Expressiveness of predicate logic

Predicate logic is much more expressive than propositional logic, having predicate and function symbols, as well as quantifiers. This expressivess comes at the cost of making validity, satisfiability and provability undecidable. The good news, though, is that checking formulas on models is practical; SQL queries over relational databases or XQueries over XML documents are examples of this in practice. Software models, design standards, and execution models of hardware or programs often are described in terms of directed graphs. Such models M are interpretations of a two-argument predicate symbol R over a concrete set A of 'states.'

Given a set of states A = {s0, s1, s2, s3}, let RM be the set {(s0, s1),(s1, s0),(s1, s1),(s1, s2),(s2, s0),(s3, s0),(s3, s2)}.

The validation of many applications requires to show that a 'bad' state cannot be reached from a 'good' state. What 'good' and 'bad' mean will depend on the context. For example, a good state may be one in which an integer expression, say $x * (y - 1)$, evaluates to a value that serves as a safe index into an array a of length 10. A bad state would then be one in which this integer expression evaluates to an unsafe value, say 11, causing an 'outof-bounds exception.' In its essence, deciding whether from a good state one can reach a bad state is the reachability problem in directed graphs.

Existential second-order logic

If predicate logic cannot express reachability in graphs, then what can, and at what cost? We seek an extension of predicate logic that can specify such important properties, rather than inventing an entirely new syntax, semantics and proof theory from scratch. This can be realized by applying quantifiers not only to variables, but also to predicate symbols. For a predicate symbol P with $n \geq 1$ arguments, consider formulas of the form

$$\exists P\, \phi \tag{2.11}$$

where ϕ is a formula of predicate logic in which P occurs. Formulas of that form are the ones of *existential second-order logic*. An example of arity 2 is

$$\exists P \forall x \forall y \forall z\, (C_1 \wedge C_2 \wedge C_3 \wedge C_4) \tag{2.12}$$

where each C_i is a Horn clause[4]

$$\begin{aligned} C_1 &\stackrel{\text{def}}{=} P(x, x) \\ C_2 &\stackrel{\text{def}}{=} P(x, y) \wedge P(y, z) \rightarrow P(x, z) \\ C_3 &\stackrel{\text{def}}{=} P(u, v) \rightarrow \bot \\ C_4 &\stackrel{\text{def}}{=} R(x, y) \rightarrow P(x, y). \end{aligned}$$

If we think of R and P as two transition relations on a set of states, then C4 says that any R-edge is also a P-edge, C1 states that P is reflexive, C2 specifies that P is transitive, and C3 ensures that there is no P-path from the node associated to u to the node associated to v. Given a model M with

interpretations for all function and predicate symbols of φ in (2.11), except P, let MT be that same model augmented with an interpretation $T \subseteq A \times A$ of P, i.e. PMT = T. For any look-up table l, the semantics of $\exists P\, \varphi$ is then $M\, l \exists P\, \varphi$ iff for some $T \subseteq A \times A$, $MT\, l\, \varphi$.