Axiomatic Semantics

Hongfei Fu

John Hopcroft Center for Computer Science
Shanghai Jiao Tong University

Apr. 22nd

Previous Lecture

- soundness of Hoare rules
- examples of Hoare rules
- non-effectiveness of Hoare rules
- weakest preconditions

Today's Topic

- relative completeness of Hoare rules
- a proof for Gödel's Incompleteness Theorem

Relative Completeness of Hoare Rules

Textbook, Page 100 – 110

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

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

Completeness of Hoare Rules

Definition: Expressiveness

The set **Assn** of extended boolean assertions is expressive if for every command c and extended boolean assertion B, there exists $A \in \mathbf{Assn}$ such that $A^I = wp^I[\![c, B]\!]$ for all interpretations I.

Completeness of Hoare Rules

Theorem

Assn is expressive.

Completeness of Hoare Rules

Theorem

Assn is expressive.

Proof

- by structural induction on commands c:

$$\forall B \in \mathbf{Assn}.\exists w[\![c, B]\!] \in \mathbf{Assn}.\forall I.(w[\![c, B]\!]^I = wp^I[\![c, B]\!])$$

Completeness of Hoare Rules

Proof: Skip

- $c =$ **skip**;

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip}$;
- $w[\![c, B]\!] := B$;

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip}$;
- $w[\![c, B]\!] := B$;
-

$$\begin{array}{lll} \sigma \in wp^I[\![\textbf{skip}, B]\!] & \text{iff} & \mathcal{C}[\![\textbf{skip}]\!](\sigma) \models^I B \\ & \text{iff} & \sigma \models^I B \\ & \text{iff} & \sigma \in w[\![c, B]\!]^I \end{array}$$

Completeness of Hoare Rules

Proof: Assignment

- $c = X := a;$

Completeness of Hoare Rules

Proof: Assignment

- $c = X := a$;
- $w[\![c, B]\!] := B[a/X]$;

Completeness of Hoare Rules

Proof: Assignment

- $c = X{:=}a;$
- $w[\![c, B]\!] := B\,[a/X];$
-

$$\begin{aligned}
\sigma \in wp^I[\![X{:=}a, B]\!] \quad \text{iff} \quad & \mathcal{C}[\![X{:=}a]\!](\sigma) \models^I B \\
\text{iff} \quad & \sigma\,[\mathcal{A}[\![a]\!](\sigma)/X] \models^I B \\
\text{iff} \quad & \sigma \models^I B\,[a/X] \\
\text{iff} \quad & \sigma \in w[\![c, B]\!]^I
\end{aligned}$$

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;
- $w[\![c, B]\!] := w[\![c_0, w[\![c_1, B]\!]]\!]$;

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;
- $w[\![c, B]\!] := w[\![c_0, w[\![c_1, B]\!]]\!]$;
-

$$
\begin{array}{lll}
\sigma \in wp^I[\![c_0; c_1, B]\!] & \text{iff} & \mathcal{C}[\![c_0; c_1]\!](\sigma) \models^I B \\
& \text{iff} & \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!](\sigma)) \models^I B \\
& \text{iff} & \mathcal{C}[\![c_0]\!](\sigma) \in wp^I[\![c_1, B]\!] \\
& \text{iff} & \mathcal{C}[\![c_0]\!](\sigma) \models^I w[\![c_1, B]\!] \\
& \text{iff} & \sigma \in wp^I[\![c_0, w[\![c_1, B]\!]]\!] \\
& \text{iff} & \sigma \in w[\![c_0, w[\![c_1, B]\!]]\!]^I \\
& \text{iff} & \sigma \in w[\![c, B]\!]^I
\end{array}
$$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;
- $w[\![c, B]\!] = (b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])$;

