University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISEN/ISCI-210: Discrete Structures

Fall 2018

Midterm Exam 2

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: Nov 14th, 2018.
- Location: Lecture center hall 25.
- Time: 9:20 am - 10:20 am (can be extended to 10:35 am).

Problem	Points	Scores
Problem 1: True or False	20	
Problem 2: Algorithm and Complexity	15	
Problem 3: Integer Representations and Modular Arithmetic	20	
Problem 4: Induction and Recursion	20	
Problem 5: Counting	25	

Problem 1: True or False (20 points)

(1) If $a \equiv b (\text{mod } m)$ holds then $c \cdot a \equiv c \cdot b (\text{mod } m)$ holds, where c is any integer.

○ True ○ False

(2) If $a \equiv b (\text{mod } m)$ holds then $c \div a \equiv c \div b (\text{mod } m)$ holds, where c is any integer.

○ True ○ False

(3) 111 is prime.

○ True ○ False

(4) Any common divisor of a and b is also a common divisor of b and r, where $a - bq = r$.

○ True ○ False

(5) In RSA cryptosystem, both the sender and the receiver share the private key.

○ True ○ False

(6) Every nonempty set of nonnegative integers has a least element.

○ True ○ False

(7) Recursive algorithms consume less space and more efficient than the corresponding iterative algorithms.

○ True ○ False

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

○ True ○ False

(9) The sum rule works, *i.e.*, $|A \cup B| = |A| + |B|$, for any tow sets A and B.

○ True ○ False

(10) Number of ways to choose k items from n items equals number of ways to choose $n - k$ items from n items.

○ True ○ False

Problem 2: Algorithm and Complexity (15 points)

(1) [**6 points**] Define the statement $f(x, y)$ is $O(g(x, y))$, $\Omega(g(x, y))$ and $\Theta(g(x, y))$, respectively.

(2) [**4 points**] Show that $(nlogn + n^2)^3$ is $O(n^6)$.

(3) [**5 points**] Suppose that $f(x)$ is $O(g(x))$ where f and g are increasing and unbounded functions. Show that $\log|f(x)|$ is $O(\log|g(x)|)$.

Problem 3: Integer Representations and Modular Arithmetic (20 points)

(1) [**3 points**] Convert a decimal expansion 121 to its binary expansion, octal expansion and hexadecimal expansion.

(2) [**4 points**] Convert $(101101111011)_2$ from its binary expansion to its octal expansion and hexadecimal expansion.

(3) [**5 points**] $(19^3 \text{ mod } 23)^2 \text{ mod } 31$.

(3) [**8 points**] Use Modular Exponention Algorithm to find $13^{43} \text{ mod } 11$.

Problem 4: Induction and Recursion (20 points)

(1) [**8 points**] Use mathematic induction to prove that $1{\cdot}1!+2{\cdot}2!+\ldots+n{\cdot}n! = (n+1)!-1$ whenever n is a positive integer.

(2) Let S be the subset of the set of ordered pairs of integers defined recursively by

Basis step: $(0,0) \in S$.

Recursive step: If $(a,b) \in S$, then $(a,b+1) \in S$, $(a+1,b+1) \in S$ and $(a+2,b+1) \in S$.

(a) [**4 points**] List the elements of S produced by the first five applications of the recursive definition.

(b) [**8 points**] Show that $a \leq 2b$ when $(a,b) \in S$. [**Hint**: *you can use strong induction or structural induction*]

Problem 5: Counting (25 points)

(1) [**10 points**] How many bit strings of length 8 either begin with three 0s or end with two 0s?

(2) [**10 points**] Use pigeohole principle to show that if five integers are selected from the first eight positive integers, there must be a pair of these integers with a sum equal to 9.

(3) [**5 points**] Prove that if n and k are integers with $1 \leq k \leq n$, then

$$k\binom{n}{k} = n\binom{n-1}{k-1}$$

.