Better generalization in IC3

Type	Conference Paper
Author	Zyad Hassan
Author	Aaron R. Bradley
Author	Fabio Somenzi
Abstract	An improved clause generalization procedure for IC3 is presented. Whereas standard generalization extracts a relatively inductive clause from a single state, called a counterexample to induction (CTI), the new procedure also extracts such clauses from other states, called counterexamples to generalization (CTG), that interfere with the primary generalization attempt. The motivation is to enable IC3 to explore states farther from the error states than are CTIs while remaining property-focused. CTGs are strong candidates for being farther but still backward reachable. Significant reductions in the maximum depth reached by IC3's priority queue-directed explicit backward search indicate that this intention is achieved in practice. The effectiveness of the new procedure is established in two independent implementations of IC3, which demonstrate an increase of 17 and 27, respectively, in the number of solved HWMCC benchmarks.
Date	2013-10
Library Catalog	IEEE Xplore
Pages	157-164
Proceedings Title	2013 Formal Methods in Computer-Aided Design
Conference Name	2013 Formal Methods in Computer-Aided Design
DOI	10.1109/FMCAD.2013.6679405
Date Added	4/6/2022, 10:10:01 AM
Modified	4/6/2022, 10:10:01 AM

Attachments

- Hassan2013_Better_generalization_in_IC3.pdf

Efficient implementation of property directed reachability

Type	Conference Paper
Author	Niklas Een
Author	Alan Mishchenko
Author	Robert Brayton
Abstract	Last spring, in March 2010, Aaron Bradley published the first truly new bit-level symbolic model checking algorithm since Ken McMillan's interpolation based model checking procedure introduced in 2003. Our experience with the algorithm suggests that it is stronger than interpolation on industrial problems, and that it is an important algorithm to study further. In this paper, we present a simplified and faster implementation of Bradley's procedure, and discuss our successful and unsuccessful attempts to improve it.
Date	October 30, 2011
Library Catalog	ACM Digital Library
Accessed	4/5/2022, 6:00:00 PM
Place	Austin, Texas
Publisher	FMCAD Inc
ISBN	978-0-9835678-1-3
Pages	125–134
Series	FMCAD '11
Proceedings Title	Proceedings of the International Conference on Formal Methods in Computer-Aided Design

Date Added 4/4/2022, 5:14:41 PM
Modified 4/9/2022, 3:34:42 PM

Attachments

- Een2011_Efficient_implementation_of_property_directed_reachability.pdf

---

Exploiting SMT for Verification of Infinite-State Systems

Type Presentation
Presenter Alberto Griggio
Date 2015
Meeting Name VTSA summer school 2015
Date Added 4/5/2022, 12:30:44 PM
Modified 4/6/2022, 10:11:06 AM

Attachments

- Griggio2015_Exploiting_SMT_for_Verification_of_Infinite-State_Systems.pdf

---

IC3 software model checking

Type Journal Article
Author Tim Lange
Author Martin R. Neuhäußer
Author Thomas Noll
Author Joost-Pieter Katoen
Abstract In recent years, the inductive, incremental verification algorithm IC3 had a major impact on hardware model checking. Also for software model checking, a number of adaptations of Boolean IC3 and combinations with CEGAR and ART-based techniques have been developed. However, most of them exploit the peculiarities of software programs, such as the explicit representation of control flow, only to a limited extent. In this paper, we present an approach that supports this explicit representation in the form of control-flow automata, and integrates it with symbolic reasoning about the data state space of the program. By maintaining reachability information specifically for each control location, we arrive at a “two-dimensional” extension of IC3, which provides a true lifting from hardware to software model checking. Moreover, we address the problem of generalization in this setting, an essential feature to ensure the scalability of IC3. We introduce several improvements that range from efficient caching of generalizations over variable reductions to syntax-oriented generalization by means of weakest preconditions. Using a prototypical implementation, we evaluate our approach on a number of case studies, including a significant subset of the SV-COMP 2018 benchmarks, and compare the outcomes with results obtained from other IC3 software model checkers.
Date 04/2020
Language en
Library Catalog DOI.org (Crossref)
URL http://link.springer.com/10.1007/s10009-019-00547-x
Accessed 4/5/2022, 9:59:41 AM
Volume 22
Pages 135-161
Publication International Journal on Software Tools for Technology Transfer
DOI 10.1007/s10009-019-00547-x
Issue 2