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;
- $w[\![c, B]\!] = (b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])$;
-

$$
\begin{array}{lll}
\sigma \in wp^I[\![c, B]\!] & \text{iff} & (\mathcal{B}[\![b]\!](\sigma) = \textbf{true} \ \& \ \mathcal{C}[\![c_0]\!](\sigma) \models^I B) \\
 & & \text{or } (\mathcal{B}[\![b]\!](\sigma) = \textbf{false} \ \& \ \mathcal{C}[\![c_1]\!](\sigma) \models^I B) \\
 & \text{iff} & (\sigma \models^I b \ \& \ \sigma \in wp^I[\![c_0, B]\!]) \\
 & & \text{or } (\sigma \models^I \neg b \ \& \ \sigma \in wp^I[\![c_1, B]\!])) \\
 & \text{iff} & (\sigma \models^I b \ \& \ \sigma \models^I w[\![c_0, B]\!]) \\
 & & \text{or } (\sigma \models^I \neg b \ \& \ \sigma \models^I w[\![c_1, B]\!])) \\
 & \text{iff} & \sigma \models^I (b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!]) \\
 & \text{iff} & \sigma \models^I w[\![c, B]\!] \\
 & \text{iff} & \sigma \in w[\![c, B]\!]^I
\end{array}
$$

Completeness of Hoare Rules

Proof: While Loop

- $c =$ **while** b **do** c' ;
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ iff it holds that

$$
\begin{array}{l}
\forall k \geq 0. \forall \sigma_0, \ldots, \sigma_k \in \Sigma. \big(\\
\quad \big[\sigma = \sigma_0 \ \& \\
\qquad \forall 0 \leq i < k. (\sigma_i \models^I b \ \& \\
\qquad\quad \mathcal{C}[\![c']\!](\sigma_i) = \sigma_{i+1}) \\
\quad \big] \\
\quad \Rightarrow \sigma_k \models^I b \vee (\neg b \wedge B) \\
\big)
\end{array}
$$

Completeness of Hoare Rules

Proof: While Loop

- difficulty: translation into an assertion in **Assn**

Completeness of Hoare Rules

Proof: While Loop

- difficulty: translation into an assertion in **Assn**
- solution: Chinese Remainder Theorem

Completeness of Hoare Rules

Chinese Remainder Theorem

- $m_1, \ldots, m_n$: positive relatively-prime natural numbers (i.e., $\gcd(m_i, m_j) = 1$ whenever $i \neq j$)

Then for any integers $a_1, \ldots, a_n$ there exists a natural number x such that $x \equiv a_i \pmod{m_i}$ for all $i = 1, \ldots, n$.

Completeness of Hoare Rules

Chinese Remainder Theorem

- $m_1, \ldots, m_n$: positive relatively-prime natural numbers (i.e., $\gcd(m_i, m_j) = 1$ whenever $i \neq j$)

Then for any integers $a_1, \ldots, a_n$ there exists a natural number x such that $x \equiv a_i \pmod{m_i}$ for all $i = 1, \ldots, n$.

Proof

For $i = 1, \ldots, n$, define $M_i := \prod_{j \neq i} m_j$. Then m_i and M_i are relatively prime. Thus we can find through the Euclidean Algorithm an integer b_i such that $b_i \cdot M_i \equiv 1 \pmod{m_i}$. Define

$$x := \left(\sum_{i=1}^{n} a_i \cdot b_i \cdot M_i \right) + \left(K \cdot \prod_{i=1}^{n} m_i \right) .$$

Then x satisfies the conditions in the statement of the theorem.

Completeness of Hoare Rules

The Gödel's Predicate

- $a \bmod b$: the remainder of a divided by b

The Gödel's predicate β over natural numbers is defined by:

$$\beta(a, b, i, x) := \ x = (a \bmod (1 + (1 + i) \cdot b)) \ .$$

Completeness of Hoare Rules

The Gödel's Predicate

- $a \bmod b$: the remainder of a divided by b

The Gödel's predicate β over natural numbers is defined by:

$$\beta(a, b, i, x) := \ x = (a \bmod (1 + (1 + i) \cdot b)) \ .$$

Exercise

- Give an assertion in **Assn** that expresses $x = (a \bmod b)$.
- Prove that β can be expressed in **Assn**.

