2D1452 Formal Methods

EXAMINATION PROBLEMS
WITH PARTIAL SOLUTIONS
12 March 2007

Dilian Gurov
KTH CSC
tel: 08-790 8198

---

1. Consider the CCS process S defined by:

$$\begin{aligned} P &\triangleq a.\overline{b}.P \\ P_1 &\triangleq P[in/a, m/b] \\ P_2 &\triangleq P[m/a, out_1/b] \\ P_3 &\triangleq P[m/a, out_2/b] \\ S &\triangleq (P_1|P_2|P_3)\backslash\{m\} \end{aligned}$$

   (a) Draw the flow–graph of the system.

   (b) Derive formally the first transition of process S by referring explicitly to the CCS transition rules (see handouts). Don't forget to annotate your derivation with rule names.
   Solution: (with rule annotations omitted)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{-}{a.\overline{b}.P \xrightarrow{a} \overline{b}.P}}{P \xrightarrow{a} \overline{b}.P}}{P[in/a,m/b] \xrightarrow{in} \overline{m}.P[in/a,m/b]}}{P_1 \xrightarrow{in} \overline{m}.P[in/a,m/b]}}{(P_1|P_2|P_3) \xrightarrow{in} (\overline{m}.P[in/a,m/b]|P_2|P_3)}}{(P_1|P_2|P_3)\backslash\{m\} \xrightarrow{in} (\overline{m}.P[in/a,m/b]|P_2|P_3)\backslash\{m\}}}{S \xrightarrow{in} (\overline{m}.P[in/a,m/b]|P_2|P_3)\backslash\{m\}}$$

   (c) Explore the whole state space of S, and draw the graph of the labelled transition system induced by S.

---

2. Prove formally the following law on CCS processes:

$$P|\tau.Q \approx \tau.(P|Q)$$

Solution: Let R be a binary relation R on CCS processes defined as follows:

$$R \stackrel{\mathsf{def}}{=} id_{\mathcal{P}} \cup \{(P|\tau.Q, \tau.(P|Q)) \mid P, Q \in \mathcal{P}\} \cup \{(P|\tau.Q, P|Q) \mid P, Q \in \mathcal{P}\}$$

where $id_{\mathcal{P}}$ is the identity relation on CCS processes. Note that relation R contains all process pairs $(P|\tau.Q, \tau.(P|Q))$. We show that R is a weak bisimulation by referring explicitly to the definition of weak bisimulation (see handouts), and therefore $P|\tau.Q \approx \tau.(P|Q)$.

For pairs $(P|\tau.Q, \tau.(P|Q))$ we have:

(i) If $P|\tau.Q \xrightarrow{\alpha} P'|\tau.Q$ for some P' such that $P \xrightarrow{\alpha} P'$,
then $\tau.(P|Q) \xrightarrow{\tau} P|Q \xrightarrow{\alpha} P'|Q$
and hence $\tau.(P|Q) \stackrel{\hat{\alpha}}{\Longrightarrow} P'|Q$ and $(P'|\tau.Q, P'|Q) \in R$.
If $P|\tau.Q \xrightarrow{\tau} P|Q$,
then $\tau.(P|Q) \xrightarrow{\tau} P|Q$
and hence $\tau.(P|Q) \stackrel{\hat{\tau}}{\Longrightarrow} P|Q$ and $(P|Q, P|Q) \in R$.

(ii) If $\tau.(P|Q) \xrightarrow{\tau} P|Q$,
then $P|\tau.Q \xrightarrow{\tau} P|Q$
and hence $P|\tau.Q \stackrel{\hat{\tau}}{\Longrightarrow} P|Q$ and $(P|Q, P|Q) \in R$.

The other two cases, for pairs (P, P) and pairs $(P|\tau.Q, P|Q)$, are similar.

