Fundamentele limbajelor de programare

Semantica Logicii Hoare. Cea mai slabă precondiție.

Traian Florin Șerbănuță și Andrei Sipoș

Facultatea de Matematică și Informatică, DL Info

Anul II, Semestrul II, 2024/2025

Secțiunea 1

Limbajul propozițiilor

Ce fel de afirmații putem face in Logica Hoare?

Pre-condiția și post-condiția se construiesc din:

- variabilele programului `M`, `N` , `Sum` din L
- numere $42, 13, 7, 3$
- **variabile logice** x, y, z, t
- operații aritmetice $+, -, *$
- relații aritmetice $\leqslant, =$
- logică propozițională **true**, **false**, $\neg$, $\wedge$, $\vee$
- cuantificatori $\forall, \exists$

Expresii aritmetice extinse

Fixăm o mulțime V, ale cărei elemente vor fi numite **variabile logice**, care vor avea oarecum același rol ca variabilele din logica de ordinul I (altul decât cel al variabilelor din IMP, numite și **variabile de program**, care reprezentau locuri în memorie, ca în limbajele imperative uzuale).

O **expresie aritmetică extinsă** va avea exact una dintre următoarele forme:

- un număr întreg n;
- o variabilă de program X (element al lui L);
- o variabilă logică x (element al lui V);
- $a_0 + a_1$, $a_0 - a_1$, $a_0 * a_1$, unde a_0 și a_1 sunt expresii aritmetice extinse.

Expresii booleene extinse (aserțiuni)

O **expresie booleană extinsă**, numită și **aserțiune**, va avea exact una dintre următoarele forme:

- o valoare booleană (**true** sau **false**);
- $a_0 = a_1$, $a_0 \leqslant a_1$, unde a_0 și a_1 sunt expresii aritmetice extinse;
- $\neg A_0$, $A_0 \wedge A_1$, $A_0 \vee A_1$, unde A_0 și A_1 sunt aserțiuni;
- $\forall x A$, unde $x \in V$ și A este o aserțiune.

Considerăm cunoscută prescurtările $A \rightarrow B$ pentru $(\neg A) \vee B$, $\exists x A$ pentru $\neg \forall x \neg A$

Substituția

Putem defini în modul absolut natural substituțiile de forma $A[x := a]$ sau $A[X := a]$, unde A este o aserțiune, $X \in L$, $x \in V$, iar a este o expresie aritmetică – nu extinsă: de aceea, nu trebuie să ne preocupăm de redenumiri de variabile logice (cum o facem la logica de ordinul I). Enunțăm doar clauza:

$$(\forall z A)[x := a] := \begin{cases} \forall z A, & \text{dacă } z = x, \\ \forall z (A[x := a]), & \text{altfel.} \end{cases}$$

Evaluarea expresiilor aritmetice extinse

Vom numi **interpretare** o funcție de la V la $\mathbb{Z}$. Pentru orice $\sigma \in \Sigma$ și orice interpretare $I : V \to \mathbb{Z}$, definim o funcție $|\cdot|_\sigma^I$ care evaluează expresii aritmetice extinse în numere întregi, în mod recursiv, în felul următor:

- pentru orice $N \in \mathbb{Z}$, $|N|_\sigma^I := N$;
- pentru orice $X \in L$, $|X|_\sigma^I := \sigma(X)$;
- pentru orice $x \in V$, $|x|_\sigma^I := I(x)$;
- pentru orice expresii aritmetice extinse a_0, a_1, avem
  $|a_0 + a_1|_\sigma^I := |a_0|_\sigma^I + |a_1|_\sigma^I$, $|a_0 - a_1|_\sigma^I := |a_0|_\sigma^I - |a_1|_\sigma^I$,
  $|a_0 * a_1|_\sigma^I := |a_0|_\sigma^I * |a_1|_\sigma^I$.

Avem că, pentru orice expresie aritmetică (ne-extinsă) a, $|a|_\sigma^I = n$ dacă și numai dacă $\langle a, \sigma \rangle \Downarrow n$.

