CS1800 Discrete Structures Final

Instructions:

1. The exam is closed book and closed notes. You may not use a calculator or any other electronic device.

2. The exam is worth 100 total points. The points for each problem are given in the problem statement and in the table below.

3. You should write your answers in the space provided; use the back sides of these sheets, if necessary.

4. You have two hours to complete the exam.

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1 [ 9 points]</td>
<td>Binary and Hex</td>
<td></td>
</tr>
<tr>
<td>Section 2 [ 8 points]</td>
<td>Logic and Circuits</td>
<td></td>
</tr>
<tr>
<td>Section 3 [12 points]</td>
<td>Modular Arithmetic</td>
<td></td>
</tr>
<tr>
<td>Section 4 [ 8 points]</td>
<td>Modular Cryptosystems</td>
<td></td>
</tr>
<tr>
<td>Section 5 [11 points]</td>
<td>Sets</td>
<td></td>
</tr>
<tr>
<td>Section 6 [12 points]</td>
<td>Counting</td>
<td></td>
</tr>
<tr>
<td>Section 7 [14 points]</td>
<td>Probability</td>
<td></td>
</tr>
<tr>
<td>Section 8 [14 points]</td>
<td>Recurrences, Induction, Big-O</td>
<td></td>
</tr>
<tr>
<td>Section 9 [12 points]</td>
<td>Algorithms and Graphs</td>
<td></td>
</tr>
</tbody>
</table>

Total

Name: _____________________  Instructor: _____________________
Section 1 [9 pts. (2,3,2,2)]: Binary and Hex

1. Suppose we write the number 10! (ten factorial) in binary. How many consecutive zeros will occur on its right-hand-side?

2. Convert (33222111)\textsubscript{4} from base 4 to base 16. Each group of 2 base 4 digits is then replaced with a single hex digit that has the same value: 3 | F | A | 9 | 5. So the hex number is (3FA95)\textsubscript{16}.

3. (a) Using 8-bit two’s complement arithmetic, add the numbers (0110 1101)\textsubscript{2} and (0110 0111)\textsubscript{2}.

(b) Convert your result to decimal.
Section 2 [8 pts. (3,2,3)]: Logic and Circuits

1. Write a logic expression with the variables $p$, $q$, and $r$ that is true exactly when $p = q$ and $q \neq r$. Your answer should be in disjunctive normal form, with two clauses.

2. (a) Write the logic expression corresponding to the circuit below (do not simplify).

(b) Simplify your expression.
Section 3 [12 pts. (3,3,3,3)]: Modular Arithmetic

1. What is the ones digit of \(7^{2222}\)?

2. (a) Use the Extended Euclidean Algorithm to find the multiplicative inverse of 47 mod 49.

(b) Solve the equation \(47x = 3 \mod 49\). Express your result as an integer in the range \(0 \leq x < 49\).

3. Find \(\gcd(a, b)\) and \(\text{lcm}(a, b)\) where \(a = 750,000\) and \(b = 36,000\).
Section 4 [8 pts. (6,2)]: Modular Cryptosystems

1. Given the RSA public key \((e, n) = (13, 85)\), you intercept the cipher text \(y = 3\). Decrypt this message.

2. RSA is supposed to be a secure encryption method, yet you just decrypted a message for which you only knew the public encryption key. How could the persons responsible for encryption make their system harder to crack?
Section 5 [11 pts. (3,1,6)]: Sets

1. As universe, we consider the set of all students enrolled at Northeastern. Let $A$ be the set of commuting students, let $B$ be the set of freshmen, let $C$ be the set of sophomores and let $D$ be the set of students who have been invited to the end-of-semester party. Using only parentheses, the letters $A, B, C, D$, and the symbols for union, intersection, complement (but not set-difference), and set inclusion ($\subseteq$), write a statement expressing that “All freshmen and all non-commuting sophomores have been invited to the party.”

2. Let $S_n = \{x \in \mathbb{R} \mid 0 < x < \frac{1}{n}\}$ for all $n > 0$.
   
   (a) What is $S_1 \cup S_2 \cup S_3 \cup S_4$ ?

   (b) What is $S_1 \cap S_2 \cap S_3 \cap S_4$ ?

3. Shade the indicated regions of the following Venn diagrams.
Section 6 [12 pts. (4 each)]: Counting
Exact answers are expected for this section. Simplify to natural numbers instead of formulas.

