CSE 311: Foundations of Computing I

Practice Midterm Exam Solutions

Name:	**Sample Solutions**		
ID:			
TA:		**Section:**	

INSTRUCTIONS:

- You have **50 minutes** to complete the exam.
- The exam is closed book. You may not use cell phones or calculators.
- All answers you want graded should be written on the exam paper.
- If you need extra space, use the back of a page. Make sure to mention that you did though.
- The problems are of varying difficulty.
- If you get stuck on a problem, move on and come back to it later.

Problem	Points	Score	Problem	Points	Score
1	20		5	5	
2	15		6	10	
3	10		7	20	
4	20				
			Σ	100	

Basic Techniques.

This part will test your ability to apply techniques that have been explicitly identified in lecture and reinforced through sections and homeworks. Remember to show your work and justify your claims.

1. To Logic. . . or Not To Logic [20 points]

(a) (5 points) Choose a meaning of $P(x, y, z)$ such that $\forall x \ \exists y \ \forall z \ \ P(x, y, z)$ is false, but $\forall x \ \forall y \ \exists z \ P(x, y, z)$ is true.

Solution: Let the domain be $\mathbb{N}$. Let $P(x, y, z)$ be "$x \geq 0 \wedge y \geq z$".

Then, the first statment is false, because, while $x \geq 0$ for everything in the domain, there is no largest number in the domain. However, the second statement is true, because $x \geq 0$ and $z = y$ satisfies the second part.

(b) (5 points) In the domain of integers, using any standard mathematical notation (but no new predicates), define Prime(x) to mean "x is prime".

Solution: Prime$(x) \equiv x \geq 2 \wedge \forall y \ ((1 \leq y \leq x \wedge y \mid x) \rightarrow (y = x \vee y = 1))$

Let the predicates $D(x, y)$ mean "team x defeated team y" and $P(x, y)$ mean "team x has played team y." Give quantified formulas with the following meanings:

(c) (5 points) Every team has lost at least one game.

Solution: $\forall x \ \exists y \ D(y, x)$

(d) (5 points) There is a team that has beaten every team it has played.

Solution: $\exists x \ \forall y \ (P(x, y) \rightarrow D(x, y))$

2. Obvious Induction Problem [15 points]
Prove for all $n \in \mathbb{N}$ that the following identity is true:

$$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$$

where $x \in \mathbb{R}, x \neq 1$.

Solution: 1. Let P(n) be the statement "$\sum_{i=0}^{n} x^i = \frac{1 - x^{n+1}}{1 - x}$" for all $n \in \mathbb{N}$.

We go by induction on n.

2. *Base Case*: When $n = 0$, P(0) is true, because since $x \neq 1$,

$$\sum_{i=0}^{0} x^i = x^0 = 1 = \frac{1 - x^1}{1 - x}.$$

3. *Induction Hypothesis*: Suppose $P(k)$ is true for some $k \in \mathbb{N}$.

4. *Induction Step*: We see that

$$\begin{aligned}
\sum_{i=0}^{k+1} x^i &= \sum_{i=0}^{k} x^i + x^{k+1} && \text{[Taking out the last term]} \\
&= \frac{1 - x^{k+1}}{1 - x} + x^{k+1} && \text{[By the IH]} \\
&= \frac{(1 - x^{k+1}) + (1 - x)x^{k+1}}{1 - x} && \text{[Algebra]} \\
&= \frac{1 - x^{k+2}}{1 - x} && \text{[Simplifying]}
\end{aligned}$$

which is what we wanted to show in the induction step.
5. Thus, we have proven P(n) for all $n \in \mathbb{N}$ by induction.

3. 311 **is Prime!** [10 points]
Find all solutions in the range $0 \leq x < 311$ to the modular equation:

$$12x \equiv 5 \pmod{311}$$

Solution: First, we compute the gcd of 311 and 12.

$$311 = 25 \cdot 12 + 11$$
$$12 = 1 \cdot 11 + 1$$
$$11 = 11 \cdot 1 + 0$$

so $gcd(311, 12) = 1$ and hence we finish the Extended Euclidean Algorithm using:

$$11 = 311 - 25 \cdot 12$$
$$1 = 12 - 11 \cdot 1$$

Now, backwards substituting:

$$1 = 12 - 1 \cdot 11 = 12 - 1 \cdot (311 - 25 \cdot 12) = 26 \cdot 12 - 1 \cdot 311$$

So, the multiplicative inverse of 12 modulo 311 is 26.
Now, we have the modular equation $12(26) \equiv 1 \pmod{311}$. Multiplying both sides by 5, we get:

$$12(26 \cdot 5) \equiv 5 \pmod{311} \rightarrow 12(130) \equiv 5 \pmod{311}$$

So, $x = 130$.

4. Even Circuits Are Fun [20 points]
The function multiple-of-three takes in two inputs: $(x_1x_0)_2$ and outputs 1 iff $3 \mid (x_1x_0)_2$.

