

## Supervisor's Opinion on the PhD Thesis of

Lukáš Charvát

The PhD thesis of Lukáš Charvát concentrates on automated methods of *verification of selected features of microprocessors* with a stress on those designed using the HW/SW co-design paradigm for embedded devices. In particular, Lukáš concentrates on *methods with formal roots*, trying to be sound as much as possible though sometimes the methods he considers sacrifice soundness in exchange for efficiency. Development of microprocessors optimised for specific purposes of concrete embedded devices is nowadays more and more common, stimulated, e.g., by the stress on energy-efficiency. There is a strong pressure on the development process to be fast, and, at the same time, the microprocessors being developed are far from trivial, including features such as pipelining, which can cause dangerous, rarely manifesting, and hard to find errors.

Thorough verification of microprocessors under design is hence highly needed, and despite it is currently done mostly by simulation and functional verification, there is an ever-rising demand for these approaches to be complemented by formal verification or at least methods with formal roots (capable of finding errors possibly missed by other approaches: as even Lukáš has shown by some of his practical results). I thus find the subject area of the thesis of Lukáš Charvát highly up to date and also highly challenging due to the complexity of the considered microprocessor designs.

The research of Lukáš Charvát was supervised jointly by me and Dr. Aleš Srmčka and conducted within the VeriFIT research group at the Faculty of Information Technology of Brno University of Technology. Especially at the beginning, the research directions were also consulted with people behind the Cudasip company producing tools for HW/SW co-design of custom microprocessors as well as tools for development of applications on these processors (compilers, assemblers, disassemblers, simulators, etc.). This collaboration allowed Lukáš to evaluate his approaches on multiple real-life microprocessors under development.

However, I have to stress that the research direction of Lukáš Charvát was to a large degree outside the primary focus of the VeriFIT research group that primarily targets software verification, analysis, and testing. Consequently, Lukáš had to be much more independent than many other PhD students. Together with a need to earn his living in the later phase of the studies, this resulted in an exceptionally long duration of the studies. Nevertheless, I have to stress that I very positively evaluate the capability of Lukáš to work independently, his invention, as well as his strong will to finish the studies despite working in the industry for a long time.

The research conducted by Lukáš was an important part of multiple research projects including projects GAP103/10/0306 and GA14-11384S of the Czech Science Foundation, the Czech Ministry of Education project COST OC10009 (and the associated European COST action IC0901 "Rich Model Toolkit"), as well as several FIT BUT institutional projects (including the IT4I Centre of Excellence).

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


- A new approach for *modelling large memories* whose models are to be used when applying formal verification (or verification with formal roots) on designs including such memories.
- A new approach for checking *correspondence of the effect of instructions* of microprocessors described on the ISA and RTL levels. The approach allowed Lukáš to find several unknown and subsequently corrected errors in microprocessors under development—despite they had been thoroughly verified by simulation and functional verification.
- A series of new approaches for checking presence of various types of *pipeline hazards* (read-after-write, write-after-read, write-after-write, as well as control hazards) in microprocessors with a single pipeline. The methods combine in a quite efficient and involved way several verifications methods, namely, data-flow analysis, SMT solving, and parametric verification based on regular model checking. The approach nicely complements the above mentioned one that considers instructions executing in isolation. The proposed methods were implemented in the Hades tool and successfully applied to several real-life microprocessors.

The results of Lukáš were published in the proceedings of five conferences or workshops published by IEEE (MTV'12 and MTV'14) and by Springer in the LNCS series (EUROCAST'13, EUROCAST'15, and MEMICS'16). Here, I would like to stress that MTV, despite being a workshop, has a strong presence of big industrial players such as Freescale, Synopsys, MentorGraphics, Intel, AMD, ARM, Cadence, etc. Moreover, the last result of Lukáš containing a unified approach to all of the above mentioned types of pipeline hazards (where dealing with control hazards was newly added) has been submitted for review into the STTT journal. Despite all the papers have Aleš Smrčka and me as co-authors, I can acknowledge that Lukáš played a major role in all of them—contributing by key ideas, a very sophisticated implementation and experiments, as well as a significant part of the writing.

As a side note, let me add that after Lukáš lost the status of a regular PhD student, he started to work as a verification engineer for the division of Automated Control Systems of Honeywell where he introduced usage of various advanced ways of testing and verification on formal roots. His work led to discovery and correction of many nasty errors in networked control systems under development. This opened a way for further collaboration of the VeriFIT research group with Honeywell, which—despite many changes that happened in Honeywell in between—recently resulted into a project of the Czech Technology Agency.

To sum up, within his PhD studies, Lukáš Charvát has proved to have creative abilities, independence, and to be able to work hard. He has also proved to be capable of working on collaborative research projects and producing practically applicable results. In my opinion, the thesis of Lukáš Charvát satisfies requirements usually associated with PhD theses in the area of computer science and I, therefore, recommend it to be accepted.

Brno, July 29, 2019

Prof.  Vojnar