1. The Leahys are going to attend a picnic, and want to prepare a variety of sandwiches to bring to share. Each sandwich must have exactly one of turkey, ham, or tofu as a base (3 options), and then each ingredient of lettuce, tomato, pickles, and capers (4 options) is completely optional, and a sandwich could have all, none, or some subset of those four ingredients. How many sandwiches are possible?

2. The Leahys would also like to bring exactly 3 board games. Each game in their collection supports a different number of players; they have 10 games in all, but only three games can support six players. How many possible different collections of 3 games can they bring if they want to bring at least one that supports six players?

3. Finally, the Leahys would like to purchase and bring some soft drinks (soda). They’ve decided 4 bottles is a good number to bring, and their local convenience store sells 8 varieties. How many different options do they have for purchasing 4 bottles? (Bottles of the same variety are not considered different; one option would be “two bottles of Coke and two bottles of Sprite.”)
Section 7 [14 pts. (3,3,4,4)]: Probability

As in the preceding section, you don’t need to simplify.

1. What is the probability of rolling a six on at least one die when rolling four six-sided dice?

2. What is the expected number of sixes when rolling four six-sided dice? (Hint: Use linearity of expectation.)

3. When rolling two six-sided dice, are rolling at least one six and rolling at least one four independent events? Show a calculation that supports your answer.

4. A board game player rolls two six-sided dice secretly and smiles. You estimate there is a 50% chance the player would smile if the sum of the dice is at least 10, and a 20% chance the player would smile with a roll of less than 10. Use Bayes’ Theorem to calculate \( \Pr[\text{rolled at least 10} \mid \text{smile}] \).
Section 8 [14 pts. (2,6,6)]: Recurrences, Induction, Big-O

1. Circle the recursive function that grows the fastest (consider using the back of the exam for scratch if you need it):

   \[ T(n) = 2T(n/2) + n \]
   \[ T(n) = 2T(n - 1) + 1 \]
   \[ T(n) = T(n/2) + 1 \]

2. Prove by induction: any amount of postage \( n \geq 8 \) can be achieved using 3 and 4 cent stamps.

3. For each pair of functions \( f(n) \) and \( g(n) \), put a check mark into each box that corresponds to a relation that holds between the functions.

\[
\begin{array}{|c|c|c|c|c|}
\hline
f(n) & g(n) & f(n) = O(g(n)) & f(n) = \Theta(g(n)) & f(n) = \Omega(g(n)) \\
\hline
5n & 100n & & & \\
\hline
\log_2 n & 2^n & & & \\
\hline
n^2 & n & & & \\
\hline
n \log_2 n & n^2 & & & \\
\hline
\log_2 n & \log_3 n & & & \\
\hline
\end{array}
\]
Section 9 [12 pts (4,4,4)]: Algorithms and Graphs

1. Circle each algorithm for which it is true that the best-case running time as a function of \( n \) is not asymptotically different from the worst-case running time (they are big-\( \Theta \) of each other).

- Insertion Sort
- Selection Sort
- Binary Search
- Mergesort

2. Consider the following pseudocode ("=" is an assignment operator):

\[
\begin{align*}
\text{counter} & := 0 \\
\text{for } p:=1 \text{ to } N \text{ do} \\
& \quad \text{for } q:=p \text{ to } N \text{ do} \\
& \quad \quad \text{counter} := \text{counter} + 1 \\
\text{return } \text{counter}
\end{align*}
\]

After the end of the outer for loop, what is the final value of the \( \text{counter} \) variable, in terms of \( N \)? (Do not leave this as a sum, and give an exact formula.)

3. If every vertex of a graph has even degree, then there is a path that travels over every edge exactly once and ends where it started (called an “Eulerian circuit”). Consider the following pseudocode that determines whether a graph has an Eulerian circuit:

\[
\begin{align*}
\text{for each vertex } v \text{ do} \\
& \quad \text{count the number of neighbors of } v \\
& \quad \text{if the number of neighbors was odd then return FALSE} \\
\text{return TRUE}
\end{align*}
\]

If the graph is represented in adjacency matrix form, give the asymptotic worst-case running time of this algorithm in terms of the number of vertices \( |V| \) and/or the number of edges \( |E| \).