CS477 Formal Software Development Methods

Elsa L Gunter
2112 SC, UIUC
egunter@illinois.edu
http://courses.engr.illinois.edu/cs477

Slides based in part on previous lectures by Mahesh Vishwanathan, and by Gul Agha

February 26, 2014

α-equivalence

- $\psi \overset{\alpha}{\equiv} \psi$
- If $\psi_1 \overset{\alpha}{\equiv} \psi_2$ then $\psi_2 \overset{\alpha}{\equiv} \psi$.
- It $\psi_1 \overset{\alpha}{\equiv} \psi_2$ and $\psi_2 \overset{\alpha}{\equiv} \psi_3$ then $\psi_1 \overset{\alpha}{\equiv} \psi_3$
- If $x \notin fv(\psi)$ and $y \notin fv(\psi)$ then $\psi \overset{\alpha}{\equiv} \psi[x \leftrightarrow y]$.
- If $\psi_i \overset{\alpha}{\equiv} \psi'_i$ for $i = 1, 2$ then
  - $(\psi_1) \overset{\alpha}{\equiv} (\psi'_1) \qquad \neg\psi_1 \overset{\alpha}{\equiv} \neg\psi'_1$
  - $\psi_1 \otimes \psi_2 \overset{\alpha}{\equiv} \psi'_1 \otimes \psi'_2$ for $\otimes \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$
  - $\mathcal{Q}\, z.\, \psi_1 \overset{\alpha}{\equiv} \mathcal{Q}\, z.\, \psi'_1$ for $\mathcal{Q} \in \{\forall, \exists\}$

α-equivalence: Example

$$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))$$
$$\stackrel{\alpha}{\equiv} (x > 3 \wedge (\exists w.\ (\forall z.\ z \geq (w - x)) \vee (z \geq w)))$$

$$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))$$
$$\stackrel{\alpha}{\equiv} (x > 3 \wedge (\exists w.\ (\forall y.\ y \geq (w - x)) \vee (z \geq w)))$$

Proof Rules

Will give Sequent version of Natural Deduction rules
All rules from Propositional Logic included

$$\frac{\Gamma \vdash \psi'[t/x]}{\Gamma \vdash \exists x.\psi}\text{ Ex I}$$

provided $\psi \overset{\alpha}{\equiv} \psi'$

$$\frac{\Gamma \vdash \exists x.\psi \quad \Gamma \cup \{(\psi[y/x])\} \vdash \varphi}{\Gamma \vdash \varphi}\text{ Ex E}$$

provided
$y \notin fv(\varphi) \cup (fv(\psi) \setminus \{x\}) \cup \bigcup_{\psi' \in \Gamma} fv(\psi')$

$$\frac{\Gamma \vdash \psi[y/x]}{\Gamma \vdash \forall x.\psi}\text{ All I}$$

provided
$y \notin (fv(\psi) \setminus \{x\}) \cup \bigcup_{\psi' \in \Gamma} fv(\psi')$

$$\frac{\Gamma \vdash \forall x.\psi \quad \Gamma \cup \{\psi'[t/x]\} \vdash \varphi}{\Gamma \vdash \varphi}\text{ All E}$$

provided $\psi \overset{\alpha}{\equiv} \psi'$

Example

Show

$$\frac{}{\{\ \} \vdash (\exists x.\, \forall y.\, x \leq y) \Rightarrow (\forall x.\, \exists y.\, y \leq x)}$$

Example

Show

$$\cfrac{\overline{\{(\exists x.\, \forall y.\, x \leq y)\} \vdash \forall x.\, \exists y.\, y \leq x}}{\{\ \} \vdash (\exists x.\, \forall y.\, x \leq y) \Rightarrow (\forall x.\, \exists y.\, y \leq x)}\ \text{Imp I}$$

Example

Show

$$\dfrac{\dfrac{\overline{\{(\exists x.\,\forall y.\,x \leq y)\} \vdash \exists y.\,y \leq x}}{\{(\exists x.\,\forall y.\,x \leq y)\} \vdash \forall x.\,\exists y.\,y \leq x}\text{ All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \leq y) \Rightarrow (\forall x.\,\exists y.\,y \leq x)}\text{ Imp I}$$

Example

Show

$$
\dfrac{\dfrac{\dfrac{\overline{\{\exists x.\,\forall y.\,x \le y\} \vdash \exists x.\,\forall y.\,x \le y} \qquad \left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \exists y.\,y \le x}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \exists y.\,y \le x}\ \text{Ex E}}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \forall x.\,\exists y.\,y \le x}\ \text{All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \le y) \Rightarrow (\forall x.\,\exists y.\,y \le x)}\ \text{Imp I}
$$

