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</td>
<td>Binary and Hex</td>
<td>10</td>
</tr>
<tr>
<td>Section 2</td>
<td>Logic and Circuits</td>
<td>10</td>
</tr>
<tr>
<td>Section 3</td>
<td>Modular Arithmetic and Prime Factors</td>
<td>12</td>
</tr>
<tr>
<td>Section 4</td>
<td>Cryptosystems</td>
<td>10</td>
</tr>
<tr>
<td>Section 5</td>
<td>Sets</td>
<td>10</td>
</tr>
<tr>
<td>Section 6</td>
<td>Counting</td>
<td>14</td>
</tr>
<tr>
<td>Section 7</td>
<td>Probability</td>
<td>10</td>
</tr>
<tr>
<td>Section 8</td>
<td>Induction, Recurrences, Big-O</td>
<td>14</td>
</tr>
<tr>
<td>Section 9</td>
<td>Algorithms and Graphs</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section 1 [10 pts. (4,3,3)]: Binary and Hex

1. Write the base 10 number 42 in (a) binary, (b) hex.
   **Sol:** (a) 101010 (b) 2A

2. Write the decimal number -10 in 8-bit two’s complement.
   **Sol:** 11110110

3. What is the result (in hex) of multiplying the hex number FFFF by the hex number 10?
   **Sol:** FFFF0
1. Write a logical formula involving the variables $x_1, x_2, x_3$, and $y$ that evaluates to true if and only if $y$ is true but at least one of the $x_i$ variables is false. Use only the operators $\lor, \land$, and $\neg$, and use parentheses as necessary to avoid ambiguity.
   \[ \text{Sol: } y \land (\neg x_1 \lor \neg x_2 \lor \neg x_3) \]

2. Simplify the logical expression $(x \land y) \lor (x \land \neg y) \lor (x \land z)$.
   \[ \text{Sol: } x \]

3. Draw a logical circuit that computes a logical AND of inputs $x$ and $y$ without using any AND gates. Use only OR and NOT gates instead. (Solutions that use more gates than the solution suggested by de Morgan’s Law may not receive full credit.)
   \[ \text{Sol: } \text{TODO} \]
1. Find $5^{10} \mod 7$ using repeated squaring. Show your work.
   **Sol:**
   \[
   5^2 \mod 7 = 25 \mod 7 = 4 \\
   5^4 \mod 7 = 4^2 \mod 7 = 16 \mod 7 = 2 \\
   5^8 \mod 7 = 2^2 \mod 7 = 4 \\
   5^{12} \mod 7 = 5^8 \mod 7 \times 5^4 \mod 7 = 4 \times 4 \mod 7 = 2
   \]

2. Find the multiplicative inverse of 12 mod 91.
   **Sol:**
   \[
   \text{gcd}(91,12) = \text{gcd}(12, 7) = \text{gcd}(7,5) = \text{gcd}(5,2) = \text{gcd}(2,1) = 1 \\
   2 \times 0 + 1 \times 1 = 1 \\
   5 \times 1 + 2 \times -2 = 1 \\
   7 \times -2 + 5 \times 3 = 1 \\
   12 \times 3 + 7 \times -5 = 1 \\
   91 \times -5 + 12 \times 38 = 1
   \]

3. Determine whether 123452 and 12345 are relatively prime. Show your work. (Hint: Factorization is probably too slow.)
   **Sol:** Yes, by Euclid’s algorithm: 123452 mod 12345 = 2, and 12345 and 2 share no factors because 12345 is odd.
Section 4 [10 pts. (3,4,3)]: Cryptosystems

1. What is wrong with the linear cipher \( y = 13x + 1 \mod 26 \)?
   Sol: 13 is not relatively prime to 26, so there will be values that don’t have unique decryptions.

2. If an RSA public key is \( e = 256, n = 1025 \), how many multiplications must take place to encrypt a message, assuming you use an efficient algorithm for exponentiation?
   Sol: 8

3. In choosing a public key \( e \) for a particular \( n = pq \), what number must \( e \) be relatively prime to, in terms of \( n \) and/or \( p \) and \( q \)?
   Sol: \( \phi(n) = (p - 1)(q - 1) \)
Section 5 [10 pts. (3,4,3)]: Sets

1. If $A$, $B$, and $C$ are sets that have nonempty intersections with each other, draw a Venn diagram that shades the result of $A - (B \cup C)$.
   \textbf{Sol:} TODO

2. If $A = \{a, b, c\}$, what is $|A \times P(A)|$?
   \textbf{Sol:} $2^3 \times 3 = 24$

3. If $P = \{x : x \text{ is prime}\}$, $S = \{y : y = 7n \text{ for some } n \in \mathbb{N}\}$, and $T = \{z : z = 3n \text{ for some } n \in \mathbb{N}\}$, describe in terms of sets $P, S, \text{ and } T$ (and union, intersection, and complement) the set containing all multiples of 21 and all prime numbers besides 3.
   \textbf{Sol:} $(S \cap T) \cup (P \cap \overline{T})$
Section 6 [14 pts. (2,2,2,3,5)]: Counting

Consider the following password-like procedures for unlocking a smartphone, and determine how many different passwords (or pass-gestures) are possible under each scheme. You don’t need to simplify your answer.

