Formal Methods for High-Assurance Software Engineering

HomeWork Assignment 05

Shahin Roozkhosh
shahin@bu.edu
U01670169

October 2020

Problem 1. For the model $\mathcal{M} = (\mathbb{N}, +, \times)$:

part 1

Solution.

$$\phi_1(x) = \forall y \, (x \times y \approx x) \tag{1}$$

part 2

Solution.

$$\phi_2(x) = \forall y \, (x \times y \approx y) \tag{2}$$

part 3

Solution.

$$\phi_3(x, y) = y \approx x + 1 \tag{3}$$

part 4

Solution.

$$\phi_4(x, y) = \exists z \, (x + z \approx y) \tag{4}$$

Problem 2. Exercise on page 7 Lec. 16: Prenex Normal Form and Skolemiztion
part 1 Show with natural deduction:

$$(\forall x \, \varphi(x, f(x))) \vdash (\forall x \exists y \, \varphi(x, y)) \tag{5}$$

Solution. Showing the validity of the wff (5) is equivalent to, show that the following wff is a tautology:

$$\forall x\ \varphi(x, f(x))) \vdash (\forall x \exists y\ \varphi(x, y) \tag{6}$$

Here we go:

1	$\forall x\ \varphi(x, f(x))$	assume
2	x_0	fresh
3	$\varphi(x_0, f(x_0))$	$\forall x$e, 6
4	$\exists y\ \varphi(x_0, y)$	$\exists y$i, 3
5	$\forall\ x \exists y\ \varphi(x, y)$	$\forall x$i, $2-4$
6	$\forall x\ \varphi(x, f(x))) \vdash (\forall x \exists y\ \varphi(x, y)$	$\rightarrow$i$6-5$

part 2 Show:

$$(\forall x \exists y\ \varphi(x, y)) \nvDash (\forall x\ \varphi(x, f(x))) \tag{7}$$

Solution. As hint suggests, it suffices to define a model that contradicts the counter assumption. There are so many ways to do this. For the sake of the contradiction assume:

$$(\forall x \exists y\ \varphi(x, y)) \models (\forall x\ \varphi(x, f(x))) \tag{8}$$

In the model $\mathcal{M} = (\mathbb{N}, +)$ Let $\varphi(x, y) = y \approx x + 1$ and define $f(x) = x$ Then:

$$\begin{aligned} \forall x \exists y\ \varphi(x, y)) &\equiv \mathbf{True}\ \text{(Since we are defining } \mathcal{M} \text{ over } \mathbb{N}) \\ \varphi(x, f(x)) = \varphi(x, x) &\equiv \mathbf{False} \\ (8) : \mathbf{True} &\models \mathbf{False} \end{aligned} \tag{9}$$

Which is a contradiction hence our counter assumption is wrong and the formula is not valid.

part 3 Show:

$$(\forall x \exists y\ \varphi(x, y)) \nvdash (\forall x\ \varphi(x, f(x))) \tag{10}$$

Solution. The essens of the Soundness and Completeness theorem (short form) states that for all wff. ϕ and ψ, $\psi \vdash \phi$ iff $\psi \models \phi$. Let:

$$\begin{aligned} \psi &= \forall x \exists y \ \varphi(x, y) \\ \phi &= \forall x \ \varphi(x, f(x)) \end{aligned} \tag{11}$$

But we just showd in part (b) that $\psi \not\models \phi$ hence, based on the theorem ($\Leftarrow$), $\psi \nvdash \phi$.

Problem 3. [LCS, page 163], Exercise 2.4.5.

Solution. **(a)**
The answer is No.
Consider this example: $(b, a) \in R^{\mathcal{M}}$, then placing it in the FO wff, $\forall x \forall y \exists z(R(x, y) \rightarrow R(y, z))$, we get: $\exists z(R(b, a) \rightarrow R(a, z))$ while there is no $(a, *) \in \mathcal{M}$ with $* \in A$. Hence we provided a counter example meaning that $\mathcal{M}$ does not Model ϕ.

Solution. **(b)**
The answer is Yes.
A naive way to justify is to consider all possible choices of x and y and determine the existence of z, but to make the solution shorter, we can say semantically speaking, we can consider this nice order of the elements of $R^{\mathcal{M}'}{}^{:(a,b)\ (b,c)\ (c,d)}$ then picking any element as a left-hand side of the $\rightarrow$, the one to the right of it would be a valid choice for the right-hand side of $\rightarrow$ in ϕ. (Consider the first element as the right hand-side of the third element).

Problem 4. [LCS, page 163], Exercise 2.4.6.

Solution. The first thing that came to my mind for this solution was to use Prof. Kfoury's approach in today's lab (Wed, Oct. 7) by writing a simple 3 line prover9 code by giving each of the two wffs as assumptions and letting the other one as the conclusion, hoping for the SEARCH FAILED answer.

Another way is to provide counter examples, assuming this language could be defined by only two of the stated wffs:

- case 1: ϕ_1 and ϕ_2 only:
  consider the model $\mathcal{M} = (\mathbb{N}, 0, P)$ which P is a 2-arry predicate that P(x,y) returns true iff $|x - y| \leq 1$, is clearly reflexive ($|x - x| \leq 1$) and symmetric

because $|x-y| = |y-x|$. But not transitive. For example, $|1-2| \leq 1$ and $|2-3| \leq 1$ but $|1-3| \not\leq 1$

- case 2: ϕ_1 and ϕ_3 only:
  consider the model $\mathcal{M} = (\mathbb{N}, \leq)$ which is clearly reflexive $(n \leq n)$ and transitive ($(n \leq m) \wedge (m \leq r) \rightarrow n \leq r$), but not symmetric. For example, $1 \leq 2$ but $2 \not\leq 1$

- case 3: ϕ_2 and ϕ_3 only:
  Consider a model of a children of a family, and the relation of "sibling-hood", which is clearly symmetric (if a and b are siblings, so as b and a) and transitive (if a and b are siblings and, b and c are also siblings, then a and c are siblings), but not reflexive because no one is a sibling of himself(herself).

Problem 5.

Solution.

Code:
`https://github.com/ro0zkhosh/CS511/blob/master/HW5/hw05_non_abelian.in`

The answer is 6. We define an abelian group (not non-abelian) and use the counter-example finding super power of mace4, to find the smallest example which is **not** abelian. Here'r the output of mace4 confirming 6 is the smallest:

```
=== Mace4 starting on domain size 2. ===

=== Mace4 starting on domain size 3. ===

=== Mace4 starting on domain size 4. ===

=== Mace4 starting on domain size 5. ===

=== Mace4 starting on domain size 6. ===
```

Group Multiplication Tables

If there are n elements in a group G, and all of the possible n^2 multiplications

of these elements are known, then this group G is unique and we can write all these n^2 multiplications in a table called group multiplication table.

m	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	0	3	2	5	4
2	2	4	0	5	1	3
3	3	5	1	4	0	2
4	4	2	5	0	3	1
5	5	3	4	1	2	0

Problem 5.

Solution.

Part 1:
`https://github.com/ro0zkhosh/CS511/blob/master/HW5/hw05_power3_1.in`

Part 2:
`https://github.com/ro0zkhosh/CS511/blob/master/HW5/hw05_power3_2.in`