Math 302 Final Exam Solutions

Dec 13, 2010

1. (5 pts each) Translate the following into Block World syntax.
   (a) There is a triangle that is between a square and a pentagon.

   ```
   E x E y E z (Triangle(x) /\ Square(y) /\ Pentagon(z) /\ Between(x,y,z))
   ```

   (b) There is only one large pentagon.

   ```
   E x (Large(x) /\ Pentagon(x) /\ (A y ((Large(x) /\ Pentagon(x)) => y=x))))
   ```

2. (10 pts) Write a derivation of the following argument.

$$\begin{array}{l} (\forall\ x \text{ in } Z)[(A(x) \to R(x)) \vee T(x)] \\ (\exists\ x \text{ in } Z)[T(x) \to P(x)] \\ (\forall\ x \text{ in } Z)[A(x) \wedge \neg P(x))] \\ \hline (\exists\ x \text{ in } Z)[R(x)] \end{array}$$

(1)	$(\forall\ x \text{ in } Z)[(A(x) \to R(x)) \vee T(x)]$	
(2)	$(\exists\ x \text{ in } Z)[T(x) \to P(x)]$	
(3)	$(\forall\ x \text{ in } Z)[A(x) \wedge \neg P(x)]$	
(4)	$(A(a) \to R(a)) \vee T(a)$	(1), universal instantiation for all $a \in Z$
(5)	$A(a) \wedge \neg P(a)$	(3), universal instantiation for all $a \in Z$
(6)	$T(a) \to P(a)$	(3), existential instantiation for some $a \in Z$
(7)	$\neg P(a)$	(5), simplification
(8)	$\neg T(a)$	(6),(7), modus tollens
(9)	$A(a) \to R(a)$	(4),(8), modus tollendo ponens
(10)	$A(a)$	(5), simplification
(11)	$R(a)$	(9),(10), modus ponens
(12)	$(\exists\ x \text{ in } Z)[R(x)]$	(11), existential generalization

3. (10 pts) Let I be a set and let $\{A_i\}_{i\in I}$ be a family of sets indexed by I. Let B be a set. Show that

$$\left(\bigcap_{i\in I} A_i\right) - B = \bigcap_{i\in I}(A_i - B).$$

   Notice that $x \in \left(\bigcap_{i\in I} A_i\right) - B$ iff $x \in \bigcap_{i\in I} A_i$ and $x \notin B$ iff $x \in A_i$ for all $i \in I$ and $x \notin B$ iff $x \in A_i - B$ for all $i \in I$ iff $x \in \bigcap_{i\in I}(A_i - B)$. Therefore $\left(\bigcap_{i\in I} A_i\right) - B = \bigcap_{i\in I}(A_i - B)$.

4. (10 pts) Find an example of a function $f : J \to K$ together with sets $Z \subseteq J$ and $W \subseteq K$ such that $f^*(W) = Z$ (or $f^{-1}(W) = Z$) and $f_*(Z) \neq W$ (or $f(Z) \neq W$).

   Let $f : \mathbb{R} \to \mathbb{R}$ be given by $f(x) = |x|$. Let $W = [-1, 1]$ and $Z = [-1, 1]$. Then $f^{-1}(W) = Z$ because if $x \in [-1, 1]$ then $0 \leq |x| \leq 1$ and if $x \in \mathbb{R}$ such that $x \notin [-1, 1]$ then $|x| > 1$. On the other hand $f(Z) = [0, 1] \neq W$.

5. (a) (2 pts) State the definition of rational number.

   A number x is a rational number if there exist $m, n \in \mathbb{Z}$, $n \neq 0$ such that $x = m/n$.

(b) (8 pts) Prove that $\sqrt{3}$ is irrational.

First, we will prove the following lemma: for an integer n, if $3|n^2$ then $3|n$. The proof is by contrapositive. If $3 \nmid n$ then either $n = 3k+1$ for some $k \in \mathbb{Z}$ or $n = 3k+2$ for some $k \in \mathbb{Z}$. In the first case,

$$n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

which is clearly not divisible by 3 (because the remainder is 1). In the second case,

$$n^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

which is clearly not divisible by 3 (because the remainder is 1).
Now we will prove that $\sqrt{3}$ is irrational by contradiction. Suppose $\sqrt{3}$ is rational. Then there exist $m, n \in \mathbb{Z}$, $n \neq 0$ such that $\sqrt{3} = m/n$. We can require that m/n be reduced to lowest terms, i.e. $\gcd(m,n) = 1$. Now,

$$\sqrt{3} = \frac{m}{n} \implies 3 = \frac{m^2}{n^2} \implies 3n^2 = m^2.$$

This shows that $3|m^2$. Hence $3|m$ by the lemma. So $m = 3k$ for some $k \in \mathbb{Z}$. Now

$$3n^2 = (3k)^2 \implies n^2 = 3k^2.$$

This shows that $3|n^2$. Hence $3|n$ by the lemma. But then 3 is a common divisor of m and n, which contradicts $\gcd(m,n) = 1$. Therefore $\sqrt{3}$ must be irrational.