Journal Abbr Int J Softw Tools Technol Transfer
ISSN 1433-2779, 1433-2787
Date Added 4/5/2022, 9:59:41 AM
Modified 4/5/2022, 9:59:41 AM

Attachments

- Lange2020_IC3_software_model_checking.pdf

Incremental design-space model checking via reusable reachable state approximations

Type Journal Article
Author Rohit Dureja
Author Kristin Y. Rozier
Date 2022-02-05
Language en
Library Catalog DOI.org (Crossref)
URL https://link.springer.com/10.1007/s10703-022-00389-5
Accessed 4/6/2022, 10:19:04 AM
Publication Formal Methods in System Design
DOI 10.1007/s10703-022-00389-5
Journal Abbr Form Methods Syst Des
ISSN 0925-9856, 1572-8102
Date Added 4/6/2022, 10:19:04 AM
Modified 7/1/2022, 3:34:26 PM

Attachments

- Dureja2022_Incremental_design-space_model_checking_via_reusable_reachable_state.pdf

---

Infinite-state invariant checking with IC3 and predicate abstraction

Type Journal Article
Author Alessandro Cimatti
Author Alberto Griggio
Author Sergio Mover
Author Stefano Tonetta
Abstract We address the problem of verifying invariant properties on infinite-state systems. We present a novel approach, IC3ia, for generalizing the IC3 invariant checking algorithm from finite-state to infinite-state transition systems, expressed over some background theories. The procedure is based on a tight integration of IC3 with Implicit Abstraction, a form of predicate abstraction that expresses abstract paths without computing explicitly the abstract system. In this scenario, IC3 operates only at the Boolean level of the abstract state space, discovering inductive clauses over the abstraction predicates. Theory reasoning is confined within the underlying SMT solver, and applied transparently when performing satisfiability checks. When the current abstraction allows for a spurious counterexample, it is refined by discovering and adding a sufficient set of new predicates. Importantly, this can be done in a completely incremental manner, without discarding the clauses found in the previous search. The proposed approach has two key advantages. First, unlike previous SMT generalizations of IC3, it allows to handle a wide range of background theories without relying on ad-hoc extensions, such as quantifier elimination or theory-specific clause generalization procedures, which might not always be available and are often highly inefficient. Second, compared to a direct exploration of the concrete transition system, the use of

abstraction gives a significant performance improvement, as our experiments demonstrate.

Date 2016-12-01
Language en
Library Catalog Springer Link
URL https://doi.org/10.1007/s10703-016-0257-4
Accessed 4/4/2022, 6:36:55 PM
Volume 49
Pages 190-218
Publication Formal Methods in System Design
DOI 10.1007/s10703-016-0257-4
Issue 3
Journal Abbr Form Methods Syst Des
ISSN 1572-8102
Date Added 4/4/2022, 6:36:55 PM
Modified 4/4/2022, 6:36:55 PM

Attachments

- Cimatti2016_Infinite-state_invariant_checking_with_IC3_and_predicate_abstraction.pdf

---

Interpolating Property Directed Reachability

Type Conference Paper
Author Yakir Vizel
Author Arie Gurfinkel
Editor Armin Biere
Editor Roderick Bloem
Abstract Current SAT-based Model Checking is based on two major approaches: Interpolation-based (Imc) (global, with unrollings) and Property Directed Reachability/IC3 (Pdr) (local, without unrollings). Imc generates candidate invariants using interpolation over an unrolling of a system, without putting any restrictions on the SAT-solver's search. Pdr generates candidate invariants by a local search over a single instantiation of the transition relation, effectively guiding the SAT solver's search. The two techniques are considered to be orthogonal and have different strength and limitations. In this paper, we present a new technique, called Avy, that effectively combines the key insights of the two approaches. Like Imc, it uses unrollings and interpolants to construct an initial candidate invariant, and, like Pdr, it uses local inductive generalization to keep the invariants in compact clausal form. On the one hand, Avy is an incremental Imc extended with a local search for CNF interpolants. On the other, it is Pdr extended with a global search for bounded counterexamples. We implemented the technique using ABC and have evaluated it on the HWMCC benchmark-suite from 2012 and 2013. Our results show that the prototype significantly outperforms Pdr and McMillan's interpolation algorithm (as implemented in ABC) on the industrial sub-category of the benchmark.
Date 2014
Language english
Place Cham
Publisher Springer International Publishing
ISBN 978-3-319-08867-9
Pages 260–276
Series Lecture Notes in Computer Science
Proceedings Title Computer Aided Verification
DOI 10.1007/978-3-319-08867-9_17
Date Added 4/4/2022, 5:14:33 PM

