FMSoft
Lecture 12 — weakest liberal preconditions and relative completeness

(lecture version)

Tadeusz Litak

Jan 15, 2019

Informatik 8, FAU Erlangen-Nürnberg

weakest liberal preconditions

- We used rules for assignment, sequencing, and of course consequence and while loops

- We used rules for assignment, sequencing, and of course consequence and while loops
- The applications of consequence rule are very easy to verify to whichever tractable subsystem of arithmetic we pick

  the only possible exception being this infinitary definition of factorial

- We used rules for assignment, sequencing, and of course consequence and while loops
- The applications of consequence rule are very easy to verify to whichever tractable subsystem of arithmetic we pick

  the only possible exception being this infinitary definition of factorial
- We see that we have a sound system which can be used for annotating programs

- We used rules for assignment, sequencing, and of course consequence and while loops
- The applications of consequence rule are very easy to verify to whichever tractable subsystem of arithmetic we pick

  the only possible exception being this infinitary definition of factorial
- We see that we have a sound system which can be used for annotating programs
- We can return now to question of (relative) completeness: are our rules as general as possible?

  again, assuming somebody gives us an oracle for arithmetic ...

- Here come weakest (liberal) preconditions

- Here come weakest (liberal) preconditions
- Define $WLP_I(c, B) := \{\sigma \in \mathsf{States}_{\mathsf{IMP}} \mid [\![c]\!]\sigma \vDash^I B\}$

  This is the semantic version of weakest liberal preconditions

  Ordinary (total) weakest preconditions are obtained with total $\perp\!\!\perp$-convention for $\vDash^I$

- Here come weakest (liberal) preconditions
- Define $WLP_I(c, B) := \{\sigma \in \mathsf{States}_{\mathsf{IMP}} \mid [\![c]\!]\sigma \models^I B\}$

  This is the semantic version of weakest liberal preconditions

  Ordinary (total) weakest preconditions are obtained with total $\perp\!\!\!\perp$-convention for $\models^I$
- Note: $\models^I \boldsymbol{\{}A\boldsymbol{\}}\, c \boldsymbol{\{}B\boldsymbol{\}}$ iff $[\![A]\!]_I \subseteq WLP_I(c, B)$

  In this way, we switch perspective to predicate transformer semantics

- For any pair c, B, can we possibly find $wlp(c, B)$ s.t. for any I, $[\![wlp(c, B)]\!]_I = WLP_I(c, B)$?

- For any pair c, B, can we possibly find $wlp(c, B)$ s.t. for any I, $[\![wlp(c, B)]\!]_I = WLP_I(c, B)$?
- Further, can we show that $\vdash \{wlp(c, B)\}\, c \{B\}$?

- For any pair c, B, can we possibly find $wlp(c, B)$ s.t. for any I, $[\![wlp(c, B)]\!]_I = WLP_I(c, B)$?
- Further, can we show that $\vdash \{ wlp(c, B) \} \, c \{ B \}$?
- Assertion languages allowing such a function are expressive

- For any pair c, B, can we possibly find $wlp(c, B)$ s.t. for any I, $[\![wlp(c, B)]\!]_I = WLP_I(c, B)$?
- Further, can we show that $\vdash \{wlp(c, B)\}\, c \{B\}$?
- Assertion languages allowing such a function are expressive
- Note that in the presence of the consequence rule, expressivity trivially implies (relative) completeness: WHY?

Let us try to define

$$wlp : \mathsf{Com} \to \mathsf{AssertHo} \to \mathsf{AssertHo} \qquad \text{by}$$

$$\begin{aligned}
&wlp(\texttt{SKIP}, B) := B \\
&wlp(\texttt{X := } a, B) := B[a/\texttt{X}] \\
&wlp(c_1\texttt{;}c_2, B) := wlp(c_1, wlp(c_2, B)) \\
&wlp(\texttt{IF } b \texttt{ THEN } c_1 \texttt{ ELSE } c_2, B) := \\
&\qquad (b \wedge wlp(c_1, B)) \vee (\neg b \wedge wlp(c_2, B)) \\
&wlp(\texttt{WHILE } b \texttt{ DO } c \texttt{ END}, B) := \textstyle\bigwedge_{n \in \mathbb{N}} A_n^{b,B,c}
\end{aligned}$$

where

$$\begin{aligned}
A_0^{b,B,c} &= \top \\
A_{n+1}^{b,B,c} &= (b \wedge wlp(c, A_n^{b,B,c})) \vee (\neg b \wedge B)
\end{aligned}$$

Theorem
IMP *is expressive, with wlp being the witnessing function*

We have to show that for any c that

(*) $\vdash \{ wlp(c, B) \} \, c \{ B \}$

(!) ...and that for any I,
$[\![wlp(c, B)]\!]_I = \{\sigma \in \mathsf{States}_{\mathsf{IMP}} \mid [\![c]\!]\sigma \vDash^I B\}$

Note that one half of (!) we could get via (*) and the Soundness Theorem.

