Abstraction–Aided Verification

Amir Pnueli
New York University and the Weizmann Institute of Science

There are two prevalent methods for verifying reactive systems: Dedutive Verification which can be applied to arbitrary (including infinite–state) systems, but requires user ingenuity and supervision, and Algorithmic Verification (model checking) which is fully automatic but is restricted to finite–state (and not too big) systems. An effective and promising approach which combines the advantages of these two methods is obtained by finitary abstraction which proposes various tchniques for abstracting infinite– state systems into finite–state ones. In these lectures we will review the general approach and present some of these techniques. We will emphasize techniques which support verification of liveness properties in addition to safety properties. The plan of the talks includes the following topics:

- The general theory of abstraction–aided verification – soundness and completeness [6],[5].
- The method of Network Invariants [7],[4].
- Deductive verification and the method of Invisible Invariants [8], [1].
- Verification of liveness properties by invisible arnking functions [3], [2].
- Counter Abstraction for safety and liveness [9].
- Predicate abstraction for shape analysis.

References

[1] T. Arons, A. Pnueli, S. Ruah, J. Xu, and L. Zuck. Parameterized verification with automatically computed inductive assertions. In Proc. 13 rd Intl. Conference on Computer Aided Verification (CAV'01), volume 2102 of Lect.Notes in Comp.Sci., Springer–Verlag, pages 221–234, 2001.

[2] Y. Fang, N. Piterman, A. Pnueli, and L. Zuck. Liveness with incomprehensible ranking. In 10th Conf. on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'04), volume 2988 of Lect.Notes in Comp.Sci., pages 482–496. Springer–Verlag, 2004.

[3] Y. Fang, N. Piterman, A. Pnueli, and L. Zuck. Liveness with invisible ranking. In 5th VMCAI, volume 2937 of Lect.Notes in Comp.Sci., pp. 223–238. Springer–Verlag, 2004.

[4] Y. Kesten, N. Piterman, and A. Pnueli. Bridging the gap between fair simulation and trace inclusion. In Proc. 15 th Intl. Conference on Computer Aided Verification (CAV'03), volume 2775 of Lect.Notes in Comp.Sci., pages 381–393, Boulder, CO, USA, 2003. Springer–Verlag.

[5] Y. Kesten and A. Pnueli. Control and data abstractions: The cornerstones of practical formal verification. Software Tools for Technology Transfer, 4(2):328–342, 2000.

[6] Y. Kesten and A. Pnueli. Verification by finitary abstraction. Information and Compu– tation, a special issue on Compositionality, 163:203–243, 2000.

[7] Y. Kesten, A. Pnueli, E. Shahar, and L. D. Zuck. Network invariant in action. In 13th International Conference on Concurrency Theory (CONCUR02), volume 2421 of Lect.Notes in Comp.Sci., pages 101–115. Springer–Verlag, 2002.

[8] A. Pnueli, S. Ruah, and L. Zuck. Automatic deductive verification with invisible invari– ants. In Proc. 7 th Intl. Conference on Tools and Algorithms for the Construction and Analysis of Systems (TACAS'01), volume 2031, pages 82–97, 2001.

[9] A. Pnueli, J. Xu, and L. Zuck. Liveness with (0, 1, ∞)–counter abstraction. In E. Brinksma and K.G. Larsen, editors, Proc. 14 th Intl. Conference on Computer Aided Ver– ification (CAV'02), volume 2404 of Lect.Notes in Comp.Sci., Springer–Verlag, pp. 107–122, 2002.