IC3 and beyond: Incremental, Inductive Verification

Aaron R. Bradley

ECEE Department, University of Colorado at Boulder
bradleya@colorado.edu

IC3, a SAT-based safety model checking algorithm introduced in 2010 [1, 2], is considered among the best safety model checkers. This tutorial discusses its essential ideas: the use of concrete states, called counterexamples to induction, to motivate lemma discovery; the incremental application of induction to generate the lemmas; and the use of stepwise assumptions to allow dynamic shifting between inductive lemma generation and propagation of lemmas as predicates.

Two perspectives on IC3 are offered: IC3 as proof finder, which highlights its ability to find mutually inductive lemmas, a crucial element of its robustness; and IC3 as bug finder, which shows that IC3's choices with respect to proof obligations result in a heuristically guided search. The latter perspective casts lemmas as refinements of estimates of states' proximities to initial states. These estimates guide the backward construction of potential counterexample traces.

IC3's context is then discussed: its evolution from earlier work and how it compares to other algorithms. Finally, the broader idea of incremental, inductive verification (IIV), of which IC3 is just one example, is explored. The IIV perspective has motivated new algorithms for analyzing ω-regular properties [4] and CTL properties [5].

A recent tutorial paper [3] provides a conceptual exposition of IC3, while an earlier tutorial paper [6] illustrates IC3's workings through detailed examples.

References

[1] Bradley, A.R.: k-step relative inductive generalization. Technical report, CU Boulder (March 2010), http://arxiv.org/abs/1003.3649
[2] Bradley, A.R.: SAT-Based Model Checking without Unrolling. In: Jhala, R., Schmidt, D. (eds.) VMCAI 2011. LNCS, vol. 6538, pp. 70–87. Springer, Heidelberg (2011)
[3] Bradley, A.R.: Understanding IC3. In: SAT (June 2012)
[4] Bradley, A.R., Somenzi, F., Hassan, Z., Zhang, Y.: An incremental approach to model checking progress properties. In: FMCAD (November 2011)
[5] Hassan, Z., Bradley, A.R., Somenzi, F.: Incremental, Inductive CTL Model Checking. In: Madhusudan, P., Seshia, S.A. (eds.) CAV 2012. LNCS, vol. 7358, p. 4. Springer, Heidelberg (2012)
[6] Somenzi, F., Bradley, A.R.: IC3: Where monolithic and incremental meet. In: FMCAD (November 2011)

P. Madhusudan and S.A. Seshia (Eds.): CAV 2012, LNCS 7358, p. 4, 2012.