CSE 311 : 22Wi Midterm Exam Solutions

1. Distributed Systems + NFT = Profit??

For the following statements, translate them into predicate logic, keeping in mind the respective domains of discourse and predicates.

(a) Translate the following statement into logic:

"Robbie owns exactly two distinct NFTs."

Let your domain of discourse be all NFTs. You should use the following predicates:

- $\texttt{RobbieOwns}(x)$ is true iff x is an NFT owned by Robbie
- $\texttt{Equals}(x, y)$ is true iff the two objects are equal (as in the exact same object)

Solution:

$\exists x, y(\neg\,\texttt{Equals}(x, y) \wedge \texttt{RobbieOwns}(x) \wedge \texttt{RobbieOwns}(y) \wedge \forall z(\texttt{RobbieOwns}(z) \rightarrow (\texttt{Equals}(x, z) \vee \texttt{Equals}(z, y))))$

(b) Translate the following statement into logic:

"Modern day systems which are partition tolerant cannot be both consistent and available."

Let your domain of discourse be all systems. You should use the following predicates:

- $\texttt{ModernDaySystem}(x)$ is true iff x is a modern day system
- $\texttt{PartitionTolerant}(x)$ is true iff x is partition tolerant
- $\texttt{Consistent}(x)$ is true iff x is consistent
- $\texttt{Available}(x)$ is true iff x is available

Solution:

This English sentence isn't as clear as we thought it was. Some people interpreted it to mean "Modern day systems, all of which are partition tolerant, cannot be both consistent and available."

Others interpreted it as "Among all the modern day systems, think about the partition tolerant-ones: those systems cannot be both consistent and available."

We intended the second, but both interpretations are reasonable, so we're giving full credit for both.

Interpretation one would mean something like:
$\forall x(\texttt{ModernDaySystem}(x) \rightarrow [\texttt{PartitionTolerant}(x) \wedge \neg(\texttt{Consistent}(x) \wedge \texttt{Available}(x))])$

Interpretation two could be translated both of the following ways:
$\forall x(\texttt{ModernDaySystem}(x) \rightarrow (\texttt{PartitionTolerant}(x) \rightarrow \neg(\texttt{Consistent}(x) \wedge \texttt{Available}(x)])))$

Also correct: $\forall x([\texttt{ModernDaySystem}(x) \wedge \texttt{PartitionTolerant}(x)] \rightarrow \neg(\texttt{Consistent}(x) \wedge \texttt{Available}(x)))$

(c) Let your domain of discourse be all integers (i.e., $\mathbb{Z}$). We define the following predicates:

- $\texttt{Perfect}(x)$ is true iff x is a perfect number
- $\texttt{Even}(x)$ is true iff x is even
- $\texttt{Greater}(a, b)$ is true iff $a > b$

Consider the following statement:

$$\forall x(\texttt{Perfect}(x) \to [\texttt{Even}(x) \vee \texttt{Greater}(x, 1000)])$$

Write (in predicate logic notation) an equivalent statement to the one above by taking the contrapositive of the implication. Your notation should be simplified, by having negations apply only to individual predicates.

Then, translate your statement into English. You do not have to use domain restriction in your translation.

Solution:

$\forall x((\neg \texttt{Even}(x) \wedge \neg \texttt{Greater}(x, 1000)) \to \neg \texttt{Perfect}(x))$

All non-even integers less-than-or-equal-to 1000 are not perfect.

2. Non-Inductible Tokens [20 points]

In his eternal pursuit for the ideal NFT, Robbie has decided to focus on creating some NFTs with various levels of scarcity. Every day, Robbie creates one new NFT and adds it to his collection.

Define the scarcity of day n's NFT as $\mathcal{S}_n = 0+1+\cdots+n$ where $n \in \mathbb{N}$. We proved in section that $\mathcal{S}_n = \frac{n(n+1)}{2}$.

Now, define the combined scarcity of the NFTs in Robbie's wallet on day n as $\mathcal{T}_n = \mathcal{S}_0 + \mathcal{S}_1 + \cdots + \mathcal{S}_n$, where $n \in \mathbb{N}$.

Now, it's your turn! Prove by way of induction for all $n \in \mathbb{N}$:

$$\mathcal{T}_0 + \mathcal{T}_1 + \cdots + \mathcal{T}_n = \frac{n(n+1)(n+2)(n+3)}{24}.$$

You may (and should) use the following as fact: $\mathcal{T}_n = \frac{n(n+1)(n+2)}{6}$.

IMPORTANT: There is NO NEED to expand out/"FOIL" out the expression when doing your inductive step! We only need to factor out expressions.