Modified 4/4/2022, 7:02:11 PM

Attachments

- Vizel2014_Interpolating_Property_Directed_Reachability.pdf

Interpolating Strong Induction

Type Book Section
Editor Isil Dillig
Editor Serdar Tasiran
Author Hari Govind Vediramana Krishnan
Author Yakir Vizel
Author Vijay Ganesh
Author Arie Gurfinkel
Abstract The principle of strong induction, also known as k-induction is one of the first techniques for unbounded SAT-based Model Checking (SMC). While elegant and simple to apply, properties as such are rarely k-inductive and when they can be strengthened, there is no effective strategy to guess the depth of induction. It has been mostly displaced by techniques that compute inductive strengthenings based on interpolation and property directed reachability (Pdr). In this paper, we present kAvy, an SMC algorithm that effectively uses k-induction to guide interpolation and Pdr-style inductive generalization. Unlike pure k-induction, kAvy uses Pdr-style generalization to compute and strengthen an inductive trace. Unlike pure Pdr, kAvy uses relative k-induction to construct an inductive invariant. The depth of induction is adjusted dynamically by minimizing a proof of unsatisfiability. We have implemented kAvy within the Avy Model Checker and evaluated it on HWMCC instances. Our results show that kAvy is more effective than both Avy and Pdr, and that using k-induction leads to faster running time and solving more instances. Further, on a class of benchmarks, called shift, kAvy is orders of magnitude faster than Avy, Pdr and k-induction.
Date 2019
Language en
Library Catalog DOI.org (Crossref)
URL http://link.springer.com/10.1007/978-3-030-25543-5_21
Accessed 4/5/2022, 9:43:33 AM
Extra Series Title: Lecture Notes in Computer Science DOI: 10.1007/978-3-030-25543-5_21
Volume 11562
Place Cham
Publisher Springer International Publishing
ISBN 978-3-030-25542-8 978-3-030-25543-5
Pages 367-385
Book Title Computer Aided Verification
Date Added 4/5/2022, 9:43:34 AM
Modified 4/5/2022, 10:18:30 AM

Attachments

- Vediramana_Krishnan2019_Interpolating_Strong_Induction.pdf

Interpolation in SMT and in Verification

Type Presentation
Presenter Alberto Griggio

Date 2015
Language en
Extra Exploiting SMT for Verification of Infinite-State Systems
Meeting Name VTSA summer school
Date Added 4/5/2022, 9:33:21 AM
Modified 4/9/2022, 3:35:58 PM

Attachments

- Griggio2015_Interpolation_in_SMT_and_in_Verification.pdf

Making PROGRESS in Property Directed Reachability

Type Conference Paper
Author Tobias Seufert
Author Christoph Scholl
Author Arun Chandrasekharan
Author Sven Reimer
Author Tobias Welp
Editor Bernd Finkbeiner
Editor Thomas Wies
Abstract With (PROGRESS) we present a fully automatic and complete approach for Hardware Model Checking under restrictions. We use the PROGRESS approach in the context of PDR/IC3 [9, 18]. Our implementation of PDR/IC3 restricts input signals as well as state bits of a circuit to constants in order to quickly explore long execution paths of the design. We are able to identify spurious proofs of safety along the way and exploit information from these proofs to guide the relaxation of the restrictions. Hence, we greatly improve the capability of PDR to find counterexamples, especially with long error paths. In experiments with HWMCC benchmarks our approach is able to double the amount of detected deep counterexamples in comparison to Bounded Model Checking as well as in comparison to PDR.
Date 2022
Language en
Library Catalog Springer Link
Place Cham
Publisher Springer International Publishing
ISBN 978-3-030-94583-1
Pages 355-377
Proceedings Title Verification, Model Checking, and Abstract Interpretation
DOI 10.1007/978-3-030-94583-1_18
Date Added 4/4/2022, 4:50:30 PM
Modified 7/19/2022, 10:14:51 AM

