CSE 311 : Midterm Exam Solutions

1. Translation

Let your domain of discourse be positive integers.

For this problem, you may use the predicates

- $\texttt{Even}(x)$ which is true if and only if x is even.
- $\texttt{Odd}(x)$ which is true if and only if x is odd.
- $\texttt{PrimePower}(x)$ which is true if and only if x is "a prime power" (which means the prime factorization of x is p^a for a prime number p and an integer a. $125 = 5^3$ is a prime power, $24 = 2^3 \cdot 3$ is not a prime power)
- $\texttt{PowerOfTwo}(x)$, which is true if and only if x is a power of 2 (i.e., $x = 2^c$ for some integer c)
- standard math predicates (e.g. $=, \neq, <, >, \geq, \ldots$)

(a) Translate the following predicate logic statement into English. Your translation must be natural.

$\forall x(\texttt{PrimePower}(x) \to \texttt{Odd}(x) \vee \texttt{PowerOfTwo}(x))$

Solution:

Every prime power is odd or a power of two.

(b) Translate "There is more than one prime power" into predicate logic. **Solution:**

$\exists x \exists y(\texttt{PrimePower}(x) \wedge \texttt{PrimePower}(y) \wedge x \neq y$.

(c) Find an equivalent statement to the one below by taking the contrapositive of the implication inside. Give your final answer in English; you do not need to show work.

"For every integer, if it is even then it is a power of two or not a prime power."

Solution:

"For every integer, if it is not a power of two and a prime power, then it is not even."

(d) Negate the following predicate logic sentence. In your final answer, negations should only be applied to single predicates.

$\exists x \forall y([\texttt{Even}(y) \vee \texttt{PrimePower}(y)] \to [\texttt{Even}(x) \wedge \texttt{Odd}(y)])$

Solution:

$\forall x \exists y[\texttt{Even}(y) \vee \texttt{PrimePower}(y)] \wedge [\texttt{Odd}(x) \vee \texttt{Even}(y)]$

2. Even Circuits Are Fun

The function multiple-of-three takes in two inputs: $(x_1x_0)_2$ and outputs 1 iff $3 \mid (x_1x_0)_2$. $(x_1x_0)_2$ represents the binary number where the first bit is x_1 and the second bit is x_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
F	F	T
F	T	F
T	F	F
T	T	T

(b) (5 points) Write multiple-of-three as a sum-of-products. (DNF) **Solution:**

multiple-of-three:
$(\neg x_1 \wedge \neg x_0) \vee (x_1 \wedge x_0)$
or in boolean algebra: $= (x_1'x_0') + (x_1x_0)$

(c) (5 points) Write multiple-of-three as a product-of-sums. (CNF) **Solution:**

multiple-of-three:
$(x_1 \vee \neg x_0) \wedge (\neg x_1 \vee x_0)$
or in boolean algebra: $= (x_1 + x_0')(x_1' + x_0)$

3. Number Theory Proof

For the questions below you may use the definitions of modular equivalence and divides and algebra.

You may not use results from the number theory formula sheet or theorems proven in class (though you may emulate those proofs!)

Finally, you may also use this fact without proving it:

Fact 1: For any two integers x, y and any prime p: if $xy \equiv 0 \pmod{p}$ then $p|x$ or $p|y$.

(a) Disprove this statement with a counterexample.

For every integer n, $ab \equiv 0 \pmod{n}$ implies $a \equiv 0 \pmod{n}$ or $b \equiv 0 \pmod{n}$. (Hint: you will need to choose n to be a composite number).

Solution:

Take $n = 10, a = 5, b = 2$. We note $5 \cdot 2 \equiv 0 \pmod{10}$ but $a \not\equiv 0 \pmod{10}$ and $b \not\equiv 0 \pmod{10}$.

Remark: There are many other examples. We can take some composite integer n (such as 10) and if we take a,b s.t. a*b = n then this should serve as a counter-example (there are other families of counter-examples).

(b) Prove that for every prime p: If $ab \equiv 0 \pmod{p}$, then $a \equiv 311p \pmod{p}$ or $b \equiv 0 \pmod{p}$.

Solution:

Let p be an arbitrary prime and a, b be arbitrary integers such that $ab \equiv 0 \pmod{p}$. Applying Fact 1 above, we have

$p|a$ or $p|b$. Applying the definition of mod twice we have:

$a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. We now divide into two cases.

