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

Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

Do not turn this page until your instructor tells you to do so.

1. Warmup

1. (2pts) If 6 is prime, then trees can walk.

   Answer: True. The antecedent is false so the statement is vacuously true

2. (2pts) $\neg(P \implies Q) \equiv (\neg P \land \neg Q)$

   Answer: False. $(P \implies Q) \equiv (\neg P \lor Q)$ and $\neg(\neg P \lor Q) \equiv (P \land \neg Q)$.

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.)

   Answer: Contrapositive: Assume the negation of the consequent, which is $\neg(a \nmid m \land p \nmid n) \equiv (a \mid m \lor p \mid n)$ (we Want To Show the negation of the antecedent to complete the contrapositive proof: $a \mid mn$). Without Loss Of Generality, assume $a \mid n$ (the argument will be analogous for if $a \mid n$). Then $\exists k \in \mathbb{Z}$ such that $n = ak$. Thus $mn = (ak)n = a(kn)$. Since $kn \in \mathbb{Z}$, we have that $a \mid mn$.

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

M: Bloof is in motion

W: Bloof is clinging to the wall

G: Bloof is on the ground

H: Bloof is healing

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."

   Answer: $M \implies \neg H$ or $H \implies \neg M$. Both are equivalent.

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.)

   Answer: $(G \lor \neg M) \implies \neg J$

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):

   - $H \implies \neg M$
   - $J \implies (\neg G \land M)$
   - $\neg(G \land W)$
   - $\neg G \implies (M \lor J)$

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

   Answer: False. If H is true, then $\neg M$ follows. The contrapositive of the second rule says that $(G \lor \neg M) \implies \neg J$ and so its antecedent is satisfied by $\neg M$ and thus $\neg J$ is also true. The contrapositive of the last statement is that $(\neg M \land \neg J) \implies G$ and so we know G is true as well since we know $\neg M$ and $\neg J$ by now. Lastly, $\neg(G \land W) \equiv (\neg G \lor \neg W) \equiv (G \implies \neg W)$. Thus, since G is true, we know $\neg W$ follows and so W is always false.

3. Proofs

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

   Answer:

   $(\Longrightarrow)$ Assume n is odd. Then $\exists k \in \mathbb{Z}$ such that $n = 2k+1$. Thus $5n+3 = 5(2k+1)+3 = 10k+5+3 = 10k+8 = 2(5k+4)$. Since $5k+4$ is an integer, $5n+3$ is a multiple of 2, showing what we wanted.

   $(\Longleftarrow)$ Contrapositive: Assume n is even (we Want To Show that $5n+3$ is odd to complete the contrapositive proof). Then $\exists k \in \mathbb{Z}$ such that $n = 2k$. Thus $5n+3 = 5(2k)+3 = 10k+3 = 2(5k+1)+1$. Since $5k+1$ is an integer, we have written $5n+3$ according to the definition of an odd number and are done.

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

   Answer: One proof for this is by induction on n.

   Base Case: $n = 0$. $2^{0+2}+3^{2\cdot 0+1} = 4+3 = 7$ which is certainly divisible by 7.

   Inductive Hypothesis: Assume for a $k \in \mathbb{N}$ that $7 \mid (2^{k+2}+3^{2k+1})$.

   Inductive Step: Consider for $k+1$.

$$\begin{aligned}
2^{(k+1)+2}+3^{2(k+1)+1} &= 2^{k+3}+3^{2k+3} \\
&= 2\cdot 2^{k+2}+3^2\cdot 3^{2k+1} \\
&= 2\cdot 2^{k+2}+(2+7)\cdot 3^{2k+1} \\
&= 2\cdot 2^{k+2}+2\cdot 3^{2k+1}+7\cdot 3^{2k+1} \\
&= 2\cdot (2^{k+2}+3^{2k+1})+7\cdot 3^{2k+1} \\
&= 2\cdot 7j+7\cdot 3^{2k+1} \text{ (for some } j \in \mathbb{Z} \text{ by Inductive Hypothesis)} \\
&= 7\cdot (2j+3^{2k+1})
\end{aligned}$$

   This concludes the proof since $2j+3^{2k+1} \in \mathbb{Z}$.

