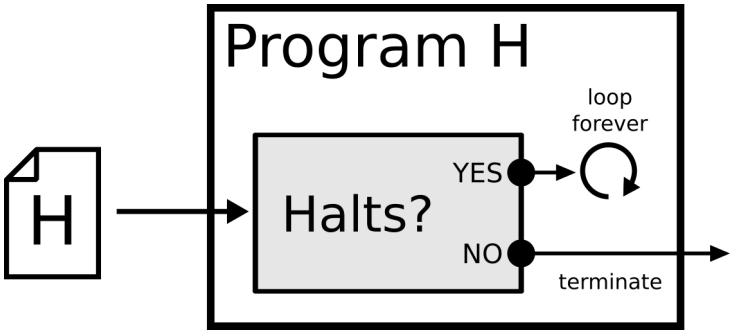
Revealed flaw in naïve set theory.

Consider Russell's set, a set of all sets which don't contain themselves: $R = \{S \mid S \notin S\}$. Then if $R \in R$, this yields a contradiction, because any element of R cannot contain itself. But if $R \notin R$, this also yields a contradition, because if it doesn't contain itself, it should be an element of R (by the definition of R).

Halting Problem

How does one determine, given an arbitrary computer program and input, whether the program will terminate?

Shown to be undecidable by Alan Turing. Assume that such a 'decider' algorithm exists. Consider the program H shown below. We will ask the decider if H terminates. If it returns yes, there is a contradiction because H will loop forever. If it returns no, there is a contradiction because H will immediately terminate.



4.2 Functions

Function
A function $f : A \mapsto B$ maps each $x \in A$ to a single $y \in B$.
If $f(a) = b$ then b is the *image* of a and a is the *preimage* of b

Domain
For a function $f : A \mapsto B$, the domain is A.

Codomain
For a function $f : A \mapsto B$, the codomain is B.

Range
The set of all images

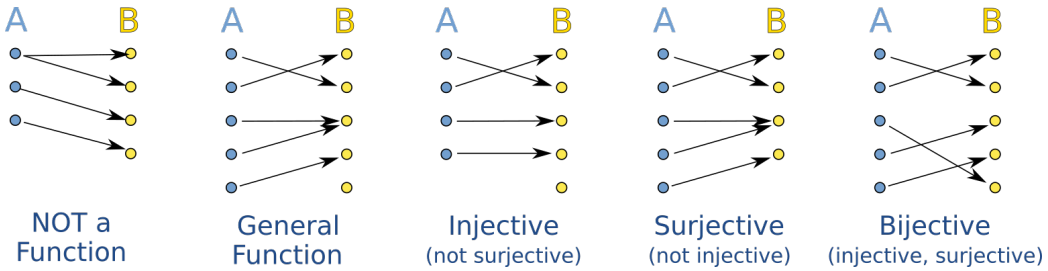
Injective Function (one-to-one)
$\forall x \forall y.(f(x) = f(y) \quad \rightarrow \quad x = y)$

Surjective Function (onto)
$\forall y \in B.\ \exists x \in A.\ (f(x) = y)$
Range = Codomain

Bijective Function
Both injective and surjective.

Inverse Function
If $f : A \mapsto B$, then $f^{-1} : B \mapsto A$ such that $f^{-1}(b) = a$ iff $f(a) = b$.
Only defined on bijections.

Composition
$f \circ g = f(g(x))$



4.3 Cardinality of Infinite Sets

Countably Infinite

Set A is countably infinite if there is a bijection between A and $\mathbb{Z}^+$
Enumeration: process of defining bijection

Countable

Set A is countable if it is either finite or countably infinite.

Enumeration of $\mathbb{Z}$

$\{0, 1, -1, 2, -2, 3, -3, \dots\}$

Enumeration of $\mathbb{Q}$

List all $x = \frac{p}{q} \in \mathbb{Q}$ by first listing all $x \mid p + q = 1$, then all $x \mid p + q = 2$, etc.

Cantor's Diagonalization Argument

Proves that the reals are uncountable.
Assume they are countable. Then the reals between [0, 1) are countable. We'll enumerate all of them as shown below.

$$\begin{array}{lllllll}
R_1 = 0. & [d_{11}] & d_{12} & d_{13} & \cdots & d_{1n} & \cdots \\
R_2 = 0. & d_{21} & [d_{22}] & d_{23} & \cdots & d_{2n} & \cdots \\
R_3 = 0. & d_{31} & d_{32} & [d_{33}] & \cdots & d_{3n} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\
R_n = 0. & d_{n1} & d_{n2} & d_{n3} & \cdots & [d_{nn}] & \cdots \\
\vdots & \vdots & \vdots & \vdots & & \vdots & \ddots
\end{array}$$

Then consider the number $R' = 0.a_1a_2a_3$ defined as follows:

$$a_i = \begin{cases} 0 & d_{ii} \neq 0 \\ 1 & d_{ii} = 0 \end{cases}$$

Then R' is guaranteed to differ from every enumerated R by at least one digit, which contradicts the claim that all possible Rs were enumerated.

