Stratified Certification for k-Induction (Extended Abstract)

Emily Yu[1], Nils Froleyks[1], Armin Biere[2], Keijo Heljanko[3]
[1] Johannes Kepler University Linz, Austria [2] University of Freiburg, Germany [3] University of Helsinki, Finland

Abstract

Our certification framework from CAV'21 for bit-level k-induction-based model checking was shown to be effective in increasing the trust of verification results even though it partially involved quantifier reasoning. In this extended abstract we summarize our follow-up work presented at FMCAD'22. There we showed how to simplify the original approach by assuming reset functions to be stratified. This way we are able to lift it to word-level and in principle to other theories where quantifier reasoning is difficult. Our FMCAD'22 method requires six simple propositional satisfiability (SAT) checks and one polynomial-time check, allowing certification to remain in co-NP while the original approach required five SAT checks and checking one quantified Boolean formula (QBF). Experimental results show a substantial performance gain for the FMCAD'22 approach. We also presented and evaluated our new tool CERTIFAIGER-WL which is able to certify k-induction-based word-level model checking.

This extended abstract of our FMCAD'22 paper [21] and its long version on arXiv [22], which is follow-up work of our CAV'21 paper [20] serves as overview on our work on certification to the audience of the MBMV'23 workshop.

Introduction

Over the past several years, there has been growing interest in system verification using word-level reasoning. Satisfiability Modulo Theories (SMT) solvers for the theory of fixed-size bit-vectors are widely used for word-level reasoning [14, 15]. For example, word-level model checking has been an important part of the hardware model checking competitions since 2019. Given the theoretical and practical importance of word-level verification, a generic certification framework for it is necessary.

As quantified bit-vectors are challenging for SMT solvers and various works have focused on eliminating quantifiers in SMT [17, 15, 16]. our main goal was to generate certificates without the need to handle quantification.

Temporal induction (aka *k*-induction) [18] is a well-known model checking technique for verifying software and hardware systems. An attractive feature of *k*-induction is that it is natural to integrate it with modern SAT/SMT solvers, making it popular in both bit-level model checking and beyond [2, 4, 8], including word-level model checking.

Certification increases confidence in verification through model checking, which is important for both safety- and business-critical applications. Earlier work has focused on generating proofs for SAT-based model checking [3, 7, 9, 13, 19, 5, 23]. For example [6] and [5] proposed an approach to certify LTL properties and a few preprocessing techniques by generating deductive proofs.

In [21] we focus on finding an inductive invariant for *k*-induction. Unlike other SAT/SMT-based techniques such as IC3 [1] and interpolation [11, 12], *k*-induction does not automatically generate an inductive invariant as certificate [10]. In our CAV'21 work [20], certification of *k*-induction was achieved via five SAT checks together with a one-alternation QBF check, redirecting the certification problem to verifying an inductive invariant in an extended model that simulates the original one.

At the heart of the FMCAD'22 [21] contribution is the idea of reducing the certification method of *k*-induction to pure SAT checks, *i.e.,* eliminating the quantifiers. This enables us to complete the certification procedure at a lower complexity, and to directly apply the framework to word-level certification. We introduce the notion of stratified simulation which allows us to reason about the simulation relation between two systems.

This stratified simulation relation can be verified by three SAT and a polynomial-time check. The latter checks whether the reset function is indeed stratified. In addition, we presented a witness circuit construction which simulates the original under the stratified simulation relation thus creating a simpler and more elegant certification construction for *k*-induction.

Our CAV'21 approach [20] only focused on bit-level model checking, and as part of the FMCAD'22 paper [21] we lifted our method to word-level checking, implemented in a toolsuite CERTIFAIGER-WL. Experiments show practicality and effectiveness of certification for word-level models. For more details see our FMCAD'22 paper [21] and its extended version on arXiv [22].

Conclusion and Future Work

Our FMCAD'22 certification framework [21] can certify *k*-induction by six SAT and one polynomial-time check. We also lifted our approach to the word-level, and implemented our method in both contexts. Experimental results demonstrate the effectiveness and efficiency.

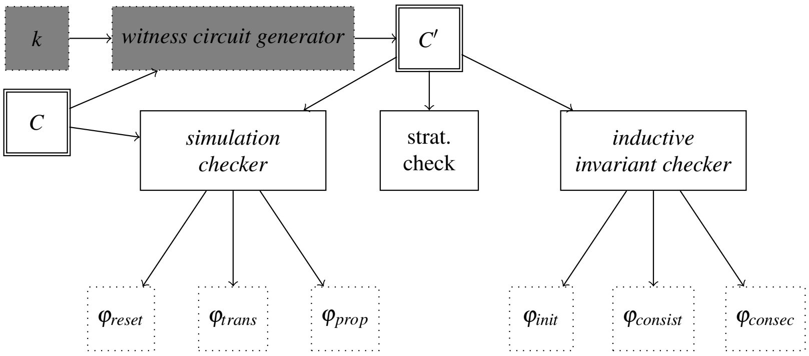

Figure 1 Given k, a model C and C' be the generated witness. The coloured area is specific to our approach for k-induction, and the rest corresponds to the general certification flow for inductive invariant checking [21].