---

3. The Alternating Bit Protocol (ABP) is a simple data transfer protocol over an unreliable medium. It consists of three agents: a sender, a receiver and a medium. It works as follows:

   - The sender inputs a message from the environment, increases its current serial number by one (modulo 2), tags the message with this serial number (represented as a bit), transmits it to the medium, and then waits for an acknowledgement. Waiting for an acknowledgement can time out, in which case the same message is resent.
   - The medium is a half-duplex channel, that is, it can transmit messages from sender to receiver and from receiver to sender, but never in both directions at the same time. The medium can non–deterministically loose messages.
   - The receiver, upon receiving a message from the medium, compares its serial number with the one of the last message put out (that is, successfully delivered to the environment), and if the two are different (that is, a new message has been received), the message is put out. In either case, an acknowledgement is then transmitted to the medium tagged with the serial number of the last message put out.
   - The sender, upon receiving the acknowledgement, compares its serial number with the one of the last message sent, and if the two numbers coincide, the sender starts all over again; otherwise the last message is resent and the sender again waits for an acknowledgement.

   Tasks:

   (a) Model the protocol as a CCS process *ABP*, *without* modelling the transmitted messages themselves (but just the alternating bit).
   Solution:

$$
\begin{aligned}
Sender0 &\triangleq in.Sending1 \\
Sending1 &\triangleq \overline{send1}.(rack1.Sender1 + rack0.Sending1 + \tau.Sending1) \\
Sender1 &\triangleq in.Sending0 \\
Sending0 &\triangleq \overline{send0}.(rack0.Sender0 + rack1.Sending0 + \tau.Sending0)
\end{aligned}
$$

$$
\begin{aligned}
Medium \triangleq\ & send0.(\overline{rec0}.Medium + \tau.Medium) \\
+\ & send1.(\overline{rec1}.Medium + \tau.Medium) \\
+\ & sack0.(\overline{rack0}.Medium + \tau.Medium) \\
+\ & sack1.(\overline{rack1}.Medium + \tau.Medium)
\end{aligned}
$$

$$
\begin{aligned}
Receiver0 &\triangleq rec1.\overline{out}.\overline{sack1}.Receiver1 + rec0.\overline{sack0}.Receiver0 \\
Receiver1 &\triangleq rec0.\overline{out}.\overline{sack0}.Receiver0 + rec1.\overline{sack1}.Receiver1
\end{aligned}
$$

$$
ABP \triangleq (Sender0 \mid Medium \mid Receiver0)\backslash\{send0, send1, rec0, rec1, sack0, sack1, rack0, rack1\}
$$

   (b) Draw the flow–graph of your model.

   (c) Provide a meaningful service specification of the protocol by means of a CCS process *SS*.
   Solution: A meaningful service specification could be (as usual):

$$
SS \triangleq in.\overline{out}.SS
$$

   (d) Argue for correctness of your protocol model, that is, explain why $ABP \approx SS$ by describing a suitable weak bisimulation.

Solution: The labelled transition system of ABP contains one transition labelled in and one transition labelled $\overline{out}$, while all other transitions are silent. The set of states can thus be partitioned into two sets: a set T of states between $\overline{out}$ and in, and a set T' of states between in and $\overline{out}$ (note that there are no silent transitions between a state in T and a state in T' and vice versa). Then, the relation

$$R \stackrel{\mathsf{def}}{=} \{(P, SS) \mid P \in T\} \cup \{(Q, \overline{out}.SS) \mid Q \in T'\}$$

must be a weak bisimulation.

---

4. Consider the labelled transition system $\mathcal{T} = (\mathcal{S}, Act, \rightarrow)$ with states $\mathcal{S} = \{s_0, s_1\}$, actions $Act = \{a, b\}$, and transition relation $\rightarrow = \{(s_0, a, s_1), (s_1, b, s_0)\}$, and consider the modal μ-calculus formula $\Phi = \mu Z.\, (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, Z$. (See handouts.)

   (a) Compute the first three fixed–point approximants of Φ. Simplify these as much as possible.
   Solution: Here are the approximants:

$$\begin{array}{lcl} \mu Z^0.\, (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, Z & = & \mathbf{ff} \\ \mu Z^1.\, (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, Z & = & (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, \mathbf{ff} \\ & = & [a]\, \mathbf{ff} \wedge \langle b \rangle \mathbf{tt} \\ \mu Z^2.\, (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, Z & = & (\langle a \rangle \mathbf{tt} \vee \langle b \rangle \mathbf{tt}) \wedge [a]\, ([a]\, \mathbf{ff} \wedge \langle b \rangle \mathbf{tt}) \end{array}$$

   (b) Based on the formal semantics of the modal μ-calculus, explain the intuitive meaning of the formula.
   Solution: The formula expresses the property that all a–paths terminate in a state where only b is enabled, or in other words, that eventually b must be taken.