Example

Show

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\exists x.\,\forall y.\,x \leq y\} \vdash \exists x.\,\forall y.\,x \leq y}\,\text{Hyp} \quad \left\{\begin{array}{c}\exists x.\,\forall y.\,x \leq y;\\ \forall y.\,z \leq y\end{array}\right\} \vdash \exists y.\,y \leq x}{\{(\exists x.\,\forall y.\,x \leq y)\} \vdash \exists y.\,y \leq x}\,\text{Ex E}}{\{(\exists x.\,\forall y.\,x \leq y)\} \vdash \forall x.\,\exists y.\,y \leq x}\,\text{All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \leq y) \Rightarrow (\forall x.\,\exists y.\,y \leq x)}\,\text{Imp I}$$

Example

Show

$$\dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \forall y.\,z \le y} \qquad \dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y;\ z \le x\end{array}\right\} \vdash \exists y.\,y \le x}}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \exists y.\,y \le x}\ \text{All E}$$

$$\dfrac{\dfrac{}{\{\exists x.\,\forall y.\,x \le y\} \vdash \exists x.\,\forall y.\,x \le y}\ \text{Hyp} \qquad \left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \exists y.\,y \le x}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \exists y.\,y \le x}\ \text{Ex E}$$

$$\dfrac{\dfrac{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \exists y.\,y \le x}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \forall x.\,\exists y.\,y \le x}\ \text{All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \le y) \Rightarrow (\forall x.\,\exists y.\,y \le x)}\ \text{Imp I}$$

Example

Show

$$\dfrac{\dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \forall y.\,z \le y}\,\text{Hyp} \quad \dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y;\ z \le x\end{array}\right\} \vdash \exists y.\,y \le x}}{\dfrac{}{\{\exists x.\,\forall y.\,x \le y\} \vdash \exists x.\,\forall y.\,x \le y}\,\text{Hyp} \quad \left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \exists y.\,y \le x}\,\text{All E}}{\dfrac{\dfrac{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \exists y.\,y \le x}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \forall x.\,\exists y.\,y \le x}\,\text{All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \le y) \Rightarrow (\forall x.\,\exists y.\,y \le x)}\,\text{Imp I}}\,\text{Ex E}$$

Example

Show

$$\dfrac{\dfrac{}{\{\exists x.\, \forall y.\, x \leq y\} \vdash \exists x.\, \forall y.\, x \leq y}\,\text{Hyp} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\, \forall y.\, x \leq y; \\ \forall y.\, z \leq y\end{array}\right\} \vdash \forall y.\, z \leq y}\,\text{Hyp} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\, \forall y.\, x \leq y; \\ \forall y.\, z \leq y;\ z \leq x\end{array}\right\} \vdash z \leq x}}{\left\{\begin{array}{c}\exists x.\, \forall y.\, x \leq y; \\ \forall y.\, z \leq y;\ z \leq x\end{array}\right\} \vdash \exists y.\, y \leq x}\,\text{Ex I}}{\left\{\begin{array}{c}\exists x.\, \forall y.\, x \leq y; \\ \forall y.\, z \leq y\end{array}\right\} \vdash \exists y.\, y \leq x}\,\text{All E}}{\{(\exists x.\, \forall y.\, x \leq y)\} \vdash \exists y.\, y \leq x}\,\text{Ex E}$$

$$\dfrac{\dfrac{\{(\exists x.\, \forall y.\, x \leq y)\} \vdash \exists y.\, y \leq x}{\{(\exists x.\, \forall y.\, x \leq y)\} \vdash \forall x.\, \exists y.\, y \leq x}\,\text{All I}}{\{\ \} \vdash (\exists x.\, \forall y.\, x \leq y) \Rightarrow (\forall x.\, \exists y.\, y \leq x)}\,\text{Imp I}$$

Example

Show

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\{\exists x.\,\forall y.\,x \le y\} \vdash \exists x.\,\forall y.\,x \le y}\,\text{Hyp} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \forall y.\,z \le y}\,\text{Hyp} \qquad \dfrac{\dfrac{}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y;\; z \le x\end{array}\right\} \vdash z \le x}\,\text{Hyp}}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y;\; z \le x\end{array}\right\} \vdash \exists y.\,y \le x}\,\text{Ex I}}{\left\{\begin{array}{c}\exists x.\,\forall y.\,x \le y;\\ \forall y.\,z \le y\end{array}\right\} \vdash \exists y.\,y \le x}\,\text{All E}}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \exists y.\,y \le x}\,\text{Ex E}}{\{(\exists x.\,\forall y.\,x \le y)\} \vdash \forall x.\,\exists y.\,y \le x}\,\text{All I}}{\{\ \} \vdash (\exists x.\,\forall y.\,x \le y) \Rightarrow (\forall x.\,\exists y.\,y \le x)}\,\text{Imp I}$$