6. (10 pts) Prove that if $x \in \mathbb{Z}$ then $x^2 \equiv 0 \mod 8$ or $x^2 \equiv 1 \mod 8$ or $x^2 \equiv 4 \mod 8$.

Let $x \in \mathbb{Z}$. Then integer division of x by 4 will give a remainder of 0, 1, 2, or 3. We will consider these cases.

$x = 4k$ **for some** $k \in \mathbb{Z}$**:** In this case,

$$x^2 = (4k)^2 = 16k^2 = 8(2k^2) \implies x^2 \equiv 0 \mod 8.$$

$x = 4k+1$ **for some** $k \in \mathbb{Z}$**:** In this case,

$$x^2 = (4k+1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1 \implies x^2 \equiv 1 \mod 8.$$

$x = 4k+2$ **for some** $k \in \mathbb{Z}$**:** In this case,

$$x^2 = (4k+2)^2 = 16k^2 + 16k + 4 = 8(2k^2 + 2k) + 4 \implies x^2 \equiv 4 \mod 8.$$

$x = 4k+3$ **for some** $k \in \mathbb{Z}$**:** In this case,

$$x^2 = (4k+3)^2 = 16k^2 + 24k + 9 = 8(2k^2 + 3k + 1) + 1 \implies x^2 \equiv 1 \mod 8.$$

Note: Another easy way to do this problem is to work with conjugacy classes modulo 8. Note that modulo 8

$$[x] \in \{[-3], [-2], [-1], [0], [1], [2], [3], [4]\}.$$

Now $[0]^2 = [0]$, $[\pm 1]^2 = [1]$, $[\pm 2]^2 = [4]$, $[\pm 3]^2 = [1]$, and $[4]^2 = [0]$. This proves the desired statement.

7. (10 pts) Let A and B be sets. Prove that $A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

First, suppose that $A \subseteq B$. If $X \subseteq A$ then $X \subseteq B$ by the transitivity of $\subseteq$ (Lemma 3.2.2(iii)). So

$$X \in \mathcal{P}(A) \implies X \subseteq A \implies X \subseteq B \implies X \in \mathcal{P}(B).$$

Hence $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Now, suppose $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. In particular, $A \in \mathcal{P}(A)$. So $A \in \mathcal{P}(B)$. But then $A \subseteq B$.

8. Let $f : A \to B$ be a function.
   (a) (3 pts) Define the left inverse and the right inverse of f.

   A function $g : B \to A$ is a left inverse of f if $g \circ f = 1_A$ and a right inverse of f if $f \circ g = 1_B$.

   (b) (7 pts) Construct an example of a function f which has a right inverse but not a left inverse. Be sure to justify your example.

   Let $f : \mathbb{R} \to \mathbb{R}^{\geq 0}$ be given by $f(x) = x^2$. Let $g : \mathbb{R}^{\geq 0} \to \mathbb{R}$ be given $g(x) = \sqrt{x}$. Then for any $x \in \mathbb{R}^{\geq 0}$

$$f \circ g(x) = f(\sqrt{x}) = (\sqrt{x})^2 = x.$$

   Hence $f \circ g = 1_{\mathbb{R}^{\geq 0}}$. So g is a right inverse of f.
   But f cannot have a left inverse. Suppose there is a function $h : \mathbb{R}^{\geq 0} \to \mathbb{R}$ such that $h \circ f = 1_{\mathbb{R}}$. Then

$$1 = h \circ f(1) = h(1^2) = h(1) = h((-1)^2) = h \circ f(-1) = -1$$

   which is clearly absurd.

   Note: We proved in class that a function f has a left inverse iff f is injective and a right inverse iff f is surjective. So all I had to do was find an example of a function that is surjective but not injective then recycle one of the ideas from that proof to show that since it is not injective, it cannot have a right left inverse.

9. (10 pts) **Extra credit problem.** Given a nonempty set of people S, let $*$ be the relation defined by $x * y$ if x is a friend of y. Let $*$ be symmetric (i.e. if x is a friend of y, then y is also a friend of x) but not reflexive (i.e. nobody is his/her own friend). Now, let n be any positive integer. Prove that in any group of n people, there is either someone who has no friends, or there are two different people who have the same number of friends.

   Since this is a nice problem to assign as Problem of the Week, I won't spell out its solution here. If you want a hint, just consider how many friends each person in S can have, then notice that if everybody has at least one friend, there aren't enough numbers to assign a different one to each person.