CS615 Spring 2010 Quiz1

Time: 30 mins Total marks: 15

- ***The quiz is open book and notes.***
- ***Results/proofs covered in class/problem sessions/assignments may simply be cited, unless specifically asked for.***
- ***Unnecessarily lengthy solutions will be penalized.***
- ***If you need to make any assumptions, state them clearly.***
- ***Do not copy solutions from others or indulge in unfair means.***

Consider the following program P along with symbolic assertions:

```
L0:  n := 0;

     {phi1}

L1:  while (n = 0)
L2:      n := f(n);
         {phi2}
L3:      *x := *y;
         {phi3}
L4:      *y := x;
         {phi4}
L5:      x := *x;
         {phi5}

L6: {phi6} // end of program
```

Let $\mathsf{list}(y, x)$ be a recursive predicate defined as follows:

$$\mathsf{list}(y, x) = (y \mapsto x) \vee \exists z.\, (y \mapsto z) \star \mathsf{list}(z, x)$$

Suppose further that the definition of function `f(n)` is not known, but it is known that `f(n)` does not access the heap and therefore never causes a memory error.

Show that $\{\mathsf{list}(y, x) \star \exists w.\, x \mapsto w\}$ P $\{\exists v.\, ((y \mapsto v) \star (v \mapsto x)) \star \mathbf{true}\}$ is a valid Hoare triple. Note that $(s, h) \models \mathbf{true}$ for any stack s and heap h.

To be specific,

- Give assertions `phi1, phi2, phi3, phi4, phi5` and `phi6` such that these assertions hold at the locations indicated in the program. Note that `phi1` must be a loop invariant, and `phi6` should be implied by `phi1` $\wedge (n \neq 0)$.
- Ensure that $\{\mathsf{list}(y, x) \star \exists w.\, x \mapsto w\}$ logically entails `phi1`, and `phi6` logically entails $\{\exists v.\, ((y \mapsto v) \star (v \mapsto x)) \star \mathbf{true}\}$.

Hint: Rewrite the precondition as the disjunction of two separation logic formulae, obtained from the recursive definition of list *and from the fact that* $\star$ *distributes over* $\vee$. *Then consider what happens if you start from each of these preconditions separately.*