Corso di Metodi Formali dell'Informatica

Recupero Compitino – 18 Giugno 2003

a.a. 2002/2003

1. (a) Si consideri la seguente regola di correttezza parziale per il ciclo while.

$$\text{(While1)} \quad \frac{\{P\}\ C\ \{INV\} \quad \{INV \wedge [\![B]\!]\ \}\ C\ \{INV\}}{\{P\}\ \texttt{while}\ (B)\ \{\ C\ \}\ \{INV \wedge \neg\, [\![B]\!]\ \}}$$

   Questa regola non è sound. Lo si provi dando un controesempio.

   (b) Si consideri la seguente altra regola di correttezza parziale per il ciclo while.

$$\text{(While2)} \quad \frac{\{P\}\ C\ \{INV\} \quad \{INV \wedge [\![B]\!]\ \}\ C\ \{INV\}}{\{P\}\ \texttt{while}\ (B)\ \{\ C\ \}\ \{R\}} \qquad \begin{array}{l} P \Rightarrow R \\ INV \wedge \neg\, [\![B]\!] \Rightarrow R \end{array}$$

   Questa regola è sound. Lo si provi informalmente.

   (c) La regola (While2) però non è sufficiente a dare un sistema completo. Lo si provi dando un controesempio (ossia, un'asserzione $\{P\}$ `while` (B) $\{\ C\ \}$ $\{R\}$ valida che non si riesce a provare con questa regola).

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

$\{\texttt{i} = n \wedge \texttt{ordered}\}$

```
while (i>=2) {
  i=i-1;
  if (A[i]>A[i+1]) {ordered = false}
}
```

$\{\Downarrow \texttt{ordered} == (\forall j, k \in [1..n].j < k \Rightarrow \texttt{A}[j] <= \texttt{A}[k])\}$

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