Dedicated Solver for Formal Verification of Electric Circuits with Multiple Power Supplies

2022-2023

Keywords: SAT Solving; SMT Solving; Logical Formulas; Integrated Circuits; Solving with Custom Theory; Optimization; `OCaml`

Context

Aniah is a Start-up that offers tools for analyzing integrated circuits at an industrial scale[1]. Aniah has introduced algorithms that significantly pushes the boundaries of the size of analyzable circuits, from a few hundred thousand elements to several trillion. Aniah is starting a collaboration with the Laboratoire de l'Informatique du Parallélisme (LIP) and the Verimag laboratory to consolidate and generalize its approach by supplementing its practical results with a theoretical backbone. One of the objectives of this study is to explore the applicability of state-of-the-art model-checking techniques to the problem of circuit electric verification.

Model-checking [13] consists in exploring all the reachable states of a system, typically to check the unreachability of a set of error states. It is a well-established technique, and has successfully been applied both to software [1, 7, 6] and hardware [2, 4]. It is usually applied to check properties on the *behavior* of a system. For example, hardware model-checking usually considers boolean values (0 and 1, possibly extended with X and Z to model short-circuits and disconnected signals), but abstracts away the physical details (typically, voltage values are not modeled). Model-checking can be either enumerative (reachable states are explored one by one), or symbolic. Symbolic model-checking consists in representing a possibly very large set of states using a symbolic formula, that can be exponentially more efficient in terms of memory footprint. Common tools for symbolic model-checking are Binary Decision Diagrams (BDD) [5] and SAT-solvers [3] that allow manipulating boolean logical formulas. Satisfiability Modulo Theory (SMT) solvers extend SAT-solvers with non-boolean variables (e.g. rational numbers, integers, or other data structures). Among other work, these approaches have successfully been applied by the supervisors of this internship for Lustre program verification [10] and SystemC program verification [9].

Aniah proposed a graph based algorithm to detect electrical errors in a hierarchical design circuit. In this regard, the algorithm first assigns a finite set of values to the input variables of the circuit. Then, by analyzing the behavior of each net within the circuit, the algorithm detects electrical errors. One of the main issues in this analysis is the time and space complexity that is exponential with respect to the size of input variables. While the existing algorithm is usually fast enough in practice thanks to the good properties of the circuit topology, we are working on using symbolic model checking tools (BDD, SAT- and SMT-solvers) to speed up verification even more, as has been done in previous works [12, 11]. We currently have a prototype tool that compiles a circuit description into a logical formula comprising both numerical variables (representing voltage values) and booleans, that we solve using the Z3 [8] SMT solver. While Z3 is a very good SMT solver, we rely on an advanced theory to encode numerical values, while we only use numbers to encode a set of totally ordered values, without using any operation like addition or multiplication (we currently don't use subtraction, but may require it later to consider some properties over relative voltages).

Some SMT solvers like Sidekick (`https://github.com/c-cube/sidekick`) are parameterized by a theory: the user can use them to design an SMT solver for a given theory without the need to re-write a SAT-solver. A typical use of these solvers is to write solvers for a theory that

[1] `https://www.aniah.fr/`

is not managed by off-the-shelf solvers, but they can also be used to write minimalist theories in the hope of getting better performance than solvers for more complete theories.

Objectives of the internship

The objective of the internship is to implement a solver based on Sidekick, for the theory of ordered values (i.e. enumerated type with a total order, without arithmetic operations — beside maybe substraction). It is then expected that the candidate will:

- implement this theory in a Sidekick-based solver
- integrate this solver as a backend for our compiler, as an alternative to Z3
- experiment on various kinds of inputs to compare the performances of this solver with Z3
- if time allows, work on performance optimization of the tool

Context of the Collaboration and Physical Location

The internship is proposed as part of the collaboration between LIP laboratory (Lyon), Verimag laboratory (Grenoble), and Aniah company (Grenoble). A post-doc (Bruno Ferres) and a CIFRE Ph.D (Oussama Oulkaid) student are already working on the subject. The student recruited for this internship will interact closely with them. A continuation on a Ph.D on a related subject is possible if the student is motivated.

