CS 511 Formal Methods for High-Assurance Software Engineering
Homework Assignment 04 - Selected Solution

Jiawen Liu

Problem 1.

1.
$$\Phi = (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3), \quad \Psi = \exists y (y \leftrightarrow \phi) \wedge (y \vee \psi_1) \wedge (y \vee \psi_2) \wedge (y \vee \psi_3)$$

In order to show Φ and Ψ are logically equivalent, it is equivalent to show: $\Phi \dashv\vdash \Psi$.

- $\Phi \vdash \Psi$
  By assigning $\phi = true$ in Φ, i.e., $\Phi[\phi \to true]$, we have:
  $$(true \vee \psi_1) \wedge (true \vee \psi_2) \wedge (true \vee \psi_3) = true.$$
  By applying the $\exists$ introduction rule on ϕ, we have Φ' as:
  $$\Phi' = \exists \phi \ (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3)$$
  Then, we introduce $(y \leftrightarrow \phi)$ by substitute ϕ with y in Φ', i.e., $(y \leftrightarrow \phi) \wedge \Phi'[\phi \to y]$ we can have:
  $$(y \leftrightarrow \phi) \wedge \exists y \ (y \vee \psi_1) \wedge (y \vee \psi_2) \wedge (y \vee \psi_3),$$
  which can be wrote as:
  $$\exists y \ (y \leftrightarrow \phi) \wedge (y \vee \psi_1) \wedge (y \vee \psi_2) \wedge (y \vee \psi_3) = \Psi.$$
- $\Psi \vdash \Phi$
  Since we know $\forall \phi$, $\phi \leftrightarrow \phi$, we can pick $y = \phi$ in Ψ as $\Psi[y \to \phi]$:
  $$\exists \phi \ (\phi \leftrightarrow \phi) \wedge (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3).$$
  Since $\phi \leftrightarrow \phi$ is always true, we ca have:
  $$\exists \phi \ (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3).$$
  Then, we can have the predicate $\Phi = (\phi \vee \psi_1) \wedge (\phi \vee \psi_2) \wedge (\phi \vee \psi_3)$.

2.
$$\Phi = \theta(\phi_1, \psi_1) \wedge \theta(\phi_2, \psi_2) \wedge \theta(\phi_3, \psi_3), \quad \Psi = \forall x \forall y (\vee_{i=1,2,3} (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_i)) \to \theta(x, y)$$

In order to show Φ and Ψ are logically equivalent, it is equivalent to show: $\Phi \dashv\vdash \Psi$.

- $\Phi \vdash \Psi$
  By what we proved in 1, we can introduce x, y into Φ as:
  $$\exists x \exists y\ (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \wedge \theta(x,y) \wedge \theta(\phi_2, \psi_2) \wedge \theta(\phi_3, \psi_3).$$
  By the $\wedge$e rule, we can get:
  $$\exists x \exists y\ (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \wedge \theta(x,y).$$
  We can prove following equation by natural deduction:
  $$\exists x (P(x) \wedge Q(x)) \vdash \forall x (P(x) \to Q(x))$$

	1	$\exists x (P(x) \wedge Q(x))$	premise
x_0	2		fresh
	3	$P(x_0) \wedge Q(x_0)$	assumption
	4	$P(x_0)$	assumption
	5	$Q(x_0)$	$\wedge_2$e 3
	6	$P(x_0) \to Q(x_0)$	$\to$i $4-5$
	7	$\forall x (P(x) \to Q(x))$	$\forall x$ i$2-4$

  Then, we can get:
  $$\forall x \forall y (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \to \theta(x,y).$$
  In the same way we can have
  $$\forall x \forall y (x \leftrightarrow \phi_2) \wedge (y \leftrightarrow \psi_2) \to \theta(x,y).$$
  $$\forall x \forall y (x \leftrightarrow \phi_3) \wedge (y \leftrightarrow \psi_3) \to \theta(x,y).$$
  By the Introduction rule of $\wedge$, we have:
  $$\begin{aligned}&\forall x \forall y (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \to \theta(x,y)\\ &\wedge \forall x \forall y (x \leftrightarrow \phi_2) \wedge (y \leftrightarrow \psi_2) \to \theta(x,y)\\ &\wedge \forall x \forall y (x \leftrightarrow \phi_3) \wedge (y \leftrightarrow \psi_3) \to \theta(x,y).\end{aligned}$$
  Then, it can be rewrite as:
  $$\forall x \forall y (\vee_{i=1,2,3} (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_i)) \to \theta(x,y) = \Psi.$$

