## CS477 Formal Software Dev 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 21, 2018

## Free Variables: Terms

Informally: free variables of a expression are variables that have an occurrence in an expression that is not bound. Written  $f_V(e)$  for expression e

Free variables of terms defined by structural induction over terms; written

- $fv(x) = \{x\}$
- $fv(f(t_1,\ldots,t_n) = \bigcup_{i=1,\ldots,n} fv(t_i)$

## Note:

- Free variables of term just variables occurring in term; no bound
- No free variables in constants
- Example:  $fv(add(1, abs(x))) = \{x\}$

Assume given structure  $S = (G, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ , term t over G, and a and b

Assume given structure  $S = (G, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ , formula  $\psi$  over G, and a

and b assignments. If for every  $x \in fv(\psi)$  we have a(x) = b(x) then

Free Variables, Assignments and Interpretation

assignments. If for every  $x \in fv(t)$  we have a(x) = b(x) then

## Free Variables: Formulae

Defined by structural induction on formulae; uses fv on terms

- $fv(true) = fv(false) = \{ \}$
- $$\begin{split} & \bullet \ \, \mathit{fv}(\mathit{r}(t_1,\ldots,t_n)) = \bigcup_{i=1,\ldots,n} \mathit{fv}(t_i) \\ & \bullet \ \, \mathit{fv}(\psi_1 \wedge \psi_2) = \mathit{fv}(\psi_1 \vee \psi_2) = \mathit{fv}(\psi_1 \Rightarrow \psi_2) = \mathit{fv}(\psi_1 \Leftrightarrow \psi_2) = \end{split}$$
   $(\mathit{fv}(\psi_1) \cup \mathit{fv}(\psi_2))$
- $fv(\forall v. \psi) = fv(\exists v. \psi) = (fv(\psi) \setminus \{v\})$

Variable occurrence at quantifier are binding occurrence

Occurrence that is not free and not binding is a bound occurrence

 $\mathcal{M}_{a}(\psi) = \mathcal{M}_{b}(\psi).$ 

Theorem

 $\mathcal{T}_a(t) = \mathcal{T}_b(a)$ .

# Syntactic Substitution versus Assignment Update

- When interpreting universal quantification  $(\forall x. \psi)$ , wanted to check interpretation of every instance of  $\psi$  where v was replaced by element of semantic domain  ${\cal D}$
- ullet How: semantically interpret  $\psi$  with assignment updated by  $v\mapsto d$ for every  $d \in \mathcal{D}$
- Syntactically?
- Answer: substitution

## Substitution in Terms

- Substitution of term t for variable x in term s (written s[t/x]) gotten by replacing every instance of x in s by t
  - x called redex; t called residue
- Yields instance of s

Formally defined by structural induction on terms:

- $\bullet x[t/x] = t$
- y[t/x] = y for variable y where  $y \neq x$
- $f(t_1,...,t_n)[t/x] = f(t_1[t/x],...,t_n[t/x])$

**Example:** (add(1, abs(x)))[add(x, y)/x] = add(1, abs(add(x, y)))

## Substitution in Formulae: Problems

- Want to define by structural induction, similar to terms
- Quantifiers must be handled with care
  - Substitution only replaces free occurrences of variable Example:

$$(x > 3 \land (\exists y. (\forall z. z \ge (y - x)) \lor (z \ge y)))[x + 2/z] = (x > 3 \land (\exists y. (\forall z. z \ge (y - x)) \lor (x + 2 \ge y)))$$

• Need to avoid free variable capture Example Problem:

$$(x > 3 \land (\exists y. (\forall z. z \ge (y - x)) \lor (z \ge y)))[x + y/z] \ne$$

$$(x > 3 \land (\exists y. (\forall z. z \ge (y - x)) \lor (x + y \ge y)))$$

Substitution in Formulae

right not defined

• true[t/x] = true

 $\mathcal{T}_a(s[t/x]) = \mathcal{T}_b(s).$ 

Theorem

• Read equations below as saying left is not defined if any expression on

false[t/x] = false

•  $(\psi_1 \otimes \psi_2)[t/x] = (\psi_1[t/x]) \otimes (\psi_2[t/x])$  for  $\emptyset \in \{\land, \lor, \Rightarrow, \Leftrightarrow\}$ 

