
CS 70 Discrete Mathematics and Probability Theory
Fall 2026 Hug, Sabin Midterm Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OPHI*

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

Direct Proofs

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

Prove each of the following claims with a direct proof.

- (a) For every natural number n , if n is odd then $3n + 4$ is odd.
- (b) For any $a, b, c \in \mathbb{Z}$, if $a \mid b$ and $b \mid c$, then $a \mid c$.
- (c) For all $n \in \mathbb{N}$, if n is divisible by 3, then $(n + 1)^2 + 2$ is divisible by 3.

Solution:

- (a) Let n be a natural number. First, we assume n is odd. By the definition of odd, $n = 2k + 1$ for some integer k . As such,

$$\begin{aligned} 3n + 4 &= 3(2k + 1) + 4 \\ &= 6k + 3 + 4 \\ &= 6k + 7 \\ &= (6k + 6) + 1 \\ &= 2(3k + 3) + 1 \end{aligned}$$

Since k is an integer, $3k + 3$ is also an integer. And by the definition of odd, $3n + 4$ is odd.

- (b) Let a, b, c be any integers. First, we assume that $a \mid b$ and $b \mid c$. By the definition of divides, there exist integers k_1, k_2 such that $b = k_1a$ and $c = k_2b$. Then,

$$\begin{aligned} c &= k_2b \\ &= k_2(k_1a) \\ &= (k_2k_1)a \end{aligned}$$

Both k_1 and k_2 are integers, so k_2k_1 is also an integer. And by the definition of divides, $a \mid c$.

- (c) Let n be a natural number. First, we assume n is divisible by 3. By the definition of divides, $n = 3k$ for some integer k . As such,

$$\begin{aligned} (n + 1)^2 + 2 &= (3k + 1)^2 + 2 \\ &= (9k^2 + 6k + 1) + 2 \\ &= 9k^2 + 6k + 3 \\ &= 3(3k^2 + 2k + 1) \end{aligned}$$

Since k is an integer, $3k^2 + 2k + 1$ is also an integer. And by the definition of divides, $(n + 1)^2 + 2$ is divisible by 3.

Propositional Logic

Pass Threshold: There are 6 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

(a) Define:

$S(x)$: student x studies regularly for the CS 70 final exam

$P(x)$: student x passes the exam

Translate the following statement into predicate logic: Not every student who studies regularly for the CS 70 final exam passes it.

(b) Suppose that P is true, Q is false, and R is true. Determine whether the following proposition is true or false.

$$R \implies (Q \vee (P \wedge \neg Q))$$

Determine whether the following proposition is Always True, Always False, or could be Either:

(c)

$$(\neg P \vee \neg Q) \wedge (\neg Q \implies P)$$

(d) Let $P(x)$ and $Q(x)$ be predicates over a universe with at least two elements.

$$(\forall x (P(x) \implies Q(x))) \vee (\forall x (Q(x) \implies P(x))).$$

Determine whether the following propositions are logically equivalent:

(e)

$$\neg(P \wedge Q) \vee R \quad \text{and} \quad (R \wedge \neg Q) \vee P$$

(f)

$$\exists x (P(x) \wedge \neg Q(x)) \quad \text{and} \quad \neg \forall x (P(x) \implies Q(x))$$

Solution:

(a) **Solution:** The quote “Not every student who studies passes” means that there exists some student who studies and does not pass:

$$\exists x (S(x) \wedge \neg P(x))$$

Equivalently,

$$\neg \forall x (S(x) \implies P(x))$$

Using quantifier negation and implication equivalence,

$$\neg \forall x (S(x) \implies P(x)) \equiv \exists x (S(x) \wedge \neg P(x))$$

Thus,

$$\exists x (S(x) \wedge \neg P(x))$$

(b) **Solution:** True.

$P \wedge \neg Q$ is true, since both P and $\neg Q$ are true. This makes the disjunction $(Q \vee (P \wedge \neg Q))$ true as well. The implication has a true hypothesis (R) and a true conclusion $(Q \vee (P \wedge \neg Q))$ so it is true.

(c) **Solution:** Could be either. Refer to the truth table:

P	Q	$\neg P \vee \neg Q$	$\neg Q \implies P$	$(\neg P \vee \neg Q) \wedge (\neg Q \implies P)$
T	T	F	T	F
T	F	T	T	T
F	T	T	T	T
F	F	T	F	F

The final column contains both T and F, so the proposition could be either true or false depending on the truth values of P and Q .

