Axiomatic Semantics

Hongfei Fu

John Hopcroft Center for Computer Science
Shanghai Jiao Tong University

Apr. 15th

Previous Lecture

- extended boolean assertions
- partial correctness assertions
- Hoare rules

Today's Topic

Axiomatic Semantics

- soundness of Hoare rules
- examples for using Hoare rules
- a start with completeness of Hoare rules

Soundness of Hoare Rules

Textbook, Page 91 – 93

Soundness and Completeness of Hoare Rules

Soundness

$\vdash \{A\}c\{B\}$ implies $\models \{A\}c\{B\}$.

Soundness and Completeness of Hoare Rules

Soundness

$\vdash \{A\}c\{B\}$ implies $\models \{A\}c\{B\}$.

Completeness

$\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$.

Soundness of Hoare Rules

Soundness

$\vdash \{A\}c\{B\}$ implies $\models \{A\}c\{B\}$.

Proof: Rule Induction

Prove that every rule is sound, i.e., the conclusion always holds if all the premises hold.

Soundness of Hoare Rules

Properties of Substitution

- a, a_0: extended arithmetic expressions in **Aexpv**
- X: a location (program variable)

Then for all interpretations I and states σ,

$$\mathcal{A}v[\![a_0\,[a/X]]\!](I,\sigma) = \mathcal{A}v[\![a_0]\!](I,\sigma\,[\mathcal{A}v[\![a]\!](I,\sigma)/X])$$

Soundness of Hoare Rules

Properties of Substitution

- a, a_0: extended arithmetic expressions in **Aexpv**
- X: a location (program variable)

Then for all interpretations I and states σ,

$$\mathcal{A}v[\![a_0\,[a/X]]\!](I,\sigma) = \mathcal{A}v[\![a_0]\!](I,\sigma\,[\mathcal{A}v[\![a]\!](I,\sigma)/X])$$

Proof

By structural induction on a_0.

Soundness of Hoare Rules

Properties of Substitution

- B: an extended boolean assertion from **Assn**
- X: a location (identifier)
- a: an arithmetic expression from **Aexp**

Then for all interpretations I and states σ, we have

$$\sigma \models^I B\,[a/X] \text{ iff } \sigma\,[\mathcal{A}[\![a]\!](\sigma)/X] \models^I B$$

Soundness of Hoare Rules

Properties of Substitution

- B: an extended boolean assertion from **Assn**
- X: a location (identifier)
- a: an arithmetic expression from **Aexp**

Then for all interpretations I and states σ, we have

$$\sigma \models^I B\,[a/X] \text{ iff } \sigma\,[\mathcal{A}[\![a]\!](\sigma)/X] \models^I B$$

Proof

By structural induction on B.

Soundness of Hoare Rules

Soundness

$\vdash \{A\}c\{B\}$ implies $\models \{A\}c\{B\}$.

Proof: Rule Induction

Prove that for every rule instance, if all the extended boolean assertions and partial correctness assertions in its premises are valid, then so is its conclusion.

Soundness of Hoare Rules

Skip

$$\frac{}{\{A\}\textbf{skip}\{A\}}$$

Soundness of Hoare Rules

Skip

$$\frac{}{\{A\}\textbf{skip}\{A\}}$$

- $\langle \textbf{skip}, \sigma \rangle \to \sigma$

Soundness of Hoare Rules

Skip

$$\frac{}{\{A\}\textbf{skip}\{A\}}$$

- $\langle \textbf{skip}, \sigma \rangle \to \sigma$
- $\sigma \models^{I} A \Rightarrow \sigma \models^{I} A$

Soundness of Hoare Rules

Skip

$$\frac{}{\{A\}\textbf{skip}\{A\}}$$

- $\langle \textbf{skip}, \sigma \rangle \to \sigma$
- $\sigma \models' A \Rightarrow \sigma \models' A$
- $\models \{A\}\textbf{skip}\{A\}$

Soundness of Hoare Rules

Assignment

$$\overline{\{B\,[a/X]\}X := a\{B\}}$$

Soundness of Hoare Rules

Assignment

$$\overline{\{B\,[a/X]\}X := a\{B\}}$$

- $\langle a, \sigma \rangle \to n$
- $\langle X := a, \sigma \rangle \to \sigma\,[n/X]$

