Prep: bring ID, water, pen and the handwritten version of this set of notes
You got this!

Logic and Function

Implies: $P \implies Q \equiv \neg(P \wedge \neg Q) \equiv \neg P \vee Q$
Converse: $Q \implies P$
Inverse: $\neg P \implies \neg Q$
Contrapositive: $\neg Q \implies \neg P$
De Morgan's Law:

$$\neg(P \wedge Q) \equiv (\neg P) \vee (\neg Q)$$
$$\neg(P \vee Q) \equiv (\neg P) \wedge (\neg Q)$$
$$\neg(\forall x\, P) \equiv \exists x\, (\neg P)$$
$$\neg(\exists x\, P) \equiv \forall x\, (\neg P)$$

Final Checks

- *Check if it is Stable Matching or Propose-and-Reject problem.*
- Polynomials in GF must mod coefficients
- RSA: write N, e, d explicitly to avoid errors
- $0 \in \mathbb{N}$ for this class
- Be careful of the bound in vertex coloring
- Be careful of base cases for graph
- Counting: rotations / inversions included?

Graph Theory (Definition)

Path: a sequence of edges, vertices distinct.
Cycle: a path (distinct vertices) with $v_1 = v_n$
Walk: a path without distinct vertices condition
Tour: a walk with $v_1 = v_n$

A cycle is a walk. A tour is a walk.

Eulerian walk: uses all edge exactly once.
Eulerian tour: walk that ends at start vertex
Hamiltonian walk/cycle: a walk/cycle that visits all vertices *exactly once*.
Hypercube $(\dim N)$: 2^N nodes, $N2^{N-1}$ edges

Function

$$f(X) = \{y \mid \exists x \in X \text{ s.t. } y = f(x)\}$$

$$f^{-1}(Y) = \{x \mid f(x) \in Y\}$$

Stable Matching

When a candidate does not immediately reject a job, the job is still assumed to "propose" to the candidate on the next day.

[Improvement Lemma] Candidate's matching can only improve. (exchange argument)

Job-Propose and Reject always terminate with matching (contradiction), gives job-optimal and candidate-pessimal (contradiction).

Job	I	II	III	C	I	II	III
A	1	2	3	1	B	C	A
B	2	3	1	2	C	A	B
C	3	1	2	3	A	B	C

$\{(A,1),(B,2),(C,3)\}$, $\{(A,3),(B,1),(C,2)\}$, $\{(A,2),(B,3),(C,1)\}$ are all stable.

Graph Theory

Lines of Attack: Induction on $|V|$, $|E|$, tree-shaving (removal of leaf node), Eulerian tours, pigeonhole,

Euler's Theorem: Planar graphs with $v \geq 3$ satisfy $v + f = e + 2$
Corollary: All planar graphs satisfy $e \leq 3v - 6$
$K_{3,3}$ **Variant**: $e \leq 2v - 4$
Kuratowski's Theorem: A graph is planar iff it doesn't contain K_5 or $K_{3,3}$

Coloring

- A graph with max degree k is $k+1$ colorable. (induct on $|V|$)
- A connected graph of max degree $d \geq 2$ can be vertex colored with d colors so long as $\exists$ vertex with degree $< d$. ($|V|$)
- Graph with max degree $d \geq 1$ can be edge colored in $2d - 1$ colors. (induct $|E|$)

Stable Matching Trivia

- Always exists a candidate who is not proposed to until the last day.
- Propose-and-reject algorithm must terminate in at most $(n-1)^2 + 1$ days.
- For even $n \geq 2$, exists instance of stable matching of n jobs and candidates with at

Error Correcting Codes

Message of n packets $(m_1, m_2, \ldots, m_n)$ where $m_i = P(i)$ for some polynomial P of at most degree $n - 1$.

Bounding of $GF(q)$, q prime:

$$q \geq \max(m_i + 1, n + k)$$
$$q \geq \max(m_i + 1, n + 2k)$$

least $2^{n/2}$ distinct stable matching. (induct on n) • In a job propose algorithm, jobs can't lie to improve their own outcomes, but can to improve others. • If candidate rejects a job in JPA, there is no stable matching in which the candidate and job is paired. • If a candidate misbehaves (rejects falsely), then it is the only candidate that can be in a rogue couple.	Error Correction: $Q(x) = P(x)E(x)$ $Q(x_i) = r_i E(x_i)$ $E(x) = (x - e_1) \dots (x - e_k)$ Fractional variant: $n'(1-\alpha) = n \Longrightarrow n' = \frac{n}{1-\alpha}$ $n'(1-2\alpha) = n \Longrightarrow n' = \frac{n}{1-2\alpha}$
RSA	Secret Sharing
Key (N, e, d). (N, e) is public. d is private. $N = pq$ where p, q are large primes. p, q must be secret, but if forgotten it's fine. Only requires d to decode. $\left(e, (p-1)(q-1)\right) = 1$ $d^{-1} \equiv e \ (\text{mod}\ (p-1)(q-1))$ $E(x) = x^e \ (\text{mod}\ N)$ $D(x) = x^d \ (\text{mod}\ N)$ Security relies on the computational intractability of obtaining x in $y = x^e \ (\text{mod}\ N)$	Bounding of $GF(q)$, q prime: Secret sharing among m people (the $+1$ comes from the secret): $q \geq \max\,(s+1, m+1)$ Can delegate sub-polynomials for hierarchy. Spy variants: spies can corrupt messages.