From C to Infinity and Back: Unbounded Auto-active Verification with VCC

Michał Moskal

Microsoft Research Redmond
michal.moskal@microsoft.com

Abstract. In this tutorial I'll show how to prove deep functional properties of tricky sequential and concurrent C programs using VCC. I'll get into induction, termination, algebraic data types, infinite maps, and lemmas, all unified as ghost data and C-like code manipulating it. Once these are provided, verification is automatic, but the development process of such annotations tends to be very interactive, thus "auto-active verification" using C as a proof language.

VCC [1] is an industrial-strength verification environment for low-level concurrent systems code written in C. VCC takes a program (annotated with function contracts, state assertions, and type invariants) and attempts to prove the correctness of these annotations. VCC's verification methodology [3] allows global two-state invariants that restrict update of shared state and enforces simple, semantic conditions sufficient for checking those global invariants modularly. VCC works by translating C, via the Boogie intermediate verification language, to verification conditions handled by the Z3 SMT solver.

The environment includes tools for monitoring proof attempts and constructing partial counterexample executions for failed proofs and has been used to verify functional correctness of tens of thousands of lines of Microsoft's Hyper-V virtualization platform and of SYSGO's embedded real-time operating system PikeOS.

VCC is available with sources for non-commercial use at `http://vcc.codeplex.com/`, and online at `http://rise4fun.com/Vcc`. A tutorial [2] is also provided.

References

1. Cohen, E., Dahlweid, M., Hillebrand, M., Leinenbach, D., Moskal, M., Santen, T., Schulte, W., Tobies, S.: VCC: A Practical System for Verifying Concurrent C. In: Berghofer, S., Nipkow, T., Urban, C., Wenzel, M. (eds.) TPHOLs 2009. LNCS, vol. 5674, pp. 23–42. Springer, Heidelberg (2009)
2. Cohen, E., Hillebrand, M.A., Moskal, M., Schulte, W., Tobies, S.: Verifying C programs: A VCC tutorial. Working Draft, `http://vcc.codeplex.com/`
3. Cohen, E., Moskal, M., Schulte, W., Tobies, S.: Local Verification of Global Invariants in Concurrent Programs. In: Touili, T., Cook, B., Jackson, P. (eds.) CAV 2010. LNCS, vol. 6174, pp. 480–494. Springer, Heidelberg (2010)

P. Madhusudan and S.A. Seshia (Eds.): CAV 2012, LNCS 7358, p. 6, 2012.