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 2, 2013

First Order Logic vs Propositional Logic

First Order Logic extends Propositional Logic with

- Non-boolean constant
- Variables
- Functions and relations (or predicates, more generally)
- Quantification of variables

Sample first order formula:

$$\forall x. \exists y. x < y \land y \le x + 1$$

Reference: Peled, *Software Reliability Methods*, Chapter 3

Signatures

Start with signature:

$$\mathcal{G} = (V, F, af, R, ar)$$

- V a countably infinite set of *variables*
- F finite set of function symbols
- $af : F \to \mathbb{N}$ gives the *arity*, the number of arguments for each function Constant c a function symbol of arity 0 ($af(c) = 0$)
- R finite set of relation symbols
- $ar : R \to \mathbb{N}$, the arity for each relation symbol
  - Assumes $= \in R$ and $ar(=) = 2$

Terms over Signature

Terms t are expressions built over a signature (V, F, af, R, ar)

$$\begin{array}{lll} t ::= v & & v \in V \\ \mid & f(t_1, \ldots, t_n) & f \in F \text{ and } n = af(f) \end{array}$$

- **Example**: $add(1, abs(x))$ where $add, abs, 1 \in F;\ x \in V$
- For constant c write c instead of $c(\,)$
- Will write $s = t$ instead of $=(s, t)$
  - Similarly for other common infixes (*e.g.* $+, -, *, <, \le, \ldots$)

Structures

Meaning of terms starts with a structure:

$$\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$$

where

- $\mathcal{G} = (V, F, af, R, ar)$ a signature,
- $\mathcal{D}$ and *domain* on interpretation
- $\mathcal{F}$ set of functions over $\mathcal{D}$; $\mathcal{F} \bigcup_{n \ge 0} \mathcal{D}^n \to \mathcal{D}$
  - **Note:** $\mathcal{F}$ can contain elements of $\mathcal{D}$ since $\mathcal{D} = (\mathcal{D}^0 \to \mathcal{D})$
- $\phi : F \to \mathcal{F}$ where if $\phi(f) \in (\mathcal{D}^n \to \mathcal{D})$ then $n = af(f)$
- $\mathcal{R}$ set of relations over $\mathcal{D}$; $\mathcal{R} \subseteq \bigcup_{n \ge 1} \mathcal{P}(\mathcal{D}^n)$
- $\rho : R \to \mathcal{R}$ where if $\rho(r) \subseteq \mathcal{D}^n$ then $n = ar(r)$

Assignments

V set of variables, $\mathcal{D}$ domain of interpretation
An assignment is a function $a : V \to \mathcal{D}$
Example:

$$V = \{w, x, y, z\}$$

$$a = \{w \mapsto 3.14, x \mapsto -2.75, y \mapsto 13.9, z \mapsto -25.3\}$$

- Assignment is a fixed association of values to variables; not “update-able”

Interpretation of Terms

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{T}_a$ of a term t is defined by structural induction on terms:

- $\mathcal{T}_a(v) = a(v)$ for $v \in V$
- $\mathcal{T}_a(f(t_1, \ldots, t_n)) = \phi(f)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}_a(t_n))$

Example of Interpretation

- $V = \{w, x, y, z\}$, $\mathcal{D} = \mathbb{R}$
- $1, add, abs \in F$, constant 1, and functions (in $\mathcal{F}$) for addition and absolute value respectively
- $a = \{w \mapsto 3.14, x \mapsto -2.75, y \mapsto 13.9, z \mapsto -25.3\}$

$$\begin{aligned}
\mathcal{T}_a(add(1, abs(x))) &= (\mathcal{T}_a(1)) + (\mathcal{T}_a(abs(x))) \\
&= 1.0 + (\mathcal{T}_a(abs(x))) \\
&= 1.0 + |\mathcal{T}_a(x)| \\
&= 1.0 + |a(x)| \\
&= 1.0 + |-2.75| \\
&= 1.0 + 2.75 \\
&= 3.75
\end{aligned}$$

First-Order Formulae

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

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

Note: Scope of quantifiers as far to right as possible

$$\begin{aligned}
\forall x.(x > y) \wedge (2 > x) \text{ same as } &\ \forall x.(x > y) \wedge (2 > x) \\
\text{not same as } &\ (\forall x.(x > y)) \wedge (2 > x)
\end{aligned}$$