5 Number Theory

Number theory deals with the study of integers and their properties. Theorems in number theory often deal with divisibility, prime numbers, and modulo.

Floor function

$\lfloor x \rfloor = n \quad \leftrightarrow \quad n \leq x < n+1 \qquad$ for $x \in \mathbb{R}$ and $n \in \mathbb{Z}$

Ceiling function

$\lceil x \rceil = n \quad \leftrightarrow \quad n-1 < x \leq n \qquad$ for $x \in \mathbb{R}$ and $n \in \mathbb{Z}$

Divisibility

$a|b \quad \leftrightarrow \quad b = ac \qquad$ for $a, b, c \in \mathbb{Z}$

Congruence Modulo

$a \equiv b \pmod{m} \quad \leftrightarrow \quad m|(a-b) \qquad$ for $a, b, m \in \mathbb{Z}$

There are some pretty important theorems in number theory that stem from the definitions of divisibility and congruence modulo.

Linearity of Divisibility:

$$(a|b) \wedge (a|c) \rightarrow a|(mb+nc)$$

where $m, n \in \mathbb{Z}$. Corollaries:

$$(a|b) \wedge (a|c) \rightarrow a|(b+c)$$
$$a|b \rightarrow a|mb$$

Division Theorem:

$$a = dq + r$$

where $a, d, q, r, \in \mathbb{Z}, \quad 0 \leq r < d, \quad r = a \bmod d.$

Congruence Modulo Theorem:

$$a \equiv b \pmod{m} \quad \leftrightarrow \quad a \bmod m = b \bmod m$$

Greatest Common Divisor

$\gcd(a, b)$ = the greatest number that divides both a and b.

Euclid's Algorithm

$\gcd(a, b) = \gcd(b, r)$ where $a = bq + r$

Base case: if $b = 0$, then $\gcd(a, b) = a$

Recursively compute $\gcd(a, b) = \gcd(b,\ a \bmod b)$

Linear Combination of GCD:

$$\gcd(a, b) = sa + tb$$

where $s, t \in \mathbb{Z}$. Corollaries:

$$(a|bc) \wedge \gcd(a, b) = 1 \quad \rightarrow \quad a|c$$

The exact values of s and t can be solved for using the Extended Euclid's Algorithm, by starting at the GCD and rewriting the result in terms of the numbers in the previous recursive step. At the end, the result is the GCD in terms of the original a and b.

Linear Congruence

$ax \equiv b \pmod{m}$ x is an unknown to be solved for.

Solutions exist iff $\gcd(a, m)|b$.

Solutions to Linear Congruence:

$$x = \frac{sb}{d} + \frac{m}{d}u$$

where $d = \gcd(a, m)$, $u \in \mathbb{Z}$.

Inverse Modulo

$a\overline{a} \equiv 1 \pmod{m}$ $\overline{a}$ is the unknown inverse modulo of a

Solution exists iff $\gcd(a, m) = 1$.

One particularly useful application of number theory is cryptography. A crude method of cryptography is *Caesar's cipher*, in which all letters in the message are rotated forward by some number of letters, k. Here, the encrypter and the decrypter both must know the key k. However, this could cause security issues. How does the sender safely communicate the key to the receiver?

In public-key cryptography, each member has both a public key and a private key. The public key is visible to everyone; the private key is known only by the member. The sender can use the receiver's public key to encrypt messages, but the encryption is a trapdoor function; it can only be decrypted if the receiver's private key is known.

The RSA algorithm is an example of a public-key cryptography system. The private key consists of two very large primes, p and q. The public key consists of a number e which is relatively prime with $p-1$ amd $q-1$, and a number n which is computed as $n = pqe$. Since the problem of prime factorization is difficult, it is impossible to efficiently determine p and q if you only know n and e. RSA works by taking a message M and encrypting it into ciphertext C.

RSA Encryption

$C = M^e \bmod n$

RSA Decryption

$M = C^d \bmod n$

d is solved by $de \equiv 1 \pmod{(p-1)(q-1)}$

diagram goes here

6 Induction

Inductive proofs aim to prove a certain property about all elements in a well-ordered set, such as the positive integers. We start by proving the theorem for a base case. Then, we assume that the theorem holds for some arbitrary case (the *inductive hypothesis*) and then prove that it must hold for the next case. By establishing this *inductive step*, we have proved that the theorem always holds.

