COMP2111 Week 6
Term 1, 2019
Hoare Logic III

Soundness of Hoare Logic

Hoare Logic is **sound** with respect to the semantics given. That is,

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (a):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (a):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (a):

$$\begin{aligned} y \in R(A) &\Leftrightarrow \exists x \in A \text{ such that } (x, y) \in R \\ &\Rightarrow \exists x \in B \text{ such that } (x, y) \in R \\ &\Leftrightarrow y \in R(B) \end{aligned}$$

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (b):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (b):

$$
\begin{aligned}
y \in R(A) \cup S(A) &\Leftrightarrow y \in R(A) \text{ or } y \in S(A) \\
&\Leftrightarrow \exists x \in A \text{ s.t. } (x, y) \in R \text{ or } \exists x \in A \text{ s.t. } (x, y) \in S \\
&\Leftrightarrow \exists x \in A \text{ s.t. } (x, y) \in R \text{ or } (x, y) \in S \\
&\Leftrightarrow \exists x \in A \text{ s.t. } (x, y) \in (R \cup S) \\
&\Leftrightarrow y \in (R \cup S)(A)
\end{aligned}
$$

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (c):

Some results on relational images

Lemma

For any binary relations $R, S \subseteq X \times Y$ and subsets $A, B \subseteq X$:

(a) *If $A \subseteq B$ then $R(A) \subseteq R(B)$*

(b) $R(A) \cup S(A) = (R \cup S)(A)$

(c) $R(S(A)) = (S; R)(A)$

Proof (c):

$$
\begin{aligned}
z \in R(S(A)) &\Leftrightarrow \exists y \in S(A) \text{ s.t. } (y, z) \in R \\
&\Leftrightarrow \exists x \in A,\ y \in S(A) \text{ s.t. } (x, y) \in S \text{ and } (y, z) \in R \\
&\Leftrightarrow \exists x \in A \text{ s.t. } (x, z) \in (S; R) \\
&\Leftrightarrow z \in (S; R)(A)
\end{aligned}
$$

Some results on relational images

Corollary

If $R(A) \subseteq A$ *then* $R^*(A) \subseteq A$

Proof:

$$
\begin{aligned}
R(A) \subseteq A &\Rightarrow R^{i+1}(A) = R^i(R(A)) \subseteq R^i(A) \\
&\Rightarrow R^{i+1}(A) \subseteq R(A) \subseteq A \\
\text{So } R^*(A) &= \left(\bigcup_{i=0}^{\infty} R^i\right)(A) \\
&= \bigcup_{i=0}^{\infty} R^i(A) \\
&\subseteq A
\end{aligned}
$$

Some results on relational images

Corollary

If $R(A) \subseteq A$ then $R^*(A) \subseteq A$

Proof:

$$
\begin{aligned}
R(A) \subseteq A \quad &\Rightarrow \quad R^{i+1}(A) = R^i(R(A)) \subseteq R^i(A) \\
&\Rightarrow \quad R^{i+1}(A) \subseteq R(A) \subseteq A \\
\text{So } R^*(A) \quad &= \quad \left(\bigcup_{i=0}^{\infty} R^i \right)(A) \\
&= \quad \bigcup_{i=0}^{\infty} R^i(A) \\
&\subseteq \quad A
\end{aligned}
$$

Some results on relational images

Corollary

If $R(A) \subseteq A$ then $R^*(A) \subseteq A$

Proof:

$$
\begin{aligned}
R(A) \subseteq A \quad &\Rightarrow \quad R^{i+1}(A) = R^i(R(A)) \subseteq R^i(A) \\
&\Rightarrow \quad R^{i+1}(A) \subseteq R(A) \subseteq A \\
\text{So } R^*(A) \quad &= \quad \left(\bigcup_{i=0}^{\infty} R^i \right)(A) \\
&= \quad \bigcup_{i=0}^{\infty} R^i(A) \\
&\subseteq \quad A
\end{aligned}
$$

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Proof:

By induction on the structure of the proof.

