University of New Mexico
Department of Computer Science

Midterm Examination

CS 261 Mathematical Foundations of Computer Science
Spring, 2010

Name:
Email:

- "Nothing is true. All is permitted" - Friedrich Nietzsche. Well, not exactly. **You are not permitted to discuss this exam with any other person.** If you do so, you will surely be smitten (collusion on any problem will result in a 0 on the test). You may consult any *other* sources including books, papers, web pages, computational devices, animal entrails, seraphim, cherubim, etc. in your quest for truth and solutions. Please acknowledge your sources.
- *Show your work!* You will not get full credit if we cannot figure out how you arrived at your answer. A numerical solution obtained via a computer program is unlikely to get much credit without a correct mathematical derivation.
- Write your solution in the space provided for the corresponding problem. Do NOT use any extra paper for your final solutions.
- If any question is unclear, ask for clarification.

Question	Points	Score	Grader
1	20		
2	20		
3	20		
4	20		
5	20		
Total	100		

1. **Logic and Proofs**

(a) (4 points) Show that $(a \to b) \wedge (a \to c)$ is logically equivalent to $a \to (b \wedge c)$. Justify each step. *Solution:*

$$\begin{aligned}
(a \to b) \wedge (a \to c) &= (\neg a \vee b) \wedge (\neg a \vee c) && (1)\\
&= ((\neg a \vee b) \wedge \neg a) \vee ((\neg a \vee b) \wedge c) && (2)\\
&= \neg a \vee ((\neg a \vee b) \wedge c) && (3)\\
&= \neg a \vee (\neg a \wedge c) \vee (b \wedge c) && (4)\\
&= \neg a \vee (b \wedge c) && (5)\\
&= a \to (b \wedge c) && (6)
\end{aligned}$$

Where step 1 follows from Example 3 in the book. Step 2 follows from the second distributive law. Step 3 follows from the second absorption law. Step 4 follows by the second distributive law. Step 5 follows by associativity and absorbtion. Step 6 follows by Example 3.

(b) (6 points) Prove that if $3x + 2$ is odd, then x is odd. *Solution: We will show the contrapositive: if x is even then $3x+2$ is even. If x is even, it equals $2k$ for some integer k. Thus $3x + 2 = 6k + 2 = 2(3k + 1)$ which is clearly an even number.*

(c) (10 points) Prove or disprove that you can tile a 7 by 7 checkerboard with dominos if the top left, top right and bottom right squares are missing. *Solution: This can't be done. We can show this with a coloring argument as follows. Color every odd square in the i-th row black, where i is an odd number, and all remaining squares red. In particular, the odd numbered squares in the first and last row will be black so the top left, top right, bottom left and bottom right squares are all black. There are thus* 22 *black squares and* 24 *red squares. However, each domino must cover both a red and a black square so the fact that there is not an equal number of each color implies that it is not possible to cover this checkerboard with dominos*

2. **Sets, Number Theory and Proofs**

(a) (6 points) Find a solution to the equation $5x \equiv 11 \pmod{21}$ using techniques from this class. Show your work! *Solution: Using Euclid's algorithm, we can find that the inverse of* 5 *mod* 21 *is* -4. *Multiplying both sides of the equation by* -4, *we get that* $x \equiv -44 \pmod{21}$ *or equivalently,* $x \equiv 19 \pmod{21}$

(b) (7 points) Prove that $11\sqrt{n}+1$ is $O(n)$ *Solution: We must find constants* n_0 *and* c *such that for all* $n \geq n_0$, $11\sqrt{n} \leq cn$. *In the previous inequality, divide both sides by* $\sqrt{n}$ *to get* $11 \leq c\sqrt{n}$. *This inequality is satisfied for* $n \geq 1$ *and* $c = 11$. *Thus we need* $n_0 = 1$ *and* $c = 11$.

(c) (7 points) Simplify the following set as much as possible: $B \cap \overline{(\bar{A} \cup B) \cap \bar{A}}$. *Solution:* $\overline{(\bar{A} \cup B) \cap \bar{A}}$ *is equivalent to* $(A \cap \bar{B}) \cup A$ *(by DeMorgan's Law), which is equivalent to the set* A *since* $A \cap X \subseteq A$ *for any* X*. Thus, the entire set is equivalent to* $B \cap A$*.*

3. **Doorbells and Litigants**

In a certain neighborhood, the houses are numbered 1 through n. One night, a mischievous mathematician circles through the neighborhood as follows. For every number i from 2 to n, the mathematician circles through the neighborhood ringing the doorbell of every house that is a multiple of i (i.e. she first circles through ringing the bells of all homes divisible by 2, then circles again to ring the bells of all homes divisible by 3, etc., etc.) The neighborhood association playfully retaliates by launching a class-action lawsuit against the mathematician. In this problem, you will use your knowledge about number theory to help them collect vital information for this lawsuit.

