Models of Computation

Written Exam on June 6, 2013

(First part: Exercises 1 and 2, 90 minutes   Second part: Exercises 3, 4 and 5, 90 minutes)
(Previous TSD students: Exercises 1, 2 and 3, 120 minutes)

Exercise 1 (7)

Given the IMP command

$$w = \textbf{while } x \neq 0 \textbf{ do } (y := y + 2x \ ; \ x := x - 1)$$

prove that, for every $\sigma, \sigma' \in \Sigma$,

$$\langle w, \sigma \rangle \to \sigma' \ \text{ implies } \ \sigma(x) \geq 0 \ \wedge \ \sigma'(y) = \sigma(y) + (\sigma(x)+1)^2 - (\sigma(x)+1)$$

while $\sigma(x) < 0 \Rightarrow \langle w, \sigma \rangle \not\to$.

Exercise 2 (8)

Given a set U, its *totally ordered subsets* (TOS) are defined as the pairs $(S, \leq)$ where $S \subseteq U$ and $\leq$ a *total* ordering on S, namely $\leq$ is a partial ordering on S with, in addition, $\forall s_1, s_2 \in S.\ s_1 \leq s_2 \vee s_2 \leq s_1$. On TOSes, a relation $\sqsubseteq$ is defined as $(S_1, \leq_1) \sqsubseteq (S_2, \leq_2)$ iff $S_1 \subseteq S_2$ and $\leq_1 \subseteq \leq_2$. Prove that TOSes with $\sqsubseteq$ form a complete partial ordering with bottom. Given two TOSes, their lub (least upper bound) and their glb (greatest lower bound) are always defined? If not, give counterexamples.

Exercise 3 (5)

Modify the denotational semantics of HOFL for the conditional statement as follow:

$$[\![\textbf{if } t_0 : int \textbf{ then } t_1 : \tau \textbf{ else } t_2 : \tau]\!]\rho = Condd([\![t_0]\!]\rho, [\![t_1]\!]\rho, [\![t_2]\!]\rho) \text{ where}$$
$$Condd(z_0, z_1, z_2) \stackrel{def}{=} if\, z_0 = \lfloor 0 \rfloor \text{ or } z_1 = z_2 \text{ then } z_1 \text{ else if } z_0 = \lfloor n \rfloor,\ n \neq 0 \text{ then } z_2 \text{ else } \perp_{(V_\tau)_\perp}.$$

Prove that if $\tau = int$ than $Condd$ is monotone continuous, while if, e.g., $\tau = int * int$ then $Condd$ is not monotone. (Hint: Take $t_1 = \textbf{if } t_\perp \textbf{ then } (0, t_\perp) \textbf{ else } (0, t_\perp)$ and $t_2 = \textbf{if } t_\perp \textbf{ then } (0,0) \textbf{ else } (0, t_\perp)$, where $t_\perp = rec\ xint.x$.) Explain why the counterexample does not apply when $\tau = int$.

Exercise 4 (5)

Consider the π-calculus agent $P = !((y)\overline{x}y.!(\overline{x}y.nil))$, give the proof of its first transition and describe informally its behavior. Finally define its *trace semantics* namely the set $\{\alpha_1\alpha_2 \ldots \alpha_n \mid \exists Q.P \xrightarrow{\alpha_1}\xrightarrow{\alpha_2} \ldots \xrightarrow{\alpha_n} Q\}$.

Exercise 5 (5)

A *DT Markow circle* is a DTMC consisting of a family $S = \{s_i\}_{i=1,\ldots,n}$ of states. The transitions are as follows, for $i = 1, \ldots, n-1$:

$$s_i \xrightarrow{a_i} s_{i+1} \qquad s_i \xrightarrow{1-a_i} s_i \qquad s_n \xrightarrow{a_n} s_1 \qquad s_n \xrightarrow{1-a_n} s_n$$

Prove for which values of the parameters Markov circles are ergodic, and find the steady state probabilities of all the states. Finally, assume that $a_i = a$, $i = 1, \ldots n$, and define all possible partitions (lumpings), different from $\{S\}$, which are bisimulations and draw the corresponding DTMCs.

