EECS 70 Cheatsheet Yunhao Cao

Set Notation $|S|$ cardinality

$\cap$ and $\cup$ or/join $\emptyset$ Empty $\subseteq$ subset $\mathcal{P}(S)$ powerset (of S)

$B \setminus A = \{x \in B \mid x \notin A\}$ $\mathbb{C}$ complex $\mathbb{R} \setminus \mathbb{Q}$ irrational $\mathbb{R}$ real

$\mathbb{N}$ natural $\mathbb{Z}$ int $\mathbb{Q}$ rational $\{\frac{a}{b} \mid a, b \in \mathbb{Z} \wedge b \neq 0\}$

Implication

$P \Rightarrow Q \equiv \neg P \vee Q$

$\neg Q \Rightarrow \neg P$ contrapositive $\not\equiv Q \Rightarrow P$ converse

Proof.

Direct $A \to B$

Contradiction A, Assume $B \to \neg B \wedge \neg A$?

Induction { weak $P(0)\checkmark$, prove $P(n) \to P(n+1)$

strong $P(0), P(1) \cdots P(4)\checkmark$ prove $P(n-4) \wedge P(n-3) \cdots \wedge P(n) \to P(n+1)$

Cases (a) (b) ✓

Stable Matching

Well-ordering Principle

- To say the "first".
- $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then $\forall S \in \mathcal{P}(S) \setminus \emptyset$ has a smallest element.

- Halts
  proof: at least one job eliminate some candidate from list each day it doesn't halt. Max n^2 iterations.
- Improvement Lemma
  day k, C receives at least one offer $(J, \dots) \Rightarrow$ end of day k C has an offer she likes at least as much as J.
  $\therefore$ day $k+1$, the job C doesn't decline on day k propose again to C, which she likes at least as much as J. Therefore by the end of day $k+1$ ...
- Terminates with a matching
  - Suppose J unpaired. J offered to n cand. and got rejected by all of them $\to (n+1)$ jobs at least. contradiction.
- ALWAYS STABLE
  - (J, C) but $J: C^* > C$. argue (J, C^*) is rogue. But since J will propose to C^* before C, by Improvement Lemma C^* loves its current match $\geq J$. Therefore prefers it to J. $\therefore$ No Job can be involved in a rogue couple.
- Is employer optimal
  - Contradict: first day (k) which some job J had offer rejected by its optimal candidate C^*. On day k.
  $\therefore$ Optimal candidate, there must exist a STABLE pairing such that: $(\dots, (J, C^*), \dots, (C', J^*) \dots)$
  Clear that $C^*: J^* > J$ since it rejected J in favor of J^* on day k. Since day k is first day any job got rejected by its opt. cand., and J^* propose to C^*, meaning J^* likes C^* $\geq$ its optimal cand. Thus $J^*: C^* \geq C'$. therefore we can argue that in the STABLE pairing exists a rogue couple (J^*, C^*).
- Is cand. pessimal.
  $T = \{\dots, (J, C), \dots\}$ be employer-optimal output from propose and reject. for contradiction, exists $S = \{\dots, (J^*, C), \dots, (J, C'), \dots\}$ for which $C: J > J^*$. Then (J, C) is a rogue pair because C is J's optimal candidate and $C: J > J^*$.

GRAPH THEORY

Directed / Undirected Edge

u, v → neighbours / adjacent

$e \Rightarrow$ incident on u, v

$G = (V, E)$ → $v_1, v_2 \dots v_n$ are distinct (uses $\forall e \in E$ exactly once.)

(Simple)	(can repeat vertices)	(Eulerian)
path $v_1 \sim v_n$	walk	walk
cycle $v_1 \sim v_n v_1$	tour ($\subseteq$ walk)	tour

COMPLETE GRAPHS

$K_n (V, E) \Rightarrow e = \frac{n(n-1)}{2}$

K_n directed has $(u, v), (v, u) \in E$

PLANAR GRAPHS

- Drawn without crossings
- Doesn't contain $K_{3,3}$ / K_5

$K_{3,3}$ K_5

- Euler's formula $v + f = e + 2$
  Proof: $e = 0, v = f = 1$
  ① Tree: $f = 1$, and $e = v - 1$
  ② Not a Tree, Find Cycle and delete any edge from the cycle. $e--$ and $f--$

Can identify nodes in the graph connected as corresponding graph through paths such that no two path share vertex.