Soundness of Hoare Rules

Assignment

$$\overline{\{B\,[a/X]\}X := a\{B\}}$$

- $\langle a, \sigma \rangle \to n$
- $\langle X := a, \sigma \rangle \to \sigma\,[n/X]$
- $\sigma \models^I B\,[a/X]$ iff $\sigma\,[n/X] \models^I B$

Soundness of Hoare Rules

Assignment

$$\overline{\{B\,[a/X]\}X := a\{B\}}$$

- $\langle a, \sigma \rangle \to n$
- $\langle X := a, \sigma \rangle \to \sigma\,[n/X]$
- $\sigma \models' B\,[a/X]$ iff $\sigma\,[n/X] \models' B$
- $\models \{B\,[a/X]\}X := a\{B\}$

Hoare Rules

Sequencing

$$\frac{\{A\}c_0\{C\}\ ,\ \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

Hoare Rules

Sequencing

$$\frac{\{A\}c_0\{C\}\ ,\ \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

- $\langle c_0; c_1, \sigma\rangle \to \sigma'$
- $\langle c_0, \sigma\rangle \to \sigma''$, $\langle c_1, \sigma''\rangle \to \sigma'$

Hoare Rules

Sequencing

$$\frac{\{A\}c_0\{C\}\ ,\ \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

- $\langle c_0; c_1, \sigma\rangle \to \sigma'$
- $\langle c_0, \sigma\rangle \to \sigma''$, $\langle c_1, \sigma''\rangle \to \sigma'$
- from $\models \{A\}c_0\{C\}$: $\sigma \models^I A \Rightarrow \sigma'' \models^I C$
- from $\models \{C\}c_1\{B\}$: $\sigma'' \models^I C \Rightarrow \sigma' \models^I B$
- $\sigma \models^I A \Rightarrow \sigma' \models^I B$

Hoare Rules

Sequencing

$$\frac{\{A\}c_0\{C\}\ ,\ \{C\}c_1\{B\}}{\{A\}c_0; c_1\{B\}}$$

- $\langle c_0; c_1, \sigma\rangle \to \sigma'$
- $\langle c_0, \sigma\rangle \to \sigma''$, $\langle c_1, \sigma''\rangle \to \sigma'$
- from $\models \{A\}c_0\{C\}$: $\sigma \models^I A \Rightarrow \sigma'' \models^I C$
- from $\models \{C\}c_1\{B\}$: $\sigma'' \models^I C \Rightarrow \sigma' \models^I B$
- $\sigma \models^I A \Rightarrow \sigma' \models^I B$
- $\models \{A\}c_0; c_1\{B\}$

Hoare Rules

Conditional Branch

$$\frac{\{A \wedge b\}c_0\{B\}\ ,\ \{A \wedge \neg b\}c_1\{B\}}{\{A\}\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1\{B\}}$$

Hoare Rules

Conditional Branch

$$\frac{\{A \wedge b\} c_0 \{B\} \ , \ \{A \wedge \neg b\} c_1 \{B\}}{\{A\} \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1 \{B\}}$$

- $\sigma \models^I (A \wedge b) \Rightarrow \mathcal{C}[\![c_0]\!](\sigma) \models^I B$
- $\sigma \models^I (A \wedge \neg b) \Rightarrow \mathcal{C}[\![c_1]\!](\sigma) \models^I B$

Hoare Rules

Conditional Branch

$$\frac{\{A \wedge b\} c_0 \{B\} \ , \ \{A \wedge \neg b\} c_1 \{B\}}{\{A\} \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1 \{B\}}$$

- $\sigma \models^I (A \wedge b) \Rightarrow \mathcal{C}[\![c_0]\!](\sigma) \models^I B$
- $\sigma \models^I (A \wedge \neg b) \Rightarrow \mathcal{C}[\![c_1]\!](\sigma) \models^I B$
- $\sigma \models^I A \Rightarrow \mathcal{C}[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!](\sigma) \models^I B$

