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 $fv(e)$ 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 variables
- No free variables in constants
- **Example**: $fv(add(1, abs(x))) = \{x\}$

Free Variables: Formulae

Defined by structural induction on formulae; uses fv on terms

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

Variable occurrence at quantifier are binding occurrence
Occurrence that is not free and not binding is a bound occurrence

Example: $fv(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y))) = \{x, z\}$
$\uparrow \quad \uparrow \quad \uparrow$

Free Variables, Assignments and Interpretation

Theorem

Assume given structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$, term t over $\mathcal{G}$, and a and b assignments. If for every $x \in fv(t)$ we have $a(x) = b(x)$ then $\mathcal{T}_a(t) = \mathcal{T}_b(a)$.

Theorem

Assume given structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$, formula ψ over $\mathcal{G}$, and a and b assignments. If for every $x \in fv(\psi)$ we have $a(x) = b(x)$ then $\mathcal{M}_a(\psi) = \mathcal{M}_b(\psi)$.

Syntactic Substitution versus Assignment Update

- When interpreting universal quantification ($\forall x.\ \psi$), wanted to check interpretation of every instance of ψ where v was replaced by element of semantic domain $\mathcal{D}$
- How: semantically - interpret ψ 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:

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

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:

    $(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[x + 2/z] =$
    $(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (x + 2 \geq y)))$

  - Need to avoid *free variable capture*
    Example Problem:

    $(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[x + y/z] \neq$
    $(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (x + y \geq y)))$

Theorem

Assume given structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$*, variable* x*, terms* s *and* t *over* $\mathcal{G}$*, and* a *assignment. Let* $b = a[x \mapsto \mathcal{T}_a(t)]$*. Then* $\mathcal{T}_a(s[t/x]) = \mathcal{T}_b(s)$.

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

Substitution in Formulae

- Defined by structural induction; uses substitution in terms
- Read equations below as saying left is not defined if any expression on right not defined
- $\mathrm{true}[t/x] = \mathrm{true}$ $\quad \mathrm{false}[t/x] = \mathrm{false}$
- $r(t_1, \ldots, t_n)[t/x] = r((t_1[t/x], \ldots, t_n[t/x]))$
- $(\psi)[t/x] = (\psi[t/x])$ $\quad (\neg\psi)[t/x] = \neg(\psi[t/x])$
- $(\psi_1 \otimes \psi_2)[t/x] = (\psi_1[t/x]) \otimes (\psi_2[t/x])$ for $\otimes \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$
- $(\mathcal{Q}\,x.\,\psi)[t/x] = \mathcal{Q}\,x.\,\psi$ for $\mathcal{Q} \in \{\forall, \exists\}$
- $(\mathcal{Q}\,y.\,\psi)[t/x] = \mathcal{Q}\,y.\,(\psi[t/x])$ if $x \neq y$ and $y \notin fv(t)$ for $\mathcal{Q} \in \{\forall, \exists\}$
- $(\mathcal{Q}\,y.\,\psi)[t/x]$ not defined if $x \neq y$ and $y \in fv(t)$ for $\mathcal{Q} \in \{\forall, \exists\}$

Substitution in Formulae

Examples

$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[x + y/z]$ not defined

$(x > 3 \wedge (\exists w.\ (\forall z.\ z \geq (w - x)) \vee (z \geq w)))[x + y/z] =$
$(x > 3 \wedge (\exists w.\ (\forall z.\ z \geq (w - x)) \vee ((x + y) \geq y)))$

Theorem

Assume given structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$*, formula* ψ *over* $\mathcal{G}$*, 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:

- $x[x \leftrightarrow y] = y$ 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 $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$, 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 $\mathcal{T}_b(y) = b(y) = a[x \mapsto a(y)][y \mapsto a(x)](x) = a(x)$ 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: Terms

Proof.

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

$$\begin{aligned}
\mathcal{T}_a(t[x \leftrightarrow y]) &= \mathcal{T}_a(f(t_1, \ldots, t_n)[x \leftrightarrow y]) \\
&= \mathcal{T}_a(f(t_1[x \leftrightarrow y], \ldots, t_n[x \leftrightarrow y])) \\
&= \phi(f)(\mathcal{T}_a(t_1[x \leftrightarrow y]), \ldots, \mathcal{T}_a(t_n[x \leftrightarrow y])) \\
&= \phi(f)(\mathcal{T}_b(t_1), \ldots, \mathcal{T}_b(t_n)) \\
&\quad \text{since } \mathcal{T}_a(t_i[x \leftrightarrow y]) = \mathcal{T}_b(t_i) \text{ for } i = 1, \ldots, n \\
&= \mathcal{T}_b(f(t_1, \ldots, t_n)) \\
&= \mathcal{T}_b(t) \quad \square
\end{aligned}$$

Renaming by Swapping: Formulae

Define the swapping of two variables in a formula $\psi[x \leftrightarrow y]$ by structural induction, using swapping on terms:

- $\mathrm{true}[x \leftrightarrow y] = \mathrm{true}$ $\quad$ $\mathrm{false}[x \leftrightarrow y] = \mathrm{false}$
- $r(t_1, \ldots, t_n)[x \leftrightarrow y] = r((t_1[x \leftrightarrow y], \ldots, t_n[x \leftrightarrow y]))$
- $(\psi)[x \leftrightarrow y] = (\psi[x \leftrightarrow y])$ $\quad$ $(\neg\psi)[x \leftrightarrow y] = \neg(\psi[x \leftrightarrow y])$
- $(\psi_1 \otimes \psi_2)[x \leftrightarrow y] = (\psi_1[x \leftrightarrow y]) \otimes (\psi_2[x \leftrightarrow y])$ for $\otimes \in \{\wedge, \vee, \Rightarrow, \Leftrightarrow\}$
- $(\mathcal{Q}\, x.\, \psi)[x \leftrightarrow y] = \mathcal{Q}\, y.\, (\psi[x \leftrightarrow y])$ for $\mathcal{Q} \in \{\forall, \exists\}$
- $(\mathcal{Q}\, y.\, \psi)[x \leftrightarrow y] = \mathcal{Q}\, y.\, (\psi[x \leftrightarrow y])$ for $\mathcal{Q} \in \{\forall, \exists\}$
- $(\mathcal{Q}\, z.\, \psi)[x \leftrightarrow y] = \mathcal{Q}\, z.\, (\psi[x \leftrightarrow y])$ for z a variable with $z \neq x$, $z \neq y$, and $\mathcal{Q} \in \{\forall, \exists\}$

Renaming by Swapping: Formulae

Examples

$$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[x \leftrightarrow y]$$
$$= (y > 3 \wedge (\exists x.\ (\forall z.\ z \geq (x - y)) \vee (z \geq x)))$$

$$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[y \leftrightarrow z]$$
$$(x > 3 \wedge (\exists y.\ (\forall z.\ z \geq (y - x)) \vee (z \geq y)))[y \leftrightarrow w]$$

Theorem

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

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
  - $(\psi_1) \overset{\alpha}{\equiv} (\psi_1')$ $\quad$ $\neg\psi_1 \overset{\alpha}{\equiv} \neg\psi_1'$
  - $\psi_1 \otimes \psi_2 \overset{\alpha}{\equiv} \psi_1' \otimes \psi_2'$ 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

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

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

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 $\psi \stackrel{\alpha}{\equiv} \psi'$

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

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 $\psi \stackrel{\alpha}{\equiv} \psi'$

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example

Show

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

Example of Failure

Let's try to show

$$\dfrac{}{\{\ \}\vdash(\forall x.\exists y.y\le x)\Rightarrow(\exists x.\forall y.x\le y)}$$

Example of Failure

Let's try to show

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

Example of Failure

Let's try to show

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

Example of Failure

Let's try to show

$$\cfrac{\cfrac{\cfrac{\overline{\{\forall x.\,\exists y.\,y \le x\} \vdash {\color{red}z} \le x}}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}\ \text{All I}}{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}\ \text{Ex I}}{\{\,\} \vdash (\forall x.\,\exists y.\,y \le x) \Rightarrow (\exists x.\,\forall y.\,x \le y)}\ \text{Imp I}$$

Example of Failure

Let's try to show

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

Example of Failure

Let's try to show

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

Example of Failure

Let's try to show

$$\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall x.\,\exists y.\,y \le x}\ \text{Hyp} \qquad \cfrac{\overline{\left\{\begin{matrix}\forall x.\,\exists y.\,y \le x; \\ \exists y.\,y \le x\end{matrix}\right\} \vdash \exists y.\,y \le x} \qquad \overline{\left\{\begin{matrix}\forall x.\,\exists y.\,y \le x; \\ \exists y.\,y \le x;\ {\color{red}z} \le x\end{matrix}\right\} \vdash z \le x}}{\left\{\begin{matrix}\forall x.\,\exists y.\,y \le x; \\ \exists y.\,y \le x\end{matrix}\right\} \vdash {\color{red}z} \le x}\ \text{Ex E}}{\{\forall x.\,\exists y.\,y \le x\} \vdash z \le x}\ \text{All E}}{\{\forall x.\,\exists y.\,y \le x\} \vdash \forall y.\,z \le y}\ \text{All I}}{\{\forall x.\,\exists y.\,y \le x\} \vdash \exists x.\,\forall y.\,x \le y}\ \text{Ex I}}{\{\,\} \vdash (\forall x.\,\exists y.\,y \le x) \Rightarrow (\exists x.\,\forall y.\,x \le y)}\ \text{Imp I}$$

Example of Failure

Let's try to show

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

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

$$\begin{array}{l}\langle command\rangle \ ::= \ \langle variable\rangle := \langle term\rangle \\ \quad \mid \langle command\rangle;\ \ldots;\ \langle command\rangle \\ \quad \mid \mathit{if}\ \langle statement\rangle\ \mathit{then}\ \langle command\rangle\ \mathit{else}\ \langle command\rangle \\ \quad \mid \mathit{while}\ \langle statement\rangle\ \mathit{do}\ \langle command\rangle\end{array}$$

- 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 Assignment Rule

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

Example:

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

The Assignment Rule

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

Example:

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

The Assignment Rule

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

Example:

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

The Assignment 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

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

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

The Assignment Rule – Your Turn

- What is the weakest precondition of

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

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

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:

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

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

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

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?

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

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

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

Which Inferences Are Correct?

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

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

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

Which Inferences Are Correct?

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

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

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

Elsa L Gunter CS477 Formal Software Dev Methods February 21, 2018 35 / 35