CS615 Autumn 2006 Quiz 4

Time: 30 mins Total marks: 10

---

- ***You must write your answers only in the spaces provided.***
- ***The exam is open book and notes.***
- ***Results/proofs covered in class/problem sessions/assignments may simply be cited, unless specifically asked for.***
- ***If you need to make any assumptions, state them clearly.***
- ***Do not copy solutions from others or indulge in unfair means.***

1. In this problem, we wish to investigate some aspects of applying abstract interpretation to a program with two real-valued variables $x$ and $y$ that take on values between $-100$ and 100.

   Let $X$ be the set of all real numbers between $-100$ and 100, i.e. $X = \{r \mid r \in \Re, -100 \leq r \leq 100\}$. The concrete domain for our abstract interpretation is the powerset of $X^2 = X \times X$. The lattice ordering in the concrete domain is the usual set inclusion ordering. Examples of two (rather arbitrary) elements in the concrete domain are $\{(x,y) \mid x^2 + y^2 \leq 25\}$ and $\{(x,y) \mid (x \leq 5) \vee (y \leq 5)\}$. Note that the first set is contained in the second set, and therefore is lesser than the second set in the lattice ordering defined by set inclusion. The bottom of this concrete lattice is the empty set and the top is the set $X^2$. The *glb* operator is set intersection and the *lub* operator is set union.

   The abstract domain for this problem is the set of real numbers $Y = \{r \mid r \in \Re, 0 \leq r \leq 2 \times 10^4\}$. The lattice ordering in the abstract domain is the usual $\leq$ ordering of real numbers. Thus, 2.9 and 5.01 are two (rather arbitrary) elements from the abstract domain, and the first one is lesser than the second in the lattice ordering defined by $\leq$.

   Let $r_1$ and $r_2$ be elements of the abstract lattice.

   (a) Express $glb(r_1, r_2)$ as an expression of the form
   _____ ? _____ : _____,
   where each blank should be filled with an expression involving nothing other than $r_1$, $r_2$ and $\leq$.

   (b) Similarly, express $glb(r_1, r_2)$ as an expression of the form
   _____ ? _____ : _____.

   The abstraction ($\alpha : \mathcal{P}(X^2) \rightarrow Y$) and concretization ($\gamma : Y \rightarrow \mathcal{P}(X^2)$) functions for the above choice of lattices are given by:
   $\alpha(S) = \max_{(x,y) \in S}(x^2 + y^2)$, and $\gamma(r) = \{(x,y) \mid x^2 + y^2 \leq r, -100 \leq x \leq 100, -100 \leq y \leq 100\}$.
   It can be shown (and may be assumed) that $(\alpha, \gamma)$ form a Galois connection.

   Now consider the following program `P` with location labels `Li`. Remember that variables `x` and `y` are real-valued in `P` and assume values from $X$.

```
L1: while (*) {
L2:    assert(x*x >= 1000);
L3:    x := x/2;
L4:    y := y/3;}
```

   We wish to construct a program `P'` with a single variable `r` that assumes values from $Y$. The value of `r` in `P'` is intended to be the best possible abstraction of the set of values of `x` and `y` in `P`. The program `P'` should be constructed such that if we start `P` with a precondition $\psi(x,y)$, and if we start `P'` with an arbitrary precondition $\alpha(\psi(x,y))$, then the set of traces of `P'` are as small a superset as possible of the set of traces of `P`.

   You may construct the program `P'` by filling in the blanks in the following skeleton. You must indicate your justification for each expression you use to fill in the blanks. Note that this is not a Boolean program and therefore you should not blindly try to apply techniques used for Boolean programs.

```
L1':   while (*) {

L2':     assert(_________________);  // corr. to stmt at L2

L3':     r := _____________;  // corr. to stmt at L3

L4':     r := _____________;  // corr. to stmt at L4}
```