Semantyka i weryfikacja programów
notatka dotycząca dowodzenia całkowitej poprawności

Treść wykładu

Notatki do wykładu https://www.mimuw.edu.pl/~tarlecki/teaching/semwer/slides/total.pdf podają na slajdzie 205 przykład reguły dla while postaci:

$$
\begin{array}{l}
[\phi] \\
\texttt{while}\ b\ \texttt{do}\ [\ \text{decr}\ \alpha\ \text{in}\ X\ \text{wrt}\ \succ\ ] \\
\{ \\
\quad [\phi \wedge b] \\
\quad I \\
\quad [\phi] \\
\} \\
[\phi \wedge \neg b]
\end{array}
$$

gdzie X jest to w zasadzie dowolny (patrz niżej) zbiór, natomiast α to funkcja częściowa[1] ze stanów programu w X.

Wcześniej (na slajdzie 203) jest powiedziane, że w takim przypadku należy:

- wykazać całkowitą poprawność ciała pętli, czyli trójkę $[\phi \wedge b]\ I\ [\phi]$ (jest ona już wpisana powyżej we wnętrze pętli), co pokaże też częściową poprawność pętli,
- sprawdzić, że $\langle X, \succ \rangle$ jest zbiorem dobrze ufundowanym (tzn. $\succ \subseteq X \times X$ jest relacją dobrze ufundowaną na zbiorze X),
- sprawdzić, że dla każdego stanu s spełniającego $\phi \wedge b$, jeśli uruchomimy I w stanie s to wynikowy stan s' spełnia $\alpha(s) \succ \alpha(s')$.

Ostatni warunek wymaga w szczególności sprawdzenia, że jeśli s spełnia $\phi \wedge b$ to $\alpha(s) \in X$ oraz $\alpha(s') \in X$.

Powyższe podejście natrafia na rozmaite subtelności techniczne (np. jak można zadawać funkcję α, albo jakie dobrze ufundowane zbiory $\langle X, \succ \rangle$ dopuszczamy). Z tego względu, slajd 205 notatek z wykładu mówi o "różnych wariantach notacyjnych, bazujących na zewnętrznych definicjach zbiorów dobrze ufundowanych i funkcjach w nie".

Przykład reguły

Poniżej zaproponowana jest konkretna reguła gwarantująca poprawność rozumowania. Można (ale nie trzeba) opierać swoje rozwiązania na wykorzystaniu tej właśnie reguły dowodzenia.

Po pierwsze, ograniczamy rozważane zbiory X do postaci $\mathbb{N}^n$ dla $n \geq 1$. Po drugie, ograniczamy rozważane relacje dobrze ufundowane $\succ$ do "ścisłego" porządku leksykograficznego $\succ_{\text{lex}}$, "ścisłego" porządku po współrzędnych $\succ_{\text{coord}}$, oraz ich kombinacji (np. $\mathbb{N}^4$ ze "ścisłym" leksykograficznym porządkiem na $\langle \mathbb{N}^2, \succ_{\text{coord}} \rangle \times \langle \mathbb{N}^2, \succ_{\text{coord}} \rangle$).

Bardziej formalnie, *dozwolone* zbiory dobrze ufundowane to $\langle \mathbb{N}, > \rangle$ oraz $\langle O_1 \times \ldots \times O_n, \succ_{\text{lex}} \rangle$ i $\langle O_1 \times \ldots \times O_n, \succ_{\text{coord}} \rangle$, gdzie $O_1, \ldots, O_n$ są *dozwolone*.

Po trzecie, ograniczamy funkcje α do postaci krotek wyrażeń arytmetycznych, czyli $(e_1, \ldots, e_n)$, gdzie $e_i \in \mathit{Expr}$.

Wreszcie, reguła, z której korzystamy, jest następująca:

$$
\frac{\phi \wedge b \Longrightarrow \alpha \in X \qquad \big[\phi \wedge b \wedge \alpha{=}(\ell_1, \ldots, \ell_n)\big]\ I\ [\phi \wedge \alpha{\prec}(\ell_1, \ldots, \ell_n) \wedge \alpha \in X]}{[\phi]\ \texttt{while}\ b\ \texttt{do}\ I\ [\phi \wedge \neg b]}
$$

gdzie zmienne $\ell_1, \ldots, \ell_n$ nie występują nigdzie w b, I, α ani w niezmienniku ϕ. Ze względu na to, że $X = \mathbb{N}^n$ zaś $\alpha = (e_1, \ldots, e_n)$, to warunek $\alpha \in X$ sprowadza się do koniunkcji $e_1 \geq 0 \wedge \ldots \wedge e_n \geq 0$.

[1] Zwykle α jest funkcją całkowitą w nadzbiór X, a my dodatkowo sprawdzamy, że dla rozważanych stanów $\alpha(s) \in X$.

Ta sama reguła, zapisana jako anotacja programu, ma postać:

$$
\begin{array}{l}
[\phi] \\
\texttt{while}\ b\ \texttt{do}\ [\ \text{decr}\ \alpha\ \text{in}\ X\ \text{wrt}\ \succ\ ] \\
\{ \\
\quad [\phi \wedge b \wedge \alpha{=}(\ell_1, \ldots, \ell_n)]\ * \\
\quad I \\
\quad [\phi \wedge \alpha{\prec}(\ell_1, \ldots, \ell_n) \wedge \alpha \in X] \\
\} \\
[\phi \wedge \neg b]
\end{array}
$$

gdzie $*$ sygnalizuje wymaganie, że zachodzi implikacja $\phi \wedge b \Longrightarrow \alpha \in X$.