• Defined by structural induction; uses substitution in terms

•  $r(t_1,...,t_n)[t/x] = r((t_1[t/x],...,t_n[t/x]))$ 

 $\bullet \ \ (\mathcal{Q} \, x. \, \psi)[t/x] = \mathcal{Q} \, x. \, \psi \ \text{for} \ \ \mathcal{Q} \in \{\forall, \exists\}$ 

 $\bullet \ (\psi)[t/x] = (\psi[t/x]) \qquad (\neg \psi)[t/x] = \neg(\psi[t/x])$ 

Assume given structure  $S = (G, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ , variable x, terms s and t

over  $\mathcal{G}$ , and a assignment. Let  $b = a[x \mapsto \mathcal{T}_a(t)]$ . Then

## Substitution in Formulae: Two Approaches

- When quantifier would capture free variable of redex, can't substitute in formula as is
- Solution 1: Make substitution partial function undefined in this case
- Solution 2: Define equivalence relation based on renaming bound variables; define substitution on equivalence classes
- Will take Solution 1 here
- Still need definition of equivalence up to renaming bound variables

•  $(Qy, \psi)[t/x] = Qy, (\psi[t/x])$  if  $x \neq y$  and  $y \notin fv(t)$  for  $Q \in \{\forall, \exists\}$ •  $(Qy, \psi)[t/x]$  not defined if  $x \neq y$  and  $y \in fv(t)$  for  $Q \in \{\forall, \exists\}$ 

## Substitution in Formulae

## **Examples**

$$(x > 3 \land (\exists y. (\forall z. z \ge (y - x)) \lor (z \ge y)))[x + y/z]$$
 not defined

$$(x > 3 \land (\exists w. (\forall z. z \ge (w - x)) \lor (z \ge w)))[x + y/z] = (x > 3 \land (\exists w. (\forall z. z \ge (w - x)) \lor ((x + y) \ge y)))$$

Assume given structure  $S = (G, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ , formula  $\psi$  over G, and a assignment. If  $\psi[t/x]$  defined, then  $a \models^{\mathcal{S}} \psi[t/x]$  if and only if  $a[x \mapsto \mathcal{T}_a(t)] \models^{\mathcal{S}} \psi$ 

## Renaming by Swapping: Terms

Define the swapping of two variables in a term  $t[x \leftrightarrow y]$  by structural induction on terms:

- $\bullet x[x \leftrightarrow y] = y \text{ and } y[x \leftrightarrow y] = x$
- $z[x \leftrightarrow y] = z$  for z a variable,  $z \neq x$ ,  $z \neq y$
- $f(t_1, \ldots, t_n)[x \leftrightarrow y] = f(t_1[x \leftrightarrow y], \ldots, t_n[x \leftrightarrow y])$

## **Examples:**

$$add(1, abs(add(x, y)))[x \leftrightarrow y] = add(1, abs(add(y, x)))$$
  
 $add(1, abs(add(x, y)))[x \leftrightarrow z] = add(1, abs(add(z, y)))$ 

## Renaming by Swapping: Terms

## Theorem

Assume given structure  $S = (G, D, F, \phi, R, \rho)$ , variables x and y, term t over  $\mathcal{G}$ , and a assignment. Let  $b = a[x \mapsto a(y)][y \mapsto a(x)]$ . Then  $\mathcal{T}_a(t[x \leftrightarrow y]) = \mathcal{T}_b(t)$ 

## Renaming by Swapping: Terms

## Proof.

By structural induction on terms, suffices to show theorem for the case where t variable, and case  $t = f(t_1, \ldots, t_n)$ , assuming result for  $t_1, \ldots, t_n$ 

