Homework 4 — CS 818A4 — Spring 2004

Problem 1

Using the rules and axiom schemata for assertions in Chapter 2 of the class notes, give a formal derivation of the axiom scheme

$$(p \mathrel{-\!\!*} q) \Rightarrow (p * r \mathrel{-\!\!*} q * r).$$

Problem 2

When α is a sequence of length n, we write $\mathbf{f}\,\alpha$ and $\mathbf{b}\,\alpha$ for the "front half" and "back half" of α, which are the sequences such that

$$\mathbf{f}\,\alpha \cdot \mathbf{b}\,\alpha = \alpha \qquad \#(\mathbf{f}\,\alpha) = n \div 2 \qquad \#(\mathbf{b}\,\alpha) = n - (n \div 2).$$

It can be shown that, when $n \geq 2$,

$$1 \leq \#(\mathbf{f}\,\alpha) < n \qquad 1 \leq \#(\mathbf{b}\,\alpha) < n \qquad 0 \leq \#(\mathbf{b}\,\alpha) - \#(\mathbf{f}\,\alpha) \leq 1.$$

We can use $\mathbf{f}$ and $\mathbf{b}$ to define a function ϕ from nonempty lists of atoms to S-expressions:

$$\begin{aligned} &\phi(\alpha) = x && \text{when } \#\alpha = 1 \text{ and } \alpha = [x] \\ &\phi(\alpha) = (\phi(\mathbf{f}\,\alpha) \cdot \phi(\mathbf{b}\,\alpha)) && \text{when } \#\alpha \geq 2. \end{aligned}$$

(In the first line x is the unique element of α. In the second line, $(- \cdot -)$ denotes the pairing operation on S-expressions.)

The function ϕ has the property that $|\phi(\alpha)| = \alpha$, where $|-|$ is the flattening function defined in Homework 3. (Moreover, $\phi(\alpha)$ is an "almost balanced" S-expression, i.e., where the depths of atoms varies by at most one.)

Define and prove correct (by an annotated specification of its body) a recursive procedure $\mathsf{unflatten}$ that will convert a list segment denoting α into a tree denoting $\phi(\alpha)$. Specifically, this procedure should satisfy

$$\begin{aligned} &\{\mathsf{lseg}\ \alpha\,(\mathsf{i}, \mathsf{k}_0) \wedge \mathsf{n} = \#\alpha \wedge \mathsf{n} \geq 1\} \\ &\mathsf{unflatten}(\mathsf{n}, \mathsf{i}\,;\mathsf{x}, \mathsf{k}) \\ &\{(\mathsf{tree}\,(\phi(\alpha))\,(\mathsf{x}) * \mathsf{i} \mapsto -, -) \wedge \mathsf{k} = \mathsf{k}_0\}. \end{aligned}$$

As with mergesort in Chapter 4, the length of the input list segment is given as a separate input parameter, and the procedure should return the final link of the input list segment as one of its results. The procedure should not allocate or deallocate heap storage. Instead, since the output tree will contain one less two-cell than the input list segment, one can construct the procedure so that the redundant two-cell occurs at the address i.

Problem 3

An assertion p is said to be *precise* iff, for all states s, h, there is at most one heap $h' \subseteq h$ such that $s, h' \models p$.

Suppose that the total-correctness specification $[\, p \,]\ c\ [\, q \,]$ holds, and the assertion q is precise. Show, by an informal metaproof, that p is precise.

Hint: Use Proposition 5 (or equivalently, 6 and 7) and Proposition 2 in Chapter 2 of the class notes.