

Exam Protocol Validation

VU University Amsterdam, 14 December 2009, 15:15-18:00

(At this exam, you may use copies of the slides without handwritten comments. Answers can be given in English or Dutch.)

(The exercises in this exam sum up to 90 points; each student gets 10 points bonus.)

- Given a sort $List$ over an arbitrary non-empty data domain D , with as constructors the empty list $[] : \rightarrow List$, and $in : D \times List \rightarrow List$ to insert an element from D at the beginning of a list.

Suppose that a total order $< : D \times D \rightarrow Bool$ has been imposed. Specify a non-constructor function $add : D \times List \rightarrow List$ that, given a datum d and a sorted list λ , outputs a sorted list, by placing d at the right position in λ . (8 pts)

- (a) Linearise, using the algorithm underlying `mcr1 -regular`, the μ CRL specification

$$\begin{aligned} Y(m:Nat) &= a(m) \cdot Z(S(m)) \cdot Y(S(m)) \\ Z(m:Nat) &= b(m) \cdot Z(m) + c(S(m)) \end{aligned} \quad (8 \text{ pts})$$

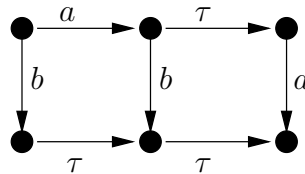
- (b) Linearise, using the algorithm underlying `mcr1`, the μ CRL specification

$$\begin{aligned} Y(m:Nat) &= a(m) \cdot Z(S(m)) \cdot Y(m) \\ Z(m:Nat) &= b(m) \cdot Z(S(m)) + c(m) \end{aligned}$$

with initial state $Y(0)$.

Would the algorithm underlying `mcr1 -regular` terminate on this specification? Explain your answer. (12 pts)

- Apply the minimization algorithm modulo branching bisimilarity to the process graph below. Describe the subsequent splits that you perform, and the results of those splits. Also draw the resulting minimized process graph.



(12 pts)

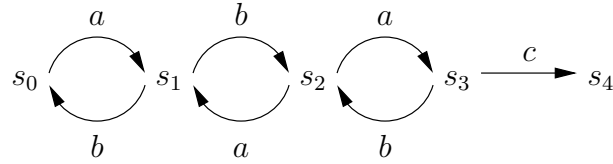
- Check for each of the following four formulas, which states in the process graph below satisfy the formula. (Explain your answers!)

(a) $\nu X. (\langle a \rangle X \vee \langle c \rangle \top)$ (3 pts)

(b) $\mu X. (\langle a \rangle X \vee \langle c \rangle \top)$ (3 pts)

(c) $\nu X. ([\langle ab \rangle^*] X)$ (5 pts)

(d) $\mu X. ([\langle ab \rangle^*] X)$ (5 pts)



5. Given the LPE

$$X(\mathsf{T}) = a \cdot X(\mathsf{F}) \qquad X(\mathsf{F}) = a \cdot X(\mathsf{T}) + \tau \cdot X(\mathsf{F})$$

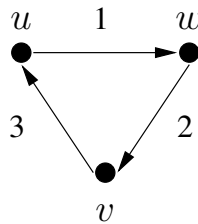
Show with the cones and foci technique that $X(\mathsf{T}) \Leftrightarrow_{rb} Y$, where $Y = a \cdot Y$. (12 pts)

6. *Leader Election Protocol:* Consider a ring network of processes. Communication is unidirectional: each process can only send messages to its clockwise neighbour. Each process has a unique identity, and there is a total ordering on the domain of identities. The process with the largest identity is elected as the leader as follows. Each process is either active or passive; initially they are all active. An active process can send out one message containing its identity. If an *active* process with identity u receives a message carrying identity v , then:

- if $u < v$, the process becomes passive, and the message is forwarded;
- if $u > v$, the process remains active, and the message is cancelled;
- if $u = v$, the process becomes the leader (i.e., it performs an action $leader(u)$).

Passive processes simply forward all incoming messages.

- (a) Give a μ CRL specification of a process in this leader election protocol, including the action declaration **act** and the communication declaration **comm**. (The data types that you use do not have to be formally specified.) Communication between processes is synchronous (i.e., you do not have to model channels as separate entities). (14 pts)
- (b) Give the initial state of the following ring network of three processes. (Apply the encapsulation operator, but not the hiding operator.) u, v, w refer to process identities, and 1,2,3 to channels.



Let $u > v > w$. Draw the process graph belonging to this network. (5 pts)

- (c) Apply the hiding operator to rename all communication actions into τ . Draw the process graph for the ring network above after minimization modulo branching bisimilarity. (3 pts)