   (c) Use the proof system for the modal μ-calculus considered in class to prove $s_0 \vdash^{\mathcal{T}} \Phi$.

---

5. Consider the Hennessy-Milner logic (HML) discussed in class (see handouts). Let us extend the logic with temporal operators $\mathsf{AG}\ \Phi$ and $\mathsf{AF}\ \Phi$, with their expected meaning as in CTL (but in the context of LTSs rather than models).

   (a) Extend the proof system for HML with proof rules for the added temporal operators.
   Hint: Observe that $\mathsf{AG}\ \Phi$ can be expressed in the modal μ-calculus as $\nu Z.\, \Phi \wedge [-]\, Z$, and $\mathsf{AF}\ \Phi$ as $\mu Z.\, \Phi \vee (\langle - \rangle\, \mathbf{tt} \wedge [-]\, Z)$. You can use this, and the rules for dealing with fixed-point formulas from the proof system for the modal μ-calculus, to get inspiration for your proof rules. In particular, you could use the idea of tagging temporal formulas with sets of visited states: $\mathsf{AG}\{A\}\ \Phi$, respectively $\mathsf{AF}\{A\}\ \Phi$. Notice that you also need to slightly generalize the rules for box and diamond, so that they can be used for modalities labelled by label sets $K \subseteq Act$. Recall that '$-$' stands for 'Act' in such modalities.
   Solution: One possibility is presented by the following four rules:

$$\mathsf{UnfAG}\ \frac{s \vdash^{\mathcal{T}} \Phi \quad s \vdash^{\mathcal{T}} [-]\, \mathsf{AG}\{A, s\}\ \Phi}{s \vdash^{\mathcal{T}} \mathsf{AG}\{A\}\ \Phi}\ s \notin A \qquad \mathsf{AxAG}\ \frac{-}{s \vdash^{\mathcal{T}} \mathsf{AG}\{A\}\ \Phi}\ s \in A$$

$$\mathsf{UnfAF1}\ \frac{s \vdash^{\mathcal{T}} \langle - \rangle\, \mathbf{tt} \quad s \vdash^{\mathcal{T}} [-]\, \mathsf{AF}\{A, s\}\ \Phi}{s \vdash^{\mathcal{T}} \mathsf{AF}\{A\}\ \Phi}\ s \notin A \qquad \mathsf{UnfAF2}\ \frac{s \vdash^{\mathcal{T}} \Phi}{s \vdash^{\mathcal{T}} \mathsf{AF}\{A\}\ \Phi}\ s \notin A$$

   (b) Consider again the LTS from Problem 4. Use the proof system you developed above to prove $s_0 \vdash^{\mathcal{T}} \mathsf{AG}\ \mathsf{AF}\ \langle b \rangle\, \mathbf{tt}$.

---

6. Prove the following equivalence on LTL formulas by explicitly referring to the semantics of LTL formulas (see handouts):

$$\mathsf{G}\ \phi \equiv \neg\ (\top\ \mathsf{U}\ \neg\phi)$$

Solution: Here follows a formal proof:

$$\begin{array}{lcl}
\pi \models^{\mathcal{T}} \neg\ (\top\ \mathsf{U}\ \neg\phi) & \Leftrightarrow & \text{not } \pi \models^{\mathcal{T}} \top\ \mathsf{U}\ \neg\phi \\
& \Leftrightarrow & \text{not } \exists i \geq 0.\ (\pi^i \models^{\mathcal{T}} \neg\phi\ \wedge\ \forall j < i.\ \pi^j \models^{\mathcal{T}} \top) \\
& \Leftrightarrow & \text{not } \exists i \geq 0.\ \pi^i \models^{\mathcal{T}} \neg\phi \\
& \Leftrightarrow & \text{not } \exists i \geq 0.\ (\text{not } \pi^i \models^{\mathcal{T}} \phi) \\
& \Leftrightarrow & \forall i \geq 0.\ \pi^i \models^{\mathcal{T}} \phi \\
& \Leftrightarrow & \pi \models^{\mathcal{T}} \mathsf{G}\ \phi
\end{array}$$