Exam 1 Helper Pt 1

LOGIC ⟷ **Set Theory** :

$\subseteq$: is a subset of

$\supseteq$: is a superset of

$\subset$: proper subset ($\neq$)

$|A|$: cardinality of

$A \wedge B = \emptyset$: disjoint

$\forall$: for all

$\rightarrow$: implies

$\leftrightarrow$: iff

$\exists$: there exists

$\wedge$: and/intersection

$\vee$: or/union

$\bar{A} = U - A$

$\neg$: negation

$\times$: Cartesian product

$\oplus$: XOR

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

De Morgan's : $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$

Tautology: always true Contradiction: always false

Satisfiable: True sometime Unsatisfiable: False all the time

Incl/Excl: $|A_1 \cup A_2 \cup \ldots \cup A_n|$ = sum of sing − sum of two intersect + sum of 3 intersect ...

p q	f	Conjunctive Clause
F F	T	$\neg p \wedge \neg q$
F T	F	$\neg p \wedge q$
T F	F	$p \wedge \neg q$
T T	T	$p \wedge q$

DNF: disjunction of conjunctions of pos & neg literals

$f \leftrightarrow (\neg p \wedge \neg q) \vee (p \wedge q)$

CNF: conjunction of disjunctions of pos & neg literals

$\neg f \rightarrow f \leftrightarrow \neg[(\neg p \wedge q) \vee (p \wedge \neg q)] = (p \vee \neg q) \wedge (\neg p \vee q)$

P: solved w/ a polynomial-time algorithm → size n solved in n^k time → also called tractable

NP: nondeterministic polynomial $\propto$: relation of P is transitive

Functions & Relations

Not onto or one to one

A → 1
B → 1
C → 3
2

Domain = {A, B, C} Co-Domain = {1, 2, 3}

A is a pre-image of 1

1 is the image of A

One-to-one: each element in the co-domain/range has one unique pre-image

Onto: each element in the co-domain is an image of some pre-image

injective: one-to-one surjective: onto bijective: onto and one to one

Binary Relation: R is defined by $R \subseteq A \times B$ aRb : related, $a \not R b$: not related

Function: Binary Relation that has restriction of being one to one mapped

Number of Binary Relations : $|P(A \times B)| = 2^{|A \times B|} = 2^{mn}$

Properties: For m element set A and n element set B

Relations can be combined like sets: $\cup, \cap, -, \oplus$

Reflexive: $(a,a) \in R$ for every element $a \in A$

Symmetric: $(b,a) \in R$ whenever $(a,b) \in R$ where $a,b \in A$

AntiSymmetric: $(a,b) \in R$ and $(b,a) \in R$, then $a = b$ where $a,b \in A$

ASymmetric: $(a,b) \in R$ implies $(b,a) \notin R$

Transitive: $(a,b) \in R$ and $(b,c) \in R$, then $(a,c) \in R$, where $a,b,c \in A$

Exam 1 Helper Pt 2

Integers

$n \bmod k$: Remainder R of Integers : $n = kq + r$

$\equiv$: Congruency is when x will have same Remainder as y when $\bmod n$

Properties: $(x \pm y) \bmod k = [(x \bmod k) \pm (y \bmod k)] \bmod k$ (also with $\times$)

$a|b$: denotes a divides b

$Z_4 = \{0,1,2,3\}$
↑ Divisible by 4

Equivalence Classes:
- $[0] : \{\ldots,-8,-4,0,4,8,\ldots\}$
- $[1] : \{\ldots,-7,-3,1,5,9,\ldots\}$
- $[2] : \{\ldots,-6,-2,2,6,10,\ldots\}$
- $[3] : \{\ldots,-5,-1,3,7,11,\ldots\}$

Mult/Add Table

x / +	0	1	2	3
0	0 / 0	1 / 0	2 / 0	3 / 0
1	1 / 0	2 / 1	3 / 2	0 / 3
2	2 / 0	3 / 2	0 / 0	1 / 2
3	3 / 0	0 / 3	1 / 2	2 / 1

Galois Field of Integers: n is prime, Z_n is also a commutative group under multiplication

Fermat's Little Theorem: b, n positive integers, n is prime, b not div by n : $b^{n-1} \equiv 1 \pmod n$

Greatest Common Divisor → prime factorization: $3000 = 2^3 \times 3 \times 5^3$

Euclid's algorithm: $\gcd(a,b) = \gcd(b,r)$, $r = a \bmod b$ $\quad 7700 = 2^2 \times 5^2 \times 7 \times 11$
↳ w/ initial condition of $(a,0) = a$ $\quad \gcd(3000, 7700) = 2^2 \times 5^2 = 100$

