CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Ayazifar and Rao

Midterm 1 Solutions

PRINT Your Name: Oski Bear

SIGN Your Name: *OSKI*

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

1. TRUE or FALSE?: 2pts each

For each of the questions below, answer TRUE or FALSE. No need to justify answer.

Please fill in the appropriate bubble!

Answer: Note that the answers provide explanations for your understanding, even though no such justification was required

1. $(\neg P \vee Q) \vee \neg(P \implies Q)$ is true for all P and Q.

   Solution: True. This is a tautology and is true because the implication $P \implies Q$ is true or not and $P \vee \neg P$ is always true.

2. $\exists n \in \mathbb{N}, \forall y \in \mathbb{Z}, n > y$.

   Solution: False. It says there is a natural number which is larger than every number in Z.

3. $\neg(\forall n \in \mathbb{N}, P(n)) \implies \exists n \in \mathbb{N}, \neg P(n)$.

   Solution: True. There must exist a counterexample.

4. $(\neg A \implies \neg B) \equiv (A \implies B)$.

   Solution: False. This is the converse not the contrapositive.

5. For $n > 2$, there is a stable marriage instance of n men and n women in which the traditional marriage algorithm takes **at least** n^2 days.

   Answer: False. If this were true, then there must have been at least $n^2 - 1 > n(n-1)$ rejections. Therefore, by Pigeonhole, somebody got rejected n times, which is impossible.

   We can get a tighter bound in the following way. Recall that there always exists a woman W who is not proposed to until the very last day. Furthermore, there can only be one man M who can propose to her on the last day, otherwise W will need to reject somebody and the algorithm continues. Thus, $n-1$ of the men don't propose to W, so they face at most $n-2$ rejections. M faces at most $n-1$ rejections. This gives us a (tight) bound of $(n-1)(n-2)+(n-1) = (n-1)^2$ rejections, which means the duration is at most $(n-1)^2+1$ days.

6. If a stable pairing P has a pair (m,w) where P is optimal for both m and w, then every stable pairing is optimal for both m and w.

   Answer: True. They would be a rogue couple in any supposed stable pairing where they are not paired, thus they would always be together in every stable pairing. Thus, every stable pairing would be optimal for both of them.

7. If at any point in the traditional marriage algorithm a woman's optimal partner proposes to her, then every stable pairing is optimal for her.

   Answer: True. It only gets better for women, so she must end up with her optimal partner. This suggests that in any other stable pairing, either this couple is rogue or this pairing is not optimal for both her and her partner, which it is. Thus, there are no pairings where they are not paired.

8. There is an n-edge, n-vertex connected graph where each pair of vertices is connected by 2 disjoint paths. (Paths are disjoint if they do not share an edge.)

   Solution: True. Consider the cycle on n vertices.

9. Consider a function $f : A \to B$, where $|A| = |B|$. An inverse function for f is a function $g : B \to A$ where $\forall x \in A, (g(f(x)) = x \wedge f(g(x)) = x)$. $f(\cdot)$ is a bijection if there is an inverse function.

   Solution: True. The existence of the inverse suggests it is one-to-one and the fact that $|A| = |B|$ suggests it is onto.

10. $f(x) = ax \pmod m$ is a bijection **if and only if** m is prime.
    Answer: False. It just needs $gcd(a,m) = 1$
11. Any graph that is a simple cycle can be vertex colored with 2 colors.
    Answer: False. Consider K_3.
12. For a hypercube of dimension 3, there is an edge between vertex 000 and 111.
    Answer: False. Edges are only between vertices that differ in one bit.

2. Short Answer. 3 pts each.

Write your answer in the simplest form possible. You should use only the variables in the question unless otherwise specified.

