CS 70 Midterm 1 Review

Fall 2020

October 11, 2020

Agenda

Agenda

- 7 Questions: You try problems, we present solutions.

Agenda

- 7 Questions: You try problems, we present solutions.
- Don't write up a complete solution to each question in the allotted time - but do think about an approach.

Agenda

- 7 Questions: You try problems, we present solutions.
- Don't write up a complete solution to each question in the allotted time - but do think about an approach.
- Please ask questions!

The Puzzle of Green-Eyed Dragons

100 green-eyed dragons live on an island. They have a rule: if you find out that you have green eyes, you must commit ritual suicide at sundown. Despite this rule, they live in peace.

One day, a visitor comes to the island and says "I see a dragon here has green eyes". The visitor leaves.

On day 100, every dragon commits suicide. Why?

Solution

- **Claim**: For every positive integer n, if there are n green-eyed dragons on the island, and a visitor says that one of them has green eyes, they commit ritual suicide on day n.

Solution

- **Claim**: For every positive integer n, if there are n green-eyed dragons on the island, and a visitor says that one of them has green eyes, they commit ritual suicide on day n.
- **Base case:** There is one green-eyed dragon. After one day, the dragon performs the ritual.

Solution

- **Claim**: For every positive integer n, if there are n green-eyed dragons on the island, and a visitor says that one of them has green eyes, they commit ritual suicide on day n.
- **Base case:** There is one green-eyed dragon. After one day, the dragon performs the ritual.
- **Inductive Hypothesis:** Assume the claim is true for n green-eyed dragons.

Solution

- **Claim**: For every positive integer n, if there are n green-eyed dragons on the island, and a visitor says that one of them has green eyes, they commit ritual suicide on day n.
- **Base case:** There is one green-eyed dragon. After one day, the dragon performs the ritual.
- **Inductive Hypothesis:** Assume the claim is true for n green-eyed dragons.
- **Inductive Step:** Now consider an island of $n+1$ green-eyed dragons. Each green-eyed dragon sees n other green-eyed dragons and thinks: "If there were only n green-eyed dragons, they would have committed suicide on day n. But they did not, so there must be $n+1$ green-eyed dragons. Including me!"

Stable Matching

In class we showed that the propose-and-reject algorithm must terminate after at most n^2 proposals. Prove a sharper bound showing that the algorithm must terminate after at most $n(n-1)+1$ proposals.

Solution

- On the day when a job, J, proposes to the last candidate on its list C, we claim that every other candidate must have some job on her string.
- This is because J gave an offer to each of these candidates, and by the Improvement Lemma, once a candidate has been proposed to she always has a job on her string.

Solution

- On the day when a job, J, proposes to the last candidate on its list C, we claim that every other candidate must have some job on her string.
- This is because J gave an offer to each of these candidates, and by the Improvement Lemma, once a candidate has been proposed to she always has a job on her string.
- Since there are $n-1$ other candidates, they must be paired with all $n-1$ remaining jobs.
- Thus there is only one proposal on this day, and since it is accepted, the algorithm halts.
  Therefore, at most one job proposes an offer to its last choice, and thus there are at most $n^2 - (n-1) = n(n-1) + 1$ proposals.

More Planar Bounds

Let G be a planar graph with n vertices, and where the smallest cycle has length k. Prove that the number of edges is at most

$$\frac{k(n-2)}{k-2}.$$

Solution

- Remember we proved something similar for bipartite (i.e. triangle-free) graphs: $|E| \leq 2|V| - 4$.

Solution

- Remember we proved something similar for bipartite (i.e. triangle-free) graphs: $|E| \leq 2|V| - 4$.
- Notice that every edge is a part of exactly two faces. We can count the number of edges by also looking at how many edges border each face.
- Since the smallest cycle has length k, every face has at least k edges, so $2|E| = |F_1| + |F_2| + \cdots \geq k|F|$.

