Corso di Metodi Formali dell'Informatica

Compitino – 6 Giugno 2003

a.a. 2002/2003

1. Si aggiunga al linguaggio MINILWil seguente comando (ciclo do-until):

$$\mathit{Com} \quad ::= \quad \ldots \mid \texttt{do}\ \{\mathit{Com}\}\ \texttt{until}\ \mathit{BExp}$$

   la cui semantica è definita dalla seguente uguaglianza:

   $[\![\texttt{do}\ \{C\}\ \texttt{until}\ B]\!]\, s = [\![C\texttt{;if (!}B\texttt{)}\{\texttt{do}\ \{C\}\ \texttt{until}\ B\}]\!]\, s$

   ossia si esegue il comando *C* una volta e poi si controlla se la condizione di uscita dal ciclo *B* è verificata; in caso contrario si riesegue il ciclo do-until.

   Si consideri la seguente traccia di regola di correttezza parziale per il ciclo do-until.

$$\text{(Do-Until)} \quad \frac{\{\ldots\}\ C\ \{\ldots\} \quad \{\ldots\}\ C\ \{\ldots\}}{\{P\}\ \texttt{do}\ \{C\}\ \texttt{until}\ B\ \{\mathit{INV} \wedge [\![B]\!]\}}$$

   (a) Si completi la traccia in modo da fornire una regola sound e completa.

   (b) Si provi informalmente la correttezza della regola data (si dia una prova analoga a quelle date nelle note per gli altri comandi di MINILW, utilizzando un diagramma di flusso).

   (c) Si provi formalmente la correttezza della regola data.

2. Si consideri la seguente asserzione alla Hoare di correttezza totale (A array a indici in $[1..n]$, $n \geq 0$, k costante intera):

   $\{\texttt{i} = 1 \wedge \neg\texttt{found}\}$

```
while (i<=n ) {
  if (A[i]==k) {found = true};
  i=i+1
}
```

   $\{\Downarrow \texttt{found} = (\exists j \in [1..n].\mathsf{A}[j] = k)\}$

   (a) Si dia la prova formale completa con il sistema di Hoare della validità dell'asserzione.

   (b) Si consideri la seguente versione ottimizzata:

   $\{\texttt{i} = 1 \wedge \neg\texttt{found}\}$

```
while (i<=n && !found) {
  if (A[i]==k) {found = true}
  else {i=i+1}
}
```

   $\{\Downarrow \texttt{found} = (\exists j \in [1..n].\mathsf{A}[j] = k)\}$

   Si dica come vanno modificate l'invariante e la funzione di terminazione date precedentemente, e si dia almeno una traccia della prova modificata.

3. Si trovi un comando *C* tale che:

   $\mathit{wp}(C, \mathsf{x} = \mathsf{y}) = \mathsf{x} \geq \mathsf{y}$,
   $\mathit{wlp}(C, \mathit{false}) = \mathsf{x} < \mathsf{y}$.

   Si giustifichi la scelta utilizzando la definizione di *wp* e *wlp*.