Formal Methods in software development

a.y.2017/2018

Prof. Anna Labella

The predicate calculus [H-R ch.2]

- The need for a richer language
- Terms and formulas
- quantifiers

Examples

- Every student preparing his homework must be left alone

$\forall x \, ((\varphi(x) \wedge \psi(x)) \rightarrow \chi(x))$

- For every natural number there is number greater than it

$\forall x \, (N(x) \rightarrow \exists y \, (N(y) \wedge G(y,x))$

$\forall x \, \exists y \, G(y,x)$

- There are people who do not like their dog

$\exists x \, \neg \varphi(x, d(x))$

Syntax

- Inductive term definition
- BNF

- $t ::= x \mid c \mid f(t_1, t_2, \ldots, t_n)$

Syntax

- Inductive definition of wff

- BNF

$\varphi ::= p(t_1,t_2,\ldots,t_n) \mid t_1=t_2 \mid (\neg\varphi) \mid (\varphi\wedge\varphi) \mid$
$(\varphi\vee\varphi) \mid (\varphi\rightarrow\varphi) \mid \forall x\varphi \mid \exists x\varphi$

Syntax

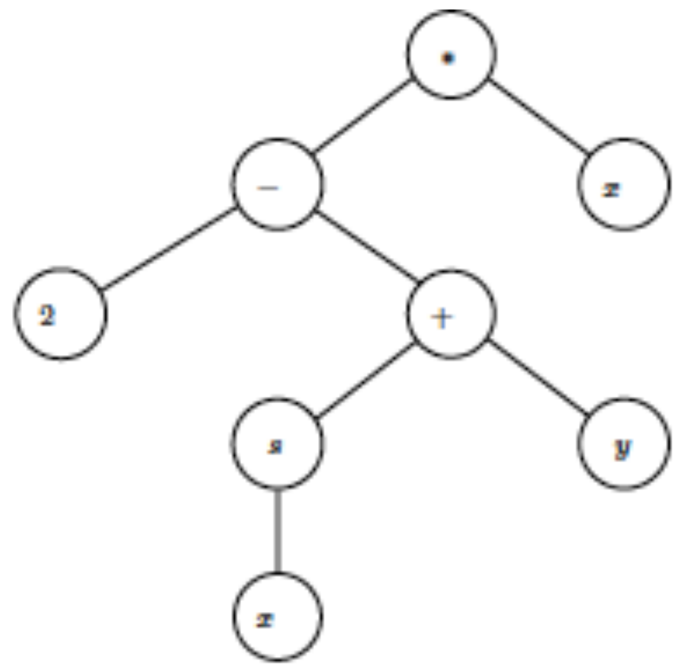
- One can always do without function symbols, using predicates and equality

- $f(x)=y$ is the same as

$$F(x,y) \wedge \forall z\, (F(x,z) \rightarrow y=z)$$

Peano's arithmetics

- Predicates: - = -, - ≤ -
- Functions : - + -, - · -, s(-),…
- Constants: 0



Exercises

Find appropriate predicates and their specification to translate the following into predicate logic:

(a) All red things are in the box.

(b) Only red things are in the box.

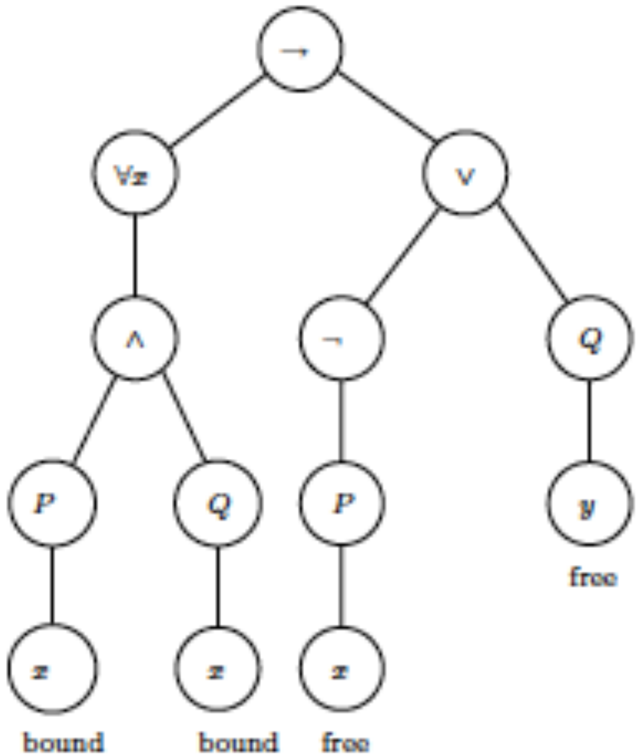
(c) No animal is both a cat and a dog.

