FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

Fakulta informačních technologií VUT
Vědecké oddělení
Božetěchova 2
612 66 Brno

Prague, November 13, 2023

Re: Review of the dissertation thesis of Martin Hruška

The submitted dissertation thesis focuses on employing automata-based techniques in testing and verification of software. The outcomes of Martin Hruška's work is not limited to scientific publications as usual, but it also contains several tools (or their extensions), proving the viability of the proposed approaches and, in turn, their practical impact. I would like to emphasize the importance and value of these, despite the fact that they are often prototypes, not being ready for industrial applications.

In the first chapter, after an introduction of the context of the work, the author clearly outlines the thesis goals and provides a brief overview of the achieved results. These results encompass two relatively independent areas: shape analysis and automated testing. The first goal involves improving state-of-the-art methods and tools for shape analysis through the formalism of forest automata and the FORESTER tool. The second goal focuses on applying forest automata in software testing, particularly for testing of manufacturing execution systems.

The thesis text is divided into two main parts, each corresponding to one of these goals. The first part is devoted to employing automata in shape analysis. In chapter 2, the state of the art is described, including methods connected to separation logic, and a description of counter-example guided abstraction refinement (CEGAR).

Department of Distributed and Dependable Systems
Malostranské nám. 2/25, 118 00 Praha 1, Czech Republic
info@d3s.mff.cuni.cz
+420 951554245

Chapter 3 provides information about shape analysis based on forest automata. It discusses several ways to represent various data structures in the heap, particularly different kinds of linked lists, since they are common data structures in the Linux kernel (and therefore worth verification). Then, the formalism of tree and forest automata is explained, along with their application in representing heap data structures. It covers theoretical aspects of this formalism and how symbolic execution can be performed on forest automata. Additionally, the CEGAR loop for the FA-based verification is described. A running example is presented to illustrate a run of the algorithm and the transformation effects on an example heap data structure. The chapter concludes with a description of the FORESTER tool, including its architecture, usage, and results of experiments executed to demonstrate its functionality.

Chapter 4 discusses the development of the FORESTER tool development, particularly its preparation for the Software Verification Competition (SV-COMP) in terms of technical steps needed to meet the competition's rules and requirements.

Chapter 5 addresses the weaknesses of current shape analysis approaches by employing tree automata, which seems to be a promising approach. Chapter 6 approaches the same problem via transforming the representation into an SMT problem, yielding promising results in terms of efficiency when tested on a selection of benchmark programs.

Chapter 7, being the only chapter of the second part of the thesis, is dedicated to automated software testing. It presents the concept of testing a complex (manufacturing) execution system via a digital twin, upon which the functionality is tested. The digital twin should, obviously, implement the same set of services/functionality (or subset thereof) as the original system. The main motivation behind this approach is that it is hard or even impossible to test the real system. The core of the testing system lies in capturing and creating communication—in the form of messages—sent among particular parts of the manufacturing system. To cover more scenarios than actually logged by the system, a tree-based approach for message abstraction (generalization) is presented, allowing for testing of even unseen communication types.

Chapter 8 concludes the thesis and outlines potential directions for future research.

The thesis is well-written and mostly easy to follow, although the first half of chapter 3 would benefit from more illustrative examples due to its abstract and complex nature, which might be challenging for those outside the automata field.

Other than the aforementioned point, I have no major comments to the thesis; I list some minor ones along with some questions here:

- The text of the thesis would benefit from another review to correct English errors and awkward phrasing, which are somewhat frequent in some parts.

- You mention “user-friendliness” of the library for working with automata as a potential direction of future work in chapter 8. Although I perfectly understand this point, do you think that a developer could use the library directly (for a general application, e.g., visualization of automata) or is the idea more like to provide the library to developers of verification tools? In the latter case, I would consider the “user-non-friendliness” a minor issue.

- In chapter 7, when generating abstract messages, could the abstraction lead to generation of messages that really do not make sense in practice? Is it still worth to examine the behaviour of the system after transferring such messages?

To sum up, the topic fits aligns well with the author’s field of study, and the problems addressed in the thesis are important to the state-of-the-art verification techniques and tools. The work contains several contributions to the field, particularly in terms of introducing new automata-based verification approaches as well as improving performance of state-of-the-art tools. The results contained within the thesis were in a great extent published in international conferences, often ranked CORE-A. From this perspective, I consider the results highly valuable. The author clearly proofs its scientific abilities to perform high-quality research, thus substantially contributing to the state of the art.

Therefore, I recommend that the committee accept the thesis as a dissertation and grant the author a doctoral degree.

Jan Kofroň
MFF UK