Hoare Rules

Conditional Branch

$$\frac{\{A \wedge b\} c_0 \{B\} \ , \ \{A \wedge \neg b\} c_1 \{B\}}{\{A\} \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1 \{B\}}$$

- $\sigma \models^I (A \wedge b) \Rightarrow \mathcal{C}[\![c_0]\!](\sigma) \models^I B$
- $\sigma \models^I (A \wedge \neg b) \Rightarrow \mathcal{C}[\![c_1]\!](\sigma) \models^I B$
- $\sigma \models^I A \Rightarrow \mathcal{C}[\![\textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1]\!](\sigma) \models^I B$
- $\models \{A\} \textbf{if } b \textbf{ then } c_0 \textbf{ else } c_1 \{B\}$

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c;$
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models^I A$

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c$;
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models^I A$
- Case 1:

$$\frac{\langle b, \sigma \rangle \to \textbf{false}}{\langle w, \sigma \rangle \to \sigma}$$

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c$;
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models' A$
- Case 1:

$$\frac{\langle b, \sigma \rangle \to \textbf{false}}{\langle w, \sigma \rangle \to \sigma}$$

- $\sigma \models' \neg b$

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c$;
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models' A$
- Case 1:

$$\frac{\langle b, \sigma \rangle \to \textbf{false}}{\langle w, \sigma \rangle \to \sigma}$$

- $\sigma \models' \neg b$
- $\sigma \models' A \wedge \neg b$;

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c$;
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models' A$
- Case 2 (a nested induction on derivation trees):

$$\frac{\langle b, \sigma \rangle \to \textbf{true}, \langle c, \sigma \rangle \to \sigma'', \langle w, \sigma'' \rangle \to \sigma'}{\langle w, \sigma \rangle \to \sigma'}$$

- $\sigma'' \models' A$ from the main induction hypothesis

Hoare Rules

While Loop

$$\frac{\{A \wedge b\}c\{A\}}{\{A\}\textbf{while } b \textbf{ do } c\{A \wedge \neg b\}}$$

- $w = \textbf{while } b \textbf{ do } c$;
- $\langle w, \sigma \rangle \to \sigma'$, $\sigma \models' A$
- Case 2 (a nested induction on derivation trees):

$$\frac{\langle b, \sigma \rangle \to \textbf{true}, \langle c, \sigma \rangle \to \sigma'', \langle w, \sigma'' \rangle \to \sigma'}{\langle w, \sigma \rangle \to \sigma'}$$

- $\sigma'' \models' A$ from the main induction hypothesis
- $\sigma' \models' A \wedge \neg b$ from the nested induction hypothesis

Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

- $\langle c, \sigma \rangle \to \sigma'$, $\sigma \models' A$

Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

- $\langle c, \sigma \rangle \to \sigma'$, $\sigma \models^I A$
- $\sigma \models^I A'$ from $\models A \Rightarrow A'$

Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

- $\langle c, \sigma \rangle \to \sigma'$, $\sigma \models' A$
- $\sigma \models' A'$ from $\models A \Rightarrow A'$
- $\sigma' \models' B'$ from $\models \{A'\}c\{B'\}$

Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

- $\langle c, \sigma \rangle \to \sigma'$, $\sigma \models^I A$
- $\sigma \models^I A'$ from $\models A \Rightarrow A'$
- $\sigma' \models^I B'$ from $\models \{A'\}c\{B'\}$
- $\sigma' \models^I B$ from $\models B' \Rightarrow B$

Soundness of Hoare Rules

Soundness

$\vdash \{A\}c\{B\}$ implies $\models \{A\}c\{B\}$.