Attachments

- Seufert2022_Making_PROGRESS_in_Property_Directed_Reachability.pdf

---

PrIC3: Property Directed Reachability for MDPs

Type Conference Paper
Editor Shuvendu K. Lahiri
Editor Chao Wang

Author Kevin Batz
Author Sebastian Junges
Author Benjamin Lucien Kaminski
Author Joost-Pieter Katoen
Author Christoph Matheja
Author Philipp Schröer
Abstract IC3 has been a leap forward in symbolic model checking. This paper proposes PrIC3 (pronounced pricy-three), a conservative extension of IC3 to symbolic model checking of MDPs. Our main focus is to develop the theory underlying PrIC3. Alongside, we present a first implementation of PrIC3 including the key ingredients from IC3 such as generalization, repushing, and propagation.
Date 2020
Language en
Short Title PrIC3
Library Catalog DOI.org (Crossref)
URL http://link.springer.com/10.1007/978-3-030-53291-8_27
Accessed 4/5/2022, 9:41:55 AM
Extra Series Title: Lecture Notes in Computer Science
Volume 12225
Place Cham
Publisher Springer International Publishing
ISBN 978-3-030-53290-1 978-3-030-53291-8
Pages 512-538
Proceedings Title Computer Aided Verification
DOI 10.1007/978-3-030-53291-8_27
Date Added 4/4/2022, 5:21:54 PM
Modified 4/5/2022, 12:03:27 PM

Attachments

- Batz2020_PrIC3.pdf

Property Directed Abstract Interpretation

Type Book Section
Editor Barbara Jobstmann
Editor K. Rustan M. Leino
Author Noam Rinetzky
Author Sharon Shoham
Abstract Recently, Bradley proposed the PDR/IC3 model checking algorithm for verifying safety properties, where forward and backward reachability analyses are intertwined, and guide each other. Many variants of Bradley's original algorithm have been developed and successfully applied to both hardware and software verification. However, these algorithms have been presented in an operational manner, in disconnect with the rich literature concerning the theoretical foundation of static analysis formulated by abstract interpretation.
Date 2016
Language en
Library Catalog DOI.org (Crossref)
URL http://link.springer.com/10.1007/978-3-662-49122-5_5
Accessed 4/5/2022, 9:43:39 AM
Extra Series Title: Lecture Notes in Computer Science DOI: 10.1007/978-3-662-49122-5_5

Volume 9583
Place Berlin, Heidelberg
Publisher Springer Berlin Heidelberg
ISBN 978-3-662-49121-8 978-3-662-49122-5
Pages 104-123
Book Title Verification, Model Checking, and Abstract Interpretation
Date Added 4/5/2022, 9:43:40 AM
Modified 4/5/2022, 9:43:42 AM

Attachments

- Rinetzky2016_Property_Directed_Abstract_Interpretation.pdf

Property directed reachability with word-level abstraction

Type Conference Paper
Author Yen-Sheng Ho
Author Alan Mishchenko
Author Robert Brayton
Abstract SAT-based Property Directed Reachability (PDR) has become the key algorithmic development for unbounded model checking of gate-level sequential circuits, but it can be inefficient when applied to word-level problems with heavy arithmetic logic. To address this issue, word-level abstraction is often performed by replacing a whole set of signals with unconstrained new primary inputs. This paper introduces PDR-WLA, a wordlevel abstraction-refinement algorithm integrated into a modified PDR implementation. The algorithm uses efficient refinement and re-uses reachability information across iterations of refinement. PDR-WLA was implemented in ABC and evaluated on a large set of industrial Verilog designs. Experimental results show significant speedups on hard problems compared to the original PDR and to a naive word-level abstraction-refinement method.
Date 10/2017
Language en
Library Catalog DOI.org (Crossref)
URL http://ieeexplore.ieee.org/document/8102251/
Accessed 4/5/2022, 9:43:16 AM
Place Vienna
Publisher IEEE
ISBN 978-0-9835678-7-5
Pages 132-139
Proceedings Title 2017 Formal Methods in Computer Aided Design (FMCAD)
Conference Name 2017 Formal Methods in Computer-Aided Design (FMCAD)
DOI 10.23919/FMCAD.2017.8102251
Date Added 4/4/2022, 5:14:56 PM
Modified 7/18/2022, 11:01:24 AM

