CS615 Homework #1

Max marks: 65 **Due Sept 30, 2008**

- *Be brief, complete and stick to what has been asked.*
- *If needed, you may cite results/proofs covered in class without reproducing them.*
- ***Do not copy solutions from others.***

1. *[10 + 10 + 10 marks]* For the program P given below, consider the Hoare triples $\{\varphi_r\}\, P\, \{\psi_r\}$ for $r \in \{1, 2, 3\}$, where φ_r and ψ_r are as given in Table 1.

```
Program P:

    L0:  i := 0;
    L1:  while (x < y) do
    L2:    x := y - x;
    L3:    y := 2*z - y;
    L4:    if (y > 0) then
    L5:       x := -x;
    L6:    else
    L7:       x := x;
    L8:    i := i + 1;
    L9:  // end of while loop
```

	$r = 1$	$r = 2$	$r = 3$
φ_r	$(x < y) \wedge (2z - y > 0) \wedge (y > 0)$	$(x < y) \wedge (2z - y > 0) \wedge (y \leq 0)$	$(x < y) \wedge (2z - y \leq 0)$
ψ_r	$i \leq 2$	$i \leq 1$	$i \leq 0$

Table 1: Pre- and post-condition pairs

For each of the three Hoare triple $\{\varphi_r\}\, P\, \{\psi_r\}$, either (i) prove the validity of the Hoare triple, indicating invariants at all program locations, or (ii) provide a counterexample, i.e., a state that satisfies the precondition, but if the program is started in this state, it terminates in a state that does not satisfy the postcondition.

Answers without justifications will fetch no marks.

2. *[5 + 10 + 10 + 10 + 10 marks]* We have seen several abstract lattices that admit natural Galois connections with the powerset lattice of concrete valuations of program variables (concrete lattice). A few examples of such abstract lattices are the lattice of intervals, lattice of convex polyhedra and lattice of difference bound matrices (DBMs). Unfortunately, not all lattices permit natural ways of establishing a Galois connection with the concrete lattice. In this question, we wish to investigate this difficulty with one such abstract lattice.

Consider a program with n real variables $x_1, x_2, \ldots x_n$. The abstract domain we wish to consider consists of spheres with centres along a fixed line (in this question, the line represented by $x_1 = x_2 = \ldots x_n$). Such a sphere can be represented by a pair of reals, representing the centre and radius of the sphere. In order to have a unique representation of a given sphere, we choose our abstract domain to be $\mathcal{A} = \mathbf{R} \times \mathbf{R}^{>0} \cup \{(0,0), (0,\infty)\}$, where $\mathbf{R}$ represents the set of reals and $\mathbf{R}^{>0}$ represents the set of positive reals.

For a program with n real variables $x_1, x_2, \ldots x_n$, the concretization function is defined as follows: $\gamma((a,b)) = \{(x_1, x_2, \ldots x_n) \mid \Sigma_{i=1}^{n}(x_i - a)^2 < b^2\}$. In other words, the abstract element (a,b) may be viewed as representing the inside of a sphere of radius b centred at $(a, a, \ldots a)$ in n-dimensional space.

(a) First of all, we'd like our abstract domain to be a complete lattice. Going by the most natural way of defining an ordering relation, we define $(a,b) \sqsubseteq (c,d)$ iff $\gamma((a,b)) \subseteq \gamma((c,d))$. It is easy to see that the bottom element of the lattice is $(0,0)$ and the top element is $(0,\infty)$

   i. Prove that the $\sqsubseteq$ ordering defined above is a partial order, i.e. it is reflexive, anti-symmetric and transitive.

   ii. How would you define the *lub* and *glb* operators in this abstract lattice? In other words, indicate how you would compute $glb((a,b),(c,d))$ and $lub((a,b),(c,d))$ for two arbitrary elements (a,b) and (c,d) in the abstract lattice.

   iii. Can you define *lub* and *glb* of any set of (not necessarily just two) elements in this abstract lattice? If so, explain how you would go about defining these operators on arbitrary subsets of abstract elements. Else, show why it is not possible to define these operators for arbitrary subsets of abstract elements.

(b) Given a set S of valuations of the n program variables, we wish to define an appropriate abstraction function $\alpha : \mathcal{P}(\mathbf{R}^n) \to \mathcal{A}$.

   Indicate how you would compute $\alpha(S)$ for $S \subseteq \mathbf{R}^n$. Note that there may not be a unique way to compute $\alpha(S)$, and so we do not expect uniform answers. Your α function should be monotone, and should have an infinite range (i.e. you are not allowed to map arbitrary subsets of concrete states to a finite number of abstract elements).

(c) For the α chosen by you, and γ given above, does α and γ form a Galois connection? If so, prove your claim. Else demonstrate using a counterexample why α and γ do not form a Galois connection.