Hoare Rules: Examples

Textbook, Page 93 – 96

Hoare Rules: Examples

$$
\begin{array}{l}
S := 0\,; \\
N := 1\,; \\
\textbf{while}\ \ \neg(N = 101)\ \ \textbf{do} \\
\quad S := S + N\,; \\
\quad N := N + 1
\end{array}
$$

Hoare Rules: Examples

$\{\textbf{true}\}$ implies $\{0 = 0\}$
$S := 0;$
$\{S = 0\}$ implies $\{S = 0 \wedge 1 = 1\}$
$N := 1;$
$\{S = 0 \wedge N = 1\}$ implies $\{2 \times S = N \cdot (N - 1)\}$
while $\neg(N = 101)$ **do**
  $\{2 \times S = N \times (N - 1) \wedge \neg(N = 101)\}$ implies
  $\{2 \times (S + N) = N \times (N + 1) \wedge \neg(N = 101)\}$
  $S := S + N;$
  $\{2 \times S = (N + 1) \times N \wedge \neg(N = 101)\}$ implies
  $\{2 \times S = (N + 1) \times N\}$
  $N := N + 1$
  $\{2 \times S = N \times (N - 1)\}$
$\{2 \times S = N \times (N - 1) \wedge \neg(\neg N = 101)\}$ implies
$\{S = 5050\}$

Hoare Rules: Examples

$$
\begin{array}{l}
P := 0\,; \\
C := 1\,; \\
\textbf{while}\ \ C \leq N\ \ \textbf{do} \\
\quad P := P + M\,; \\
\quad C := C + 1
\end{array}
$$

Hoare Rules: Examples

$\{1 \leq N\}$
$P := 0;\ \{1 \leq N \wedge P = 0\}$
$C := 1;\ \{1 \leq N \wedge P = 0 \wedge C = 1\}$

$\{P = M \times (C - 1) \wedge C \leq N + 1\}$
while $C \leq N$ **do**
$\{P = M \times (C - 1) \wedge C \leq N + 1 \wedge C \leq N\}$
$P := P + M;\ \{P = M \times C \wedge C \leq N + 1 \wedge C \leq N\}$
$C := C + 1\ \{P = M \times (C - 1) \wedge C \leq N + 1\}$

$\{P = M \times (C - 1) \wedge C \leq N + 1 \wedge \neg(C \leq N)\}$
$\{P = M \times N\}$

Hoare Rules: Examples

$$\begin{array}{l}\textbf{while}\ \ \neg(Y = 0)\ \ \textbf{do}\\ \quad Y := Y - 1\,;\\ \quad X := 2 \times X\end{array}$$

Hoare Rules: Examples

$\{i \geq 0 \wedge Y = i \wedge X = 1\}$
$\{X \times 2^Y = 2^i \wedge Y \geq 0\}$

while $\neg(Y = 0)$ **do**
$\{X \times 2^Y = 2^i \wedge Y \geq 0 \wedge \neg(Y = 0)\}$
$Y := Y - 1;$ $\{Y \geq 0 \wedge 2 \times X \times 2^Y = 2^i\}$
$X := 2 \times X$ $\{X \cdot 2^Y = 2^i \wedge Y \geq 0\}$

$\{X \cdot 2^Y = 2^i \wedge Y \geq 0 \wedge Y = 0\}$
$\{X = 2^i\}$

Hoare Rules: Examples

$$\begin{array}{l}\textbf{while}\ \ \neg(X \leq 0)\ \ \textbf{do}\\ \quad Y := X \times Y\,;\\ \quad X := X - 1\end{array}$$

Hoare Rules: Examples

$\{X = n \wedge n \geq 0 \wedge Y = 1\}$
$\{Y \times X! = n! \wedge X \geq 0\}$

while $X > 0$ **do**
$\{Y \times X! = n! \wedge X \geq 0 \wedge X > 0\}$
$Y := X \times Y$;
$\{Y \times X! = n! \cdot X \wedge X \geq 0 \wedge X > 0\}$
$X := X - 1$
$\{Y \times X! = n! \wedge X \geq 0\}$

$\{Y \times X! = n! \wedge X \geq 0 \wedge \neg(X > 0)\}$
$\{Y = n!\}$

Hoare Rules: Examples

$$
\begin{array}{l}
\textbf{while}\ \ \neg(Y = 0)\ \ \textbf{do} \\
\quad (\,\textbf{while}\ \ \textbf{even}(Y)\ \ \textbf{do}\ \ X := X \times X\,;\ \ \ Y := Y/2\,)\,; \\
\quad Z := Z \times X\,; \\
\quad Y := Y - 1
\end{array}
$$