Removal of the QBF quantifiers has reduced the theoretical complexity of the problem compared to [20] and also reduced the overall runtime overhead of the certification. In future work we plan to obtain formally verified certificate checkers by using theorem proving. How to certify liveness properties is important further research too.

References

[1] A. R. Bradley. SAT-based model checking without unrolling. In *VMCAI*, volume 6538 of *LNCS*, pages 70–87. Springer, 2011.

[2] A. Champion, A. Mebsout, C. Sticksel, and C. Tinelli. The Kind 2 model checker. In *CAV*, volume 9780 of *LNCS*, pages 510–517. Springer, 2016.

[3] S. Conchon, A. Mebsout, and F. Zaïdi. Certificates for parameterized model checking. In *FM*, volume 9109 of *LNCS*, pages 126–142. Springer, 2015.

[4] L. M. de Moura, S. Owre, H. Rueß, J. M. Rushby, N. Shankar, M. Sorea, and A. Tiwari. SAL 2. In *CAV*, volume 3114 of *LNCS*, pages 496–500. Springer, 2004.

[5] A. Griggio, M. Roveri, and S. Tonetta. Certifying proofs for LTL model checking. In *FMCAD*, pages 1–9. IEEE, 2018.

[6] A. Griggio, M. Roveri, and S. Tonetta. Certifying proofs for SAT-based model checking. *Formal Methods Syst. Des.*, 57(2):178–210, 2021.

[7] A. Gurfinkel and A. Ivrii. K-induction without unrolling. In *FMCAD*, pages 148–155. IEEE, 2017.

[8] D. Jovanovic and B. Dutertre. Property-directed k-induction. In *FMCAD*, pages 85–92. IEEE, 2016.

[9] T. Kuismin and K. Heljanko. Increasing confidence in liveness model checking results with proofs. In *HVC*, volume 8244 of *LNCS*, pages 32–43. Springer, 2013.

[10] Z. Manna and A. Pnueli. *Temporal verification of reactive systems - safety*. Springer, 1995.

[11] K. L. McMillan. Interpolation and SAT-based model checking. In *CAV*, volume 2725 of *LNCS*, pages 1–13. Springer, 2003.

[12] K. L. McMillan. An interpolating theorem prover. *Theor. Comput. Sci.*, 345(1):101–121, 2005.

[13] K. S. Namjoshi. Certifying model checkers. In *CAV*, volume 2102 of *LNCS*, pages 2–13. Springer, 2001.

[14] A. Niemetz, M. Preiner, and A. Biere. Precise and complete propagation based local search for satisfiability modulo theories. In *CAV*, volume 9779 of *LNCS*, pages 199–217. Springer, 2016.

[15] A. Niemetz, M. Preiner, and A. Biere. Propagation based local search for bit-precise reasoning. *Formal Methods Syst. Des.*, 51(3):608–636, 2017.

[16] A. Niemetz, M. Preiner, A. Reynolds, C. W. Barrett, and C. Tinelli. Solving quantified bit-vectors using invertibility conditions. In *CAV*, volume 10982 of *LNCS*, pages 236–255. Springer, 2018.

[17] A. Niemetz, M. Preiner, A. Reynolds, Y. Zohar, C. W. Barrett, and C. Tinelli. Towards satisfiability modulo parametric bit-vectors. *J. Autom. Reason.*, 65(7): 1001–1025, 2021.

[18] M. Sheeran, S. Singh, and G. Stålmarck. Checking safety properties using induction and a SAT-solver. In *FMCAD*, volume 1954 of *LNCS*, pages 108–125. Springer, 2000.

[19] L. G. Wagner, A. Mebsout, C. Tinelli, D. D. Cofer, and K. Slind. Qualification of a model checker for avionics software verification. In *NFM*, volume 10227 of *LNCS*, pages 404–419, 2017.

[20] E. Yu, A. Biere, and K. Heljanko. Progress in certifying hardware model checking results. In *CAV*, volume 12760 of *LNCS*, pages 363–386. Springer, 2021.

[21] E. Yu, N. Froleyks, A. Biere, and K. Heljanko. Stratified certification for k-induction. In *FMCAD*, volume 3, pages 59–64. TU Vienna Academic Press, 2022.

[22] E. Yu, N. Froleyks, A. Biere, and K. Heljanko. Stratified certification for k-induction, 2022. URL `https://arxiv.org/abs/2208.01443`.

[23] Z. Yu, A. Biere, and K. Heljanko. Certifying hardware model checking results. In *ICFEM*, volume 11852 of *LNCS*, pages 498–502. Springer, 2019.