Analog cu cele anterioare, pentru orice $I : V \to \mathbb{Z}$, $x \in V$ și $N \in \mathbb{Z}$, definim interpretarea $I_{x \mapsto N}$, pentru orice $y \in V$, prin:

$$I_{x \mapsto N}(y) := \begin{cases} N, & \text{dacă } y = x, \\ I(y), & \text{altfel.} \end{cases}$$

Evaluarea asertiunilor

Definim acum, pentru $\sigma \in \Sigma$, $I : V \to \mathbb{Z}$ și A asertiune, relația $\sigma \models^I A$, în mod recursiv, în felul următor:

- $\sigma \models^I \textbf{true}$, $\sigma \not\models^I \textbf{false}$;
- pentru orice expresii aritmetice extinse a_0, a_1, avem
  $\sigma \models^I a_0 = a_1$ dacă și numai dacă $|a_0|^I_\sigma = |a_1|^I_\sigma$,
  $\sigma \models^I a_0 \leqslant a_1$ dacă și numai dacă $|a_0|^I_\sigma \leqslant |a_1|^I_\sigma$;
- pentru orice asertiuni A_0, A_1, avem
  $\sigma \models^I \neg A_0$ dacă și numai dacă $\sigma \not\models^I A_0$,
  $\sigma \models^I A_0 \wedge A_1$ dacă și numai dacă $\sigma \models^I A_0$ și $\sigma \models^I A_1$,
  $\sigma \models^I A_0 \vee A_1$ dacă și numai dacă $\sigma \models^I A_0$ sau $\sigma \models^I A_1$;
- pentru orice $x \in V$ și orice asertiune A, avem
  $\sigma \models^I \forall x A$ dacă și numai dacă, pentru orice $N \in \mathbb{Z}$, $\sigma \models^{I_{x \mapsto N}} A$.

Avem că, pentru orice expresie booleană (ne-extinsă) b, $\sigma \models^I b$ dacă și numai dacă $\langle b, \sigma \rangle \Downarrow \langle \textbf{true} \rangle$. Notăm cu $\models A$ faptul că, pentru orice σ și I, $\sigma \models^I A$. Notăm și $A^I := \{\sigma \in \Sigma \mid \sigma \models^I A\}$.

Semantica enunțurilor Hoare (folosind semantica big-step)

Fie $\{A\}\ c\ \{B\}$ un enunț Hoare, unde A și B sunt asertțiuni, iar c este o instrucțiune.

Definim semantica acestora în felul următor:

- pentru orice σ și I, $\sigma \models^I \{A\}c\{B\}$ dacă $\sigma \models^I A$ implică faptul că, pentru orice σ' cu $\langle c, \sigma\rangle \Downarrow \langle\sigma'\rangle$, $\sigma' \models^I B$;
- pentru orice I, $\models^I \{A\}c\{B\}$ dacă, pentru orice σ, $\sigma \models^I \{A\}c\{B\}$, sau, echivalent, pentru orice $\langle c, \sigma\rangle \Downarrow \langle\sigma'\rangle$, $\sigma \models^I A$ implică $\sigma' \models^I B$;
- $\models \{A\}c\{B\}$ dacă, pentru orice I, $\models^I \{A\}c\{B\}$.

Logica Hoare

- $\{Q\}\ \texttt{skip}\ \{Q\}$ (Skip)
- $\{Q[x := e]\}\ \texttt{x := e}\ \{Q\}$ (Atribuire)
- $\dfrac{\{P_w\}\ \texttt{S}\ \{Q\}}{\{P_s\}\ \texttt{S}\ \{Q\}}$ *dacă* $\models P_s \to P_w$ (Întărire pre)
- $\dfrac{\{P\}\ \texttt{S}\ \{Q_s\}}{\{P\}\ \texttt{S}\ \{Q_w\}}$ *dacă* $\models Q_s \to Q_w$ (Slăbire post)
- $\dfrac{\{P\}\ \texttt{S}_1\ \{Q\} \qquad \{Q\}\ \texttt{S}_2\ \{R\}}{\{P\}\ \texttt{S}_1\texttt{;S}_2\ \{R\}}$ (Secvențiere)
- $\dfrac{\{P \wedge b\}\ \texttt{S}_1\ \{Q\} \qquad \{P \wedge \neg b\}\ \texttt{S}_2\ \{Q\}}{\{P\}\ \texttt{if b then S}_1\ \texttt{else S}_2\ \{Q\}}$ (If)
- $\dfrac{\{P \wedge b\}\ \texttt{S}\ \{P\}}{\{P\}\ \texttt{while b do S}\ \{P \wedge \neg b\}}$ (While)