Example of Failure

Let's try to show 1

$$\frac{}{\{\ \} \vdash (\forall x.\, \exists y.\, y \leq x) \Rightarrow (\exists x.\, \forall y.\, x \leq y)}$$

Example of Failure

Let's try to show 2

$$\dfrac{\dfrac{}{\{\forall x.\, \exists y.\, y \leq x\} \vdash \exists x.\, \forall y.\, x \leq y}}{\{\ \} \vdash (\forall x.\, \exists y.\, y \leq x) \Rightarrow (\exists x.\, \forall y.\, x \leq y)}\ \text{Imp I}$$

Example of Failure

Let's try to show 3

$$\dfrac{\dfrac{\overline{\{\forall x.\, \exists y.\, y \leq x\} \vdash \forall y.\, z \leq y}}{\{\forall x.\, \exists y.\, y \leq x\} \vdash \exists x.\, \forall y.\, x \leq y}\ \text{Ex I}}{\{\ \} \vdash (\forall x.\, \exists y.\, y \leq x) \Rightarrow (\exists x.\, \forall y.\, x \leq y)}\ \text{Imp I}$$

Example of Failure

Let's try to show 4

$$\frac{\dfrac{\dfrac{\dfrac{}{\{\forall x.\, \exists y.\, y \leq x\} \vdash z \leq x}}{\{\forall x.\, \exists y.\, y \leq x\} \vdash \forall y.\, z \leq y}\text{ All I}}{\{\forall x.\, \exists y.\, y \leq x\} \vdash \exists x.\, \forall y.\, x \leq y}\text{ Ex I}}{\{\ \} \vdash (\forall x.\, \exists y.\, y \leq x) \Rightarrow (\exists x.\, \forall y.\, x \leq y)}\text{ Imp I}$$

Example of Failure

Let's try to show 5

$$\dfrac{\dfrac{}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall x.\,\exists y.\,y \leq x} \quad \dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x\end{array}\right\} \vdash z \leq x}}{\{\forall x.\,\exists y.\,y \leq x\} \vdash z \leq x}\ \text{All E}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash z \leq x}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall y.\,z \leq y}\ \text{All I}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall y.\,z \leq y}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \exists x.\,\forall y.\,x \leq y}\ \text{Ex I}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash \exists x.\,\forall y.\,x \leq y}{\{\ \} \vdash (\forall x.\,\exists y.\,y \leq x) \Rightarrow (\exists x.\,\forall y.\,x \leq y)}\ \text{Imp I}$$

Example of Failure

Let's try to show 6

$$\dfrac{\dfrac{}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall x.\,\exists y.\,y \leq x}\text{Hyp} \quad \dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x\end{array}\right\} \vdash z \leq x}}{\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash z \leq x}{\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall y.\,z \leq y}{\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash \exists x.\,\forall y.\,x \leq y}{\{\,\} \vdash (\forall x.\,\exists y.\,y \leq x) \Rightarrow (\exists x.\,\forall y.\,x \leq y)}\text{Imp I}}\text{Ex I}}\text{All I}}\text{All E}$$

Example of Failure

Let's try to show 7

$$\dfrac{\dfrac{}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall x.\,\exists y.\,y \le x}\text{Hyp} \quad \dfrac{\dfrac{\dfrac{}{\textit{Something}}\textit{Lab} \quad \dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x;\ z \le x\end{array}\right\} \vdash z \le x}}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x\end{array}\right\} \vdash z \le x}\text{Ex E}}{}\text{All E}}{\dfrac{\dfrac{\dfrac{\{\forall x.\,\exists y.\,y \le x\} \vdash z \le x}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}\text{All I}}{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}\text{Ex I}}{\{\ \} \vdash (\forall x.\,\exists y.\,y \le x) \Rightarrow (\exists x.\,\forall y.\,x \le y)}\text{Imp I}}$$

Example of Failure

Let's try to show 8

$$\dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x;\ z \le x\end{array}\right\} \vdash z \le x}\ \text{Hyp}$$