Attachments

- Ho2017_Property_directed_reachability_with_word-level_abstraction.pdf

---

Property-directed incremental invariant generation

Type Journal Article

Author Aaron R. Bradley

Author Zohar Manna

Abstract A fundamental method of analyzing a system such as a program or a circuit is invariance analysis, in which one proves that an assertion holds on all reachable states. Typically, the proof is performed via induction; however, an assertion, while invariant, may not be inductive (provable via induction). Invariant generation procedures construct auxiliary inductive assertions for strengthening the assertion to be inductive. We describe a general method of generating invariants that is incremental and property-directed. Rather than generating one large auxiliary inductive assertion, our method generates many simple assertions, each of which is inductive relative to those generated before it. Incremental generation is amenable to parallelization. Our method is also property-directed in that it generates inductive assertions that are relevant for strengthening the given assertion. We describe two instances of our method: a procedure for generating clausal invariants of finite-state systems and a procedure for generating affine inequalities of numerical infinite-state systems. We provide evidence that our method scales to checking safety properties of some large finite-state systems.

Date 07/2008

Language en

Library Catalog DOI.org (Crossref)

URL https://dl.acm.org/doi/10.1007/s00165-008-0080-9

Accessed 4/5/2022, 9:42:38 AM

Volume 20

Pages 379-405

Publication Formal Aspects of Computing

DOI 10.1007/s00165-008-0080-9

Issue 4-5

Journal Abbr Form. Asp. Comput.

ISSN 0934-5043, 1433-299X

Date Added 4/5/2022, 9:42:38 AM

Modified 4/5/2022, 9:53:29 AM

Attachments

- Bradley2008_Property-directed_incremental_invariant_generation.pdf

---

Property-Directed Inference of Universal Invariants or Proving Their Absence

Type Journal Article

Author Aleksandr Karbyshev

Author Nikolaj Bjørner

Author Shachar Itzhaky

Author Noam Rinetzky

Author Sharon Shoham

Abstract We present Universal Property Directed Reachability (PDR ∀), a property-directed semi-algorithm for automatic inference of invariants in a universal fragment of first-order logic. PDR ∀ is an extension of Bradley's PDR/IC3 algorithm for inference of propositional invariants. PDR ∀ terminates when it discovers a concrete counterexample, infers an inductive universal invariant strong enough to establish the desired safety property, or finds a proof that such an invariant does not exist . PDR ∀ is not guaranteed to terminate. However, we prove that under certain conditions, for example, when reasoning about programs manipulating singly linked lists, it does. We implemented an analyzer based on PDR ∀ and applied it to a collection of list-manipulating programs. Our analyzer was able to automatically infer universal invariants strong enough to establish memory safety and certain functional correctness properties, show the absence of such invariants for certain natural programs and specifications, and detect bugs. All this without the need for user-supplied abstraction predicates.

Date 2017-03-29

Language	en
Library Catalog	DOI.org (Crossref)
URL	https://dl.acm.org/doi/10.1145/3022187
Accessed	4/5/2022, 9:43:26 AM
Volume	64
Pages	1-33
Publication	Journal of the ACM
DOI	10.1145/3022187
Issue	1
Journal Abbr	J. ACM
ISSN	0004-5411, 1557-735X
Date Added	4/5/2022, 9:43:26 AM
Modified	4/5/2022, 9:43:26 AM

Attachments

- Karbyshev2017_Property-Directed_Inference_of_Universal_Invariants_or_Proving_Their_Absence.pdf