- Case: *t* variable
  - Subcase: t = x. Then  $\mathcal{T}_a(x[x \leftrightarrow y]) = \mathcal{T}_a(y) = a(y)$  and  $\mathcal{T}_b(x) = b(x) = a[x \mapsto a(y)][y \mapsto a(x)](x) = a[x \mapsto \mathcal{T}_a(y)](x) = a(y)$ so  $\mathcal{T}_a(t[x \leftrightarrow y]) = \mathcal{T}_b(t)$
  - Subcase: t = y. Then  $\mathcal{T}_a(y[x \leftrightarrow y]) = \mathcal{T}_a(x) = a(x)$  and  $\mathcal{T}_b(y) = b(y) = a(x) + a(y)[y \mapsto a(x)](x) = a(x)$  so  $\mathcal{T}_a(t[x \leftrightarrow y]) = \mathcal{T}_b(t)$
  - Subcase: t = z variable,  $z \neq x$  and  $z \neq y$ . Then  $\mathcal{T}_a(z[x\leftrightarrow y]) = \mathcal{T}_a(z) = a(z)$  and  $\mathcal{T}_b(z) = b(z) = a[x \mapsto a(y)][y \mapsto a(x)](z) = a[x \mapsto \mathcal{T}_a(y)](z) = a(z)$ so  $\mathcal{T}_a(t[x \leftrightarrow y]) = \mathcal{T}_b(t)$

Renaming by Swapping: Formulae

induction, using swapping on terms:

•  $\text{true}[x \leftrightarrow y] = \text{true}$ 

 $\otimes \in \{\land, \lor, \Rightarrow, \Leftrightarrow\}$ 

 $z \neq y$ , and  $Q \in \{ \forall, \exists \}$ 

Define the swapping of two variables in a formula  $\psi[x \leftrightarrow y]$  by structural

•  $r(t_1,\ldots,t_n)[x\leftrightarrow y]=r((t_1[x\leftrightarrow y],\ldots,t_n[x\leftrightarrow y]))$ 

•  $(\psi_1 \otimes \psi_2)[x \leftrightarrow y] = (\psi_1[x \leftrightarrow y]) \otimes (\psi_2[x \leftrightarrow y])$  for

•  $(Qx.\psi)[x \leftrightarrow y] = Qy.(\psi[x \leftrightarrow y])$  for  $Q \in \{\forall, \exists\}$ 

•  $(Qy.\psi)[x \leftrightarrow y] = Qy.(\psi[x \leftrightarrow y])$  for  $Q \in \{\forall, \exists\}$ 

•  $(\psi)[x \leftrightarrow y] = (\psi[x \leftrightarrow y])$   $(\neg \psi)[x \leftrightarrow y] = \neg(\psi[x \leftrightarrow y])$ 

 $false[x \leftrightarrow y] = false$ 

# Renaming by Swapping: Terms

## Proof.

• Case:  $t = f(t_1, \dots, t_n)$ . Assume  $\mathcal{T}_a(t_i[x \leftrightarrow y]) = \mathcal{T}_b(t_i)$  for  $i = 1, \ldots, n$ . Then

$$\begin{split} \mathcal{T}_{\textbf{a}}(t[\textbf{x}\leftrightarrow \textbf{y}]) &= \mathcal{T}_{\textbf{a}}(f(t_1,\ldots,t_n)[\textbf{x}\leftrightarrow \textbf{y}]) \\ &= \mathcal{T}_{\textbf{a}}(f(t_1[\textbf{x}\leftrightarrow \textbf{y}],\ldots,t_n[\textbf{x}\leftrightarrow \textbf{y}])) \\ &= \phi(f)(\mathcal{T}_{\textbf{a}}(t_1[\textbf{x}\leftrightarrow \textbf{y}]),\ldots,\mathcal{T}_{\textbf{a}}(t_n[\textbf{x}\leftrightarrow \textbf{y}])) \\ &= \phi(f)(\mathcal{T}_{\textbf{b}}(t_1),\ldots,\mathcal{T}_{\textbf{b}}(t_n)) \\ &\text{since } \mathcal{T}_{\textbf{a}}(t_i[\textbf{x}\leftrightarrow \textbf{y}]) = \mathcal{T}_{\textbf{b}}(t_i) \text{ for } i=1,\ldots,n \\ &= \mathcal{T}_{\textbf{b}}(f(t_1,\ldots,t_n)) \\ &= \mathcal{T}_{\textbf{b}}(t) \quad \Box \end{aligned}$$

