# Supervisor's Opinion on the Ph.D. Thesis of

## Ondřej Lengál

The Ph.D. thesis of Ondřej Lengál concentrates on efficient techniques of using finite word and tree automata in automata-based symbolic formal verification of infinite-state systems. Formal verification of computer-based systems is nowadays a rather lively research topic due to the complexity of such systems is constantly increasing, and at the same time, the demands on their quality are rising too. Despite a lot of research effort has been devoted to developing efficient formal verification techniques and many of such techniques have already found their way into the industry, a lot of problems concerning the degree of automation, scalability, and generality of the state-of-the-art verification techniques remain open. This is, in particular, true for various kinds of infinite-state systems. The goal of the work of Ondřej was therefore to significantly improve this situation by means of developing new automata-based techniques suitable for verification of infinite-state systems, with a particular stress on programs with dynamic linked data structures, which belong among the most demanding class of programs from the point of view of formal verification.

The research of Ondřej was supervised by me, co-supervised by dr. Lukáš Holík, and conducted within the VeriFIT research group at the Faculty of Information Technology of the Brno University of Technology (FIT BUT). The research was an important part of multiple research projects including projects of the Czech Science Foundation (projects 202/13/37876P, P103/10/0306, 13-37876P, and 14-11384S), the Czech Ministry of Education (project COST OC10009 and the long term institutional project MSM0021630528), the EU-Czech IT4Innovations Centre of Excellence, the European COST Action IC0901, as well as several projects of the internal grant agency of the BUT. Apart from that, Ondřej was a member of the team of the doctoral project 102/09/H042 of the Czech Science Foundation, which included only specially selected students from FIT BUT and the Faculty of Informatics of the Masaryk University in Brno. The results achieved by Ondřej were an important contribution to all these projects.

The main contributions of the research of Ondřej Lengál presented in his thesis include the following:

- An extension of the sooner proposed *shape analysis based on forest automata* into a fully-automated technique. The formalism of forest automata (FAs) is based on tree automata (TAs) and a hierarchical encoding of sets of heaps, in which sets of subgraphs, represented using lower-level FAs, are used as symbols of a higher-level FA. The developed extension automatically searches for a suitable hierarchy of the FAs needed to analyse a given program and thus avoids the previous need to provide the hierarchy manually. The usability of the FA-based shape analysis improved significantly in this way, which was shown by its experimental evaluation on a large class of data structures occurring in practice.

- An extension of the FA-based analysis with a *support for ordered data*. This extension, together with the previous contribution, allows one to automatically verify programs with data structures that rely on ordering relations between data, such as binary search trees or skip lists. This is the first work that I am aware of that managed to fully automatically verify a fully-fledged implementation of two- and three-level skip lists.

- Development of a new *decision procedure for separation logic* based on tree automata. The decision procedure works for a practical class of data structures, containing various flavours of (nested) lists, and is both effective and efficient, as proved by the three medals that its implementation won in the first competition of separation logic solvers SL-COMP'14.

- Optimization of the *decision procedure for weak monadic second-order logic of one successor* (WS1S) with the use of the so-called nested antichains. This work brought a new insight into the structure of the automata emerging in the decision procedure, and exploited the structure in a novel symbolic encoding together with algorithms for manipulating this encoding. Moreover, I do believe that this work has a great potential for further improvements.

- A new algorithm for *top-down inclusion checking* on non-deterministic tree automata optimised by using antichains and downward simulations. This algorithm is experimentally proved to often significantly outperform the so-far prevailing bottom-up inclusion checking.

- Development of *symbolic encodings of non-deterministic tree automata* and efficient algorithms for their manipulation. The encoding has been used as an efficient backend for the decision procedure for WS1S mentioned previously.

- The above presented algorithms have been implemented in a new *library for dealing with non-deterministic tree automata* called VATA. Within the implementation of this library, a number of low-level optimisations of the basic algorithms proposed in the thesis as well as taken from the literature was proposed and implemented to make the library highly efficient.

The above mentioned works have been published in six papers at highly ranked international conferences (ATVA'11, TACAS'12, CAV'13, ATVA'13, APLAS'14, TACAS'15) and in one journal paper accepted for publication in Acta Informatica. Moreover, Ondřej also significantly contributed to the development of the Forester tool and was the main driving force that allowed Forester to participate in the 4$^{th}$ competition on software verification SV-COMP'15. All the mentioned works have several co-authors, but I can acknowledge that Ondřej contributed by key ideas as well as by a very sophisticated implementation and experiments to all of them.

During his Ph.D. studies, Ondřej Lengál has proved to have creative abilities, independence, and to be able to work hard. He has also proved to be capable of a tight international cooperation with researchers from leading international teams. In my opinion, the thesis of Ondřej Lengál satisfies all requirements usually associated with Ph.D. theses in the area of computer science, and I therefore recommend it to be accepted.

Brno, April 7, 2015

Prof. Ing. Tomáš Vojnar, Ph.D.