Backward Refinement for Verifying Distributed Algorithms

K. Sere*   M. Waldén**

We present a new verification method for distributed algorithms. The basic idea is that an algorithm to be verified is stepwise transformed into a high level specification through a number of correctness-preserving steps. At each step some mechanism of the algorithm is identified and abstracted away while the basic computation in the original algorithm is preserved. In this way the algorithm becomes more coarse-grained. Only the essential parts of the algorithm are then left for final verification.

The method is formalized within the *refinement calculus* [1] using *superposition refinement* [2] in a backward direction.

The idea is as follows. We verify an algorithm through a number of backward refinement steps. Each step can be verified within the refinement calculus using the superposition refinement rule. The correctness of the final algorithm is then easily verified, thereby establishing the correctness of the original algorithm. An extensive case study is described in [4]. An additional contribution of the backward refinement method is that the algorithm will be described as consisting of some basic computation and a number of mechanisms added on top of this.

Our method is closely related to the reduction method of Lipton [3]. In contrast to Lipton, the method presented here is based on a formal calculus, the refinement calculus, for reasoning about programs. The main purpose of the refinement calculus is to provide a basis for the stepwise refinement approach to program construction. Our work shows how this calculus can be used to verify an algorithm.

References

[1] R. J. R. Back. *On the correctness of refinement in program development.* Ph.D. thesis, Report A-1978-4, Department of computer science, University of Helsinki, Finland, 1978.

[2] R. J. R. Back and K. Sere. *Superposition refinement of Reactive Systems.* Series A–144, Reports on Computer Science and Mathematics, Åbo Akademi University, Finland, 1993.

[3] R. J. Lipton. Reduction: A Method of Proving Properties of Parallel Programs. *Communications of th ACM 18*, No 12, pages 717–721, 1975.

[4] K. Sere and M. Waldén. *Verification of a Distributed Algorithm due to Chu.* Manuscript, Department of Computer Science, Åbo Akademi University, Turku, Finland, 1994. Abstract presented at the 13th Symposium on Principles of Distributed Computing (PODC'94), Los Angeles, USA.

*University of Kuopio, Department of Computer Science and Applied Mathematics, P.O.Box 1627, SF-70211 Kuopio, Finland, e-mail: Kaisa.Sere@uku.fi

**Åbo Akademi University, Department of Computer Science, SF-20520 Turku, Finland, e-mail: mwalden@abo.fi