Experiments in Verifying Low Level Concurrent C Code

Wolfram Schulte
(schulte@microsoft.com)

Abstract

The Verified C project adds design by contract programming to C. The program verifier VCC accepts annotated C programs, generates logical verification conditions from them and passes them on to an automatic theorem prover to either prove the correctness of the program or find errors in it. VCC is build to verify the functional correctness of Microsoft's hypervisor code base. The first step in developing VCC so far has been the efficient encoding of a faithful memory model. The next step is the development of a programming methodology which allows for automatic verification of annotated low level concurrent code. In this talk, I will report on the design of VCC, and on first experiments in applying it.