CS615 Graded Homework #1

Max Marks: 35 **Due date: Mar 5, 2010 (5 pm)**

- *Be brief, complete and stick to what has been asked.*
- *If needed, you may cite results/proofs covered in class without reproducing them.*
- ***Discussion among students is fine, but the solution you turn in must be your own solution in your own words. Cases of copying or indulgence in unfair means will be severely penalized, including award of FR grade.***

Problems on Hoare proofs:

1. Consider the program `P` given below, in which `f` is an unspecified (as yet) function.

```
Program P
 L0:  i := 1;
 L1:  s := 3;
 L2:  while (i <= n) // outer while loop
 L3:    s := s + r;
 L4:    j := 1;
 L5:    while (j <= m) // inner while loop
 L6:      s := f(s);   // function call
 L7:      j := j + 1
 L8:    // end of inner while loop
 L9:    i := i + 1
 L10: // end of outer while loop
```

   Prove the following Hoare triples:

   (a) *[10 marks]* $\{(m \geq 0) \wedge (n \geq 0)\}$ `let f(x) = ret := x + 1 in P` $\{s = (m + r).n + 3\}$.

   (b) *[10 marks]* $\{(m > 0) \wedge (n \geq 0) \wedge (0 \leq r \leq 2)\}$ `let f(x) = local t.  t := x mod 3; ret := 3*(x - t) in P` $\{s = 3^{mn} \times 3\}$.

   Note that since we have a nested loop in the above problems, you are required to obtain a separate loop invariant for each loop. However, these loop invariants are dependent, in general.

2. Let $\mathsf{list1}$ and lasso be recursively defined predicates in separation logic, as given below.

$$\mathsf{list1}(x, y) \equiv (x \mapsto y) \vee \exists u.\, ((x \mapsto u) \star \mathsf{list1}(u, y))$$

$$\mathsf{lasso}(x) \equiv (\exists y.\, (x \mapsto y) \star (y \mapsto x)) \vee \exists v.\, (\mathsf{list1}(x, v) \star \mathsf{lasso}(v))$$

   (a) *[5 marks]* Give an alternative definition of $\mathsf{lasso}(x)$ that is non-recursive (you can use the $\mathsf{list1}$ predicate in your definition if needed), and is semantically equivalent to the recursive definition provided above. By semantic equivalence, we mean that for *every* state (s, h) that satisfies one of the definitions, (s, h) also satisfies the other definition.

   (b) *[10 marks]* Now consider the program `Q` given below.

```
Program Q
L0:  t1 := 0; // NULL value of pointer
L1:  while (x1 != t1)
L2:    t2 := x1;
L3:    x1 := *x1;
L4:    if (x1 = t1) then
L5:      x1 := t2
L6:    else
L7:      x1 := x1;
L8:    // end of if-then-else
L9:    *t2 := t1;
L10:    t1 := t2;
L11: // end of while
```

Is the Hoare triple $\{\mathsf{lasso}(x1)\}$ `Q` $\{\mathsf{list1}(x1, 0)\}$ valid? If yes, give a proof. Else, give a counterexample, i.e. an initial state (s, h) satisfying $\mathsf{lasso}(x1)$ such that `Q` terminates starting from (s, h) and the final state does not satisy $\mathsf{list1}(x1, 0)$.