Mathematics for Computer Science

José Proença & Alexandre Madeira
(slides from Luis Soares Barbosa)

HASLab
HIGH-ASSURANCE SOFTWARE LABORATORY
INESCTEC

Universidade do Minho

Predicate calculus
September-October, 2017

Introduction

Predicate, or first order logic is an extension of propositional logic that allows the use of variables of types other than Boolean.

A formula is a Boolean expression in which some Boolean variables may have been replaced by:

- Predicates, which are relations whose arguments may be of arbitrary types. The relation names (e.g. equal, less) are called predicate symbols. Infix notation is sometimes used for predicates, as in $x \leq y$.
- Universal and existential quantification

Examples

Types

… as formalization of the domains of discourse

- Examples: $x : \boldsymbol{N}$, $p : \mathrm{B}$, table : $Att_1 \times Att_2 \times Att_3$
- Place additional restrictions on the definition of textual substitution (in $E[x := F]$ x and F must have the same type) and equality.
- Main issue in programming languages: from untyped to strongly typed languages (in which a type is assigned to each expression by syntactic rules)
- overloading, polymorphism and subtyping

Quantification

$$\forall_{x:\boldsymbol{N}} \,.\, \text{even}(x) \Rightarrow \text{odd}(x+1)$$

or

$$\exists_{x:\boldsymbol{N}} \,.\, (12 < x \leq 999) \Rightarrow \text{prime}(x)$$

or

$$\forall_{x:\boldsymbol{N}} \,.\, (\exists_{y:\boldsymbol{N}} \,.\, (y \geq 2 \wedge y \neq x) \Rightarrow (x \ mod \ y = 0)) \Rightarrow \neg\text{prime}(x)$$

- free variables and substitution!

Quantification

A handier notation

$$\langle \forall\, x{:}\boldsymbol{N} \;:\; \mathrm{even}(x) \;:\; \mathrm{odd}(x+1) \rangle$$

or

$$\langle \exists\, x{:}\boldsymbol{N} \;:\; 12 < x \leq 999 \;:\; \mathrm{prime}(x) \rangle$$

or

$$\langle \forall\, x{:}\boldsymbol{N} \;:\; \langle \exists\, y{:}\boldsymbol{N} \;:\; y \geq 2 \wedge y \neq x \;:\; \mathrm{rem}(x,y) = 0 \rangle \;:\; \neg\mathrm{prime}(x) \rangle$$

Syntax

$$E \;:=\; \textsc{True} \mid \textsc{False} \mid v \mid \ldots \mid \langle \Theta\, x{:}X \;:\; E \;:\; E \rangle \mid \mathit{pred}(\overline{E})$$

where $\Theta \in \{\forall, \exists\}$, X belongs to a set of domains of discourse, and $\mathit{pred}(\overline{E})$ are predicates applied to expressions.

Axioms for Predicate Calculus

Let $(\Theta = \forall$ and $\theta = \wedge)$ or $(\Theta = \exists$ and $\theta = \vee)$

$$
\begin{array}{rl}
\text{(one point)} & \langle \Theta\, x{:}X \,:\, x = E \,:\, P \rangle = P[x := E] \\
\text{(distributivity)} & \langle \Theta\, x{:}X \,:\, R \,:\, P \rangle \,\theta\, \langle \Theta\, x{:}X \,:\, R \,:\, Q \rangle = \\
 & \qquad \langle \Theta\, x{:}X \,:\, R \,:\, P \,\theta\, Q \rangle \\
\text{(range split)} & \langle \Theta\, x{:}X \,:\, R \vee S \,:\, P \rangle = \\
 & \qquad \langle \Theta\, x{:}X \,:\, R \,:\, P \rangle \,\theta\, \langle \Theta\, x{:}X \,:\, S \,:\, P \rangle \\
\text{(interchange)} & \langle \Theta\, x{:}X \,:\, R \,:\, \langle \Theta\, y{:}Y \,:\, Q \,:\, P \rangle \rangle = \\
 & \qquad \langle \Theta\, y{:}Y \,:\, Q \,:\, \langle \Theta\, x{:}X \,:\, R \,:\, P \rangle \rangle \\
\text{(nesting)} & \langle \Theta\, x{:}X, y{:}Y \,:\, R \wedge Q \,:\, P \rangle = \\
 & \qquad \langle \Theta\, x{:}X \,:\, R \,:\, \langle \Theta\, y{:}Y \,:\, Q \,:\, P \rangle \rangle
\end{array}
$$

Some rules for $\forall$ and $\exists$

$$
\begin{aligned}
\text{(empty range-}\exists\text{)} \quad & \langle \exists\, x{:}X \;:\; \textsc{False} \;:\; P \rangle = \textsc{False} \\
\text{(empty range-}\forall\text{)} \quad & \langle \forall\, x{:}X \;:\; \textsc{False} \;:\; P \rangle = \textsc{True} \\
\text{(trading)} \quad & \langle \forall\, x{:}X \;:\; R \;:\; P \rangle = \langle \forall\, x{:}X \;::\; R \Rightarrow P \rangle \\
(\vee \text{ dist over } \forall) \quad & P \vee \langle \forall\, x{:}X \;:\; R \;:\; Q \rangle = \langle \forall\, x{:}X \;:\; R \;:\; P \vee Q \rangle \\
\text{(de Morgan)} \quad & \langle \exists\, x{:}X \;:\; R \;:\; \neg P \rangle = \neg \langle \forall\, x{:}X \;:\; R \;:\; P \rangle
\end{aligned}
$$

Recall de Morgan laws from propositional calculus:

$$\neg(p \wedge q) \equiv (\neg p \vee \neg q)$$

and

$$\neg(p \vee q) \equiv (\neg p \wedge \neg q)$$

Predicate calculus and theories

- The pure predicate calculus includes the axioms of propositional calculus, together with the axioms for quantifications
- The inference rules are Substitution, Transitivity, Leibniz and its variant for quantification
- In the pure predicate calculus, the relation symbols are uninterpreted (except for equality), so the logic provides no specific rules for manipulating them.
- With these symbols uninterpreted, we can develop general rules for manipulation that are sound no matter what meanings we ascribe to the function symbols. Thus, the pure predicate calculus is sound in all domains that may be of interest.