1. Write a logical formula that describes the proposition: *the square of any natural number is a natural number.*
   Answer: $\forall n \in N, \exists m \in N, n^2 = m$
2. What is the number of edges in an n-vertex acyclic graph having k connected components?
   Answer: $n-k$. Starting from n components, each edge addition either creates a cycle or reduces the number of components by 1. Thus, to get to k components, one can and has to add $n-k$ edges.
3. What is the number of edges in a planar graph where every face has five sides? (Answer in terms of v, the number of vertices.)
   Answer: $5(v-2)/3$. Eulers $v+f = e+2$. $5f = 2e$ by counting edge face adjacencies. This implies $v + 2e/5 = e+2$, which implies $e = 5(v-2)/3$. Notice this puts conditions on the values of v for which this can hold.
4. If there are $n/2$ leaves in an n-vertex tree, what is the average degree of the other $n/2$ vertices? (Assume n is even.)
   Answer: Total degree is $2(n-1)$. The degree of those vertices is $n/2$, so remaining total degree is $2n - n/2 - 2$, the average degree of the remaining $n/2$ vertices is thus $3 - 4/n$.
5. For a hypercube of dimension 4, how many edges (u,v) are there where u has a leading 0 and v has a leading 1?
   Answer: 8. The number of vertices in each cube is 8 and each has a mate in the other subcube.
6. What is the longest simple cycle in a d-dimensional hypercube, for $d > 1$?
   Answer: 2^d. They have a Hamiltonian cycle as proved in discussion.
7. For positive x, y, $2^x = 1 \pmod n$ and $2^y = 1 \pmod n$ what is $2^{gcd(x,y)} \pmod n$?
   Answer: 1. There is r,s where $gcd(x,y) = rx + sy$. Thus, we have $a^{gcd(x,y)} = a^{rx+sy} = (a^x)^r (a^y)^s = (1)^r (1)^s = 1 \pmod n$
8. If $x - y < x/2$, then $y >$ _____. (The answer should be in terms of x.)
   Answer: $x/2$. This is just algebra but happens to be part of the proof that the gcd algorithm's first argument decreases by a factor of two every other iteration.
9. The least common multiple of two positive numbers m and n is the smallest positive number that is a multiple of both. What is the least common multiple of m and n in terms of m, n and $d = gcd(m,n)$?
   Answer: $\frac{nm}{d}$. There has to be all the factors of n and m, but multiplying them together gives the factors in d twice. We can remove them by dividing.
10. What is the maximum number of solutions in $\{0, 1, \ldots, n-1\}$ to the equation $ax = b \pmod n$ if $gcd(n,a) = d$? (Answer in terms of n and d.)
    Answer: d. If b is a multiple of d, then answer is d, otherwise there are no solutions.

11. What is the size of the range of the function $f(x) = ax \pmod{n}$ where $x \in \{0, 1, \ldots, n-1\}$ if $gcd(n,a) = d$?

    Answer: n/d. The multiples of d is the range of this function.

12. For a prime p, how many numbers in $\{0, 1, \ldots, p^2 - 1\}$ have an inverse modulo p^2? (Answer in terms of p.)

    Answer: $p(p-1)$. The number of values in that range that are relatively prime to p

13. Given x and m with $gcd(x,m) = d$, and $d = ax + bm$, what is a value of z where $zx = 5d \pmod{m}$? (In terms of some subset of the variables x, m, a, d and b.)

    Answer: $5a$. $ax = ax + bm = d \pmod{m}$ and then multiply by 5.

14. What is $2^{75} \pmod{73}$?

    Answer: $8 \pmod{73}$. $2^{72} = 1 \pmod{73}$ makes it simple.

15. Let $p > 2$ be prime. What is $2^{k(p-1)} \pmod{p}$?

    Answer: 1. A quick test of exponents and FLT.

16. Find $x \pmod{20}$ that satisfies the equations: $x = 2 \pmod{4}$ and $x = 4 \pmod{5}$?

    Solution: 14. $2(5)(5^{-1} \pmod{4}) + 4(3)(3^{-1}) \pmod{5}) = 14 \pmod{20}$

17. If $gcd(m,n) = 1$, let $x = a + km$, what should k be to satisfy $x = b \pmod{n}$?

    Answer: $m^{-1}(b-a) \pmod{n}$. For $a + km = b \pmod{n}$, and solve.

18. What are the last two digits of 49^{19}? (Hint: $gcd(4,25) = 1$ and $24 = -1 \pmod{25}$.)

    Answer: 49. $49^{19} = (1)^{19} = 1 \pmod{4}$ and $(49)^{19} = (-1)^{19} = -1 \pmod{25}$. That is raising to the 19th power didn't change the modulus in either case. Thus, the value $\pmod{100}$ doesn't change either and we have that the result is 49. If one didn't notice that this is a fixed point, reconstructing using the CRT will work.

19. A fixed point of a function is a value x where $f(x) = x$. Consider the function $f(x) = x^3 \pmod{mn}$ for relatively prime $m > 2$ and $n > 2$. Note that $x = -1$, $x = 0$, and $x = 1$ are fixed points for x^3. Find another fixed point of $f(\cdot)$. (Your answer can include m, n and their inverses.)

    Answer: $n(n^{-1} \pmod{m}) - m(m^{-1} \pmod{n})$. A fixed point for x^3 are $x = 1$ or $x = -1$. That is also true $\pmod{m}$ and $\pmod{n}$ as well. So, take $x = 1 \pmod{m}$ and $x = -1 \pmod{n}$. Thus, we have $n(n^{-1} \pmod{m}) - m(m^{-1} \pmod{n})$.

