

Math 1350
Fall 2010
Exam 2

Name:

Directions:
Complete all eight questions.

Show your work. A correct answer without any scratch work or justification may not receive much credit.

You may not use any notes, calculators, or other electronic devices.
You have 75 minutes.

<i>A</i>	<i>B</i>	<i>C</i>	<i>D</i>	<i>E</i>	<i>F</i>	<i>G</i>	<i>H</i>	<i>I</i>	<i>J</i>	<i>K</i>	<i>L</i>	<i>M</i>
0	1	2	3	4	5	6	7	8	9	10	11	12
<i>N</i>	<i>O</i>	<i>P</i>	<i>Q</i>	<i>R</i>	<i>S</i>	<i>T</i>	<i>U</i>	<i>V</i>	<i>W</i>	<i>X</i>	<i>Y</i>	<i>Z</i>
13	14	15	16	17	18	19	20	21	22	23	24	25

Problem 1: _____ / 12

Problem 2: _____ / 13

Problem 3: _____ / 13

Problem 4: _____ / 12

Problem 5: _____ / 12

Problem 6: _____ / 13

Problem 7: _____ / 13

Problem 8: _____ / 12

Total: _____ / 100

1. Write 99 (base 10) in binary.

We compute $\frac{99}{2} = 49.5$, so $99 = 2 \times 49 + 1$, and the last digit is 1.

Next, $\frac{49}{2} = 24.5$, so $49 = 2 \times 24 + 1$, and the next last digit is 1.

Next, $\frac{24}{2} = 12$, so $24 = 2 \times 12 + 0$, and the third last digit is 0.

After this, $\frac{12}{2} = 6$, so $12 = 2 \times 6 + 0$, and the fourth last digit is 0.

$\frac{6}{2} = 3$ means that $6 = 2 \times 3 + 0$, and the fifth to last digit is 0.

$\frac{3}{2} = 1.5$, which gives us $3 = 2 \times 1 + 1$, and the sixth last digit is 1.

Finally, 1 is the same in any base, so the first digit is 1. The answer is 1100011.

2. Compute the sum $GILACXA + BCADAKL$ in base 26.

We add

$$\begin{array}{rcccccc} & & & & B & & \\ & G & I & L & A & C & X & A \\ + & B & C & A & D & A & K & L \\ \hline H & K & L & D & D & H & L & \end{array}$$

3. The following table gives a Boolean function f with 3-bit inputs and 1-bit outputs. Give an explicit formula for f , and simplify as much as possible.

$x_1x_2x_3$	$f(x_1x_2x_3)$
0 0 0	0
0 0 1	0
0 1 0	1
0 1 1	0
1 0 0	1
1 0 1	0
1 1 0	0
1 1 1	1

$$\begin{aligned}
 f(x_1x_2x_3) &= (1+x_1) \cdot x_2 \cdot (1+x_3) + x_1 \cdot (1+x_2) \cdot (1+x_3) + x_1 \cdot x_2 \cdot x_3 \text{ MOD } 2 \\
 &= x_1 + x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 + x_1 \cdot x_2 \cdot x_3 \text{ MOD } 2
 \end{aligned}$$

If you did not simplify you lost 4 points. You could lose at most 3 points if you made mistakes while simplifying. Not getting the original equation was much more costly. Leaving out MOD 2 in your final answer cost one point.

4. Show that $\mathcal{O}(\ln n) = \mathcal{O}(\ln(n^5))$.

Suppose $f(n)$ is in $\mathcal{O}(\ln n)$. By definition there are nonnegative numbers M and N so that $f(n) \leq M \cdot \ln n$ for all $n \geq N$. Since $\ln n \leq \ln n^5$ for all $n \geq 1$, we know that $f(n) \leq M \cdot \ln n^5$ for all $n \geq N$. So, by definition, $f(n)$ is in $\mathcal{O}(\ln n^5)$. Now we know that $\mathcal{O}(\ln n) \subseteq \mathcal{O}(\ln(n^5))$.

To finish we must show that $\mathcal{O}(\ln n^5) \subseteq \mathcal{O}(\ln n)$. So, suppose $f(n)$ is in $\mathcal{O}(\ln n^5)$. The laws of logarithms tells us that $\ln n^5 = 5 \ln n$. By definition there exist M and N so that $f(n) \leq M \cdot \ln n^5 = M \cdot 5 \ln n$ for all $n \geq N$. Therefore, $f(n) \leq M' \cdot \ln n$ for all $n \geq N$ if $M' = M/5$. Hence $f(n)$ is in $\mathcal{O}(\ln n)$, which shows that $\mathcal{O}(\ln n^5) \subseteq \mathcal{O}(\ln n)$.

