Formal Methods in Computer-Aided Design 2022

Verification of Distributed Protocols: Decidable Modeling and Invariant Inference

Oded Padon
VMware Research
Palo Alto, CA, USA
oded.padon@gmail.com

Verification of distributed protocols and systems, where both the number of nodes in the systems and the state-space of each node are unbounded, is a long-standing research goal. In recent years, efforts around the Ivy verification tool [1]–[4] have pushed a strategy of modeling distributed protocols and systems in a new way that enables decidable deductive verification [5]–[8], i.e., given a candidate inductive invariant, it is possible to *automatically* check if it is inductive, and to produce a *finite* counterexample to induction in case it is not inductive. Complex protocols require quantifiers in both models and their invariants, including forall-exists quantifier alternations. Still, it is possible to obtain decidability by enforcing a stratification structure on quantifier alternations, often achieved using modular decomposition techniques, which are supported by Ivy. Stratified quantifiers lead not only to theoretical decidability, but to reliably good solver performance in practice, which is in contrast to the typical instability of SMT solvers over formulas with complex quantification.

Reliable automation of invariant checking and finite counterexamples open the path to automating invariant inference [9]. An invariant inference algorithm can propose a candidate invariant, automatically check it, and get a finite counterexample that can be used to inform the next candidate. For a complex protocol, this check would typically be performed thousands of times before an invariant is found, so reliable automation of invariant checking is a critical enabler. Recently, several invariant inference algorithms [9]–[18] have been developed that can find complex quantified invariants for challenging protocols, including Paxos and some of its most intricate variants.

In the tutorial I will provide an overview of Ivy's principles and techniques for modeling distributed protocols in a decidable fragment of first-order logic. I will then survey several recently developed invariant inference algorithms for quantified invariants, and present one such algorithm in depth: Primal-Dual Houdini [13]. Primal-Dual Houdini is based on a new mathematical duality, and is obtained by deriving the formal dual of the well-known Houdini algorithm. As a result, Primal-Dual Houdini possesses an interesting formal symmetry between the search for proofs and for counterexamples.

References

[1] O. Padon, K. L. McMillan, A. Panda, M. Sagiv, and S. Shoham, "Ivy: Safety verification by interactive generalization," in *PLDI 2016*. [Online]. Available: https://doi.org/10.1145/2908080.2908118

[2] K. L. McMillan and O. Padon, "Deductive verification in decidable fragments with ivy," in *SAS 2018*. [Online]. Available: https://doi.org/10.1007/978-3-319-99725-4_4

[3] ——, "Ivy: A multi-modal verification tool for distributed algorithms," in *CAV 2020*. [Online]. Available: https://doi.org/10.1007/978-3-030-53291-8_12

[4] K. L. McMillan, "Ivy," https://github.com/kenmcmil/ivy.

[5] O. Padon, G. Losa, M. Sagiv, and S. Shoham, "Paxos made EPR: decidable reasoning about distributed protocols," *OOPSLA 2017*. [Online]. Available: https://doi.org/10.1145/3140568

[6] M. Taube, G. Losa, K. L. McMillan, O. Padon, M. Sagiv, S. Shoham, J. R. Wilcox, and D. Woos, "Modularity for decidability of deductive verification with applications to distributed systems," in *PLDI 2018*. [Online]. Available: https://doi.org/10.1145/3192366.3192414

[7] O. Padon, J. Hoenicke, G. Losa, A. Podelski, M. Sagiv, and S. Shoham, "Reducing liveness to safety in first-order logic," *POPL 2018*. [Online]. Available: https://doi.org/10.1145/3158114

[8] O. Padon, J. Hoenicke, K. L. McMillan, A. Podelski, M. Sagiv, and S. Shoham, "Temporal prophecy for proving temporal properties of infinite-state systems," *Formal Methods Syst. Des.*, vol. 57, no. 2, pp. 246–269, 2021. [Online]. Available: https://doi.org/10.1007/s10703-021-00377-1

[9] A. Karbyshev, N. S. Bjørner, S. Itzhaky, N. Rinetzky, and S. Shoham, "Property-directed inference of universal invariants or proving their absence," *J. ACM*, vol. 64, no. 1, pp. 7:1–7:33, 2017. [Online]. Available: https://doi.org/10.1145/3022187

[10] Y. M. Y. Feldman, J. R. Wilcox, S. Shoham, and M. Sagiv, "Inferring inductive invariants from phase structures," in *CAV 2019*. [Online]. Available: https://doi.org/10.1007/978-3-030-25543-5_23

[11] J. R. Koenig, O. Padon, N. Immerman, and A. Aiken, "First-order quantified separators," in *PLDI 2020*. [Online]. Available: https://doi.org/10.1145/3385412.3386018

[12] J. R. Koenig, O. Padon, S. Shoham, and A. Aiken, "Inferring invariants with quantifier alternations: Taming the search space explosion," in *TACAS 2022*. [Online]. Available: https://doi.org/10.1007/978-3-030-99524-9_18

[13] O. Padon, J. R. Wilcox, J. R. Koenig, K. L. McMillan, and A. Aiken, "Induction duality: primal-dual search for invariants," *POPL 2022*. [Online]. Available: https://doi.org/10.1145/3498712

[14] H. Ma, A. Goel, J. Jeannin, M. Kapritsos, B. Kasikci, and K. A. Sakallah, "I4: incremental inference of inductive invariants for verification of distributed protocols," in *SOSP 2019*. [Online]. Available: https://doi.org/10.1145/3341301.3359651

[15] T. Hance, M. Heule, R. Martins, and B. Parno, "Finding invariants of distributed systems: It's a small (enough) world after all," in *NSDI 2021*. [Online]. Available: https://www.usenix.org/conference/nsdi21/presentation/hance

[16] A. Goel and K. A. Sakallah, "On symmetry and quantification: A new approach to verify distributed protocols," in *NFM 2021*. [Online]. Available: https://doi.org/10.1007/978-3-030-76384-8_9

[17] J. Yao, R. Tao, R. Gu, J. Nieh, S. Jana, and G. Ryan, "DistAI: Data-driven automated invariant learning for distributed protocols," in *OSDI 2021*. [Online]. Available: https://www.usenix.org/conference/osdi21/presentation/yao

[18] J. Yao, R. Tao, R. Gu, and J. Nieh, "DuoAI: Fast, automated inference of inductive invariants for verifying distributed protocols," in *OSDI 2022*. [Online]. Available: https://www.usenix.org/conference/osdi22/presentation/yao

https://doi.org/10.34727/2022/isbn.978-3-85448-053-2_4