Corso di Metodi Formali dell'Informatica

Sesto Compitino – 6 Febbraio 2002

a.a. 2001/2002

1. Si consideri la seguente nozione di *strongest postcondition* (postcondizione più forte) di un comando C rispetto ad una precondizione P: intuitivamente, $sp(C, P)$ è la condizione più forte che sicuramente vale al termine dell'esecuzione di C, sapendo che all'inizio vale P. Ad esempio la postcondizione più forte per `x=x+1` rispetto alla precondizione $\mathtt{x} > 5$ è $\mathtt{x} > 6$; un'altra postcondizione (meno forte) è $\mathtt{x} > 0$.

   Formalmente:

   $sp(C, P)(s) = tt$ se e solo se esiste s' tale che $[\![C]\!]\, s' = s$ e $P(s')$.

   (a) (Punti 2) Si dia una definizione equivalente in termini di insiemi di stati.

   (b) (Punti 2) È vero che se $\{P\}\ C\ \{\Downarrow R\}$ è valida allora $sp(C, P) \Rightarrow R$? Si giustifichi la risposta.

   (c) (Punti 2) In quale caso $sp(C, P) = \mathit{false}$? Si giustifichi la risposta.

   (d) (Punti 3) Si ricavi una caratterizzazione esplicita per $sp(C_1\,;C_2, P)$. Si giustifichi (almeno informalmente) la risposta.

2. Si consideri la seguente asserzione alla Hoare di correttezza parziale (A array di dimensione n, n costante positiva):

   $\{\mathtt{i} = 1 \wedge \forall j \in [1..n].\mathsf{A}[j] \geq 0\}$

   ```
   while (i!=n+1) {
     if (A[i]>0) {A[i] = A[i]-1}
     else {i=i+1}
   }
   ```

   $\{\forall j \in [1..n].\mathsf{A}[j] = 0\}$

   (a) (Punti 14) Si dia la prova formale completa con il sistema di Hoare della validità dell'asserzione. **NB:** si ricordi che perchè l'espressione `A[i]` risulti definita occorre che il valore di `i` sia compreso nell'intervallo $[1..n]$.

   (b) (Punti 4) Si consideri l'asserzione analoga a quella data, ma di correttezza totale, e si descriva una funzione di terminazione adatta a provarne la validità, giustificando la scelta.

3. (Punti 5) Si consideri la seguente asserzione alla Hoare di correttezza parziale:

   $\{\neg\mathtt{found} \wedge \mathtt{x} = x_0\}$

   ```
   while (!found) {
     if (x==y) {found=true}
     else {x=x-1}
   }
   ```

   $\{\mathtt{y} \leq x_0\}$

   Si dia un'invariante *INV* adatta a provare la validità dell'asserzione, giustificando la scelta. Occorre cioè far vedere che *INV* vale all'inizio, che $\mathit{INV} \wedge \mathtt{found}$ implica la postcondizione e che se vale $\mathit{INV} \wedge \neg\mathtt{found}$ prima di eseguire il body allora vale ancora *INV* dopo. Non è richiesta la prova formale completa con il sistema di Hoare.