   Alternate proof: We can also prove this using modular arithmetic without induction. Namely, we want to show that $2^{n+2}+3^{2n+1} \equiv 0 \pmod 7$

$$\begin{aligned}
2^{n+2}+3^{2n+1} &\equiv 2^2\cdot 2^n+(-4)^{2n+1} \quad (\text{since } 3 \equiv -4 \pmod 7) \\
&= 4\cdot 2^n+(-1)^{2n+1}(4)^{2n+1} \\
&= 4\cdot 2^n-(4)^{2n+1} \\
&= 4\cdot (2^n-(4)^{2n}) \\
&= 4\cdot (2^n-(2^2)^{2n}) \\
&= 4\cdot (2^n-2^{4n}) \\
&= 4\cdot (2^n-2^n2^{3n}) \\
&= 4\cdot 2^n\cdot (1-2^{3n}) \\
&= 4\cdot 2^n\cdot (1-(2^3)^n) \\
&\equiv 4\cdot 2^n\cdot (1-1^n) \quad (\text{since } 2^3 = 8 \equiv 1 \pmod 7) \\
&= 0
\end{aligned}$$

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? If you answered *No*, name a rogue couple.
Answer: No, this is not stable. The couple $(A,2)$ is a rogue couple since they would both rather be paired with each other than their current pairing.

(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:

Answer: $(A,2)(B,1),(C,3)$ is one stable pairing and $(A,2)(B,3),(C,1)$ is another. You just need to list one of them.

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.
Answer: False. Consider the following:

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

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

In this case, everyone's least favorite candidate is 3 and everyone's least favorite job is C. Thus it's not surprising that pairing them together in the following pairing is in fact stable: $(A,1)$, $(B,2)$, and $(C,3)$.

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.
Answer: False. Consider the following preferences:

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

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

There is only one stable pairing for this, namely $(A,1)$, $(B,2)$, and $(C,3)$, yet 3 is not C's top choice.

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

Answer: Exactly one. The first run is a job-optimal pairing and the second run is a job-pessimal pairing. Since these pairings are one and the same, this must mean there is only one pairing possible (we showed this in HW 2).

5. Graphs w/ Friends

All graphs are simple and undirected unless otherwise specified.

1. (3pts) The complete graph K_4 has an Eulerian tour.

   Answer: False. Each vertex in K_4 has degree 3 and so is not an even degree graph, a necessary (and sufficient) condition for there being an Eulerian tour.

2. (3pts) K_6 is planar.

   Answer: False. K_6 contains K_5 which is not planar.

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?

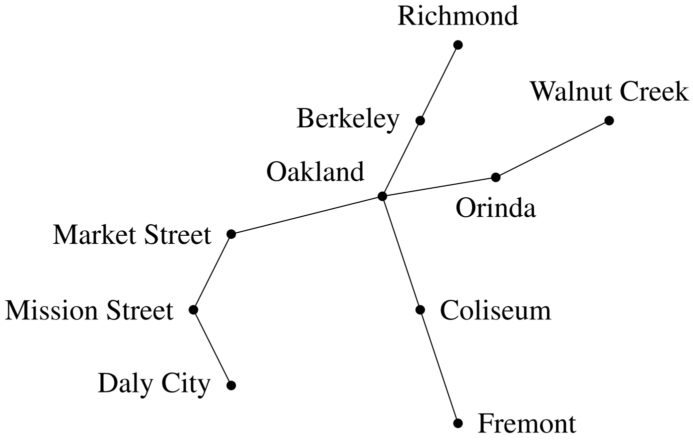
   Answer: 7. This is an application of the degree-sum formula. Knowing how many friends each child has is knowing the degree of a vertex where each child is a vertex and an edge between children is a friendship. Adding up all the degrees and dividing by two (to account for double-counting edges) is a how gives an application of the degree-sum formula: $(4+3+3+2+1+1)/2 = 14/2 = 7$.

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?

   Answer: 3. The number of bits that differ between the two strings is 3 and thus there will be the path that flips those bits one at a time to get from one vertex to the other by definition of the 5-cube.

6. Euler's BART Speedrun

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



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

   Answer: Yes. Oakland is the root of the tree.

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

   Answer: Yes. All trees are bipartite.

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

   Answer: 4. 4 is the maximum degree of this graph (Oakland).

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?

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

   Answer: No. Add any of the following edges:

   - (Walnut Creek, Fremont)
   - (Walnut Creek, Richmond)
   - (Walnut Creek, Daly City)
   - (Fremont, Daly City)
   - (Fremont, Richmond)
   - (Daly City, Richmond)

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?

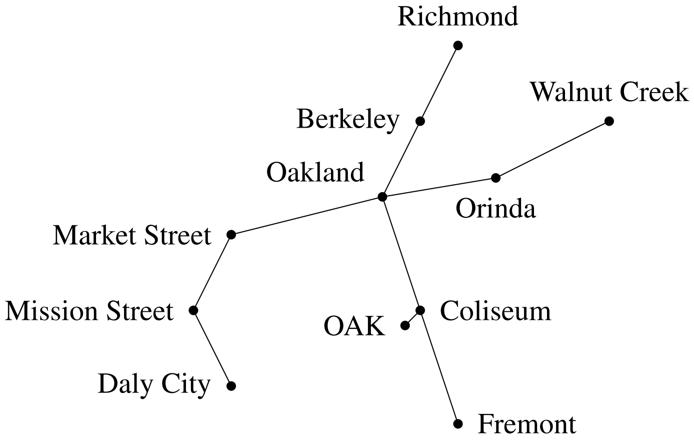
   If there are multiple possible pairs, choose one pair of edges that creates Eulerian tour.