Points could be earned by stating CLEARLY some of the following:

- The definition of \mathcal{O} .
- The definition of \mathcal{O} using $\ln n$ and $\ln n^5$ correctly.
- Stating that $\ln n^5 = 5 \ln n$.
- Recognizing that you have to show that $\mathcal{O}(\ln n^5) \subseteq \mathcal{O}(\ln n)$ AND $\mathcal{O}(\ln n) \subseteq \mathcal{O}(\ln n^5)$.
- Correctly using M and N in the different cases.
- Showing that $\frac{\ln n^5}{\ln n} = \frac{1}{5}$ and stating correctly how this was important.

Points were lost for anything stated which was not true.

5. Let $\mu(n) = 3^n + n^2$. Is $\mu(n) \in \mathcal{O}(5^n)$?

To say that $\mu(n) \in \mathcal{O}(f(n))$ means that there are constants $M, N > 0$ such that for all $n > N$, $\mu(n) \leq Mf(n)$. We are given $\mu(n) = 3^n + n^2$ and $f(n) = 5^n$.

Since $3 < 5$, we get $3^n < 5^n$ for all $n > 0$.

Since n^2 is a polynomial in n and 5^n is exponential in n , we know that eventually, 5^n will outrun n^2 . That is, there is some $N > 0$ such that for all $n > N$, $5^n > n^2$.

We use this N and $M = 2$ and get that for all $n > N > 0$,

$$\mu(n) = 3^n + n^2 < 5^n + 5^n = M5^n.$$

Therefore, $\mu(n) \in \mathcal{O}(5^n)$.

6. A 4-bit linear feedback shift register has 00010011 appear in its output stream. Find the next four digits in the output stream after these.

To compute an additional digit at each step, if the previous four digits were $b_1, b_2, b_3,$ and $b_4,$ then the new digit is $c_1b_1 + c_2b_2 + c_3b_3 + c_4b_4$ for appropriate constants $c_1, c_2, c_3,$ and $c_4.$ The fifth, sixth, seventh, and eighth digits are each computed from the previous four digits. Each gives us an equation in terms of the previous digits. These equations are

$$0 = 1c_4 + 0c_3 + 0c_2 + 0c_1$$

$$0 = 0c_4 + 1c_3 + 0c_2 + 0c_1$$

$$1 = 0c_4 + 0c_3 + 1c_2 + 0c_1$$

$$1 = 1c_4 + 0c_3 + 0c_2 + 1c_1$$

This gives us four equations in four variables, so we can solve.

$$0 = c_4$$

$$0 = c_3$$

$$1 = c_2$$

$$1 = c_4 + c_1$$

$$1 = c_1$$

Hence, each new digit can be computed as $b_1 + b_2.$ We use this to compute the next four digits as 0101.

7. Let $f_k(x)$ be a Boolean function defined by

$$f_{k_1 k_2}(x_1 x_2) = (x_1 + k_1 \cdot x_2 \text{ MOD } 2)(k_2 + x_1 \cdot x_2 \text{ MOD } 2).$$

Compute the output of the Feistel function $F_{10}(1011)$.

$F_k(x_1 x_2 x_3 x_4) = x_3 x_4 || x_1 x_2 \oplus f_k(x_3 x_4)$. So the answer is

$$\begin{aligned} 11 || 10 \oplus f_{10}(11) &= (1 + 1 \cdot 1 \text{ MOD } 2)(0 + 1 \cdot 1 \text{ MOD } 2) \\ &= 11 || 10 \oplus 01 = 11 || 11 = 1111. \end{aligned}$$

8. A hash function $H(x)$ outputs 96-bit binary strings. Eve observes a message x from Alice to Bob whose hash is $H(x) = y$. Suppose that Eve tries to find another message v so that $H(v) = y$ by randomly trying 6 different messages x_1, x_2, \dots, x_6 . Assume that H is constructed so that for inputs chosen at random, each output is equally likely. What is the probability that Eve is successful? (Do NOT attempt to simplify your answer.)

The probability that any single guess by Eve hashes to y is $\frac{1}{2^{96}}$. So the probability that any single guess is not y is $1 - \frac{1}{2^{96}}$. The probability that none of the guesses are correct is

$$\left(1 - \frac{1}{2^{96}}\right)^6.$$

Thus the probability that she is successful is

$$1 - \left(1 - \frac{1}{2^{96}}\right)^6.$$

Partial credit, 7 points, could be earned by arguing that there are six chances so that the probability that the first or the second or the third or... or the sixth is successful is

$$\frac{1}{2^{96}} + \frac{1}{2^{96}} + \frac{1}{2^{96}} + \dots + \frac{1}{2^{96}} = \frac{6}{2^{96}}.$$

This is close, but not quite right as it ignores the (very remote) possibility that she might get it right more than once.

Partial credit was also given if you approached the problem as in the sample problem (although this is not really correct), 5 points if your answer was close to zero, 3 points if it was close to one.

Many people had answers that were not between zero and one - these are totally wrong.