VERIFICATION METHODS BASED ON PROPOSITIONAL LOGIC SATISFIABILITY

Keijo Heljanko

Helsinki University of Technology (TKK)
Laboratory for Theoretical Computer Science
P.O. Box 5400, FI-02015 TKK, Finland
email: Keijo.Heljanko@tkk.fi

Computer aided verification is an approach that uses computerized algorithms to automatically search for design errors (bugs) in system designs such as complex microprocessors, safety critical control systems, and communication protocol implementations. In all these fields we build a mathematical model of the set of all behaviors the analyzed system has, and then check this model against the required design specifications expressed using e.g., linear temporal logic (LTL).

We report on a number of new techniques to make model checking more efficient for large systems. The approaches are based on mapping the temporal logic model checking problems into propositional logic satisfiability (SAT) problem [3, 2, 1], benefiting from recent advances in SAT solving technology.

The results have been done in collaboration with authors listed in the references below.

References

[1] A. Biere, K. Heljanko, T. Junttila, T. Latvala, and V. Schuppan. Linear encodings of bounded LTL model checking. *Logical Methods in Computer Science*, 2(5:5), 2006. (doi: 10.2168/LMCS-2(5:5)2006).

[2] K. Heljanko, T. A. Junttila, M. Keinänen, M. Lange, and T. Latvala. Bounded model checking for weak alternating Büchi automata. In T. Ball and R. B. Jones, editors, *CAV*, volume 4144 of *Lecture Notes in Computer Science*, pages 95–108. Springer, 2006.

[3] K. Heljanko, T. A. Junttila, and T. Latvala. Incremental and complete bounded model checking for full PLTL. In K. Etessami and S. K. Rajamani, editors, *CAV*, volume 3576 of *Lecture Notes in Computer Science*, pages 98–111. Springer, 2005.