**UNIVERSITY OF EDINBURGH**

**FACULTY OF SCIENCE AND ENGINEERING**

**MASTER OF SCIENCE IN COMPUTER SCIENCE**

# COMMUNICATIONS AND CONCURRENCY

**Monday 24 April 2000**

**9:30 to 11:00**

**Examiners:**

**I. Watson (External)**

**R.N. Ibbett (Chairman)**

**INSTRUCTIONS TO CANDIDATES**

**Answer any TWO questions.**

**All questions carry equal weight.**

1. This question concerns writing a CCS controller TELLER for bank teller machines. We begin with a very simplified situation where we suppose TELLER communicates with customers considered as unknown CCS agents and with a cash-supply agent, SUPPLY.

   Customers interact with the teller machines by inserting a bank card, typing a code and then requesting a sum of cash. If the code is correct, the teller machine obtains the cash from SUPPLY, gives it to the customer and returns the card; if not, the teller machine retains the card.

   (a) Draw a flow-diagram for this system and write the CCS agents TELLER and SUPPLY. The agents should be written in value-passing CCS and you can assume three value sets, Card, of cards, Code, of codes and Pound, of pounds; you will need a relation Correct(card,code) for code authorisation. Make sure your flow diagram clearly indicates agent ports, the lines between them and their names. [*7 marks*]

   (b) Translate TELLER into basic CCS and draw the (infinite!) transition diagram of the translation, using appropriate conventions. [*5 marks*]

   (c) The above version of TELLER is both unrealistic and limited. For example it is unrealistic in that there is no explicit assumption of a limit to the money supply available to SUPPLY, nor any limit to the cash that a customer can withdraw. Reimplement TELLER taking these assumptions into account. You should introduce a new agent ACCOUNTS which can communicate with TELLER concerning customers' account balances. Explain clearly any new lines needed. [*6 marks*]

   (d) Give two more ways in which the above system is either unrealistic or limited, meaning either a way the current version of TELLER works that real ones do not, or a feature of real ones that the current version lacks. Show how one of them could be overcome by writing yet another version of TELLER, explaining clearly any new agents or lines needed. [*7 marks*]

   **Note** In (c) and (d) you do not need to write out all the details of the new versions of TELLER, as long as you explain clearly the changes you made from previous versions.

2. (a) A *simple duplicator* agent $D$ in value-passing CCS has ports labelled by $a$, $\overline{b}$ and $\overline{c}$. Its behaviour is to input a boolean value (i.e. 0 or 1) at $a$ and then output it, first at $\overline{b}$ and then at $\overline{c}$; thereafter it performs no more actions.

A *simple conjunctive* agent $A$ has ports labelled by $b$, $c$ and $\overline{d}$. Its behaviour is to input boolean values $x$ and $y$ at $b$ and $c$, and then output their conjunction $x \wedge y$ at $\overline{d}$; thereafter it performs no more actions.

Define $D$ and $A$. *[2 marks]*

(b) Using equational reasoning, show that the following equation is true

$$(D \mid A)\backslash b\backslash c = a(x).\overline{d}(x).\mathbf{0}$$

(assume $a, b, c, d$ are all different).

[**Hint:** You could either work directly in value-passing CCS, or else first translate to basic CCS. ] *[4 marks]*

(c) A *repetitive* duplicator $D'$ is identical to a simple one, except that after performing the actions at $a, \overline{b}$ and $\overline{c}$ it returns to its initial state; a repetitive conjunctive agent $A'$ is defined similarly.

Give definitions of $D'$ and $A'$ in value-passing CCS. *[2 marks]*

(d) One might expect that the following equation was true

$$(D' \mid A')\backslash b\backslash c = B$$

where $B =_{\text{def}} a(x).\overline{d}(x).B$. Explain informally why that is not the case. *[2 marks]*

Give a version of the above equation in basic CCS, ignoring issues of value-passing, and prove formally that the resulting equation is not true. *[2 marks]*

(e) Change $D'$ and $A'$ to $D''$ and $A''$ by adding a synchronisation communication using a new control port $s$, so that the following equation is true

$$(D'' \mid A'')\backslash b\backslash c\backslash s = B$$

*[3 marks]*

Now prove this equation is true using equational reasoning. *[6 marks]*

(f) What equation might you expect to be true of the "reverse" combination $(A[a/d] \mid D[b'/b, c'/c])\backslash d)$? What difficulty would arise? Would the same synchronised versions as before overcome this difficulty? If not, give ones that would. *[4 marks]*

3. (a) As is well known, strong bisimulation satisfies the "logical recursion equation" that for any agents $P$ and $Q$, $P \sim Q$ holds iff, for all $\alpha$ in Act,

(i) Whenever $P \xrightarrow{\alpha} P'$ then, for some $Q'$, $Q \xrightarrow{\alpha} Q'$ and $Q' \sim P'$

and

(ii) Whenever $Q \xrightarrow{\alpha} Q'$ then, for some $P'$, $P \xrightarrow{\alpha} P'$ and $P' \sim Q'$.

Prove the first half of this, i.e. that $P \sim Q$ implies the conjunction, beginning from the definition of $\sim$ as the union of all strong bisimulation relations.

[*2 marks*]

(b) Imagine that basic CCS included—as well as the usual combinators—a unary *a-reporter* combinator $R_a$ which uses a special name $r$ to report occurrences of $a$ (it is assumed that $r$ and $a$ are different). Its transition rules are

$$\frac{P \xrightarrow{\alpha} P'}{R_a(P) \xrightarrow{\alpha} R_a(P')}$$

(for $\alpha \neq a$), and

$$\frac{P \xrightarrow{a} P'}{R_a(P) \xrightarrow{a} r.R_a(P')}$$

Show that for any agents $P$ and $Q$,

$$R_a(P + Q) \sim R_a(P) + R_a(Q)$$

and also that

$$R_a(\mathbf{0}) \sim \mathbf{0}$$

[**Hint:** Use 3(a). ] [*6 marks*]

(c) Show that $\sim$ is a congruence for $R_a$, i.e. that for any agents $P$ and $Q$, if $P \sim Q$ then $R_a(P) \sim R_a(Q)$.

[**Hint:** Find a suitable strong bisimulation. ] [*5 marks*]

(d) Show that

$$R_a(P \mid Q) \sim R_a(P) \mid R_a(Q)$$

does not always hold (use a counterexample).

[**Hint:** Choose simple $P$ and $Q$ and use the previous results (and perhaps some evident facts relating $R_a$ and prefixing) to simplify both sides. ] [*5 marks*]

*QUESTION CONTINUES ON NEXT PAGE*

(e) There is a more general $K$-*reporter* combinator $R_K$ for sets of names $K$, where each $a$ in $K$ is reported by a distinct name $r_a$. Give the transition rules for $R_K$. [*2 marks*]

Consider the assertion that for all agents $P$,

$$R_K(R_L(P)) \sim R_{(K \cup L)}(P)$$

Show this is not always true using a counterexample. What extra condition would make the assertion true? Give a strong bisimulation that could be used to show the resulting restricted assertion is true. (You may assume that the reporting names $r_a$, for $a$ in $K \cup L$, are all different and are also distinct from any of the reported names.) [*5 marks*]