Proof Outline di programmi deterministici: correttezza parziale

Sia S^* un **programma annotato** con asserzioni, alcune etichettate con **inv**. I **proof outline** per la correttezza parziale sono definiti induttivamente come segue:

(i) $\{p\}\ skip\ \{q\}$ (ii) $\{p[u := t]\}\ u := t\ \{p\}$ (iii) $\dfrac{\{p\}\ S_1^*\ \{r\}\quad \{r\}\ S *_2\ \{q\}}{\{p\}\ S_1^*;\ \{r\}\ S_2^*\ \{q\}}$

(iv) $$\frac{\{p \wedge B\}\ S_1^*\ \{q\}\quad \{p \wedge \neg B\}\ S_2^*\ \{q\}}{\{p\}\ \textbf{if}\ B\ \textbf{then}\ \{p \wedge B\}\ S_1^*\ \{q\}\ \textbf{else}\ \{p \wedge \neg B\}\ S_2^*\ \{q\}\ \textbf{fi}\ \{q\}}$$

(v) $$\frac{\{p \wedge B\}\ S^*\ \{p\}}{\{\textbf{inv} : p\}\ \textbf{while}\ B\ \textbf{do}\ \{p \wedge B\}\ S^*\ \{p\}\ \textbf{od}\ \{p \wedge \neg B\}}$$

(vi) $$\frac{p \to p_1\quad \{p_1\}\ S^*\ \{q_1\}\quad q_1 \to q}{\{p\}\{p_1\}\ S^*\ \{q_1\}\{q\}}$$ (vii) $$\frac{\{p\}\ S^*\ \{q\}}{\{p\}\ S^{**}\ \{q\}}$$

dove S^{**} è ottenuto da S^* omettendo alcune annotazioni senza etichetta **inv**.

Definizione. Un proof outline $\{p\}\ S^*\ \{q\}$ per la correttezza parziale è **standard** se ogni sottoprogramma T di S è preceduto da esattamente un'asserzione in S^*, $pre(T)$, e non ci sono altre asserzioni in S^*.

Teorema.

(i) $\{p\}\ S^*\ \{q\} \implies \vdash_{PD} \{p\}\ S\ \{q\}$.

(ii) $\vdash_{PD} \{p\}\ S\ \{q\} \implies$ there exists a standard proof outline $\{p\}\ S^*\ \{q\}$.

Resto di un programma

Definizione. Sia T un sottoprogramma di S. Definiamo $at(T, S)$, il resto del programma S quando il controllo si trova all'inizio del sottoprogramma T come segue:

(i) se $S \equiv S_1; S_2$, se T sottoprogramma di S_1 allora $at(T, S) \equiv at(T, S_1)$, se T sottoprogramma di S_2 allora $at(T, S) \equiv at(T, S_2)$;

(ii) se $S \equiv$ **if** B **then** S_1 **else** S_2 **fi** e T sottoprogramma di S_i, allora $at(T, S) \equiv at(T, S_i)$ $(i = 1, 2)$;

(iii) se $S \equiv$ **while** B **do** S' **od** e T sottoprogramma di S', allora $at(T, S) \equiv at(T, S'); S$;

(iv) se $T \equiv S$, allora $at(T, S) \equiv S$.

Correttezza Forte

Sia $\{p\}\ S^*\ \{q\}$ standard. Se $\langle S, \sigma\rangle \rightarrow^* \langle R, \tau\rangle$, dove $\sigma \models p$, allora

- $R \equiv at(T, S)$, T sottoprogramma di $S \Longrightarrow \tau \models pre(T)$
- $R \equiv E \Longrightarrow \tau \models q$.

Proof Outline per la correttezza totale

Siano S^*, S^{**} programmi annotati con asserzioni, alcune etichettate con **inv** o **bd**. Un **proof outline** per la correttezza totale è definito dalle regole (i)–(iv), (vi) più la seguente regola:

(vii) $$\frac{\{p \wedge B\}\ S^*\ \{p\}\quad \{p \wedge B \wedge t = z\}\ S^{**}\ \{t < z\}\quad p \rightarrow t \geq 0}{\{\textbf{inv} : p\}\{\textbf{bd} : t\}\ \textbf{while}\ B\ \textbf{do}\ \{p \wedge B\}\ S^*\ \{p\}\ \textbf{od}\ \{p \wedge \neg B\}\}}$$

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

Verifica di programmi paralleli: correttezza parziale

Correttezza parziale delle componenti

Il sistema di regole per la correttezza parziale di componenti comprende le regole in *PD* più la regola per le **regioni atomiche**:

$$\frac{\{p\}\ S\ \{q\}}{\{p\}\ \langle S\rangle\ \{q\}}$$

I proof outline per la correttezza parziale di componenti sono generati dalle regole per programmi deterministici più la regola:

$$(\mathsf{X}) \qquad \frac{\{p\}\ S^*\ \{q\}}{\{p\}\ \langle S^*\rangle\ \{q\}}$$

Un proof outline $\{p\}\ S^*\ \{q\}$ è **standard** se ogni sottoprogramma **normale** T in S è preceduto da esattamente un'asserzione, $pre(T)$,e non ci sono ulteriori asserzioni in S^*. In particolare, non ci sono asserzioni all'interno di regioni atomiche.