(d) **Solution:**

Either. For a true model, take $P(x)$ and $Q(x)$ to have the same truth value for every x ; then both universal implications are true. For a false model, let the universe be $\{a, b\}$ with $P(a)$ and $Q(b)$ true, and $P(b)$ and $Q(a)$ false. The first implication fails at a , while the second fails at b .

(e) **Solution:** Not Logically Equivalent.

Counterexample: if P, Q are true and R is false, the LHS is false since $\neg(P \wedge Q)$ and R are both false. The RHS is true since P is true.

(f) **Solution:** Logically Equivalent.

$$\begin{aligned}
 \exists x(P(x) \wedge \neg Q(x)) &\equiv \exists x(\neg(P(x) \vee Q(x))) \\
 &\equiv \exists x(\neg(P(x) \implies Q(x))) \\
 &\equiv \neg \forall x(P(x) \implies Q(x))
 \end{aligned}$$

Proof Techniques

Pass Threshold: There are 2 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

(a) Prove that there is a unique real number x that satisfies

$$x + a = a + x = a$$

for all $a \in \mathbb{R}$.

(b) Prove the following statement: for any integers a and b , a is even and b is odd if and only if $ab + 7b - 2a - 14$ is odd.

Solution:

(a) **Solution:** Let $x = 0$. Then

$$a + 0 = 0 + a = a$$

for all $a \in \mathbb{R}$. To show that $x = 0$ is unique, we proceed by contradiction.

Suppose there exist two solutions $x = e_1$ and $x = e_2$ with $e_1 \neq e_2$. Then

$$e_1 = e_1 + e_2 = e_2.$$

Contradiction! Therefore, $x = 0$ is a unique solution.

(b) **Solution:** Since this is an iff statement, we need to prove both directions.

- Forward ($\Rightarrow$): Assume a is even and b is odd. Then, we can write $a = 2k$ for some integer k and $b = 2m + 1$ for some integer m . Substituting these into the expression, we have:

$$\begin{aligned}ab + 7b - 2a - 14 &= (2k)(2m + 1) + 7(2m + 1) - 2(2k) - 14 \\&= 4km + 2k + 14m + 7 - 4k - 14 \\&= 4km + 14m + 2k - 4k + 7 - 14 \\&= 4km + 14m - 2k - 7 \\&= 2(2km + 7m - k - 3) + 1\end{aligned}$$

Since $2km + 7m - k - 3$ is an integer, $ab + 7b - 2a - 14$ is odd.

- Backward ($\Leftarrow$): Assume $ab + 7b - 2a - 14$ is odd. Then, we can factorize the expression as follows:

$$\begin{aligned}ab + 7b - 2a - 14 &= b(a + 7) - 2(a + 7) \\&= (a + 7)(b - 2)\end{aligned}$$

Since the product of $a + 7$ and $b - 2$, two integers, is odd, each must be odd as well. Thus, $a + 7 = (a + 6) + 1$ is odd, which means $a + 6$, and therefore a is even. Similarly, $b - 2 = (b - 3) + 1$ is odd, which means $b - 3$ is even, and therefore b is odd. So, a is even and b is odd, and we have proved both directions of the statement.

Induction

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

- (a) Alice and Zoe play a game with two piles of raisins, taking turns. On her turn, a player must perform two actions:

1. Choose one pile and completely eat all its raisins.
2. From the remaining pile, pick *any positive number* of raisins to gather into a *new* second pile, preparing the next turn. But if the remaining pile has only 1 raisin, then the player cannot split the pile and instead **loses the game**.

Alice gets the first turn. Prove that if there is a pile containing an even number of raisins on Alice's turn, then Alice can guarantee she wins. (*Hint.* Use induction the size of the even pile **on Alice's turns**. Trusting the claim, Alice wants to always receive an even pile on **her** next turn, but how can she force this from Zoe?)

Solution:

- (a) **Solution:** If there is a pile of exactly 2 raisins, then Alice eats the *other* pile and splits the pile of 2 into two piles both of size 1. Zoe then loses the game on her turn. Suppose instead the pile of even size has $k > 2$ raisins, and suppose for induction that Alice wins whenever **on her turn** there is a pile of even size less than k .