6.1 Mathematical Induction

Show: $\forall x \in \mathbb{Z}^+.\ P(x)$
Proof by induction

- Base case: Prove $P(1)$
- Inductive step: Prove that $P(n) \to P(n+1)$
- QED.

Sometimes, may need to establish more than one base case. See selected proofs.

Other times, we may need a stronger inductive hypothesis. Instead of assuming $P(n)$, we may want to assume $P(1) \wedge P(2) \wedge \cdots \wedge P(n)$. Such a method is called *strong induction*, although it's not significantly different from regular induction.

6.2 Recursion and Structural Induction

Recursive definition
A way of defining structures such as sequences, functions, and sets. Starts with a base case, then repeatedly constructs the next element by referring to previous elements.
Example: $f(1) = 1,\ f(2) = 1;\ f(n) = f(n-1) + f(n-2)$

Closed-form definition
An explicit definition for a structure that doesn't involve recursion.
Example: $f(x) = x^2 + 1$

Strings can be built recursively, over an *alphabet* of characters Σ. The set of all strings formed according to a recursive rule is called the *language* Σ^*. A simple recursive definition for a language:

Show: Language Building
Recursive definition

- $\varepsilon \in \Sigma^*$ Base case: empty string in language
- $(\omega \in \Sigma^*) \wedge (x \in \Sigma) \quad \rightarrow \quad \omega x \in \Sigma^*$

Structural induction is induction over a recursively-defined structure.

Show: $\forall x \in S.\ P(x)$
Proof by induction

- Prove $P(x)$ in base case of recursive definition.
- Prove P(element) $\rightarrow$ P(recursively generated element) using recursive step.
- QED.

For proofs of the form $\forall s, t.P(s,t)$, use base case $P(s_1) = \forall t.P(s_1, t)$. See selected proofs for examples.

6.3 Generalized Induction

Well-Ordered
A set is well-ordered if it has a total order, and every subset has a well-defined least element.

Total Order
A total order exists if there is a well-defined predence $\preceq$:

- Antisymmetry: $(a \preceq b) \wedge (b \preceq a) \rightarrow a = b$
- Transitivity: $(a \preceq b) \wedge (b \preceq c) \rightarrow a \preceq c$
- Totality: $(a \preceq b) \vee (b \preceq a)$

The ordered pairs, defined as the Cartesian product $\mathbb{Z} \times \mathbb{Z}$, is well ordered by the following definition:

$$(x_1, y_1) \preceq (x_2, y_2) \quad \text{if} \begin{cases} x_1 < x_2, & \text{or} \\ x_1 = x_2 \wedge y_1 \leq y_2 \end{cases}$$

It is possible to use induction on any well-ordered set.

Show: $\forall x \in S.\ P(x)$
Proof by induction

- Prove $P(a)$ for least element a
- Strong induction: prove $P(a) \wedge \cdots \wedge P(e') \rightarrow P(e)$, where $\{a \cdots e'\} \preceq e$
- QED.

7 Combinatorics

Sometimes we are interested in counting the total number of possibilities of some certain scenario. This scenario can often be broken down into multiple sub-parts, some of which may be sequentially related, while others may be alternatives.

Sum Rule
When considering possibilities over several alternatives, the total number of possibilities is the sum of the possibilities in each alternative.

Product Rule
When considering possibilities in sequential, dependent events, the total number of possibilities is the product of the possibilities in each event.

Inclusion-Exclusion Principle
$|A| = |B| + |C| - |B \cap C|$
Prevents overlapping in sum rule.

Pigeonhole principle
If there are n objects to put in k boxes, then there exists a box with at least $\lceil n/k \rceil$ objects.

Counting techniques include permutations, where order matters, and combinations, where order doesn't matter.

Permutation

Obtain and arrange r objects out of n objects.

$$P(n,r) = \frac{n!}{(n-r)!}$$

Combination

Choose r objects out of n objects.

$$C(n,r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$$

Permutation with repetition

Obtain and arrange r objects out of n types of objects.

$$P^*(n,r) = n^r$$

Combination with repetition

Choose r objects from n types of objects.

$$C^*(n,r) = \binom{n+r-1}{r}$$

Binomial Theorem:

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

Corollaries:

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

8 Graph Theory

Graph
A graph $G = (V, E)$ is a set of vertices V connected by edges E.