Predicate calculus and theories

Adding axioms that give meanings to some of the (uninterpreted) relational symbols gives rise to a theory

- The theory of integers (with $+, -, *, \leq$, etc and the usual axioms)
- The theory of sets (with $\cup, \cap, \in, \subseteq$, etc and the usual axioms)

Modelling

- Modelling a statement in the propositional calculus requires associating boolean variables with the subpropositions of the statement.
- Modelling a statement in the predicate calculus requires defining predicate symbols and other functions to capture relationships between variables.

Examples

- *Every student took one mathematics class and passed one programming*
- *Every student who passed a mathematics class with grade 15 or higher got a diploma of merit*

Modelling exercises[1]

Let P be the set of all planets, $earth(x)$ mean "x is an earth-like planet.", and $life(x)$ mean "x supports life."
What is the correct interpretation of each of the following?

1. $\langle \forall\, x{:}P \;:\; life(x) \;:\; earth(x) \rangle$
2. $\langle \forall\, x{:}P \;::\; earth(x) \rangle \vee \langle \forall\, x{:}P \;::\; life(x) \rangle$
3. $\langle \forall\, x{:}P \;::\; earth(x) \vee \; earth(x) \rangle$
4. $\langle \forall\, x{:}P \;::\; earth(x) \rangle \vee \langle \forall\, x{:}P \;::\; earth(x) \rangle$
5. $\neg \langle \forall\, x{:}P \;::\; earth(x) \vee life(x) \rangle$

[1] from `https://www.zweigmedia.com/RealWorld/logic/logic7.html`

Modelling exercises

- All men are mortal. Socrates is a man. Therefore, Socrates is mortal.
- For all numbers x, if x is greater than 1, then x is greater than 0.
- The square of every negative integer is positive.
- Not every integer is positive.
- No positive integer is negative.
- All integers are positive or no integers are positive.

Modelling exercises

Let P be the set of all planets, A the set of all astronauts, and $travel(x, y)$ mean "x will travel to y".

- Every astronaut will travel to at least one planet.
- Some astronauts will travel to every planet.
- Other astronauts will travel to no planets.
- $\langle \forall\, y{:}P :: \langle \exists\, x{:}A :: travel(x, y) \rangle\rangle$
- $\langle \forall\, y{:}P :: \langle \exists\, x{:}A :: \neg travel(x, y) \rangle\rangle$

Going generic

$$\langle \Sigma\, i{:}\mathbb{N} \;:\; 1 < i < 100 \;:\; i^2 \rangle$$

vs

$$\Sigma_{i=1}^{100}\, i^2$$

In general

$$\langle \Theta\, x : X \;:\; R \;:\; P \rangle$$

to express: apply θ to the values P computed for all x in X satisfying R, providing P is of type M and (M, θ, u) forms an Abelian monoid.

Universal and existential quantification

- $\forall$ is generalised conjunction: $(\mathsf{B}, \wedge, \textsc{True})$ forms a monoid.
- $\exists$ is generalised disjunction: $(\mathsf{B}, \vee, \textsc{False})$ forms a monoid.

Distributed operations Θ

Every binary, commutative operation θ defined on a monoid (i.e. associative and with an identity element) can be extended to a distributed (or reduced) operation Θ acting on a set.

Examples

- $(\mathsf{B}, \wedge, \textsc{True})$
- $(\mathsf{B}, \vee, \textsc{False})$
- $(\boldsymbol{N}, +, 0)$
- $(\boldsymbol{N}, *, 1)$
- $(\mathcal{P}(X), \cup, \emptyset)$

Going generic

Some general rules for (M, θ, u)

$$
\begin{aligned}
\text{(empty range)} \quad & \langle \Theta\, x{:}X \;:\; \textsc{False} \;:\; P \rangle = u \\
\text{(one point)} \quad & \langle \Theta\, x{:}X \;:\; x = E \;:\; P \rangle = P[x{:}= E] \\
\text{(distributivity)} \quad & \langle \Theta\, x{:}X \;:\; R \;:\; P \rangle \,\theta\, \langle \Theta\, x{:}X \;:\; R \;:\; Q \rangle = \\
& \qquad \langle \Theta\, x{:}X \;:\; R \;:\; P \theta Q \rangle \\
\text{(range split)} \quad & \langle \Theta\, x{:}X \;:\; R \vee S \;:\; P \rangle = \\
& \qquad \langle \Theta\, x{:}X \;:\; R \;:\; P \rangle \,\theta\, \langle \Theta\, x{:}X \;:\; S \;:\; P \rangle \\
\text{(interchange)} \quad & \langle \Theta\, x{:}X \;:\; R \;:\; \langle \Theta\, y : Y \;:\; Q \;:\; P \rangle \rangle = \\
& \qquad \langle \Theta\, y : Y \;:\; Q \;:\; \langle \Theta\, x{:}X \;:\; R \;:\; P \rangle \rangle \\
\text{(nesting)} \quad & \langle \Theta\, x{:}X, y{:}Y \;:\; R \wedge Q \;:\; P \rangle = \\
& \qquad \langle \Theta\, x{:}X \;:\; R \;:\; \langle \Theta\, y{:}Y \;:\; Q \;:\; P \rangle \rangle
\end{aligned}
$$