Completeness of Hoare Rules

Lemma

For any sequence $n_0, \ldots, n_k$ of natural numbers there are natural numbers $n, m > 0$ such that

$$\forall 0 \leq j \leq k. \forall x. (\beta(n, m, j, x) \Leftrightarrow x = n_j)$$

Completeness of Hoare Rules

Lemma

For any sequence $n_0, \ldots, n_k$ of natural numbers there are natural numbers $n, m > 0$ such that

$$\forall 0 \leq j \leq k. \forall x. (\beta(n, m, j, x) \Leftrightarrow x = n_j)$$

Proof

Define $m := (\max\{k, n_0, \ldots, n_k\})!$ and $p_i := 1 + (1 + i) \cdot m$ for $i = 0, \ldots, k$.

Completeness of Hoare Rules

Lemma

For any sequence $n_0, \ldots, n_k$ of natural numbers there are natural numbers $n, m > 0$ such that

$$\forall 0 \leq j \leq k. \forall x. (\beta(n, m, j, x) \Leftrightarrow x = n_j)$$

Proof

Define $m := (\max\{k, n_0, \ldots, n_k\})!$ and $p_i := 1 + (1 + i) \cdot m$ for $i = 0, \ldots, k$.

- $p_0, \ldots, p_k$ are relative primes.
- $n_i < p_i$ for $i = 0, \ldots, k$.

Completeness of Hoare Rules

Lemma

For any sequence $n_0, \ldots, n_k$ of natural numbers there are natural numbers $n, m > 0$ such that

$$\forall 0 \leq j \leq k. \forall x. (\beta(n, m, j, x) \Leftrightarrow x = n_j)$$

Proof

Define $m := (\max\{k, n_0, \ldots, n_k\})!$ and $p_i := 1 + (1 + i) \cdot m$ for $i = 0, \ldots, k$.

- $p_0, \ldots, p_k$ are relative primes.
- $n_i < p_i$ for $i = 0, \ldots, k$.

By Chinese Remainder Theorem, there exists a natural number n such that $n \equiv n_i \pmod{p_i}$ for $i = 0, \ldots, k$. From $0 \leq n_i < p_i$, $(n \bmod p_i) = n_i$.

Completeness of Hoare Rules

The Predicate F

$$F(x, y) := x \geq 0 \ \& \ \exists z \geq 0.[(x = 2 \cdot z \Rightarrow y = z) \ \& \ (x = 2 \cdot z + 1 \Rightarrow y = -z - 1)]$$

Completeness of Hoare Rules

The Predicate F

$$F(x,y) := x \geq 0 \ \& \ \exists z \geq 0.[(x = 2 \cdot z \Rightarrow y = z) \ \& \ (x = 2 \cdot z + 1 \Rightarrow y = -z - 1)]$$

Properties:

- $(F(x,y)$ and x is even$) \Rightarrow y = \frac{x}{2}$;
- $(F(x,y)$ and x is odd$) \Rightarrow y = -\frac{x-1}{2} - 1$;

Completeness of Hoare Rules

The Predicate F

$$F(x,y) := x \geq 0 \ \& \ \exists z \geq 0.[(x = 2 \cdot z \Rightarrow y = z) \ \& \ (x = 2 \cdot z + 1 \Rightarrow y = -z - 1)]$$

Properties:

- ($F(x,y)$ and x is even) $\Rightarrow y = \frac{x}{2}$;
- ($F(x,y)$ and x is odd) $\Rightarrow y = -\frac{x-1}{2} - 1$;
- a bijection between natural numbers and integers

Completeness of Hoare Rules

The Predicate $\beta^{\pm}$

$$\beta^{\pm}(n, m, j, y) := \exists x. \, (\beta(n, m, j, x) \wedge F(x, y))$$

Completeness of Hoare Rules

The Predicate $\beta^{\pm}$

$$\beta^{\pm}(n, m, j, y) := \exists x.\, (\beta(n, m, j, x) \wedge F(x, y))$$

Lemma

For any sequence $n_0, \ldots, n_k$ of integers, there are natural numbers $n, m > 0$ such that for all $0 \leq j \leq k$ and all integers y we have

$$\beta^{\pm}(n, m, j, y) \Leftrightarrow y = n_j \ .$$

Gödel's Predicate

Lemma

For any sequence $n_0, \ldots, n_k$ of integers, there are natural numbers $n, m > 0$ such that for all $0 \leq j \leq k$ and all integers y we have

$$\beta^{\pm}(n, m, j, y) \Leftrightarrow y = n_j \ .$$

Proof

Construct the sequence $n'_0, \ldots, n'_k$ such that $F(n'_j, n_j)$ holds for all $0 \leq j \leq k$. From the previous lemma for β, there exist natural numbers $n, m > 0$ such that

$$\forall 0 \leq j \leq k. \forall x. \left(\beta(n, m, j, x) \Leftrightarrow x = n'_j\right)$$

Then the result follows from that $(F(x, y) \ \& \ x = n'_j) \Rightarrow y = n_j$.