1. A four-digit PIN consisting of digits from the range 0-9. PINs consisting of 4 consecutive digits (such as 1234 and 0123, but not 2468) or 4 identical digits (7777) are not allowed.
   **Sol:** $10000 - 7 - 10 = 9983$

2. A swipe that hits four points among nine possible points arranged around the screen. No point can be repeated. (The locations of the points don’t matter.)
   **Sol:** $P(9,4) = 9*8*7*6$

3. A scheme where the user must touch 4 points among 9 in any order to unlock the phone.
   **Sol:** $C(9,4) = 9*8*7*6/4*3*2*1$

4. An eight character password, made from 26 uppercase characters, 10 digits, and 12 special characters, that uses at least one special character or digit.
   **Sol:** $48^8 - 26^8$

5. A sequence of emoticons that consists of 2 different emoticons, chosen from 100 possibilities, that are pressed a total of 12 times (with identical emoticons not necessarily consecutive). Sequences that just contain one kind of emoticon aren’t allowed.
   **Sol:** $C(100,2) * (2^{12} - 2)$
Section 7 [10 pts. (3,4,3)]: Probability

You can leave your answers unsimplified in this section as well.

1. What is the probability that, when rolling two six-sided dice, the two dice show different results from each other? (I.e., the roll is not “doubles”?)

   **Sol:** Six ways to get doubles, so $\Pr(\text{Doubles}) = 6/36 \implies \Pr(\neg \text{Doubles}) = 1 - 6/36 = 5/6$

2. In a 44 student class with 20 males and 24 females, three are chosen at random (without replacement) to lead discussion groups. What is the probability that all three students are the same gender as each other?

   **Sol:** All males: $\binom{20}{3}/\binom{44}{3}$
   All females: $\binom{24}{3}/\binom{44}{3}$
   Either: $(\binom{20}{3} + \binom{24}{3})/\binom{44}{3}$

3. What is the expected number of females picked in the preceding question? (Hint: You can use linearity of expectation here.)

   **Sol:** $24/44 \times 3 = 6/11 \times 3 = 18/11$
Section 8 [14 pts. (7,3,4)]: Induction, Recurrences, Big-O

1. Prove by induction that, in the following sequence, \( a_n < 2^n \) for all \( n \geq 1 \): \( a_1 = 1 \), \( a_2 = 2 \), \( a_3 = 3 \), \( a_n = a_{n-1} + a_{n-2} + a_{n-3} \).

**Sol:** Base cases:
- \( n = 1 : 1 < 2^1 \)
- \( n = 2 : 2 < 2^2 = 4 \)
- \( n = 3 : 3 < 2^3 = 8 \)

Assume the formula is true for \( 1 \leq n \leq k \). Proof that this implies its truth for \( n = k + 1 \):

Using the inductive hypothesis to substitute the formula into the formula for \( a_{k+1} \), we get

\[
a_{k+1} = a_k + a_{k-1} + a_{k-2} < 2^k + 2^{k-1} + 2^{k-2} + \ldots + 2^0 = 2^{k+1} - 1
\]

since a binary number with all 1’s is 1 less than the next power of two after its largest digit. So \( a_{k+1} < 2^{k+1} \) and this proves the formula for \( n = k + 1 \).

2. Give the asymptotic (big-Theta) running time of an algorithm described by the time recurrence \( T(N) = 3T(n - 1) + 1 \).

**Sol:** \( \Theta(3^N) \)

3. Order the following functions from slowest growing to fastest growing (in terms of big-O): \( n^2 \), \( 10n \), \( 1.01^n \), \( n \log_2 n \).

**Sol:** \( 10n, n \log_2 n, n^2, 1.01^n \)
Section 9 [10 pts (3, 3, 4)]: Algorithms and Graphs

1. Which is guaranteed to produce a shortest path - breadth-first search, depth-first search, both, or neither?
   Sol: Breadth-first search

2. Among Insertion Sort, Selection Sort, and Mergesort, (a) which has the best worst-case running time, and (b) which has the best best-case running time?
   Sol: (a) Mergesort (b) Insertion Sort

3. A Hamiltonian Cycle is a cycle that repeats no vertices and hits every vertex in the graph. Does a graph with a Hamiltonian Cycle always have a spanning tree? If so, explain how to produce such a tree, given a Hamiltonian Cycle. If not, draw a counterexample graph where a Hamiltonian Cycle exists, but no spanning tree exists.
   Sol: Yes - dropping any edge from the Hamiltonian Cycle produces a spanning tree.