Notăm $\vdash \{\mathbf{P}\}\ \texttt{c}\ \{\mathbf{Q}\}$ dacă $\{P\}\ \texttt{c}\ \{Q\}$ aparține mulțimii definite de aceste reguli.

Teorema de corectitudine

Teorema de corectitudine

Pentru orice A, B, c cu $\vdash \{A\}c\{B\}$, avem $\models \{A\}c\{B\}$.

Demonstrație (inducție după regulile Hoare, pe sărite)

$\{Q[x := e]\}\ \mathtt{x := e}\ \{Q\}$ (Atribuire)

Fie σ, I astfel incât $\sigma \models^I Q[x := e]$ și σ' astfel încât $\langle \mathtt{x := e}, \sigma\rangle \Downarrow \langle\sigma'\rangle$.
Atunci există n astfel încât $\langle e, \sigma\rangle \Downarrow \langle n\rangle$ și $\sigma' = \sigma[x := n]$.
Avem că $|e|^I_\sigma = n$ și se poate demonstra prin inducție asupra lui Q că $\sigma \models^I Q[x := e]$ implică $\sigma' \models^I Q$.

$$\frac{\{P\}\ \mathtt{S}_1\ \{Q\} \qquad \{Q\}\ \mathtt{S}_2\ \{R\}}{\{P\}\ \mathtt{S}_1; \mathtt{S}_2\ \{R\}}$$ (Secvențiere)

Presupunem ipoteza adevărată pentru $\{P\}\ \mathtt{S}_1\ \{Q\}$ și $\{Q\}\ \mathtt{S}_2\ \{R\}$. Fie σ, I astfel încât $\sigma \models^I P$ și σ' astfel încât $\langle \mathtt{S}_1; \mathtt{S}_2, \sigma\rangle \Downarrow \langle\sigma'\rangle$. Atunci există σ'' astfel încât $\langle \mathtt{S}_1, \sigma\rangle \Downarrow \langle\sigma''\rangle$ și $\langle \mathtt{S}_2, \sigma''\rangle \Downarrow \langle\sigma'\rangle$.
Din ipoteza de inducție pentru $\{P\}\ \mathtt{S}_1\ \{Q\}$ avem că $\sigma'' \models^I Q$.
Din ipoteza de inducție pentru $\{Q\}\ \mathtt{S}_2\ \{R\}$ avem că $\sigma' \models^I R$.

Teorema de corectitudine

Teorema de corectitudine

Pentru orice A, B, c cu $\vdash \{A\}c\{B\}$, avem $\models \{A\}c\{B\}$.

Demonstrație (cont.)

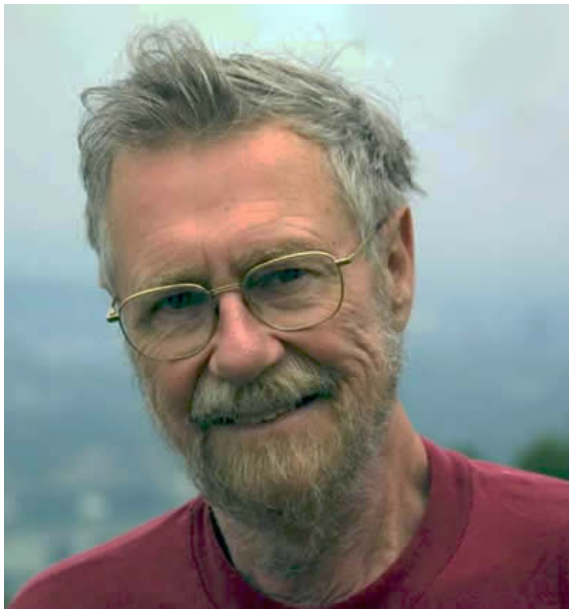
$$\frac{\{A \wedge b\}\ \mathtt{S}\ \{A\}}{\{A\}\ \mathtt{while\ b\ do\ S}\ \{A \wedge \neg b\}}\ (\textsc{While})$$