- $\Psi \vdash \Phi$
  By rewrite Ψ, we have:
  $$\begin{aligned}&\forall x \forall y \Big(((x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1))\\ &\vee ((x \leftrightarrow \phi_2) \wedge (y \leftrightarrow \psi_2))\\ &\vee ((x \leftrightarrow \phi_3) \wedge (y \leftrightarrow \psi_3)) \Big) \to \theta(x,y).\end{aligned}$$
  Then it can be equivalently rewrite as:
  $$\begin{aligned}&\forall x \forall y (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \to \theta(x,y)\\ &\wedge \forall x \forall y (x \leftrightarrow \phi_2) \wedge (y \leftrightarrow \psi_2) \to \theta(x,y)\\ &\wedge \forall x \forall y (x \leftrightarrow \phi_3) \wedge (y \leftrightarrow \psi_3) \to \theta(x,y).\end{aligned}$$
  By $\forall x \forall y (x \leftrightarrow \phi_1) \wedge (y \leftrightarrow \psi_1) \to \theta(x,y)$, we can get: $\theta(\phi_1, \psi_1)$. Then, we can have:
  $$\theta(\phi_1, \psi_1) \wedge \theta(\phi_2, \psi_2) \wedge \theta(\phi_3, \psi_3)$$

Problem 2.

(a) Let θ_a be the transition relation where all the self loops are excluded defined as:

$$
\begin{aligned}
\theta_a(p_1,p_2,p_3,p_4) \overset{\text{def}}{=} \;& ((\neg p_1 \land \neg p_2) \to (\neg p_3 \land p_4)) && \text{(from } s_1\text{)}\\
& \land((\neg p_1 \land p_2) \to (p_3 \land \neg p_4)) && \text{(from } s_2\text{)}\\
& \land((p_1 \land \neg p_2) \to ((\neg p_3 \land \neg p_4) \lor (p_3 \land p_4))) && \text{(from } s_3\text{)}\\
& ((\neg p_3 \land \neg p_4) \to (p_1 \land \neg p_2)) && \text{(to } s_1\text{)}\\
& \land((\neg p_3 \land p_4) \to (\neg p_1 \land \neg p_2)) && \text{(to } s_2\text{)}\\
& \land((p_3 \land \neg p_4) \to (\neg p_1 \land p_2)) && \text{(to } s_3\text{)}\\
& \land((p_3 \land p_4) \to (p_1 \land \neg p_2)) && \text{(to } s_4\text{)}
\end{aligned}
$$

Let ϕ_{a_0} be a path from $s_1 \to s_2 \to s_3$:

$$\phi_{a_0}(p_1,\cdots,p_6) = \theta_a(p_1,p_2,p_3,p_4) \land \theta_a(p_3,p_4,p_5,p_6)$$

$n=1$**:** We have the path where all the s_1, s_2, s_3 are visited the once defined as ϕ_{a1}:

$$\phi_a(p_1,\cdots,p_8) = \texttt{init}(p_1,p_2) \land \phi_{a_0}(p_1,\cdots,p_6) \land \theta_a(p_5,p_6,p_7,p_8) \land \texttt{end}(p_7,p_8)$$

$n>1$**:** We have the path where all the s_1, s_2, s_3 are visited the same times $n>1$ defined as ϕ_a:

$$
\begin{aligned}
\phi_a(p_1,\cdots,p_{6n+2}) = \;& \texttt{init}(p_1,p_2) \land \phi_{a_0}(p_1,\cdots,p_6) \land \theta_a(p_5,p_6,p_7,p_8)\\
& \land \cdots \land \phi_{a_0}(p_{6n-6},\cdots,p_{6n}) \land \theta_a(p_{6n-1},p_{6n},p_{6n+1},p_{6n+2}) \land \texttt{end}(p_{6n+1},p_{6n+2})
\end{aligned}
$$