Alice again eats the *other* pile. Then, she splits the pile of size k into two piles of sizes 1 and $k - 1$. Zoe must eat the pile of size 1, or else she immediately loses thereafter. We know k is even, so $k - 1$ is odd. Then no matter how Zoe splits this pile, one of the two resulting piles must have an even number of raisins. Furthermore, both piles have size less than k , and it is Alice's turn. Thus by the inductive hypothesis, Alice can always win from here.

Thus Alice can always guarantee victory.

Note that Alice did not have to split the even pile into 1 and $k - 1$; alternatively, she could choose *any* odd-odd partition. Then no matter which pile Zoe eats, the remaining pile has an odd number of raisins. Zoe immediately loses if this pile has only 1 raisin; otherwise, she splits this odd pile in two, still necessarily leaving another (smaller) even pile for Alice.

This problem is adapted from *A Decade of the Berkeley Math Circle*, p. 159.

Modular Arithmetic

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

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

- (a) Compute $67^{6767} \pmod{68}$.
- (b) Compute $98 \cdot 99 \cdot 100 \pmod{101}$.
- (c) Let $x \equiv 5 \pmod{12}$. Find k such that $2x + 6 \equiv k \pmod{6}$.
- (d) Prove that if $a \equiv b \pmod{m}$, then $a + c \equiv b + c \pmod{m}$ for any integer c .
- (e) For how many values of $a \in \{0, 1, \dots, 15\}$ does a^{-1} exist modulo 16?

Solution:

- (a) **Solution:** Since $67 \equiv -1 \pmod{68}$ and 6767 is odd,

$$67^{6767} \equiv (-1)^{6767} = -1 \equiv \boxed{67} \pmod{68}.$$

- (b) **Solution:**

$$98 \cdot 99 \cdot 100 \equiv (-3)(-2)(-1) = -6 \equiv \boxed{95} \pmod{101}.$$

(c) **Solution:** By definition of congruence, $x \equiv 5 \pmod{12}$ means $x = 5 + 12n$ for some integer n . Then

$$\begin{aligned}2x + 6 &= 2(5 + 12n) + 6 \\&= 10 + 24n + 6 \\&= 16 + 24n\end{aligned}$$

Since 6 divides 24, $24n \equiv 0 \pmod{6}$, so

$$2x + 6 \equiv 16 \equiv 4 \pmod{6}$$

Therefore $k = \boxed{4}$.

(d) **Solution:** Since $a \equiv b \pmod{m}$, by definition $a = b + km$ for some integer k . Adding c to both sides,

$$\begin{aligned}a + c &= (b + km) + c \\&= b + c + km\end{aligned}$$

This says $a + c$ and $b + c$ differ by a multiple of m , so $a + c \equiv b + c \pmod{m}$.

(e) **Solution:** The inverse exists exactly when $\gcd(a, 16) = 1$. This occurs when $a = 1, a = 3, a = 5, a = 7, a = 9, a = 11, a = 13$, or $a = 15$. This gives $\boxed{8}$ total values.

CRT

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

(a) Find the smallest natural number x that satisfies all three of the following congruences:

$$\begin{aligned}x &\equiv 2 \pmod{5} \\x &\equiv 1 \pmod{6} \\x &\equiv 4 \pmod{7}\end{aligned}$$

Solution:

(a) **Solution:** We can use the Chinese Remainder Theorem to find such an x .

$$x \equiv 2 \pmod{5}$$

$$x \equiv 1 \pmod{6}$$

$$x \equiv 4 \pmod{7}$$

• We have the moduli $n_1 = 5, n_2 = 6, n_3 = 7$, so $N = n_1 n_2 n_3 = 5 \cdot 6 \cdot 7 = 210$.

• We have $a_1 = 2, a_2 = 1, a_3 = 4$.