Solution

- Remember we proved something similar for bipartite (i.e. triangle-free) graphs: $|E| \leq 2|V| - 4$.
- Notice that every edge is a part of exactly two faces. We can count the number of edges by also looking at how many edges border each face.
- Since the smallest cycle has length k, every face has at least k edges, so $2|E| = |F_1| + |F_2| + \cdots \geq k|F|$.
- Recall Euler's Theorem now: $|V| - |E| + |F| = 2$.
- Rearranging, we get that $|F| = 2 - |V| + |E|$. So

$$2|E| \geq k|F| = 2k - k|V| + k|E|$$

$$|E| \leq \frac{k(|V| - 2)}{k - 2}$$

Modular Arithmetic

Let n be a positive integer, and a is an integer that is relatively prime to n. Prove that if $a^x \equiv 1 \pmod{n}$ and $a^y \equiv 1 \pmod{n}$ then

$$a^{\gcd(x,y)} \equiv 1 \pmod{n}$$

.

Solution

- By Extended Euclid's Algorithm, we know that there exists r and s such that $xr + ys = \gcd(x, y)$.

Solution

- By Extended Euclid's Algorithm, we know that there exists r and s such that $xr + ys = \gcd(x, y)$.
- Therefore, we know that $a^{\gcd(x,y)} \equiv a^{xr+ys} \equiv (a^x)^r \cdot (a^y)^s \equiv 1^r \cdot 1^s \equiv 1 \pmod{n}$.

Breaking RSA

(a) Alice sends the same message, $m < N$, to two friends, Bob and Carol, using the standard RSA protocol. Bob's public key is (N, e_1) and Carol's is (N, e_2), where $\gcd(e_1, e_2) = 1$. Explain how an eavesdropper, Eve, can decrypt m by observing the encrypted messages that Alice sends to Bob and Carol.

(b) Dennis decides to simplify the RSA cryptosystem as follows. Instead of choosing the usual type of public key $(N = pq, e)$, he instead chooses a key (N, e) where N is a prime and e is an integer in $\{2, ..., N-1\}$ with $\gcd(N-1, e) = 1$. To send a message m to Dennis, Alice sends the encrypted message $m^e \pmod{N}$. Is Dennis' scheme secure? Explain.

Solution to part (a)

Sending messages (N, e_1) *and* (N, e_2), $\gcd(e_1, e_2) = 1$.

Solution:

Solution to part (a)

Sending messages (N, e_1) *and* (N, e_2), $\gcd(e_1, e_2) = 1$.

Solution:
Key Idea: Use the extended gcd algorithm.

Solution to part (a)

Sending messages (N, e_1) *and* (N, e_2), $\gcd(e_1, e_2) = 1$.

Solution:
Key Idea: Use the extended gcd algorithm.
Since $\gcd(e_1, e_2) = 1$, Eve can use the extended gcd algorithm to efficiently find $a, b \in \mathbb{Z}$ such that $ae_1 + be_2 = 1$.

Solution to part (a)

Sending messages (N, e_1) *and* (N, e_2), $\gcd(e_1, e_2) = 1$.

Solution:
Key Idea: Use the extended gcd algorithm.
Since $\gcd(e_1, e_2) = 1$, Eve can use the extended gcd algorithm to efficiently find $a, b \in \mathbb{Z}$ such that $ae_1 + be_2 = 1$.
Observing me_1 and me_2, she can then proceed to compute

$$(m^{e_1})^a \cdot (m^{e_2})^b \equiv m^{ae_1} \cdot m^{be_2} \equiv m^{ae_1+be_2} \equiv m \pmod{N}.$$

Solution to part (b)

Using $N = p$ in the standard RSA protocol.

Solution:

Solution to part (b)

Using $N = p$ in the standard RSA protocol.

Solution:
Since e is relatively prime to $N - 1$, Eve can efficiently compute the inverse $e^{-1} \pmod{N-1}$ (using the extended gcd algorithm). Furthermore, since $ee^{-1} \equiv 1 \pmod{N-1}$, it must be the case that $ee^{-1} = k(N-1) + 1$ for some $k \in \mathbb{Z}$.

