Assoc. Prof. Dr. Florian Zuleger

Technische Universität Wien
Institut für Logic and Computation
AB Formal Methods in
Systems Engineering
Favoritenstraße 9-11/192-4, 1040 Wien

T: +43-(1)-58801-18449
F: +43-(1)-58801-18492
E: zuleger@forsyte.tuwien.ac.at

Wien, 01.12.2023

Evaluation of the PhD thesis
"Static Analysis of C Programs"
by Viktor Malík

I. Doctoral Thesis

Appropriateness and Relevance:
The thesis addresses highly relevant problems within the area of static program analysis. By focusing on the development of new techniques for verifying low-level C programs, the thesis tackles important challenges in ensuring the correctness and equivalence of real-world systems code. The chosen area is appropriate and aligns with the current needs and advancements in the field of software verification and formal methods.

A summary of the Contributions of the Thesis:
The primary goal of the thesis is to advance the state-of-the-art in formal verification of low-level C programs. The contributions of the thesis come in two parts. The first set of contributions include the introduction of two new abstract domains specialized for template-based invariant synthesis: A shape domain for reasoning about pointer-based data structures on the heap, and an array domain for reasoning about the contents of arrays. These domains allow combined reasoning about the structure and values of heap and array data, enabling reasoning about the shape of linked structures on the heap and the contents of arrays. These contributions have been integrated into the 2LS framework, significantly enhancing its capabilities for verifying programs using complex data structures. The second set of contributions consist of a novel method for lightweight static analysis of semantic equivalence between versions of a project, focusing on functions and global variables. This uses a novel combination of lightweight techniques like LLVM IR comparison and program slicing, addressing scalability issues in comparing large C projects. The method has been implemented in a tool called DiffKemp, which can compare thousands of functions in large projects like the Linux kernel in minutes, achieving useful results where other approaches fail due to scalability issues.

Novelty and Significance:
The results of the thesis demonstrate a high level of novelty and significance within static program analysis. The proposed abstract domains and the proposed semantic comparison approach represent innovative steps towards long-standing challenges in verifying and maintaining low-level system code. These contributions have the potential to significantly impact the further development of formal verification

techniques, particularly in the context of complex real-world programs. Furthermore, the practical applications of the results are evident in the improved capabilities of 2LS and the development of the DiffKemp tool for semantic comparison, as evidenced in the comparison against related tools from the literature, addressing critical needs in software engineering and system maintenance.

Evaluation of the Formal Aspects of the Thesis:
The thesis is well structured and written to a high academic standard. Technical topics are explained clearly and rigorously. Results are evaluated experimentally on realistic benchmarks, supporting the validity of the contributions.

Quality of Publications
The core results have been published in high-quality international venues, including top conferences in software engineering and formal methods (FMCAD,TACAS,ICST,NETYS). The quantity and impact of the publications are commensurate with requirements for a doctoral dissertation in this research area.

II. Candidate's Overall Achievements

Overall R&D Activities Evaluation:
The overall evaluation of the research and development activities presented in the thesis reflects a comprehensive and impactful contribution to the field of static program analysis. The development of new techniques, integration into existing frameworks, and implementation of practical tools demonstrate a strong commitment to advancing the state-of-the-art in formal verification. The competitive results, awards, and successful application of the contributions in real-world scenarios further underscore the excellence and impact of the R&D activities conducted as part of the thesis.

III. Conclusion

The doctoral thesis demonstrates an excellent understanding of static analysis and formal methods, particularly in the realm of low-level C programs. The student's contributions, such as the proposed abstract domains and the method for semantic equivalence checking, make significant contributions to the field. The comprehensive contributions made in the thesis, combined with the successful implementation of the proposed solutions, make a compelling case for the student's academic merit and warrant the award of a doctoral degree in recognition of their substantial achievements in the field of computer science and software engineering.

Assoc. Prof. Dipl.-Math. Dr.techn. Florian Zuleger