Worst Case is when $a = fib(n)$, $b = fib(n+1)$

Lowest Common Multiple: $lcm(a,b) = [a,b] \div [\gcd(a,b)]$

Fraction in simplest form: $[(a) \div (\gcd(a,b))] \div [(b) \div (\gcd(a,b))]$

Extended Euclids Algorithm: $g = sa + tb$, where $g = \gcd(a,b)$

Ex: $\gcd(6700, 3000) = 100 \rightarrow 100 = 13 \times 6700 - 29 \times 3000$

Base Changing: $10^{d-1} \leq n \leq 10^d - 1 \rightarrow d \approx \log_{base} n$

$a \preceq b$ $(S, \preceq)$
Comparable: if $a \preceq b$ or $b \preceq a$
Incomparable: if neither $a \preceq b$ nor $b \preceq a$
Total/Linear Order Chain

Proof Techiques

Counter-Example: example that disproves a statement (disproof)

Proof by contradiction: indirect proof → assuming the opposite to be true leads to contradiction

Induction → [Basis Step : $P(1)$ is true $\quad (P(n))$ + Need Proposition
→ Induction : $P(k)$ is true, so $P(k+1)$ is true and $P(n)$ is too]

$Fib(n) = Fib(n-1) + Fib(n-2)$, $n \geq 2$, $Fib(0) = 0$, $Fib(1) = 1$

2-Tree: Every node has exactly two children if it is not a leaf

Binary Tree: Every node has at most 2 children : "left"/"right" child

Inorder Traversal: → left node → back → right node

Binary Search Tree: Binary Tree w/ keys associated w/ nodes

Poset: (S, R)
S: Set
R: Partial ordering

Relations

Equivalence Relation: A is ER iff is: reflexive, symmetric, transitive

Equivalence Class: $[a]_R = \{s \mid (s,a) \in R\}$, $b \in [a]_R$: b is representative of eqclass

Partition: Collection of disjoint non empty subsets of A, w/ A as their union

$\preceq$: Partial Order: A is a PO if it is: reflexive, antisymmetric, transitive

Quiz Refrence Sheet Pt1

Quiz 1

10/10

1. $A = \{a, b\}$, $B = \{1,2,3\}$ $|P(A) \times P(B)| = 2^2 \times 2^3 = 2^5 = 32$
2. Cardinality of power set of $\{1, 2, \ldots, n\}$ is 2^n
3. $A = \{a,b,c,d\}$, $B = \{X, Y, b, d, e\} \to A - B = \{a, c\}$
4. Two sets are disjoint iff the intersection of A, B is the empty set
5. Convinient type of diagram.. set-theoretical operations... Venn Diagram
6. DeMorgans Law for sets states the complement of the union of two sets A & B is the intersection of their complements
7. Power set of $\{0,1\}$ is $\{\{0\}, \{\}, \{1\}, \{0,1\}\}$
8. Universal Set $= \{0,1,2,3,4,5,6\}$, $A = \{0,2,4,6\}$ $\overline{A} = \{1,3,5\}$
9. $A = \{a,b,c,d\}$, $B = \{b,d,f\} \to A \cup B = \{a,b,c,d,f\}$
10. $|A| : 120$, $|B| : 230$, $|A \cap B| = 75$, $|A \cup B| = |A| + |B| - |A \cap B| = 120 + 230 - 75 = 275$

Quiz 2

10/10

1. Change for Greedy Method to not work w/o nickels : 30 ¢
2. see Quiz 1 - 8
3. Stanard Proof Techniaue : Mathematical Induction
4. formula for the cardinality of union of n sets interms of intersections : Princ. Incl/Exclusion
5. Parts of Induction: n=k induction assum. Basis, Induct. Hyp., n=k+1 P(N) Holds
6. Greedy Algorithm proof techniaue: proof by contradiction
7. $\sqrt{2}$ is irrational proof techniaue: proof by contradiction
8. $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| = 55 + 100 + 75 - 10 - 12 - 0 + 0 = 208$
9. $1 + 2 + 3 + \ldots + 99 + 100 + 101 = 5151$ $(n(n+1)/2)$ $101(102)/2 = 5151$
10. $1 + 3 + 5 + \ldots + 95 + 97 + 99 = 2500$ $(99 = 2k-1, k = 50 \to k^2 = 2500)$