(a) (5 points) Draw a table of values (e.g. a truth table) for multiple-of-three.

Solution:

x_1	x_0	multiple-of-three
0	0	1
0	1	0
1	0	0
1	1	1

(b) (5 points) Write multiple-of-three as a sum-of-products.

Solution:

$$\text{multiple-of-three} = (x_1'x_0') + (x_1x_0)$$

(c) (5 points) Write multiple-of-three as a product-of-sums.

Solution:

$$\text{multiple-of-three} = (x_1 + x_0')(x_1' + x_0)$$

(d) (5 points) Write multiple-of-three as a simplified expression (don't bother explaining what rules you're using).

Solution:

$$\text{multiple-of-three} = (x_1 + x_0)' + (x_1x_0)$$

5. Irrationally Rational [5 points]
Recall the definition of irrational is that a number is not rational, and that

$$\text{Rational}(x) \equiv \exists p\ \exists q\ x = \frac{p}{q} \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0$$

For this question, you may assume that π is irrational. Disprove that if x and y are irrational, then x + y is irrational.

Solution: Note that π is irrational, and multiplying by -1 maintains irrationality (because if it didn't, then we could find p, q by multiplying by -1, getting p, q, and choosing $-p$ and q). Finally, note that $\pi + (-\pi) = 0$, which is rational.

6. Rationally Irrational [10 points]
Recall the definition of irrational is that a number is not rational, and that

$$\text{Rational}(x) \equiv \exists p\, \exists q\, x = \frac{p}{q} \wedge \text{Integer}(p) \wedge \text{Integer}(q) \wedge q \neq 0$$

Prove that if x and y are rational and $x \neq 7$, then $\dfrac{y^2}{x-7}$ is rational.
Solution: Short solution: Suppose x, y are rational and $x \neq 7$. Then by definition $x = p/q$ for some integers p and q with $q \neq 0$. Therefore $x-7 = p/q-7 = \frac{p-7q}{q}$. Since $x \neq 7$, we have $p-7q \neq 0$. It follows that $\frac{1}{x-7} = \frac{q}{p-7q}$ is rational since q and $p-7q$ are integers and $p-7q \neq 0$. Now since $\frac{y^2}{x-7} = y \cdot y \cdot \frac{1}{x-7}$ we see that $\frac{y^2}{x-7}$ is the product of three rational numbers. In class, we showed that the product of rational numbers is also rational. Since y and $\frac{1}{x-7}$ are both rational, the product $y \cdot y \cdot \frac{1}{x-7} = \frac{y^2}{x-7}$ is also rational as required.
Longer solution not assuming what was done in class: Suppose x, y are rational and $x \neq 7$. Then by definition $x = p/q$ for some integers p and q with $q \neq 0$ and $y = r/s$ for some integers r and s for $s \neq 0$. Therefore $x - 7 = p/q - 7 = \frac{p-7q}{q}$. Since $x \neq 7$, we have $p - 7q \neq 0$. Also $y^2 = (r/s)^2 = \frac{r^2}{s^2}$. Therefore

$$\frac{y^2}{x-7} = \frac{\frac{r^2}{s^2}}{\frac{p-7q}{q}} = \frac{r^2 \cdot q}{s^2 \cdot (p-7q)}.$$

Since $s \neq 0$ and $p - 7q \neq 0$ we have $s^2 \cdot (p-7q) \neq 0$. Also, since r and q are integers $r^2 \cdot q$ is an integer and since s, p, and q are integers $s^2 \cdot (p-7q)$ is an integer. Therefore $\frac{y^2}{x-7}$ is quotient of integers $r^2 \cdot q$ and $s^2 \cdot (p-7q)$, the latter of which is $\neq 0$. Thus, it follows that $\frac{y^2}{x-7}$ is rational.

A Moment's Thought!

This section tests your ability to think a little bit more insightfully. The approaches necessary to solve these problems may not be immediately obvious. Remember to show your work and justify your claims.

7. Gotta $\square$ m $\forall$ [20 points]

We say that k is *a square modulo* m iff there is some integer j such that $k \equiv j^2 \pmod{m}$.
Let $T = \{m \ : \ m = n^2 + 1 \text{ for some integer } n\}$.

(a) (8 points) Prove that if $m \in T$, then -1 is a square modulo m.

Solution: Let m be an arbitrary element of T.

Then, $m = n^2 + 1$ for some integer n by definition of T.

Therefore, $m \mid (n^2 + 1)$. So, $n^2 \equiv -1 \pmod{m}$, which means -1 is a square modulo m.

(b) (12 points) Prove that for all integers m and k, if $m \in T$ and k is a square modulo m then $-k$ is also a square modulo m.

Solution: Let m be an arbitrary element of T, and suppose that k is a square modulo m. Then, $k \equiv j^2 \pmod{m}$ for some integer j.

Multiplying both sides of the congruence by -1, we get $-k \equiv (-1)j^2 \pmod{m}$.

