Logics of Programs	Homework 3 Solutions
CS686 Spring 2001	Tuesday, March 20, 2001

1. The direction $(\rightarrow)$ is immediate from the definition of the $\langle\ \rangle$ operator. For the direction $(\leftarrow)$, suppose $\vDash \langle\alpha\rangle p \leftrightarrow \langle\beta\rangle p$. Let $\mathfrak{K}$ be a Kripke frame and let $(s,t) \in \mathfrak{m}_{\mathfrak{K}}(\alpha)$. Construct a new Kripke frame $\mathfrak{K}'$ that is identical to $\mathfrak{K}$ except for the meaning of p, for which we define $\mathfrak{m}_{\mathfrak{K}'}(p) = \{t\}$. Since p does not occur in α or β, the meanings of α and β are not affected; thus $\mathfrak{m}_{\mathfrak{K}'}(\alpha) = \mathfrak{m}_{\mathfrak{K}}(\alpha)$ and $\mathfrak{m}_{\mathfrak{K}'}(\beta) = \mathfrak{m}_{\mathfrak{K}}(\beta)$. Since $(s,t) \in \mathfrak{m}_{\mathfrak{K}'}(\alpha)$, we have $s \in \mathfrak{m}_{\mathfrak{K}'}(\langle\alpha\rangle p)$. Since $\mathfrak{K}' \vDash \langle\alpha\rangle p \leftrightarrow \langle\beta\rangle p$, we also have $s \in \mathfrak{m}_{\mathfrak{K}'}(\langle\beta\rangle p)$, thus $(s,t) \in \mathfrak{m}_{\mathfrak{K}'}(\beta)$. Since (s,t) was arbitrary, $\mathfrak{m}_{\mathfrak{K}}(\alpha) = \mathfrak{m}_{\mathfrak{K}}(\beta)$.

2. (a) In any model $\mathfrak{K}$,

$$\begin{array}{rcll}
\mathfrak{m}_{\mathfrak{K}}(a(ba)^*) & = & \mathfrak{m}_{\mathfrak{K}}(a) \circ \bigcup_{n\geq 0}(\mathfrak{m}_{\mathfrak{K}}(b) \circ \mathfrak{m}_{\mathfrak{K}}(a))^n & \text{definition of ; and } * \\
& = & \bigcup_{n\geq 0}(\mathfrak{m}_{\mathfrak{K}}(a) \circ (\mathfrak{m}_{\mathfrak{K}}(b) \circ \mathfrak{m}_{\mathfrak{K}}(a))^n) & \text{distributivity of } \circ \text{ over } \cup \\
& = & \bigcup_{n\geq 0}((\mathfrak{m}_{\mathfrak{K}}(a) \circ \mathfrak{m}_{\mathfrak{K}}(b))^n \circ \mathfrak{m}_{\mathfrak{K}}(a)) & \text{associativity of } \circ \\
& = & (\bigcup_{n\geq 0}(\mathfrak{m}_{\mathfrak{K}}(a) \circ \mathfrak{m}_{\mathfrak{K}}(b))^n) \circ \mathfrak{m}_{\mathfrak{K}}(a) & \text{distributivity of } \circ \text{ over } \cup \\
& = & \mathfrak{m}_{\mathfrak{K}}((ab)^*a) & \text{definition of ; and } *.
\end{array}$$

   (b) We show that $\vDash \langle(a^*b)^*a^*\rangle p \rightarrow \langle(a \cup b)^*\rangle p$ and $\vDash \langle(a \cup b)^*\rangle p \rightarrow \langle(a^*b)^*a^*\rangle p$. For the former, we have $\mathfrak{m}_{\mathfrak{K}}(a) \subseteq \mathfrak{m}_{\mathfrak{K}}(a \cup b)$ and $\mathfrak{m}_{\mathfrak{K}}(b) \subseteq \mathfrak{m}_{\mathfrak{K}}(a \cup b)$. Reasoning in PDL,