Quiz 3

8/10

1. Disjunction means "or"
2. Binary search tree w/ distinct keys → the key in any node is greater than left and smaller than all keys in right
3. yields false iff p is true and q is false : $p \to q$
4. $p \leftrightarrow q$ is the same as $(p \to q) \wedge (q \to p)$
5. BST outputs keys in sorted order : In order traversal
6. Contrapositive of $p \to q$ is $\neg q \to \neg p$
7. Conjunction means "and"
8. Inverse of $p \to q$ is $\neg p \to \neg q$
9. Number of edges of a tree w/ 100 nodes is 99
10. Total number of nodes of a two tree having 60 internal nodes is 121

Quiz Refrence Sheet Pt 2

Quiz 4 9/10

1. Two formulas are logically equivalent if they have the same value for each interpr
2. which is not NP-complete (assuming $P \neq NP$): Sorting a list
3. NP stands for nondeterministic polynomial
4. A formula is a contradiction iff it is false for every interpretation
5. A formula is in DNF iff it is a disjunction of conjuctions of literals
6. DeMorgans Law states $\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q$
7. A formula is a tautology iff it is true for every intrepretation
8. A formula is in CNF iff it is a conjunction of disjunctions of literals
9. A formula is satisfiable if it is true for some interpretation
10. $p \oplus q$ in DNF is $(p \wedge \neg q) \vee (\neg p \wedge q)$

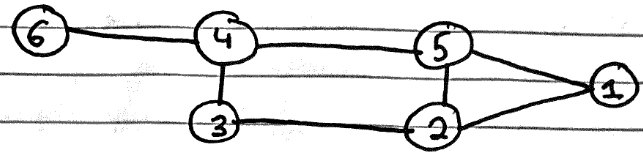
Quiz 5 9/10

1. number of relations for $\{1,2,3\}$ and $\{a,b,c,d\}$ is $2^{3 \times 4} = 2^{12} = 4096$
2. Equivalence relation corres. to partition of $\{1,2,3,4,5\}, \{\{1,4\},\{2,3,5\}\}$
   $= \{(1,1),(2,2),(3,3),(4,4),(5,5),(1,4),(4,1),(2,3),(3,2),(5,2),(2,5),(3,5),(5,3)\}$
3. function of set $A \to B$ is binary relation on A & B w/restricted each a is related to exactly one b
4. Surjective: onto
5. relation is symmetric if $(a,b) \in R \Rightarrow (b,a) \in R \ \forall a,b \in R$
6. Injective: 1:1
7. inverse of relation $\{(1,1),(1,2),(3,4)\}$ is $\{(1,1),(2,1),(4,3)\}$
8. equivalence relation properties: reflexive, symmetric, transitive
9. a poset is a set together w/a partial order on the set
10. bijective: 1:1 & onto

Supplemental Notes

Graph

Graph is defined by a Set of Vertices/Nodes $V=V(G)$
Set of Edges $E=E(G)$ where e is unordered $\{a,b\}$ of distinct V's
e is incident w/ end vertices a & b and a & b are adjacent
$n=n(G)$: num V & $n=|V|$ $m=m(G)$: num E & $m=|E|$
↳ n : Order of G ↳ m : size of G
$G=(V,E)$ where $V=\{1,2,3,4,5,6\}$, $E=\{12,15,23,25,34,45,46\}$:



Graphs are fundamental to design and analysis of networks w/ their associated algorithms & protocols, modeling underlying topology

Degree of vertex V, denoted by $deg(v)$ is #edges incident w/ v

Let $\delta=\delta(G)$ be min degree on all vertices & $\Delta=\Delta(G)$ be max degree

Then: $\delta \le deg(v) \le \Delta(G)$

Euler's Degree Formula: $\sum_{v \in V} deg(v) = 2m$ (Sum of all degrees of all vertices is twice num E)

* # vertices of odd degree is even (vice versa)

Regular Graph: each vertex has same degree r → $m=\frac{nr}{2}$

Complete Graph: n vertices on K_n, every pair of vertices are adjacent

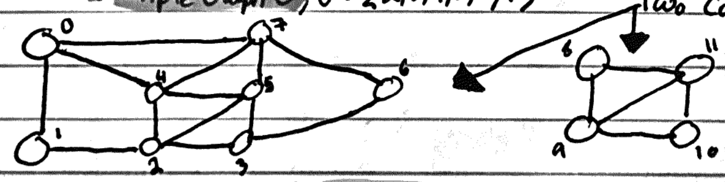
Subgraph: $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$ → H is subgraph