•  $(Qz, \psi)[x \leftrightarrow y] = Qz, (\psi[x \leftrightarrow y])$  for z a variable with  $z \neq x$ ,

## Renaming by Swapping: Formulae

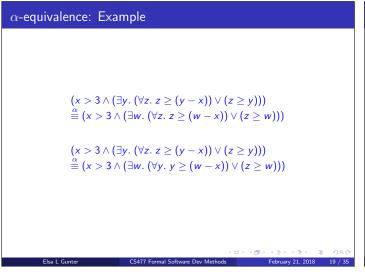
## Examples

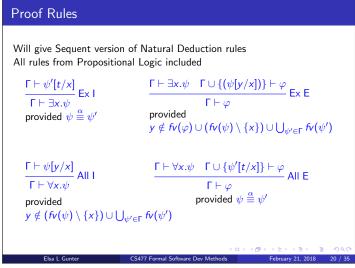
$$\begin{array}{l} (x > 3 \land (\exists y. \ (\forall z. \ z \geq (y - x)) \lor (z \geq y)))[x \leftrightarrow y] \\ = (y > 3 \land (\exists x. \ (\forall z. \ z \geq (x - y)) \lor (z \geq x))) \\ (x > 3 \land (\exists y. \ (\forall z. \ z \geq (y - x)) \lor (z \geq y)))[y \leftrightarrow z] \\ (x > 3 \land (\exists y. \ (\forall z. \ z \geq (y - x)) \lor (z \geq y)))[y \leftrightarrow w] \end{array}$$

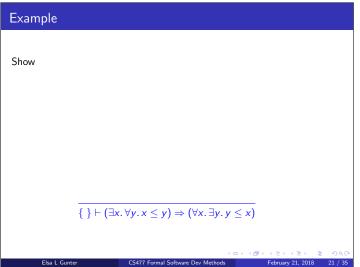
Assume given structure  $S = (G, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ , variables x and y, formula  $\psi$  over  $\mathcal{G}$ , and a assignment. If  $x \notin fv(t)$  and  $y \notin fv(t)$  then  $\psi[x \leftrightarrow y] \equiv \psi$ 

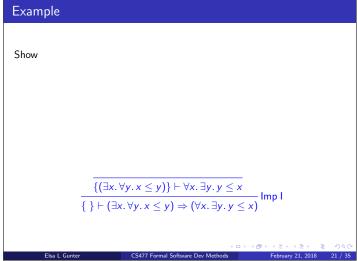
## $\alpha$ -equivalence

- $\bullet \ \ \text{If} \ \psi_1 \stackrel{\alpha}{\equiv} \psi_2 \ \text{then} \ \psi_2 \stackrel{\alpha}{\equiv} \psi.$
- $\bullet$  It  $\psi_1\stackrel{lpha}{\equiv}\psi_2$  and  $\psi_2\stackrel{lpha}{\equiv}\psi_3$  then  $\psi_1\stackrel{lpha}{\equiv}\psi_3$
- If  $x \notin fv(\psi)$  and  $y \notin fv(\psi)$  then  $\psi \stackrel{\alpha}{=} \psi[x \leftrightarrow y]$ .
- If  $\psi_i \stackrel{\alpha}{=} \psi_i'$  for i = 1, 2 then
  - $\bullet \ (\psi_1) \stackrel{\alpha}{\equiv} (\psi_1') \qquad \neg \psi_1 \stackrel{\alpha}{\equiv} \neg \psi_1'$
  - $\begin{array}{l} \bullet \;\; \psi_1 \otimes \psi_2 \stackrel{\alpha}{\equiv} \psi_1' \otimes \psi_2' \; \text{for} \; \otimes \in \{\land, \lor, \Rightarrow, \Leftrightarrow\} \\ \bullet \;\; \mathcal{Q} \, z. \, \psi_1 \stackrel{\alpha}{\equiv} \; \mathcal{Q} \, z. \, \psi_1' \; \text{for} \; \mathcal{Q} \in \{\forall, \exists\} \end{array}$