By the Chinese Remainder Theorem,

$$x \equiv a_1 u_1 + a_2 u_2 + a_3 u_3 \pmod{N},$$

where

$$u_i = \frac{N}{n_i} \left(\frac{N}{n_i} \right)^{-1}_{n_i}.$$

To find the u_i 's:

$$\begin{aligned} u_1 &= \frac{N}{n_1} \left(\left(\frac{N}{n_1} \right)^{-1} \pmod{n_1} \right) \\ &= \frac{210}{5} \left(\left(\frac{210}{5} \right)^{-1} \pmod{5} \right) \\ &= 42(42^{-1} \pmod{5}) \\ &= 42(2^{-1} \pmod{5}) \\ &= 42 \cdot 3 \\ &= 126 \end{aligned}$$

$$\begin{aligned} u_2 &= \frac{N}{n_2} \left(\left(\frac{N}{n_2} \right)^{-1} \pmod{n_2} \right) \\ &= \frac{210}{6} \left(\left(\frac{210}{6} \right)^{-1} \pmod{6} \right) \\ &= 35(35^{-1} \pmod{6}) \\ &= 35(5^{-1} \pmod{6}) \\ &= 35 \cdot 5 \\ &= 175 \end{aligned}$$

$$\begin{aligned} u_3 &= \frac{N}{n_3} \left(\left(\frac{N}{n_3} \right)^{-1} \pmod{n_3} \right) \\ &= \frac{210}{7} \left(\left(\frac{210}{7} \right)^{-1} \pmod{7} \right) \\ &= 30(30^{-1} \pmod{7}) \\ &= 30(2^{-1} \pmod{7}) \\ &= 30 \cdot 4 \\ &= 120 \end{aligned}$$

Putting it all together to find x :

$$\begin{aligned}x &= a_1u_1 + a_2u_2 + a_3u_3 \\&= 2 \cdot 126 + 1 \cdot 175 + 4 \cdot 120 \\&= 907 \\&\equiv \boxed{67} \pmod{210}\end{aligned}$$

RSA

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 2 questions correct.

Each subpart should be able to be done independently of the other subparts.

- (a) Alice and Bob set up an RSA scheme where Alice chooses $p = 17$, $q = 5$, and $e = 23$. What is Alice's public key, and what encryption function $E(x)$ does Bob use to send her a message x ? Box your answers to both questions; both must be correct to receive credit.
- (b) Alice and Bob set up an RSA scheme where $p = 17$, $q = 5$, and $e = 23$. Find the smallest positive value of d that can serve as the private key.
- (c) Alice sets up RSA with $p = 7$, $q = 13$, $e = 5$, and $d = 29$. Worried that her scheme is insecure, she changes e to 77 and keeps everything else the same. Is the scheme still correct? Briefly explain in 3 sentences or less.

Solution:

- (a) **Solution:** We have $N = pq = 17 \cdot 5 = 85$. So, the public key is $(N, e) = (85, 23)$. Bob encrypts using the public key (N, e) , so

$$E(x) \equiv \boxed{x^{23} \pmod{85}}.$$

(b) **Solution:** The private key is

$$d \equiv e^{-1} \pmod{(p-1)(q-1)} \equiv 23^{-1} \pmod{64}.$$

Running the extended Euclidean algorithm on 64 and 23:

$$\begin{aligned} (1) \cdot 64 + (0) \cdot 23 &= 64, \\ (0) \cdot 64 + (1) \cdot 23 &= 23, \\ (1) \cdot 64 + (-2) \cdot 23 &= 18, \\ (-1) \cdot 64 + (3) \cdot 23 &= 5, \\ (4) \cdot 64 + (-11) \cdot 23 &= 3, \\ (-5) \cdot 64 + (14) \cdot 23 &= 2, \\ (9) \cdot 64 + (-25) \cdot 23 &= 1. \end{aligned}$$

Taking the last equation modulo 64 gives

$$(-25) \cdot 23 \equiv 1 \pmod{64}.$$

Since $-25 \equiv 39 \pmod{64}$,

$$39 \cdot 23 \equiv 1 \pmod{64}.$$

Thus,

$$d \equiv 39 \pmod{64}.$$

(c) **Solution:** Yes. Since $(p-1)(q-1) = 6 \cdot 12 = 72$, the new exponent is $e' = 77 = e + (p-1)(q-1)$. Therefore

$$e'd = ed + (p-1)(q-1)d \equiv ed \equiv 1 \pmod{(p-1)(q-1)}.$$

Since $e'd \equiv 1 \pmod{(p-1)(q-1)}$, d is the inverse of e' , so decryption still recovers the message: $x^{e'd} \equiv x \pmod{91}$.

