Logics for Mobility

Luca Cardelli

Microsoft Research, Cambridge

Abstract

The ambient calculus is a process calculus based on mobility, where processes reside at the nodes of a dynamic hierarchy of locations. It becomes natural to discuss properties that hold at particular locations, and to discuss the dynamic evolution of the hierarchy of locations. We use a logic as a way of formalizing such descriptions.

We describe a modal logic for the ambient calculus, whose main novelty is the introduction of spatial connectives (in addition to standard and temporal connectives). Our logic can be used for specifying mobility protocols, for expressing mobility policies, and as a playground for model checking of mobile computation, with potential applications to bytecode verification of mobile code. Mobility properties of varying degrees of difficultly can be established and checked by typechecking, by model checking, or by proof search (as in proof-carrying code). In our latest development, we have extended our logic to describe systems including hidden and secret locations.