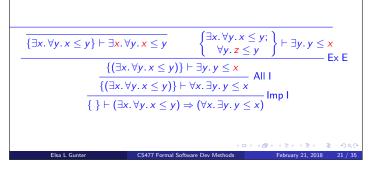




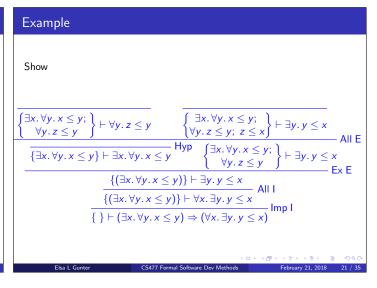
Example

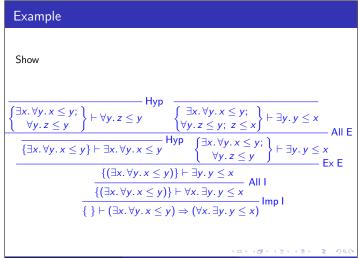
Show

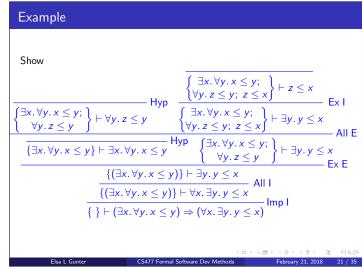
Show  $\frac{\{(\exists x. \forall y. x \leq y)\} \vdash \exists y. y \leq x}{\{(\exists x. \forall y. x \leq y)\} \vdash \forall x. \exists y. y \leq x} \text{ All I} \\ \frac{\{(\exists x. \forall y. x \leq y)\} \vdash \forall x. \exists y. y \leq x}{\{\} \vdash (\exists x. \forall y. x \leq y) \Rightarrow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

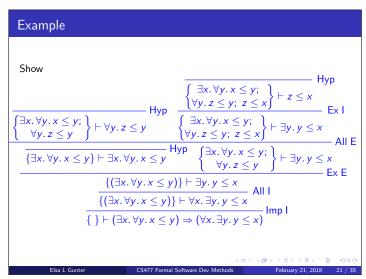


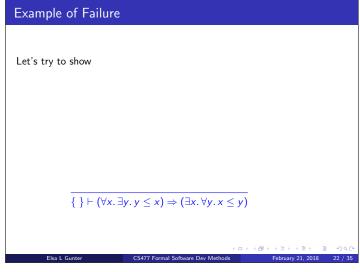
# Show $\frac{\{\exists x. \forall y. x \leq y\} \vdash \exists x. \forall y. x \leq y}{\{\exists x. \forall y. x \leq y\}} \vdash \exists y. y \leq x}{\{(\exists x. \forall y. x \leq y)\} \vdash \exists y. y \leq x} \vdash \{x \in \{(\exists x. \forall y. x \leq y)\} \vdash \forall x. \exists y. y \leq x} \vdash \{x \in \{(\exists x. \forall y. x \leq y)\} \vdash \forall x. \exists y. y \leq x} \vdash \{x \in \{(\exists x. \forall y. x \leq y)\} \vdash \forall x. \exists y. y \leq x} \vdash \{x \in \{(\exists x. \forall y. x \leq y)\} \vdash \{x \in \{(\exists x. x \in \{x\} \mid x)\} \vdash \{x \in \{(\exists x. x \in \{x\} \mid x)\} \vdash \{x \in \{x\} \mid x)\} \vdash \{x \in \{(\exists x. x \in \{x\} \mid x)\} \vdash \{x \in \{x\} \mid x)\} \vdash \{x \in \{(\exists x. x \in \{x\} \mid x)\} \vdash \{x \in \{x\} \mid x)\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{(\exists x. x \in \{x\} \mid x)\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\} \mid x\} \vdash \{x \in \{x\} \mid x\}$











