Logics of Programs	**Homework 4 Solutions**
CS686 Spring 2001	**Friday, April 20**

1. We wish to give a proof in KAT that the following statements are equivalent:

   (a) $pb = bp$

   (b) $p\overline{b} = \overline{b}p$

   (c) $bp\overline{b} + \overline{b}pb = 0$.

   By symmetry, it suffices to show the equivalence of (a) and (c). Assuming (a), we have

   $$bp\overline{b} + \overline{b}pb \quad = \quad pb\overline{b} + \overline{b}bp \quad = \quad p0 + 0p \quad = \quad 0.$$

   Conversely, assuming (c), we have $bp\overline{b} = \overline{b}pb = 0$. Then

   $$\begin{array}{rclclclcl} pb & = & (b+\overline{b})pb & = & bpb + \overline{b}pb & = & bpb + 0 & = & bpb, \\ bp & = & bp(b+\overline{b}) & = & bpb + bp\overline{b} & = & bpb + 0 & = & bpb; \end{array}$$

   therefore $pb = bp$.

2. (a) The direction ($\Rightarrow$) holds in any Kleene algebra: if $p \leq q$ and $q = 0$, then $p = 0$ follows from transitivity of $\leq$. The other direction does not hold. Let q be an atomic program and let $p = qq$. Certainly $q = 0 \to qq = 0$ in any relational model, but this does not imply that $qq \leq q$. For example, take the states to be $\{0, 1\}$ and interpret q as the relation $\{(0,1),\ (1,0)\}$.

   (b) Suppose $\mathsf{REL} \not\models p \leq q$. Let K be a relational model with $(s,t) \in \mathfrak{m}_K(p) - \mathfrak{m}_K(q)$. Reinterpret u and v so that $\mathfrak{m}_K(u) = (s,s)$ and $\mathfrak{m}_K(v) = (t,t)$. This can be done without changing the interpretation of p or q by the assumption that neither u nor v occurs in p or q. Then $\mathfrak{m}_K(upv) = \{(s,t)\}$ but $\mathfrak{m}_K(uqv) = \varnothing$, so $K \not\models uqv = 0 \to upv = 0$.

   The converse follows immediately from the transitivity of $\leq$.

3. We wish to show that the following μ-formulas are equivalent:

   (a) $\mu X.\mu Y.\varphi$

   (b) $\mu Y.\mu X.\varphi$

   (c) $\mu Z.\varphi[X/Z][Y/Z]$.

By symmetry, it suffices to show the equivalence of (a) and (c).

Using the De Morgan laws $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$ and $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$, the modal duality laws $\neg\mathtt{<}\alpha\mathtt{>}\varphi \equiv \mathtt{[}\alpha\mathtt{]}\neg\varphi$ and $\neg\mathtt{[}\alpha\mathtt{]}\varphi \equiv \mathtt{<}\alpha\mathtt{>}\neg\varphi$, the μ/ν duality laws $\neg\mu X.\varphi \equiv \nu X.\neg\varphi[X/\neg X]$ and $\neg\nu X.\varphi \equiv \mu X.\neg\varphi[X/\neg X]$, and double negation law $\neg\neg\varphi \equiv \varphi$, we can move all negations inward so that they only appear applied to atomic propositions. This is called *positive form*.

Recall the two μ-rules

(i) $\mu X.\varphi \equiv \varphi[X/\mu X.\varphi]$

(ii) $\dfrac{\varphi[X/\psi] \to \psi}{\mu X.\varphi \to \psi}$

First we show the implication

$$\mu X.\mu Y.\varphi \quad\to\quad \mu Z.\varphi[X/Z, Y/Z].$$

By rule (ii), it suffices to show

$$\mu Y.\varphi[X/\mu Z.\varphi[X/Z, Y/Z]] \quad\to\quad \mu Z.\varphi[X/Z, Y/Z].$$

Again by rule (ii), it suffices to show

$$\varphi[X/\mu Z.\varphi[X/Z, Y/Z]][Y/\mu Z.\varphi[X/Z, Y/Z]] \quad\to\quad \mu Z.\varphi[X/Z, Y/Z].$$

But this is equivalent to

$$\varphi[X/\mu Z.\varphi[X/Z, Y/Z], Y/\mu Z.\varphi[X/Z, Y/Z]] \quad\to\quad \mu Z.\varphi[X/Z, Y/Z],$$

which is just an instance of rule (i).