(b) (Either one of the possible path is correct)
Let θ_{b1} defined as the transition relation for the loop between s_2, s_3:

$$
\begin{aligned}
\theta_{b_1}(p_1,p_2,p_3,p_4) \overset{\text{def}}{=} \;& \land((\neg p_1 \land p_2) \to (p_3 \land \neg p_4)) && \text{(from } s_2\text{)}\\
& \land((p_1 \land \neg p_2) \to ((p_3 \land p_4) \lor (\neg p_3 \land p_4))) && \text{(from } s_3\text{)}\\
& \land((\neg p_3 \land p_4) \to (p_1 \land \neg p_2)) && \text{(to } s_2\text{)}\\
& \land((p_3 \land \neg p_4) \to (\neg p_1 \land p_2)) && \text{(to } s_3\text{)}\\
& \land((p_3 \land p_4) \to (p_1 \land \neg p_2)) && \text{(to } s_4\text{)}
\end{aligned}
$$

Let ϕ_{b_0} be the path representing the loop between s_2 and s_3:

$$\phi_{b_0}(p_1,\cdots,p_6) = \theta_{b_1}(p_1,p_2,p_3,p_4) \land \theta_{b_1}(p_3,p_4,p_5,p_6)$$

Then one of the valid execution paths where the s_1 is visited just once and the s_2, s_3 are visited twice is:

$$\phi_{b1}(p_1,\cdots,p_{12}) = \texttt{init}(p_1,p_2) \land \phi_{a_0}(p_1,\cdots,p_6) \land \phi_{b_0}(p_5,\cdots,p_{10}) \land \theta_{b_1}(p_9,p_{10},p_{11},p_{12}) \land \texttt{end}(p_{11},p_{12})$$

Let θ_{b2} defined as the transition relation where the s_1 is visited twice by self loop:

$$
\begin{aligned}
\theta_{b_2}(p_1,p_2,p_3,p_4) \overset{\text{def}}{=} \;& ((\neg p_1 \land \neg p_2) \to (\neg p_3 \land \neg p_4)) && \text{(from } s_1\text{)}\\
& ((\neg p_3 \land \neg p_4) \to (\neg p_1 \land \neg p_2)) && \text{(to } s_1\text{)}
\end{aligned}
$$

Then one of the valid execution paths where the s_1 is visited twice by self loop and the s_2, s_3 are visited forth is:

$$
\begin{aligned}
\phi_{b2}(p_1,\cdots,p_{18}) = \;& \texttt{init}(p_1,p_2) \land \theta_{b2}(p_1,p_2,p_3,p_4) \land \phi_{a_0}(p_3,\cdots,p_8) \land \phi_{b_0}(p_7,\cdots,p_{12})\\
& \land \phi_{b_0}(p_{11},\cdots,p_{16}) \land \phi_{b_0}(p_{15},\cdots,p_{20}) \land \theta_{b_1}(p_{19},p_{20},p_{21},p_{22}) \land \texttt{end}(p_{21},p_{22})
\end{aligned}
$$

Since θ_a from problem (a) can represent the transition relation where s_1 can be visited second time from s_3, then we have the last possible path as:

$$\begin{aligned}\phi_{b2}(p_1,\cdots,p_{18}) = \quad & \texttt{init}(p_1,p_2)\land\phi_{a_0}(p_1,\cdots,p_6)\land\theta_a(p_5,p_6,p_7,p_8)\land\phi_{a_0}(p_7,\cdots,p_{12}) \\ & \land\phi_{b_0}(p_{11},\cdots,p_{16})\land\phi_{b_0}(p_{15},\cdots,p_{20})\land\theta_{b_1}(p_{19},p_{20},p_{21},p_{22})\land\texttt{end}(p_{21},p_{22})\end{aligned}$$

This path represent s_1 is re-visited after the first time of visiting s_3. s_1 can also be visited after looping once, twice or third times on $s_2 \to s_3$ by just adjust the order or ϕ_{a_0} and θ_a.

Problem 3.