Hoare Rules: Examples

$\{X = m \wedge Y = n \wedge Z = 1 \wedge n \geq 0\}$
$\{Y \geq 0 \wedge m^n = Z \times X^Y\}$
while $\neg(Y = 0)$ **do**
$\{Y \geq 0 \wedge m^n = Z \times X^Y \wedge \neg(Y = 0)\}$
(**while** **even**(Y) **do**
$\{Y \geq 0 \wedge m^n = Z \times X^Y \wedge \neg(Y = 0) \wedge \textbf{even}(Y)\}$
$X := X \times X$; $\{Y \geq 0 \wedge m^n = Z \times X^{Y/2} \wedge \neg(Y = 0) \wedge \textbf{even}(Y)\}$
$Y := Y/2$ $\{Y \geq 0 \wedge m^n = Z \times X^Y \wedge \neg(Y = 0)\}$);
$\{Y \geq 0 \wedge m^n = Z \times X^Y \wedge \neg(Y = 0) \wedge \neg\textbf{even}(Y)\}$
$Z := Z \times X$; $\{Y \geq 0 \wedge m^n = Z \times X^{Y-1} \wedge \neg(Y = 0) \wedge \neg\textbf{even}(Y)\}$
$Y := Y - 1$ $\{Y \geq 0 \wedge m^n = Z \times X^Y\}$
$\{Y \geq 0 \wedge m^n = Z \times X^Y \wedge Y = 0\}$
$\{m^n = Z\}$

Hoare Rules: Examples

$$
\begin{array}{l}
\textbf{while } \neg(M = N) \textbf{ do} \\
\quad \textbf{if } M \leq N \textbf{ then} \\
\qquad N := N - M \\
\quad \textbf{else} \\
\qquad M := M - N
\end{array}
$$

Hoare Rules: Examples

$\{M = m \wedge N = n \wedge 1 \leq m \wedge 1 \leq n\}$
$\{\gcd(M, N) = \gcd(m, n)\}$

while $\neg(M = N)$ **do**
  $\{\gcd(M, N) = \gcd(m, n) \wedge \neg(M = N)\}$
  if $M \leq N$ **then**
    $\{\gcd(M, N) = \gcd(m, n) \wedge \neg(M = N) \wedge M \leq N\}$
    $N := N - M$ $\{\gcd(M, N) = \gcd(m, n)\}$
  else
    $\{\gcd(M, N) = \gcd(m, n) \wedge \neg(M = N) \wedge \neg(M \leq N)\}$
    $M := M - N$ $\{\gcd(M, N) = \gcd(m, n)\}$
  $\{\gcd(M, N) = \gcd(m, n)\}$

$\{\gcd(M, N) = \gcd(m, n) \wedge M = N\}$
$\{N = \gcd(m, n)\}$

Completeness of Hoare Rules

Completeness of Hoare Rules

Effective Proof Systems

A proof system is effective if there exists an algorithm such that

- upon an input rule instance, then the algorithm outputs "yes",
- otherwise the algorithm outputs "no" or does not terminate.

Completeness of Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

Completeness of Hoare Rules

Consequence

$$\frac{\models A \Rightarrow A' \ , \ \{A'\}c\{B'\} \ , \ \models B' \Rightarrow B}{\{A\}c\{B\}}$$

Problem

- How to check $\models A \Rightarrow A'$ and $\models B' \Rightarrow B$?

Completeness of Hoare Rules

Gödel's Incompleteness Theorem

There is no effective proof system for **Assn** such that the theorems coincide with valid assertions in **Assn**.

Completeness of Hoare Rules

Gödel's Incompleteness Theorem

There is no effective proof system for **Assn** such that the theorems coincide with valid assertions in **Assn**.

Corollary

There is no effective proof system for partial correctness assertions such that its theorems are precisely the valid partial correctness assertions.

Completeness of Hoare Rules

Gödel's Incompleteness Theorem

There is no effective proof system for **Assn** such that the theorems coincide with valid assertions in **Assn**.

Corollary

There is no effective proof system for partial correctness assertions such that its theorems are precisely the valid partial correctness assertions.

Proof

$\models B$ iff $\models \{\textbf{true}\}\textbf{skip}\{B\}$.

