Supervisor's Opinion on the PhD Thesis of

Martin Hruška

The PhD thesis of Martin Hruška concerns primarily applications of finite automata in automated formal analysis and verification as well as in automated testing. In the former case, the stress is on the so-called shape analysis and formal verification of programs with complex, pointer-linked, dynamic data structures. In the latter case, the thesis targets automated testing of the control of distributed manufacturing systems. I find both of the subject areas up to date, challenging, and attracting ongoing research efforts from both academia as well as industry.

In more detail, the works of Martin Hruška summarized in his PhD thesis have come with the following contributions:

1. *Shape analysis based on forest automata.* The first contribution consists in the proposal of an original way of checking spuriousness of counter-examples stemming from the use of abstraction in shape analysis based on so-called forest automata (tuples of mutually linked and possibly nested tree automata), followed by an approach of refining the abstraction used in case a spurious counterexample is indeed detected. To the best of my knowledge, this approach is one of a very few existing approaches allowing CEGAR-based analysis in the context of programs with complex pointer-based dynamic data structures. It helped the Forester tool, in which it was implemented, to handle some programs that, e.g., none of the tools participating in the international software verification competition SV-COMP can handle. Moreover, Martin Hruška has significantly contributed to multiple cases of the Forester analyser participating in several different editions of SV-COMP. He has also contributed to preparing an extensive chapter on the entire approach to shape analysis based on forest automata that is to be published in a book devoted to tools participating in SV-COMP.

2. *Automata on graphs and shape analysis in 2LS.* Further contributions of Martin Hruška in the area of shape analysis include an original concept of automata on graphs inspired by the Courcelle's theorem. These automata can represent richer classes of graphs than forest automata and still enjoy some nice algorithmic properties making them a potential new formalism for implementing shape analyses. In another work, Martin contributed (though in a lesser degree) to a new approach of handling programs with dynamic data structures in the 2LS framework based on predicate logic, SAT/SMT solving, templates of invariants, and abstraction.

3. *Automata in testing manufacturing execution systems.* The final contribution of Martin is from a rather different area than the previous ones, but it still involves a use of automata. Namely, it is an approach of learning a model of the communication between a manufacturing execution system, machines, and an enterprise resource planning (ERP) system, which can subsequently be used for generating testing scenarios for the manufacturing system.

The research of Martin Hruška was conducted within the VeriFIT research group at the Faculty of Information Technology of Brno University of Technology (FIT BUT). The research on the 2LS framework involved collaboration with Dr. Peter Schrammel from DiffBlue, Ltd., and University of Sussex, UK. On the other hand, the research direction concerning automated testing of manufacturing systems involved a collaboration with the UNIS company, a producer of the Pharis manufacturing execution system.

The research that Martin Hruška contributed to was conducted within multiple research projects including several projects of the Czech Science Foundation as well as the Czech Technology agency, H2020 ECSEL projects, and also an ERC.CZ project. For his research, Martin has received the PhD talent scholarship of the Brno City and the South Moravia region.

The results presented in the thesis of Martin Hruška have been published in regular papers at two major international conferences: namely, VMCAI'17 and FMCAD'18 (though, in the latter case, the contribution of Martin is lesser). Three SV-COMP competition papers published at the prestigious TACAS conference described participation of the Forester tool in various editions of SV-COMP. Moreover, an extensive chapter on the Forester analyzer has been accepted to a book on the tools participating in the international competition in software verification SV-COMP. The results concerning graph automata and automated testing of manufacturing execution systems were published at the NETYS'21 and EUROCAST'22 international conferences.

At this place, I would like to note that despite the mentioned works include a single regular paper published at a major conference with Martin as the main author, I see this as compensated by the other mentioned publications. I would also like to note that the paper on graph automata published at NETYS resulted from a rather long and hard work, which did not lead to a more significant publication primarily because there appeared a paper from another team that covered quite some of the results that Martin was aiming at.

In addition, Martin contributed to two further works that are not included in the thesis: namely, (1) a combination of the Predator shape analyzer and the Symbitioc verifier based on symbolic execution (and other techniques), and (2) the new efficient finite automata library MATA and its experimental evaluation. These works were published in the proceedings of TACAS'20 (again as a competition paper) in the former case and in the proceedings of CADE'23 in the latter case (with another paper under preparation for TACAS'24).

To sum up, within his PhD studies, Martin Hruška has achieved multiple original research results. He has proved to be creative, capable of independent and systematic work, and also able to perform both conceptual research as well as to produce advanced implementations of the studied methods. He has also showed to be able to work on collaborative research projects, to cooperate with foreign researchers as well as the industry. In my opinion, the thesis of Martin Hruška satisfies requirements usually associated with PhD theses in the area of computer science and therefore I recommend it to be accepted.

Brno, July 25, 2023

Prof. Ing. Tomáš Vojnar, Ph.D.