CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Hug, Sabin

Midterm

PRINT Your Name: ______________________________, ______________________________
(last) (first)

PRINT Your Student ID: ______________________________

PRINT Your Exam Room: ______________________________

SID of the person sitting to your left: ______________________________

SID of the person sitting to your right: ______________________________

SID of the person sitting in front of you: ______________________________

SID of the person sitting behind you: ______________________________

Read This.

- There will be no clarifications. We will correct any mistakes post-exam in as fair a manner as possible. Please just answer the question as best you can and move on even if you feel it is a mistake.
- Due to the above. Please move on. There are lots of problems to get points from. Do not get stuck. This is good advice anyway. In fact, we repeat it below.
- Anything written outside the boxes provided will not be graded.

Advice.

- The questions vary in difficulty. In particular, the exam is not in the order of difficulty and quite accessible short answer and proof questions are late in the exam. No points will be given for a blank answer, and there will be no negative points on the exam. **So do really scan over the exam.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult only *one sheet of notes on both sides*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture, unless otherwise stated. That is, if we ask you to prove a statement, prove it from basic definitions, e.g., "$d \mid x$ means $x = kd$ for some integer k" is a definition.**
- The exam has 160 points. Some questions where you are asked to prove something are worth more points, but not always that much more, so move on if you get stuck and come back later.

1. Warmup

1. (2pts) If 6 is prime, then trees can walk. ○ True ○ False
2. (2pts) $\neg(P \implies Q) \equiv (\neg P \land \neg Q)$ ○ True ○ False
3. (6pts) Let $m,n,a \in \mathbb{Z}$. Prove that if $a \nmid mn$, then $a \nmid m$ and $a \nmid n$.
   (Recall: $c \nmid d$ means c does not divide d.)

2. The Logic Of Bloof

You are designing a small indie video game and need to encode the game's mechanics in logic! You've set up the following states for Bloof, your game's avatar:

J: Bloof is jumping

G: Bloof is on the ground

M: Bloof is in motion

H: Bloof is healing

W: Bloof is clinging to the wall

1. (3pts) Use the propositions defined above to express in propositional logic the following statement: "Bloof is not healing unless Bloof is not in motion."

2. (3pts) Write the *contrapositive* of the following statement using the above propositions in propositional logic: "If Bloof is jumping, then Bloof is not on the ground and is in motion." (Note: Be careful with your parentheses.)

3. (4pts) Let's say you now have a new draft of the logic you want in the game (ignore any answers you got in previous statements):

   - $H \implies \neg M$
   - $J \implies (\neg G \wedge M)$
   - $\neg(G \wedge W)$
   - $\neg G \implies (M \vee J)$

   If we set it so that Bloof is healing (i.e. H is True), what can you say about the proposition W?

   ○ True ○ False ○ Could be either

3. Proofs

1. (6pts) Prove that for all $n \in \mathbb{N}$, n is odd if and only if $5n+3$ is even.

2. (6pts) Prove that $7 \mid (2^{n+2} + 3^{2n+1})$ for all $n \in \mathbb{N}$.

4. Stable(?) Matchings

1. Consider the following preference lists for jobs, A, B, C and candidates $1, 2, 3$.

Jobs	Preferences
A	$2 > 3 > 1$
B	$2 > 3 > 1$
C	$1 > 3 > 2$

Candidates	Preferences
1	$A > B > C$
2	$A > C > B$
3	$C > A > B$

(a) (4pts) Consider the following pairing: $(A, 1)$, $(B, 2)$, and $(C, 3)$. Is this matching stable?

○ Yes ○ No

If you answered *No*, name a rogue couple.

(b) (4pts) Describe a stable matching between jobs and candidates from these preferences (if the previous question's pairing was stable, then list a different matching that is also stable).

A: □ B: □ C: □

For the following parts, determine whether the statement is true or false.

2. (3pts) It is impossible for a pairing to be stable if the pairing has a couple (J, C) such that C is J's least favorite candidate and J is C's least favorite job.

○ True ○ False

3. (3pts) If a job is paired with the same candidate in every stable matching, then that candidate is at the top of the job's preference list.