Polynomials

Pass Threshold: There are 3 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

(a) Use Lagrange interpolation to find the unique polynomial $p(x)$ of degree at most 2 over $\text{GF}(11)$ that passes through all of the following points:

$$(1, 7) \quad (3, 5) \quad (4, 0)$$

Make sure $p(x)$ is of the form $a_2x^2 + a_1x + a_0$, where $a_2, a_1, a_0 \in \{0, 1, \dots, 10\}$. To help you get started, we've provided $\Delta_2(x)$, which corresponds to the second point given.

$$\Delta_2(x) = 5x^2 + 8x + 9$$

(b) Let $f(x)$ and $g(x)$ be polynomials over $\text{GF}(11)$ of degrees exactly 4 and 3, respectively. What is the greatest possible number of distinct roots of $f(x)g(x)$?

- (c) Find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = 70x^{72} + 2x^{26} + 7$ over $\text{GF}(13)$.

Solution:

- (a) **Solution:** Each $\Delta_i(x)$ will be 1 when x is the x -value of the i th point, and 0 at the two other relevant points. Thus, $p(x)$ can be created by a linear combination of $\Delta_i(x)$'s multiplied by the desired y value at each point. This gives us $p(x) = 7\Delta_1(x) + 5\Delta_2(x) + 0\Delta_3(x)$. (Notice that we do not need to actually compute $\Delta_3(x)$, since it'll be multiplied by 0 anyway.)

$\Delta_2(x)$ was given in the problem, but just for completeness, here's how we obtain $\Delta_2(x)$: we want $\Delta_2(x)$ to be 0 when $x = 1$ or $x = 3$, and $\Delta_2(x)$ to be 1 when $x = 2$.

$$\begin{aligned}\Delta_2(x) &\equiv (x-1)(x-4)((3-1)(3-4))^{-1} \pmod{11} \\ &\equiv (9)^{-1}(x-1)(x-4) \pmod{11} \\ &\equiv 5(x-1)(x-4) \pmod{11} \\ &\equiv 5(x^2 - 5x + 4) \pmod{11} \\ &\equiv 5x^2 - 25x + 20 \pmod{11} \\ &\equiv 5x^2 + 8x + 9 \pmod{11}\end{aligned}$$

Similarly, we want $\Delta_1(x)$ to be 0 when $x = 2$ or $x = 3$, and $\Delta_1(x)$ to be 1 when $x = 1$.

$$\begin{aligned}\Delta_1(x) &\equiv (x-2)(x-3)((1-2)(1-3))^{-1} \\ &\equiv 6^{-1}(x-2)(x-3) \pmod{11} \\ &\equiv 2(x-2)(x-3) \pmod{11} \\ &\equiv 2(x^2 - 5x + 6) \pmod{11} \\ &\equiv 2x^2 - 10x + 12 \pmod{11} \\ &\equiv 2x^2 + 8x + 2 \pmod{11}\end{aligned}$$

Putting everything together,

$$\begin{aligned}p(x) &= 7\Delta_1(x) + 5\Delta_2(x) + 0\Delta_3(x) \\ &= 7(2x^2 + 8x + 2) + 5(5x^2 + 8x + 9) \\ &\equiv 14x^2 + 56x + 14 + 25x^2 + 40x + 45 \pmod{11} \\ &\equiv 39x^2 + 96x + 59 \pmod{11} \\ &\equiv \boxed{6x^2 + 8x + 4} \pmod{11}\end{aligned}$$

- (b) **Solution:** The product $f(x)g(x)$ has degree $4 + 3 = 7$. By Property 1, it has at most $\boxed{7}$ distinct roots.

- (c) **Solution:** We can apply Fermat's Little Theorem, which states that for any prime p , $a^p \equiv a \pmod{p}$ for all a . (This takes the form of FLT in the notes and multiplies both sides by a , making the equivalence hold even for $a \equiv 0$.)

We want to find a polynomial $g(x)$ with degree strictly less than 13 such that $f(a) \equiv g(a) \pmod{13}$ for any integer a .

