Quiz

Synthesis, Analysis, and Verification 2010

Tuesday, March 16, 2010

Last Name : _____

First Name : _____

Exercise	**Points**	**Achieved Points**
1	10	
2	10	
3	10	
4	20	
5	20	
6	30	
Total	100	

Problem 1: Relations (10 points)

In this quiz we use the following notation:

- S is a set of all states
- $\mathsf{sp} : 2^S \times 2^{S \times S} \to 2^S$ is defined by

$$\mathsf{sp}(P, r) = \{s' \mid \exists s.s \in P \wedge (s, s') \in r\}$$

- $\mathsf{wp} : 2^{S \times S} \times 2^S \to 2^S$ is defined by

$$\mathsf{wp}(r, Q) = \{s \mid \forall s'.(s, s') \in r \to s' \in Q\}$$

- Diagonal relation Δ_A for $A \subseteq S$ and $r \subseteq S \times S$ is defined by

$$\Delta_A = \{(s, s) \mid s \in A\}$$

Task: prove the following equation:

$$sp(P, r) = sp(S, \Delta_P \circ r)$$

Problem 2: Strongest postcondition of diagonal relation (10 points)

Consider the set

$$sp(P, \Delta_A) \tag{1}$$

Task: Express (1) using sets S, P, A, using only set operations $\cap, \cup, \setminus$ (in particular, do not use set comprehensions $\{...\}$, sp, or wp). Prove that your expression is equal to (1).

Problem 3: Weakest precondition of diagonal relation (10 points)

Consider the set

$$wp(\Delta_A, Q) \tag{2}$$

Task: Express (2) using sets S, P, A, using only set operations $\cap, \cup, \setminus$ (in particular, do not use set comprehensions $\{...\}$, sp, or wp). Prove that your expression is equal to (2).

Problem 4: Interpreting first-order logic formulas (20 points)

Consider the formula:

$$\forall x.\forall y.\exists m.(\neg R(x,x) \wedge (\neg R(x,y) \vee (R(x,m) \wedge R(m,y)))) \tag{3}$$

Consider the following structures $I = (D, \alpha)$, indicate whether (3) is true or false in I. Here D is the universe of interpretation and $\alpha(R) \subseteq D^2$ denotes the meaning of the relation symbol R in the structure I.

1. $D = \{a, b, c\}$, $\alpha(R) = \{(a, b), (b, c)\}$
2. $D = \{a, b, c\}$, $\alpha(R) = \{(a, b), (b, a), (a, c), (c, a), (b, c), (c, b)\}$
3. $D = \mathbb{Q}$ (the set of rational numbers), $\alpha(R) = \{(x, y) \mid x < y\}$.
4. $D = \mathbb{Z}$ (the set of integers), $\alpha(R) = \{(x, y) \mid x < y\}$.

Task a): Write true if the formula is true in the structure, write false if the formula is false in the structure. If you do not know the answer, do not write anything, a wrong answer will result in negative points.

Task b): Choose a structure I_1 from the list above in which the formula is true and indicate which one you have chosen. Then find and describe a function $f : D \times D \to D$ such that, for all values x, y, the following formula is true in the structure I_1.

$$R(x, y) \to (R(x, f(x, y)) \wedge R(f(x, y), y))$$

Problem 5: Validity and satisfiability of first-order logic formulas (20 points)

Consider the following first-order logic formulas:

1. $(\exists x.(P(x) \land Q(x))) \leftrightarrow ((\exists x.P(x)) \land (\exists x.Q(x)))$
2. $\forall x.\exists y.R(x, y)$
3. $((\forall x.P(x)) \lor (\forall x.Q(x))) \rightarrow (\forall x.(P(x) \lor Q(x)))$
4. $(\exists x.(P(x) \rightarrow (\forall y.P(y))))$
5. $(\exists x.P(x) \land Q(x)) \land (\forall y.\neg Q(y))$
6. $(\forall x \forall y.(R(x, y) \rightarrow \neg R(y, x))) \rightarrow \neg(\exists z.R(z, z))$

Task a): Next to each formula indicate indicate whether it is:

- valid (true in all interpretations)
- unsatisfiable (false in all interpretations)
- neither valid nor unsatisfiable

Do not write answers that you do not know; wrong answers will bring negative points.

Task b): If you found a formula above that is neither valid nor unsatisfiable, give an interpretation I_1 where the formula is true and an interpretation I_0 where the formula is false.

Problem 6: Hoare Triples and Loop Invariants (30 points)

Consider a programming language that supports integer variables, as well as variables that denote sets of integers and binary relations on integers (all integers are unbounded).
The command $\mathsf{lookup}(k, r)$ looks up a value v such that $(k, v) \in r$. If such value exists, it returns one such value as a singleton set $\{v\}$. If no such value exists, it returns the emptyset $\{\}$. (Note that, for each k, there can in general be zero, one, or more values v such that $(k, v) \in r$.)

Task a) [5 points]. Write a Hoare triple describing $\mathsf{lookup}(k, r1)$ in the form

$$\{precondition\}$$
$$v1 = \mathsf{lookup}(k, r1)$$
$$\{postcondition\}$$

Task b) [25 points]. Consider the following program, where the variables r1,r are relations, v1,W are sets of integers, and k is an integer.

```
// Precondition: ∀i.∀v.(i,v) ∈ r → 0 ≤ i
r1 = r;
k = 0;
W = {};
while // invariant Inv
      (r1 != {})
{
  v1 = lookup(k,r1);
  if (v1 = {}) {
    k = k + 1
  } else {
    W = W ∪ v1;
    r1 = r1 \ ({k} × v1)
  }
}
// Postcondition: W = range(r)
```

We use the notation

$$\mathsf{range}(r) = \{v \mid \exists i.(i, v) \in r\}$$

Find an appropriate loop invariant, Inv, and use it to prove that, whenever we run the above program in a state that satisfies the Precondition, its final state satisfies the Postcondition. You need to explain why (1) the invariant holds initially in *all* states that satisfy the precondition, why (2) it is inductive (preserved on each execution of the loop body starting from *any* state satisfying only the invariant), and why (3) it can be used to prove the Postcondition. State each of these conditions as a Hoare triple, and prove it. Your proof of individual Hoare triples need not be very detailed.
Feel free to use any notation of sets, relations, and quantifiers in your invariants and Hoare triples. The invariant should be "as simple as possible, but no simpler". It is crucial that your invariant is correct (conditions (1),(2),(3) hold).
Optional Task c) (does not affect the points or the grade). Suppose that we modify the code above by inserting the assignment command 'k = k + 1' also in the second branch of 'if'. Does your original invariant still apply to the modified program?