The internship is proposed by LIP, Verimag and Aniah. The physical location of the internship is to be discussed with applicants. The student will visit other sites and meetings with all co-supervisors will be organised frequently.

- Laboratoire de l'Informatique du Parallélisme (LIP) – École Normale Supérieure de Lyon.
- Laboratoire Verimag, Grenoble.
- Aniah, Grenoble.

Required profile

The candidate should be familiar with algorithm design, understand the basics of Boole's algebra and logic. Good programming skills are required for the experimental validation of the approach. Since Sidekick is implemented in OCaml, prior knowledge of OCaml is appreciated, but the student can learn OCaml's basics during the internship. While the application domain is electronics, no knowledge of electronics is required to perform this internship.

How to apply

Send an email to matthieu.moy@univ-lyon1.fr, Pascal.Raymond@univ-grenoble-alpes.fr, bruno.ferres@inria.fr and mehdi.khosravian@aniah.fr with your CV, a short text describing your motivation, and any document that can support your application.

Advisors

- Matthieu Moy, maître de conférences UCBL/LIP, `https://matthieu-moy.fr/`
- Pascal Raymond, chargé de recherche CNRS/Verimag, `http://www-verimag.imag.fr/~raymond/`
- Bruno Ferres, post-doct researcher at LIP, `https://perso.ens-lyon.fr/bruno.ferres`.
- Mehdi Khosravian, Algorithm engineer in Aniah, `https://www.linkedin.com/in/mehdikhosravian/`

References

[1] Thomas Ball, Vladimir Levin, and Sriram K Rajamani. A decade of software model checking with slam. *Communications of the ACM*, 54(7):68–76, 2011.

[2] Ilan Beer, Shoham Ben-David, Cindy Eisner, and Avner Landver. Rulebase: An industry-oriented formal verification tool. In *33rd Design Automation Conference Proceedings, 1996*, pages 655–660. IEEE, 1996.

[3] Armin Biere, Alessandro Cimatti, Edmund Clarke, and Yunshan Zhu. Symbolic model checking without bdds. In *International conference on tools and algorithms for the construction and analysis of systems*, pages 193–207. Springer, 1999.

[4] Aaron R Bradley. Sat-based model checking without unrolling. In *International Workshop on Verification, Model Checking, and Abstract Interpretation*, pages 70–87. Springer, 2011.

[5] Jerry R Burch, Edmund M Clarke, Kenneth L McMillan, David L Dill, and Lain-Jinn Hwang. Symbolic model checking: 1020 states and beyond. *Information and computation*, 98(2):142–170, 1992.

[6] Patrice Godefroid. Software model checking: The verisoft approach. *Formal Methods in System Design*, 26(2):77–101, 2005.

[7] Daniel Kroening and Michael Tautschnig. Cbmc–c bounded model checker. In *International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 389–391. Springer, 2014.

[8] Leonardo de Moura and Nikolaj Bjørner. Z3: An efficient smt solver. In *International conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340. Springer, 2008.

[9] Matthieu Moy, Florence Maraninchi, and Laurent Maillet-Contoz. Lussy: an open tool for the analysis of systems-on-a-chip at the transaction level. *Design Automation for Embedded Systems*, 10(2):73–104, 2005.

[10] Pascal Raymond. Synchronous program verification with lustre/lesar. *Modeling and Verification of Real-Time Systems*, page 7, 2008.

[11] S Rodriguez-Chavez, AA Palma-Rodriguez, E Tlelo-Cuautle, and SX-D Tan. Graph-based symbolic and symbolic sensitivity analysis of analog integrated circuits. In *Analog/RF and Mixed-Signal Circuit Systematic Design*, pages 101–122. Springer, 2013.

[12] Guoyong Shi. A survey on binary decision diagram approaches to symbolic analysis of analog integrated circuits. *Analog Integrated Circuits and Signal Processing*, 74(2):331–343, 2013.

[13] Wikipedia contributors. Model checking — Wikipedia, the free encyclopedia, 2021. [Online; accessed 21-September-2021].