CS1800 Discrete Structures Midterm

Version B

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, Octal, and Hexadecimal</td>
<td>14</td>
</tr>
<tr>
<td>Section 2</td>
<td>Logic</td>
<td>12</td>
</tr>
<tr>
<td>Section 3</td>
<td>Modular Arithmetic &amp; Algorithms</td>
<td>14</td>
</tr>
<tr>
<td>Section 4</td>
<td>Modular Cryptosystems</td>
<td>12</td>
</tr>
<tr>
<td>Section 5</td>
<td>Sets</td>
<td>6</td>
</tr>
<tr>
<td>Section 6</td>
<td>Counting</td>
<td>12</td>
</tr>
<tr>
<td>Section 7</td>
<td>Permutations and Combinations</td>
<td>15</td>
</tr>
<tr>
<td>Section 8</td>
<td>Proofs</td>
<td>15</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

Name: ___________________________ NU ID#: ___________________________
Instructor: ___________________________
Section 1 [14 pts (6, 3, 2, 3)]: Binary, Octal, and Hexadecimal

1. Convert the base 2 number 101011 to (a) decimal, (b) hexadecimal, (c) octal (base 8).

2. Find the 8-bit two’s complement representation of −37.

3. Assuming we are using an 8-bit two’s complement representation, name the smallest positive value that would produce overflow when added to the number 4.

4. Suppose we add the decimal numbers 119 and 13 using 8-bit two’s complement arithmetic. What is the result (expressed in decimal notation)?
Section 2 [12 pts (4, 4, 4)]: Logic

1. Simplify the expression \((a \land b) \lor (a \land (\neg b \lor \neg a))\)

2. Draw a logical circuit with three inputs that evaluates to true exactly when at least two of its three inputs are true.

3. Rewrite the expression \(a \land b \land c\) using only \(\lor\) (OR) and \(\neg\) (NOT) operators instead of \(\land\) (AND).
Section 3 [14 pts (5,3,3,3)]: Modular Arithmetic and Algorithms

1. (a) Use fast exponentiation (repeated squaring) to compute $4^{16} \mod 11$.

   (b) Use your work from the previous problem to compute $4^{22} \mod 11$.

2. Find the GCD of 8100 and 1800, using whatever method you prefer.

3. Use Euclid’s algorithm to find gcd(253, 175). Show all steps.

4. How many integers between 1 and 128 are relatively prime to 128?
Section 4 [12 pts (5, 4, 3)]: Modular Cryptosystems

1. Find coefficients $a$ and $b$ for the decryption function $x = ay + b \mod 26$ of the linear cipher $y = 5x + 15 \mod 26$.

2. Suppose that the RSA public key $(7, 33)$ has been used to produce ciphertext “2”.
   - (a) What is the private key?

   (b) Decrypt the message.
Section 5 \[6 \text{ pts } (2,2,2)\]: Sets

If our universe is the integers $\mathbb{Z}$, and $O$ represents all odd integers, and $S$ represents the set of integers divisible by 7, describe the following sets using union, intersection, and complement.

1. The set of all odd integers divisible by 7.

2. The set of all even integers.

3. The set of all integers that are even or divisible by 7.
Section 6 [12 pts (4, 4, 4)]: Counting

For this section and the next, you can leave your answer unsimplified, but at least give the numbers to multiply.

1. A movie theater has three showtimes this Saturday: morning, afternoon, and evening and 20 movies to choose from.
   
   (a) In how many ways can it select a different movie for each time slot?
   
   (b) In how many ways can it select a movie for each time slot, possibly with repetition, so that not all movies are the same?

2. Suppose that the movie theater sold 700 tickets last Saturday. How many people, at least, attended the most popular of the three shows?
Section 7 [15 pts (3, 3, 4, 5)]: Permutations and Combinations

In this section as well, you need not multiply out your answer.

In a certain country, license plates consist of three vowels (from A, E, I, O, U) and three digits (from 0, 1, ..., 9).

1. How many license plates are possible if the three vowels must precede the three digits and repetitions are allowed? For example, AAU577 is a valid license plate but A5AU77 is not.

2. How many license plates are possible if the three vowels must precede the three digits and repetitions are not allowed? For example, AEU579 is a valid license plate but A5EU79 is not.

3. How many license plates are possible if the three vowels may be anywhere and repetitions are allowed? For example, 57A7AU is a valid license plate.

4. How many license plates are possible if the three vowels may be anywhere and repetitions aren’t allowed? For example, 57A9EU is a valid license plate.
Section 8 [15 pts (7,8)]: Proofs

1. Prove that if $p$ divides $n$, then $\phi(n) \leq (n - n/p)$. Do not use any formulas for $\phi(n)$.

2. Prove that for all odd $n$, the sum of $\binom{n}{i}$ for $0 \leq i \leq n/2$ is $2^{n-1}$. 