CIS6333

Homework 1 (due Friday, February 1)

1. (Propositional Calculus - 10 points)

Let P, Q, R range over state predicates of some program.
Prove or disprove the following:

a) $P \vee (P \wedge Q) \equiv P$
b) $P \wedge (Q \vee R) \equiv (P \vee Q) \wedge (P \vee R)$
c) $\neg(P \equiv Q) \equiv \neg P \equiv \neg Q$
d) $P \equiv Q \equiv (P \vee Q) \equiv (P \wedge Q)$

2. (More Propositional Calculus - 6 points)
----

a) Prove $\neg\neg P \equiv P$
b) Prove the identity of $\vee$, $P \vee false \equiv P$, by transforming its more structured side into its simpler side.
c) Prove $P \Rightarrow Q \equiv \neg P \vee \neg Q \equiv \neg P$

3. (Predicate Calculus - 10 points)
----

a) Prove $(\forall x : R : P \equiv Q) \Rightarrow ((\forall x : R : P) \equiv (\forall x : R : Q))$
b) Prove $\neg(\exists x : R : P) \equiv (\forall x : R : \neg P)$
c) Translate the following English statements into predicate logic:
(i) Every positive integer is smaller than the absolute value of some negative integer. (Use $abs.i$ for the absolute value of i)
(ii) Real number i is the largest real solution of the equation $f.i = i + 1$
(iii) No integer is larger than all others.
d) Translate into English the meaning of :
(i) $(\exists x, y : x \in R \wedge y \in R : (f.x < 0 \wedge 0 < f.y) \Rightarrow (\exists z : z \in Reals : f.z = 0))$
(ii) $(\forall z : z \in Integers \wedge even.z : (\forall w : w \in Integers \wedge odd.w : z \neq w))$

4. (Closure) -- 30 points

Let P and Q range over state predicates of a program *prog*. Recall that the statements of each action of *prog* are terminating.
Recall that in class we defined:

$$\text{closed } P \text{ iff } \{P\}\ prog\ \{P\}$$

`True or False? (Explain your answer.)`

a) closed $false$
b) closed $true$
c) (closed P or closed Q) implies (closed $(P \vee Q)$)
d) (closed $\neg P$) implies (closed P)
e) (closed $(P \vee Q)$) implies $(\forall\ s :: \{P\}\ s\ \{Q\})$
f) (exists $s :: \{P\}\ s\ \{false\}$) implies (closed $\neg P$)
g) closed $(P \vee Q)$
    implies $(\forall\ s :: \{P\}$ s $\{P \vee Q\})$
h) closed P and closed Q and $(R \Rightarrow (P \wedge Q))$
    implies closed R
i) closed P and closed Q and closed R
    implies closed $(P \wedge (Q \wedge R))$

```
5. (Leads-to) -- 24 points
--------------------------
```

Let P, Q, and R range over state predicates of a program *prog*.

`True or False? (Explain your answer.)`

a) *false* leads-to $P \vee Q$
b) (P leads-to Q) implies (($P \wedge Q$) leads-to Q)
c) (P leads-to Q) implies (($P \wedge R$) leads-to Q)
d) ((P leads-to Q) and (P leads-to R)) implies (P leads-to ($Q \wedge R$))
e) (P leads-to Q) and (($Q \vee R$) leads-to T)
    implies (($P \vee R$) leads-to T)
f) P leads-to Q and P leads-to R and closed R
    implies (P leads-to ($Q \wedge R$))

```
6. (Variant functions) - 20 points
----------------------------------
```

For each program described below, prove, by exhibiting a variant function, that the desired progress property holds, or show that the progress property does not hold. Assume the semantics of minimal progress: At every step in the computation, if some action is enabled, then some enabled action is executed.

a) Let $x.j$ be an integer for $0 \le j < N$. For each j in the range $0 < j < N$, consider the program action:

$$x.j < x.(j-1) \quad \rightarrow \quad x.j, x.(j-1) := x.(j-1), x.j$$

The progress property to be verified is:

$true$ leads-to $(\forall j : 0 < j < N : x.j >= x.(j-1))$

b) Given are line segments $L.1, L.2, ..., L.N$ in the X-Y plane (assume all $2N$ endpoints are unique) and a program that consists of one action for each pair $(L.j, L.K)$ of line segments:

```
L.j and L.k intersect    -->   swap any one endpoint of L.j
                               with any one endpoint of L.k,
                               thus making L.j and L.k nonintersecting
```

The progress property to be verified is: "the program eventually terminates"

```
7. (Verifying closure and leads-to)
-----------------------------------
```

Consider the program $TRANS$ over the boolean variables b, c, and d :

$$\begin{array}{l} b \quad\quad \longrightarrow c := true \\ \| \\ b \wedge c \longrightarrow d := true \end{array}$$

Are the following properties true in $TRANS$? (Explain your answer carefully. A formal proof is not necessary.)

(i) closed $(\neg b \ \wedge \ c)$
(ii) closed $(\neg c \ \wedge \ d)$
(iii) c leads-to d
(iv) b leads-to d

Does the variant function

(3 − number of variables of $TRANS$ that are true)

suffice to verify the leads-to predicate in part (iii)? in part (iv)?

```
8. (Distributed load balancing)
-------------------------------
   Prove either that the desired liveness specification holds
   by exhibiting a variant function, or show that it does not hold.

   Let x.j be an integer for each node j in an undirected graph.
   For each pair of neighboring nodes j and k in the graph,
   consider the program action:

       (x.j - x.k) > 1     -->    x.j, x.k := x.j - 1, x.k + 1

   The liveness specification to be verified for this set of actions is:

       true  leads-to  (forall j, k:  j and k are neighboring nodes:
                                              |x.j-x.k| <= 1)
```

```
9. (Verifying Hoare-triples)
----------------------------
```

Let m , n, and l be integers, and M and N be integer constants. Carefully prove or disprove the following Hoare-triples. (Formal proofs are not necessary, but are encouraged).

(a) $\{m = M\}$

$$m < 0 \longrightarrow m \ := \ -m$$

$\{m = |M|\}$

(b) $\{m > M\}$

$$m > n \longrightarrow m, n \ := \ n, m$$

$\{m \leq n\}$

Here are two new rules about Hoare-triples:

Rule of Sequential Assignment:

Let x and y be variables and E and F be expressions whose value are in the domain of x and y, respectively,a and let P be a state predicate.

$$\{(P\ [y := F])\ [x := E]\} \quad true \longrightarrow x := E\ ;\ y := F \quad \{P\}$$

Rule of Guards:

Let $prog$ be a program with two actions $g1 \longrightarrow st1$ and $g2 \longrightarrow st2$, and let Q and R be state predicates of $prog$.

$$Q \ \Rightarrow \ g1 \vee g2\ ,$$
$$\{Q\}\ g1 \longrightarrow st1\ \{R\}\ ,$$
$$\{Q\}\ g2 \longrightarrow st2\ \{R\}$$

implies

$$\{Q\}\ prog\ \{R\}$$

Prove or disprove the following Hoare-triples:

(c) $\{m{=}M \wedge n{=}N\}$

$$true \longrightarrow n := n{+}m\ ;\ m := n{-}m\ ;\ n := n{-}m$$

$\{m{=}N \wedge n{=}M\}$

(d) $\{true\} \quad l \leq m \longrightarrow n := m \quad [\!] \quad m \leq l \longrightarrow n := l \quad \{n = max(l, m)\}$