CS611 Midterm

Monday, 19 October 1998

1. (a) What does it mean when we say that $\{A\}c\{B\}$ is valid?

   (b) What does it mean when we say that $[A]c[B]$ is valid?

2. In the proof of $< c, \sigma > \rightarrow \sigma'$ implies $\mathcal{C}[\![c]\!]\sigma = \sigma'$, why was it important to use rule induction as opposed to structural induction on c?

3. Which of the following are CPOs? If so, is it pointed and why? If it is not a CPO, explain why, and briefly state how to make it a pointed CPO.

   (a) natural numbers with $\leq$

   (b) natural numbers with $\geq$

   (c) interval [0,1] of rationals under $\leq$

   (d) A set with one element, a, and the trivial relation $a \sqsubseteq a$

   (e) if $(A, \sqsubseteq_A)$ and $(B, \sqsubseteq_B)$ are pointed CPOs, the sum space $A + B$, where the set in this case is the disjoint union of A and B, and $\sqsubseteq_{A+B}$ is defined as: $\begin{cases} \sqsubseteq_A & \text{if both arguments were originally in } A, \\ \sqsubseteq_B & \text{if both arguments were originally in } B, \\ \text{undefined} & \text{otherwise.} \end{cases}$

   (f) if D is a CPO and E a pointed CPO, the continuous function space $[D \to E]$

4. Let D be a pointed cpo (i.e., with a least element $\perp$) and let f be a continuous function from D to D. Take $d = \texttt{lub}\{f^i(\perp) | i >= 0\}$. That is, d is the least upper bound of the chain $\{\perp, f(\perp), f(f(\perp)), ...\}$.

   (a) Show that d is a fixed point of f.

5. Consider the parallel command, $c_1||c_2$. One way to add it to IMP is by adding the following rules:

$$\texttt{skip}\,||c \rightarrow_1 c \qquad c||\,\texttt{skip} \rightarrow_1 c$$

$$\frac{c_1 \rightarrow_1 c_1'}{c_1||c_2 \rightarrow_1 c_1'||c_2} \qquad \frac{c_2 \rightarrow_1 c_2'}{c_1||c_2 \rightarrow_1 c_1||c_2'}$$

An alternative way is by adding the rules:

$$\texttt{skip}\,||c \rightarrow_1 c \qquad c_1||c_2 \rightarrow_1 c_2||c_1 \qquad \frac{c_1 \rightarrow_1 c_1'}{c_1||c_2 \rightarrow_1 c_1'||c_2}$$

Explain briefly why these do not result in the same semantics.

6. Suppose we restricted IMP so that it only manipulates 32-bit signed integers and redefined +,-, and * to work like machine arithmetic. Call the resulting language IMP32. Suppose further that we restrict the language of assertions to use only 32-bit integers.

   Now suppose that I gave you an ML-function:

   ```
   wp : command * assertion -> assertion
   ```

   with the property that `wp (c,B)` returns the weakest pre-condition of the command c with respect to the assertion B.

   (a) Is there a decision procedure to determine whether or not $\models A$ for any IMP32 assertion? Sketch briefly why or why not.

   (b) Suppose you do have a decision procedure, *valid_assertion*, for determining whether or not $\models A$. How can you combine this with `wp` to determine if a partial correctness assertion is valid?