Notăm $w :=$`while` b `do` S. Presupunem $\models \{A \wedge b\}S\{A\}$ (ip. inducție).
Fie $I : V \to \mathbb{Z}$. Demonstrăm că pentru orice σ, σ' astfel încât $\langle w, \sigma\rangle \Downarrow \langle\sigma'\rangle$, $\sigma \models^I A$ implică $\sigma' \models^I A \wedge \neg b$ prin inducție după regulile big-step.
Dacă $\frac{\langle b,\sigma\rangle\Downarrow\langle\mathtt{false}\rangle}{\langle w,\sigma\rangle\Downarrow\sigma}$ (While-false):
Avem $\sigma' = \sigma$ și deducem $\sigma \not\models^I b$, deci $\sigma \models^I \neg b$, deci $\sigma \models^I A \wedge \neg b$.
Dacă $\frac{\langle b,\sigma\rangle\Downarrow\langle\mathtt{true}\rangle \qquad \langle S,\sigma\rangle\Downarrow\langle\sigma''\rangle \qquad \langle w,\sigma''\rangle\Downarrow\langle\sigma'\rangle}{\langle w,\sigma\rangle\Downarrow\sigma'}$ (While-true):
Putem presupune ipoteza de inducție pentru $\langle w, \sigma''\rangle \Downarrow \langle\sigma'\rangle$, adică, dacă $\sigma'' \models^I A$, atunci $\sigma' \models^I A \wedge \neg b$.
Deoarece $\langle b, \sigma\rangle \Downarrow \langle\mathtt{true}\rangle$, avem $\sigma \models^I b$, deci $\sigma \models^I A \wedge b$, și deoarece $\models \{A \wedge b\}S\{A\}$ și $\langle S, \sigma\rangle \Downarrow \langle\sigma''\rangle$, înseamnă că $\sigma'' \models^I A$, deci $\sigma' \models^I A \wedge \neg b$.

Secțiunea 2

Cea mai slabă precondiție

Edsger W. Dijkstra



- A inventat în 1956 un algoritm de determinare a celor mai scurte drumuri într-un graf
- A inventat în ~1962 noțiunea de *semafoare* pentru sincronizarea accesului la resurse în programarea concurentă
- A câștigat premiul Turing în 1972 pentru sustinerea programării structurate
- A introdus în 1975 **calculul celei mai slabe precondiții** ca o tehnică alternativă pentru verificarea corectitudinii programelor imperative

Calculul celei mai slabe pre-condiții

Logica Hoare ne prezintă probleme logice

- Dată fiind o pre-condiție P, codul $\mathtt{S}$, și post-condiția Q,
- este adevărat că $\{P\}\ \mathtt{S}\ \{Q\}$?

Calculul celei mai slabe pre-condiții descrie o **funcție**

- Dat fiind codul $\mathtt{S}$ și post-condiția Q
- găsiți acel P care este *cea mai slabă pre-condiție* pentru $\mathtt{S}$ și Q.

Cea mai slabă precondiție (semantică)

Pentru orice instrucțiune c, orice aserțiune B și orice interpretare I, definim **cea mai slabă precondiție liberală**[1] (**semantică**) a lor prin

mulțimea stărilor inițiale pentru care, după execuția lui c, B e adevărată

$$wls^I(c, B) := \{\sigma \in \Sigma \mid \text{pentru orice } \sigma' \in \Sigma \text{ cu } \langle c, \sigma\rangle \Downarrow \langle\sigma'\rangle,\ \sigma' \models^I B\}.$$

Avem că, pentru orice A, B, c, I, $\models^I \{A\}c\{B\}$ dacă și numai dacă $A^I \subseteq wls^I(c, B)$ (exercițiu!).

Am vrea să **capturăm** această mulțime ca o aserțiune W, adică să găsim W astfel încât $W^I = wls^I(c, B)$, pentru orice I.

[1] Liberală, în sensul că acceptă ideea de neterminare.