○ True ○ False

4. (3pts) In a stable matching instance, if we run the propose-reject algorithm twice, once with jobs proposing and once with candidates proposing and the exact same pairing is produced by both runs, what can we say about the number of stable matchings?

○ None ○ Exactly one ○ Must be more than one ○ Not determined by this outcome

5. Graphs w/ Friends

All graphs are simple and undirected unless otherwise specified.

1. (3pts) The complete graph K_4 has an Eulerian tour. ○ True ○ False
2. (3pts) K_6 is planar. ○ True ○ False
3. (3pts) You're babysitting 6 children and each tells you how many friends they have in the group: One child has 4 friends, two children have 3 friends, one child has 2 friends, and two children have 1 friend. Assuming all friendships are mutual (i.e. if child A is friends with child B, then child B is friends with child A, and this counts as exactly 1 friendship), how many distinct friendships are there total amongst the children?

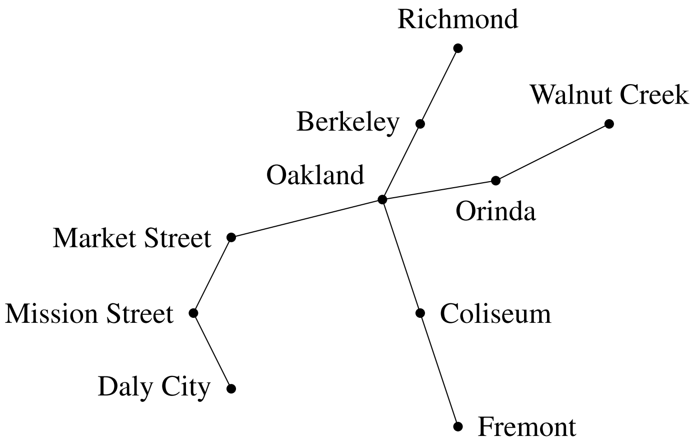
   □

4. (3pts) In a 5-dimensional hypercube (i.e. the vertices are all 5-bit strings where two vertices share an edge if they differ in exactly one bit location), what is the length of the shortest path from the vertex labeled 10010 to the vertex labeled by 01000?

   □

6. Euler's BART Speedrun

Consider the following (simplified) graph of the BART train network.



1. (2pts) Is the BART network graph a tree?

   ○ Yes ○ No

2. (2pts) Is the BART network graph bipartite?

   ○ Yes ○ No

3. (2pts) What is the minimum number of colors needed to edge color the BART network graph?

In recent years, many people have attempted to "speed run" the system. To "speed run" the system, you must visit every edge on the graph. After hearing about this trend, BART planners are considering using graph theory to expand the network to better accommodate speedrunners.

Recall: An Eulerian Walk is a walk that uses each edge exactly once. An Eulerian Tour is the same as an Eulerian Walk except that your walk must end on the vertex you started on.

1. (3pts) Does the BART network graph contain an Eulerian walk?

   ○ Yes ○ No

   If you answered *No*, what edge can be added for it to contain one (if there are multiple possible answers, just choose one)?

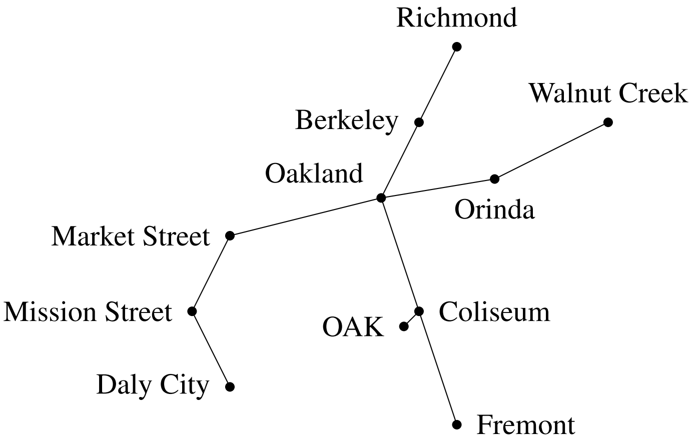
2. (3pts) Feeling unsatisfied, a small group of speedrunners are now attempting an "extreme speedrun" which starts and ends at the same station.