## Example of Failure

Let's try to show

$$\frac{ \{ \forall x. \exists y. y \le x \} \vdash \exists x. \forall y. x \le y}{\{ \} \vdash (\forall x. \exists y. y \le x) \Rightarrow (\exists x. \forall y. x \le y)} \operatorname{Imp} I$$

# Let's try to show $\frac{\overline{\{\forall x.\,\exists y.\,y\leq x\}\vdash \forall y.\,z\leq y}}{\{\forall x.\,\exists y.\,y\leq x\}\vdash \exists x.\,\forall y.\,x\leq y}\,\mathop{\mathsf{Ex}}\nolimits \, I}\\ \frac{\{\,\}\vdash (\forall x.\,\exists y.\,y\leq x)\ni (\exists x.\,\forall y.\,x\leq y)}{\{\,\}\vdash (\forall x.\,\exists y.\,y\leq x)\Rightarrow (\exists x.\,\forall y.\,x\leq y)}\,\mathop{\mathsf{Imp}}\nolimits \, I}$

## Example of Failure

Let's try to show

$$\frac{ \left\{ \forall x. \exists y. y \le x \right\} \vdash \mathbf{z} \le x}{\left\{ \forall x. \exists y. y \le x \right\} \vdash \forall y. z \le y} \text{ All I}$$

$$\frac{ \left\{ \forall x. \exists y. y \le x \right\} \vdash \exists x. \forall y. x \le y}{\left\{ \exists x. \exists y. y \le x \right\} \Rightarrow \left( \exists x. \forall y. x \le y \right)} \text{ Imp I}$$

# Example of Failure

Example of Failure

Let's try to show

$$\frac{\left\{\forall x. \exists y. y \leq x\right\} \vdash \forall x. \exists y. y \leq x}{\left\{\forall x. \exists y. y \leq x\right\} \vdash z \leq x} \text{All E}$$

$$\frac{\left\{\forall x. \exists y. y \leq x\right\} \vdash z \leq x}{\left\{\forall x. \exists y. y \leq x\right\} \vdash \forall y. z \leq y} \text{All I}$$

$$\frac{\left\{\forall x. \exists y. y \leq x\right\} \vdash \forall y. z \leq y}{\left\{\forall x. \exists y. y \leq x\right\} \vdash \exists x. \forall y. x \leq y} \text{Imp I}$$

$$\frac{\left\{\left\{\right\} \vdash (\forall x. \exists y. y \leq x\right\} \vdash \exists x. \forall y. x \leq y}{\left\{\right\} \vdash (\forall x. \exists y. y \leq x) \Rightarrow (\exists x. \forall y. x \leq y)} \text{Imp I}$$

# Example of Failure

Let's try to show

$$\frac{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash \forall x. \exists y. y \leq x}{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash z \leq x} } \text{All E}$$

$$\frac{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash z \leq x}{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash \forall y. z \leq y} } \text{All I}$$

$$\frac{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash \forall y. z \leq y}{ \left\{ \forall x. \exists y. y \leq x \right\} \vdash \exists x. \forall y. x \leq y} } \text{Imp I}$$

$$\frac{ \left\{ \left\{ \right\} \vdash \left( \forall x. \exists y. y \leq x \right\} \Rightarrow \left( \exists x. \forall y. x \leq y \right) \right] }{ \left\{ \left\{ \right\} \vdash \left( \forall x. \exists y. y \leq x \right\} \Rightarrow \left( \exists x. \forall y. x \leq y \right) \right\} }$$