Spanning Subgraph: Subgraph H contains all vertices of G

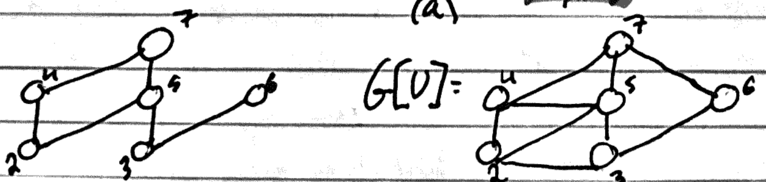
Subset U of V(G), subgraph G[U] induced by U is the subgraph w/ vertex set U and edge set of all edges in G w/ both end vertices in U

Component: A connected induced sub graph that is not contained in strict bigger connected subgraph

Sample Graph G, $U=\{2,3,4,5,6,7\}$ Two Connect Components



A disconnected graph G
(a)



a subgraph spanning U (b) The subgraph induced by U

Supplemental Notes

Graph

Bipartite: exists a bipartition of vertex set V into X & Y such that every edge has one end in X and the other in Y

Isomorphism: V & E are equal w/o labels (look same)

Bijective mapping $\beta: V \to V'$ from $G=(V,E) \to G'=(V',E')$

$\{u,w\} \in E$ iff $\{\beta(u), \beta(w)\} \in E'$ → Not NP complete

Path of length p $(p \geq 0)$ joining vertices u & v is a alternating sequence of $p+1$ vertices and p edges: $u_0 e_1 u_1 e_2 \dots e_p u_p$ where $u_0 \to u_p$

u_0: initial vertex u_p: terminal vertex interior: remaining vertices

* Vertices in a path can be repeated, but edges must be distinct

Walk: path where edges are repeated

Closed Path / Circuit: $u_0 = u_p$

Simple Circut / Cycle: simple closed path

Eulerian Path/Trail: path containing every edge in graph exactly once

Eulerian Circuit/Tour: circuit containing every edge exactly once

Hamiltonian Path: simple path containing every vertex in graph

Hamiltonian Cycle: cycle that contains every vertex in graph

Distance between u,v: $d(u,v)$ is shortest of all paths

↳ if not connected $d(u,v) = \infty$

Diameter of a Graph is the maximum distance between two vertices

Connected if vertices $u,v \in V$ if there is a path that joins them (leght 0 when $u=v$)

Depth-First-Search: test if graph is connected (Breadth First Search)

↳ Can also compute what vertices are connected

A proper vertex k-coloring of graph → k colors → no monochromatic edges: Coloring Graph

RSA

RSA: widely used public key cryptosystem $E \to D$ E: public, encrypts D: private, decrypts

Ex. m is encrypted: $C \equiv m^e \pmod{n} \to m \equiv C^d \pmod{n}$ decrypted

* to recover m, $m < n$

Euler's Totient Theorem: $b^{\varphi(n)} \equiv 1 \pmod{n}$

Rivest-Shamir-Aldelman: Let $n = pq$ where p & q are prime, let e be an integer relatively prime w $\varphi(n)$, let d be the multiplicative inverse mod $\varphi(n)$, that is, $ed \equiv 1 \pmod{\varphi(n)}$ then for any integer m, $m^{ed} \equiv m \pmod{n}$

Supplemental Notes

Graphs

Planar Graph: graphs embedded in the plane w/o crossing edges
F: set of faces ϕ: number of faces

Nonplanar Graph: No matter what, atleast two edges cross

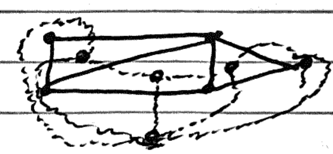
Subdivision S of graph G is made by replacing each edge e w/ a path join the same two vertices as e (subdividing the edge)

- G is subdivision of itself : if G is nonplanar $\longleftrightarrow$ if G contains nonplanar subdivision

Kuratowski's Theorem: A graph G is nonplanar iff it contains a subgraph that is isomorphic to a subdivision of K_5 or $K_{3,3}$

Euler's Degree Formula: $\sum_{g \in F} \deg(g) = 2m$
↳ if G is face s-regular: $m = \frac{sn}{2}$

Dual Graph:



Euler's Polyhedron Formula: G, a connect planar graph, with n vertices, m edges and ϕ faces: $n - m + \phi = 2$ ("connected" is required)

Polyhedron: planar graph that is vertex r-regular & face s-regular
↳ $n = \frac{2m}{r}$, $\phi = \frac{2m}{s} \rightarrow m = \frac{2}{2/r + 2/s - 1}$ By Eulers Degree & Polyhedron

