CS 511 Formal Methods for High-Assurance Software Engineering
Homework Assignment 05 - Selected Solution

Jiawen Liu

Problem 1. Given model $\mathscr{M} = \{\mathbb{N}, +, \times\}$, the wff are defined over $\mathscr{M}$ as:

1. $\phi_1(x) = \forall y.\ (x + y \approx y)$
2. $\phi_2(x) = \forall y.\ (x \times y \approx y)$
3. $\phi_3(x, y) = \exists z.\ (\phi_2(z) \wedge (x + z \approx y)$
4. $\phi_4(x, y) = \exists z.\ (\neg\phi_1(z)) \wedge (x + z \approx y)$

Problem 2.

1. $\forall x.\ \phi(x, f(x)) \vdash \forall x \exists y.\ \phi(x, y)$

	1	$\forall x.\ \phi(x, f(x))$	premise
x_0	2		fresh
	3	$\phi(x_0, f(x_0))$	(e$\forall x.$)1
	4	$\exists y.\ \phi(x_0, y)$	(i$\exists y.$)3
	5	$\forall x. \exists y.\ \phi(x, y)$	(i$\forall x.$)4

2. Let $\mathscr{M} \overset{\text{def}}{=} \{\mathbb{N}, 0, <, +\}$, $\phi(x, y) \overset{\text{def}}{=} x < y$ and $f(x) \overset{\text{def}}{=} 0$, then we have:
(1) $\forall x \exists y.\ \phi(x, y)$ is true. Since for any $x \in \mathbb{N}$, we can always find a value $y \in \mathbb{N}$ greater than x.
(2) $\forall x.\ \phi(x, f(x))$ is false. Since for any $x \in \mathbb{N}$, $x < 0$ is never ture.
From (1) and (2), we can derive that:

$$\forall x \exists y.\ \phi(x, y) \not\models \forall x.\ \phi(x, f(x))$$

3. By the soundness, we have if $\Gamma \vdash \phi$, then $\Gamma \models \phi$, where Γ be a set of WFF's and ϕ a WFF.
By the result from 2, we have $\forall x \exists y.\ \phi(x, y) \not\models \forall x.\ \phi(x, f(x))$. Then we can know:

$$\forall x \exists y.\ \phi(x, y) \nvdash \forall x.\ \phi(x, f(x))$$

Problem 3.

1. $\mathscr{M} \not\models \phi$
   By the definition of R, we have $R(b,c)$. While we cannot find any $z \in A$, s.t. $(c,z) \in R$.
   Then we can derive, $\forall x \forall y$ s.t. $R(x,y)$, there not always $\exists z$, s.t. $R(y,z)$.
   Then we can know: $\mathscr{M} \not\models \forall x \forall y \exists z. R(x,y) \to R(y,z)$, i.e. $\mathscr{M} \not\models \phi$.

2. $\mathscr{M} \models \phi$

   Proof. By induction on the $R(x,y)$ in $\forall x \forall y \exists z. R(x,y) \to R(y,z)$, we have following cases:

   case $R(a,b)$
   In this case, we have $x = a$ and $y = b$. Then we can easily find $z = c$ s.t. $R(b,c)$.
   So we have $R(a,b) \to R(b,c)$, i.e. $\exists z.\ R(x,y) \to R(y,z)$ proved for this case.

   case $R(b,c)$
   In this case, we have $x = b$ and $y = c$. Then we can easily find $z = b$ s.t. $R(c,b)$.
   So we have $R(b,c) \to R(c,b)$, i.e. $\exists z.\ R(x,y) \to R(y,z)$ proved for this case.

   case $R(c,b)$
   In this case, we have $x = c$ and $y = b$. Then we can easily find $z = c$ s.t. $R(b,c)$.
   So we have $R(c,b) \to R(b,c)$, i.e. $\exists z.\ R(x,y) \to R(y,z)$ proved for this case.

   Since in all of the cases, the $\exists z.\ R(x,y) \to R(y,z)$ can be proved, then we have:

   $$\forall x \forall y \exists z. R(x,y) \to R(y,z),$$

   i.e. $\mathscr{M} \models \phi$ $\square$

Problem 4.

(a) Let $A = \{a,b,c\}$.
Let $P = \{(a,a),(b,b),(c,c),(a,b),(b,a),(b,c),(c,b)\}$.
Then we have ϕ_1 and ϕ_2 is true in this model, while the transitivity (i.e., ϕ_3) is false.

(b) Let $A = \{a,b,c\}$.
Let $P = \{(a,a),(b,b),(c,c),(a,b),(a,c),(b,c)\}$.
Then we have ϕ_1 and ϕ_3 is true in this model, while the symmtric (i.e., ϕ_2) is false.

(c) Let $A = \{a,b,c\}$.
Let $P = \{(a,a),(b,b),(a,b),(b,a)\}$.
Then we have ϕ_2 and ϕ_3 is true in this model, while the reflexivity (i.e., ϕ_1) is false.

Problem 5. `https://github.com/jiawenliu/CS511/blob/master/homework/hw5/hw5-p5.in`

	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 6. `https://github.com/jiawenliu/CS511/blob/master/homework/hw5/hw5-p6-a.in` `https://github.com/jiawenliu/CS511/blob/master/homework/hw5/hw5-p6-b.in`