Completeness of Hoare Rules

Corollary

There is no effective proof system for partial correctness assertions such that its theorems are precisely the valid partial correctness assertions.

Proof (by contradiction)

- $\models \{\textbf{true}\}c\{\textbf{false}\}$ iff c diverges (does not terminate) on all states.
- The set $\{c \mid \forall \sigma \in \Sigma.\mathcal{C}[\![c]\!](\sigma) = \bot\}$ is not checkable (or recursively enumerable) (Textbook, Appendix A).

Completeness of Hoare Rules

Corollary

There is no effective proof system for partial correctness assertions such that its theorems are precisely the valid partial correctness assertions.

Proof (by contradiction)

- $\models \{\textbf{true}\}c\{\textbf{false}\}$ iff c diverges (does not terminate) on all states.
- The set $\{c \mid \forall \sigma \in \Sigma.\mathcal{C}[\![c]\!](\sigma) = \bot\}$ is not checkable (or recursively enumerable) (Textbook, Appendix A).

Corollary

The proof system of Hoare rules is not effective.

Completeness of Hoare Rules

Relative Completeness

The Hoare rules are relatively complete if $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$ for all parital correctness assertions $\{A\}c\{B\}$.

Completeness of Hoare Rules

Relative Completeness

The Hoare rules are relatively complete if $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$ for all parital correctness assertions $\{A\}c\{B\}$.

Theorem

The proof system of Hoare rules is relatively complete.

Completeness of Hoare Rules

Weakest Preconditions

- motivation: $\vdash \{A\} c_0; c_1 \{B\}$
- approach: an extended boolean assertion C such that $\vdash \{A\} c_0 \{C\}$ and $\vdash \{C\} c_1 \{B\}$

Completeness of Hoare Rules

Weakest Preconditions

- motivation: $\vdash \{A\} c_0; c_1 \{B\}$
- approach: an extended boolean assertion C such that $\vdash \{A\} c_0 \{C\}$ and $\vdash \{C\} c_1 \{B\}$

Question

Does such C really exist?

Completeness of Hoare Rules

Weakest Preconditions

- c: a command
- B: an extended boolean assertion
- I: an interpretation

Then we define the weakest precondition $wp^I[\![c, B]\!]$ by

$$wp^I[\![c, B]\!] := \{\sigma \in \Sigma_\perp \mid \mathcal{C}[\![c]\!](\sigma) \models^I B\}$$

Weakest Precondition

Weakest Preconditions

- $wp^I[\![c, B]\!] := \{\sigma \in \Sigma_\perp \mid \mathcal{C}[\![c]\!](\sigma) \models^I B\}$
- $\models^I \{A\}c\{B\}$ iff $A^I \subseteq wp^I[\![c, B]\!]$

Completeness of Hoare Rules

Weakest Precondition: Our Goal

For every c, B, there exists $A \in \mathbf{Assn}$ such that $A^I = wp^I[\![c, B]\!]$ for every interpretation I.

Completeness of Hoare Rules

Weakest Precondition: Our Goal

For every c, B, there exists $A \in \mathbf{Assn}$ such that $A^I = wp^I[\![c, B]\!]$ for every interpretation I.

Corollary

- $\sigma \models^I \{A'\}c\{B\}$ iff $\sigma \models^I A' \Rightarrow A$
- $\models \{A'\}c\{B\}$ iff $\models A' \Rightarrow A$

Summary

- soundness of Hoare rules
- examples for Hoare rules
- relative completeness
- weakest preconditions

Homeworks

Problem

Consider the command c to be

$$Z := X; X := Y; Y := Z \ .$$

with locations X, Y, Z. Prove through Hoare rules that the partial correctness assertion

$$\{X = i \wedge Y = j\} c \{X = j \wedge Y = i\}$$

is valid, where i, j are integer variables.

Homeworks

Problem

Let c be the command **while** $X \leq 100$ **do** $X := X + 2$ with location X. Prove through the Hoare rules that

$$\models \{X \leq 100 \wedge (\exists i.X = 2 \times i + 1)\} c \{X = 101\}$$

where i is an integer variable.