HKN CS70 Midterm 1 Review

Allen Xiao, Edwin Liao, Sung Roa Yoon, Varun Pai
2.26.2012

some slides adapted from Jon Kotker

Propositional Logic

Quantifiers

$\exists$: in this universe, I can find at least one

$\forall$: in this universe, every one is

Implication

$\Rightarrow$: if A then B

== (not A) or B

== if (not B) then (not A)

Logical Implication

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

contrapositive

Propositional Logic

For non-negative integers x and y, let P(x,y) be the proposition that $x + y > xy$.

Are the following True, False, or Undertermined?

1) $\forall x \; \exists y \; P(x, y)$

true

2) $\exists x \; \exists y \; P(x, y)$

true

3) $\forall x \; \forall y \; P(x, y)$

false

Propositional Logic

Which of the following implications are true?

1) If we are in 306 Soda, then Christmas is in December.

   true ⇒ true is true

2) If the Earth is flat, then horses can speak English.

   false ⇒ false is true

3) If Coca-Cola is a soda, then it is only sold at Trader Joes.

   true ⇒ false is false

4) If it's raining in Tokyo, then it is the capital of Japan.

   anything ⇒ true is true

5) If you are here for EE20, then the midterm is on Wednesday.

   false ⇒ anything is true

Proofs

Direct:

It is raining ⇒ more auto accidents will happen

Assume it is raining

It is raining ⇒ the road is wet

the road is wet ⇒ cars will slip on the road

cars will slip on the road ⇒ more auto accidents will happen

Therefore more auto accidents will happen

Contraposition:

It is raining ⇒ my cat is inside

show instead: my cat is **not** inside ⇒ it is **not** raining

Assume my cat is not inside

my cat is not inside ⇒ it is not wet outside

it is not wet outside ⇒ it is not raining

Therefore it is **not** raining

So (my cat is **not** inside ⇒ it is **not** raining) ≡ (it is raining ⇒ my cat is inside)

Proofs

Direct:

$p \Rightarrow q$

Assume p

...

q

Therefore q

Contraposition:

$p \Rightarrow q$

show instead: **not** q $\Rightarrow$ **not** p

Assume **not** q

...

Therefore it is **not** p

So (**not** q $\Rightarrow$ **not** p) $\equiv$ (p $\Rightarrow$ q)

Proofs

Contradiction: (may seem similar to contrapositive, different)

I am alive and healthy ⇒ I can breathe

Assume I can **not** breathe
I am alive and healthy ⇒ I am thinking

I can't breathe ⇒ my brain gets no oxygen

my brain gets no oxygen ⇒ I am **not** thinking

contradiction, therefore I am alive and healthy

Cases: (try ALL the possibilities!)

any number c that is a perfect cube (n^3) ⇒ c is a multiple of 9, or +/- 1 a multiple of 9

case 1: n is a multiple of 3 (k):

$n^3 = 27k^3$

$27k^3 \% 9 = 0$ done

case 2: n is (k) + 1:

$n^3 = 27k^3 + 27k^2 + 9k + 1$

$(27k^3 + 27k^2 + 9k + 1) \% 9 = 1$ done

case 2: n is (k) - 1:

$n^3 = 27k^3 - 27k^2 + 9k - 1$

$(27k^3 - 27k^2 + 9k - 1) \% 9 = -1$ done

Proofs

Contradiction: (may seem similar to contrapositive, different)

$p \Rightarrow q$

Assume **not** q

...

s

...

not s

contradiction, therefore q

Cases: (try ALL the possibilities!)

