University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISCI-521: Discrete Math with Applications

Spring 2019

Midterm Exam

Name: _____ ID #: _____ Score: _____

- This is a OPEN BOOK & OPEN NOTE exam. Also, you cannot access the Internet or use your laptop computer. Do the exam independently.
- There are a total of 100 points in the exam. Plan your work accordingly.
- Write out the steps for all problems to receive the full credit. Use additional pages if necessary.
- Date: April 11, 2019.
- Location: Lecture center 3B.
- Time: 2:45 pm - 5:35 pm.

Problem	Points	Scores
Problem 1: True or False	20	
Problem 2: Logical Equivalence	10	
Problem 3: Algorithm and Complexity	10	
Problem 4: Euclidean algorithm	10	
Problem 5: Integer Representations and Modular Exponentiation	10	
Problem 6: Induction and Recursion	10	
Problem 7: Counting and Probability	15	
Problem 8: Relations	15	

Problem 1: True or False (20 points)

(1) The expression $\forall x \exists y \exists z P(x, y, z, c)$ is a well-formed formula.

◦ True ◦ False

(2) The time complexity of a recursive algorithm may depend critically on the number of recursive calls it makes.

◦ True ◦ False

(3) Let $f : Z \to Z$ be defined by $f(x) = 5x^3 - x$. Then the function $f(x)$ is an one-to-one (injective) and onto (surjective) function.

◦ True ◦ False

(4) Greedy algorithm can guarantee the smallest number of coins in the coin exchange optimization problem.

◦ True ◦ False

(5) The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $gcd(a_i, a_j) = 1$ when $1 \leq i < j \leq n$.

◦ True ◦ False

(6) Both the sender and the receiver share the same private key in the RSA cryptosystem.

◦ True ◦ False

(7) In the intersection of k sets, if we assume that there are k positions being fixed, then |the intersection of k sets| $= (n - k)!$

◦ True ◦ False

(8) Two random variables x and y are said to be independent, if and only if $E[f(x)g(x)] = E[f(x)]E[g(x)]$.

◦ True ◦ False

(9) The time complexity of the Fast Integer Multiplication Algorithm is $O(nlogn)$.

◦ True ◦ False

(10) The relation R on a set A is transitive if and only if $R^n \subseteq R$ for all positive integers n.

◦ True ◦ False

Problem 2: Logical Equivalence (10 points)

Show that $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$ is a tautology.

(1) [**5 points**] By constructing truth table.

(2) [**5 points**] By applying the known logical equivalence laws.

Problem 3: Algorithm and Complexity (10 points)

(1) **[3 points]** State the definition of the fact that $f(n)$ is $O(g(n))$, where $f(n)$ and $g(n)$ are functions from the set of positive integers to the set of real numbers.

(2) **[7 points]** Use the definition of the fact that $f(n)$ is $O(g(n))$ directly to prove the complexity for the binary search algorithm is $O(logn)$.

Problem 4: Euclidean algorithm (10 points)

(1) **[5 points]** How many divisions are required to find $gcd(144, 233)$ using the Euclidean algorithm?

(2) **[5 points]** Find $gcd(2n+1, 3n+2)$, where n is a positive integer. [Hint: Use the Euclidean algorithm.]

Problem 5: Integer Representations and Modular Exponentiation (10 points)

(1) **[3 points]** Convert 43 to binary, octal and hexadecimal representations.

(2) **[7 points]** Use Modular Exponention Algorithm to find 11^{43} mod 9.

Problem 6: Induction and Recursion (10 points)

(1) **[6 points]** Use mathematical induction to show that

$$\frac{1}{1\times 4}+\frac{1}{4\times 7}+\ldots+\frac{1}{(3n-2)\times(3n+1)}=\frac{n}{3n+1} \tag{1}$$

whenever n is a positive integer.

(2) **[4 points]** Give a recursive definition of the set of positive integers congruent to 2 modulo 3.

Problem 7: Counting and Probability (15 points)

(1) **[5 points]** Show that if there are 30 students in a class, then at least two have last names that begin with the same letter.

(2) **[5 points]** We say a bit string is unbalanced if there are more ones than zeroes or more zeros than ones. How many 10-bit strings are unbalanced?

(3) **[5 points]** Show that if E_1 , E_2 , ..., E_n are events from a finite sample space, then $p(E_1 \cup E_2 \cup \ldots \cup E_n) \leq p(E_1) + p(E_2) + \ldots + p(E_n)$. This is known as **Boole's inequality**.

Problem 8: Relations (15 points)

(1) **[6 points]** Show that the relation R on $Z \times Z$ defined by $(a, b)R(c, d)$ if and only if $a + d = b + c$ is an equivalence relation.

(2) **[4 points]** What is the equivalence class of $(1, 2)$ with respect to the equivalence relation in (1)?

(3) **[5 points]** Give an interpretation of the equivalence classes for the equivalence relation R in (1). [Hint: Look at the difference $a - b$ corresponding to (a, b).]