Simple Graph
No loops; maximum 1 edge per pair of vertices

Degree of a vertex
$\deg(v)$ = number of edges connecting to v

Directed Graph
Directed edges (arcs) which are ordered; vertex has in-degree ($\deg^+(v)$) and out-degree ($\deg^-(v)$)

Induced Subgraph
If $V' \subseteq V$, the induced subgraph G' contains exactly V' and all edges in E that connect vertices in V'.

Complete Graph
K_n is the simple, undirected graph with n vertices such that every pair of vertices is connected with an edge.

Bipartite Graph
Simple, undirected graph; V can be partitioned into V_1 and V_2 such that every edge in E connects V_1 to V_2 (no edges within either partition).

Star Graph
A graph with a central vertex v; all edges connect v to another vertex.

Colorability
A graph is k-colorable if each vertex can be colored one of k colors such that no neighboring vertices share the same color.

Chromatic Number
A graph has chromatic number c iff it is c-colorable but not $(c-1)$-colorable

Handshaking Theorem:

$$\sum_{v \in V} \deg(v) = 2|E|$$

Corollaries:

For directed graphs, $\sum \deg^-(v) = \sum \deg^+(v) = |E|$

Colorability:

A simple graph G is (max-degree + 1)-colorable.

Path

A series of edges that connects two vertices; length = number of edges
Simple path: no repeated edges

Connectedness

A graph is connected if there is a path between any two vertices.

Connected Component

A subgraph G' is a connected component of G iff G' is connected and there is no edge connecting G' to any other vertex in G.

Circuit

A path from v to v
Simple circuit: no repeated edges

Cycle

A simple circuit with no repeated vertices (other than v).

Bipartite Graphs, Cycles, Colorability:

Bipartite graph $\leftrightarrow$ All cycles are even length $\leftrightarrow$ 2-colorable

Tree
A connected, undirected graph with no cycles.

Forest
A graph whose connected components are all trees.

Leaf
A vertex with degree 1. Every tree has at least one leaf.

Unique path definition of a tree:

An undirected graph is a tree iff
there is a unique path between any two vertices.

Number of edges in a tree:

A tree with n vertices has $n - 1$ edges.

Rooted Tree
A tree witha designated root vertex, where every edge is directed away from the root. This defines a hierarchy which allows for parent-child relationships to be defined.

Subtree
The subtree at v includes v and all its descendants.

Level
The level of v is the length of the path from v to the root.

m-ary Tree
A rooted tree where every vertex has no more than m children.
If $m = 2$ it is a binary tree.

Full m-ary Tree
Every internal node has exactly m children.

Balanced m-ary Tree
All leaves are either at level h or $h - 1$, where h is the height.
No correlation between being balanced and being full.

Planar Graph
A graph that can be drawn in the plane with no edges intersecting

Region/Face
An area in the bounded by edges in a planar graph. Includes the outer region.

Degree of a region
$\deg(R)$ is the number of edges bordering R

Euler's Formula:

$$|R| = |E| - |V| + 2$$

where $G = (V, E)$ is a planar graph. Corollaries:

$$|E| \leq 3|V| - 6$$

$$\exists v \in V.\ \deg(v) < 6$$

Euler Circuit
A simple circuit containing every edge in G.

Euler Path
A simple path containing every edge in G.

Hamilton Circuit
A simple circuit visiting every vertex in G exactly once. Is a cycle.

Hamilton Path
A simple path visiting every vertex in G exactly once.

Euler Circuits/Paths:

A multigraph G has a Euler circuit iff all vertices have even degree. If there are exactly two vertices with odd degree, it contains an Euler path but no circuit.

9 Algorithms

9.1 Asymptotic Analysis

Compexity Theory

Concerned with finding an *asymptotic estimate* for the *number of operations* necessary for an algorithm, with regard to input size.

Big O

An expression for an upper bound for a function $f(n)$.
Function $f(n)$ is $O(g(n))$ if there are positive constants $C,\ k$ such that

$$\forall n > k.\ f(n) \leq C \cdot g(n)$$

Big Ω

An expression for a lower bound for a function $f(n)$.
Function $f(n)$ is $\Omega(g(n))$ if there are positive constants $C,\ k$ such that

$$\forall n > k.\ f(n) \geq C \cdot g(n)$$

Big Θ

An expression for a tight bound for a function $f(n)$.
Function $f(n)$ is $\Theta(g(n))$ if it is both $O(g(n))$ and $\Omega(g(n))$.