Subformulae

- A subformula of formula ψ is a formula the occurs in ψ
  - More rigorous definition by structural induction on formulae
  - ψ subformula of ψ
  - Use proper subformula to exclude ψ
- Write $\bigwedge_{i=1,\ldots,n} \psi_i$ for $\psi_1 \wedge \ldots \wedge \psi_n$
  - ψ_i called a conjunct
- Write $\bigvee_{i=1,\ldots,n} \psi_i$ for $\psi_1 \vee \ldots \vee \psi_n$
  - ψ_i called a disjunct

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\mathrm{true}) = \mathbf{T}$ $\qquad \mathcal{M}_a(\mathrm{false}) = \mathbf{F}$

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$
- $\mathcal{M}_a((\psi)) = \mathcal{M}_a(\psi)$

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$
- $\mathcal{M}_a((\psi)) = \mathcal{M}_a(\psi)$
- $\mathcal{M}_a(\neg\psi) = \mathbf{T}$ if $\mathcal{M}_a(\psi) = \mathbf{F}$ and $\mathcal{M}_a(\neg\psi) = \mathbf{F}$ if $\mathcal{M}_a(\psi) = \mathbf{T}$

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$
- $\mathcal{M}_a((\psi)) = \mathcal{M}_a(\psi)$
- $\mathcal{M}_a(\neg\psi) = \mathbf{T}$ if $\mathcal{M}_a(\psi) = \mathbf{F}$ and $\mathcal{M}_a(\neg\psi) = \mathbf{F}$ if $\mathcal{M}_a(\psi) = \mathbf{T}$
- $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{T}$ and $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{F}$ otherwise

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$
- $\mathcal{M}_a((\psi)) = \mathcal{M}_a(\psi)$
- $\mathcal{M}_a(\neg\psi) = \mathbf{T}$ if $\mathcal{M}_a(\psi) = \mathbf{F}$ and $\mathcal{M}_a(\neg\psi) = \mathbf{F}$ if $\mathcal{M}_a(\psi) = \mathbf{T}$
- $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{T}$ and $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{F}$ otherwise
- $\mathcal{M}_a(\psi_1 \vee \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{T}$ or $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \vee \psi_2) = \mathbf{F}$ otherwise

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

For give assignment $a : V \to \mathcal{D}$, the interpretation $\mathcal{M}_a$ of a formula ψ assigning a value in $\{\mathbf{T}, \mathbf{F}\}$ is defined by structural induction on formulae:

- $\mathcal{M}_a(\text{true}) = \mathbf{T}$ $\quad\mathcal{M}_a(\text{false}) = \mathbf{F}$
- $\mathcal{M}_a(r(t_1, \ldots, t_n)) = \rho(r)(\mathcal{T}_a(t_1), \ldots, \mathcal{T}(t_n))$
- $\mathcal{M}_a((\psi)) = \mathcal{M}_a(\psi)$
- $\mathcal{M}_a(\neg\psi) = \mathbf{T}$ if $\mathcal{M}_a(\psi) = \mathbf{F}$ and $\mathcal{M}_a(\neg\psi) = \mathbf{F}$ if $\mathcal{M}_a(\psi) = \mathbf{T}$
- $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{T}$ and $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \wedge \psi_2) = \mathbf{F}$ otherwise
- $\mathcal{M}_a(\psi_1 \vee \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{T}$ or $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \vee \psi_2) = \mathbf{F}$ otherwise
- $\mathcal{M}_a(\psi_1 \Rightarrow \psi_2) = \mathbf{T}$ if $\mathcal{M}_a(\psi_1) = \mathbf{F}$ or $\mathcal{M}_a(\psi_2) = \mathbf{T}$, and $\mathcal{M}_a(\psi_1 \Rightarrow \psi_2) = \mathbf{F}$ otherwise

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

Let
$$a + [v \mapsto d](w) = \begin{cases} d & \text{if } w = v \\ a(w) & \text{if } w \neq v \end{cases}$$

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

Let
$$a + [v \mapsto d](w) = \begin{cases} d & \text{if } w = v \\ a(w) & \text{if } w \neq v \end{cases}$$

- $\mathcal{M}_a(\forall v.\psi) = \mathbf{T}$ if for every $d \in \mathcal{D}$ we have $\mathcal{M}_{a+[v\mapsto d]}(\psi) = \mathbf{T}$, and $\mathcal{M}_a(\forall v.\psi) = \mathbf{F}$ otherwise