Completeness of Hoare Rules

Proof: While Loop

- $c =$ **while** b **do** c' ;
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ iff it holds that

$$
\begin{array}{l}
\forall k \geq 0. \forall \sigma_0, \ldots, \sigma_k \in \Sigma. \big(\\
\quad \big[\sigma = \sigma_0 \ \& \\
\qquad \forall 0 \leq i < k. (\sigma_i \models^I b \ \& \\
\qquad\quad \mathcal{C}[\![c']\!](\sigma_i) = \sigma_{i+1}) \\
\quad \big] \\
\quad \Rightarrow \sigma_k \models^I b \vee (\neg b \wedge B) \\
\big)
\end{array}
$$

Completeness of Hoare Rules

Proof: While Loop

- ℓ locations (program variables): $\bar{X} := (X_1, \ldots, X_\ell)$
- encoding: each σ_i as an integer vector $\bar{s}_i = (s_{i,1}, \ldots, s_{i,\ell})$

Completeness of Hoare Rules

Proof: While Loop

- ℓ locations (program variables): $\bar{X} := (X_1, \ldots, X_\ell)$
- encoding: each σ_i as an integer vector $\bar{s}_i = (s_{i,1}, \ldots, s_{i,\ell})$

$\mathcal{C}[\![c]\!](\sigma) \models^I B$ iff it holds that

$$
\begin{aligned}
&\forall k \geq 0. \forall \bar{s}_0, \ldots, \bar{s}_k. (\\
&\quad [\sigma \models^I X = \bar{s}_0 \ \& \\
&\qquad \forall 0 \leq i < k. (\models^I b\left[\bar{s}_i/\bar{X}\right] \ \& \\
&\qquad\quad \models^I (w[\![c', \bar{X} = \bar{s}_{i+1}]\!] \wedge \neg w[\![c', \mathbf{false}]\!])\left[\bar{s}_i/\bar{X}\right]) \\
&\quad] \\
&\quad \Rightarrow \models^I (b \vee B)\left[\bar{s}_k/\bar{X}\right] \\
&)
\end{aligned}
$$

Completeness of Hoare Rules

Proof: While Loop

$\mathcal{C}[\![c]\!](\sigma) \models^I B$ iff $\sigma \models^I w[\![c, B]\!]$ where

$$w[\![c, B]\!] :=$$

$$\forall k \geq 0. \forall n_1, m_1, \ldots, n_\ell, m_\ell > 0. \Big(
\Big[\big(\textstyle\bigwedge_{j=1}^{\ell} \beta^{\pm}(n_j, m_j, 0, X_j)\big) \ \wedge
\forall 0 \leq i < k. \big(\forall \bar{y}. \big(\textstyle\bigwedge_{j=1}^{\ell} \beta^{\pm}(n_j, m_j, i, y_j) \Rightarrow b\left[\bar{y}/\bar{X}\right]\big) \ \wedge
\big(\forall \bar{y}, \bar{z}. [\textstyle\bigwedge_{j=1}^{\ell} (\beta^{\pm}(n_j, m_j, i, y_j) \wedge \beta^{\pm}(n_j, m_j, i+1, z_j)) \ \Rightarrow
(w[\![c', \bar{X} = \bar{z}]\!] \wedge \neg w[\![c', \mathbf{false}]\!])\left[\bar{y}/\bar{X}\right]]\big)\big)
\Big]
\Rightarrow \big(\forall \bar{y}. \big(\textstyle\bigwedge_{j=1}^{\ell} \beta^{\pm}(n_j, m_j, k, y_j)\big) \Rightarrow (b \vee B)\left[\bar{y}/\bar{X}\right]\big)
\Big)$$

Completeness of Hoare Rules

Theorem (Expressiveness)

For every command c and extended boolean assertion B, there exists $A \in \mathbf{Assn}$ such that $A^I = wp^I[\![c, B]\!]$ for all interpretations I.