Something *Lab*

$$\dfrac{\dfrac{}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall x.\,\exists y.\,y \le x}\ \text{Hyp} \qquad \dfrac{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x;\ z \le x\end{array}\right\} \vdash z \le x}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x\end{array}\right\} \vdash z \le x}\ \text{Ex E}}{\{\forall x.\,\exists y.\,y \le x\} \vdash z \le x}\ \text{All E}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \le x\} \vdash z \le x}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}\ \text{All I}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}\ \text{Ex I}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}{\{\ \} \vdash (\forall x.\,\exists y.\,y \le x) \Rightarrow (\exists x.\,\forall y.\,x \le y)}\ \text{Imp I}$$

Example of Failure

Let's try to show 9

$$\dfrac{}{\mathit{Something}} \quad \mathit{Lab}$$

$$\dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x;\ z \leq x\end{array}\right\} \vdash z \leq x}\ \text{Hyp}$$

$$\dfrac{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x;\ z \leq x\end{array}\right\} \vdash z \leq x}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x\end{array}\right\} \vdash z \leq x}\ \text{Ex E}$$

$$\dfrac{}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall x.\,\exists y.\,y \leq x}\ \text{Hyp}$$

$$\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall x.\,\exists y.\,y \leq x \qquad \left\{\begin{array}{c}\forall x.\,\exists y.\,y \leq x;\\ \exists y.\,y \leq x\end{array}\right\} \vdash z \leq x}{\{\forall x.\,\exists y.\,y \leq x\} \vdash z \leq x}\ \text{All E}$$

$$\dfrac{\dfrac{\dfrac{\{\forall x.\,\exists y.\,y \leq x\} \vdash z \leq x}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \forall y.\,z \leq y}\ \text{All I}}{\{\forall x.\,\exists y.\,y \leq x\} \vdash \exists x.\,\forall y.\,x \leq y}\ \text{Ex I}}{\{\ \} \vdash (\forall x.\,\exists y.\,y \leq x) \Rightarrow (\exists x.\,\forall y.\,x \leq y)}\ \text{Imp I}$$

Example of Failure

Let's try to show 10

$$
\dfrac{
  \dfrac{}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall x.\,\exists y.\,y \le x}\;\text{Hyp}
  \qquad
  \dfrac{
    \dfrac{\dfrac{}{\textit{Something}}\;\textit{Lab} \quad \dfrac{}{\left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x;\ z \le x\end{array}\right\} \vdash z \le x}\;\text{Hyp}}{}
  }{
    \left\{\begin{array}{c}\forall x.\,\exists y.\,y \le x;\\ \exists y.\,y \le x\end{array}\right\} \vdash z \le x
  }\;\text{Ex E}
}{
  \dfrac{
    \dfrac{
      \dfrac{\{\forall x.\,\exists y.\,y \le x\} \vdash z \le x}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}\;\text{All I}
    }{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}\;\text{Ex I}
  }{\{\ \} \vdash (\forall x.\,\exists y.\,y \le x) \Rightarrow (\exists x.\,\forall y.\,x \le y)}\;\text{Imp I}
}\;\text{All E}
$$

Floyd-Hoare Logic

- Also called Axiomatic Semantics
- Based on formal logic (first order predicate calculus)
- Logical system built from axioms and inference rules
- Mainly suited to simple imperative programming languages
- Ideas applicable quite broadly

Floyd-Hoare Logic

- Used to formally prove a property (post-condition) of the state (the values of the program variables) after the execution of program, assuming another property (pre-condition) of the state holds before execution

Floyd-Hoare Logic

- Goal: Derive statements of form

$$\{P\}\ C\ \{Q\}$$

  - P, Q logical statements about state, P precondition, Q postcondition, C program

- Example:

$$\{x = 1\}\ x := x + 1\ \{x = 2\}$$

Floyd-Hoare Logic

- **Approach:** For each type of language statement, give an axiom or inference rule stating how to derive assertions of form

$$\{P\}\ C\ \{Q\}$$

  where C is a statement of that type
- Compose axioms and inference rules to build proofs for complex programs

Partial vs Total Correctness

- An expression $\{P\}\ C\ \{Q\}$ is a partial correctness statement
- For total correctness must also prove that C terminates (i.e. doesnt run forever)
  - Written: $[P]\ C\ [Q]$
- Will only consider partial correctness here

Simple Imperative Language

- We will give rules for simple imperative language

$$\langle \textit{command} \rangle \; ::= \; \langle \textit{variable} \rangle := \langle \textit{term} \rangle$$
$$\mid \langle \textit{command} \rangle; \; \ldots; \; \langle \textit{command} \rangle$$
$$\mid \textit{if} \; \langle \textit{statement} \rangle \; \textit{then} \; \langle \textit{command} \rangle \; \textit{else} \; \langle \textit{command} \rangle$$
$$\mid \textit{while} \; \langle \textit{statement} \rangle \; \textit{do} \; \langle \textit{command} \rangle$$