   Answer: Add one of the following pairs of edges:

   - (Walnut Creek, Fremont), (Daly City, Richmond)
   - (Walnut Creek, Richmond), (Fremont, Daly City)
   - (Walnut Creek, Daly City), (Fremont, Richmond)

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.

Answer: Every Eulerian walk must start or end at OAK.

There is only one edge incident to OAK and so once you enter OAK you can never leave (without reusing that edge), thus it can not be in the middle of an Eulerian walk.

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.

Answer: We proceed by inducting over the number of edges.

Base Case: Say $|E|=0$. Then there are no edges and so $\forall v \in V\ deg(v)=0$. Adding all the zeroes will equal zero which is the same as 2 times zero, the number of edges.

Inductive Hypothesis: Say there is a $k\in\mathbb{N}$ such that for all graphs $G=(V,E)$ such that $|E|=k$ it is the case that $\sum_{v\in V} deg(v)=2|E|$.

Inductive Step: Consider an arbitrary graph $G=(V,E)$ such that $|E|=k+1$. Take an arbitrary edge $\{v_1,v_2\}$ from G and remove it. The remaining graph has k edges and so we have $\sum_{v\in V} deg(v)=2k$ for the remaining graph by the Inductive Hypothesis.

Now, we can add the edge back in and we get our original G back while only affecting the degree of v_1 and v_2 (by definition of the degree of a vertex). Namely, $deg(v_1)$ and $deg(v_2)$ increase by exactly one each, by definition. This means the LHS of our degree sum increases by 2 when adding the edge and so the equality we were guaranteed by the Inductive Hypothesis alters to become $\sum_{v\in V} deg(v)=2k+2$ (this is precisely and rigorously *where* double-counting an edge occurs). Lastly, $2k+2=2(k+1)=2|E|$ and so the RHS matches our degree-sum formula and we are done.

Alternate Solution: Induction on vertices also works. The main difference is that we will have to use strong induction; i.e., our strong inductive hypothesis will be that for $0\le n\le k$, the degree sum formula holds for every n vertex graph.

Then, in the inductive proof, we consider an arbitrary $k+1$ vertex graph and remove a vertex with m edges, creating a k vertex graph where $\sum_{v\in V} deg(v)=2k$. Now, when we add the vertex back, the number of edges in the graph increases by m, so the RHS increases by $2m$. Each edge contributes 2 degrees to the total degree sum (1 for each vertex it connects to), so the total degree sum (LHS) also increases by $2m$. Therefore, the degree sum formula still holds for the $k+1$ vertex graph.

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 $n\in\mathbb{N}$.

   Answer: True. $6\equiv 1 \pmod 5$ so $6^n-1\equiv 1^n-1=1-1=0 \pmod 5$.

2. (3pts) If $xy\equiv 0 \pmod 6$, then either $x\equiv 0 \pmod 6$ or $y\equiv 0 \pmod 6$.

   Answer: False. $x=2$ and $y=3$ satisfy the antecedent but not the consequent.

3. (3pts) 9 divides $4^m + 5^m$ for all **odd** $m \in \mathbb{N}$.

   Answer: True. $5 \equiv -4 \pmod{9}$, thus $4^m + 5^m \equiv 4^m + (-4)^m = 4^m + (-1)^m 4^m = 4^m - 4^m = 0 \pmod{9}$ since $(-1)^m = -1$ if m is odd.

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).

   Answer: 2. p can't be congruent to $0 \pmod{3}$ lest it is 3 (but $p > 3$) or it is divisible by 3 (but p is prime). It also can't be congruent to 1 lest $q = p + 2 = 1 + 2 \equiv 0 \pmod{3}$. Thus is must congruent to $2 \pmod{3}$ (for example, $p = 5$ and $q = 7$).

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

   Answer: 1. The one's place of a number is revealed by looking at it $\pmod{10}$. Since $9 \equiv -1 \pmod{10}$, we have that $9^{68} \equiv (-1)^{68} = 1 \pmod{10}$.

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?

   Answer: 5. The decryption exponent needs to be $d \equiv e^{-1} \pmod{(p-1)(q-1)}$. For the given values, this means we need to find $5^{-1} \pmod{24}$. 5 is its own inverse $\pmod{24}$. This may not make it the most secure public key/private key pair but this is how to compute d from e for these values.