MOD – Written Exam on June 6, 2013

Exercise 1

Proof by special rule induction $P(\langle w,\sigma\rangle \to \sigma') \overset{def}{=} \sigma(x) \geq 0$

$\sigma'(y) = \sigma(y) + (\sigma(x)+1)^2 - \sigma(x) - 1$

$$\frac{\langle x \neq 0, \sigma\rangle \to false}{\langle w,\sigma\rangle \to \sigma}$$

$\sigma(x) = 0$

$\sigma(x) \overset{?}{\geq} 0$

$\sigma(y) = \sigma(y) + 1 - 1 = \sigma(y)$ QED.

$$\frac{\langle x\neq 0,\sigma\rangle \to true \quad \langle y := y+2x; x := x-1, \sigma\rangle = \sigma'' \quad \langle w,\sigma''\rangle \to \sigma'}{\langle w,\sigma\rangle \to \sigma'}$$

$\sigma(x) \neq 0 \quad \sigma'' = \sigma[\sigma(y) + 2\sigma(x)/y, \ \sigma(x)-1/x]$

$\sigma''(x) \geq 0 \quad \sigma'(y) = \sigma''(y) + (\sigma''(x)+1)^2 - \sigma''(x) - 1$

$\sigma(x) \overset{?}{\geq} 0 \qquad \sigma''(x) = \sigma(x) - 1 \qquad \sigma(x) = \sigma''(x) + 1 \geq 0$ QED

$\sigma'(y) \overset{?}{=} \sigma(y) + (\sigma(x)+1)^2 - \sigma(x) - 1$

$$\begin{aligned}\sigma'(y) &= \sigma(y) + 2\sigma(x) + (\sigma(x) - 1 + 1)^2 - (\sigma(x) - 1) - 1 \\ &= \sigma(y) + 2\sigma(x) + (\sigma(x)+1)^2 - 2(\sigma(x)+1) + 1 - \sigma(x) \\ &= \sigma(y) + (\sigma(x)+1)^2 - \sigma(x) - 1 \qquad \text{QED.}\end{aligned}$$

We prove $\langle w,\sigma\rangle \not\to$ if $\sigma(x) < 0$ with the rule:

$$\frac{\sigma \in S \quad \forall \sigma' \in S.\ \langle c,\sigma'\rangle \to \sigma'' \Rightarrow \sigma'' \in S \quad \forall \sigma' \in S. \langle b,\sigma'\rangle \to true}{\langle w,\sigma\rangle \not\to}$$

where $S = \{\sigma \mid \sigma(x) < 0\}$. In fact, $\sigma(x) < 0 \Rightarrow \sigma(x) - 1 < 0$

Exercise 2

We prove $\sqsubseteq$ is a partial ordering.

$(S,\leq)\sqsubseteq(S,\leq) \iff S\subseteq S$ and $\leq\ \subseteq\ \leq$ obvious

$$\left.\begin{array}{l}(S_1,\leq_1)\sqsubseteq(S_2,\leq_2) \iff S_1\subseteq S_2 \quad \leq_1\subseteq\leq_2\\ (S_2,\leq_2)\sqsubseteq(S_1,\leq_1) \iff S_2\subseteq S_1 \quad \leq_2\subseteq\leq_1\end{array}\right\} \begin{array}{l}S_1=S_2\\ \leq_1=\leq_2 \quad \text{QED}\end{array}$$

$$\left.\begin{array}{l}(S_1,\leq_1)\sqsubseteq(S_2,\leq_2) \iff S_1\subseteq S_2 \quad \leq_1\subseteq S_2\\ (S_2,\leq_2)\sqsubseteq(S_3,\leq_3) \iff S_2\subseteq S_3 \quad \leq_2\subseteq S_3\end{array}\right\} \begin{array}{l}S_1\subseteq S_3\\ \leq_1\subseteq\leq_3\\ (S_1,\leq_1)\sqsubseteq(S_3,\leq_3) \quad \text{QED}\end{array}$$

With bottom.

