Enabling Formal Verification of Data-Aware Hardware Models

Technical University of Munich

Department of Informatics

Chair of Robotics, Artificial Intelligence and Real-time Systems

Background

With the evergrowing reliance on computer systems, interest in the verification of such has seen an incredible increase in popularity over the past decades [2, Ch. 1]. While this is especially the case for safety critical applications, verifying the compliance of a system to a given specification has become a standard requirement in many different domains of system design. Therefore, formal methodologies have been developed which allow for mathematically proven and comprehensive verification of a system.

This thesis will be conducted in the domain of systems design with SystemVerilog and will focus on enabling formal verification of systems in which data is intensively involved. The methodology used for formal verification is model checking, where the conformity of a system's model to a given set of properties is verified by exploring the model's state space.

Description

As good as formal verification sounds, there are serious limitations on the models and properties which can be verified with model checking in reality [2, Ch. 2]. One of the biggest limitations of model checking is the so-called *state space explosion*. The term refers to the fact that a system's state space grows exponentially with the amount of data stored in the system. This can very quickly lead to issues during the traversal of the model's state space due to time and/or memory constraints.

Hence, in the context of hardware verification, model checking is most feasible for the verification of control logic, for example the handshake behavior of low-level protocols. Such control signals usually require only few registers, resulting in a relatively small state space.

Nonetheless, sometimes the data paths in a system are required for verification as well. Taking into consideration the data signals of a design greatly increases its state space, since data is usually stored in large registers. Due to the state space explosion problem, this can leave formal verification of such systems infeasible.

The goal of the thesis is to enable formal verification of certain models in which data, e.g. fixed-point numbers, is involved. So far, not much effort has been invested into the formal verification of these specific models. This means that a lot of exploration will be necessary to assess how well model checking can be applied to the models and to establish a verification flow. It might be required to exploit properties of the models and the data in order to reduce the verification effort or even to make verification possible in the first place.

Inspiration might be taken for instance from [1], [3], [4] or [5].

Tasks

1. Establish basic verification flow for simple designs
2. Determine for which data-aware models state-space explosion is the main barrier for model checking
3. Develop technique to abstract data-aware system designs for model checking
4. Extend verification flow to allow verification of data-aware models
5. Evaluate methodologies against real-world applications used in the industry

Supervisor:
Prof. Dr.-Ing. Matthias Althoff

Advisor:
Tobias Ladner, M.Sc.

Research project:
FAI

Type:
MA

Research area:
Formal Verification

Programming language:
SystemVerilog

Required skills:
Model Checking, Abstraction, Reduction

Language:
English

Date of submission:
June 1, 2024

For more information please contact us:

Phone: +49 (89) 289 - 18140

E-Mail: tobias.ladner@tum.de

Website: www.ce.cit.tum.de/air/

References

[1] Matthias Althoff. An introduction to cora 2015. In *Proc. of the 1st and 2nd Workshop on Applied Verification for Continuous and Hybrid Systems*, pages 120–151. EasyChair, December 2015.

[2] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT press, 2008.

[3] Elaheh Ordoni, Jutta Mülle, and Klemens Böhm. Reduction of data-value-aware process models: A relevance-based approach. *Inf. Syst.*, 114(C), 3 2023.

[4] V. Paruthi, N. Mansouri, and R. Vemuri. Automatic data path abstraction for verification of large scale designs. In *Proceedings International Conference on Computer Design. VLSI in Computers and Processors*, pages 192–194, 1998.

[5] Aleksandr Zaks, Zijiang Yang, Ilya Shlyakhter, Franjo Ivancic, Srihari Cadambi, Malay K. Ganai, Aarti Gupta, and Pranav Ashar. Bitwidth reduction via symbolic interval analysis for software model checking. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 27(8):1513–1517, 2008.

Technical University of Munich

Department of Informatics

Chair of Robotics, Artificial Intelligence and Real-time Systems