Correttezza forte di componenti

Sia S una componente e $\{p\}\ S^*\ \{q\}$ un proof outline per la correttezza parziale. Se $\langle S, \sigma\rangle \rightarrow^* \langle R, \tau\rangle$, dove $\sigma \models p$, allora

- $R \equiv at(T, S)$ dove T è un sottoprogramma normale di S e $\tau \models pre(T)$ oppure
- $R \equiv E$ e $\tau \models q$.

Verifica di programmi paralleli: non interferenza

Definizione.

(i) Sia S una componente, $\{p\}\ S^*\ \{q\}$ uno standard proof outline, R un comando con precondizione $pre(R)$. R **non interferisce** con $\{p\}\ S\ \{q\}$ se, per ogni asserzione r in $\{p\}\ S^*\ \{q\}$, la formula $\{r \wedge pre(R)\}\ R\ \{r\}$ vale.

(ii) 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 di S_i interferisce con $\{p_j\}\ S_j^*\ \{q_j\}$, per $i \neq j$.

Regola per il parallelismo con variabili condivise

$$\frac{\text{I proof outline standard } \{p_i\}\ S_i^*\ \{q_i\},\ i \in \{1,\ldots,n\},\ \text{sono privi di interferenza}}{\{\bigwedge_{i=1}^{n} p_i\}\ [S_1|\ldots|S_n]\ \{\bigwedge_{i=1}^{n} q_i\}}$$

Incompletezza

Lemma. Il sistema *PD*+regola per il parallelismo è incompleto.

E.g. non è derivabile la formula:

$$\{\textbf{true}\}\ [X := x + 2 | x := 0]\ \{x = 0 \vee x = 2\}\ .$$

Il sistema PSV

Il **sistema PSV** consiste delle seguenti regole

- regole del sistema *PD*;
- regola per azioni atomiche;
- regola per il parallelismo con variabili condivise;
- regola delle variabili ausiliarie:

$$\frac{\{p\}\ S\{q\}}{\{p\}\ S_0\ \{q\}}$$

  dove S_0 è ottenuto da S cancellando gli assegnamenti a variabili in A, per A insieme di variabili ausiliarie di S tale che $free(q) \cap A = \emptyset$.
  Un insieme $A \subseteq var(S)$ è un **insieme di variabili ausiliarie** di S se ogni variabile di A occorre in S solo in assegnamenti del tipo $z := t$ con $z \in A$.

- regole ausiliarie.

Regole Ausiliarie

Invarianza: $\dfrac{free(p) \cap change(S) = \emptyset}{\{p\}\ S\ \{p\}}$

Disgiunzione: $\dfrac{\{p\}\ S\ \{q\}\ \{r\}\ S\ \{q\}}{\{p \vee r\}\ S\ \{q\}}$

Congiunzione: $\dfrac{\{p_1\}\ S\ \{q_1\}\ \{p_2\}\ S\ \{q_2\}}{\{p_1 \wedge p_2\}\ S\ \{q_1 \wedge q_2\}}$

$\exists$-*Introduzione*: $\dfrac{\{p\}\ S\ \{q\}}{\{\exists x : p\}\ S\ \{q\}}\quad x \notin var(S) \cup free(q)$

Invarianza: $\dfrac{\{r\}\ S\ \{q\}}{\{p \wedge r\}\ S\ \{p \wedge q\}}\quad free(p) \cap change(S) = \emptyset$

Correttezza forte di programmi paralleli

Siano $\{p_i\}\ S_i^*\ \{q_i\}$, $i \in \{1, \ldots, n\}$ proof outline standard di componenti prive di interferenza. Se

$$\langle [S_1 | \ldots | S_n], \sigma] \rangle \rightarrow^* \langle [R_1 | \ldots | R_n], \tau \rangle$$

dove $\sigma \models \bigvee_{i=1}^{n} p_i$, allora, per ogni $j \in \{1, \ldots, n\}$,

- se $R_j \equiv at(T, S_j)$ per T sottoprogramma normale di S_j, allora $\tau \models pre(T)$;
- se $R_j \equiv E$, allora $\tau \models q_j$.

In particolare, se $\langle [S_1 | \ldots | S_n], \sigma] \rangle \rightarrow^* \langle E, \tau \rangle$, allora $\tau \models \bigwedge_{i=1}^{n} q_i$.

Corollario.

(i) La regola del **parallelismo con variabili condivise** è **corretta** rispetto alla correttezza parziale di programmi paralleli.

(ii) Il sistema **PSV** è **corretto** rispetto alla correttezza parziale di programmi paralleli.