Interpretation of Formulae

Fix structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

Let
$$a + [v \mapsto d](w) = \begin{cases} d & \text{if } w = v \\ a(w) & \text{if } w \neq v \end{cases}$$

- $\mathcal{M}_a(\forall v.\psi) = \mathbf{T}$ if for every $d \in \mathcal{D}$ we have $\mathcal{M}_{a+[v\mapsto d]}(\psi) = \mathbf{T}$, and $\mathcal{M}_a(\forall v.\psi) = \mathbf{F}$ otherwise
- $\mathcal{M}_a(\exists v.\psi) = \mathbf{T}$ if there exists $d \in \mathcal{D}$ such that $\mathcal{M}_{a+[v\mapsto d]}(\psi) = \mathbf{T}$, and $\mathcal{M}_a(\forall v.\psi) = \mathbf{F}$ otherwise

Modeling First-order Formulae

Given structure $\mathcal{S} = (\mathcal{G}, \mathcal{D}, \mathcal{F}, \phi, \mathcal{R}, \rho)$ where $\mathcal{G} = (V, F, af, R, ar)$

- $(\mathcal{S}, \mathcal{M})$ model for first-order language over signature $\mathcal{G}$
- Truth of formulae in language over signature $\mathcal{G}$ depends on structure $\mathcal{S}$
- Assignment a models ψ, or a satisfies ψ, or $a \models^{\mathcal{S}} \psi$ if $\mathcal{M}_a(\psi) = \mathbf{T}$
- ψ is valid for $\mathcal{S}$ if $a \models^{\mathcal{S}} \psi$ for some a.
- $\mathcal{S}$ is a model of ψ, written $\models^{\mathcal{S}} \psi$ if every assignment for $\mathcal{S}$ satisfies ψ.
- ψ is valid, or a tautology if ψ valid for every mode. Write $\models \psi$
- ψ_1 logically equivalent to ψ_2 if for all structures $\mathcal{S}$ and assignments a, $a \models^{\mathcal{S}} \psi_1$ iff $a \models^{\mathcal{S}} \psi_2$

Examples

- Assignment $\{x \mapsto 0\}$ satisfies $\exists y.x < y$ valid in interval $[0,\ 1]$; assignment $\{x \mapsto 1\}$ doesn't
- $\forall x.\exists y.x < y$ valid in $\mathbb{N}$ and $\mathbb{R}$, but not interval $[0,\ 1]$
- $(\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$ tautology
  - Why?

Sample Tautologies

All instances of propositional tautologies

Sample Tautologies

All instances of propositional tautologies

$$\models (\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$$

Sample Tautologies

All instances of propositional tautologies

$$\models (\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$$

$$\models ((\forall x.\forall y.\psi) \Leftrightarrow (\forall y.\forall x.\psi))$$

Sample Tautologies

All instances of propositional tautologies

$$\models (\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$$

$$\models ((\forall x.\forall y.\psi) \Leftrightarrow (\forall y.\forall x.\psi))$$

$$\models ((\forall x.\psi) \Rightarrow (\exists x.\psi))$$

Sample Tautologies

All instances of propositional tautologies

$$\models (\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$$

$$\models ((\forall x.\forall y.\psi) \Leftrightarrow (\forall y.\forall x.\psi))$$

$$\models ((\forall x.\psi) \Rightarrow (\exists x.\psi))$$

$$\models (\forall x.\psi_1 \wedge \psi_2) \Leftrightarrow ((\forall x.\psi_1) \wedge (\forall x.\psi_2))$$

Sample Tautologies

All instances of propositional tautologies

$$\models (\exists x.\forall y.(y \leq x)) \Rightarrow (\forall y.\exists x.(y \leq x))$$

$$\models ((\forall x.\forall y.\psi) \Leftrightarrow (\forall y.\forall x.\psi))$$

$$\models ((\forall x.\psi) \Rightarrow (\exists x.\psi))$$

$$\models (\forall x.\psi_1 \wedge \psi_2) \Leftrightarrow ((\forall x.\psi_1) \wedge (\forall x.\psi_2))$$

$$(\exists x.\psi_1 \wedge \psi_2) \Rightarrow ((\exists x.\psi_1) \wedge (\exists x.\psi_2))$$

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**: $fv(add(1, abs(x))) = \{x\}$