Verification of Parallel Programs with the Owicki-Gries and Rely-Guarantee Methods in Isabelle/HOL

Leonor Prensa Nieto
Technische Universität München, Institität für Informatik
`http://www.in.tum.de/~prensani`

November 23, 2001

In this talk I would like to present the work of my PhD thesis. This thesis presents the first formalization of the Owicki-Gries method and its compositional version, the rely-guarantee method, in a theorem prover. These methods are widely used for correctness proofs of parallel imperative programs with shared variables. The syntax, semantics and proof rules for a simple while-language extended with parallelism and synchronization are defined in Isabelle/HOL, which is the instantiation of higher-order logic in the theorem prover Isabelle. The original systems as found in the literature were designed for verification of parallel programs with a fixed number of components. We formalized the proof rules such that they also provide for programs parameterized in the number of parallel components. Their correctness w.r.t. the semantics is proven mechanically and the completeness proofs for both methods are extended to the new case of parameterized programs.

The availability of a theorem prover is advantageous because it enables us to verify programs with infinite state spaces and highly expressive specifications. A disadvantage is that the verification process is, in general, not fully automatic. However, it can be partially automated by defining a tactic for the generation of verification conditions based on the proof rules. Using this tactic we have verified several non-trivial examples for parameterized and non-parameterized programs. The most involved examples are two garbage-collection algorithms, the second one parametric in the number of mutators.