FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

The Board of Doctoral Study
Faculty of Mathematics and Physics
Charles University
Ke Karlovu 3
121 16 Prague 2

Prague, August 18, 2017

Re: Pavel Jančík, Doctoral thesis – Advisor's reference

The submitted doctoral thesis concentrates upon one of the main problems arising in software verification – its efficiency. In particular, it addresses two challenges. First, in the area of explicit model checking, it focuses on reduction of state representation based on dead heap-variables analysis; second, in the area of interpolation-based verification, it introduces an approach to reduction of Craig interpolants used in the verification process. The work has been done in the scope of the Czech Science Foundation project 14-11384S and the Charles University Grant 712712.

The thesis starts with an introduction of the field of verification and the high-level issues on which it focuses. The second chapter is devoted to description of the state-of-the-art approaches and tools for software verification; in particular, methods for storing and comparing states in explicit model checking. State-of-the-art techniques for dead variable analysis are described in details, for they are one of the thesis topics. The second part of the chapter is devoted to symbolic verification. Here, bounded model checking and, in particular, interpolation-based verification are described. Again, a lot of attention is paid to the proof-reduction and interpolant-reduction techniques. Chapter three refines the goals by adding more details in light of the previous chapter. Chapter four describes the contribution in the area of state representation. This is based on detection of dead heap variables, which can be, in turn, removed from the program state representation, since they cannot influence future behaviour of the program under verification. In particular, two types of analysis have been introduced – hybrid analysis and dynamic analysis, differing in speed and precision. Both analyses have been implemented in the scope of Java PathFinder and evaluated on a set of benchmarks including several non-trivial ones. Chapter five describes the contribution in the area of interpolation-based verification. Here, the Labelled Interpolation System is extended with a partial variable assignment allowing for computing a more focused interpolants, i.e., interpolants that over-approximate the desired set of states in a more precise way, being itself smaller than the corresponding ones computed without the assignment. Since the interpolants are frequently used during a particular verification task, this reduction leads to a more efficient verification process, in terms of both memory and time. Chapter six concludes the thesis by summarizing the contribution. The author has also included proofs of several properties of interpolants as well as the bisimulation relation between the original and reduced state space for partial variable reduction. The proofs can be found in the appendix of the thesis.

Department of Distributed and Dependable Systems
Malostranské nám. 2/25, 118 00 Praha 1
phone: 951554245, fax: 951554323
e-mail: info@d3s.mff.cuni.cz

Most results of the thesis have been published in proceedings of international peer-reviewed conferences and an impacted journal published by Springer. At the time of writing this reference, another journal publication co-authored by Pavel is in a review process.

In my view, Pavel Jančík has proved the ability of performing high-quality research with internationally relevant results. This thesis only confirms this fact. Thus, I strongly recommend the thesis for defence and to grant the Doctor degree to him.

Jan Kofroň
advisor