- Sides: edges that bound faces clockwise
  - Counted twice: if has face on both sides.
    $\sum_{i=1}^{f} s_i = 2e$
  - Assume $e \geq 2(v \geq 3)$. $\forall i (s_i \geq 3) \Rightarrow 3f \leq 2e$

$v + f = e + 2$

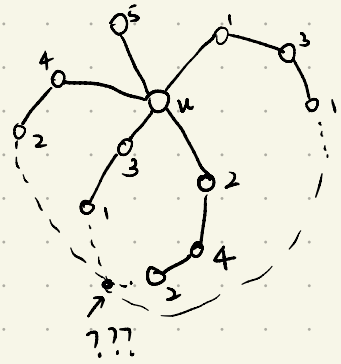
$\downarrow$

$-e - 6 \geq -3v$

$e \leq 3v - 2$ → planar graphs are sparse

Cannot have too many edges

- Duality
  $(G^*)^* = G$
  Start a vertex in center of each face, connect vertices if faces share vertex.
- Bipartite (can be 2-colored)
  - Vertices split into L, R groups and edges only go between groups.
  - Does not contain odd length cycles $\Rightarrow$ we can greedily color with two colors.
- FIVE COLOR THEOREM
  - If $e \leq 3v - 6 \to$ we're done.



Hypercubes

$V = \{0, 1\}^n$, vertices are connected if they differ in one bit.

$e = \frac{2^n \cdot n}{2}$

2^n: # of v ; n: # of possible bits to flip for each vertex

Let $S \subseteq V$ ($|S| \leq |V - S|$). E_S is the set of edges connecting S to $V - S$. Holds that $|E_S| \geq |S|$

Euler's Theorem

G (undirected) has an Eulerian tour iff $2 \mid \deg(a)$ and connected (except for isolated vertices)

only if: G has Eu. tour → G is connected and G has even deg.
Every vertex connected by an edge must be on tour, thus connected to other vertices.
All edges incident to a vertex must be paired up. enter $\Leftrightarrow$ exit. first $\Leftrightarrow$ last entering first edge.

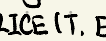
if: G has even deg. G is connected $\Rightarrow$ G has Eu. tour.

def FindTour(G, s):
tries to travel G by pick an edge starting in S. always returns a tour (though not always Eulerian) starting and ending in s (since all vertices have even degs.).

def SPLICE($T, T_1, \dots T_n$): $\Rightarrow T_1 \dots T_n$ are Eulerian Tours that share goes along T but when no edges but intersect with T. intersects with T_i, traverses through T_i then continue.

```
def EULER(G, s):
    T = findTour(G, s)
    Let G1 ... Gk be connected components
    when edges from T is removed from
    G. and they intersects T first at s1 ... sk.
    Output SPLICE(T, Euler(G1, s1) ... Euler(Gk, sk));
end Euler.
```

Trees



- connected. no cycles
- $v = e + 1$
- delete any edge, disconnected.
- adds an edge, creates a cycle

EECS70 CheatSheet Yunhao Cao

Modular Arithmetic

① $x' \pmod m$ exists when $\gcd(m,x)=1$

when x' exists, it is UNIQUE over mod n.

② $x \geq y > 0$. $\gcd(x,y) = \gcd(y, x \pmod y)$ ($r = x - qy$; gcd divides x divides y; gcd divides r; divides y; gcd divides $r+qy$)

$\gcd(x,0) = x$.

③ to find inverse,

$ax + bm = \gcd(x,m)$

$x' \equiv a \pmod m$ if $\gcd(x,m)=1$.