Completeness of Hoare Rules

Lemma

For any command c and assertion $B \in \mathbf{Assn}$, if $w[\![c, B]\!]$ is any assertion satisfying that $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I, then $\vdash \{w[\![c, B]\!]\}c\{B\}$.

Completeness of Hoare Rules

Lemma

For any command c and assertion $B \in \mathbf{Assn}$, if $w[\![c, B]\!]$ is any assertion satisfying that $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I, then $\vdash \{w[\![c, B]\!]\}c\{B\}$.

Proof

By structural induction on c.

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip};$

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

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip}$;

$$\overline{\{A\}\textbf{skip}\{A\}}$$

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
- $\sigma \models^I w[\![c, B]\!]$ iff $\sigma \models^I B$;

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip}$;

$$\overline{\{A\}\textbf{skip}\{A\}}$$

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
- $\sigma \models^I w[\![c, B]\!]$ iff $\sigma \models^I B$;
- $\models w[\![c, B]\!] \Leftrightarrow B$;

Completeness of Hoare Rules

Proof: Skip

- $c = \textbf{skip}$;

$$\overline{\{A\}\textbf{skip}\{A\}}$$

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
- $\sigma \models^I w[\![c, B]\!]$ iff $\sigma \models^I B$;
- $\models w[\![c, B]\!] \Leftrightarrow B$;
- $\vdash \{w[\![c, B]\!]\}c\{B\}$;

Completeness of Hoare Rules

Proof: Assignment

- $c = X := a;$

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

Completeness of Hoare Rules

Proof: Assignment

- $c = X{:=}a;$

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;

Completeness of Hoare Rules

Proof: Assignment

- $c = X{:=}a;$

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
-

$$\begin{array}{lll} \sigma \in w[\![c, B]\!]^I & \text{iff} & \sigma \in wp^I[\![X{:=}a, B]\!] \\ & \text{iff} & \mathcal{C}[\![X{:=}a]\!](\sigma) \models^I B \\ & \text{iff} & \sigma\,[\mathcal{A}[\![a]\!](\sigma)/X] \models^I B \\ & \text{iff} & \sigma \models^I B\,[a/X] \end{array}$$

- $\models w[\![c, B]\!] \Leftrightarrow B\,[a/X]$ and hence $\vdash \{w[\![c, B]\!]\}c\{B\}$

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
-

$$\begin{aligned}
\sigma \in w[\![c, B]\!]^I \quad \text{iff} \quad & \sigma \in wp^I[\![c_0; c_1, B]\!] \\
\text{iff} \quad & \mathcal{C}[\![c_0; c_1]\!](\sigma) \models^I B \\
\text{iff} \quad & \mathcal{C}[\![c_1]\!](\mathcal{C}[\![c_0]\!](\sigma)) \models^I B \\
\text{iff} \quad & \mathcal{C}[\![c_0]\!](\sigma) \models^I w[\![c_1, B]\!] \\
\text{iff} \quad & \sigma \in w[\![c_0, w[\![c_1, B]\!]]\!]^I
\end{aligned}$$

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

- $\models w[\![c, B]\!] \Leftrightarrow w[\![c_0, w[\![c_1, B]\!]]\!]$
- $\vdash \{w[\![c_1, B]\!]\}c_1\{B\}$
- $\vdash \{w[\![c_0, w[\![c_1, B]\!]]\!]\}c_0\{w[\![c_1, B]\!]\}$

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

- $\models w[\![c, B]\!] \Leftrightarrow w[\![c_0, w[\![c_1, B]\!]]\!]$
- $\vdash \{w[\![c_1, B]\!]\}c_1\{B\}$
- $\vdash \{w[\![c_0, w[\![c_1, B]\!]]\!]\}c_0\{w[\![c_1, B]\!]\}$
- $\vdash \{w[\![c_0, w[\![c_1, B]\!]]\!]\}c\{B\}$

