CS1800 Discrete Structures Final  
Version A

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. *SHOW YOUR WORK FOR ALL PROBLEMS.*

5. 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>11 points</td>
<td>Binary and Other Bases</td>
</tr>
<tr>
<td>Section 2</td>
<td>12 points</td>
<td>Logic and Circuits</td>
</tr>
<tr>
<td>Section 3</td>
<td>12 points</td>
<td>Modular Arithmetic and Algorithms</td>
</tr>
<tr>
<td>Section 4</td>
<td>10 points</td>
<td>Sets and Set Operations</td>
</tr>
<tr>
<td>Section 5</td>
<td>10 points</td>
<td>Counting</td>
</tr>
<tr>
<td>Section 6</td>
<td>14 points</td>
<td>Probability</td>
</tr>
<tr>
<td>Section 7</td>
<td>15 points</td>
<td>Algorithms, Recurrences, Growth of Functions</td>
</tr>
<tr>
<td>Section 8</td>
<td>16 points</td>
<td>Proofs</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Section 1 [11 pts (3,4,4) ]: Binary and Other Bases

1. Convert the number -17 to 8-bit two’s complement.
   **Sol:** 11101111

2. What is the result, in hexadecimal, of multiplying the hexadecimal number 0xABCD by the decimal number 256? **Hint:** You do not need to convert these numbers to a common base or actually perform the multiplication.
   **Sol:** 0xABCD00

3. Suppose that a given hexadecimal number has \(d\) total hex digits, of which exactly \(k\) are non-zero hex digits. What are the minimum and maximum number of 1s in the binary representation of this number and why?
   **Sol:** The minimum is \(k\) and the maximum is \(4k\), since a nonzero hex digit must have at least one bit in its binary representation and may have as many as all 4 (F).
Section 2 [12 pts (2,3,3,4)]: Logic and Circuits

A k-input parity gate is a logic gate whose output is 1 if and only if an odd number of its inputs is 1.

1. A 2-input parity gate is equivalent to what logic gate that we discussed in the course?
   Sol: XOR

2. Give the truth table for a 3-input parity gate.
   Sol: True rows are 001, 010, 100, 111.

3. Give a Boolean formula in DNF form for a 3-input parity gate.
   Sol: \((\neg a_1 \land \neg a_2 \land a_3) \lor (\neg a_1 \land a_2 \land \neg a_3) \lor (a_1 \land \neg a_2 \land \neg a_3) \lor (a_1 \land a_2 \land a_3)\)

4. Consider the 4-input circuit shown below. What function of the inputs \(a_1, a_2, a_3, a_4\) does this circuit compute and why?

   Sol: It computes a 4-input parity circuit. Exactly one of the two input gates needs to have odd parity for all the bits to have odd parity, since two inputs with odd parity or two inputs with even parity would both have even parity.
Section 3 [12 pts (4, 2, 3, 3)]: Modular Arithmetic and Algorithms

1. Calculate $7^{10}$ mod 11 using repeated squaring.
   
   **Sol:**
   
   $7^2 \mod 11 = 5, 7^4 \mod 11 = 5^2 \mod 11 = 3, 7^8 \mod 11 = 3^2 \mod 11 = 9, 7^{10} = 7^8 \cdot 7^2 \mod 11 = 9 \cdot 5 \mod 11 = 1$

2. The following are candidate RSA public/private key pairs. For each such pair, determine whether the pairs are valid RSA keys. If they are valid, state why; if they are not valid, state why not.

   (a) Public: $(e, n) = (7, 32)$. Private: $(d, n) = (5, 32)
   
   **Sol:** Invalid: 32 is not the product of two primes.

   (b) Public: $(e, n) = (7, 33)$. Private: $(d, n) = (4, 33)$
   
   **Sol:** Invalid: 4 is not the multiplicative inverse of 7 (mod 20), since $4 \cdot 7 = 28 = 8$ (mod 20). Or: 4 is not relatively prime to 20.

   (c) Public: $(e, n) = (7, 33)$. Private: $(d, n) = (3, 33)$
   
   **Sol:** Valid: 33 is the product of two primes, 3 and 11. $(3 - 1) \cdot (11 - 1) = 2 \cdot 10 = 20$. 7 is relatively prime to 20. 3 is the multiplicative inverse of 7 (mod 20), since $3 \cdot 7 = 21 = 1$ (mod 20).
Section 4 [10 pts (3,4,3)]: Sets and Set Operations

For the following problems, let $A = \{a, b, c\}, B = \{b, c, d\}, C = \{d, e, f, g\}$, with universe $U = \{a, b, c, d, e, f, g\}$.

1. Write out the set that results from the operations $(A \cup B) - C$.
   Sol: $\{a, b, c\}$

2. How many elements are in $\mathcal{P}(A \times B)$?
   Sol: $2^{3 \times 3} = 512$

3. If $D = \{x | x \in \mathbb{Z}, x^2 \leq 9\}$, what is $|D|$?
   Sol: $7 (\{-3, -2, -1, 0, 1, 2, 3\})$
Section 5 10 pts (5,5): Counting
For these problems, we expect your answers to be simplified into integers for full credit.

