Corso di Metodi Formali dell'Informatica

Soluzioni 20 Febbraio 2002

a.a. 2001/2002

1. Scegliamo come invariante $\texttt{diff} = x_0 - \texttt{x}$.

   Il corrispondente albero di prova è il seguente (abbiamo indicato con *C* il ciclo while).

$$\dfrac{\dfrac{\dfrac{}{\{\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \neq \texttt{y}\}\ \texttt{x=x-1}\ \{\texttt{diff} + 1 = x_0 - \texttt{x}\}}\,(A{+}C) \quad \dfrac{}{\{\texttt{diff} + 1 = x_0 - \texttt{x}\}\ \texttt{diff=diff+1}\ \{\texttt{diff} = x_0 - \texttt{x}\}}\,(Assign)}{\{\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \neq \texttt{y}\}\ \texttt{x=x-1;diff=diff+1}\ \{\texttt{diff} = x_0 - \texttt{x}\}}\,(Seq)}{\{\texttt{diff} = 0 \wedge \texttt{x} = x_0\}\ C\ \{\texttt{diff} = x_0 - \texttt{y}\}}\,(W{+}C)$$

   Proviamo che le side conditions della regola (While+Cons) sono verificate:

   - $\texttt{diff} = 0 \wedge \texttt{x} = x_0$ implica banalmente $\texttt{diff} = x_0 - \texttt{x}$;
   - $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} = \texttt{y}$ implica banalmente $\texttt{diff} = x_0 - \texttt{y}$.

   Proviamo che la side condition di (Assign+Cons) è verificata:

   $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \neq \texttt{y}$ implica banalmente $(\texttt{diff} + 1 = x_0 - \texttt{x})[\texttt{x} - 1/\texttt{x}]$, cioè $\texttt{diff} = x_0 - \texttt{x}$.

2. Perchè la corrispondente asserzione di correttezza totale sia valida occorre che, per ogni stato che verifica la precondizione, il comando *C* termini e nello stato finale valga la postcondione. È facile vedere che invece a partire da uno stato per cui vale la precondizione e $x_0 < \texttt{y}$ il comando non termina.

3. Si può aggiungere la condizione $x_0 \geq \texttt{y}$, ottenendo l'asserzione di correttezza totale

   $\{\texttt{diff} = 0 \wedge \texttt{x} = x_0 \wedge x_0 \geq \texttt{y}\}$

   ```
   while (x!=y) {
     x=x-1;diff=diff+1
   }
   ```

   $\{\Downarrow \texttt{diff} = x_0 - \texttt{y}\}$

   Scegliamo come nuova invariante $\mathit{INV} = \texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y}$, e come funzione di terminazione $t\colon \mathit{States} \to \mathbb{Z}$ definita da $t(s) = s(\texttt{x}) - s(\texttt{y})$.

   Il nuovo albero di prova è il seguente.

$$\dfrac{\dfrac{\dfrac{}{\{\mathit{INV} \wedge \texttt{x} \neq \texttt{y}\}\ \texttt{x=x-1}\ \{\Downarrow \texttt{diff} + 1 = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y}\}}\,(A{+}C) \quad \dfrac{}{\{\texttt{diff} + 1 = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y}\}\ \texttt{diff=diff+1}\ \{\Downarrow \mathit{INV}\}}\,(Assign)}{\{\mathit{INV} \wedge \texttt{x} \neq \texttt{y}\}\ \texttt{x=x-1;diff=diff+1}\ \{\Downarrow \mathit{INV}\}}\,(Seq)}{\{\texttt{diff} = 0 \wedge \texttt{x} = x_0 \wedge x_0 \geq \texttt{y}\}\ C\ \{\Downarrow \texttt{diff} = x_0 - \texttt{y}\}}\,(W{+}C)$$

   Proviamo che le side conditions della regola (While+Cons) sono verificate:

   - $\texttt{diff} = 0 \wedge \texttt{x} = x_0 \wedge x_0 \geq \texttt{y}$ implica banalmente $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y}$;
   - $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} = \texttt{y} \wedge \texttt{x} \geq \texttt{y}$ implica banalmente $\texttt{diff} = x_0 - y$.
   - *t* è una funzione di terminazione per *C* e *INV* perchè è facile vedere che:
     - $t(\{\mathit{INV} \wedge \texttt{x} \neq \texttt{y}\}) \subseteq \mathbb{N}$,
     - per ogni s in $\{\mathit{INV} \wedge \texttt{x} \neq \texttt{y}\}$, $t([\![\texttt{x=x-1;diff=diff+1}]\!]\, s) < t(s)$.

   Proviamo che la side condition di (Assign+Cons) è verificata:

   $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y} \wedge \texttt{x} \neq \texttt{y}$ implica banalmente $(\texttt{diff} + 1 = x_0 - \texttt{x} \wedge \texttt{x} \geq \texttt{y})[\texttt{x} - 1/\texttt{x}]$, cioè $\texttt{diff} = x_0 - \texttt{x} \wedge \texttt{x} - 1 \geq \texttt{y}$.