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Proof:

By induction on the structure of the proof.

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Proof:

By induction on the structure of the proof.

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Base case: Assignment rule

$$\frac{}{\{\varphi[e/x]\}\, x := e\, \{\varphi\}} \quad \text{(ass)}$$

Need to show $\{\varphi[e/x]\}\, x := e\, \{\varphi\}$ is always valid. That is,

$$[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle.$$

Observation: $[\![\varphi[e/x]]\!]^{\eta} = [\![\varphi]\!]^{\eta'}$ where $\eta' = \eta[x \mapsto [\![e]\!]^{\eta}]$

So if $\eta \in \langle\varphi[e/x]\rangle$ then $\eta' \in \langle\varphi\rangle$

Recall: $(\eta, \eta'') \in [\![x := e]\!]$ if and only if $\eta'' = \eta[x \mapsto [\![e]\!]^{\eta}]$,

So $[\![x := e]\!](\eta) \in \langle\varphi\rangle$ for all $\eta \in \langle\varphi[e/x]\rangle$

So $[\![x := e]\!](\langle\varphi[e/x]\rangle) \subseteq \langle\varphi\rangle$

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big)$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big) \subseteq [\![Q]\!]\big(\langle\psi\rangle\big) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]([\![P]\!](\langle\varphi\rangle))$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]([\![P]\!](\langle\varphi\rangle)) \subseteq [\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]([\![P]\!](\langle\varphi\rangle))$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]([\![P]\!](\langle\varphi\rangle)) \subseteq [\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]([\![P]\!](\langle\varphi\rangle))$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]([\![P]\!](\langle\varphi\rangle)) \subseteq [\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]([\![P]\!](\langle\varphi\rangle))$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]([\![P]\!](\langle\varphi\rangle)) \subseteq [\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Inductive case 1: Sequence rule

$$\frac{\{\varphi\}\, P\, \{\psi\} \qquad \{\psi\}\, Q\, \{\rho\}}{\{\varphi\}\, P; Q\, \{\rho\}} \quad \text{(seq)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ and $\{\psi\}\, Q\, \{\rho\}$ are valid. Need to show that $\{\varphi\}\, P; Q\, \{\rho\}$ is valid.

Recall: $[\![P; Q]\!] = [\![P]\!]; [\![Q]\!]$

So: $[\![P; Q]\!](\langle\varphi\rangle) = [\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big)$ (see Lemma 1(c))

By IH: $[\![P]\!](\langle\varphi\rangle) \subseteq \langle\psi\rangle$ and $[\![Q]\!](\langle\psi\rangle) \subseteq \langle\rho\rangle$

So: $[\![Q]\!]\big([\![P]\!](\langle\varphi\rangle)\big) \subseteq [\![Q]\!]\big(\langle\psi\rangle\big) \subseteq \langle\rho\rangle$ (see Lemma 1(a))

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, predicates φ and ψ, and $X \subseteq \textsc{Env}$:

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle))$

Proof (a):

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, predicates φ and ψ, and $X \subseteq \textsc{Env}$:

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle))$

Proof (a):

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, predicates φ and ψ, and $X \subseteq \textsc{Env}$:

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle))$

Proof (a):

$$\begin{aligned} \eta' \in [\![\varphi]\!](X) &\Leftrightarrow \exists \eta \in X \text{ s.t. } (\eta, \eta') \in [\![\varphi]\!] \\ &\Leftrightarrow \exists \eta \in X \text{ s.t. } \eta = \eta' \text{ and } \eta \in \langle\varphi\rangle \\ &\Leftrightarrow \eta' \in X \cap \langle\varphi\rangle \end{aligned}$$

Two more useful results

Lemma

For $R \subseteq \textsc{Env} \times \textsc{Env}$, predicates φ and ψ, and $X \subseteq \textsc{Env}$:

(a) $[\![\varphi]\!](X) = \langle\varphi\rangle \cap X$

(b) $R(\langle\varphi \wedge \psi\rangle) = ([\![\varphi]\!]; R)(\langle\psi\rangle))$

Proof (b):

$$\langle\varphi \wedge \psi\rangle = \langle\varphi\rangle \cap \langle\psi\rangle = [\![\varphi]\!](\langle\psi\rangle)$$

$$\begin{aligned} \text{So } R(\langle\varphi \wedge \psi\rangle) &= R\big([\![\varphi]\!](\langle\psi\rangle)\big) \\ &= ([\![\varphi]\!]; R)(\langle\psi\rangle) \qquad \text{(see Lemma 1(b))} \end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}}\ \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&= [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}}\ \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&= [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}}\ \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&= [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&= [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&= [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&\quad = [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&\quad = [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\quad \subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&\quad = [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&\quad = [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\quad \subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 2: Conditional rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\psi\} \qquad \{\varphi \wedge \neg g\}\, Q\, \{\psi\}}{\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}} \quad \text{(if)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\psi\}$ and $\{\varphi \wedge \neg g\}\, Q\, \{\psi\}$ are valid. Need to show that $\{\varphi\}\ \textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}\ \{\psi\}$ is valid.

Recall: $[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!] = [\![g; P]\!] \cup [\![\neg g; Q]\!]$

$$\begin{aligned}
&[\![\textbf{if}\ g\ \textbf{then}\ P\ \textbf{else}\ Q\ \textbf{fi}]\!](\langle\varphi\rangle) \\
&\quad = [\![g; P]\!](\langle\varphi\rangle) \cup [\![\neg g; Q]\!](\langle\varphi\rangle) && \text{(see Lemma 1(b))} \\
&\quad = [\![P]\!](\langle g \wedge \varphi\rangle) \cup [\![Q]\!](\langle \neg g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\
&\quad \subseteq \langle\psi\rangle && \text{(by IH)}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle)) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle)) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$[\![g; P]\!](\langle\varphi\rangle) = [\![P]\!](\langle g \wedge \varphi\rangle) \quad \text{(see Lemma 2(b))}$$

$$\subseteq \langle\varphi\rangle \quad \text{(IH)}$$

$$\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) \subseteq \langle\varphi\rangle \quad \text{(see Corollary)}$$

$$\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) = [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle)) \quad \text{(see Lemma 1(c))}$$

$$\subseteq [\![\neg g]\!](\langle\varphi\rangle) \quad \text{(see Lemma 1(a))}$$

$$= \langle\neg g \wedge \varphi\rangle \quad \text{(see Lemma 2(a))}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$[\![g; P]\!](\langle\varphi\rangle) = [\![P]\!](\langle g \wedge \varphi\rangle) \quad \text{(see Lemma 2(b))}$$

$$\subseteq \langle\varphi\rangle \quad \text{(IH)}$$

$$\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) \subseteq \langle\varphi\rangle \quad \text{(see Corollary)}$$

$$\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) = [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle)) \quad \text{(see Lemma 1(c))}$$

$$\subseteq [\![\neg g]\!](\langle\varphi\rangle) \quad \text{(see Lemma 1(a))}$$

$$= \langle\neg g \wedge \varphi\rangle \quad \text{(see Lemma 2(a))}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned} [\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))} \\ &\subseteq \langle\varphi\rangle && \text{(IH)} \end{aligned}$$

So $[\![g; P]\!]^*(\langle\varphi\rangle) \subseteq \langle\varphi\rangle$ (see Corollary)

So $[\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) = [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle))$ (see Lemma 1(c))

$\subseteq [\![\neg g]\!](\langle\varphi\rangle)$ (see Lemma 1(a))

$= \langle\neg g \wedge \varphi\rangle$ (see Lemma 2(a))