Completeness of Hoare Rules

Proof: Sequential Composition

- $c = c_0; c_1$;

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

- $\models w[\![c, B]\!] \Leftrightarrow w[\![c_0, w[\![c_1, B]\!]]\!]$
- $\vdash \{w[\![c_1, B]\!]\}c_1\{B\}$
- $\vdash \{w[\![c_0, w[\![c_1, B]\!]]\!]\}c_0\{w[\![c_1, B]\!]\}$
- $\vdash \{w[\![c_0, w[\![c_1, B]\!]]\!]\}c\{B\}$
- $\vdash \{w[\![c, B]\!]\}c\{B\}$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all I;
-

$$\begin{array}{lll} \sigma \models^I w[\![c, B]\!] & \text{iff} & \sigma \in wp^I[\![c, B]\!] \\ & \text{iff} & (\mathcal{B}[\![b]\!](\sigma) = \textbf{true} \ \& \ \mathcal{C}[\![c_0]\!](\sigma) \models^I B) \\ & & \text{or } (\mathcal{B}[\![b]\!](\sigma) = \textbf{false} \ \& \ \mathcal{C}[\![c_1]\!](\sigma) \models^I B) \\ & \text{iff} & (\sigma \models^I b \ \& \ \sigma \models^I w[\![c_0, B]\!]) \\ & & \text{or } (\sigma \models^I \neg b \ \& \ \sigma \models^I w[\![c_1, B]\!]) \\ & \text{iff} & \sigma \models^I (b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!]) \end{array}$$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $\models w[\![c, B]\!] \Leftrightarrow [(b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])]$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $\models w[\![c, B]\!] \Leftrightarrow [(b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])]$
- $\vdash \{w[\![c_0, B]\!]\} c_0 \{B\}$ and $\vdash \{w[\![c_1, B]\!]\} c_1 \{B\}$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $\models w[\![c, B]\!] \Leftrightarrow [(b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])]$
- $\vdash \{w[\![c_0, B]\!]\} c_0 \{B\}$ and $\vdash \{w[\![c_1, B]\!]\} c_1 \{B\}$
- $\models (w[\![c, B]\!] \wedge b) \Rightarrow w[\![c_0, B]\!]$
- $\models (w[\![c, B]\!] \wedge \neg b) \Rightarrow w[\![c_1, B]\!]$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $\models w[\![c, B]\!] \Leftrightarrow [(b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])]$
- $\vdash \{w[\![c_0, B]\!]\} c_0 \{B\}$ and $\vdash \{w[\![c_1, B]\!]\} c_1 \{B\}$
- $\models (w[\![c, B]\!] \wedge b) \Rightarrow w[\![c_0, B]\!]$
- $\models (w[\![c, B]\!] \wedge \neg b) \Rightarrow w[\![c_1, B]\!]$
- $\vdash \{w[\![c, B]\!] \wedge b\} c_0 \{B\}$ and $\vdash \{w[\![c, B]\!] \wedge \neg b\} c_1 \{B\}$

Completeness of Hoare Rules

Proof: Conditional Branch

- $c =$ **if** b **then** c_0 **else** c_1 ;

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

- $\models w[\![c, B]\!] \Leftrightarrow [(b \wedge w[\![c_0, B]\!]) \vee (\neg b \wedge w[\![c_1, B]\!])]$
- $\vdash \{w[\![c_0, B]\!]\} c_0 \{B\}$ and $\vdash \{w[\![c_1, B]\!]\} c_1 \{B\}$
- $\models (w[\![c, B]\!] \wedge b) \Rightarrow w[\![c_0, B]\!]$
- $\models (w[\![c, B]\!] \wedge \neg b) \Rightarrow w[\![c_1, B]\!]$
- $\vdash \{w[\![c, B]\!] \wedge b\} c_0 \{B\}$ and $\vdash \{w[\![c, B]\!] \wedge \neg b\} c_1 \{B\}$
- $\vdash \{w[\![c, B]\!]\} c \{B\}$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that

- $\models \{A \wedge b\} c' \{A\}$;
- $\models (A \wedge \neg b) \Rightarrow B$.

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that

- $\models \{A \wedge b\} c' \{A\}$;
- $\models (A \wedge \neg b) \Rightarrow B$.