Solution to part (b)

Using $N = p$ in the standard RSA protocol.

Solution:
Since e is relatively prime to $N - 1$, Eve can efficiently compute the inverse $e^{-1} \pmod{N-1}$ (using the extended gcd algorithm). Furthermore, since $ee^{-1} \equiv 1 \pmod{N-1}$, it must be the case that $ee^{-1} = k(N-1) + 1$ for some $k \in \mathbb{Z}$.
Consequently Eve can compute

$$(m^e)^{e^{-1}} \equiv m^{ee^{-1}} \equiv m^{k(N-1)+1} \equiv (m^{N-1})^k \cdot m \equiv m \pmod{N}$$

where the last congruence follows from Fermat's Little Theorem.

Interpol Warning

Consider the set of four points $\{(-1, 1), (0, 2), (1, 5), (2, 40)\}$. Find the unique polynomial over $\mathbb{R}$ of degree ≤ 3 that passes through these points by either solving a system of linear equations or by Lagrange Interpolation.

Solution

By solving a system of linear equations:

Solution

By solving a system of linear equations:
Suppose desired polynomial is of form $ax^3 + bx^2 + cx + d$. Then

Solution

By solving a system of linear equations:
Suppose desired polynomial is of form $ax^3 + bx^2 + cx + d$. Then

$$\begin{aligned} -a + b - c + d &= 1 \\ d &= 2 \\ a + b + c + d &= 5 \\ 8a + 4b + 2c + d &= 40 \end{aligned}$$

Solution

By solving a system of linear equations:
Suppose desired polynomial is of form $ax^3 + bx^2 + cx + d$. Then

$$\begin{aligned} -a + b - c + d &= 1 \\ d &= 2 \\ a + b + c + d &= 5 \\ 8a + 4b + 2c + d &= 40 \end{aligned}$$

Solving this system (elimination, substitution, etc.) gives $a = 5, b = 1, c = -3, d = 2$. Therefore the polynomial is $5x^3 + x^2 - 3x + 2$.

By Lagrange Interpolation:

By Lagrange Interpolation:
Delta functions!

By Lagrange Interpolation:
Delta functions!

$$\Delta_{-1}(x) = \frac{x(x-1)(x-2)}{(-1)(-1-1)(-1-2)} = -\frac{1}{6}(x^3 - 3x^2 + 2x)$$

$$\Delta_0(x) = \frac{(x+1)(x-1)(x-2)}{(1)(-1)(-2)} = \frac{1}{2}(x^3 - 2x^2 - x + 2)$$

$$\Delta_1(x) = \frac{(x+1)(x)(x-2)}{(1+1)(1)(1-2)} = -\frac{1}{2}(x^3 - x^2 - 2x)$$

$$\Delta_2(x) = \frac{(x+1)(x)(x-1)}{(2+1)(2)(2-1)} = \frac{1}{6}(x^3 - x)$$

Then we want the polynomial to be

Then we want the polynomial to be

$$\begin{aligned}
&\Delta_{-1}(x) + 2\Delta_0(x) + 5\Delta_1(x) + 40\Delta_2(x) \\
&= -\frac{1}{6}(x^3 - 3x^2 + 2x) + 2\frac{1}{2}(x^3 - 2x^2 - x + 2) \\
&\quad - 5\frac{1}{2}(x^3 - x^2 - 2x) + 40\frac{1}{6}(x^3 - x) \\
&= 5x^3 + x^2 - 3x + 2
\end{aligned}$$

Same answer as solving system of linear equations.

Then we want the polynomial to be

$$\begin{aligned}
&\Delta_{-1}(x) + 2\Delta_0(x) + 5\Delta_1(x) + 40\Delta_2(x) \\
&= -\frac{1}{6}(x^3 - 3x^2 + 2x) + 2\frac{1}{2}(x^3 - 2x^2 - x + 2) \\
&\quad - 5\frac{1}{2}(x^3 - x^2 - 2x) + 40\frac{1}{6}(x^3 - x) \\
&= 5x^3 + x^2 - 3x + 2
\end{aligned}$$

Same answer as solving system of linear equations.

