BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Supervisor's Opinion on the PhD Thesis of

Tomáš Fiedor

The PhD thesis of Tomáš Fiedor concentrates on efficient techniques of using *automata* in *formal verification*. With the ever-rising usage of computer-based systems in all areas of human lives, including safety-critical systems, methods of formal verification are constantly gaining more importance. However, due to the rising complexity of systems to be verified, the scalability, precision, and/or generality of automated formal verification methods are still not sufficient despite many advances achieved in this area. Many of these approaches use automata either directly or indirectly (e.g., through their application when solving satisfiability of formulae in various logics). Improvements of various techniques of dealing with automata can thus significantly help to improve current formal verification approaches. I hence find the subject area of the thesis of Tomáš Fiedor highly up to date and important.

The research of Tomáš Fiedor was conducted within the VeriFIT research group at the Faculty of Information Technology of Brno University of Technology. In particular, Tomáš was co-supervised by Assoc. Prof. Adam Rogalewicz, and he tightly collaborated with Dr. Lukáš Holík and Dr. Ondřej Lengál too. Moreover, in one of the concrete research directions covered by the thesis, Tomáš collaborated in an intense way with Dr. Florian Zuleger and Dr. Moritz Sinn from the Faculty of Informatics of Vienna University of Technology.

The research conducted by Tomáš Fiedor was an important part of multiple research projects, including five projects of the Czech Science Foundation (the most recent one being the project No. GA17-12465S "ROBUST: Verification and Bug Hunting for Advanced Software") as well as the H2020 ECSEL project "AQUAS: Aggregated Quality Assurance for Systems". Moreover, it was also a part of several institutional projects at FIT BUT, including the IT4I Centre of Excellence. For his research, Tomáš has received a research scholarship from Red Hat too.

From my point of view, the main contributions of the research of Tomáš Fiedor presented in his thesis include:

- A new *decision procedure for the WS1S logic* based on *automata* and their pruning using principles of *(nested) antichains*. This decision procedure was implemented in the dWiNa tool and shown to be able to outpeform the well-known MONA tool in some cases.

- Another novel *decision procedure for WS1S* that is based on a *lazy construction* of the automaton corresponding to the given formula, interleaved with an *on-the-fly check of its emptiness*. In this case, the automaton is represented symbolically using so-called *language terms*. This procedure, together with various further optimisations (such as antiprenexing), has been implemented in the Gaston tool and managed to be faster than both MONA and dWiNa on some formulae.

- An approach for *analysing amortised time complexity* of programs manipulating with *complex dynamic linked data structures*. The approach is based on an original set of *norms* over

dynamic linked data structures and on using results of *automatic shape analysis* for converting programs with dynamic linked data structures into *integer programs*, whose amortized complexity can subsequently be analyzed by an analyzer for integer programs. The approach has been implemented in the Ranger tool that combines the Forester shape analyser (based on a notion of forest automata) and the Loopus complexity analyser for integer programs. Using the approach, precise time complexity was for the first time obtained fully automatically for some programs.

The results were published in the proceedings of three well-known conferences—namely, TACAS'15, TACAS'17, and VMCAI'18—as well as in the Acta Informatica journal. The publications have so far attracted 7 citations (without self-citations). The publications have multiple co-authors, but I can confirm that Tomáš Fiedor played a major role on all of them: namely, he contributed some of the key ideas, participated on the writing, and performed most of the implementation and experiments.

As a side note, let me add that, apart from the works presented in his thesis, Tomáš Fiedor is also actively developing a dynamic analyser called *Perun* designed for *dynamic performance analysis* and *detection of performance regressions*. A number of bachelor and master students is cooperating on the developement of Perun under supervision of Tomáš Fiedor. Perun is an important contribution within the H2020 ECSEL project Aquas, and it is going to be developed within the recently started H2020 ECSEL project Arrowhead Tools too. Moreover, Tomáš is also co-supervising development of the *Looper plugin* of the Facebook Infer static analyser that is intended as a replacement of the Loopus analyser.

To sum up, within his PhD studies, Tomáš Fiedor has achieved multiple significant research results. He has proved to be creative and to be capable of working independently, systematically, and hard. He has also showed to be able to work on collaborative research projects, to cooperate with foreign researchers, as well as to lead a group of cooperating students. In my opinion, the thesis of Tomáš Fiedor satisfies requirements usually associated with PhD theses in the area of computer science and therefore I recommend it to be accepted.

Brno, November 27, 2019 Prof. Tomáš Vojnar