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).

   Answer: Yes, this is an example of RSA actually being what's called a homomorphic encryption scheme for multiplication (i.e. multiplying the encryptions of values correspondingly multiplies the values themselves when decrypted). We decrypt the value ab per usual and see that $(ab)^d = a^d b^d = (x^e)^d (y^e)^d = x^{ed} y^{ed} \equiv xy \pmod{N}$ by construction of RSA.

9. Chinese Remainder Theorem (8pts)

Consider the following congruences:

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

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:

$$cx \equiv ca \pmod{cp}$$
$$dx \equiv db \pmod{dq}$$

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

Answer: Note that these two systems are actually equivalent to each other. Looking at the first equation, we can say that $cx \equiv ca \pmod{cp}$ can be written in its algebraic form $cx = ca + kcp$ for some integer k. Then, we can divide both sides by c (which is an invertible operation) to get the equation $x = a + kp$ which is equivalent to $x \equiv a \pmod{p}$. We can do the exact same for the second equation.

Thus, there is still going to be a unique solution mod pq, let us denote it as x'. If we now want to consider mod $cdpq$, we notice that any solution of the form $x' + kpq$ will be equivalent to x in mod pq, and thus is still a solution. k can range from any value in the set $\{0, 1, \ldots, cd-1\}$, for which there are **cd** possible values.

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 $h(x) = f(x) + g(x)$?
   Answer: k. The highest degree term of f has no like terms to combine with from g since it has less degree and so its non-zero coefficient will remain and remain the highest degree term of $h(x)$.

   (b) (3pts) What is the degree of $r(x) = f(x)g(x)$?
   Answer: $k+j$. After applying distributivity to multiply all the terms of $f(x)$ with the terms of $g(x)$, the highest degree term will be the multiplication of the highest degree term of $f(x)$ (i.e. k) and the highest degree term of $g(x)$ (i.e. j). Multiplying two terms adds their exponents and we get the result.

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 $\forall x \in \mathbb{Z}$, $f(x) \equiv g(x) \pmod 5$.

   Answer: Using Fermat's Little Theorem we know that $x^5 \equiv x \pmod 5$. Thus we can take $f(x)$ and simplify the exponents to $g(x) = 4x^4 + x^3 + 2x + 3$ and $f(x) \equiv g(x) \pmod 5$.

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

   Answer: $3(x-3)(x-4) \pmod 7$. This is Lagrange interpolation.

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.

   Answer: 125. A degree 4 polynomial is determined by 5 points, 2 of which are already specified. Thus, for any 3 unused input values, the corresponding outputs could be anything in GF(5) with each possible triple of outputs yielding a distinct polynomial when combined with the initial 2 points. Since each output value can take on 5 values in GF(5), there are $5^3 = 125$ possibilities.

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 ≥ 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 ≥ 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.)

   2

   (a) **Answer:** 23

   (b) **Answer:** 12

   (c) **Answer:** 4

   (d) **Answer:** 1

   (e) **Answer:** The number of points given out to Professors, TAs, and Head TAs is $2*12+4*4+7*1=47$. We reserve one extra point for the secret. p must also be $> s$, or else the secret would be reduced to some smaller number $s-kp$. Thus, we have $p \geq \max(s+1, 48)$

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?
   Answer: 14. We need $n = 10$ points of a degree 9 polynomial to interpolate it but we have $k = 2$ general errors (i.e. corrupted points). To handle k general errors, we use Berlekamp-Welch decoding and thus need $n+2k$ points. Namely, having $k = 2$ errors means we need $2k = 4$ more correct points to decode.

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?

Answer: $\binom{30}{12}$. There are 30 indices the 12 errors could occur and so we are *choosing* 12 indices from the possible 30.

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

   Answer: $(p-1)p^d$. There are $p-1$ possible values for the leading coefficient (can't choose 0 since that would mean the degree is less than d) and p possible values for the d others coefficients. Use the first rule of counting.

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?

   Answer: $\frac{10!}{4!}$. This is ordered sampling without replacement (because of the broken number pad). You have 10 choices for the first digit but then can't use that number again, so 9 choices for the second, and so on. Thus $10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5$.

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?

   Answer: $\binom{14}{4}$. There are $n = 5$ dishes and $k = 10$ meals you want. You're getting all the meals at once to have and use however you want over the coming days, so the order doesn't matter, and you can buy each meal as many or as little times as you want (i.e. with replacement). Thus this is a stars and bars questions where you have $n-1 = 4$ separators to put within $n+k-1 = 14$ spaces.

13. Doodle Page.

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