   These speedrunners are looking for *Eulerian tour*; which two edges could be added to the BART network graph to create an Eulerian tour?

   If there are multiple possible pairs, choose one pair of edges that creates Eulerian tour.

3. (3pts) Speedrunners aren't the BART network planner's only priority.

   To encourage tourism, BART has added one edge and one vertex to the network graph to create a new line to the Oakland International Airport (OAK):



   To appease concerned locals, BART will not add more edges to the OAK vertex. The OAK vertex, therefore, will always be degree one and an Eulerian tour of the network cannot exist. What restriction does this place on any Eulerian *walks* in the system, even if many more edges are added amongst *other* stations? Say the restriction in 10 words or less but don't provide justification.

7. **Graph Induction** (8pts)

For a graph $G = (V,E)$, we know the Degree-Sum Formula (a.k.a. The Handshake Lemma):

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

We've argued intuitively that this is true because each edge is double-counted. This makes perfect sense, but we're in CS70 and we want to *rigorously* prove that this is true. Use induction to prove that the degree-sum formula holds for all undirected graphs.

8. Modular Arithmetic

When working under arithmetic modulo N, give your answers in the range $\{0, 1, \ldots, N-1\}$.

1. (3pts) 5 divides $6^n - 1$ for all $n \in \mathbb{N}$. ○ True ○ False
2. (3pts) If $xy \equiv 0 \pmod 6$, then either $x \equiv 0 \pmod 6$ or $y \equiv 0 \pmod 6$. ○ True ○ False
3. (3pts) 9 divides $4^m + 5^m$ for all **odd** $m \in \mathbb{N}$. ○ True ○ False
4. (3pts) Let $p > 3$ be a prime. Twin primes are two prime numbers that are only 2 apart – i.e. p and q prime such that $q = p + 2$. For $p < q$ twin primes, what values can $p \pmod 3$ be? Write your answer(s) as an integer(s).

   □

5. (4pts) What is the last digit of the number 9^{68} (i.e. what number 0-9 is in the "one's place")?

   □

6. (4pts) Bob implements RSA, generating primes $p = 5$ and $q = 7$ with encryption exponent $e = 5$. What is the decryption exponent d that he computes for himself?

   □

7. (4pts) Bob needs values x and y from Alice for a calculation. She uses Bob's public key to encrypt the values, $a \equiv x^e \pmod N$ and $b \equiv y^e \pmod N$, but before sending a and b she remembers that Bob's calculation only needs the value $xy \pmod N$. Alice just multiplies a and b and sends $ab \pmod N$. Does decrypting this actually get $xy \pmod N$ like Bob wanted? Justify your answer (assume RSA was set up correctly and works as we've seen).

9. Chinese Remainder Theorem (8pts)

Consider the following congruences:

$$\begin{aligned} x &\equiv a \pmod{p} \\ x &\equiv b \pmod{q} \end{aligned}$$

where p,q are coprime. Recall that the Chinese Remainder Theorem tells us that there exists a unique solution $x \pmod{pq}$.

Now, consider the new system of congruences:

$$\begin{aligned} cx &\equiv ca \pmod{cp} \\ dx &\equiv db \pmod{dq} \end{aligned}$$

Where c,d are nonzero natural numbers. How many solutions x in mod $cdpq$ exist (if any)? Justify your answer.

10. Polynomials

We say a polynomial is of degree d if it can be written in the form $a_d x^d + a_{d-1} x^{d-1} + \cdots a_0$. We say that a polynomial is of degree exactly d if $a_d \neq 0$.

1. Polynomial $f(x)$ has degree exactly k and polynomial $g(x)$ has degree exactly $j < k$. Consider these polynomials over the reals $\mathbb{R}$.

   (a) (3pts) What is the degree of $h(x) = f(x) + g(x)$?

   (b) (3pts) What is the degree of $r(x) = f(x)g(x)$?

2. (4pts) Over $GF(5)$, find an equivalent polynomial $g(x)$ (i.e. outputs the same values when given the same inputs) to $f(x) = 4x^{84} + x^{23} + 2x^5 + 3$ such that g has degree strictly less than 5. That is, it should be the case that $\forall x \in \mathbb{Z}$, $f(x) \equiv g(x) \pmod 5$.