Since $x^{13} \equiv x \pmod{13}$, we can repeatedly substitute x^{13} with x , effectively reducing the exponent by 12. We can only do this as long as the exponent remains greater than or equal to 13, so we end up with

$$g(x) = 70x^{12} + 2x^2 + 7 \equiv 5x^{12} + 2x^2 + 7 \pmod{13}$$

Secret Sharing & ECCs

Pass Threshold: There are 4 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

- (a) Sidharth wants to send you a message with an unknown number of points. To guard against 1 general error, Sidharth sends you 5 points. How many points were in the original message that Sidharth wanted to send?
- (b) Professor Sabin is sending Ricardo an n -packet email. The email service that Professor Sabin uses takes k packets and replaces them with random values.

True or False: Ricardo will be able to recover the message using the Berlekamp–Welch algorithm if Professor Sabin sends $n + k$ packets.

- (c) Large Technology @ Berkeley recently acquired a huge sponsorship from Computing Co! To protect the sum of money, they secure it with a polynomial secret sharing scheme involving 2 co-presidents and 10 officers. To access the funds, they require either 2 co-presidents to contribute their secrets, or 1 co-president and 7 officers. If no co-presidents are involved, it should be impossible to access the funds.

Design a secret sharing scheme for this, using polynomials of lowest degree possible.

To get full credit for this question, you must get all subparts correct.

- (i) How many polynomials do you need for this system to work?
- (ii) What are the degrees of your polynomials? *You do not need to fill in every box.*
- (iii) How many points does each co-president get?
- (iv) How many points does each officer get?
- (d) The answer to this question, s , is locked in a degree-1 polynomial $P(x)$ over $\text{GF}(p)$ with $p = 5$, where $P(0) = s$. However, in a series of (un)fortunate events, 3 of the points on $P(x)$ have been leaked on this midterm.

$$P(1) = \text{The page number of the front page} \pmod{p}$$

$$P(2) = \text{The page number of the Induction question} \pmod{p}$$

$$P(3) = \text{The page number of the Modular Arithmetic question} \pmod{p}$$

Solution:

- (a) **Solution:** Sidharth sends you $n + 2k = 5$ points, guarding against $k = 1$ general error. Thus, his original message consists of $n = \boxed{3}$ points.
- (b) **Solution:** False. Professor Sabin's email client is corrupting these points so we would need to send $n + 2k$ points.
- (c) **Solution:**
 A top-level polynomial $P(x)$ with $P(0)$ as the secret, and one polynomial $Q(x)$ for the officers with $Q(0) = P(3)$. The co-presidents hold $P(1)$ and $P(2)$; two points recover $P(x)$, and the officers' point $P(3)$ plus one co-president's point also suffices. Without a co-president, the officers know only the single point $P(3)$. Any 7 of the 10 officers must be able to recover $Q(x)$.
- (i) $\boxed{2}$
- (ii) $\boxed{1 \text{ of degree } 1, 1 \text{ of degree } 6}$
- (iii) $\boxed{1}$
- (iv) $\boxed{1}$
- (d) **Solution:** The leaked points are $P(1) = 1$, $P(2) = 2$, and $P(3) = 3$ (pages 1, 7, and 8, reduced mod 5). $P(x) = x$ is a degree-1 polynomial over $\text{GF}(5)$ that goes through all 3 leaked points. Hence, $s = P(0) = \boxed{0}$.

Graphs

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 4 questions correct.

- (a) K_4 is planar.
- (b) K_5 has an Eulerian tour.
- (c) All dice can be viewed as planar graphs wrapped around a sphere. A 12-sided die thus has 12 faces to roll. If we know there are 20 pointy vertices to 12-sided dice, then how many edges are there on a 12-sided die?
- (d) 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 labelled 10010 to the vertex labelled by 01000?
- (e) Prove that if a graph has a vertex that has odd degree, there must be another vertex that has odd degree.

Solution:

- (a) True. Doesn't contain K_5 or $K_{3,3}$.
- (b) True. Each vertex has degree 4 and so K_5 is connected, even graph.
- (c) 30. $f = 12$, $v = 20$, and so $v + f = e + 2$ implies that $e = 30$.
- (d) 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.

- (e) Contradiction: Assume there is a graph $G = (V, E)$ that has a vertex v' of odd degree but every other vertex has even degree. By the Degree-sum Formula (AKA the Handshake Lemma), $\sum_{v \in V} \deg(v) = 2|E|$, thus the sum of all the vertices' degrees will be a multiple of 2 and thus even. Since adding any amount of even numbers together will still be an even number and $\deg(v)$ is even for every $v \neq v'$, we have that $\sum_{v \neq v'} \deg(v)$ is even. Thus, $\sum_{v \in V} \deg(v) = \deg(v') + \sum_{v \neq v'} \deg(v) = \text{odd} + \text{even} = \text{odd}$. But this contradicts that the handshake lemma tells us that this sum should result in an even number.