$p \Rightarrow q$

case 1: ... (show $p \Rightarrow q$ holds)

case 2: ... (show $p \Rightarrow q$ holds)

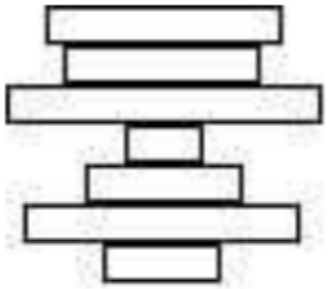
...

show that the list of cases is **exhaustive**, i.e. covering every case possible

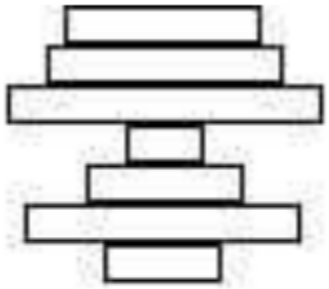
in each case, show that the implication holds

Induction

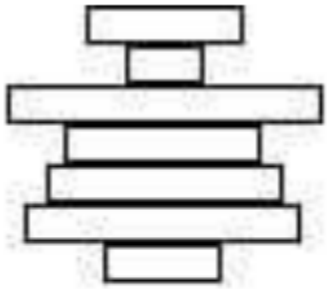
In his twenties, Professor Sinclair used to work at Cheeseboard. Part of his daily job was to sort huge stacks (largest on the bottom) of pizzas using only his spatula. The only operation he was allowed to do was to flip pizzas with his spatula using the stick-and-flip operation shown below. Prove that no matter how many pizzas Prof. Sinclair was given, he could always order them using some sequence of stick-and-flip operations.



initial stack



after flippling top two pizzas in initial stack



after flipping top five pizzas in initial stack

Induction at the RSF

Prove that every amount of postage that is at least 12 cents can be made from 4-cent and 5-cent stamps.

Stable Marriage Problem: Basic Overview

- There are n men and n women. Each man has an ordered preference list of the n women, and each woman has a similar list of the n men. (No ties allowed).
- **Stability:** A pairing is unstable if there is a man and a woman who prefer each other to their current partners.
- **Rogue partners:** A man and a woman who prefer each other to their current partners.
- When we have n men and n women, as opposed to n men who are looking for roommates or such, there is a guarantee that a stable pairing exists.

Traditional Marriage Algorithm: Basic Overview

- **Every Morning:** Each man goes to the first woman on his list not yet crossed off and proposes to her.
- **Every Afternoon:** Each woman says "Maybe, come back tomorrow" to the man she likes best among the men who have proposed to her and "No, I will never marry you!" to all the rest.
- **Every Evening:** Each rejected suitor crosses off the woman who rejected him from his list.
- The above loop is repeated each successive day until there are no more rejected suitors. On this day, each woman marries the man she has on a string.
- **THIS LOOP IS MALE OPTIMAL (IT FAVORS THE MALE'S DESIRES OVER THE FEMALES)**
- If you want to find female optimal solution, then you do the loop except replace the gender nouns.

Find a male or a female optimal pairing. (depending on what you prefer)

Men	First	Second	Third
1	A	C	B
2	C	A	B
3	C	B	A

Women	First	Second	Third
A	2	3	1
B	1	3	2
C	1	2	3

Find a male or a female optimal pairing. (depending on what you prefer)

Men	First	Second	Third
1	A	C	B
2	C	A	B
3	C	B	A

Women	First	Second	Third
A	2	3	1
B	1	3	2
C	1	2	3

Male Optimal: [(1, A), (2, C), (3, B)]

Female Optimal: [(A, 2), (B, 3), (C, 1)]

Quick True or False Questions (In Male Optimal TMA With m men and m women)

- Can every man get the woman on the top of his list even though the woman does not have him at the top of her list?

- If a man has a woman on the bottom of his list, and the woman has him in the bottom of her list, can there be stable pairings with him and her together for all m?

- If there are more than one stable pairing for a TMA, can any pairing be both male optimal and female optimal?

- If a man is second on every woman's list, can there be a stable pairing where the man ends up with his least favorite woman?

Quick True or False Questions (In Male Optimal TMA With m men and m women)

- Can every man get the woman on the top of his list even though the woman does not have him at the top of her list?
  YES
- If a man has a woman on the bottom of his list, and the woman has him in the bottom of her list, can there be stable pairings with him and her together for all m?