(d) Every prize was won by a boy.

(e) A boy won every prize.

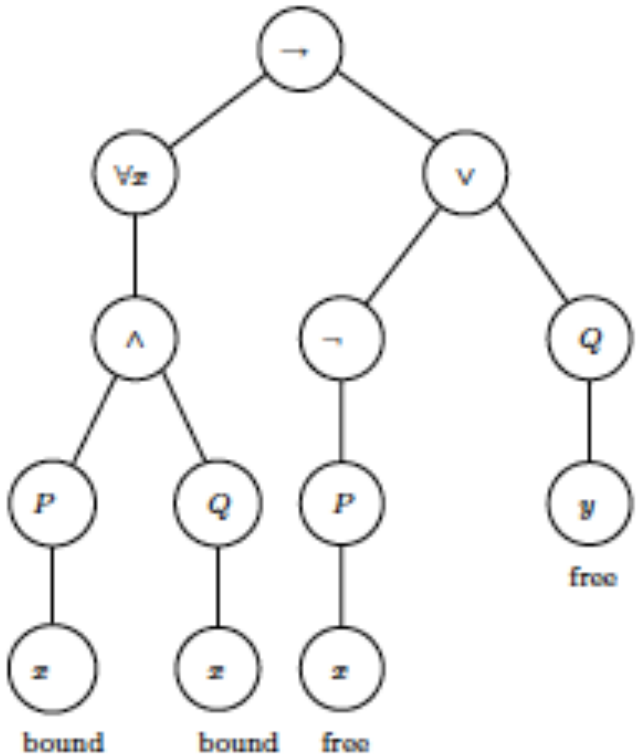
Syntax

Free and bounded variables



Syntax

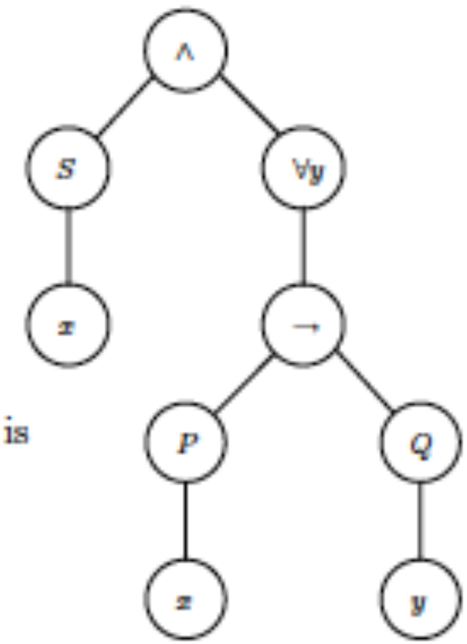
Open and closed formulas



Syntax

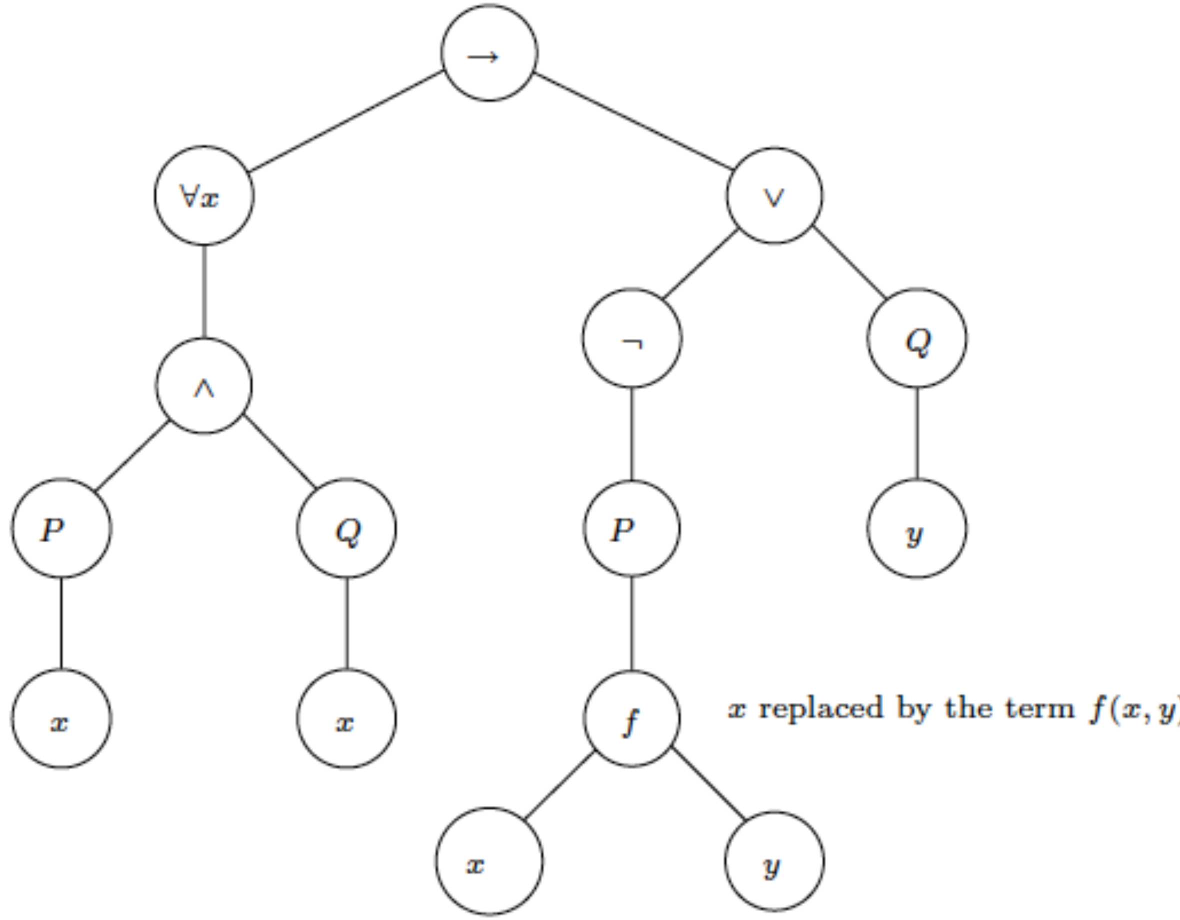
Free and bounded variables

the term $f(y, y)$ is not free for x in this formula



Syntax

Be careful with substitution!



Natural deduction 1

A special predicate: equality

=(-,-) or - = -

Natural deduction 2

Proof rules for equality

$$\frac{}{t = t} =\mathrm{i}$$

$$\frac{t_1 = t_2 \quad \phi[t_1/x]}{\phi[t_2/x]} =\mathrm{e}$$

Natural deduction 3

We can prove symmetry

$$t_1 = t_2 \vdash t_2 = t_1$$

1	$t_1 = t_2$	premise
2	$t_1 = t_1$	$=$i
3	$t_2 = t_1$	$=$e $1, 2$

Natural deduction 3

And also transitivity

$$t_1 = t_2,\ t_2 = t_3 \vdash t_1 = t_3$$

1	$t_2 = t_3$	premise
2	$t_1 = t_2$	premise
3	$t_1 = t_3$	$=$e $1, 2$

Exercises

Prove the validity of the following sequents using, among others, the rules $=$i and $=$e. Make sure that you indicate for each application of $=$e what the rule instances ϕ, t_1 and t_2 are.