$$\begin{array}{rcl}
\langle a^*b\rangle p & \leftrightarrow & \langle a^*\rangle\langle b\rangle p \\
& \rightarrow & \langle(a \cup b)^*\rangle\langle(a \cup b)^*\rangle p \\
& \rightarrow & \langle(a \cup b)^*(a \cup b)^*\rangle p \\
& \leftrightarrow & \langle(a \cup b)^*\rangle p,
\end{array}$$

thus

$$\begin{array}{rcl}
\langle(a^*b)^*a^*\rangle p & \leftrightarrow & \langle(a^*b)^*\rangle\langle a^*\rangle p \\
& \rightarrow & \langle(a \cup b)^{**}\rangle\langle(a \cup b)^*\rangle p \\
& \leftrightarrow & \langle(a \cup b)^*\rangle\langle(a \cup b)^*\rangle p \\
& \leftrightarrow & \langle(a \cup b)^*(a \cup b)^*\rangle p \\
& \leftrightarrow & \langle(a \cup b)^*\rangle p.
\end{array}$$

These arguments use the various properties of PDL listed in Axioms 5.5 p. 173 and Theorem 5.15 p. 181, as well as monotonicity of $<>$ (Corollary 5.9, p. 176).
For the latter, it suffices to show $\vDash [(a^*b)^*a^*]p \to [(a \cup b)^*]p$. Using properties of Axiom 5.5 and Theorem 5.15,

$$
\begin{aligned}
[(a^*b)^*a^*]p &\leftrightarrow [a^*]p \wedge [a^*b(a^*b)^*a^*]p \\
&\to [aa^*]p \wedge [aa^*b(a^*b)^*a^*]p \\
&\leftrightarrow [a]\,[a^*]p \wedge [a]\,[a^*b(a^*b)^*a^*]p \\
&\leftrightarrow [a]\,([a^*]p \wedge [a^*b(a^*b)^*a^*]p) \\
&\leftrightarrow [a]\,[(a^*b)^*a^*]p,
\end{aligned}
$$

$$
\begin{aligned}
[(a^*b)^*a^*]p &\to [a^*b(a^*b)^*a^*]p \\
&\leftrightarrow [a^*]\,[b]\,[(a^*b)^*a^*]p \\
&\to [b]\,[(a^*b)^*a^*]p.
\end{aligned}
$$

By Axiom 5.5(iv) and propositional reasoning,

$$[(a^*b)^*a^*]p \;\to\; [a \cup b]\,[(a^*b)^*a^*]p.$$

By the loop invariance rule (LI) on p. 182, we have

$$[(a^*b)^*a^*]p \;\to\; [(a \cup b)^*]\,[(a^*b)^*a^*]p.$$

Then by Theorem 5.15(i) and monotonicity,

$$[(a^*b)^*a^*]p \;\to\; [(a \cup b)^*]p.$$

(c) Translating to PDL, we wish to show that the two programs

$$(b?; p; (c?; q)^*; \overline{c}?)^*; \overline{b}? \tag{1}$$
$$b?; p; ((b \vee c)?; (c?; q \cup \overline{c}?; p))^*; \neg(b \vee c)? \;\cup\; \overline{b}? \tag{2}$$

are equivalent. (The trailing $\overline{b}?$ in (2) represents the phantom **else skip** clause in the outer conditional.) Unwinding (1) using Theorem 5.5(x), we get the equivalent program

$$b?; p; (c?; q)^*; \overline{c}?(b?; p; (c?; q)^*; \overline{c}?)^*; \overline{b}? \;\cup\; \overline{b}?,$$

so it suffices to show that the following two programs are equivalent:

$$(c?; q)^*; \overline{c}?(b?; p; (c?; q)^*; \overline{c}?)^*; \overline{b}? \tag{3}$$
$$((b \vee c)?; (c?; q \cup \overline{c}?; p))^*; \neg(b \vee c)? \tag{4}$$