3. (4pts) Give a polynomial of degree 2 over GF(7) that contains the points $(0,1)$, $(3,0)$, and $(4,0)$.

4. (4pts) You know two points on a polynomial of degree at most 4. How many polynomials over GF(5) are there that could be the polynomial that you got your two points from? Write an integer.

11. Pineapple on Pizza?!

CS70 staff is split between pineapple and pepperoni pizza. The EECS credit card number is stored in a secret polynomial at $f(0)$. The EECS department is broke and can only afford a single polynomial. Design a secret sharing scheme using points from *one polynomial* so that ties can be broken according to the constraints:

- Professors (2 people): If both professors agree, they can unlock $f(0)$ with their points.
- Head TAs (4 people, only matters if professors tie): 1 Professor and ($\geq$) 3 Head TAs can share their points to unlock $f(0)$.
- TAs (7 people, only matter if professors tie and Head TAs tie): 1 professor, 2 Head TAs, and ($\geq$) 4 TAs can share their points to unlock $f(0)$ together.

Assume $f(0)$ can't be recovered with less people than what is described in the constraints. For example, 1 Professor and 3 Head TAs can unlock the secret, but 4 Head TAs and 7 TAs alone cannot unlock the secret if they do not have the support of a Professor.

1. (1 point each for parts (a) through (d), 2 points for part (e))
   Fill in the blanks to complete the following secret sharing scheme that satisfies these conditions.

   We encode the secret number as $P(0)$ in a degree ___(a)___ polynomial $P(x)$.

   In order to satisfy the first condition (where both professors agree), each professor receives ___(b)___ points on $P(x)$.

   In order to satisfy the second condition (where 1 professor and $\geq$ 3 Head TAs agree), each Head TA receives ___(c)___ points on $P(x)$.

   Lastly, in order to satisfy the third condition (where 1 professor, 2 Head TAs, and $\geq$ 4 TAs agree), each TA receives ___(d)___ points on $P(x)$.

   We will work in a Galois Field for a sufficiently large prime p. Firstly, p needs to be large enough such that the secret s is not truncated. Next, all points given out to Professors, Head TAs, and TAs (**as well as the point** $(0, f(0))$ **reserved for the secret**) must all be distinct. To ensure that we have enough points to give out, we will work in a Galois Field for a prime $p \geq$ ___(e)___. (Give a tight bound. You may write your answer potentially in terms of s, as well as the *max* function.)

(a)

(b)

(c)

(d)

(e)

2. (4pts) Discard your answer to the previous problem (i.e. this will not depend on it). Say a degree 9 polynomial was used for the secret sharing scheme. Enough of the CS70 staff agree on a type of pizza and they gather their shares of secret points in a pile to recover the polynomial!

   But one of the professors wrote down **two** of his points incorrectly (*ahem*, Professor Hug...). All of the points are already mixed together and we can't tell which points are the two errors. Luckily, everyone loves pineapple pizza so much that there were more points than needed in the pile! Assuming those were the only two corrupted points, what is the minimum number of points that needed to have been in the pile to still be able to unambiguously recover the polynomial?

12. Counting.

Throughout this question, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you should not use any summation or product notation (i.e. you may not use $\sum$ or $\prod$).

1. (4pts) You receive a message of 30 bits. Over the transmission 12 errors occurred (12 of the bits were flipped) but you don't know which ones were corrupted. How many possible ways could those 12 errors have been distributed across message?

2. (4pts) How many polynomials of degree *exactly* $d < p$ are there over $GF(p)$ for a prime p (i.e. using coefficients from $\{0,1,2,\ldots,p-1\}$)?

3. (4pts) You're selecting a 6-digit pin using the numbers 0-9, but the number pad you're using is awful. Each button you press gets stuck so you can only ever use a number once. How many different 6-digit pins could you choose with this broken number pad?

4. (4pts) A restaurant sells 5 different pre-packaged frozen dishes and you want to buy 10 meals to keep yourself easily fed while studying for a midterm. How many different ways can you make this purchase, assuming they never sell out of any dish and you buy all 10 meals at once?

13. Doodle Page.

Feel free to use this page for scratch work, providing any comments about the exam, or to draw a fun picture!