Average Degree in planar graph (α): $m \leq 3n-6$

$$\alpha = \frac{2m}{n} \leq \frac{2 \times (3n-6)}{n} = 6 - \frac{12}{n} < 6$$

↳ there must exist a vertex of degree 5 or smaller

Spanning tree: tree of G containing (spans) all vertices, number edges $= n-1$

1   3   16   125

$K_n = n^{n-2}$ → # spanning trees w/ n vertices - Cayley's Theorem

Connecting all vertices

Minimum Spanning Tree: Minimum weight of all spanning trees

Kruskal's Algorithm: Build tree w/ lowest weights first

Konigsberg Bridge Problem: multigraph problem solved by Euler
↳ multigraph has a Eulerian Circuit iff it is connected and every vertex has an even degree

Supplemental Notes

Graphs

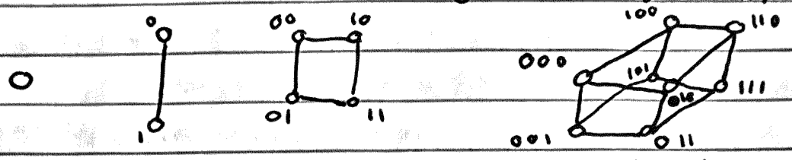
Multigraph contains an **Eulerian trail** iff connected, exactly two vertex have odd degree

Hypercube: k-dimensional hypercube H_k has 2^k vertices

containing set of all 0/1 k tuples

↳ $V(H_k) = \{(x_1, \ldots, x_k) \mid x_i \in \{0,1\},\ i = 1, \ldots, k$

two vertices in $V(H_k)$ are joined w/ an edge of H_k, when differing in one component



Recursive Hypercube Construction: Take two isomorphic H_{k-1} & join w/ a matching

Gray Codes of k-bits is an ordering k-bit strings so consecutive strings differ in one position

4 Bit: 0000 0001 0011 0010 0110 0111 0101 0100 1100 1101 111 1110 1010 1011 1001 1000 0000

↳ Applications: rotary & optic encoders, Karnaugh maps, & error detection

↳ Gray codes correspond to Hamiltonian Cycles in Hypercubes

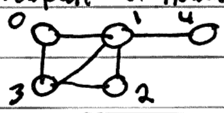
k-dimensional hypercube H_k contains Hamiltonian cycle for all $k \geq 2$

Graph G w/ $n \geq 3$ vertices w/ min. degree at least $\frac{n}{2}$ is Hamiltonian

↳ **Dirac's Theorem generalization:** graph G w/ $n \geq 3$ vertices

Such that each pair of nonadjacent vertices u & v → $\deg(u) + \deg(v) \geq n$ → Hamiltonian

Sample Graph:



Adjacency Matrix: $\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$

Adjacency List:
0: 1 3
1: 0 2 4 3
2: 1 3
3: 0 1 2
4: 1

Adjacency Matrix Pros & Cons: easy standard operations (new edge, deleting edges), n^2 memory edges, sparse → inefficient, dense → efficient (Big Graphs) must use

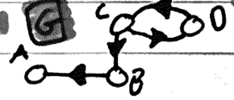
Adjacency List: efficient storage, sparse → efficient, dense → worse

Digraph $D = (V, E)$ of vertex set V and **directed edges** set E (edges are ordered pairs)

↳ E is relation on V, adjacency relation, $(a,b) \in E$, a is tail, b is head (can be ab)

Adj List
A:
B: A
C: B, D
D: C

G



$V = \{A, B, C, D\}$ * Adjacency Matrix if edge from $i \to j$

$E = \{(C,D), (D,C), (C,B), (B,A)\}$ $\begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

Weighted Digraph: Edges have weight labels, Matrix uses weight

Directed paths, trails, walks need to be directed from initial to terminal vertex

Let D be a digraph $D = (V, E)$ w/ $V = \{1, 2, \ldots, n\}$ & Adj Mat $A = (a_{ij})_{n \times n}$

Let $A^k = (a_{ij}^{(k)})_{n \times n}$ denote k^{th} power of A:

$a_{ij}^{(k)}$ is the number of walks from i to j of length k

Supplemental Notes

Graphs

Out-Neighorhood: set w/ a is all vertices b that are out-adjacent or simply adjacent to a, i.e. for which there is an edge (a,b)

In-Neigborhood: set w/ b is all vertices a that are in-adjacent to b, i.e., for which there is an edge (a,b)