1. How many different undirected graphs are possible with the same set of 5 vertices \( V = \{A, B, C, D, E\} \), but different sets of edges \( E \)?
   Sol: \( C(5,2) = \frac{5\times4}{2} = 10 \) possible edges that could either be there or not, so \( 2^{10} = 1024 \) possible graphs.

2. A group of 9 people will be broken into 3 teams of 3, with each team assigned a letter A, B, or C. How many ways are there to do this?
   Sol: \( C(9,3)\times C(6,3) = \frac{9\times8\times7}{3\times2}(\frac{6\times5\times4}{3\times2}) = 1680. \)
Section 6 [14 pts (3.5,6)]: Probability

Give your probabilities and expectations as simplified fractions or integers.

1. When rolling four six-sided dice, what is the probability of rolling the same number on all six dice?
   \textbf{Sol:} 6 possible values among $6^4$ results $= 1/6^3 = 1/216$.

2. A set of tiles A,B,C,D,E,F is randomly shuffled. What is the probability that the tiles A,B,C are adjacent and in order in the resulting ordering?
   \textbf{Sol:} 4 places for ABC: A B C - - -, - A B C - -, - - A B C -, - - - A B C (0-3 leading tiles). The remaining slots have 3! possibilities. So the numerator of this probability is 4*6. The denominator is the number of ways to permute all the tiles, 6!. So the probability is $4 \times 6/6! = 1/5 \times 3 \times 2 = 1/30$.

3. A graph has 10 vertices, and we are independently putting each possible edge in E with probability 0.5. What is the expected number of cycles of length 3?
   \textbf{Sol:} For any particular cycle, $(1/2)^3 = 1/8$ probability that all three edges are present. There are $C(10,3) = 120$ possible cycles. So the expected number of cycles is $1/8 \times 120 = 15$. 


Section 7 [15 pts (4,4,3,4)]: Algorithms, Recurrences, Growth of Functions

1. Given the beginning of a sequence $a_1 = 2; a_2 = 9; a_3 = 22; a_4 = 41; a_5 = 66; a_6 = 97$, find the general closed-form formula.

   **Sol:** $3n^2 - 2n + 1$

2. Is the choice of constants $c = 2, n_0 = 100$ sufficient to prove $100n = O(n)$ by the definition of big-O, assuming these constants mean what they usually do? Explain why or why not.

   **Sol:** No, because $100(100) \leq 2(100)$ is not true, so the definition of big-O isn’t satisfied at $n_0$.

3. An algorithm for arrays works as follows:
   - it analyses each element of the input array (one pass)
   - then recurses (calls itself) on a chunk of at most three quarters of the array

   (a) Write the recursion for the running time.

   **Sol:** $T(N) = T(3N/4) + N$

(b) Given that the work done by the algorithm is $N + (3/4)N + (3/4)^2N + \ldots$ use an infinite geometric series to estimate the total number of operations as a function of $N$.

   **Sol:** $N * 1/(1 - 3/4) = 4N$
Section 8 [16 pts (7, 3, 6)]: Proofs

1. Prove that every undirected graph has an even number of vertices of odd degree.
   
   **Sol:** By the handshaking lemma, the sum of all the degrees of the graph is even. So the total degree sum must equal 0 mod 2. Each even degree vertex contributes 0 mod 2 to this sum, and each odd degree vertex contributes 1 mod 2 to this sum. An odd number of odd vertices would create a sum of 1 mod 2, which is impossible. So the number of odd degree vertices must be even.
2. A sequence is given by base $a_0 = 0$ and recurrence $a_{n+1} = -a_n + 1 + (-1)^n$ for $n \geq 0$

(a) Prove that $a_{n+2} = a_n + 2 * (-1)^{n+1}$ for $n \geq 0$.

**Sol:** Just by substituting twice in the original formula, we have

$a_{n+2} = -(a_n + 1 + (-1)^n) + 1 + (-1)^{n+1}$

$= a_n - 1 - (-1)^n + 1 + (-1)^{n+1}$

$= a_n - (-1)^n + (-1)^{n+1}$

$= a_n + (-1)^{n+1} + (-1)^{n+1}$

$= a_n + 2 * (-1)^{n+1}$

(b) Prove by induction that all values in the sequence are even.

**Sol:** Base cases: $a_0 = 0$ is even.

$a_1 = 0 + 1 + (-1)^0 = 2$ is even.

Inductive hypothesis: Suppose all $a_n$ are even for $n \leq k$.

Inductive step: By what was proven in the earlier part, $a_{k+1} = a_{k-1} + 2 * (-1)^{k+1}$. By the inductive hypothesis, $a_{k-1}$ is even. $2 * (-1)^{k+1}$ has a factor of 2, and therefore is also even, so the whole right side is even for $a_{k+1}$, and therefore, $a_{k+1}$ is even.