(a)
$$\exists x\, \exists y\, \exists z.\ \neg(x \leftrightarrow y) \wedge \neg(y \leftrightarrow z) \wedge \neg(z \leftrightarrow x) \wedge \forall w.\ ((w = x) \vee (w = z) \vee (w = y))$$

(b)
$$\forall w.\ \exists x\, \exists y\, \exists z.\ ((w = x) \vee (w = z) \vee (w = y))$$

(c) $n = 1$, $\theta_1 = \forall w.\ \exists x.(w \leftrightarrow x)$.
$n = k$, $\theta_k = \forall w.\ \exists x_1, \cdots, x_k \neg(x_1 \leftrightarrow x_2) \wedge \cdots \wedge \neg(x_1 \leftrightarrow x_k) \wedge \cdots \wedge \neg(x_{k-1} \leftrightarrow x_k) \wedge\ ((w = x_1) \vee \cdots \vee (w = x_k))$
Then, we have *infinite set of FO sentences which hold in a model iff the model has infinitely many distinct elements* defined as θ_∞:
$$\theta_\infty = \bigwedge_{i \geq 1} \theta_i$$

Problem 4.

(a)

$$\exists x\ (S \to Q(x)) \vdash S \to \exists x\ Q(x)$$

	1	$\exists x\ (S \to Q(x))$	premise
x_0	2		fresh
	3	$S \to Q(x_0)$	assumption
	4	S	assumption
	5	$Q(x_0)$	$\to$e 3,4
	6	$\exists x\ Q(x)$	$\exists x$ i 5
	7	$S \to \exists x\ Q(x)$	$\to$i 4 − 6
	8	$S \to \exists x\ Q(x)$	$\exists x$ e 1,2 − 7

(b)

$$S \to \exists x\ Q(x) \vdash \exists x\ (S \to Q(x))$$

	1	$S \to \exists x\ Q(x)$	premise
	2	S	assumption
	3	$Q(x)$	$\to$e 1,2
x_0	4		fresh
	5	$Q(x_0)$	assumption
	6	$Q(x_0)$	$\exists x$ e 3,4 − 5
	7	$S \to Q(x_0)$	$\to$i 2 − 6
	8	$\exists x\ (S \to Q(x))$	$\exists x$ i 7

(c)

$$\exists x\ P(x) \to S \vdash \forall x\ (P(x) \to S)$$

	1	$\exists x\ P(x) \to S$	premise
x_0	2		fresh
	3	$P(x_0)$	assumption
	4	$\exists x\ P(x)$	$\exists x$ i 3
	5	S	$\to$e 1,4
	6	$P(x_0) \to S$	$\to$i 3,4 − 5
	7	$\forall x\ (P(x) \to S)$	$\forall x$ i 2 − 6

(d)

$$\forall x\ P(x) \to S \vdash \exists x\ (P(x) \to S)$$

	1	$\forall x\ P(x) \to S$	premise
	2	$\neg(\exists x\ (P(x) \to S))$	assumption
x_0	3		fresh
	4	$\neg P(x_0)$	assumption
	5	$P(x_0)$	assumption
	6	$\bot$	$\neg$e $4,5$
	7	S	$\bot$e 6
	8	$P(x_0) \to S$	$\to$i $5-7$
	9	$\exists x\ (P(x) \to S)$	$\exists x$ i 8
	10	$\bot$	$\neg$e $2,9$
	11	$\neg\neg P(x_0)$	$\neg$i $4-10$
	12	$P(x_0)$	$\neg\neg$e 11
	13	$\forall x\ P(x)$	$\forall x$ i 12
	14	S	$\to$e $1,13$
	15	$P(x_0)$	assumption
	16	S	copy 14
	17	$P(x_0) \to S$	$\to$i $15-16$
	18	$\exists x\ (P(x) \to S)$	$\forall x$ i 17
	19	$\bot$	$\bot$i $2,17$
	20	$\neg\neg\exists x\ (P(x) \to S)$	$\neg$i $2-19$
	21	$\exists x\ (P(x) \to S)$	$\neg\neg$e 20

Problem 5. `https://github.com/jiawenliu/CS511/blob/master/homework/hw4/hw4-p5.py`

Problem 6. `https://github.com/jiawenliu/CS511/blob/master/homework/hw4/hw4-p6.in`