## Example of Failure

Let's try to show 
$$\frac{\left\{ \forall x. \exists y. y \le x; \right\} \vdash \exists y. y \le x \quad \left\{ \exists y. y \le x; \right\} \vdash z \le x}{\left\{ \exists y. y \le x; \right\} \vdash z \le x} \quad \text{Ex E}$$

$$\frac{\left\{ \forall x. \exists y. y \le x \right\} \vdash \forall x. \exists y. y \le x \quad \left\{ \exists y. y \le x; \right\} \vdash z \le x}{\left\{ \forall x. \exists y. y \le x \right\} \vdash z \le x} \quad \text{All I}$$

$$\frac{\left\{ \forall x. \exists y. y \le x \right\} \vdash \forall x. \exists y. y \le x \right\} \vdash z \le x}{\left\{ \forall x. \exists y. y \le x \right\} \vdash \forall y. z \le y} \quad \text{All I}$$

$$\frac{\left\{ \forall x. \exists y. y \le x \right\} \vdash \forall x. \exists y. y \le x \right\} \vdash \exists x. \forall y. x \le y}{\left\{ \forall x. \exists y. y \le x \right\} \vdash \exists x. \forall y. x \le y} \quad \text{Imp I}$$

## Example of Failure

Let's try to show

$$\frac{\left\{ \forall x. \exists y. y \leq x; \right\} \vdash \exists y. y \leq x}{\left\{ \exists y. y \leq x; \right\} \vdash z \leq x} \vdash \exists y. y \leq x} \qquad \frac{\left\{ \forall x. \exists y. y \leq x; \right\} \vdash z \leq x}{\left\{ \exists y. y \leq x; \bigotimes \leq x \right\} \vdash z \leq x} \quad \text{Ex E}$$

$$\frac{\left\{ \forall x. \exists y. y \leq x \right\} \vdash \forall x. \exists y. y \leq x}{\left\{ \forall x. \exists y. y \leq x \right\} \vdash z \leq x} \quad \text{All I}$$

$$\frac{\left\{ \forall x. \exists y. y \leq x \right\} \vdash z \leq x}{\left\{ \forall x. \exists y. y \leq x \right\} \vdash \forall y. z \leq y} \quad \text{Ex I}$$

$$\frac{\left\{ \forall x. \exists y. y \leq x \right\} \vdash \exists x. \forall y. x \leq y}{\left\{ \forall x. \exists y. y \leq x \right\} \vdash \exists x. \forall y. x \leq y} \quad \text{Imp I}$$

# 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,
- 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  $\{P\}$   $\in$   $\{Q\}$  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

```
\begin{split} &\langle command \rangle \; ::= \; \langle variable \rangle := \langle term \rangle \\ &| \; \langle command \rangle; \; \dots; \; \langle command \rangle \\ &| \; if \; \langle statement \rangle \; then \; \langle command \rangle \; else \; \langle command \rangle \\ &| \; while \; \langle statement \rangle \; do \; \langle command \rangle \end{split}
```

• Could add more features, like for-loops

《□》《□》《壹》《臺》 臺 ◆○Q √ Methods February 21, 2018 28 / 3

## Substitution

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

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

 ←□→ ←②→ ←②→ ←②→
 □→ ←②→
 □→ ←②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 □→ ◆②→
 <

## The Assingment Rule

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

Example:

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

( , ) ~ , ) ( ^ = )

Elsa L Gunter

CS477 Formal Software Dev Methods

l > ← 분 > ← 분 > - 현 = - ∽ Q(

# The Assingment Rule

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

Example:

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

## The Assingment Rule

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

Example:

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

## 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

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

$$\left\{ \begin{array}{c} ? \\ x := x + y \\ \left\{ x + y = wx \right\} \end{array} \right\}$$

## The Assignment Rule – Your Turn

• What is the weakest precondition of

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

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

• Examples:

Precondition Strengthening

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

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

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

## Precondition Strengthening

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

- 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  $P \Rightarrow P'$

## Which Inferences Are Correct?

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

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

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

## Which Inferences Are Correct?

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

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

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

## Which Inferences Are Correct?

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

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

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

## Which Inferences Are Correct?

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

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

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