Stable Matching

Concepts & Definitions:

- Matching: A set of edges without common vertices;
- Stable Matching: A matching where, given an order of preference for each element, there does not exist a pair (A, B) such that (A, B) would be better together than with their current matches;
- Perfect Matching: A matching such that every element is part of exactly 1 pair;
- Reworded: A perfect matching is such that every vertex v ∈ V(G) is incident to exactly one (u, v) ∈ E(G)

Theorems, Lemmas, Claims, [...] (w/o proofs):

- *Boy Proposal Algorithm* always terminates in a stable matching;
- In BPA, no girl ever rejects a valid partner;
- In BPA, every boy is matched to the best possible valid choice;
- In BPA, every girl is matched to the worst possible valid choice;

Basics of Graph Theory

Concepts & Definitions:

- K_n is a complete graph on n vertices, $|V(K_n)| = n,\ |E(K_n)| = \binom{n}{2}$;
- P_n is a path on n vertices, $|V(P)| = n,\ |E(P)| = n - 1$
- C_n is a cycle on n vertices;
- A graph H is a subgraph of G if $V(H) \subseteq V(G),\ E(H) \subseteq E(G)$;
- A bipartition (A, B) of the vertex set of a graph G is a partition such that every edge has one end in A and one end in B;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- Handshake lemma: $\sum_{v \text{ in } V(G)} deg_G(v) = 2|E(G)|$;
- If G is a forest, then $|V(G)| - |E(G)| = comp(G)$;
- If G is a connected graph and $deg_G(v) \leq 2\ \forall v \varepsilon V$, then G is a cycle or path;
- A graph G is bipartite if and only if it contains no odd cycles;

Matchings & Vertex Covers

Concepts & Definition):

- A set $M \subseteq E(G)$ is a matching of a graph G if every vertex in G is incident to at most one edge in M
- The matching number of a graph G, $\vartheta(G)$, is the maximum number of edges in a matching in G;
- A set $X \subseteq V(G)$ is a vertex cover of a graph G if every edge in G has at least one end in X;
- The minimum size of a vertex cover on the graph G, $\tau(G)$, is the minimum number of vertices in a vertex cover of G;
- A graph G is d-regular if all vertices in G have exactly d incident edges;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- $\vartheta(G) \leq \tau(G)$;
- $\tau(G) \leq 2\vartheta(G)$;
- **König**: If G is bipartite, the $\vartheta(G) = \tau(G)$;
- If G is d-regular and bipartite, then it has a perfect matching;

Edge Colouring & Systems of Distinct Representatives:

Concepts & Definitions:

- $\chi'(G)$ is the minimum number of colours needed to appropriately colour the edges of G;
- $\Delta(G)$ is the maximum degree of a vertex in G;
- A system of distinct representatives of a collection of finite sets $S_1, S_2, ..., S_k$ is a sequence $(x_1, x_2, ..., x_k)$ *such that* $x_i \varepsilon S_i \ \forall i$ and $x_i \neq x_j \ \forall i \neq j$;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- $\chi'(G) \geq \Delta(G)$;
- If G is d-regular and bipartite, then $\chi'(G) = d$;
- **Hall**: If G is a graph with a bipartition (A, B), then there exists a matching M which uses all vertices in A if and only if $|N(S)| \geq |S| \ \forall \ S \subseteq A$;
- A collection of sets $S_1, S_2, ..., S_k$ has a system of distinct representatives if and only if $|\bigcup_{i \varepsilon I} S_I| \geq |I|$;

Graph Colouring:

Concepts & Definitions:

