Concurrency and Process Algebra

Date: Tuesday 3rd June 2014
Time: 09:45 - 11:45

Please answer any THREE Questions from the FIVE Questions provided

This is a CLOSED book examination

The use of electronic calculators is NOT permitted
1. Modelling and implementing concurrent systems.

a) In the context of concurrent systems, explain briefly but clearly what is meant by the following:

   i. Mutual exclusion,  
   ii. A monitor.

Explain the mechanisms that a monitor may provide to allow controlled access by multiple processes.  

b) Consider a buffer of fixed size used for buffering between two processes, one producing items which are buffered and another consuming items from the buffer, as in the picture:

Consider a simple case of this where the two actions put and get interface between a buffer of fixed size, say 5 items, and all the data items are considered the same (i.e. we need only keep a count of the number of items in the buffer). Using an indexed process definition and guarded actions for the buffer, describe an FSP model of this system as a composite of three processes: the PRODUCER, the CONSUMER and the BUFFER.  

c) How would you modify your FSP process definitions to describe multiple versions of the producer and consumer processes accessing a single buffer?  

d) Give an implementation of the buffer, producer and consumer defined in Part (b) as three class definitions in Java. You may describe the buffer as an array of fixed size, with position nextfree as the next free slot and nextitem as the next item to be taken from the buffer. You may use arithmetic modulo the buffer size to ensure that these are positions in the buffer.  

e) Explain clearly (i) how the model and its implementation relate to the concept of a monitor, and (ii) how process interaction in your FSP model is captured in the Java implementation.
2. On FSP rules.

a) Give the inference rules for the parallel operator \(||\) in FSP. Explain clearly how synchronised and unsynchronised transitions of concurrent systems are described by these rules.  

Consider the following FSP process definitions which provide a simple model of a machine and its operator.

\[
\begin{align*}
\text{MACHINE} &= \{ \text{start} \rightarrow \text{RUNNING} \}, \\
\text{RUNNING} &= \{ \text{run} \rightarrow \text{RUNNING} \\
& \quad \quad | \text{pause} \rightarrow \text{PAUSED} \\
& \quad \quad | \text{stop} \rightarrow \text{MACHINE} \}, \\
\text{PAUSED} &= \{ \text{resume} \rightarrow \text{RUNNING} \\
& \quad \quad | \text{stop} \rightarrow \text{MACHINE} \}, \\
\text{OPERATOR} &= \{ \text{start} \rightarrow \text{OPERATOR} \\
& \quad \quad | \text{pause} \rightarrow \text{OPERATOR} \\
& \quad \quad | \text{resume} \rightarrow \text{OPERATOR} \\
& \quad \quad | \text{stop} \rightarrow \text{OPERATOR} \}.
\end{align*}
\]

\[\text{SYSTEM} = (\text{MACHINE} \ || \ | \text{OPERATOR}).\]

b) Using transition rules for FSP, provide a detailed derivation of the start transition that the SYSTEM process can make. Carefully explain the rules that you use at each step of the derivation.  

c) Further, give a derivation that, after the initial start transition, the system may then immediately execute a run transition. Again, explain the rules used at each step of your derivation.  

d) Describe precisely how a labelled transition system may be constructed from an FSP process definition using FSP rules.  

e) Use this analysis to draw a labelled transition system that corresponds to the composite FSP process SYSTEM above. You should construct a system with the minimum number of states.
3. On the equivalence of FSP processes.

a) Provide and explain a formal definition of (not an algorithm for) strong bisimilarity between two labelled transition systems, and hence define strong bisimulation for FSP processes. (3 marks)

b) By giving two example processes, show that processes may have the same set of traces but not be strongly bisimilar. Justify your answer.