From (a), we know that $n^2 \equiv -1 \pmod{m}$. Thus, we have $-k \equiv n^2 j^2 \pmod{m}$.

So, $-k \equiv (nj)^2 \pmod{m}$, which means $-k$ is a square modulo m.

CSE 311: Foundations of Computing I

Logical Equivalences Reference Sheet

Identity

$$p \wedge \mathsf{T} \equiv p$$
$$p \vee \mathsf{F} \equiv p$$

Domination

$$p \vee \mathsf{T} \equiv \mathsf{T}$$
$$p \wedge \mathsf{F} \equiv \mathsf{F}$$

Idempotency

$$p \vee p \equiv p$$
$$p \wedge p \equiv p$$

Commutativity

$$p \vee q \equiv q \vee p$$
$$p \wedge q \equiv q \wedge p$$

Associativity

$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$
$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$

Distributivity

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$
$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

Absorption

$$p \vee (p \wedge q) \equiv p$$
$$p \wedge (p \vee q) \equiv p$$

Negation

$$p \vee \neg p \equiv \mathsf{T}$$
$$p \wedge \neg p \equiv \mathsf{F}$$

DeMorgan's Laws

$$\neg(p \vee q) \equiv \neg p \wedge \neg q$$
$$\neg(p \wedge q) \equiv \neg p \vee \neg q$$

Double Negation

$$\neg\neg p \equiv p$$

Law of Implication

$$p \rightarrow q \equiv \neg p \vee q$$

Contrapositive

$$p \rightarrow q \equiv \neg q \rightarrow \neg p$$

CSE 311: Foundations of Computing I

Boolean Algebra Axioms (and Some Theorems)

Axioms

Closure

$a + b$ is in $\mathbb{B}$

$a \bullet b$ is in $\mathbb{B}$

Commutativity

$$a + b = b + a$$
$$a \bullet b = b \bullet a$$

Associativity

$$a + (b + c) = (a + b) + c$$
$$a \bullet (b \bullet c) = (a \bullet b) \bullet c$$

Identity

$$a + 0 = a$$
$$a \bullet 1 = a$$

Distributivity

$$a + (b \bullet c) = (a + b) \bullet (a + c)$$
$$a \bullet (b + c) = (a \bullet b) + (a \bullet c)$$

Complementarity

$$a + a' = 1$$
$$a \bullet a' = 0$$

Theorems

Null

$$X + 1 = 1$$
$$X \bullet 0 = 0$$

Idempotency

$$X + X = X$$
$$X \bullet X = X$$

Involution

$$(X')' = X$$

Uniting

$$X \bullet Y + X \bullet Y' = X$$
$$(X + Y) \bullet (X + Y') = X$$

Absorbtion

$$X + X \bullet Y = X$$
$$(X + Y') \bullet Y = X \bullet Y$$
$$X \bullet (X + Y) = X$$
$$(X \bullet Y') + Y = X + Y$$

DeMorgan

$$(X + Y + \cdots)' = X' \bullet Y' \bullet \cdots$$
$$(X \bullet Y \bullet \cdots)' = X' + Y' + \cdots$$

Consensus

$$(X \bullet Y) + (Y \bullet Z) + (X' \bullet Z) = X \bullet Y + X' \bullet Z$$
$$(X + Y) \bullet (Y + Z) \bullet (X' + Z) = (X + Y) \bullet (X' + Z)$$

Factoring

$$(X + Y) \bullet (X' + Z) = X \bullet Z + X' \bullet Y$$
$$X \bullet Y + X' \bullet Z = (X + Z) \bullet (X' + Y)$$

CSE 311: Foundations of Computing I

Axioms & Inference Rules

Excluded Middle

$$\therefore \quad A \vee \neg A$$

Direct Proof

$$\frac{A \Rightarrow B}{\therefore \quad A \to B}$$

Modus Ponens

$$\frac{A \qquad A \to B}{\therefore \qquad B}$$

Intro $\wedge$

$$\frac{A \qquad B}{\therefore \quad A \wedge B}$$

Elim $\wedge$

$$\frac{A \wedge B}{\therefore\ A \qquad B}$$

Intro $\vee$

$$\frac{A}{\therefore\ A \vee B \quad B \vee A}$$

Elim $\vee$

$$\frac{A \vee B \qquad \neg A}{\therefore \qquad B}$$

Intro $\exists$

$$\frac{P(c) \text{ for some } c}{\therefore \qquad \exists x\ P(x)}$$

Elim $\forall$

$$\frac{\forall x\ P(x)}{\therefore\ P(a) \text{ for any } a}$$

Intro $\forall$

$$\frac{\text{Let } a \text{ be arbitrary} \ldots P(a)}{\therefore\ \forall x\ P(x) \qquad (\text{If no other name in } P \text{ depends on } a)}$$

Elim $\exists$

$$\frac{\exists x\ P(x)}{\therefore\ P(c) \text{ for some } \textit{special } c \qquad \text{list dependencies for } c}$$