Using (a), (3) is equivalent to

$$((c?;q)^*;\overline{c}?;b?;p)^*;(c?;q)^*;\overline{c}?;\overline{b}?$$

and using (b), this is equivalent to

$$(c?;q \cup \overline{c}?;b?;p)^*;\overline{c}?;\overline{b}?. \tag{5}$$

Now by distributivity of $\circ$ over $\cup$, (4) is equivalent to

$$((b \vee c)?;c?;q \cup (b \vee c)?;\overline{c}?;p)^*;\neg(b \vee c)?$$

and using the easily established fact that $\varphi?;\psi?$ is equivalent to $(\varphi \wedge \psi)?$, this becomes

$$(((b \vee c) \wedge c)?;q \cup ((b \vee c) \wedge \overline{c})?;p)^*;\neg(b \vee c)?,$$

which by propositional reasoning is equivalent to

$$(c?;q \cup (\overline{c} \wedge b)?;p)^*;(\overline{c} \wedge \overline{b})?.$$

Again using the fact that $\varphi?;\psi?$ is equivalent to $(\varphi \wedge \psi)?$, this is equivalent to (5), which was to be shown.

3. (a)

$$\frac{\{\varphi_1 \wedge \psi\}\ \alpha_1\ \{\psi\}, \quad \ldots, \quad \{\varphi_n \wedge \psi\}\ \alpha_n\ \{\psi\}}{\{\psi\}\ \mathbf{do}\ \varphi_1 \to \alpha_1 \mid \cdots \mid \varphi_n \to \alpha_n\ \mathbf{od}\ \{\psi \wedge \neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n\}}$$

(b) Using the encoding in PDL on p. 167 of HKT, we must show

$$\psi \to [(\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n)^*;(\neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)?]\,(\psi \wedge \neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)$$

under the assumptions

$$\varphi_i \wedge \psi \to [\alpha_i]\,\psi, \quad 1 \le i \le n.$$

Starting with the assumptions, by propositional logic, we have

$$\psi \to \varphi_i \to [\alpha_i]\,\psi, \quad 1 \le i \le n.$$

Using Axioms 5.5(vi) and (v) on p. 173, we have

$$\psi \to [\varphi_i?;\alpha_i]\,\psi, \quad 1 \le i \le n.$$

Again by propositional logic, we have

$$\psi \to [\varphi_1?;\alpha_1]\,\psi \wedge \cdots \wedge [\varphi_n?;\alpha_n]\,\psi,$$

and by Axiom 5.5(iv) we have

$$\psi \to [\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n]\,\psi.$$

Applying the loop invariance rule (LI), p. 182, we obtain

$$\psi \to [(\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n)^*]\,\psi. \tag{6}$$

We also have

$$\psi \to (\neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n) \to (\psi \wedge \neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)$$

by propositional reasoning. It follows from Axiom 5.5(vi) that

$$\psi \to [(\neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)?]\,(\psi \wedge \neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n).$$

Combining this with (6) and using monotonicity of $[\;]$ (Theorem 5.7(iii), p. 175), we have

$$\psi \to [(\varphi_1?;\alpha_1 \cup \cdots \cup \varphi_n?;\alpha_n)^*]\,[(\neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n)?]\,(\psi \wedge \neg\varphi_1 \wedge \cdots \wedge \neg\varphi_n),$$

and the desired conclusion follows from Axiom 5.5(v).

4. The map

$$\mathit{ends} : X \quad \mapsto \quad \{(\mathbf{first}(\sigma), \mathbf{last}(\sigma)) \mid \sigma \in X\}$$

from sets of traces on K to binary relations on K maps $\mathrm{tr}_{\mathfrak{K}}(\alpha)$ to $\mathfrak{m}_{\mathfrak{K}}(\alpha)$ and $\mathrm{tr}_{\mathfrak{K}}(\varphi)$ to $\mathfrak{m}_{\mathfrak{K}}(\varphi)$. This can be shown easily by induction on syntax, using the fact that *ends* commutes with the operators $\cup$ and $\circ$ on sets of traces and binary relations. It follows that a PDL formula is valid over relational models iff it is valid over trace models.