- A vertex colouring of a graph G is a map which assigns to every vertex of G a colour $C(v)$ such that, if vertices u and v are adjacent, $C(u) \neq C(v)$;
- A k-colouring is a colouring requiring k colours;
- $\chi(G)$, the chromatic number of G, is the minimum number k of colours needed for a k-colouring;
- A graph G is k-degenerate if for every subgraph H of G contains a vertex v such that $deg_H(v) \leq k$;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- **Erdös**: For all $k, \ l > 0$, there exists a graph $G = G(k, l)$ such that $\chi(G) \geq k$ and every cycle in G has length $\geq l$;
- $\chi(G) \leq \Delta(G) + 1$;
- If G is a k-degenerate graph, then $\chi(G) \leq k + 1$;

Planar Graphs:

Concepts & Definitions:

- A graph G is said to be planar if it can be drawn such that its edges are disjoint except for their common endpoints;

- $Reg(G)$ denotes the number of regions on a planar graph;
- A graph H is a subdivision of a graph G if H can be obtained from G by replacing some edges by paths with the same endpoints, which otherwise don't share vertices;
- Contracting an edge with ends u, v in a graph G is done by deleting u, v, adding a new vertex w adjacent to all vertices in $G \setminus u \setminus v$ which were adjacent to either u or v in G. The result is denoted as G/e;
- A graph H is a minor of G if H can be obtained from G by repeatedly contracting edges, deleting edges, or deleting vertices;
- If H is a minor of G, we denote $H \leq_m G$;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- **Euler**: If G is a connected planar graph, then $|V(G)| - |E(G)| + Reg(G) = 2$;
- Let G be a planar graph with $|V(G)| \geq 3$, then $|E(G)| \leq 3|V(G)| - 6$;
- $\chi(G) \leq 4$ for every planar graph G;
- **Kuratowski**: A graph G is planar if and only if it does not contain a subgraph which is a subdivision of K_5 or $K_{3,3}$;
- Minor Variant: A graph G is planar if and only if it does not contain K_5 or $K_{3,3}$ as a minor;

Discrete Probability Fundamentals:

Note: I made a similar sheet for Math 323 (Probability). If you need to brush up on that class, you can find it here: http://aprnt.ca/pdfs/MATH323.pdf

Concepts & Definitions:

- Discrete Probability: Analysis of mathematical models of random processes or events on finite or countably infinite probability spaces;
- Sample space: A set of outcomes;
- Event: A subset of the sample space;
- Probability function (PF): A function p which maps the sample set onto the real number line such that:
  - $p(x) \geq 0 \ \forall x \varepsilon S$;
  - $\sum_{x \varepsilon S} p(x) = 1$;
  - $p(A) = \sum_{x \varepsilon A} p(x)$;
- Independence: Two events A, B are independent if the occurrence of one does not affect the occurrence of the other (that is, $p(A|B) = p(A)$);
- Pairwise independence: Given a set of events $A_1, ..., A_n$, they are pairwise independent if all pairs of events in the set are independent of each other;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- For any PF p and events A, B, $p(A \cup B) = p(A) + p(B) - P(A \cap B)$;
- Bayes' Theorem: $p(A|B) = \frac{p(B|A)p(A)}{p(B)}$;

- Two events are independent if $p(A \cap B) = p(A)p(B)$ (This product can be expanded for any number of events and the theorem will hold);
- Law of Total Probability: Let S be the probability space such that $S = B_1 \cup B_2 \cup ... \cup B_n$, and all B_i are pairwise disjoint, then for any event A: $p(A) = p(A|B_1)p(B_1) + p(A|B_2)p(B_2) + ... + p(A|B_n)p(B_n)$;

Random Variables & Expectation:

Concepts & Definitions:

