CSM 70 Discrete Mathematics and Probability Theory

Spring 2016 Midterm 1 Review

Logic

Proposition Problems

1. Distribute negations so that negations only apply to single propositions: $\neg((A \Rightarrow \neg B) \vee (P \wedge Q))$

2. True or false? $((\neg P \Rightarrow \neg Q) \Leftrightarrow (P \Rightarrow Q))$

3. True or false? $(P \Rightarrow Q) \Leftrightarrow (\neg((\neg Q) \wedge P))$

Quantify These!

True or False?

1. $(\forall x, \exists y : P(x,y)) \Leftrightarrow (\forall y, \exists x : P(x, y))$

2. $(\forall x, \exists y : P(x,y)) \Rightarrow (\exists x : \exists y : P(x,y))$

3. $(\exists x : \forall y, P(x,y)) \Rightarrow (\forall y, \exists x : P(x,y))$

4. $(\exists x : \forall y, P(x,y)) \Leftrightarrow (\forall y, \exists x : P(x,y))$

Methods of Proof

Proofs for Days

1. Prove that the sum of two even integers is even

2. If x is not the sum of two even integers, then x is odd

3. Every integer that is a perfect cube is equal to, one less than, or one more than a multiple of 9

4. There is no smallest positive rational number

5. $$\sum_{i=1}^{n} 2^i = 2^{n+1} - 2$$

6. A package that costs 12 cents or more can be paid for with some number of 4 cent and 5 cent stamps

Stable Marriage

How do we obtain a pairing that is female optimal and male pessimal?

1. Prove that only one man can be rejected $n - 1$ times.

2. **Extra**: Use this to prove a bound of $n(n-1) + 1$ on the number of days.

3. **Challenge**: construct an example for $n = 3$

Short Exercises

1. What is the minimum number of days the algorithm can take? In what situations will this happen?

2. Construct a scenario with 4 men and 4 women that takes 5 days to run

3. Reconstruct the preference list of the men and women involved in the following algorithm:

A	-	-	-	-	-	-	-	1
B	4	4	3, ~~4~~	3	2, ~~3~~	2	2	2
C	3	1, ~~3~~	1	1	1	1	~~1~~, 4	4
D	~~1~~, 2	2	2	~~2~~, 4	4	3, ~~4~~	3	3

Graph Theory

Even Steven

Prove that the sum of the degrees of the vertices of any graph is even.

Cycling Through Graphs

Prove that a graph is bipartite if and only if it contains no cycles of odd length.

Walking in Cycles

If a connected graph has at most two odd degree vertices, then it has an Eulerian walk between them.

Tree’s Degrees

Show that if G is a tree with maximum degree greater than or equal to k, then G has at least k leaves.

Paths and Degrees

Let G be a graph where all vertices have degree at least d. Prove that G contains a path of length d.

Collapsing Bridges

Edge e is a bridge if the graph G' with edge e removed has more connected components than the original graph. Prove that if each vertex has even degree then there are no bridges.

Disjoint Cycles

Prove that given a connected graph $G = (V, E)$, the degrees of all vertices of G are even if and only if there is a set of edge-disjoint cycles in G that cover the edges of G. (That is, the edge set of G is the disjoint union of the edge sets of these cycles.)

Party Planning

Prove that every set of 6 people contain at least three mutual acquaintances or three mutual strangers.

Vicious Cycle

Prove that every graph with n vertices and at least n edges must have a cycle

Hamilton and Cubes

For any $n \geq 2$, the n-dimensional hypercube has a Hamiltonian cycle.

Cube is Life
For any $n \geq, 2$, the n-dimensional hypercube has a Hamiltonian cycle.

Modular Arithmetic

Divide by K
Prove that the product of any $k \geq 1$ consecutive integers is divisible by k.

So You Think You Can FLT?

1) $4^{10} \pmod{11}$

2) $4^{275} \pmod{11}$

RSA

Becoming Alice

Alice wants to send Bob a message $m = 5$ using his public key ($n = 26$, $e = 11$). What ciphertext $E(m)$ will Alice send?

Cracking RSA

Suppose Bob's RSA public key is (e, n), where e is the encryption key, and $n = pq$ is the product of two primes. Alice has just sent a secret message $c = me \bmod n$ to Bob using Bob's public key.

(a) Explain how Bob can decrypt the message he has received

(b) Now suppose that by eavesdropping on their conversation you managed to overhear the ciphertext c. Moreover, when crafting his public key Bob foolishly chose primes that were too small, so that by continuously running a fast factoring algorithm on one of Berkeley's supercomputing clusters for two weeks, you eventually manage to factor n, and recover p and q. Given e, p, q, and c, explain how you can now efficiently recover plaintext m of Alice's message to Bob.

Decrypting CIA

Imagine you are a CIA double agent. As a good spy you have discovered that agents Smith and Jones share the same modulo in their respective RSA public keys.

$s = 9, n = 179$

$j = 13, n = 179$

After some days sniffing the network, you see that the CIA director has sent the same message m to both agents. He sent $C_s = 32$ and $C_j = 127$. Can you recover the original message?

Thanks for coming! :)