- extended-gcd(x,m) ⇒ returns d, a, b

if $y=0$ then return $(x,1,0)$ → $x = 1x + 0$

else

$(d', a', b') :=$ extended-gcd$(m, x \pmod m)$ →

return$(d, b', a' - (x \operatorname{div} m) * b')$

$d' = \gcd(m, x \pmod m) = a'm + b'(x - \lfloor \frac{x}{m} \rfloor m)$

$d = d' = b'x + (a' - \lfloor \frac{x}{m} \rfloor) m$

CRT

$n_1, \dots n_k \in \mathbb{Z}^+$, coprime, $N = \prod_{i=1}^{k} n_i$

$x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$, $x \equiv a_3 \pmod{n_3}$ ....

$\Downarrow$

$x \equiv (\sum_{i=1}^{k} a_i b_i) \pmod N$

$b_i = \frac{N}{n_i} (\frac{N}{n_i})^{-1}$

$\Downarrow$

$(\frac{N}{n_i})^{-1} \pmod{n_i}$

FLT

$a^{n-1} \equiv 1 \pmod n \iff a^n \equiv a \pmod n$ (n is prime)

$a \neq -1, 1, 0$

RSA

P, q prime $N = pq$, e is small prime.

message x, encrypt$(x) = x^e \pmod N$

$d = e^{-1} \pmod{(p-1)(q-1)}$, decrypt$(x^e) = (x^e)^d \pmod N$

to validate, use CRT.

Secret Sharing

secret at $P(0)$. Give $P(1), P(2), \dots$ in GF(N)

Lagrange Interpolation

$\Delta_i(x) = \frac{\prod_{j \neq i} (x - x_j)}{\prod_{j \neq i} (x_i - x_j)}$ ⇒ $P(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$

Error Correcting Codes

General Error

$Q(x) = P(x) E(x)$ $\quad E(x) = \prod (x - e_i)$

Note that $P(i)E(i) = r_i E(i)$

$Q(i) = r_i E(i)$

Counting

Binomial Theorem

$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

$\binom{n}{k+1} = \binom{n-1}{k} + \binom{n-2}{k} + \dots + \binom{k}{k}$

Derangements

$D_n = (n-1)(D_{n-1} + D_{n-2}) = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Inclusion-Exclusion

$|A_1 \cup \dots \cup A_n| = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,\dots,n\}: |S|=k} |\cap_{i \in S} A_i|$

$= \sum_{i=1}^{n} |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| \dots$

Countability

If we can reach a bijection between S and $\mathbb{N}$, then S is countable.

Diagonalization Proof.

$0.①_2 \; 5 \; 1 \; 2 \; 5 \dots$

$0.1③ \; 5 \; 1 \; 4 \; 5 \dots$

$\ddots$

Computability

Uncomputable if we can solve the Halting problem.

Probability Theory

$\mathbb{P}[A] = \sum_{w \in A} \mathbb{P}(w)$

$\mathbb{P}[w|B] = \frac{\mathbb{P}(w)}{\mathbb{P}(B)}$

$\mathbb{P}[A|B] = \frac{\mathbb{P}[A \cap B]}{\mathbb{P}[B]} = \frac{\mathbb{P}[B|A]\,\mathbb{P}[A]}{\mathbb{P}[B]}$

$\mathbb{P}[B] = \sum_{i=1}^{n} \mathbb{P}[B \cap A_i] = \sum_{i=1}^{n} \mathbb{P}[B|A_i]\,\mathbb{P}[A_i]$

Independance:

$\mathbb{P}[A|B] = \mathbb{P}[A]$, $\mathbb{P}[B|A] = \mathbb{P}[B]$

Inclusion-Exclusion:

$\mathbb{P}[A_1 \cup \cdots \cup A_n] = \sum_{k=1}^{n} (-1)^{k-1} \sum_{S \subseteq \{1,\dots,n\}, |S|=k} \mathbb{P}[\cap_{i \in S} A_i]$

$= \sum_{i=1}^{n} \mathbb{P}[A_i] - \sum_{i<j} \mathbb{P}[A_i \cap A_j] + \sum_{i<j<k} \mathbb{P}[A_i \cap A_j \cap A_k] - \cdots$

Markov's Inequality (≥ 0 rvs only)