Outdegree: outdeg(v) is #edges w/tail v (cardinality of out-neighborhood of v)

Indegree: indeg(v) is #edges w/head v (cardinality of in-neighborhood of v)

$\sum_{v \in V} outdeg(v) = \sum_{v \in V} indeg(v) = m = \#$ edges

Directed Acyclic Graph (DAG): digraph w/o any directed cycles

Source: Vertex v where all edges incident w/v are directed out, indeg(v) = 0

Sink: Vertex v where all edges incident w/v are directed in, outdeg(v) = 0

DAG modeling round-robin tournament contains directed Hamiltonian Path joining unique sink & source

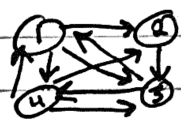
↳ path determines a ranking of players from best to worst (good for ordering tasks)

PageRank was developed in 1996 at Stanford by Larry Page & Sergey Brin (cofounder of google)

Web diagraph W: V(W) consists of webpages, E(W) is hyperlinks p → q

Page Rank of webpage p $R[p] = \sum_{q \in N_{in}(p)} \frac{R[q]}{d_{out}(q)}$

where $d_{out}(q)$ is outdegree of q, or the # of hyperlinks q contains



$R_1 : \frac{1}{2}R_3 + \frac{1}{3}R_4$
$R_2 : \frac{1}{3}R_1 + \frac{1}{3}R_4$
$R_3 : \frac{1}{3}R_1 + R_2 + \frac{1}{3}R_4$
$R_4 : \frac{1}{3}R_1 + \frac{1}{2}R_3$

Random Walk Matrix: matrix B for random walk on W $B[p,q] = \begin{cases} \frac{1}{d_{out}(p)}, & pq \in E(W) \\ 0 & \text{otherwise} \end{cases}$

Letting pagerank R be the vector/array R[p] of p, the formula is $R = B^T R$ where R is eigenvector of B & B^T, for eigenvalue of 1

Since 1 is the largest eigenvalue of B, R is principal eigenvector

$R_i[p] = \sum_{q \in N_{in}(p)} \frac{R_{i-1}[q]}{d_{out}(q)}, \; i = 1, 2, \ldots$ R(0) chosen to vector of nonnegative reals w/entries sum of 1

Probability a surfer will end up on page p after i steps: $R_i[p] = (B^T)^i R_0[p]$

Vector R_i will converge to principal eigenvector R if W satisfies:

1. W is strongly-connected (every two vertices p → q, there is a directed path p → q)
2. W is aperiodic (some int N such all k ≥ N, W contains closed walk of length k starting any vertex)

To ensure it converges, Damping Factor d is introduced (between 0 & 1)

Let n be #nodes of web digraph W:

$$R[p] = \frac{1-d}{n} + d \sum_{q \in N_{in}(p)} \frac{R[q]}{d_{out}(q)}$$

Supplemental Notes

Graphs

Difference of Random Web Surfer w/ Damping Factor: randomly jump to an arbitrary page w/ prob of $\frac{1-d}{n}$, otherwise will go w/ equal prob $\frac{d}{\deg^+(q)}$ to page in out-neighborhood of q

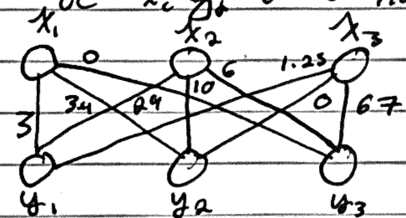
Combinations & Counting

Traveling Salesman Problem is a Hamiltonian Cycle w/ weight
↳ # Hamitonian Cycles starting & ending w/ city 1 is $n!$

TSP has $(n-1)!$ choices and is NP-Hard

Combinatoric Explosion: so many cases, cannot be computed in real time

Weighted Complete Bipartite Graph: $G=(V,E)$ w/ vertex bipartition $V = X \cup Y$, where $X=\{x_1,\dots,x_{n-1}\}$ & $Y=\{y_1,\dots,y_{n-1}\}$, each edge $x_i y_j$ of G has real weight ω_{ij} for $i,j \in \{1,\dots,n\}$



$$\Rightarrow \begin{pmatrix} 3 & 3.4 & 0 \\ 29 & 10 & 6 \\ 1.25 & 0 & 67 \end{pmatrix}$$

