CSL750: Foundations of Automatic Verification

I semester 2005-06
Take-home Minor Thu 22 Sep 2005 - 28 Sep 2005

---

1. Consider the following game comparing two processes P and Q. Each game consists of two "subgames". $P \overline{\sim} Q$ iff the Challenger does **not** have a winning strategy for either of the two subgames.

   subgame 1 . Repeat the following two steps until one of them cannot make a move.

      (a) Challenger makes a move on P.
      (b) Responder makes a *corresponding* move on Q

   subgame 2 Same as subgame 1 with the Challenger playing Q and responder playing P.

   (a) Show that $\overline{\sim}$ is an equivalence relation.
   (b) Show that $P \overline{\sim} Q \not\Rightarrow P \sim Q$.
   (c) Argue that $P \sim Q \Rightarrow P \overline{\sim} Q$.
   (d) If the game is considered to consist only of subgame 1 then show that the resulting relation is a preorder (i.e. it is reflexive and transitive)

2. CCS may be used to define abstract data types of various kinds.

   (a) Use (value-passing) CCS to define the behaviour of a stack of elements of an arbitrary data type of values. The actions of the stack are the usual — `empty()` to check for emptiness, `push (x)` to push an element on stack, $\overline{\texttt{pop}()}$ which removes the top element of the (nonempty) stack, and $\overline{\texttt{top(t)}}$ which outputs the value of the top element of the stack (but does not remove it!).
   (b) Now consider a Turing machine which accepts the language $\{a^n b^n c^n | n \geq 0\}$. Construct the transition table of this Turing machine. Now simulate the behaviour of this machine using the stack data type that you have defined above. Assume that the only actions that are visible for any input to the Turing machine are the actions $\overline{\texttt{accept}}$ and $\overline{\texttt{reject}}$. All other actions you define are internal to the construction.

3. For any process P, let $\mathsf{traces}(P) = \{u \in Act^* | \exists P' : P \xrightarrow{u} P'\}$.

   (a) Show that $\mathsf{traces}(P)$ is a prefix-closed set, i.e. $w \in \mathsf{traces}(P) \wedge w = uv$ implies $u \in \mathsf{traces}(P)$.
   (b) Show that $P \sim Q$ implies $\mathsf{traces}(P) = \mathsf{traces}(Q)$.
   (c) Show that $P \overline{\sim} Q$ implies $\mathsf{traces}(P) = \mathsf{traces}(Q)$.

4. (a) Prove that $FIFO_k(\varepsilon) \not\sim FIFO_m(\varepsilon)$ for all $k, m > 0$ and $k \neq m$.
   (b) **Open question! I am not sure of the answer myself!** If possible, prove that for any implementation IMP_k, $IMP_k \approx^c FIFO_k$ for corresponding sequences of values over arbitrary domains D iff $IMP_k \approx^c FIFO_k$ for sequences of values over a finite domain D' with $|D'| \geq$????. Assume that over both domains the only operation allowed is equality-checking for values in the domain. If it is not possible to prove such a result try to give an impossibility proof, or at least explain why any attempt at proving such a result is going to fail.