$\mathbb{P}[X \geq c] \leq \frac{\mathbb{E}[X]}{c}$

(Generalized) $\mathbb{P}[|Y| \geq c] \leq \frac{\mathbb{E}[|Y|^r]}{c^r}$

Chebyshev's Inequality

$\mathbb{P}[|X - \mu| \geq c] \leq \frac{\mathrm{Var}(X)}{c^2}$

Law of Large Nums

$\mathbb{P}[|\frac{1}{n} S_n - \mu| > \varepsilon] \leq \frac{\mathrm{Var}(\frac{1}{n}S_n)}{\varepsilon^2} = \frac{\sigma^2}{n\varepsilon^2} \to 0$ as $n \to \infty$

Inference Function

$C(g) = \mathbb{E}[c(Y, g(X))]$

(expected error; cost)

LLSE:

$\mathrm{cost} = |Y - a - bX|^2$

$L[Y|X] = a + bX = \mathbb{E}(Y) + \frac{\mathrm{cov}(X,Y)}{\mathrm{var}(X)}(X - \mathbb{E}(X))$

b proj of Y onto $g(X) \to$ Linear functs of X

Linear Regression → Converges to LLSE

observes k samples $(X_i, Y_i) \cdots$

$\mathrm{cost} = \frac{1}{k} \sum_{k=1}^{K} |Y_k - a - bX_k|^2$

MMSE: $g(x) = \mathbb{E}[Y|X]$

$\mathbb{E}[Y|X=x] = \sum_y y\, \mathbb{P}[Y=y|X=x] = \sum_y y \frac{\mathbb{P}[X=x, Y=y]}{\mathbb{P}[X=x]}$

Random Variable (Discrete)

$X: \Omega \to \mathbb{R}$ (discrete: $x(w) : w \in \Omega$)

Bernoulli Distribution $X \sim \mathrm{Bernoulli}(p)$

$\mathbb{P}[X=i] = \begin{cases} p & \text{if } i=1 \\ 1-p & \text{if } i=0 \end{cases}$

Binomial Distribution $X \sim \mathrm{Bin}(n, p)$

$\mathbb{P}[X=i] = \binom{n}{i} p^i (1-p)^{n-i}$

Hypergeometric Distribution $Y \sim \mathrm{hypergeometric}(N, B, n)$ (total balls, total black balls, sample #)

$\mathbb{P}[Y=k] = \binom{n}{k} \frac{B}{N} \times \frac{B-1}{N-1} \cdots \frac{B-k+1}{N-k+1} \times \frac{N-B}{N-k} \times \cdots \times \frac{N-B-(n-k)+1}{N-n+1}$

(getting k black balls; sampling without replacement)

$= \frac{\binom{B}{k}\binom{N-B}{n-k}}{\binom{N}{n}}$

Joint distribution of X and Y

$\{((a,b), \mathbb{P}[X=a, Y=b]) : a \in A, b \in B\}$

$\mathbb{P}[X=a] = \sum_{b \in B} \mathbb{P}[X=a, Y=b]$

Independence of X and Y:

$\mathbb{P}[X=a, Y=b] = \mathbb{P}[X=a]\,\mathbb{P}[Y=b] \quad \forall a, b$

Expectation

$\mathbb{E}[X] = \sum_{a \in A} a \times \mathbb{P}[X=a]$

$\mathbb{E}[X+Y] = \mathbb{E}[X] + \mathbb{E}[Y]$

$\mathbb{E}(cX) = c\,\mathbb{E}(X)$

Tail Sum Formula

If X takes values $\{0, 1, 2 \cdots\}$,

$\mathbb{E}[X] = \sum_{i=1}^{\infty} \mathbb{P}[X \geq i]$

Continuous RV.

