CIS 301, Spring 2008, Exam III, model solutions

Question 1 *A:* $\forall i \forall j((i < k \land j < k \land i \neq j) \rightarrow \mathtt{a}[i] \neq \mathtt{a}[j])$.

B: From the loop test we see that at loop exit we have $\mathtt{q} \geq k-1$, which combined with the invariant entails that $\mathtt{q} = k-1$. Now let j be given, with $j < k-2$; we must prove that either $\mathtt{a}[j+1]$ is greater than both of $\mathtt{a}[j]$ and $\mathtt{a}[j+2]$, or smaller than both. There are two cases; in both we exploit that $j < \mathtt{q}$ and $j+1 < \mathtt{q}$.

j **is odd** : The invariant tells us that $\mathtt{a}[j] < \mathtt{a}[j+1]$, and since $j+1$ is even, the invariant further tells us that $\mathtt{a}[j+2] < \mathtt{a}[j+1]$. This establishes (the first disjunct of) the desired conclusion.

j **is even** : The invariant tells us that $\mathtt{a}[j+1] < \mathtt{a}[j]$, and since $j+1$ is odd, the invariant further tells us that $\mathtt{a}[j+1] < \mathtt{a}[j+2]$. This establishes (the second disjunct of) the desired conclusion.

C: It is sufficient to assign zero to $\mathtt{q}$. Then $\mathrm{perm}(\mathtt{a}, a_0)$ follows from the precondition; we have $\mathtt{q} < k$ due to $k \geq 1$ being in the precondition; finally, $\forall(j < q \rightarrow \ldots)$ holds vacuously.

D: We use $\mathtt{a}'$ to denote the new value of $\mathtt{a}$. Recall that our assumptions are that $\mathtt{q}$ is odd, and that $\mathtt{a}[\mathtt{q}+1] < \mathtt{a}[\mathtt{q}]$; we must establish (since $\mathtt{q}$ is odd) that $\mathtt{a}'[\mathtt{q}] < \mathtt{a}'[\mathtt{q}+1]$. For that purpose, it will suffice to execute $\mathtt{swap}(\mathtt{a}[\mathtt{q}], \mathtt{a}[\mathtt{q}+1])$.

We are not done with our proof obligations yet, however; since we have modified $\mathtt{a}[\mathtt{q}]$, we need to check that the invariant is maintained also when $j = \mathtt{q}-1$. But $\mathtt{q}-1$ is even, so the invariant ensures that $\mathtt{a}[\mathtt{q}] < \mathtt{a}[\mathtt{q}-1]$; we must prove that $\mathtt{a}'[\mathtt{q}] < \mathtt{a}'[\mathtt{q}-1]$. But by our case assumption $\mathtt{a}[\mathtt{q}+1] < \mathtt{a}[\mathtt{q}]$ we get $\mathtt{a}[\mathtt{q}+1] < \mathtt{a}[\mathtt{q}-1]$, which amounts to the desired $\mathtt{a}'[\mathtt{q}] < \mathtt{a}'[\mathtt{q}-1]$.

E:

```
q := 0;
while q < k - 1 do
    if (odd(q) ∧ a[q + 1] < a[q]) ∨ (even(q) ∧ a[q] < a[q + 1])
    then swap(a[q], a[q + 1])
    fi;
    q := q + 1
od
```

Question 2 The basis step is when $x = \mathsf{nil}$, and the claim follows (even with "=") since

$$\begin{aligned} & \mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(\mathsf{nil}))) = \mathit{sumlist}(\mathit{incr}(\mathsf{nil})) = \mathit{sumlist}(\mathsf{nil}) = 0 + 0 \\ = \ & \mathit{sumlist}(\mathsf{nil}) + \mathit{len}(\mathsf{nil}). \end{aligned}$$

For the inductive step, where x is of the form $m \copyright y$, we assume

$$\mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(y))) \geq \mathit{sumlist}(y) + \mathit{len}(y)$$

and our task is to prove

$$\mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(x))) \geq \mathit{sumlist}(x) + \mathit{len}(x).$$

If $m \geq 0$, the goal follows from the calculation

$$\begin{aligned} \mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(x))) &= \text{(definition of } \mathit{nonneg}) \\ \mathit{sumlist}(\mathit{incr}(m \copyright \mathit{nonneg}(y))) &= \text{(definition of } \mathit{incr}) \\ \mathit{sumlist}((m+1) \copyright \mathit{incr}(\mathit{nonneg}(y))) &= \text{(definition of } \mathit{sumlist}) \\ (m+1) + \mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(y))) &\geq \text{(induction hypothesis)} \\ (m+1) + \mathit{sumlist}(y) + \mathit{len}(y) &= \text{(rearrange)} \\ (m + \mathit{sumlist}(y)) + (1 + \mathit{len}(y)) &= \text{(definition of } \mathit{sumlist} \text{ and } \mathit{len}) \\ \mathit{sumlist}(x) + \mathit{len}(x) & \end{aligned}$$

If $m < 0$, the goal follows from the calculation

$$\begin{aligned} \mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(x))) &= \text{(definition of } \mathit{nonneg}) \\ \mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(y))) &\geq \text{(induction hypothesis)} \\ \mathit{sumlist}(y) + \mathit{len}(y) &\geq \text{(since } 0 \geq m+1) \\ (m+1) + \mathit{sumlist}(y) + \mathit{len}(y) &= \text{(rearrange)} \\ (m + \mathit{sumlist}(y)) + (1 + \mathit{len}(y)) &= \text{(definition of } \mathit{sumlist} \text{ and } \mathit{len}) \\ \mathit{sumlist}(x) + \mathit{len}(x) & \end{aligned}$$

Now assume that we want to prove the claim with "=" instead of "≥". Then it is easy to see that the above proof would carry through, except that the inductive step for the case $m < 0$ only works when $0 = m + 1$. This shows that we have $\mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(x))) = \mathit{sumlist}(x) + \mathit{len}(x)$ whenever x is a list where all elements are ≥ -1. (For example, if $x = [5, 0, -1, 3]$ we have $\mathit{sumlist}(\mathit{incr}(\mathit{nonneg}(x))) = \mathit{sumlist}(\mathit{incr}([5, 0, 3])) = \mathit{sumlist}([6, 1, 4]) = 11$ whereas $\mathit{sumlist}(x) + \mathit{len}(x) = 7 + 4 = 11$.)