---

Property-Directed Reachability as Abstract Interpretation in the Monotone Theory

Type	Journal Article
Author	Yotam M. Y. Feldman
Author	Mooly Sagiv
Author	Sharon Shoham
Author	James R. Wilcox
Abstract	Inferring inductive invariants is one of the main challenges of formal verification. The theory of abstract interpretation provides a rich framework to devise invariant inference algorithms. One of the latest breakthroughs in invariant inference is property-directed reachability (PDR), but the research community views PDR and abstract interpretation as mostly unrelated techniques. This paper shows that, surprisingly, propositional PDR can be formulated as an abstract interpretation algorithm in a logical domain. More precisely, we define a version of PDR, called Λ-PDR, in which all generalizations of counterexamples are used to strengthen a frame. In this way, there is no need to refine frames after their creation, because all the possible supporting facts are included in advance. We analyze this algorithm using notions from Bshouty's monotone theory, originally developed in the context of exact learning. We show that there is an inherent overapproximation between the algorithm's frames that is related to the monotone theory. We then define a new abstract domain in which the best abstract transformer performs this overapproximation, and show that it captures the invariant inference process, i.e., Λ-PDR corresponds to Kleene iterations with the best transformer in this abstract domain. We provide some sufficient conditions for when this process converges in a small number of iterations, with sometimes an exponential gap from the number of iterations required for naive exact forward reachability. These results provide a firm theoretical foundation for the benefits of how PDR tackles forward reachability.
Date	2022-01-18
Language	en
Library Catalog	arXiv.org
URL	http://arxiv.org/abs/2111.00324
Accessed	4/5/2022, 9:42:48 AM
Extra	arXiv: 2111.00324
Publication	arXiv:2111.00324 [cs]
Date Added	4/5/2022, 9:42:49 AM
Modified	7/18/2022, 11:01:13 AM

Notes:

Extended version of a POPL 2022 paper: https://dl.acm.org/doi/10.1145/3498676

Attachments

- Feldman2022_Property-Directed_Reachability_as_Abstract_Interpretation_in_the_Monotone_Theory.pdf

---

QF_BV Model Checking with Property Directed Reachability

Type	Conference Paper
Author	Tobias Welp
Author	Andreas Kuehlmann
Abstract	In 2011, property directed reachability (PDR) was proposed as an efficient algorithm to solve hardware model checking problems. Recent experimentation suggests that it outperforms interpolationbased verification, which had been considered the best known algorithm for this purpose for almost a decade. In this work, we present a generalization of PDR to the theory of quantifier free formulae over bitvectors (QF BV), illustrate the new algorithm with representative examples and provide experimental results obtained from experimentation with a prototype implementation.
Date	2013
Language	en
Library Catalog	DOI.org (Crossref)
URL	http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6513614
Accessed	4/5/2022, 9:44:05 AM
Place	Grenoble, France
Publisher	IEEE Conference Publications
ISBN	978-1-4673-5071-6
Pages	791-796
Proceedings Title	Design, Automation & Test in Europe Conference & Exhibition (DATE), 2013
Conference Name	Design Automation and Test in Europe
DOI	10.7873/DATE.2013.168
Date Added	4/5/2022, 9:44:05 AM
Modified	4/5/2022, 9:55:51 AM

Attachments

- Welp2013_QF_BV_Model_Checking_with_Property_Directed_Reachability.pdf

---

Safety model checking with complementary approximations

Type	Conference Paper
Author	Jianwen Li
Author	Shufang Zhu
Author	Yueling Zhang
Author	Geguang Pu
Author	Moshe Y. Vardi
Abstract	Formal-verification techniques, such as model checking, are becoming popular in hardware design. SAT-based model checking techniques, such as IC3/PDR, have gained a significant success in the hardware industry. In this paper, we present a new framework for SAT-based safety model checking, named Complementary Approximate Reachability (CAR). CAR is based on standard reachability analysis, but

	instead of maintaining a single sequence of reachable-state sets, CAR maintains two sequences of over- and under-approximate reachable-state sets, checking safety and unsafety at the same time. To construct the two sequences, CAR uses standard Boolean-reasoning algorithms, based on satisfiability solving, one to find a satisfying cube of a satisfiable Boolean formula, and one to provide a minimal unsatisfiable core of an unsatisfiable Boolean formula. We applied CAR to 548 hardware model-checking instances, and compared its performance with IC3/PDR. Our results show that CAR is able to solve 42 instances that cannot be solved by IC3/PDR. When evaluated against a portfolio that includes IC3/PDR and other approaches, CAR is able to solve 21 instances that the other approaches cannot solve. We conclude that CAR should be considered as a valuable member of any algorithmic portfolio for safety model checking.
Date	2017-11
URL	https://ieeexplore-ieee-org.dist.lib.usu.edu/document/8203765
Extra	ISSN: 1558-2434
Pages	95-100
Proceedings Title	2017 IEEE/ACM international conference on computer-aided design (ICCAD)
DOI	10.1109/ICCAD.2017.8203765
Date Added	4/4/2022, 5:14:35 PM
Modified	4/4/2022, 5:17:57 PM