For the other direction

$$\mu Z.\varphi[X/Z, Y/Z] \quad\to\quad \mu X.\mu Y.\varphi,$$

by rule (ii) it suffices to show

$$\varphi[X/\mu X.\mu Y.\varphi, Y/\mu X.\mu Y.\varphi] \quad\to\quad \mu X.\mu Y.\varphi.$$

But by two applications of rule (i),

$$\begin{aligned}
\mu X.\mu Y.\varphi &\equiv \mu Y.\varphi[X/\mu X.\mu Y.\varphi] \\
&\equiv \varphi[X/\mu X.\mu Y.\varphi][Y/\mu Y.\varphi[X/\mu X.\mu Y.\varphi]] \\
&\equiv \varphi[X/\mu X.\mu Y.\varphi][Y/\mu X.\mu Y.\varphi] \\
&\equiv \varphi[X/\mu X.\mu Y.\varphi, Y/\mu X.\mu Y.\varphi].
\end{aligned}$$

4. (a) If $A \mapsto \sigma[X/A](\varphi)$ is continuous, then by definition, for all chains $\mathcal{C}$,

$$\sigma[X/\bigcup \mathcal{C}](\varphi) \quad = \quad \bigcup_{A \in \mathcal{C}} \sigma[X/A](\varphi).$$

Applying this map to $\sigma(\omega X.\varphi)$,

$$\begin{aligned}
\sigma[X/\sigma(\omega X.\varphi)](\varphi) &= \sigma[X/\bigcup_{n<\omega} \sigma(nX.\varphi)](\varphi) \\
&= \bigcup_{n<\omega} \sigma[X/\sigma(nX.\varphi)](\varphi) \\
&= \bigcup_{n<\omega} \sigma((n+1)X.\varphi) \\
&= \sigma(\omega X.\varphi).
\end{aligned}$$

Thus $\sigma(\omega X.\varphi)$ is a fixpoint.

(b) ($\Rightarrow$) Since $\sigma(\mu X.\mathtt{[}a\mathtt{]}X) = \bigcup_\alpha \sigma(\alpha X.\mathtt{[}a\mathtt{]}X)$, it suffices to show for all α that if $s \in \sigma(\alpha X.\mathtt{[}a\mathtt{]}X)$ then there are no infinite a-paths out of s. We show this by transfinite induction. Using the fact that for all ordinals α, limit or successor,

$$\sigma(\alpha X.\mathtt{[}a\mathtt{]}X) \quad = \quad \bigcup_{\beta<\alpha} \sigma((\beta+1)X.\mathtt{[}a\mathtt{]}X), \tag{1}$$

we have

$$\begin{aligned}
&\sigma(\alpha X.\mathtt{[}a\mathtt{]}X) \\
&\quad = \bigcup_{\beta<\alpha} \sigma((\beta+1)X.\mathtt{[}a\mathtt{]}X) \\
&\quad = \bigcup_{\beta<\alpha} \sigma[X/\sigma(\beta X.\mathtt{[}a\mathtt{]}X)](\mathtt{[}a\mathtt{]}X) \\
&\quad = \bigcup_{\beta<\alpha} \{s \mid \forall t\ (s,t) \in \mathfrak{m}_K(a) \ \Rightarrow\ t \in \sigma(\beta X.\mathtt{[}a\mathtt{]}X)\} \\
&\quad \subseteq \bigcup_{\beta<\alpha} \{s \mid \forall t\ (s,t) \in \mathfrak{m}_K(a) \ \Rightarrow\ \text{there are no infinite } a\text{-paths out of } t\} \\
&\quad = \{s \mid \forall t\ (s,t) \in \mathfrak{m}_K(a) \ \Rightarrow\ \text{there are no infinite } a\text{-paths out of } t\} \\
&\quad = \{s \mid \text{there are no infinite } a\text{-paths out of } t\}.
\end{aligned}$$

($\Leftarrow$) Suppose that there are no infinite a-paths out of s in the model K. Then the relation

$$R \quad \stackrel{\text{def}}{=} \quad \{(u,v) \in \mathfrak{m}_K(a) \mid (s,u) \in \mathfrak{m}_K(a^*)\}$$

