

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

Jiří Šimáček

The Ph.D. thesis of Jiří Šimáček is devoted to automata-based symbolic formal verification of programs with dynamic linked data structures and, further, to efficient ways of dealing with automata in symbolic verification in general. Formal verification of software is nowadays a very hot topic due to the complexity of software is constantly increasing, and at the same time, the demands on its quality are rising too. Moreover, programs with pointers and dynamic linked data structures belong among those programs which are especially difficult to write and whose quality is difficult to assure using traditional approaches such as testing. Their formal verification is, however, also very demanding due to the necessity of dealing with their infinite state spaces consisting of configurations that have a form of general graphs. Automata-based methods to verification of such programs known at the beginning of the work of Jiří Šimáček used to belong among the most general fully automated approaches in the given area, but they were not very scalable. The goal of the work of Jiří was therefore to significantly improve this situation.

The research of Jiří Šimáček, on which his Ph.D. thesis is built on, was conducted under a double degree (co-tutelle) agreement between the Faculty of Information Technology of the Brno University of Technology (FIT BUT), on whose side I was the supervisor of Jiří, and the VERIMAG laboratory of Université Joseph Fourier in Grenoble, later renamed to Université de Grenoble, on whose side Jiří was supervised by Prof. Yassine Lakhnech and co-supervised by Dr. Radu Iosif. The research was an important part of multiple research projects including projects of the Czech Science Foundation (projects 102/07/0322, P103/10/0306, and P201/09/P531), the Czech Ministry of Education (project COST OC10009 and the long term institutional project MSM0021630528), the European COST Action IC0901, as well as the Czech-French Barrande projects MEB 020840 and 021023. Apart from that, Jiří was a member of the team of the doctoral project 102/09/H042 of the Czech Science Foundation that included only specially selected students from FIT BUT and the Faculty of Informatics of the Masaryk University in Brno. The results achieved by Jiří were an important contribution to all these projects.

The main contributions of the research of Jiří Šimáček presented in his thesis include the following:

- A new notion of the so-called *forest automata* suitable for encoding sets of heap graphs. The notion combines the expressive power of tree automata with a structuring mechanism allowing for their efficient local manipulation in symbolic verification. The notion is also extended by a principle of hierarchical structuring allowing for a natural description of hierarchically structured dynamic linked data structures quite common in practice.
- A *symbolic verification procedure for formal verification of programs with dynamic linked data structures* based on the notion of forest automata. The procedure includes efficient ways of symbolically executing program statements on forest automata as well as optimised ways for abstracting forest automata and for checking inclusion on them. The procedure has been implemented in a tool called Forester and experimentally shown to provide very promising results (often beating state-of-the-art tools from the area of verification of programs with dynamic linked data structures in terms of efficiency and/or generality).
- An optimised algorithm for *computing simulations on labelled transition systems* (LTSs) that significantly improves the efficiency of computing simulations on tree automata by their translation to LTSs. This is quite important since the use of simulation relations is crucial

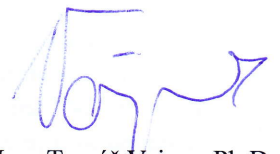
for the state-of-the-art algorithms for reducing the size of nondeterministic tree automata and for checking inclusion of their languages.

- 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.
- 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 several papers at highly ranked international conferences (CAV'11, ATVA'11, TACAS'12) as well as at the MEMICS'09 workshop. The work published at MEMICS'09 was among 6 papers from among of 45 papers submitted to the workshop that were selected for publication in the international journal Computing and Informatics. Moreover, the work published at CAV'11 was selected among 6 papers out 161 papers submitted to the conference for publication in the renowned international journal Formal Methods in System Design. In addition, some parts of the thesis, namely those devoted to optimised abstraction on forest automata and the automatic inference of their hierarchical structuring, have not yet been published, but it is planned that they will form the basis of a paper to be submitted to some major conference in the near future. All the mentioned works have several co-authors, but I can acknowledge that Jiří contributed by key ideas as well as by a very sophisticated implementation and experiments to all of them.

During his Ph.D. studies, Jiří Šimáček 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 Jiří Šimáček satisfies all requirements usually associated with Ph.D. theses in the area of computer science, and I therefore recommend it to be accepted.

Brno, July 31, 2012



Prof. Ing. Tomáš Vojnar, Ph.D.