An example of expanding/FOILing is going from $(x+y)(5y+z)$ to $5xy + xz + 5y^2 + yz$.
An example of factoring is: $5x + xy = x(5+y)$.

Solution:

First, note that $\mathcal{T}_n = \mathcal{S}_0 + \mathcal{S}_1 + \cdots + \mathcal{S}_n$. So, we are trying to prove $(\mathcal{S}_0) + (\mathcal{S}_0 + \mathcal{S}_1) + \cdots + (\mathcal{S}_0 + \mathcal{S}_1 + \cdots + \mathcal{S}_n) = \frac{n(n+1)(n+2)(n+3)}{24}$.

Let $P(n)$ be the statement:

$$\mathcal{T}_0 + \mathcal{T}_1 + \cdots + \mathcal{T}_n = \frac{n(n+1)(n+2)(n+3)}{24}.$$

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

Base Case: $\mathcal{T}_0 = \mathcal{S}_0 = \frac{0(0+1)}{2} = 0 = \frac{0(0+1)(0+2)(0+3)}{24}$, so $P(0)$ holds.

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

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

$$\begin{aligned}
\mathcal{T}_0 + \mathcal{T}_1 + \cdots + \mathcal{T}_{k+1} &= (\mathcal{T}_0 + \mathcal{T}_1 + \cdots + \mathcal{T}_k) + \mathcal{T}_{k+1} && \text{Associativity} \\
&= \left(\frac{k(k+1)(k+2)(k+3)}{24}\right) + \mathcal{T}_{k+1} && \text{Inductive Hypothesis} \\
&= \frac{k(k+1)(k+2)(k+3)}{24} + \frac{(k+1)(k+2)(k+3)}{6} && \mathcal{T}_n = \frac{n(n+1)(n+2)}{6} \text{ as given} \\
&= \frac{k(k+1)(k+2)(k+3)}{24} + \frac{4(k+1)(k+2)(k+3)}{24} \\
&= \frac{k(k+1)(k+2)(k+3) + 4(k+1)(k+2)(k+3)}{24} \\
&= \frac{(k+1)(k+2)(k+3)(k+4)}{24} && \text{Factor out } (k+1)(k+2)(k+3)
\end{aligned}$$

This proves $P(k+1)$.

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

3. NFT's $\neq$ Boring

(a) Translate the following statement into logic:

> There is a "neutral number", such that any real number a when added to the neutral number yields a.

Let your domain of discourse be all real numbers (i.e., $\mathbb{R}$). You may use the mathematical operator $+$ and quantifiers ($\exists$, $\forall$). You can *only* use the following predicate:

- $\texttt{Equals}(a, b)$ is true iff $a = b$

You may not define a predicate "neutral" you must incorporate that meaning directly with just $\texttt{Equals}(a, b)$.

Solution:

$\exists e \forall a (\texttt{Equals}(a + e, a))$

(b) We call an integer b "**boring** for $\pmod{n}$ arithmetic" iff for all a: $a + b \equiv a \pmod{n}$, where $a, b \in \mathbb{Z}$.

Show that for integers b and b' where both b and b' are boring for $\pmod{n}$ arithmetic, that $b \equiv b' \pmod{n}$. For this problem you may **not** use any of the identities on the number theory reference sheet.

You must complete this proof using only the definitions of mod and divides and algebra.

For example, you cannot subtract a from both sides of a **modular** equation (as that would be applying the "adding congruences" theorem), but you can subtract a from both sides of a "regular = equation," as that's "just algebra."

A reminder of definitions:

- $a \equiv b \pmod{m}$ iff $m \mid (b - a)$ (def of mod)
- $a \mid b$ iff $\exists (k \in \mathbb{Z})\ b = ka$ (def of divides)

Solution:

Let n be an arbitrary integer greater than 1, and let b, b' be arbitrary boring numbers for $\pmod{n}$ arithmetic.

Since both b and b' are boring, we can write: $a + b \equiv a \pmod{n}$ and $a + b' \equiv a \pmod{n}$.

Applying the definition of mod, we have: $n \mid (a + b - a)$, which means $n \mid b$ and $n \mid (a + b' - a)$ which means $n \mid b'$.

Applying the definition of divides we have: $nk = b$ and $nk' = b'$ for integers k, k'.

Subtracting and factoring out n, we have: $n(k - k') = b - b'$.

Since k, k' are integers, their difference is an integer. We can thus apply the definition of divides and get: $n \mid (b - b')$.

And applying the definition of mod, we have: $b \equiv b' \pmod{n}$, as required.