(a) (4 points) How many homes had their doorbell rung exactly once? Your answer should be as a function of n and given using (tight) big-O notation (i.e. assume n is very large). *Solution: The homes x such that x is prime had their bells rung exactly once. Thus, by the prime number theorem, the answer is $O(n/\ln n)$*

(b) (6 points) For those homes that had their doorbell rung more than once, when were they first woken up? I.e. on what circling of the neighborhood was their doorbell first rung by the mathematician? Again express your answer with big-O notation as a function of n. *Solution: If the doorbell was rung more than once for a home x, then x is composite. Thus as we showed in class, at least one divisor of x must be no more than $\sqrt{x}$. Since $x \leq n$, the answer is $O(\sqrt{n})$.*

(c) (10 points) What is the total number of times that the mathematician rang a doorbell? Again use big-O notation. Hint: You may find a result you showed in hw4 useful. *Solution: The total number of times that a doorbell was rung is no more than $\sum_{i=2}^{n} n/i = n\sum_{i=2}^{n} 1/i$ which is $O(n \lg n)$ via an integral upperbound as done in hw4 problem 3*

4. **Number Tricks**

(a) (8 points) Consider the following magic "trick". Think of any number n, now compute n^4, divide n^4 by 5 and let r be the remainder. Using my magical powers I can guess that the number r is either 0 or 1. Explain why this trick works by proving that r will always be either 0 or 1. Hint: You will find a theorem discussed in class useful. *Solution: If* 5 *divides* n *then* $n = 5k$ *for some integer* k *and* $n^4 = 5^4k^4$. *Thus,* 5 *divides* n^4. *If* 5 *does not divide* n, *then* **Fermat's Little Theorem** *tells us that* $n^4 \bmod 5$ *is* 1. *Thus, the remainder when we divide* n^4 *by* 5 *is either* 0 *or* 1.

(b) (12 points) Consider the following magic trick. You think of any number. You tell me what the remainder is when you divide your number by 4. You tell me the remainder when you divide your number by 25. Using my magical powers, I then tell you the last two digits of your number. Describe the algorithm I use to perform this trick and why it works. Hint: You will find (another) important theorem discussed in class useful. *Solution:* 25 *and* 4 *are relatively prime (you can verify this by computing* $gcd(25, 4)$ *or just realizing that the factoring of* $25 = 5^2$, $4 = 2^2$ *and so they share no common factors. Thus we can use the* **Chinese Remainder Theorem** *to determine* $n \bmod (25 * 4)$ *whenever we know both* $n \bmod 25$ *and* $n \bmod 4$. *Finally, note that* $n \bmod 100$ *is just the last two digits of* n. *Note this trick would not work if we used the numbers* 50 *and* 2 *for example since they are not relatively prime! Now here is the algorithm for this trick. Let* $r_1 = n \bmod 25$ *and* $r_2 = n \bmod 4$. *Then* $m_1 = 25$, $m_2 = 4$, $M_1 = 4$, $M_2 = 25$, $y_1 = 4^{-1} \bmod 25 = 19$ *and* $y_2 = 25^{-1} \bmod 4 = 1$. *Thus the magician calculates:* $x = r_1 * 4 * 19 + r_2 * 25 * 1 \bmod 100$ *which is* $(76r_1 + 25r_2) \bmod 100$. *Try this out for several values of* r_1 *and* r_2 *and marvel at the mathematical magic!*

5. **Public Key Cryptography**

Imagine Bob wants to send a message to Sue such that 1) only Sue can read the message; and 2) Sue can verify that Bob is the person who sent the message. In this problem, you will show how to do this with RSA cryptography, even when all communication is by broadcast. To solve this problem, you will need two pairs of public and private keys. For consistency of notation, please let p_1, q_1, d_1 be the first set of private keys and n_1, e_1 be the first set of public keys (where the public and private keys are constructed as discussed in class). Similarly, let p_2, q_2, d_2 be the second set of private keys and n_2, e_2 be the second set of public keys. Also let $f_1(x) = x^{e_1} \bmod n_1$ and $g_1(x) = x^{d_1} \bmod n_1$. And similarly, let $f_2(x) = x^{e_2} \bmod n_2$ and $g_2(x) = x^{d_2} \bmod n_2$. Finally let m be the message that Bob wants to send to Sue.

This problem can be done in two rounds. In the first round, the following happens:

Bob generates p_1, q_1, d_1, n_1, e_1 and broadcasts n_1, e_1.
Sue generates p_2, q_2, d_2, n_2, e_2 and broadcasts n_2, e_2.

You will now determine what happens in the second round, *using the above notation. Note: You must use the above notation to receive credit for this problem.*

(a) (7 points) What does Bob broadcast? *Solution: Let $s = g_1(m)$ (s is the signature for m). Then Bob broadcasts $m' = f_2(\text{“}ms\text{”})$*

(b) (7 points) What does Sue compute in order to decrypt and verify Bob's message? *Solution: Sue computes $g_2(m'))$ in order to retrieve the message “m s”. She then computes $f_1(s)$ and verifies that it equals m.*

(c) (6 points) Describe briefly (2-3 sentences) why this scheme allows Sue to decrypt the message and verify that it came from Bob. *Solution: As shown in class, g_2 is the inverse of f_2 so $g_2(f_2(x)) = x$. This shows that Sue can decrypt Bob's message to get “m s”. Similarly, f_1 is the inverse of g_1 so $f_1(s)$ will equal m.*