$$\forall n > k.\ C_1 \cdot g(n) \leq f(n) \leq C_2 \cdot g(n)$$

Limit Definitions:

$$f(n) \text{ is } O(g(n)) \quad \text{if} \quad \lim_{x \to \infty} \frac{f(n)}{g(n)} < \infty$$

$$f(n) \text{ is } \Omega(g(n)) \quad \text{if} \quad \lim_{x \to \infty} \frac{f(n)}{g(n)} > 0$$

$$f(n) \text{ is } \Theta(g(n)) \quad \text{if} \quad 0 < \lim_{x \to \infty} \frac{f(n)}{g(n)} < \infty$$

9.2 Recurrence Relations

Recurrence Relation
A recursively defined sequence

Linear Homogeneous Recurrence Relation
A recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

Characteristic Equation
The characteristic equation for a linear homogeneous recurrence relation of the form shown above is

$$r^k = c_1 r^{k-1} + c_2 r^{k-2} + \cdots + c_k$$

Characteristic Roots
The roots of the characteristic equation.

Solving Linear Homogeneous RRs
If the RR has k characteristic roots $r_1 \cdots r_k$, each with multiplicity 1:

$$a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots + \alpha_k r_k^n$$

Generally, if there are k roots $r_1 \cdots r_k$ with multiplicities $m_1 \cdots m_k$:

$$a_n = \sum_{i=0}^{k} r_i^n (\alpha_{i,0} + n\alpha_{i,1} + \cdots + n^{m_i - 1}\alpha_{i,m_i-1})$$

The α coefficients are solved using the given initial conditions for the RR.

Linear Non-Homogeneous Recurrence Relation

A recurrence relation of the form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k} + F(n) = L_H + F(n)$$

Where L_H is called the *associated homogeneous recurrence relation.*

Particular Solution

A solution that satisfies the recurrence but not necessarily the initial conditions.

Finding a Particular Solution

Consider $F(n) = s^n(b_0 + b_1 n + \cdots + b_t n^t)$. If s is a characteristic root of the associated homogeneous RR with multiplicity m (where $m = 0$ if s is not a root):

$$a_n^p = n^m s^n (p_0 + p_1 n + \cdots + p_t n^t)$$

Generate p coefficients by plugging particular solution into original RR.

Solution to a Linear Non-Homogeneous Recurrence Relation:

If a_n^h is the solution to the associated relation
and a_n^p is a particular solution, then every
solution is of the form $a_n = a_n^h + a_n^p$.

9.3 Master Theorem

Divide And Conquer Algorithms

Recursive algorithms that divide the problem into subproblems, solve them, and combine their solutions to conquer the problem.

Recurrence of an algorithm

$T(n)$ denotes the number of steps taken on input size n.
Binary Search: $T(n) = T(n/2) + 1$
Merge Sort: $T(n) = 2 \cdot T(n/2) + 4n$

Master Theorem:

For a divide-and-conquer algorithm with recurrence

$$T(n) = a \cdot T(n/b) + cn^d :$$

$$T(n) \text{ is } \Theta(n^d) \qquad \text{if} \quad a < b^d$$

$$T(n) \text{ is } \Theta(n^d \log_b n) \quad \text{if} \quad a = b^d$$

$$T(n) \text{ is } \Theta(n^{\log_b a}) \qquad \text{if} \quad a > b^d$$

where $a, c \geq 1,\ d \geq 0,\ b > 1$.

10 Miscellaneous

10.1 Useful results and theorems

- $\sqrt{2}$ is irrational
- There exists an irrational x, y such that x^y is rational
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ and vice versa
- $f^{-1} \circ f$ is the identity function $I(x) = x$
- $\lfloor -x \rfloor = -\lceil x \rceil$
- $\lfloor x + k \rfloor = \lfloor x \rfloor + k \qquad k \in \mathbb{Z}$
- $(a|b) \wedge (b|c) \rightarrow a|c$
- Every integer greater than 1 is either prime or a product of primes
- If n is composite, it has a prime divisor $p \leq \sqrt{n}$
- There are infinite primes
- $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$
- If $ca \equiv cb \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$
- Pascal's identity: $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$
- If a graph contains an odd length circuit, then it contains an odd length cycle
- An m-ary tree of height h contains at most m^h leaves
  A tree with n leaves has $h \geq \log_m n$
- If $f(n)$ is a polynomial of degree d, then $f(n)$ is $O(n^d)$
- If $f_1(n)$ is $O(g_1(n))$ and $f_2(n)$ is $O(g_2(n))$:
  - $(f_1 + f_2)$ is $O(\max(g_1, g_2))$
  - $(f_1 \cdot f_2)$ is $O(g_1 \cdot g_2)$

10.2 Selected Proofs