Definirea celei mai slabe precondiții (wp)

Vom avea:

$$
\begin{aligned}
wp(\textbf{skip}, B) &:= B \\
wp(X := a, B) &:= B[X := a] \\
wp(c_0; c_1, B) &:= wp(c_0, wp(c_1, B)) \\
wp(\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1, B) &:= (b \wedge wp(c_0, B)) \vee (\neg b \wedge wp(c_1, B)).
\end{aligned}
$$

Pentru **while**, notăm $w :=$`while` b `do` c și folosind că
$w \sim$`if` b `then` $(c; w)$ `else skip`, trebuie ca

$$
\begin{aligned}
wp(w, B) &= wp(\texttt{if } b \texttt{ then } (c; w) \texttt{ else skip}, B) \\
&= (b \wedge wp(c; w, B)) \vee (\neg b \wedge wp(\texttt{skip}, B)) \\
&= (b \wedge wp(c, wp(w, B))) \vee (\neg b \wedge B)
\end{aligned}
$$

Definirea celei mai slabe precondiții (while)

Vrem ca $wp(w, B) = (b \wedge wp(c, wp(w, B))) \vee (\neg b \wedge B)$

Definim șirul de asertiuni $(P_k)_{k \in N}$ recursiv astfel:

- $P_0 := \neg b \wedge B$
- $P_{k+1} := b \wedge wp(c, P_k)$

Presupunem că avem dijuncții infinitare în limbaj și definim

$$wp(w, B) := \bigvee_{k \in \mathbb{N}} P_k.$$

Intuiție: Dacă $\sigma \models^I wp(w, B)$, atunci

- există un k astfel încât $\sigma \models^I P_k$, deci
- execuția lui w din starea σ se va opri după k iterații și
- B va fi adevărată în starea finală.

Presupuneri Suplimentare (semantice)

Formula pentru while capturează ideea de terminare.

Definim deci, **cea mai slabă precondiție semantică** pentru instrucțiunea c față de post-condiția B în interpretarea I ca:

mulțimea stărilor inițiale pentru care execuția lui c se termină și B e adevărată în starea de după

$$ws^I(c, B) := \{\sigma \in \Sigma \mid \text{există } \sigma' \in \Sigma \text{ astfel încât } \langle c, \sigma\rangle \Downarrow \langle \sigma'\rangle \text{ și } \sigma' \models^I B\}.$$

Avem că $ws^I(c, B) \subseteq wls^I(c, B)$ ($wls^I(c, B)$ include și stările pentru care execuția nu se termină).

Observație: dacă execuția lui c se termină *în orice stare*, atunci $ws^I(c, B) = wls^I(c, B)$ (exercițiu!)

Teoremă

$wp(c, B)^I = ws^I(c, B)$

Demonstrație (inducție după regulile de definire ale lui *wp*)

Tratăm doar cazul pentru $w =$`while` b `do` S. Din ipoteza de inducție, presupunem că (1) pentru orice B, $wp(S, B)^I = ws^I(S, B)$
Pentru $\subseteq$“, fie σ cu $\sigma \models^I \bigvee_{k\in\mathbb{N}} P_k$, deci există $k \in \mathbb{N}$ cu $\sigma \models^I P_k$. Facem inducție după k.
Pentru $k = 0$, avem $\sigma \models^I \neg b \wedge B$, deci (2) $\sigma \models^I \neg b$ și (3) $\sigma \models^I B$. Din (2), $\langle b, \sigma\rangle \Downarrow \langle$`false`$\rangle$. Atunci $\langle w, \sigma\rangle \Downarrow \langle\sigma\rangle$ și concluzia e demonstrată datorită lui (3).
Pentru pasul de inducție, presupunem $\sigma \models^I b \wedge wp(c, P_k)$, deci (2) $\sigma \models^I b$ și (3) $\sigma \models^I wp(c, P_k)$. Din (2) $\langle b, \sigma\rangle \Downarrow \langle$`true`$\rangle$. Din (1) și (3), $\sigma \in ws^I(S, P_k)$, deci există σ'' astfel încăt (4) $\langle S, \sigma\rangle \Downarrow \langle\sigma''\rangle$ și $\sigma'' \models^I P_k$. Din ipoteza de inducție pentru k, există σ' astfel încât (5) $\langle w, \sigma''\rangle \Downarrow \langle\sigma'\rangle$ și (6) $\sigma' \models^I B$. Din (2), (4) și (5) rezultă că $\langle w, \sigma\rangle \Downarrow \langle\sigma'\rangle$ și folosind (6), că $\sigma \in ws^I(w, B)$.