A perfect Matching corresponds to a traversal of the matrix

Matching: set of edges that have no vertex in common

Perfect Matching: Matching that spans all of the vertices

Weight of a Matching $\omega(M)$ is sum of edges, $\sum_{e \in M} \omega(e)$

Maximum-Weight Perfect Matching: maximizes $\omega(M)$

Hungarian Algorithm helps efficiently solve perfect match calculations

A permutation of a set S is a bijective mapping from S to itself:

$S=\{1,2,3\}$: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

123 132 213 231 312 321

The number of permutations in $n!$

The Multiplication Principle: m successive distinct and independent steps w/ n_k outcomes possible for the k^{th} step, total # outcomes: $n_1 \times n_2 \times \dots \times n_m$

The addition Principle: disjoint sets in n_k elements for the k^{th}: $n_1 + n_2 + \dots + n_m$

Lexicographic Order: given any permutations π_1 & π_2, let i be the first positive where they disagree, $\pi_1 < \pi_2$ iff $\pi_1(i) < \pi_2(i)$ means π_1 is lexicographically smaller than π_2

Ex: $546132 < 546123$, $612354 < 512346$, $231564 < 231645$

Supplemental Notes

Combinations & Counting

r-permutation of an n-element set is a linear ordering of r elements of the set. Let $P(n,r)$ be # permutations of an n-element set, using mult. prin.: $P(n,r) = \frac{n!}{(n-r)!}$

Circular permutations: Seating of n people has $(n-1)!$ ways to sit people

Combination: unordered selection of r-elements from an n-element set: $C(n,r)\binom{n}{r}$

↳ $C(n,r) = \binom{n}{r} = \frac{P(n,r)}{r!} = \frac{n!}{r!\,(n-r)!}$ for number of combinations

Ex: 5 card poker hands: $\frac{52!}{5!\,47!} = 2{,}598{,}960$; 13 card bridge hands: $\frac{52!}{13!\,39!}$

Ex: # Full Houses: $\overset{\text{rank}}{\text{pair}} = C(13,1) = 13$, $\overset{\text{suits}}{\text{pair}} : C(4,2) = 6$, $\overset{\text{rank}}{\text{three}} = 12$, $\overset{\text{suit}}{\text{three}} = C(4,3) = 4$

↳ $C(13,1) \times C(4,2) \times C(12,1) \times C(4,3) = 13 \times 6 \times 12 \times 4 = 3744$

$P(n; r_1, r_2, \ldots, r_k) = \frac{n!}{r_1!\,r_2!\cdots r_k!}$ → k distinct symbols where the i^{th} symbol has multiplicity r_i for $i \to k$, $n = \sum r_k$, $P(n; r_1, \ldots, r_k)$ is permutation w/ repetition.

Number of integer solutions to: $x_1 + x_2 + \ldots x_r = n$ is: $C[n-1, r-1]$ $\quad x_i \geq 1$, $i = 1, \ldots, r$

Also, when $x_i \geq 0$ → $C[n+r-1, r-1]$

Newton's Identity: $C[n,k] \times C[k,m] = C[n,m] \times C[n-m, k-m]$

Pascal's Identity: $C[n,k] = C[n-1,k] + C[n-1,k-1]$

↳ $C[n,k] = C[n, n-k]$

Binomial Theorem (Newton): $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$ ← Proof

(binomial coefficients: $C[n,k]$ & $\binom{n}{k}$)

Pascal's Triangle: triangle of binomial coefficients (sums to 2^n)

Multinomial Coefficient: $P(n; r_1, \ldots, r_k) = \frac{n!}{r_1! \cdots r_k!}$ → $\binom{n}{r_1\, r_2 \cdots r_k}$

↳ Theorem $(x_1 + \ldots + x_k)^n = \sum_{r_1 + \cdots + r_k = n} \binom{n!}{r_1\, r_2 \cdots r_k} x_1^{r_1} x_2^{r_2} \cdots x_k^{r_k}$

Quiz Reference Sheet pt 3

$\boxed{\text{Quiz 6}}$ 9/10

1. # of edges of complete graph w/ 100 vertices is 4950... $\frac{99 \times 100}{2}$
2. Hamiltonian cycle is a cycle that contains every vertex
3. Two graphs are isomorphic iff there is a bijective mapping between vertex sets of the two graphs that perserves adjacencies
4. The connected components of a graph can be computed w/ Depth-First-Trav
5. # of edges of 3-regular graph w/ 100 vertices is $150 = \frac{3n}{2}$
6. Eulers degree formula states that the Σ of degrees over all the vertices equals twice the number of edges
7. RSA was discovered by Rivest, Shamir, and Adleman
8. Euler's totient function $\varphi(n)$ is the number of integers between 1 & n-1, inclusive, that are rel. prime to n
9. Euler's Totient Theorem states ~~$b^{\varphi(n)} \equiv 1$ for all b not divis. by n~~
   $b^{\varphi(n)} \equiv 1$ for all b rel. prime to n
10. private key computed from public key w/ extended Euclid GCD algorithm