(a) $(y = 0) \wedge (y = x) \vdash 0 = x$

(b) $t_1 = t_2 \vdash (t + t_2) = (t + t_1)$

(c) $(x = 0) \vee ((x + x) > 0) \vdash (y = (x + x)) \to ((y > 0) \vee (y = (0 + x)))$.

Natural deduction 1

Proof rules for universal quantification

$$\frac{\forall x\, \phi}{\phi[t/x]}\ \forall x\,\mathrm{e}.$$

where t is free for x in ϕ

$$\frac{\boxed{\begin{array}{l} x_0 \\ \qquad \vdots \\ \qquad \phi[x_0/x] \end{array}}}{\forall x\, \phi}\ \forall x\,\mathrm{i}.$$

where x_0 is a fresh variable

Natural deduction 2

Proof rules for existential quantification

$$\frac{\phi[t/x]}{\exists x \phi}\ \exists x\,\mathrm{i}$$

where t is free for x in ϕ

$$\frac{\exists x\,\phi \qquad \boxed{\begin{array}{c} x_0\ \phi[x_0/x] \\ \vdots \\ \chi \end{array}}}{\chi}\ \exists\mathrm{e}$$

where x_0 is a fresh variable

Examples of proofs

proof of the sequent $\forall x\,(P(x) \to Q(x)),\ \forall x\,P(x) \ \vdash\ \forall x\,Q(x)$:

1		$\forall x\,(P(x) \to Q(x))$	premise
2		$\forall x\,P(x)$	premise
3	x_0	$P(x_0) \to Q(x_0)$	$\forall x$ e 1
4		$P(x_0)$	$\forall x$ e 2
5		$Q(x_0)$	$\to$e 3, 4
6		$\forall x\,Q(x)$	$\forall x$ i 3–5

where x_0 is a fresh variable

Examples of proofs

$P(t), \forall x\,(P(x) \to \neg Q(x)) \vdash \neg Q(t)$ for any term t:

1	$P(t)$	premise
2	$\forall x\,(P(x) \to \neg Q(x))$	premise
3	$P(t) \to \neg Q(t)$	$\forall x\,\mathrm{e}\ 2$
4	$\neg Q(t)$	$\to\mathrm{e}\ 3, 1$

Exercises

(a) Find a (propositional) proof for $\phi \to (q_1 \wedge q_2) \vdash (\phi \to q_1) \wedge (\phi \to q_2)$.

(b) Find a (predicate) proof for $\phi \to \forall x\, Q(x) \vdash \forall x\, (\phi \to Q(x))$, provided that x is not free in ϕ.
(Hint: whenever you used $\wedge$ rules in the (propositional) proof of the previous item, use $\forall$ rules in the (predicate) proof.)

(c) Find a proof for $\forall x\, (P(x) \to Q(x)) \vdash \forall x\, P(x) \to \forall x\, Q(x)$.
(Hint: try $(p_1 \to q_1) \wedge (p_2 \to q_2) \vdash p_1 \wedge p_2 \to q_1 \wedge q_2$ first.)

Exercises

Consider the following boolean formulas. Compute their unique reduced OBDDs with respect to the ordering $[x, y, z]$. It is advisable to first compute a binary decision tree and then to perform the removal of redundancies.

(a) $f(x, y) \stackrel{\text{def}}{=} x \cdot y$
(b) $f(x, y) \stackrel{\text{def}}{=} x + y$
(c) $f(x, y) \stackrel{\text{def}}{=} x \oplus y$
(d) $f(x, y, z) \stackrel{\text{def}}{=} (x \oplus y) \cdot (\overline{x} + z)$.

Given the boolean formula $f(x_1, x_2, x_3) \stackrel{\text{def}}{=} x_1 \cdot (x_2 + \overline{x_3})$, compute its reduced OBDD for the following orderings:

(a) $[x_1, x_2, x_3]$
(b) $[x_3, x_1, x_2]$
(c) $[x_3, x_2, x_1]$.