Comparing Specification with Proved Properties of Clean Dynamics[1]

László Lövei, Máté Tejfel, Mónika Mészáros, Zoltán Horváth, and Tamás Kozsik

Clean dynamics can be used for implementing mobile code in a functional programming language. Dynamics are type safe, but other semantical properties are not checked before application of the dynamically linked code in the consumer. A language for expressing semantical requirements and an algorithm for comparing requirements with proven properties of the dynamics are presented in the current paper. Sparkle, the dedicated theorem prover of Clean is extended for dealing with open specifications. The properties of the consumer application can be proved based on the requirements are satisfied by the dynamics. New kinds of propositions and tactics are introduced in the paper for dealing with such proofs. The applicability of the new concepts and tools are demonstrated by a running example. The model of comparing properties with requirements is designed in language independent way, so the results may be applicaple for Erlang and other functional languages supporting dynamic code loading.

References

[1] K.M. Chandy and J. Misra. Parallel program design: a foundation. *Addison-Wesley*, 1989.

[2] Z. Horváth, P. Achten, T. Kozsik, and R. Plasmeijer. Verification of the Temporal Properties of Dynamic Clean Processes. *Proceedings of Implementation of Functional Languages, IFL'99*, Lochem, The Netherlands, Sept. 7–10, 1999. pp. 203–218.

[3] M. de Mol, M. van Eekelen, and R. Plasmeijer. Theorem Proving for Functional Programmers, *Sparkle: A Functional Theorem Prover*, Springer Verlag, LNCS 2312, p. 55 ff., 2001.

[4] Z. Horváth, T. Kozsik, and M. Tejfel. Extending the Sparkle Core language with object abstraction. *Acta Cybernetica* 17 (2005), pp. 419-445.

[5] Z. Horváth, T. Kozsik, and M. Tejfel. Proving Invariants of Functional Programs. *Proceedings of Eighth Symposium on Programming Languages and Software Tools*, Kuopio, Finland, June 17-18, 2003., pp. 115-126

[6] Z. Horváth, T. Kozsik, and M. Tejfel. Verifying invariants of abstract functional objects—a case study. *6th International Conference on Applied Informatics*, Eger, Hungary January 27-31 2004.

[1]Supported by the Hungarian National Science Research Grant (OTKA), Grant Nr.T037742., by Bolyai Research Scholarship and by ELTE CNL Lab.