Lemă ajutătoare

Dacă $\langle w, \sigma\rangle \Downarrow \langle \sigma'\rangle$ atunci există $n \geqslant 0$ și un șir finit de stări $(\sigma_i)_{i\leqslant n}$ cu $\sigma_0 = \sigma$, $\sigma_n = \sigma'$, $\langle b, \sigma_n\rangle \Downarrow \langle \texttt{false}\rangle$ și, pentru orice i cu $0 \leqslant i < n$, $\langle b, \sigma_i\rangle \Downarrow \langle \texttt{true}\rangle$ și $\langle S, \sigma_i\rangle \Downarrow \langle \sigma_{i+1}\rangle$.

Demonstrație (inducție după regulile big-step)

Dacă $\dfrac{\langle b,\sigma\rangle \Downarrow \langle \texttt{false}\rangle}{\langle w,\sigma\rangle \Downarrow \sigma}$ (While-false)

Alegem $n = 0$ și avem $\langle b, \sigma_0\rangle \Downarrow \langle \texttt{false}\rangle$.

Dacă $\dfrac{\langle b,\sigma\rangle \Downarrow \langle \texttt{true}\rangle \qquad \langle S,\sigma\rangle \Downarrow \langle \sigma''\rangle \qquad \langle w,\sigma''\rangle \Downarrow \langle \sigma'\rangle}{\langle w,\sigma\rangle \Downarrow \sigma'}$ (While-true):

Din ipoteza de inducție pentru $\langle w, \sigma''\rangle \Downarrow \langle \sigma'\rangle$ există $n' \geqslant 0$ și un șir finit de stări $(\sigma'_i)_{i\leqslant n'}$ cu $\sigma'_0 = \sigma''$, $\sigma'_{n'} = \sigma'$, $\langle b, \sigma'_{n'}\rangle \Downarrow \langle \texttt{false}\rangle$ și, pentru orice i cu $0 \leqslant i < n'$, $\langle b, \sigma'_i\rangle \Downarrow \langle \texttt{true}\rangle$ și $\langle S, \sigma'_i\rangle \Downarrow \langle \sigma'_{i+1}\rangle$.

Definim $n = n' + 1$ și $\sigma_0 = \sigma$, $\sigma_{i+1} = \sigma'_i$ pentru $0 \leqslant i \leqslant n$. Se verifică că $\langle b, \sigma_0\rangle \Downarrow \langle \texttt{true}\rangle$ și $\langle S, \sigma_0\rangle \Downarrow \langle \sigma_1\rangle$

Teoremă

Fie I o interpretare. pentru orice c, B, Atunci $wp(c, B)^I = ws^I(c, B)$.

Demonstrație (cont.)

Pentru $\supseteq$“, fie $\sigma \in ws^I(w, B)$. Deci există σ' astfel încât $\langle w, \sigma\rangle \Downarrow \langle\sigma'\rangle$ și $\sigma' \models^I B$.
Aplicând lema ajutătoare, fie $n \geqslant 0$ și un șir finit de stări $(\sigma_i)_{i\leqslant n}$ cu $\sigma_0 = \sigma$, $\sigma_n = \sigma'$, $\langle b, \sigma_n\rangle \Downarrow \langle\texttt{false}\rangle$ și, pentru orice i cu $0 \leqslant i < n$, $\langle b, \sigma_i\rangle \Downarrow \langle\texttt{true}\rangle$ și $\langle S, \sigma_i\rangle \Downarrow \langle\sigma_{i+1}\rangle$.
Se arată, apoi, că, pentru orice j cu $0 \leqslant j \leqslant n$, avem $\sigma_{n-j} \models^I P_j$, prin inducție după j (exercițiu!). Avem, deci, că $\sigma = \sigma_0 \models^I P_n$.

