FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

for(syte
Formal Methods
in Systems Engineering

Univ. Prof. Dr. Helmut Veith
Technische Universität Wien
Institut für Informationssysteme

Arbeitsbereich Formal Methods in
Systems Engineering

Favoritenstraße 9-11/184-4
1040 Wien

T +43 (1) 58801 18403
F +43 (1) 58801 18493
veith@forsyte.tuwien.ac.at
www.forsyte.tuwien.ac.at

Sylva Sadovská
Faculty of Information Technology
Brno University of Technology
Božetěchova 2

**Report on the PhD Thesis „Automata in Infinite-State Formal Verification"
submitted by Ing. Ondřej Lengál**

In my report, I will follow the guidelines laid out in your letter from May 18, 2015.

Is the topic appropriate to the particular area of dissertation and is it up-to-date from the viewpoint of the present level of knowledge?

While model checking has been extremely successful for certain classes of simple software such as device drivers, the analysis of dynamic data structures on the heap has remained a central technical challenge. In fact, it is widely believed that the lack of good verification methods for the heap is the key obstacle to broad application of model checking in software engineering.

The problem is difficult because dynamic data structures can describe arbitrarily complex graph structures – trees, lists, but also more complicated graphs – that are hard to predict by a static analysis. (In contrast, flat data types such as int and float exhibit a much more predictable behavior in most programs.) It is thus necessary to identify and to study formalisms based on logic or automata that are able to capture the complexity of data structures on the heap, but have good algorithmic properties. The thesis by Mr. Lengál studies several of these formalisms from an automata-theoretic and a logical point of view:

- tree automata
- forest automata
- separation logic
- monadic second order logic WS1S

These formalisms are subject to extensive investigation by leading international research groups in academia and in international research labs. Thus, the thesis is clearly concerned with a topic of strong current interest.

Is the work original and does it mean a contribution to the area – specify where the new contribution lies?

The thesis makes multiple original technical contributions:

- In introduces the box learning technique which is able to infer a compact representation of complex graph structures on the heap. The method is implemented in the tool Forester and experimentally compared to the older tool Predator. The results demonstrate that the box learning technique is as powerful as manual techniques, and that the performance of the Forester tool is comparable to Predator, although Forester has broader applicability
- It extends forest automata to handle dynamic data structures with ordered data such as binary search trees or skip lists. Since other tools cannot handle these complex data structures, experimental comparison is not possible.
- It describes novel decision procedures for separation logic and monadic second order logic based on tree automata, and implements them in the tools SPEN and dWiNA. The SPEN tool was a winner in a category of the separation logic contest SL-COMP 14.
- It develops new algorithms to check inclusion of tree automata, and implements them in the VATA open source library. VATA is used for Forester, SPEN, and other tools.

Thus, the thesis has made significant contributions to both the theory and the practical implementation of automata-based methods in computer-aided verification.

By the standards of many countries, half of these results would suffice for a PhD thesis.

Has the core of the doctoral thesis been published at an appropriate level?

The results have been published in 3 papers in the two international top conferences on computer-aided verification – CAV, and twice TACAS – as well as two papers in the leading Asian conference ATVA, a paper in the well-known conference APLAS, and a journal paper in Acta Informatica (Springer). Thus, Mr. Lengál's thesis has lead to 7 international top publications, which is well above the standards that I know from my work experience in Austria, Germany, and the US.

Does the list of the candidate's publications imply that he is a person with an outstanding research erudition?

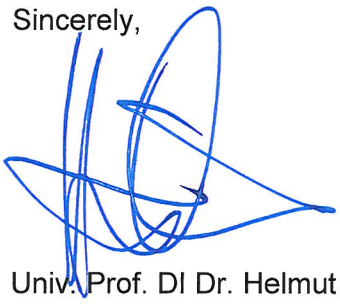
Yes. Many international researchers have a comparable publication record only in the 2nd or 3rd year of their postdoc phase.

FAKULTÄT
FÜR !NFORMATIK
Faculty of Informatics

for(syte
Formal Methods
in Systems Engineering

In conclusion, this is an excellent PhD thesis based on deep and novel research results that were published at international top venues. Without any doubt, the doctoral thesis by Mr. Lengál meets the requirements for the conferment of the title PhD.

Sincerely,



Univ. Prof. DI Dr. Helmut Veith

Vienna, June 15, 2015