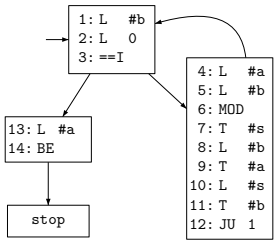
RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

CHAIR OF
COMPUTER SCIENCE 2
SOFTWARE MODELING
AND VERIFICATION
(MOVES)

— Master's Thesis —

Control flow automaton based bounded model checking



What is it all about?

Correctness of software has always been a major concern for developers. While in some domains a system failure might only annoy the user, there are also certain domains, where failures may entail high economical cost or even pose a danger to life. In the latter domains failures are intolerable and ensuring safety is the most crucial goal. The formal verification of software promises to mitigate those risks by ensuring the absence of logical errors in the program. In particular, model checking is a famous push-button approach for analyzing a system model against a logical specification. However, its applicability is severely hampered by the state-explosion problem, i.e. the exponential growth of the state space. To tackle this problem the approach of bounded model checking (BMC) [BCCZ99] takes the transition relation of the program and unrolls it up to a certain number of steps. While this abandons completeness, i.e. it does not prove the absence of errors, in practice BMC shows to be highly efficient in the presence of errors. To obtain the transition relation from a program, control flow automata have shown to be a highly efficient and versatile way for representing control and data flow [BCG+09]. The goal of this thesis is to develop a bounded model checking technique based on a control flow automaton and implement it in the existing model checking framework.

What is to be done?

1. Investigate encodings for bounded model checking based on control flow automata.
2. Implement all findings in the VPLC model checking framework written in F#.
3. Evaluate your implementation on case studies.

Requirements

- Solid background in theoretical computer science.
- Lectures on model checking.
- Some background in functional programming.

Contact

- Tim Lange, `tim.lange@cs.rwth-aachen.com`, Tel. 0241/80-21206, or
- Thomas Noll, `noll@cs.rwth-aachen.de`, Tel. 0241/80-21213

References

[BCCZ99] Armin Biere, Alessandro Cimatti, Edmund M. Clarke, and Yunshan Zhu, Symbolic model checking without bdds, TACAS, 1999, pp. 193–207.

[BCG+09] Dirk Beyer, Alessandro Cimatti, Alberto Griggio, M. Erkan Keremoglu, and Roberto Sebastiani, Software model checking via large-block encoding, FMCAD, 2009, pp. 25–32.