$(\emptyset,\emptyset)$ is the smallest element. It is a total ordering: $\forall s_1,s_2.\ s_1\leq s_2 \vee s_2\leq s_1$: quantification is vacuum.

Complete PO

$(S_0,\leq_0)\sqsubseteq(S_1,\leq_1)\sqsubseteq\cdots$ has a lub $\left(\bigcup S_i, \bigcup\leq_i\right)=(S',\leq)$

We must prove that S' is a total ordering.

We assume $s_1,s_2\in S'$ and we must prove that $s_1\leq s_2$ or $s_2\leq s_1$. Assume that for some K $s_1,s_2\in S'_K$ and either $s_1\leq_K s_2$ or $s_2\leq_K s_1$. Since $\leq$ is larger than $\leq_K$, we will also have $s_1\leq s_2$ or $s_2\leq s_1$.

Neither lubs nor glb are always defined

Example: $U=\{a,b\}$ $S_1=(\{a\},\{(a,a)\})$ $S_2=(\{b\},\{(b,b)\})$

Two possibilities: $S_{lub}=(\{a,b\},\{(a,a),(b,b),(a,b)\})$ S'_{lub} with (b,a)

Similarly, taking the glbs of S_{lub} and S'_{lub} you get either S_1 or S_2

Exercise 3

- **Case $\tau = int$**

Function Condd is continuous in every argument

Take z_0. Then the domain is flat and it is enough to prove monotonicity

Two cases:

- $z_1 = z_2 = \bar{z}$. Then function $Cond(z_0, \bar{z}, \bar{z})$ is a constant with z_0
- $\perp_{N_\perp} \sqsubseteq \lfloor 0 \rfloor$ and $z_1 \neq z_2$. Then $Cond(\perp_{N_\perp}, z_1, z_2) \sqsubseteq Cond(\lfloor 0 \rfloor, z_1, z_2)$ is obvious since $Cond(\perp_{N_\perp}, z_1, z_2) = \perp_{N_\perp}$
- $\perp_{N_\perp} \sqsubseteq \lfloor n \rfloor$ similarly

Take z_1. Again the domain is flat $\to$ monotonicity

cases

- $z_0 = \perp_{N_\perp}$ $z_2 = \perp_{N_\perp}$ Then $Condd(z_0, z_1, z_2)$ is the constant $\perp_{N_\perp}$
- $z_0 = \perp_{N_\perp}$ $z_2 = \lfloor n \rfloor$ Then $Condd(z_0, z_1, z_2) =$ if $z_1 = \lfloor n \rfloor$ then $\lfloor n \rfloor$ else $\perp_{N_\perp}$, OK
- $z_0 = \lfloor 0 \rfloor$ Then $Condd(z_0, z_1, z_2)$ is the identity
- $z_0 = \lfloor n \rfloor$ $n \neq 0$ then $Condd(z_0, z_1, z_2)$ is the constant z_2

Take z_2. Similarly to z_1

- **Case $\tau = int * int$**

Counterexample : $[\![t_1]\!]\rho = Condd([\![rec\ x.x]\!]\rho, [\![(0, rec\ x.x)]\!]\rho, [\![(0, rec\ x.x)]\!]\rho)$
$= Condd(\perp_{N_\perp}, \lfloor(0, \perp_{N_\perp})\rfloor, \lfloor(0, \perp_{N_\perp})\rfloor) = \lfloor(0, \perp_{N_\perp})\rfloor$

$[\![t_2]\!]\rho = Condd(\perp_{N_\perp}, \lfloor(0,0)\rfloor, \lfloor(0, \perp_{N_\perp})\rfloor) = \perp_{(V_{int * int})_\perp}$

Thus while $[\![(0, rec\ x.x)]\!]\rho \sqsubseteq [\![(0,0)]\!]\rho$ we have $[\![t_1]\!]\rho \not\sqsubseteq [\![t_2]\!]\rho$.