Attachments

- Li2017_Safety_model_checking_with_complementary_approximations.pdf

---

SAT-Based Model Checking without Unrolling

Type	Conference Paper
Author	Aaron R. Bradley
Editor	Ranjit Jhala
Editor	David Schmidt
Abstract	A new form of SAT-based symbolic model checking is described. Instead of unrolling the transition relation, it incrementally generates clauses that are inductive relative to (and augment) stepwise approximate reachability information. In this way, the algorithm gradually refines the property, eventually producing either an inductive strengthening of the property or a counterexample trace. Our experimental studies show that induction is a powerful tool for generalizing the unreachability of given error states: it can refine away many states at once, and it is effective at focusing the proof search on aspects of the transition system relevant to the property. Furthermore, the incremental structure of the algorithm lends itself to a parallel implementation.
Date	2011
Language	english
Place	Berlin, Heidelberg
Publisher	Springer
ISBN	978-3-642-18275-4
Pages	70–87
Series	Lecture Notes in Computer Science
Proceedings Title	Verification, Model Checking, and Abstract Interpretation
DOI	10.1007/978-3-642-18275-4_7
Date Added	4/4/2022, 5:14:45 PM
Modified	7/19/2022, 10:14:19 AM

Attachments

- Bradley2011_SAT-Based_Model_Checking_without_Unrolling.mp4

Sequential Verification Using Reverse PDR

Type Journal Article
Author Tobias Seufert
Author Christoph Scholl
Abstract In the last few years IC3 resp. PDR made a great stir as a SAT-based hardware verification approach without needing to unroll the transition relation as in Bounded Model Checking (BMC). Motivated by different strengths of forward and backward traversal observed in BDD based model checking, we consider Reverse PDR which starts its analysis with the initial states instead of the unsafe states as in original PDR. We show great benefits of Reverse PDR both by a theoretical and an experimental analysis. Finally, we profit from parallelism offered by modern multi-core processors and use a portfolio approach combining the advantages of Reverse and original PDR.
Language en
Library Catalog Zotero
Pages 11
Date Added 4/5/2022, 9:43:46 AM
Modified 4/5/2022, 9:43:46 AM

Attachments

- SeufertSequential_Verification_Using_Reverse_PDR.pdf

SMT-based Unbounded Model Checking with IC3 and Approximate QE

Type Journal Article
Author Cesare Tinelli
Language en
Library Catalog Zotero
Pages 70
Date Added 4/5/2022, 10:00:23 AM
Modified 4/5/2022, 10:00:23 AM

Attachments

- TinelliSMT-based_Unbounded_Model_Checking_with_IC3_and_Approximate_QE.pdf

Software Model Checking via IC3

Type Conference Paper
Series Editor David Hutchison
Series Editor Takeo Kanade
Series Editor Josef Kittler
Series Editor Jon M. Kleinberg
Series Editor Friedemann Mattern
Series Editor John C. Mitchell
Series Editor Moni Naor
Series Editor Oscar Nierstrasz
Series Editor C. Pandu Rangan
Series Editor Bernhard Steffen