- Could add more features, like for-loops

Substitution

- Notation: $P[e/v]$ (sometimes $P[v \to e]$)
- Meaning: Replace every v in P by e
- Example:

$$(x+2)[y-1/x] = ((y-1)+2)$$

The Assingment Rule

$$\overline{\{P[e/x]\}\ x\ :=\ e\ \{P\}}$$

Example:

$$\overline{\{\quad ?\quad\}\ x\ :=\ y\ \{\,x\ = 2\,\}}$$

The Assingment Rule

$$\frac{}{\{P[e/x]\}\ x\ :=\ e\ \{P\}}$$

Example:

$$\frac{}{\{\ \boxed{} = 2\}\ x\ :=\ y\ \{\boxed{x} = 2\ \}}$$

The Assingment Rule

$$\overline{\{P[e/x]\}\ x\ :=\ e\ \{P\}}$$

Example:

$$\overline{\{\ \boxed{x} = 2\}\ x\ :=\ y\ \{\boxed{x} = 2\ \}}$$

The Assingment Rule

$$\overline{\{P[e/x]\}\ x\ :=\ e\ \{P\}}$$

Examples:

$$\overline{\{y = 2\}\ x\ :=\ y\ \{x = 2\}}$$

$$\overline{\{y = 2\}\ x\ :=\ 2\ \{y = x\}}$$

$$\overline{\{x + 1 = n + 1\}\ x\ :=\ x + 1\ \{x = n + 1\}}$$

$$\overline{\{2 = 2\}\ x\ :=\ 2\ \{x = 2\}}$$

The Assignment Rule – Your Turn

- What is the weakest precondition of

$$x := x + y \{ x + y = wx \}?$$

$$\{ \quad ? \quad \}$$
$$x := x + y$$
$$\{ x + y = wx \}$$

- What is the weakest precondition of

$$x := x + y \; \{ x + y = wx \}?$$

$$\{ (x + y) + y = w(x + y) \}$$
$$x := x + y$$
$$\{ x + y = wx \}$$

Precondition Strengthening

$$\frac{(P \Rightarrow P')\,\{P'\}\ C\ \{Q\}}{\{P\}\ C\ \{Q\}}$$

- Meaning: If we can show that P implies P' (*i.e.* $(P \Rightarrow P')$) and we can show that $\{P\}\ C\ \{Q\}$, then we know that $\{P\}\ C\ \{Q\}$
- P is stronger than P' means $P \Rightarrow P'$

Precondition Strengthening

- Examples:

$$\frac{x = 3 \Rightarrow x < 7 \quad \{x < 7\}\ x\ :=\ x + 3\ \{x < 10\}}{\{x = 3\}\ x\ :=\ x + 3\ \{x < 10\}}$$

$$\frac{\mathit{True} \Rightarrow (2 = 2) \quad \{2 = 2\}\ x\ :=\ 2\ \{x = 2\}}{\{\mathit{True}\}\ x\ :=\ 2\ \{x = 2\}}$$

$$\frac{x = n \Rightarrow x + 1 = n + 1 \quad \{x + 1 = n + 1\}\ x\ :=\ x + 1\ \{x = n + 1\}}{\{x = n\}\ x\ :=\ x + 1\ \{x = n + 1\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}$$

$$\frac{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

$$\frac{\{x * x < 25\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}\ \mathit{YES}$$

$$\frac{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

$$\frac{\{x * x < 25\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ :=\ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}\ YES$$

$$\frac{\{x = 3\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}\ NO$$

$$\frac{\{x * x < 25\}\ x\ := \ x * x\ \{x < 25\}}{\{x > 0 \wedge x < 5\}\ x\ := \ x * x\ \{x < 25\}}$$

Which Inferences Are Correct?

$$\frac{\{x > 0 \land x < 5\}\ x\ :=\ x * x\ \{x < 25\}}{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}\ \textit{YES}$$

$$\frac{\{x = 3\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \land x < 5\}\ x\ :=\ x * x\ \{x < 25\}}\ \textit{NO}$$

$$\frac{\{x * x < 25\}\ x\ :=\ x * x\ \{x < 25\}}{\{x > 0 \land x < 5\}\ x\ :=\ x * x\ \{x < 25\}}\ \textit{YES}$$