- If S is some probability space, a random variable (RV) X is a function which maps S to the real number line;
- The probability distribution function (PDF) of a RV X defines the probabilities of some event on X occurring, that is, $p(X = v) = \sum_{s \varepsilon S,\, X(s)=v} p(s)$;
- The expectation of a RV X, $E(X)$, is the average value adopted by X (Note that $E(X)$ might take on a value that X itself cannot), $E(X) = \sum_{s \varepsilon S,\, X(s)=v} X(s)p(s)$;
- Two RVs X, Y are independent if $p((X = x) and (Y = y)) = p(X = x)p(Y = y)\ \forall x, y$;
- A Bernoulli trial is a RV which takes on the value of 0 or 1, so:
    - $p(X = 1) = p$
    - $p(X = 0) = 1 - p$
    - $E(X) = p$
- A RV X is said to have a binomial distribution if $X = X_1 + X_2 + ... + X_n$, where $E(X_i) = p$:
    - $p(X = x) = \binom{n}{x} p^x (1-p)^{n-x}$;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- Linearity of Expectation: Let X, Y be RVs, and $a, b\ \varepsilon\ \Re$, then $E(aX + bY) = aE(X) + bE(Y)$;
- If X, Y are independent RVs, then $E(XY) = E(X)E(Y)$;

Applications of Discrete Probability:

- Given the secretary problem:
    - Look at first k applicants. When those have passed and been rejected, accept now the first applicant who arrives and is better than the k applicants.
    - Results in $\sim \frac{k}{n} ln(\frac{n}{k})$ success rate
    - The optimal k value can be calculated to be $k \simeq \frac{n}{e}$
- If we have n balls and n bins (the latter numbered $B_1,\ B_2,\ ...,\ B_n$), and the function $max_i(B_i)$ denotes the maximum number of balls found in any bin, then $E(max_i(B_i)) \leq ceil(2log(n)) + 1$

Chernoff Bounds:

Concepts & Definitions:

- Chernoff Bound: Gives exponentially decreasing bounds on the complementary cumulative distribution function of sums of independent RVs;
- Quicksort: An algorithm which accepts as input a sequence of numbers $x_1, x_2, ..., x_n$ and outputs that sequence ordered by taking the first element, x_1, then placing all following elements into one of 2 groups: larger than x_1 or smaller than x_1. Perform Quicksort recursively on both of these new sequences. Output the “smaller than” group, x_1, the “larger than” group, in that order.
    - In processing a sequence via Quicksort, every occurrence of a number being compared to another is called a *comparison*;

Theorems, Lemmas, Claims, [...] (w/o proofs):
- Markov Inequality: where X is a non-negative RV, c is some positive constant, then $p(X \geq c) \leq \frac{E(X)}{c}$;
    - For some strictly increasing function $f : \Re \to \Re$, $p(f(X) \geq f(c)) \leq \frac{E(f(X))}{f(c)}$;
- Chernoff Bound:
    - Let $X_1, X_2, ..., X_k$ be independent Bernoulli RVs such that $p(X_i = 1) = p_i$, $p(X_i = 0) = 1 - p_i$,
    - Let $X = X_1 + X_2 + ... + X_k$, $\mu = E(X) = \sum_{i=1}^{k} p_i$, $\delta > 0$
    - $P(X \geq (1+\delta)\mu) \leq (\frac{e^{\delta}}{(1+\delta)^{(1+\delta)}})^{\mu}$;
- Let X, μ be as above, and $0 < \delta < 1$, then $p(X \geq (1+\delta)\mu) \leq e^{\frac{-1}{3}\mu\delta^2}$;
- Assume a sequence of numbers $x_1, x_2, ..., x_n$ is randomly sorted, let X denote the number of comparisons made by Quicksort, then $E(X) \leq 2n * log(n)$;
    - Moreover, a sorting algorithm involving only comparisons cannot be guaranteed to terminate in $< n * log(n)$ steps;
- The depth of a Quicksort recursion sequence is expected to be $< 32 * log(n)$, and is always at least $lg(n)$;

Counting:

Concepts & Definitions:
- A function $f : X \to Y$ is
    - An injection if $f(x_i) \neq f(x_j)\ \forall\ i \neq j$
    - A surjection if $\forall y \varepsilon Y\ \exists\ x \varepsilon X\ s.t.\ f(x) = y$
    - A bijection if it is both an injection and a surjection
- The number of trees which exist on n vertices:
    - Let $tl(n)$ define the number of trees with n vertices from the vertex set $[n]$
    - Let $tu(n)$ define the number of unlabelled trees on n vertices;