3. Short Proofs. 5 pts each.

1. Prove that if $d \nmid n^2$ then $d \nmid n$. ($d \nmid n$ means n is not a multiple of d.)

   Solution: By contraposition: $d|n \implies d|n^2$.
   $d|n$ means there is an integer k where $n = kd$, we then have $n^2 = k^2d^2 = (k^2d)d$ which implies $d|n^2$ since k^2d is an integer.

2. Prove by induction that $(1-x)^n \geq 1 - nx$ for any natural number $n \geq 1$ and $0 < x < 1$.

   Solution: Base Case: $(1-x)^1 = (1-x) \geq (1-(1)x)$.
   Induction Step: $(1-x)^n = (1-x)^{n-1}(1-x) \geq (1-(n-1)x)(1-x) = (1-nx+(n-1)x^2) \geq (1-nx)$.
   We used the induction hypothesis in the first inequality, and the fact that $(n-1)x^2$ is positive for $n \geq 2$.

3. Prove that $x^2 = 7$ has no rational solutions.

   Solution:

Let a/b be a solution in reduced form to this equation and plug in to get

$$\left(\frac{a}{b}\right)^2 = 7.$$

Or we have $a^2 = 7b^2$, which indicates that 7 is a factor of a^2, and thus of a since 7 is not a perfect square. But since 7 is not a perfect square, we have that b^2 must also be a multiple of 7. This contradicts the notion that a/b was in reduced form.

4. Sleepiness.

1. (5 pts) Consider a set of intervals $[s_1, e_1], \ldots, [s_n, e_n]$ where s_i is the start time and e_i is the end time of an interval. The associated interval graph has a vertex for each interval and an edge between any pair of intervals that overlap; for example, if $i_1 = [3,5]$ and $i_2 = [4,6]$ and $i_3 = [6,7]$, there are edges (i_1, i_2), and (i_2, i_3) but no edge between i_1 and i_3.

   Prove that if there is a cycle in an interval graph then there is a point in time where at least 3 intervals overlap.

   Solution: Suppose for contradiction that within the cycle, $n_1, \ldots, n_k$, there does not exist three intervals that overlap. Let n_1 be the nap with the smallest start time. Since n_3 is connected to n_2, we cannot have n_3 overlap with n_1, so n_3's start time must happen after n_1's end time. But then n_4's start time must occur after n_3's start time, so the start times of the nodes will strictly increase. This is a contradiction, since the last nap, n_k, in the cycle must overlap with n_1.

2. (3 pts) Argue that for a graph $G = (V, E)$, if $|E| \geq |V|$, then G has a cycle.

   Solution: If the graph is connected, it cannot be acyclic as it has more than $|V| - 1$ edges and is not a tree. If it is disconnected, by the pigeonhole principle at least of the connected components has at least as many edges as vertices and we can apply the previous argument to that component.

3. (4 pts) Seven students each fall asleep three times during CS 70 lecture. Furthermore, for every two of these seven students, there exists a time when both of them are sleeping. Prove that there must be some time when at least three students were sleeping at once.

   Solution: Give each student three vertices, representing each of the times they fell asleep. Draw an edge between two vertices if the respective naps overlap. There are $7 \cdot 3 = 21$ vertices and $\frac{7 \cdot 6}{2} = 21$ edges. Therefore, this graph must have a cycle. By part (a), there must be three naps that overlap.

5. Colorings.

Define *exploding* a graph G as making a copy of it called G', and then adding an edge between each vertex $v \in G$ and its copy $v' \in G'$. Note that exploding a graph doubles the number of vertices. So, exploding an $(n-1)$-dimensional hypercube gets us an n-dimensional hypercube.

Jonathan has a graph G and wants to destroy all edges. At each step, he can choose to perform one of the following operations:

- Remove an odd-degree vertex and all its incident edges.
- Explode the graph.

Prove to Jonathan that no matter what graph G he starts with, he can get rid of all *edges* in a finite number of operations.

To help you out, we will break this down into parts. Define $f(G)$ as the smallest number of colors needed to vertex-color G.

1. (4 pts) Prove that exploding a graph where $f(G) > 1$ does not increase $f(G)$.
2. (4 pts) Suppose every vertex in G has even degree, and let G_{boom} be its exploded graph. Given a coloring of G_{boom}, prove that you can remove all vertices of a particular color in G_{boom}. (Potentially in multiple steps.)
3. (2 pts) Prove that if $f(G) = 1$, then Jonathan is done.
4. (4 pts) Now finish the proof: prove that there exists a finite sequence of operations for Jonathan to destroy all edges. (You may use results from previous parts.)

