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 6, 2013

First-Order Formulae

Given signature (V, F, af, R, ar), terms defined by

$$t ::= v \qquad v \in V$$
$$\mid \quad f(t_1, \ldots, t_n) \quad f \in F \text{ and } n = af(f)$$

Formulae defined by First-order formulae built from terms using relations, logical connectives, quantifiers:

$$\begin{array}{llll} form ::= \mathrm{true} & \mid & False & \\ \mid \ r(t_1, \ldots, t_n) & & & r \in R,\ t_i \text{ terms},\ n = ar(r) \\ \mid \ (form) & \mid & \neg form & \\ \mid \ form \wedge form & \mid & form \vee form & \\ \mid \ form \Rightarrow form & \mid & form \Leftrightarrow form & \\ \mid \ \forall v.form & \mid & \exists v.form & \end{array}$$

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 binding occurrence; occurrence not free, not binding is bound occurrence

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

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

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 *swaptxy* 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:

- $\text{true}[x \leftrightarrow y] = \text{true}$ $\quad$ $\text{false}[x \leftrightarrow y] = \text{false}$
- $r(t_1, \ldots, t_n)[x \leftrightarrow y] = r((t_1[x \leftrightarrow y], \ldots, t_n[x \leftrightarrow y]))$
- $(\psi)[x \leftrightarrow y] = (\psi[x \leftrightarrow y])$ $\quad$ $(\neg\psi)[x \leftrightarrow y] = \neg(\psi[x \leftrightarrow y])$
- $(\psi_1 \otimes \psi_2)[x \leftrightarrow y] = (\psi_1[x \leftrightarrow y]) \otimes (\psi_2[x \leftrightarrow y])$ 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 $\mathcal{Q} \in \{\forall, \exists\}$

Examples

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

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

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 $y \notin fvt$ then $\psi[x \leftrightarrow y] \equiv \psi$

$\Gamma \vdash \varphi AllE$