Case 1: $a \equiv 0 \pmod{p}$. By definition of equivalence, $p|a$, so $pk = a$ for some integer k. Then $pk - 311p = a - 311p$. Factoring, $p(k-311) = a - 311p$. Since k is an integer, $k - 311$ is as well, and we have $p|(a-311p)$. Thus $a \equiv 311p \pmod{p}$

Case 2: $b \equiv 0 \pmod{p}$

In this case we're already done! :D

In both cases, we have our desired conclusion. Since a, b, p were arbitrary the implication holds for every prime p

4. Induction Proof

Prove that $6 | \left(10^{2n} + 2\right)$ for all $n \in \mathbb{Z}^+$ using induction on n.

Recall that $\mathbb{Z}^+$ is the positive integers (i.e., starting at 1).

Don't forget to define your predicate as part of your proof!

Hint: $198 = 6 \cdot 33$. **Solution:**

Let $P(n)$ be the statement:

$$6 \mid 10^{2n} + 2$$

We prove that $P(n)$ is true for all $n \in \mathbb{Z}^+$ by induction on n.

Base Case: $P(1)$:
$10^{2\cdot 1} + 2 = 10^2 + 2 = 102 = 17 \cdot 6$
By the definition of division, $6|102$, $P(1)$ holds.

Inductive Hypothesis: Suppose that $P(k)$ is true for some arbitrary $k \in \mathbb{Z}^+$.

Inductive Step: We show $P(k+1)$:

$$\begin{aligned} 10^{2\cdot(k+1)} + 2 &= 10^{2k+2} + 2 \\ &= 10^{2k} \cdot 100 + 2 \\ &= (6j - 2) \cdot 100 + 2 \quad \text{Inductive Hypothesis} \\ &= 600j - 198 \\ &= (100j - 33) \cdot 6 \end{aligned}$$

By the definition of division, $6|10^{2\cdot(k+1)} + 2$, so this proves $P(k+1)$.

Conclusion: $P(n)$ holds for all $n \in \mathbb{Z}^+$ by the principle of induction.

5. First Proof [12 points]

(a) Prove $(A \cup B) \setminus (A \cap B) \subseteq [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$
You must format your proof as an English proof and structure your proof by introducing arbitrary element(s) of sets as appropriate.
We recommend drawing a picture of the sets for yourself so you see why the statement is true. [7 points]
Solution:

Let x be an arbitrary element of $A \cup B \setminus (A \cap B)$. By definition of $\setminus$, $x \in A \cup B$ and $x \notin A \cap B$. Since $x \in A \cup B$ (by definition of union) we have $x \in A$ or $x \in B$. We divide into cases:

Case 1: $x \in A$: In this case, we have $x \in A$ and $x \notin A \cap B$. This is exactly the definition of $x \in A \setminus (A \cap B)$. We therefore have $x \in A \setminus (A \cap B)$ or $x \in B \setminus (A \cap B)$. Then by definition of union, $x \in [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$.

Case 2: $x \in B$: In this case, we have $x \in B$ and $x \notin A \cap B$. This is exactly the definition of $x \in B \setminus (A \cap B)$. We therefore have $x \in A \setminus (A \cap B)$ or $x \in B \setminus (A \cap B)$. Then by definition of union, $x \in [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$.

Since x was arbitrary, $(A \cup B) \setminus (A \cap B) \subseteq [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$.

(b) From (only) what you've written above, can you conclude: $(A \cup B) \setminus (A \cap B) = [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$ (we've changed the subset from (a) to an equals sign).

If you can conclude the new statement, briefly (1-2 sentences) explain why.
If you cannot conclude the new statement, what statement do you still need to prove to get the new conclusion? (you can give you answer in English, set notation, or predicate logic notation – whichever you find most convenient). [2 points]

Solution:

You cannot conclude the new statement. You still need to prove the other direction of the inclusion, i.e. that $(A \cup B) \setminus (A \cap B) \supseteq [A \setminus (A \cap B)] \cup [B \setminus (A \cap B)]$

(c) Disprove the following statement: $(A \cup B) \setminus (A \cap B) = [(A \cup B) \setminus A] \cap [(A \cup B) \setminus B]$ [3 points **Solution:**

Consider $A = \{1, 2, 3\}$, $B = \{3, 4\}$

Then $(A \cup B) \setminus (A \cap B) = \{1, 2, 3, 4\} \setminus \{3\} = \{1, 2, 4\}$

While $[(A \cup B) \setminus A] \cap [(A \cup B) \setminus B] = [\{1, 2, 3, 4\} \setminus \{1, 2, 3\}] \cap [\{1, 2, 3, 4\} \setminus \{3, 4\}] = [\{4\}] \cap \{1, 2\} = \varnothing$.

The sets are not equal, as required.

Remark: Just about any sets A, B that are not comparable with subset (i.e., such that both $A \setminus B$ and $B \setminus A$ are nonempty) will produce a counter-example here.