UNIVERSITY OF EDINBURGH

FACULTY OF SCIENCE AND ENGINEERING

COMPUTER SCIENCE FOUR

COMMUNICATION AND CONCURRENCY

Wednesday 25 April 2001

14:00 to 15:30

Examiners:

Prof. K. Turner (External)

Prof. G. Plotkin (Chairman)

INSTRUCTIONS TO CANDIDATES

Answer any TWO questions.

All questions carry equal weight.

1. (a) What is an inference diagram for basic CCS? Give the inference diagram for the transition

$$((a.c.0 + b.0) \mid \overline{a}.d.0)\backslash a \xrightarrow{\tau} (c.0 \mid d.0)\backslash a$$

[*5 marks*]

(b) A distributed voting system consists of a *central registry* R connected to n voting stations V_i (for $i = 1, n$). To vote, a voter presents *vid*—his/her *voter identification*—at any V_i; this is then checked and, if correct, the voter can then proceed to present his/her vote to the station.

(i) Give a flow diagram for the system. On the basis of this diagram, give a CCS agent for the whole system, written in terms of constants V_i and R (for the voting stations and the central registry). [*6 marks*]

(ii) Give (value-passing) CCS definitions of the V_i and R; the code for the V_i's must be identical except for renaming. In doing this, assume that R contains a database *registry* and there is a predicate

$$Correct(registry, vid)$$

to check correctness, and a function

$$add(registry, vote)$$

which returns a new database updated by the vote. [*6 marks*]

(iii) The above system is subject to fraud. Amend it so that R detects double voting, informing the authorities, not counting the double vote and not alerting the fraudulent voter. You may assume any needed extra predicates or functions; state clearly what they are and what they mean. [*8 marks*]

2. (a) State the definition of weak bisimulation. [*5 marks*]

(b) Consider the following two place buffer, where we abstract from the values stored.

$$\begin{aligned} B &\stackrel{\text{def}}{=} \texttt{in}.B' \\ B' &\stackrel{\text{def}}{=} \texttt{in}.B'' + \overline{\texttt{out}}.B \\ B'' &\stackrel{\text{def}}{=} \overline{\texttt{out}}.B' \end{aligned}$$

It is possible to build this buffer out of cells. In this example we are interested in "lossy" cells, C and D.

$$\begin{aligned} C &\stackrel{\text{def}}{=} \texttt{in}.C' \\ C' &\stackrel{\text{def}}{=} \overline{\texttt{write}}.C + \tau.C' \end{aligned}$$

$$\begin{aligned} D &\stackrel{\text{def}}{=} \texttt{write}.D' \\ D' &\stackrel{\text{def}}{=} \overline{\texttt{out}}.D + \tau.D' \end{aligned}$$

Prove that $B \approx (C|D)\backslash\{\texttt{write}\}$. [*10 marks*]

(c) Consider the following CTL property $\Phi = [\texttt{in}]AF\langle\overline{\texttt{out}}\rangle\texttt{tt}$

i. What property does this formula express in words?
ii. Prove or disprove that $B \models \Phi$.
iii. Prove or disprove that $(C|D)\backslash\{\texttt{write}\} \models \Phi$. [*10 marks*]

3. Commercial systems involving distributed transactions utilise commit protocols to guarantee atomicity of a transaction. The definition of atomic commit is given by means of a set of axioms, which include the following.

(A1) No two participants that decide, do so differently.

(A2) If a participant decides commit then all participants voted yes.

(A3) If all participants voted yes then the decision will be to commit.

(A4) A participant is allowed to vote no.

It is common to model such a protocol as a family of participants who synchronise with a coordinator. The coordinator makes the global decision to commit or to abort in accordance with the axioms. A participant P_i can be described as follows.

$$\begin{array}{lcl} P_i & \stackrel{\text{def}}{=} & \texttt{prepare}_i.\,Vote_i \\ Vote_i & \stackrel{\text{def}}{=} & \overline{\texttt{yes}}_i.\,Wait_i + \overline{\texttt{no}}_i.P_i \\ Wait_i & \stackrel{\text{def}}{=} & \texttt{commit}_i.P_i + \texttt{abort}_i.P_i \end{array}$$

The coordinator tells P_i to prepare, and then P_i votes on the transaction (yes or no) and tells the cordinator who collects the votes, and then makes the global decision.

(a) Assume that there are two participants P_1 and P_2. Let L be the following set of actions.

$$L = \{\texttt{prepare}_i, \texttt{yes}_i, \texttt{no}_i, \texttt{commit}_i, \texttt{abort}_i \;:\; 1 \leq i \leq 2\}$$

Define an agent Co who is the coordinator such that

$$System = (P_1|P_2|Co)\backslash L$$

describes atomic commit. You should include in your definition of Co explicit observable actions $\overline{\texttt{commit}}$ and $\overline{\texttt{abort}}$, representing global commit and abort. *[12 marks]*

(b) Prove that your system obeys the axioms. Describe any assumptions you make about what it is to obey these axioms. *[8 marks]*

(c) Discuss how you might extend the definition of Co to cope with an arbitrary number of participants. You are allowed to reformulate the participants, P_i. *[5 marks]*