Series Editor	Madhu Sudan
Series Editor	Demetri Terzopoulos
Series Editor	Doug Tygar
Series Editor	Moshe Y. Vardi
Series Editor	Gerhard Weikum
Editor	P. Madhusudan
Editor	Sanjit A. Seshia
Author	Alessandro Cimatti
Author	Alberto Griggio
Abstract	IC3 is a recently proposed verification technique for the analysis of sequential circuits. IC3 incrementally overapproximates the state space, refuting potential violations to the property at hand by constructing relative inductive blocking clauses. The algorithm relies on aggressive use of Boolean satisfiability (SAT) techniques, and has demonstrated impressive effectiveness.
Date	2012
Language	en
Library Catalog	DOI.org (Crossref)
URL	http://link.springer.com/10.1007/978-3-642-31424-7_23
Accessed	4/5/2022, 9:44:17 AM
Extra	Series Title: Lecture Notes in Computer Science
Volume	7358
Place	Berlin, Heidelberg
Publisher	Springer Berlin Heidelberg
ISBN	978-3-642-31423-0 978-3-642-31424-7
Pages	277-293
Proceedings Title	Computer Aided Verification
DOI	10.1007/978-3-642-31424-7_23
Date Added	4/4/2022, 5:13:52 PM
Modified	4/5/2022, 12:28:34 PM

Attachments

- Cimatti2012_Software_Model_Checking_via_IC3.pdf

Software Verification with PDR: An Implementation of the State of the Art

Type	Journal Article
Author	Dirk Beyer
Author	Matthias Dangl
Abstract	Property-directed reachability (PDR) is a SAT/SMT-based reachability algorithm that incrementally constructs inductive invariants. After it was successfully applied to hardware model checking, several adaptations to software model checking have been proposed. We contribute a replicable and thorough comparative evaluation of the state of the art: We (1) implemented a standalone PDR algorithm and, as improvement, a PDR-based auxiliary-invariant generator for k-induction, and (2) performed an experimental study on the largest publicly available benchmark set of C verification tasks, in which we explore the effectiveness and efficiency of software verification with PDR. The main contribution of our work is to establish a reproducible baseline for ongoing research in the area by providing a well-engineered reference implementation and an experimental evaluation of the existing techniques.
Date	2020-03
Short Title	Software Verification with PDR
URL	https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7439737/
Accessed	4/22/2021, 6:00:00 PM

Volume 12078
Pages 3–21
Publication Tools and Algorithms for the Construction and Analysis of Systems
DOI 10.1007/978-3-030-45190-5_1
Date Added 4/4/2022, 5:14:36 PM
Modified 4/4/2022, 5:29:34 PM

Attachments

- Beyer2020_Software_Verification_with_PDR.pdf

Word level property directed reachability

Type Conference Paper
Author Hari Govind V K
Author Grigory Fedyukovich
Author Arie Gurfinkel
Abstract Verification approaches based on constraint solvers are successfully applied in firmware and other low-level code that interfaces with hardware. While for proving safety of gate-level sequential circuits, it often suffices to bit-blast and reduce to SAT-based IC3 or Property Directed Reachability (IC3/PDR), for handling machine-level instructions that perform arithmetic and data manipulation operations, word-level reasoning should be conducted. However, because of poor support for interpolation and quantifier elimination in the theory of bit-vectors (BV), previous attempts to lift IC3/PDR to word level required integrating it into an external abstraction-refinement loop. Aiming to reach more scalable bit-precise verification, we propose to bring useful insights from PDR-based verification algorithms used in software. In particular, instead of using bit-blasting to eliminate quantifiers from BV-formulas, we present a less expensive method for iterative approximate quantifier elimination in BV. It naturally supports all bit-operators and can be optimized further by applying rules inspired by modular linear arithmetic. Finally, we leverage recent techniques on learning inductive invariants based on explicit global guidance, thus allowing the approach to bypass interpolation. Our implementation on top of Spacer, a PDR-based verifier shows that such a word-level PDR is promising and can be more effective than state-of-the-art.
Date 2020-11-02
Language en
Library Catalog DOI.org (Crossref)
URL https://dl.acm.org/doi/10.1145/3400302.3415708
Accessed 4/5/2022, 9:42:57 AM
Place Virtual Event USA
Publisher ACM
ISBN 978-1-4503-8026-3
Pages 1-9
Proceedings Title Proceedings of the 39th International Conference on Computer-Aided Design
Conference Name ICCAD '20: IEEE/ACM International Conference on Computer-Aided Design
DOI 10.1145/3400302.3415708
Date Added 4/4/2022, 5:14:55 PM
Modified 4/5/2022, 9:54:30 AM

Attachments

- K2020_Word_level_property_directed_reachability.pdf