Then we have

- $\vdash \{A \wedge b\} c' \{A\}$ from the induction hypothesis;
- $\vdash \{A\} c \{A \wedge \neg b\}$ from the while-loop rule;
- $\vdash \{A\} c \{B\}$ from the consequence rule;

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$.

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^{I} A \wedge b$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models' A \wedge b$
- $\sigma \models' w[\![c, B]\!]$ and $\sigma \models' b$
- $\mathcal{C}[\![c]\!](\sigma) \models' B$ and $\sigma \models' b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c'; c]\!](\sigma) \models^I B$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c'; c]\!](\sigma) \models^I B$
- $\mathcal{C}[\![c]\!](\mathcal{C}[\![c']\!](\sigma)) \models^I B$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c'; c]\!](\sigma) \models^I B$
- $\mathcal{C}[\![c]\!](\mathcal{C}[\![c']\!](\sigma)) \models^I B$
- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$;

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c'; c]\!](\sigma) \models^I B$
- $\mathcal{C}[\![c]\!](\mathcal{C}[\![c']\!](\sigma)) \models^I B$
- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$;
- $\mathcal{C}[\![c']\!](\sigma) \models^I w[\![c, B]\!] (= A)$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models \{A \wedge b\} c' \{A\}$. The reasoning is as follows.

- $\sigma \models^I A \wedge b$
- $\sigma \models^I w[\![c, B]\!]$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c'; c]\!](\sigma) \models^I B$
- $\mathcal{C}[\![c]\!](\mathcal{C}[\![c']\!](\sigma)) \models^I B$
- $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$;
- $\mathcal{C}[\![c']\!](\sigma) \models^I w[\![c, B]\!] (= A)$
- $\models \{A \wedge b\} c' \{A\}$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

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

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

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

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

- $\sigma \models^I A \wedge \neg b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I \neg b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

- $\sigma \models^I A \wedge \neg b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I \neg b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c]\!](\sigma) = \sigma$ and $\sigma \models^I B$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

- $\sigma \models^I A \wedge \neg b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I \neg b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c]\!](\sigma) = \sigma$ and $\sigma \models^I B$
- $\sigma \models^I (A \wedge \neg b) \Rightarrow B$

Completeness of Hoare Rules

Proof: While Loop

- $c = \textbf{while}\ b\ \textbf{do}\ c'$;
- $A := w[\![c, B]\!]$;

We show that $\models (A \wedge \neg b) \Rightarrow B$. The reasoning is as follows.

- $\sigma \models^I A \wedge \neg b$
- $\mathcal{C}[\![c]\!](\sigma) \models^I B$ and $\sigma \models^I \neg b$
- $\mathcal{C}[\![c]\!] = \mathcal{C}[\![\textbf{if}\ b\ \textbf{then}\ c'; c\ \textbf{else skip}]\!]$
- $\mathcal{C}[\![c]\!](\sigma) = \sigma$ and $\sigma \models^I B$
- $\sigma \models^I (A \wedge \neg b) \Rightarrow B$
- $\models (A \wedge \neg b) \Rightarrow B$

Completeness of Hoare Rules

Theorem (Relative Completeness)

For any partial correctness assertion $\{A\}c\{B\}$, $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$.

Completeness of Hoare Rules

Theorem (Relative Completeness)

For any partial correctness assertion $\{A\}c\{B\}$, $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$.

Proof

- Suppose that $\models \{A\}c\{B\}$.

Completeness of Hoare Rules

Theorem (Relative Completeness)

For any partial correctness assertion $\{A\}c\{B\}$, $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$.

Proof

- Suppose that $\models \{A\}c\{B\}$.
- We have $\vdash \{w[\![c, B]\!]\}c\{B\}$ where $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all interpretations I.

Completeness of Hoare Rules

Theorem (Relative Completeness)

For any partial correctness assertion $\{A\}c\{B\}$, $\models \{A\}c\{B\}$ implies $\vdash \{A\}c\{B\}$.