Here $\perp_{(V_{int*int})_\perp} \sqsubseteq \lfloor(0, \perp_{N_\perp})\rfloor \sqsubseteq \lfloor(0,0)\rfloor$ while $\lfloor n \rfloor \sqsubseteq d$ implies $d = \lfloor n \rfloor$.

Exercise 4

$$!((y)\overline{x}y.!(\overline{x}y.nil)) \xrightarrow{\alpha} Q \longleftarrow P \mid (y)\overline{x}y.!(\overline{x}y.nil) \xrightarrow{\alpha} Q \Leftarrow$$

$$\frac{Q = !P \mid Q_1}{} \quad (y)\overline{x}y.!(\overline{x}y.nil) \xrightarrow{\alpha} Q_1 \quad x \in bn(\alpha) \leftarrow$$

$$\frac{Q_1 = Q_2[w/y]}{\alpha = \overline{x}(w)} \quad \overline{x}y.!(\overline{x}y.nil) \xrightarrow{\overline{x}y} Q_2 \quad w \neq x$$

$$\frac{Q_2 = !(\overline{x}y.nil)}{} \quad \square$$

$$!((y)\overline{x}y.!(\overline{x}y.nil)) \xrightarrow{\overline{x}(w)} \underline{P} \mid !\overline{x}w.nil \quad w \neq x$$

Agent P can produce any number of processes of the form $!\overline{x}w_i.nil$, where w_i is different from x and from all w_j previously extruded. As soon as a process $!\overline{x}w_i.nil$ is created, it can start sending on channel $\overline{x}$ any number of messages $\overline{x}w_i$.

The trace semantics of P thus contains all the strings of the form

$$\overline{x}(w_0).\{xw_0\}^*.\overline{x}(w_1).\{xw_0, xw_1\}^* \cdots \quad i \neq j \Rightarrow$$

$$\cdots \overline{x}(w_n).\{xw_i\}^*_{i=1,\dots,n} \cdots \quad w_i \neq w_j \text{ and } w_i \neq x$$

where V^* is the set of all strings on V and $\{w_i\}_{i \in \omega}$ is a family of names all different and different from x.

Exercise 5

- To be ergodic we must have $a_i \neq 0$, $i=1,\dots,n$ to guarantee reachability, and should exist i with $a_i \neq 1$, otherwise all path are of length n.

- The steady state equations are

$$a_n s_n + (1-a_1) s_1 = s_1 \qquad a_n s_n = a_1 s_1$$

$$a_{i-1} s_{i-1} + (1-a_i) s_i = s_i \qquad a_{i-1} s_{i-1} = a_i s_i \qquad a_i s_i = a_j s_j \quad \forall i,j$$

$$a_{n-1} s_{n-1} + (1-a_n) s_n = s_n \qquad a_{n-1} s_{n-1} = a_n s_n$$

$$s_1 + \frac{a_1}{a_2} s_1 + \dots + \frac{a_1}{a_n} s_1 = 1 \qquad s_1 = \frac{1}{1+\frac{a_1}{a_2}+\dots+\frac{a_1}{a_n}}$$

$$s_1 = \frac{1}{a_1} \frac{1}{\frac{1}{a_1}+\frac{1}{a_2}+\dots+\frac{1}{a_n}}$$

$$\boxed{s_i = \frac{1}{a_i} \frac{1}{\frac{1}{a_1}+\frac{1}{a_2}+\dots+\frac{1}{a_n}} \qquad i=1,\dots,n}$$

- It is easy to see that contiguous states cannot be lumped together: e.g. for $\{s_1, s_2, s_3\}$ to be a bisimulation class, we must have $\alpha(s_1)([s_4]) = \alpha(s_2)([s_4]) = \alpha(s_3)([s_4])$, but the first two values are necessarily 0, while the third is a_3.

Thus the only possibility is to pick up a divisor d of n and to let $s_i \simeq s_j$ iff $i=j \mod d$. The "minimal" Markov circle is a Markov circle with n/d states and the same transition probability a.