Solution:

1. Color G with $f(G)$ colors, and denote the colors $0, 1, 2, 3, \ldots, f(G)-1$. Color G' the same way, but replace color i with $i+1 \pmod{f(G)}$. All edges within G and G' do not invalidate the coloring, and edges between also do not since $i \neq i+1 \pmod{f(G)}$ if $f(G) > 1$.
2. After exploding G, we have a graph where every vertex has odd degree. Take color 0, and remove all vertices of that color one at a time. The removal of a 0-colored vertex does not decrease the degree of any other 0-colored vertex, because they cannot be connected by an edge, else they cannot both be colored 0.
3. Suppose Jonathan is not done. Then, there must still be an edge (u, v). But u and v must have different colors, so $f(G) > 1$. By contraposition, we have proven the statement.
4. The algorithm is to first remove odd degree vertices one at a time until either no edges remain, in which case we are done, or until all vertices have even degree.

   Then, we explode the graph and apply our procedure from part (b) to decrease the $f(G)$ by 1. Thus, within a finite number of operations, we can always decrease $f(G)$ by 1, until $f(G) = 1$. By part (c), we have reached our goal.

6. Chicken Nuggets.

In this problem, we explore the conundrum that Jonathan and Emaan face when they visit McDonald's. The chicken nuggets are sold in boxes of two different quantities, and they're interested in which quantities of chicken nuggets can be bought.

1. (3 pts) Find (x, y) that satisfy the equation $7x + 11y = 53$, where x and y have to be non-negative integers, and y is as small as it can be. *Hint: try taking mods of both sides to eliminate a variable first* **Solution:** Take $\pmod 7$ of both sides to get $4y \equiv 4 \pmod 7$. Multiplying both sides by 2 gives us $y \equiv 1 \pmod 7$. Therefore, the smallest y that works is $y = 1$. Plugging that in yields $x = 6$, so $(x, y) = (6, 1)$.
2. (3 pts) Explain why $7x + 11y = 59$ has no non-negative integer solutions for (x, y).

   Solution: Again, take $\pmod 7$ of both sides to get $4y \equiv 3 \pmod 7$. Multiplying both sides by $4^{-1} \equiv 2 \pmod 7$ gives us $y \equiv 6 \pmod 7$. Therefore, the smallest that y can be is 6. However, this means x must be at most $\frac{59-6\cdot 11}{7} = -1$, which is a contradiction.
3. Consider a store where chicken nuggets are sold in boxes of m and n with $\gcd(m, n) = 1$. Buying x boxes of m chicken nuggets and y boxes of n chicken nuggets yields $xm + yn$ chicken nuggets.

   (a) (2 pts) For any solution to $xm + yn = mn - m - n$, what is $x \pmod n$?

   Solution: -1 or $n - 1$.

(b) (4 pts) Argue that there is no solution for $xm + yn = mn - m - n$ where x and y are both non-negative integers.

Solution: If $k = mn - m - n = xm + yn$, we see that $x = -1 \pmod{n}$. The minimim value of this is $n-1$. Now the expression $(n-1)m + yn = mn - m + ny$. This is greater than $mn - m - n$ for any non-negative y.

4. The following two parts will prove that $mn - m - n$ is the largest number of chicken nuggets that **cannot** be bought.

(a) (3 pts) Prove that for any integer z, there is a solution to $xm + yn = z$ where $0 \leq x \leq n-1$.

Solution: By extended Euclid, there is x', y' such that $x'm + y'n = 1$. Therefore, taking $(x, y) = (zx', zy')$, we get $xm + yn = z$, which guarantees us the existence of an integer solution. Now, take $\pmod{n}$ on both sides of the equation.
Now $x = m^{-1}z \pmod{n}$, and $x = m^{-1}z \pmod{n}$ has a representative in $\{0, \ldots, n-1\}$.
Thus, we have $xm = z \pmod{n}$ or $z = xm + kn$ for some value of k. That is, take $y = k$.
Alternative: One can notice that when x is positive (which is without loss of generality), one can subtract n from x and add m to y and $xm + yn$ does not change. Thus, one can do this until x is in the right range.

(b) (3 pts) Argue that for any $z > mn - m - n$, there is a solution to $xm + yn = z$ where x and y are non-negative.

Solution: Again, by extended Euclid there is $z = xm + yn$ where possibly one of x positive and y is negative. (W.l.o.g.)
As per above we can assume $x \leq n - 1$.
We have $xm \leq (n-1)m = mn - m$, and notice for $y < 0$, we have $xm + yn \leq mn - m - n$. Thus, for $z > mn - m - n$, y is not negative.