CS615 Homework #1

Max marks: 60 **Due Sept 11, 2007**

- *Be brief, complete and stick to what has been asked.*
- ***Do not copy solutions from others.***

1. *[10 + 10 + 10 marks]* The following programs use the simple language studied in class, with the addition of the integer subtraction operator. Each program statement is labeled for ease of reference. In program (c), `f(z)` and `g(z)` refer to unspecified expressions that return integer values.

	(a)	(b)	(c)
Precond $\{\phi\}$	$\{\exists k.\,(k > 1) \wedge (y = 3k)\}$	$\{(8x < y < 16x) \wedge (x > 0)\}$	$\{z > 0\}$
Postcond $\{\psi\}$	$\{y = x\}$	$\{z \leq y + 4\}$	$\{y \leq 0\}$

Program P (a):

```
L1:  x := 0;
L2:  while (x < y) {
L3:    x := x + 1;
L4:    y := y - 2;
L5:  }
```

Program P (b):

```
L1:  z := 0;
L2:  while (x != y) {
L3:    if (x < y) {
L4:       x := 2*x;
L5:    } else {
L6:       x := x - 1;
L7:    }
L8:    z := z + 1;
L9:  }
```

Program P (c):

```
L1:  x := 1;
L2:  y := 1;
L3:  while (z > 0) {
L4:    if (f(z) > 0) {
L5:       x := x - 1;
L6:       y := y - 1;
L7:    } else {
L8:       x := x - f(z);
L9:       y := y + f(z);
L10:   }
L11:   z := g(z);
L12: }
L13: while (x > 0) {
L14:   x := x - 1;
L15:   y := y - 1;
L16: }
```

You are required to check if the Hoare triple $\{\phi\}\,P\,\{\psi\}$ evaluates to True in each of the three cases. You must indicate what first-order logic formulae you are using to describe the state prior to execution of each statement (use a statement's label to refer to it). You must also indicate which inference rule of Hoare Logic is used to justify the above formulae at each statement, starting from the given pre- and post-conditions.

If you need to use loop invariants, please state them explicitly.

2. Let $(\mathcal{P}(S), \subseteq, \emptyset, S, \cup, \cap)$ and $(\mathcal{L}, \sqsubseteq, \bot, \top, \sqcup, \sqcap)$ be complete lattices, where $\mathcal{P}(S)$ denotes the powerset of S.

   (a) Let $\alpha : \mathcal{P}(S) \to \mathcal{L}$ and $\gamma : \mathcal{L} \to \mathcal{P}(S)$ be functions satisfying the following properties:

   - α is a monotone function.
   - γ is a monotone function.
   - $\forall a \in \mathcal{P}(S), \forall b \in \mathcal{L},\ \alpha(a) \sqsubseteq b \Leftrightarrow a \subseteq \gamma(b)$.

   Show that

   i. *[10 marks]* $\alpha(\gamma(b)) \sqsubseteq b$ for all $b \in \mathcal{L}$

   ii. *[10 marks]* $a \subseteq \gamma(\alpha(a))$ for all $a \in \mathcal{P}(S)$.

   A pair (α, γ) satisfying the above properties is called a *Galois connection*. In our context, we will refer to α as an *abstraction* function, and to γ as a *concretization* function.

   (b) Let $F_C : \mathcal{P}(S) \to \mathcal{P}(S)$ be a monotone function. Our interpretation of F_C is a function that computes the next concrete set of states, i.e. $F_C(a)$ gives the set of concrete states reached after one step of execution of the program starting from a set a of concrete states. Let $F_A : \mathcal{L} \to \mathcal{L}$ be the next state computing function in the abstract lattice, and is defined by $F_A(b) = \alpha(F_C(\gamma(b)))$.

   i. *[5 marks]* Let $a_0 \subseteq S$, and $b_0 = \alpha(a_0)$. Recall that when trying to compute $\lim_{i\to\infty} \bigcup_{j=0}^{i} F_C^{(j)}(a_0)$ and $\lim_{i\to\infty} \bigsqcup_{j=0}^{i} F_A^{(j)}(b_0)$, we defined two new functions, $\mathcal{F}_C(a) = a_0 \cup F_C(a)$ for all $a \in \mathcal{P}(S)$, and $\mathcal{F}_A(b) = b_0 \sqcup F_A(b)$ for all $b \in \mathcal{L}$.
   Prove that $lfp(\mathcal{F}_C) \subseteq \gamma(lfp(\mathcal{F}_A))$. In our context, this is equivalent to showing that $\lim_{i\to\infty} \mathcal{F}_C^{(i)}(\emptyset) \subseteq \gamma(\lim_{i\to\infty} \mathcal{F}_A^{(i)}(\bot))$.

   ii. *[5 marks]* Let $F'_A : \mathcal{L} \to \mathcal{L}$ be a monotone function such that $F_A(b) \sqsubseteq F'_A(b)$ for all $b \in \mathcal{L}$. Similar to what we did with F_A, let us now define $\mathcal{F}'_A(b) = b_0 \sqcup F'_A(b)$ for all $b \in \mathcal{L}$. It is easy to show by induction on i that $\mathcal{F}_A^{(i)}(\bot) \sqsubseteq \mathcal{F}_A^{'(i)}(\bot)$. Please don't show this proof in your solution sheets. Instead, show that $lfp(\mathcal{F}_A) \sqsubseteq lfp(\mathcal{F}'_A)$. In our context, this is equivalent to showing that $\lim_{i\to\infty} \mathcal{F}_A^{(i)}(\bot) \sqsubseteq \lim_{i\to\infty} \mathcal{F}_A^{'(i)}(\bot)$