Alternate (constructive) proof: We can use the FindTour algorithm from the notes to find another vertex of odd degree: Start at the odd degree vertex and walk to new vertices by crossing any available edge arbitrarily while removing each edge that is crossed until you get stuck. This algorithm must halt since we remove an edge on each iteration and there are only a finite amount of edges. We will argue that you must get stuck at a different vertex that has odd degree: We can never get stuck at a vertex that had even degree since entering and leaving such a vertex always deletes edges in pairs (the one you entered on and the one you left on) which always allows you to leave each time you enter due to there being an even number of edges on it. Further we never get stuck at the starting node because it starts with an odd degree and you start by leaving from there and deleting the edge that was taken, thus leaving an even number of edges attached to it left. Thus we never get stuck there by the same argument made for the vertices that started with an even degree.

Thus we never get stuck at the original odd degree vertex nor at an even degree vertex, yet we must get stuck somewhere since the algorithm must halt and so where it halts must be a new vertex that also has odd degree.

Graph Induction

Pass Threshold: There is 1 question for this topic. To pass the topic on this midterm, you must get at least 1 question correct.

- (a) 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. Use induction to prove that the degree-sum formula holds for all undirected graphs.

Solution:

- (a) 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. Our inductive hypothesis will be that for some k , the degree sum formula holds for every k 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.

Stable Matching

Pass Threshold: There are 5 questions for this topic. To pass the topic on this midterm, you must get at least 3 questions correct.

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

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

- (a) Consider the following pairing: $(A, 1)$, $(B, 2)$, and $(C, 3)$. Is this matching stable?
If you answered *No*, name a rogue couple.
- (b) 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).

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

- (c) 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.
- (d) 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.

- (e) 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?

Solution:

- (a) 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) $(A, 2), (B, 1), (C, 3)$ is one stable pairing and $(A, 2), (B, 3), (C, 1)$ is another. You just need to list one of them.
- (c) False. Consider the following:

Jobs	Preferences	Candidates	Preferences
A	$1 > 2 > 3$	1	$A > B > C$
B	$1 > 2 > 3$	2	$A > B > C$
C	$1 > 2 > 3$	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 $(C, 3)$.

- (d) False. Consider the following preferences:

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

- (e) 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).

Synthesis Question: CRT, revisited...

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.

Solution: 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 $\{0, 1, \dots, cd - 1\}$, for which there are cd possible values.

Synthesis Question: Rogue Delegates

The planning committee for The International Conference on Hackathon Organization has designed the following secret sharing scheme:

70 points of a 49-degree shared polynomial have each been assigned to the 70 delegations, one point per delegation.

Each delegation contains 10 delegates. They each receive a point of a degree 5 delegation-specific polynomial. Delegates can come together to recover their delegation's point on the shared polynomial using the delegation-specific polynomial.

A *rogue delegate* is an all-powerful delegate: they know all of the polynomials and have control over which delegation that they are placed in. The rogue delegates purposely manipulate their point on their delegation-specific polynomial to mess up the conference.

The planning committee will use the Berlekamp-Welch algorithm on the delegation-specific polynomials and on the shared polynomial to attempt to recover the correct secret. What is the smallest number of rogue delegates that can attend the conference and corrupt the committee's ability to recover the correct secret?

Justify your answer.

Solution: 33 delegates.

SID:

For a degree 49 polynomial, 50 points must be received correctly, and thus 10 errors out of a total of 70 points can be tolerated. Thus, the rogue delegates must create 11 corruptions on the shared polynomial in order to prevent the committee from recovering the correct secret.

For each delegation, 6 correct points are required, and thus $6 + 2 \cdot 2 = 10$ points need to be sent to counter 2 errors, so 2 errors out of 10 points is the most that can be tolerated. Thus, only 3 rogue delegates are necessary to corrupt that delegation's point on the shared polynomial.

Then, $3 \cdot 11 = 33$ rogue delegates are sufficient to prevent the committee from recovering the correct secret.

Doodle Page.

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