$\boxed{\text{Quiz 7}}$ 10/10

1. # of faces of planar connected graph w/ 100 vertices and 200 edges is 102
2. Kruskal's Algorithm for computing a minimum spanning tree is based on sorting edges in non-decreasing order of their weights and growing a forest by choosing next smallest edge that does not form a cycle
3. The number of regular polyhedra is 5
4. A graph is non-planar iff contains subgraph that is isomorphic to a subdivision of K_5 or $K_{3,3}$
5. Gray codes correspond to Hamiltonian cycle in hypercubes
6. A graph contains an Eularian ~~Cycle~~ Circuit iff it is connected and every vertex has an even degree
7. # spanning trees of K_{10} is 100,000,000
8. fewest vertices of a nonplanar graph is 5
9. diameter of hypercube of dimension 10 is 10
10. # of edges of a hypercube of dimension 10 is 5120

Quiz Reference Sheet Pt 4

9/10

Quiz 8

1. Topological sort of a DAG is a list of the vertices so that for each edge (u,v) vertex u occurs before vertex v
2. A sink in a DAG is a vertex v such that all edges incident with v have head v
3. Page Rank utilizes the web digraph
4. A source in a DAG is a vertex v such that all edges incident with v have tail v
5. DAG stands for Directed Acyclic Graph
6. A DAG is a digraph with no directed cycles
7. The transpose of the matrix for PageRank is the matrix for a random walk
8. Two standard implementations of a graph are adjacency matrix and adjacency lists
9. A digraph is a vertex set V, edgeset E, where E is a relation on V
10. The number of edges of a graph with 10 vertices where the average degree of a vertex is 4 is 20 since average degree = 2m/n

Supplemental Notes

Combinations & Counting

General Principle of Inclusion-Exclusion with n-sets:

$$|A_1 \cup \dots \cup A_n| = \sum_{k=0}^{n} (-1)^{k+1} \times \text{sum of sizes of intersections of all } n \text{ sets}$$

Consider an element which belongs to exactly k sets, say $A_1, \dots, A_k$:

Counted $C[k,1] - C[k,2] + C[k,3] + \cdots (-1)^{k+1} C[k,k] = 1$ # of times

Fixed Point: permutation π is an index i such $\pi(i) = i$

Derangement: permutation with no fixed points

Let A_i be #permutations on n elements where there is fixed point in position i, $i = 1, \dots, n$ Then $A = A_1 \cup \dots \cup A_n$ and

$d_n = n! - |A| = n! - |A_1 \cup \dots \cup A_n|$ (d_n is derangements set for $n = i$)

$$\frac{d_n}{n!} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \dots + (-1)^n \frac{1}{n!}$$

$$\lim_{n \to \infty} \left[\frac{d_n}{n!} = 1 \dots \right] = e^{-1} \approx .36788$$

For large n, fraction of permutations that are derangements or the probability of choosing a derangement is e^{-1}

Probability Theory

Statistics: Inferences on stats on data are made under the framework of Probability Theory

Algorithms Analysis & Design too

Discrete Sample Space S is a nonempty set that has only a finite or countably infinite number of elements

Outcome: an element with the Discrete Sample Space

Event: Subset of the Discrete Sample Space

Probability Density Function (PDF) p on a Discrete Sample Space:

For each $s \in A$, $0 \le p(s) \le 1$ $\rightarrow$ $\sum_{s \in S} p(s) = 1$

Also called a probability mass function

$P(E) = \sum_{s \in E} p(s)$ $\rightarrow$ $p(s)$ is the probability of outcome s; $P(E)$ is the sum of all outcome's probability

Let $S_1, \dots, S_n$ be n^{th} sample space, the cartesian product is:

$$S = S_1 \times S_2 \times \cdots \times S_n = \{(s_1, s_2, \dots, s_n) : s_i \in S_i, i = 1, 2, \dots, n\}$$

& probability of an outcome: $p(s) = p(s_1) \times p(s_2) \times \dots \times p(s_n)$

Let $E_1, \dots, E_n$ be events in sample space $S_1, \dots, S_n$ Then:

$$P(E_1 \times \dots \times E_n) = P(E_1) P(E_2) \cdots P(E_n)$$