(or rather, its converse) is well-founded. We prove by well-founded induction on this relation that if $(s,u) \in \mathfrak{m}_K(a^*)$, then $u \in \sigma(\mu X.[a]X)$. Suppose $(s,u) \in \mathfrak{m}_K(a^*)$. For any v such that $(u,v) \in \mathfrak{m}_K(a)$, we have $(u,v) \in R$, therefore by the induction hypothesis, $v \in \sigma(\mu X.[a]X)$. Since v was arbitrary, $u \in \sigma[X/\sigma(\mu X.[a]X)]([a]X) = \sigma(\mu X.[a]X)$.

(c) Let κ be a sufficiently large ordinal, and consider the Kripke frame with states $\{\alpha \mid \alpha < \kappa\}$ and a-transitions $\{(\alpha,\beta) \mid \beta < \alpha\}$. We prove by transfinite induction that for all ordinals α, β with $\beta < \kappa$ and all σ,

$$\beta \in \sigma(\alpha X.[a]X) \quad \Leftrightarrow \quad \beta < \alpha.$$

Using (1), we have

$$\begin{aligned}
\beta \in \sigma(\alpha X.[a]X) \quad &\Leftrightarrow \quad \beta \in \bigcup_{\gamma<\alpha} \sigma((\gamma+1)X.[a]X) \\
&\Leftrightarrow \quad \exists\gamma < \alpha \quad \beta \in \sigma((\gamma+1)X.[a]X) \\
&\Leftrightarrow \quad \exists\gamma < \alpha \quad \beta \in \sigma[X/\sigma(\gamma X.[a]X)]([a]X) \\
&\Leftrightarrow \quad \exists\gamma < \alpha \quad \forall\delta < \beta \quad \delta \in \sigma(\gamma X.[a]X) \\
&\Leftrightarrow \quad \exists\gamma < \alpha \quad \forall\delta < \beta \quad \delta < \gamma \qquad \text{induction hypothesis} \\
&\Leftrightarrow \quad \exists\gamma < \alpha \quad \beta \leq \gamma \\
&\Leftrightarrow \quad \beta < \alpha.
\end{aligned}$$

5. Let $a = a_1 \cup \cdots \cup a_n$ and $a^+ = aa^*$. An infinite path is fair with respect to the i^{th} resource if either

- p_i is false at infinitely many states along the path, indicating that the i^{th} request is disabled infinitely often, or
- a_i labels infinitely many edges along the path, indicating that the i^{th} request is satisfied infinitely often;

equivalently, if the path is of the form $(a^+;(a_i \cup \neg p_i?))^\omega$. There is an infinite path of this form starting a given state if that state satisfies

$$\textbf{repeat}\,(a^+;(a_i \cup \neg p_i?)).$$

Similarly, an infinite path is fair with respect to all n resources iff it is of the form

$$(a^+;(a_1 \cup \neg p_1?);a^+;(a_2 \cup \neg p_2?);\cdots;a^+;(a_n \cup \neg p_n?))^\omega.$$

The order of the $a_i \cup \neg p_i?$ does not matter, since all of them have to occur infinitely often. Thus there is an infinite path of this form starting a given state if that state satisfies

$$\textbf{repeat}\,(a^+;(a_1 \cup \neg p_1?);a^+;(a_2 \cup \neg p_2?);\cdots;a^+;(a_n \cup \neg p_n?)).$$

Expressed in the μ-calculus, this is

$$\nu X.\texttt{<}a^+;(a_1 \cup \neg p_1?);a^+;(a_2 \cup \neg p_2?);\cdots;a^+;(a_n \cup \neg p_n?)\texttt{>}X.$$

The program is fairly terminating from a given state iff there are no infinite paths starting at that state that are fair with respect to all n resources; that is, if the state satisfies

$$\mu X.\texttt{[}a^+;(a_1 \cup \neg p_1?);a^+;(a_2 \cup \neg p_2?);\cdots;a^+;(a_n \cup \neg p_n?)\texttt{]}X.$$

We can get rid of the program operators $^+$, ?, $\cup$, and ; if we like, as shown in class.