Give a third FSP process that can be used to distinguish your two processes, i.e. when the third process is combined with the first two by parallel composition, different sets of traces result. (4 marks)

c) Describe an algorithm for computing whether two FSP processes are strongly bisimilar. Your description should explain clearly the steps of the algorithm. (6 marks)

d) Consider the following two FSP definitions of simplified vending machines.

\[ VM1 = (select \rightarrow (drink \rightarrow P \mid chocolate \rightarrow P)), \]
\[ \quad P = (deliver \rightarrow reset \rightarrow VM1). \]
\[ VM2 = (select \rightarrow Q), \]
\[ \quad Q = (drink \rightarrow R \mid chocolate \rightarrow deliver \rightarrow S), \]
\[ \quad R = (deliver \rightarrow reset \rightarrow VM2), \]
\[ \quad S = (reset \rightarrow select \rightarrow (drink \rightarrow deliver \rightarrow S \mid chocolate \rightarrow R)). \]

Use the algorithm you described in answer to Part (3c) above to determine whether or not the process \( VM1 \) is strongly bisimilar to \( VM2 \). (5 marks)

e) What is the minimal FSP process that is strongly bisimilar to \( VM2 \)? Justify your answer using the results of your algorithm, or otherwise. (2 marks)
4. On properties and property checking.

a) Explain what is meant by a safety property and a liveness property for a concurrent system. Give an example of a real system together with a safety property and a liveness property that are required to hold for the system. (4 marks)

b) A safety property is defined in FSP as a process definition prefixed by the keyword property, as in the example below:

\[
\text{property CYCLE\_PROPERTY = (wash \rightarrow rinse \rightarrow dry \rightarrow CYCLE\_PROPERTY).}
\]

Explain the difference between CYCLE\_PROPERTY and the process CYCLE defined below. In particular, draw the labelled transition systems for both. (2 marks)

\[
\text{CYCLE = (wash \rightarrow rinse \rightarrow dry \rightarrow CYCLE).}
\]

c) Consider the following model of a dishwasher.

\[
\begin{align*}
\text{range S} & = 0..3 \\
\text{DISHWASHER} & = (\text{on } \rightarrow \text{STATE}[0]) , \\
\text{STATE}[s:S] & = \\
& \left( \begin{array}{l}
\text{when (s==0) closedoor } \rightarrow \text{STATE}[s+1] \\
| \text{when (s==0) opendoor } \rightarrow \text{buzz } \rightarrow \text{STATE}[0] \\
| \text{when (s==1) wash } \rightarrow \text{STATE}[s+1] \\
| \text{when (s==2) pause } \rightarrow \text{PAUSED}[s] \\
| \text{when (s==2) rinse } \rightarrow \text{STATE}[s+1] \\
| \text{when (s==3) pause } \rightarrow \text{PAUSED}[s] \\
| \text{when (s==3) dry } \rightarrow \text{off } \rightarrow \text{DISHWASHER} ,
\end{array} \right) , \\
\text{PAUSED}[s:S] & = (\text{restart } \rightarrow \text{STATE}[s-1]) .
\end{align*}
\]

Draw the labelled transition system corresponding to the DISHWASHER process. (3 marks)

d) Now draw the labelled transition system corresponding to the following composite process. (5 marks)

\[
\text{DISHWASHER } || \text{ CYCLE\_PROPERTY}
\]

e) Provide an informal justification, and a counterexample execution trace, explaining why the dishwasher fails the safety property CYCLE\_PROPERTY. (4 marks)

f) Correct the definition of the dishwasher so that the desired safety property is satisfied. (2 marks)
5. Concurrency concepts.

a) Explain briefly but clearly the following concepts applied to concurrent systems. You should use illustrative examples. (4 marks)

   i) Deadlock
   ii) Livelock

b) What four conditions on a system ensure that deadlock is a possibility? Give a clear explanation of each condition. (4 marks)

c) Consider the following FSP model of two resources (a printer and a scanner), and two users.

   RESOURCE = (get -> put -> RESOURCE).
   USER1 = (printer.get -> scanner.get -> copy ->
              printer.put -> scanner.put -> USER1).
   USER2 = (scanner.get -> printer.get -> copy ->
              printer.put -> scanner.put -> USER2).
   || SYS = ( u1: USER1 || u2: USER2
              || (u1,u2)::printer:RESOURCE
              || (u1,u2)::scanner:RESOURCE ).

This model may reach deadlock.

i) Give an example of a trace to deadlock and explain the deadlock that occurs. (2 marks)

ii) Explain clearly how the model violates each of the conditions you described in answer to Part (b). (2 marks)

iii) For each of these conditions, describe a solution, i.e. describe FOUR separate modifications of the above system, each of which prevents one of the conditions holding. Your descriptions should be clearly explained in terms of access to the printer and scanner, but need not be expressed in FSP. (4 marks)

iv) Express TWO of these solutions in FSP by modifying the FSP model above. (4 marks)