A report on the PhD thesis

Automata in infinite-state formal verification

that has been submitted at the Faculty of Information Technology,
Brno University of Technology, by

Ondřej Lengál

Reviewer: Prof. Petr Jančar
Faculty of Electrical Engineering and Computer Science,
VŠB - Technical University of Ostrava

Overview of the thesis

The submitted thesis is written in English and has around 170 pages; it contains three main parts, presented in 11 chapters (including Introduction and Conclusion).

The thesis contributes to the area of verification of software systems; in particular, it pushes further the bounds of automated formal verification of memory-safety properties of programs manipulating dynamic data structures (like linked lists, trees, and more general structures using pointers).

The presented research is based on the work that has been pursued by the author with his supervisor (prof. T. Vojnar) and with other members of his research group, often also with their international collaborators (from the renowned institutes in France, Sweden, and Taiwan).

One class of automated verification methods is based on finite (word or tree) automata: the automata describe (over-approximations of) sets of configurations, and they are transformed by performing program-commands, until reaching a fixpoint (maybe by accelerations causing the over-approximations of the set of reachable states). *The first part of the thesis* describes new enhancements of a method based on forest automata; it deals in particular with a full automation of the method of abstract boxes (turning a general graph-structure into a forest-structure, i.e. into a set of trees), and also takes the data-items in the structure into account. The main publication on which this part is based was presented at the prominent conference CAV (Computer Aided Verification) in 2013.

Besides automata, also various types of logics are used for capturing the sets of configurations in verification. *The second part of the thesis* describes new procedures for deciding a fragment of the separation logic, and of the weak second-order logic of one-successor (WS1S), which are standard examples of logics used in this area. Here we can highlight the publication at the renowned international conference TACAS (Tools and Algorithms for Construction and Analysis of Systems) in 2015.

The work in the above areas is underpinned by efficient handling of nondeterministic finite tree automata. This topic, including the library VATA of implemented procedures, is dealt with in *the third part of the thesis*. This work was also reported in a contribution at the

established international symposium ATVA (Automated Technology for Verification and Analysis) in 2011.

Evaluation

The thesis is well-written, which also demonstrates the scientific maturity of the author. It is also commendable that he tries to give partly informal explanations before technical definitions and procedures. I think that these informal parts could have been still more extended, and equipped with more examples and explanations of the key novel ideas in the author's contribution. I suppose he will concentrate on such example-based explanations during his defence.

1/ The topic of the thesis

surely belongs to the area of Computer science and technology, it is well rooted in the current state-of-the-art and it reacts to the actual research problems in verification.

2/ Originality of the contribution

All the three parts of the thesis have brought original research results, as is also demonstrated by the acceptance to the top publication venues. There is also a very positive aspect that the theoretical results have been verified by experiments with prototype software tools where O. Lengál has been often the main developer.

3/ Publication of the kernel of the thesis

The reported work has been presented at some top competitive conferences, and one part should also soon appear in a journal form. In this sense, it is clear that it has been accepted as a quality research by the scientific community. This is also underlined by other international researchers who refer to the respective papers.

4/ Scientific erudition

All publications of Ondřej Lengál have co-authors but I have no doubts about his significant contribution to all of them. (He has also often presented the joint works at the respective conferences.) In my opinion he has indeed demonstrated that he is able to pursue high-level research and reach significant results. A part of this demonstration is the thesis itself, in which the achieved results are presented by the author in one framework, and at a very solid level.

Conclusion. The author has demonstrated the ability to perform a solid research, achieving high-quality results when measured by international research standards. I can see his thesis as a high-quality PhD thesis in the area of computer science and technology.

Ostrava, 17 June 2015