PDF $= f(x)$

$\mathbb{P}[a \leq X \leq b] = \int_a^b f(x)\,dx$

CDF $= F(x) = \mathbb{P}[X \leq x] = \int_{-\infty}^{x} f(z)\,dz$

$\mathbb{E}(X) = \int_{-\infty}^{\infty} x\, f(x)\,dx$

$\mathrm{Var}(X) = \int_{-\infty}^{\infty} x^2 f(x)\,dx - (\mathbb{E}(X))^2$

Joint Density:

JDF: $f: \mathbb{R}^2 \to \mathbb{R}$

$f(x,y) \geq 0 \quad \forall x, y \in \mathbb{R}$

$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(x,y)\,dx\,dy = 1$

Exponential distribution (geometric) $X \sim \mathrm{Exp}(\lambda)$

$f(x) = \begin{cases} \lambda e^{-\lambda x} & (x \geq 0) \\ 0 & \text{otherwise} \end{cases}$

$\mathbb{E}(X) = \frac{1}{\lambda}$ $\mathrm{Var}(X) = \frac{1}{\lambda^2}$

Function of RV.

If $Y = f(X)$, $\mathbb{E}(Y) = \sum_x f(x)\,\mathbb{P}[X=x]$

Variance

$\mathrm{Var}(X) = \mathbb{E}[(X-\mu)^2] = \mathbb{E}(X^2) - 2\mathbb{E}(X\mu) + \mathbb{E}(\mu^2) = \mathbb{E}(X^2) - 2\mu^2 + \mu^2$

$= \mathbb{E}(X^2) - \mu^2$

$\mathrm{Var}(cX) = c^2 \mathrm{Var}(X)$

$\mathrm{Var}(X+Y) = \mathrm{Var}(X) + \mathrm{Var}(Y) + 2\mathrm{Cov}(X,Y)$

$\mathrm{Cov}(X,Y) = \mathbb{E}(XY) - \mathbb{E}(X)\mathbb{E}(Y)$

If X and Y independent, $\mathbb{E}(XY) = \mathbb{E}(X)\mathbb{E}(Y)$

$\mathrm{Corr}(X,Y) = \frac{\mathrm{Cov}(X,Y)}{\sigma(X)\sigma(Y)}$

(σ: SD of $X = \sqrt{\mathrm{Var}(X)}$)

Geometric Distribution $X \sim \mathrm{Geometric}(p)$

"how many times do we have to wait"

$\mathbb{P}[X=i] = (1-p)^{i-1} p$

$\mathrm{Var}(X) = \frac{1-p}{p^2}$ $\mathbb{E}(X) = p \sum_{i=1}^{\infty} i(1-p)^{i-1}$

Poisson Dist $X \sim \mathrm{Poisson}(\lambda) \to Y \sim \mathrm{Binomial}(n, \frac{\lambda}{n})$ as $n \to \infty$

$\mathbb{P}[X=i] = \frac{\lambda^i}{i!} e^{-\lambda}$

$\mathbb{E}(X) = \lambda$ $\mathrm{Var}(X) = \lambda$

$X \sim \mathrm{Poisson}(\lambda)$ and $Y \sim \mathrm{Poisson}(\mu)$, XY independent,

$X + Y \sim \mathrm{Poisson}(\lambda + \mu)$

Normal Distribution (cont.)

$\mu \in \mathbb{R}$, $\sigma > 0$ $\quad X \sim N(\mu, \sigma^2)$

$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(x-\mu)^2/(2\sigma^2)}$

$\mathbb{E}(X) = \mu$, $\mathrm{Var}(X) = \sigma^2$

$\mu = 0, \sigma = 1 \to$ standard N

$X \sim N(0,1)$ and $Y \sim N(0,1)$, XY independent, then

$Z = aX + bY \sim N(0, a^2 + b^2)$

$X \sim N(\mu_x, \sigma_x^2)$ and $Y \sim N(\mu_y, \sigma_y^2)$

XY independent, then

$Z = aX + bY \sim N(\mu_x + \mu_y, a^2\sigma_x^2 + b^2\sigma_y^2)$

Central Limit Theorem

$S_n = \sum_{i=1}^{n} X_i$, X_i are iid. rv.

$\mathbb{E}(X_i) = \mu$.

then

$\mathbb{P}[\frac{S_n - n\mu}{\sigma\sqrt{n}} \leq c] \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{c} e^{-x^2/2}\,dx$