Verifica di Programmi: Correttezza Totale

Verifica di Componenti

La correttezza totale di componenti può essere dimostrata usando il sistema TD + la regola per regioni atomiche.

Tuttavia la "naturale" regola *while* per la costruzione dei **proof outline** per la correttezza totale di componenti non può essere utilizzata per dimostrare la correttezza totale di programmi paralleli:

$$\frac{\begin{array}{c}\{p \wedge B\}\ S^*\ \{p\} \\ \{p \wedge B \wedge t = z\}\ S^{**}\ \{t < z\} \\ p \rightarrow t \geq 0\end{array}}{\{\textbf{inv} : p\}\{\textbf{bd} : t\}\ \textbf{while}\ B\ \textbf{do}\ \{p \wedge B\}\ S^*\ \{p\}\ \textbf{od}\ \{p \wedge \neg B\}}$$

dove t è un'espressione intera e z una variabile intera che non compare in p, t, B, S^{**}.

Path

Definizione. Sia S una componente sequenziale. L'insieme **path(S)** è definitio per induzione su S:

- $path(skip) = \{\epsilon\}$
- $path(u := t) = \{u := t\}$
- $path(\langle S \rangle) = \{\langle S \rangle\}$
- $path(S_1; S_2) = path(S_1); path(S_2)$
- $path(\textbf{if } B \textbf{ then } S_1 \textbf{ else } S_2 \textbf{ fi}) = path(S_1) \cup path(S_2)$
- $path(\textbf{while } B \textbf{ do } S \textbf{ od}) = \{\epsilon\}$.

Proof Outline per la Correttezza Totale

(1) $\{p \wedge B\}\ S^*\ \{p\}$ standard
(2) $\{pre(R) \wedge t = z\}\ R\ \{t \leq z\}$ per ogni assegnamento normale o regione atomica R in S
(3) per ogni $\pi \in path(S)$ esiste un assegnamento normale o regione atomica R in π t.c. $\{pre(R) \wedge t = z\}\ R\ \{t < z\}$
(4) $p \rightarrow t \geq 0$

$\{\textbf{inv} : p\}\{\textbf{bd} : t\}$ **while** B **do** $\{p \wedge B\}\ S^*\ \{p\}$ **od** $\{p \wedge \neg B\}$

dove $pre(T)$ è un'asserzione che precede R nel proof outline $\{p \wedge B\}\ S^*\ \{p\}$.

Assenza di Interferenza

Definizione.

- $\{p\}\ S^*\ \{q\}$ proof outline per la componente S, A comando con precondizione $pre(A)$.
  A **non interferisce** con $\{p\}\ S^*\ \{q\}$ se
  - per ogni asserzione r in $\{p\}\ S^*\ \{q\}$, vale la formula $\{r \wedge pre(A)\}\ A\ \{r\}$;
  - per ogni funzione bound t in $\{p\}\ S^*\ \{q\}$, vale la formula $\{pre \wedge t = z\}\ A\ \{t \leq z\}$, dove z non occorre in A, t, $pre(A)$.

- Sia $[S_1|\ldots|S_n]$ un programma parallelo. Gli standard proof outline $\{p_i\}\ S_i^*\ \{q_i\}$, $i \in \{1,\ldots,n\}$ sono **privi di interferenza** se nessun assegnamento normale o regione atomica A in S_i interferisce con i proof outline $\{p_j\}\ S_j^*\ \{q_j\}$, per $j \neq i$.