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]([\![g; P]\!]^*(\langle\varphi\rangle)) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\ \textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}\ \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while}\ g\ \textbf{do}\ P\ \textbf{od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 3: While rule

$$\frac{\{\varphi \wedge g\}\, P\, \{\varphi\}}{\{\varphi\}\, \textbf{while } g \textbf{ do } P \textbf{ od}\, \{\varphi \wedge \neg g\}} \quad \text{(loop)}$$

Assume $\{\varphi \wedge g\}\, P\, \{\varphi\}$ is valid. Need to show that $\{\varphi\}\, \textbf{while } g \textbf{ do } P \textbf{ od}\, \{\varphi \wedge \neg g\}$ is valid.

Recall: $[\![\textbf{while } g \textbf{ do } P \textbf{ od}]\!] = [\![g; P]\!]^*; [\![\neg g]\!]$

$$\begin{aligned}
[\![g; P]\!](\langle\varphi\rangle) &= [\![P]\!](\langle g \wedge \varphi\rangle) && \text{(see Lemma 2(b))}\\
&\subseteq \langle\varphi\rangle && \text{(IH)}\\
\text{So } [\![g; P]\!]^*(\langle\varphi\rangle) &\subseteq \langle\varphi\rangle && \text{(see Corollary)}\\
\text{So } [\![g; P]\!]^*; [\![\neg g]\!](\langle\varphi\rangle) &= [\![\neg g]\!]\big([\![g; P]\!]^*(\langle\varphi\rangle)\big) && \text{(see Lemma 1(c))}\\
&\subseteq [\![\neg g]\!](\langle\varphi\rangle) && \text{(see Lemma 1(a))}\\
&= \langle\neg g \wedge \varphi\rangle && \text{(see Lemma 2(a))}
\end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$

Inductive case 4: Consequence rule

$$\frac{\varphi' \to \varphi \qquad \{\varphi\}\, P\, \{\psi\} \qquad \psi \to \psi'}{\{\varphi'\}\, P\, \{\psi'\}} \quad \text{(cons)}$$

Assume $\{\varphi\}\, P\, \{\psi\}$ is valid and $\varphi' \to \varphi$ and $\psi \to \psi'$. Need to show that $\{\varphi'\}\, P\, \{\psi'\}$ is valid.

Observe: If $\varphi' \to \varphi$ then $\langle \varphi' \rangle \subseteq \langle \varphi \rangle$

$$\begin{aligned} [\![P]\!](\langle \varphi' \rangle) &\subseteq [\![P]\!](\langle \varphi \rangle) && \text{(see Lemma 1(a))} \\ &\subseteq \langle \psi \rangle && \text{(IH)} \\ &\subseteq \langle \psi' \rangle \end{aligned}$$

Soundness of Hoare Logic

Theorem

If $\vdash \{\varphi\}\, P\, \{\psi\}$ *then* $\models \{\varphi\}\, P\, \{\psi\}$

Summary

- Set theory revisited
- Soundness of Hoare Logic
- Completeness of Hoare Logic

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

$\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.

$\Rightarrow$ Hoare Logic is not complete.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

$\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.

$\Rightarrow$ Hoare Logic is not complete.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

$\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.

$\Rightarrow$ Hoare Logic is not complete.

Incompleteness

Theorem (Gödel's Incompleteness Theorem)

There is no proof system that can prove every valid first-order sentence about arithmetic over the natural numbers.

$\Rightarrow$ There are true statements that do not have a proof.

$\Rightarrow$ Because of (cons) there are valid triples that result from valid, but unprovable, consequences.

$\Rightarrow$ Hoare Logic is not complete.

Relative completeness of Hoare Logic

Theorem (Relative completeness of Hoare Logic)

With an oracle that decides the validity of predicates,

$$\textit{if } \models \{\varphi\}\, P\, \{\psi\} \textit{ then } \vdash \{\varphi\}\, P\, \{\psi\}\,.$$