Note: If the polynomial is modulo p, replace any fractions with multiplying by the denominator's inverse modulo p.

Counting Review

(a) How many orderings are there of the numbers from 1 to $2n$, in which the numbers $1, \ldots, n$ occur in an increasing order (but not necessarily contiguously)?

(b) Two committees are to be formed from a group of n citizens. In how many ways can these committees be formed, so that each person serves on at most one committee, and each committee contains at least one member?

(c) A Social Security Number is any sequence of nine digits. How many Social Security Numbers have at least eight different digits?

Solution to part (a)

- Suppose we have $2n$ empty spots in a row that we need to fill with numbers.

Solution to part (a)

- Suppose we have $2n$ empty spots in a row that we need to fill with numbers.
- Choose n of these and fill in $1, \ldots, n$ in increasing order.

Solution to part (a)

- Suppose we have $2n$ empty spots in a row that we need to fill with numbers.
- Choose n of these and fill in $1, \ldots, n$ in increasing order.
- For the remaining n spots, there are $n!$ ways to put $n+1, \ldots, 2n$ into them.
- In total, we have $\binom{2n}{n} n! = \frac{(2n)!}{n!}$.

Solution to part (b)

- Big picture: Each person has to go on either committee 1, committee 2, or neither.

Solution to part (b)

- Big picture: Each person has to go on either committee 1, committee 2, or neither.
- Let x, y be the number of people on each committee, and z be those not on one. Since each person is either on one committee or not, $x + y + z = n$.
- Each committee contains at least one member, so $x, y \geq 1$.

Solution to part (b)

- Big picture: Each person has to go on either committee 1, committee 2, or neither.
- Let x, y be the number of people on each committee, and z be those not on one. Since each person is either on one committee or not, $x + y + z = n$.
- Each committee contains at least one member, so $x, y \geq 1$.
- If we let $x' = x - 1, y' = y - 1$, then we are looking for non-negative solutions to $x' + y' + z = n - 2$. By balls and boxes, this is $\binom{(n-2)+3-1}{3-1} = \binom{n}{2}$.

Solution to part (c)

- At least eight different digits $\implies$ Exactly eight or nine.

Solution to part (c)

- At least eight different digits $\implies$ Exactly eight or nine.
- Case 1: Exactly eight different digits. There are $\binom{10}{2}$ ways to choose the eight digits, and $\binom{8}{1}$ ways to choose the repeated digit. Then we need to permute 7 distinct digits and 2 identical ones, which has $9!/2$ ways.

Solution to part (c)

- At least eight different digits $\implies$ Exactly eight or nine.
- Case 1: Exactly eight different digits. There are $\binom{10}{2}$ ways to choose the eight digits, and $\binom{8}{1}$ ways to choose the repeated digit. Then we need to permute 7 distinct digits and 2 identical ones, which has $9!/2$ ways.
- Case 2: Exactly nine different digits. There are $\binom{10}{9} = 10$ ways to select the digits, and 9! ways to permute.

Solution to part (c)

- At least eight different digits $\implies$ Exactly eight or nine.
- Case 1: Exactly eight different digits. There are $\binom{10}{2}$ ways to choose the eight digits, and $\binom{8}{1}$ ways to choose the repeated digit. Then we need to permute 7 distinct digits and 2 identical ones, which has $9!/2$ ways.
- Case 2: Exactly nine different digits. There are $\binom{10}{9} = 10$ ways to select the digits, and $9!$ ways to permute.
- In total, our answer is

$$\binom{10}{2}\binom{8}{1} \cdot \frac{9!}{2} + 10 \cdot 9! = \frac{10 \cdot 9}{2 \cdot 1} \cdot 8 \cdot \frac{9!}{2} + 10! = 19 \cdot 10!.$$