Proof

- Suppose that $\models \{A\}c\{B\}$.
- We have $\vdash \{w[\![c, B]\!]\}c\{B\}$ where $w[\![c, B]\!]^I = wp^I[\![c, B]\!]$ for all interpretations I.
- By the consequence rule and $\models A \Rightarrow w[\![c, B]\!]$, we obtain $\vdash \{A\}c\{B\}$.

Proving Gödel's Incompleteness Theorem

Textbook, Page 110 – 112

Gödel's Incompleteness Theorem

Theorem

The set $\{A \in \mathbf{Assn} \mid\!\models A\}$ is not recursively enumerable.

Gödel's Incompleteness Theorem

Theorem

The set $\{A \in \mathbf{Assn} \mid\!\models A\}$ is not recursively enumerable.

Proof (by Contradiction)

- Suppose that $\{A \in \mathbf{Assn} \mid\!\models A\}$ is recursively enumerable.

Gödel's Incompleteness Theorem

Theorem

The set $\{A \in \mathbf{Assn} \mid\!\models A\}$ is not recursively enumerable.

Proof (by Contradiction)

- Suppose that $\{A \in \mathbf{Assn} \mid\!\models A\}$ is recursively enumerable.
- For each command c, construct the assertion

$$A := w[\![c, \mathbf{false}]\!] \left[\vec{0}/\bar{X}\right] \quad .$$

Gödel's Incompleteness Theorem

Theorem

The set $\{A \in \mathbf{Assn} \mid\!\models A\}$ is not recursively enumerable.

Proof (by Contradiction)

- Suppose that $\{A \in \mathbf{Assn} \mid\!\models A\}$ is recursively enumerable.
- For each command c, construct the assertion

$$A := w[\![c, \mathbf{false}]\!] \left[\vec{0}/\bar{X}\right] \quad .$$

- c does not terminate on the input $\vec{0}$ iff $\models A$.

Gödel's Incompleteness Theorem

Theorem

The set $\{A \in \mathbf{Assn} \mid\!\models A\}$ is not recursively enumerable.

Proof (by Contradiction)

- Suppose that $\{A \in \mathbf{Assn} \mid\!\models A\}$ is recursively enumerable.
- For each command c, construct the assertion

$$A := w[\![c, \mathbf{false}]\!] \left[\vec{0}/\bar{X}\right] \quad .$$

- c does not terminate on the input $\vec{0}$ iff $\models A$.
- However, the set of all those c's is known to be not recursively enumerable (Textbook, Appendix A).

Gödel's Incompleteness Theorem

Gödel's Incompleteness Theorem

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

Gödel's Incompleteness Theorem

Gödel's Incompleteness Theorem

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

Proof (by Contradiction)

- Suppose that there is an effective proof system for **Assn**.

Gödel's Incompleteness Theorem

Gödel's Incompleteness Theorem

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

Proof (by Contradiction)

- Suppose that there is an effective proof system for **Assn**.
- By enumerating the set of all proofs (derivation trees), the set

$$\{A \in \textbf{Assn} \mid\mid\!\!= A\}$$

would become recursively enumerable. Contradiction.

Summary

- relative completeness of Hoare rules
- a proof for Gödel's Incompleteness Theorem
- finishing all of the operational, denotational and axiomatic semantics for imperative programs

Homework A

Problem

Let c be the command **while** $X \leq 100$ **do** $X := (2 \times X) + 1$ with location X. Calculate the weakest precondition $wp^I[\![c, B]\!]$ where the postcondition $B = X \geq 150$ and the interpretation I is dummy (i.e., of no use) here.

Homework B

Problem

Let c be the following command:

$$\begin{array}{l}\textbf{while}\ \ N \leq M\ \ \textbf{do}\\ \quad [L := 1;\\ \quad\ \ \textbf{while}\ \ 2 \times L \times N \leq M\ \ \textbf{do}\ \ L := 2 \times L;\\ \quad\ \ K := K + L;\\ \quad\ \ M := M - (L \times N)]\end{array}$$

Prove through the Hoare rules that $\models \{A\}c\{B\}$ where

- the precondition A is $M = m \wedge M \geq 0 \wedge N \geq 1 \wedge K = 0$, and
- the postcondition B is $m = (K \times N) + M \wedge 0 \leq M \wedge M < N$, and
- m is an integer variable.