Seminar Hora Informaticae — Institute of Computer Science, Prague

Tuesday, April 22, 2025, 13.30 – 15.30 (1.30 – 3:30 PM) CEST

Meeting Room 318, Address: Pod Vodárenskou věží 2, Prague 8

Meeting ID: 914 0834 4018, Passcode: 668534

https://cesnet.zoom.us/j/91408344018?pwd=x2QIz4F42BxlMSmWc1HOwHHA7Uw7PN.1

Jan Onderka, Institute of Computer Science, Czech Academy of Sciences:

Abstraction-Based Machine-Code Program Verification.

Formal verification of programs in their binary machine-code representation can be used to prove or disprove low-level properties not verifiable using source code, such as correct manipulation of processor peripherals or the maximal used program stack size. While machine-code verification has been problematic due to the diversity of processor architectures and loss of higher-level information in machine code, I present a general verification solution based on model checking with an Input-based Three-valued Abstraction Refinement framework, applicable to arbitrary mu-calculus properties and digital systems expressible as Finite-State Machines. I introduce a free and open-source tool machine-check (https://machine-check.org) that instantiates the framework for Computation Tree Logic properties and digital systems described in a subset of the Rust programming language. We show and discuss its ability to verify properties of machine-code programs for the ATmega328P microcontroller, finding a previously unknown bug in one of the evaluated programs.

References:

[1] Onderka, J., Ratschan, S. Fast three-valued abstract bit-vector arithmetic. In Finkbeiner, B., Wies, T., editors, Proceedings of the 23rd International Conference on Verification, Model Checking, and Abstract Interpretation, VMCAI 2022, pages 242–262. Springer Nature Switzerland, Cham, 2022. ISBN: 978-3-030-94583-1. doi:10.1007/978-3-030-94583-1_12.

[2] Onderka, J. Formal verification of machine-code systems by translation of simulable descriptions. In Proceedings of the 13th Mediterranean Conference on Embedded Computing, MECO 2024. Budva, Montenegro, 2024. doi:10.1109/MECO62516.2024.10577942.

[3] Onderka, J., Ratschan, S. Input-based three-valued abstraction refinement (preprint). arXiv:2408.12668 [cs.LO]. 2024. https://arxiv.org/abs/2408.12668

Jan Onderka (https://onderjan.net) is a formal verification researcher focusing on verification of machine-code programs, supported by his background in digital system design and electrical engineering. He is employed at the Institute of Computer Science, Czech Academy of Sciences, and is a doctoral candidate at the Faculty of Information Technology, Czech Technical University (CTU) in Prague.

HORA INFORMATICAE (meaning: TIME FOR INFORMATICS) is a broad-spectrum scientific seminar devoted to all core areas of computer science and its interdisciplinary interfaces with other sciences and applied domains. Original contributions addressing classical and emerging topics are welcome. Founded by Jiří Wiedermann, the seminar is running since 1994 at the Institute of Computer Science of the Czech Academy of Sciences in Prague.

https://www.cs.cas.cz/horainf