Theorems, Lemmas, Claims, [...] (w/o proofs):
- If $f : X \to Y$ is an injection, then $|X| \leq |Y|$;
- Pigeonhole Principle: If $f : X \to Y$ and $|Y| < |X|$, then f is not an injection

- If $f : X \to Y$ is a bijection, then $|X| = |Y|$
- Multiplication Principle: The number of sequences of the form $a_1, a_2, ..., a_n$ such that $a_i \varepsilon A_i$, $|A_i| = k_i$ is $k_1 k_2 ... k_n$;
- Number of injections on $f : [n] \to [k]$: $\frac{n!}{(n-k)!}$;
- Number of bijections on $f : [n] \to [k]$: $n!$;
- Division Principle: Let $f : X \to Y$ be a function such that $f^{-1}(y) = \{x \varepsilon X : f(x) = y\}$ and $|f^{-1}(y)| = m \ \forall \ y \varepsilon Y$, then $|Y| = \frac{|X|}{m}$;
- Binomial Theorem: $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$;
    - Pascal Triangle Inequality: $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$;
- $tl(n) = n^{n-2} \ \forall n \geq 2$;
- $tu(n) * n! \geq tl(n)$

Catalan Numbers:

Concepts & Definitions:

- Catalan Numbers: Let C'_n defines the number of ordered sequences consisting of $n\ (+1)$s and $n\ (-1)$s. $C'_n = \binom{2n}{n}$;
    - C_n defines all above-mentioned sequences with the additional restriction that all partial sums must be non-negative;
- Dyck Path: A path from $(0, 0)$ to $(2n, 0)$ on the cartesian plane consisting of steps $(+1, +1)$ and $(+1, -1)$ such that the path never goes below the x-axis. There are C_n such paths;
- Rooted Plane Tree with $n+1$ vertices: A tree with a specified root and n children. There are C_n such trees;
- Planted Trivalent Tree with $2n+2$ vertices: A dedicated root vertex has degree 1, all other vertices have degree 3 or 1. There are C_n such trees;
- Triangulations of a $(n+2)$-gon, there are C_n ways of triangulating a labelled $(n+2)$-gon;

Theorems, Lemmas, Claims, [...] (w/o proofs):

- $C_n = \frac{1}{n+1}\binom{2n}{n}$;
- For $n \geq 1$: $C_n = C_0 C_{n-1} + C_1 C_{n-2} + ... + C_{n-2} C_1 + C_{n-1} C_0$;

Generating Functions:

- Generating function: a way of encoding an infinite sequence of numbers by treating them as coefficients of a power series;
    - $F(x) = \sum_{n=0}^{\infty} f(n) x^n$
- Determine $f(n)$ (the desired infinite sequence) by considering $F(x)$;
- Method for determining $f(n)$:
    - Find a recursion for $f(n)$

    - Multiply each term of the recursion by x^n and sum over values of n for which recursion holds
    - Solve the resulting equation to find $F(x)$
    - By expressing $F(x)$ as a power series, determine $f(n)$
- Suppose we are given k disjoint sets $S_1, S_2, ..., S_k$, let $f_i(n)$ be the number of valid ways of choosing n objects from set S_i. Furthermore, let $F_i(x) = \sum_{n=0}^{\infty} f_i(n)x^n$.
    - Let $f(n)$ be the number of ways of choosing n objects from all above sets (and their associated constraints), and $F(x) = \sum_{n=0}^{\infty} f(n)x^n$. Then, $F(x) = F_1(x)F_2(x)...F_n(x)$
- Generalized Binomial Theorem: $(1+x)^r = \sum_{n=0}^{\infty} \binom{r}{n} x^n$
    - $\frac{1}{1+x} = \sum_{n=0}^{\infty} (-1)^n x^n$