- If there are more than one stable pairing for a TMA, can any pairing be both male optimal and female optimal?

- If a man is second on every woman's list, can there be a stable pairing where the man ends up with his least favorite woman?

Quick True or False Questions (In Male Optimal TMA With m men and m women)

- Can every man get the woman on the top of his list even though the woman does not have him at the top of her list?
  YES
- If a man has a woman on the bottom of his list, and the woman has him in the bottom of her list, can there be stable pairings with him and her together for all m?
  YES
- If there are more than one stable pairing for a TMA, can any pairing be both male optimal and female optimal?

- If a man is second on every woman's list, can there be a stable pairing where the man ends up with his least favorite woman?

Quick True or False Questions (In Male Optimal TMA With m men and m women)

- Can every man get the woman on the top of his list even though the woman does not have him at the top of her list?
  YES
- If a man has a woman on the bottom of his list, and the woman has him in the bottom of her list, can there be stable pairings with him and her together for all m?
  YES
- If there are more than one stable pairing for a TMA, can any pairing be both male optimal and female optimal?
  NO
- If a man is second on every woman's list, can there be a stable pairing where the man ends up with his least favorite woman?

Quick True or False Questions (In Male Optimal TMA With m men and m women)

- Can every man get the woman on the top of his list even though the woman does not have him at the top of her list?
  YES
- If a man has a woman on the bottom of his list, and the woman has him in the bottom of her list, can there be stable pairings with him and her together for all m?
  YES
- If there are more than one stable pairing for a TMA, can any pairing be both male optimal and female optimal?
  NO
- If a man is second on every woman's list, can there be a stable pairing where the man ends up with his least favorite woman?
  YES

Polynomials

1) Suppose I had a secret to share among 10 people, but I also want at least 6 people to get together before they can figure out the secret. What degree polynomial should I use?

7 (d+1)

2) How many polynomials of degree (at most) 4 are there GF(19)?

19^5

3) Suppose you are given two points (x1, x2) and (x2, y2). How many distinct degree 2 polynomials are there that go through these two points mod m? What about degree 3?

need 3 points to determine a unique degree 2 polynomial!

for degree 2: m

for degree 3: m^2

Secret Sharing

- There are n people total.
- There must be at least k number of people in agreement to solve the secret.
- The secret code is some natural number s.
- The secret sharing takes place in GF(q) where q is a prime number larger than n and s.
- We pick a random polynomial P(x) of degree k – 1 such that P(0) = s, and give the keys P(1) to P(n) to the corresponding officer.
- K number of officer can easily use Lagrange interpolation to find the secret, but any less number of officers can obtain no information.

Secret Sharing Problems

- Why must we solve the secret sharing problem in modulo field?

- What is the issue with having the secret being larger than the mod value?

- What is the issue with having the total number of people involved being greater than the mod value?

Secret Sharing Problems

- Why must we solve the secret sharing problem in modulo field? **Because we cannot compute the lagrange interpolation without division, and division isn't closed for integers outside mod field**
- What is the issue with having the secret being larger than the mod value?

- What is the issue with having the total number of people involved being greater than the mod value?

Secret Sharing Problems

- Why must we solve the secret sharing problem in modulo field?
  Because we cannot compute the lagrange interpolation without division, and division isn't closed for integers outside mod field
- What is the issue with having the secret being larger than the mod value?
  You can never find the correct secret because the correct solution will produce an equivalent number to the secret, not the actual number.
- What is the issue with having the total number of people involved being greater than the mod value?

Secret Sharing Problems

- Why must we solve the secret sharing problem in modulo field?
  Because we cannot compute the lagrange interpolation without division, and division isn't closed for integers outside mod field
- What is the issue with having the secret being larger than the mod value?
  You can never find the correct secret because the correct solution will produce an equivalent number to the secret, not the actual number.
- What is the issue with having the total number of people involved being greater than the mod value?
  Because then one of the people involved will have the actual secret number, or a minimum of k people may be insufficient to discover the secret (two of them have the same coefficient!)