A se vedea și cursul de master “Program Verification”:

https://cs.unibuc.ro/~ddiaconescu/2019/pv/

Teorema de completitudine (relativă)

Fie c astfel încât execuția lui c **se termină in orice stare**.

Lemă

Fie B cu $\vdash \{wp(c, B)\}c\{B\}$. Fie A cu $\models \{A\}c\{B\}$. Atunci $\vdash \{A\}c\{B\}$.

Demonstrație

Din regula de slăbire a pre-condiției, e suficient să arătăm că
$\models A \to wp(c, B)$. Fie I. Cum $\models^I \{A\}c\{B\}$, avem
$A^I \subseteq wls^I(c, B) = ws^I(c, B) = wp(c, B)^I$, deci $\models^I A \to wp(c, B)$.

Teorema de completitudine

Pentru orice A, B, cu $\models \{A\}c\{B\}$, avem $\vdash \{A\}c\{B\}$.

Demonstrația teoremei de completitudine

Demonstrație (inducție structurală după c)

Din lema este suficient, la fiecare pas, să arătăm că, pentru orice B, $\vdash \{wp(c, B)\}c\{B\}$.
Vom trata cazurile instrucțiunilor **if** și **while**.
Pentru **if**, notăm $i :=$`if` b `then` c_0 `else` c_1. Știm:

$$wp(i, B) = (b \wedge wp(c_0, B)) \vee (\neg b \wedge wp(c_1, B)).$$

Este imediat că $\models wp(i, B) \wedge b \rightarrow wp(c_0, B)$. Din ipoteza de inducție, știm $\vdash \{wp(c_0, B)\}\ \mathrm{c}_0\ \{B\}$, așadar, din regula intăririi pre-condiției, scoatem $\vdash \{wp(i, B) \wedge b\}\ \mathrm{c}_0\ \{B\}$. Analog, $\vdash \{wp(i, B) \wedge \neg b\}\ \mathrm{c}_1\ \{B\}$. Concluzia rezultă aplicând regula pentru **if**.
Pentru **while**, notăm $w :=$`while` b `do` c și $A := wp(w, B)$.

Demonstrația teoremei de completitudine

Demonstrație (cont.)

Claim 1: $\models \{A \wedge b\} c \{A\}$.
Dem. claim: Fie I și (1) $\langle c, \sigma\rangle \Downarrow \langle \sigma''\rangle$. Presupunem $\sigma \models^I A \wedge b$, deci (2) $\langle b, \sigma\rangle \Downarrow \langle \texttt{true}\rangle$. Vrem $\sigma'' \in A^I = wp(w, B)^I = ws^I(w, B)$. Fie σ' cu (3) $\langle w, \sigma''\rangle \Downarrow \langle \sigma'\rangle$. Vrem $\sigma' \models^I B$. Din (2), (1), și (3), avem $\langle w, \sigma\rangle \Downarrow \langle \sigma'\rangle$. Cum $\sigma \models^I A$, adică $\sigma \in ws^I(w, B)$, rezultă $\sigma' \models^I B$.
Claim 2: $\models (A \wedge \neg b) \rightarrow B$.
Dem. claim: Fie σ, I cu $\sigma \models^I A \wedge \neg b$. Vrem $\sigma \models^I B$. Cum $\langle b, \sigma\rangle \Downarrow \langle \texttt{false}\rangle$, $\langle w, \sigma\rangle \Downarrow \langle \sigma\rangle$, iar cum $\sigma \in A^I = ws^I(w, B)$, avem $\sigma \models^I B$.
Demonstrăm acum că $\vdash \{A\}\ \texttt{w}\ \{B\}$. Aplicând ipoteza de inducție pe primul claim, avem $\vdash \{A \wedge b\}\ \texttt{c}\ \{A\}$, deci, din regula pentru **while**, avem $\vdash \{A\}\ \texttt{w}\ \{A \wedge \neg b\}$. Aplicând regula slăbirii post-condiției și al doilea claim, avem $\vdash \{A\}\ \texttt{w}\ \{B\}$.