Theorem
IMP *is expressive, with wlp being the witnessing function*

We have to show that for any c that

(*) $\vdash \{wlp(c, B)\}\, c\, \{B\}$

(!) ...and that for any I,
$[\![wlp(c, B)]\!]_I = \{\sigma \in \mathsf{States}_{\mathsf{IMP}} \mid [\![c]\!]\sigma \vDash^I B\}$

Note that one half of (!) we could get via (*) and the Soundness Theorem.

That is, if we show (*), then soundness yields for any I,

$[\![wlp(c, B)]\!]_I \subseteq \{\sigma \in \mathsf{States}_{\mathsf{IMP}} \mid [\![c]\!]\sigma \vDash^I B\}$

Proof.

The proof is by induction on c. We need to prove both (*) and (!) clauses together for each construct, as in some inductive steps we want to use both of them at the same time.

We do not present all steps in the logically right order. For convenience group them as follows:

1. present non-`WHILE` (*) clauses
2. present non-`WHILE` (!) clauses

   assuming previous inductive steps of (*) and (!) have been established
3. present (*) and (!) for `WHILE`

   assuming previous inductive steps of (*) and (!) have been established

The (*) claim is straightforward for almost every program construct apart from `WHILE` (apart from a trivial boolean transformation for `IF`).

The situation with non-WHILE clauses of the missing half of (!) is similar, but let us see it in more detail: for any σ,

- $[\![\ \texttt{SKIP}\ ]\!]\sigma\ (=\sigma) \vDash^I B$ implies

  (in fact, is equivalent to)

  $\sigma \vDash^I B = wlp(\ \texttt{SKIP}\ , B)$

The situation with non-$\texttt{WHILE}$ clauses of the missing half of (!) is similar, but let us see it in more detail: for any σ,

- $[\![\ \texttt{SKIP}\ ]\!]\sigma\ (= \sigma) \vDash^I B$ implies

  (in fact, is equivalent to)

  $\sigma \vDash^I B = wlp(\ \texttt{SKIP}\ , B)$

- $[\![\ \texttt{X}\ \ \texttt{:=}\ a]\!]\sigma\ (= \sigma[[\![a]\!]\sigma/\ \texttt{X}\ ]) \vDash^I B$ is ...

  now we use an equivalence we proved before (when?) in the opposite direction

  ...equivalent to $\sigma \vDash^I B[a/\texttt{X}] = wlp(\ \texttt{X}\ \ \texttt{:=}\ a, B)$

The situation with non-WHILE clauses of the missing half of (!) is similar, but let us see it in more detail: for any σ,

- $[\![\ \mathtt{SKIP}\ ]\!]\sigma\ (= \sigma) \vDash^{I} B$ implies

  (in fact, is equivalent to)

  $\sigma \vDash^{I} B = wlp(\ \mathtt{SKIP}\ , B)$

- $[\![\ \mathtt{X}\ \ \mathtt{:=}\ a]\!]\sigma\ (= \sigma[[\![a]\!]\sigma/\ \mathtt{X}\ ]) \vDash^{I} B$ is ...

  now we use an equivalence we proved before (when?) in the opposite direction

  ...equivalent to $\sigma \vDash^{I} B[a/\mathtt{X}] = wlp(\ \mathtt{X}\ \ \mathtt{:=}\ a, B)$

- $[\![c_1\ \mathtt{;}\ c_2]\!]\sigma\ (= [\![c_2]\!]([\![c_1]\!]\sigma)) \vDash^{I} B$ by IH implies that $[\![c_1]\!]\sigma \vDash^{I} wlp(c_2, B)$ and using IH again gets us home

The situation with non-WHILE clauses of the missing half of (!) is similar, but let us see it in more detail: for any σ,

- $[\![\texttt{SKIP}]\!]\sigma \ (= \sigma) \vDash^I B$ implies

  (in fact, is equivalent to)

  $\sigma \vDash^I B = wlp(\texttt{SKIP}, B)$
- $[\![\texttt{X} := a]\!]\sigma \ (= \sigma[[\![a]\!]\sigma/\texttt{X}]) \vDash^I B$ is ...

  now we use an equivalence we proved before (when?) in the opposite direction

  ...equivalent to $\sigma \vDash^I B[a/\texttt{X}] = wlp(\texttt{X} := a, B)$
- $[\![c_1 \ ; \ c_2]\!]\sigma \ (= [\![c_2]\!]([\![c_1]\!]\sigma)) \vDash^I B$ by IH implies that $[\![c_1]\!]\sigma \vDash^I wlp(c_2, B)$ and using IH again gets us home
- $[\![\texttt{IF} \ b \ \texttt{THEN} \ c_1 \ \texttt{ELSE} \ c_2]\!]\sigma \vDash^I B$ left as exercise (trivial splitting of cases)

We have finished 2 out of 3 points in the expressivity proof

The difficult part is `WHILE`: to be done next time