Lecture Notes in Computer Science 7795

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Advanced Research in Computing and Software Science
Subline of Lectures Notes in Computer Science

Nir Piterman Scott A. Smolka (Eds.)

Tools and Algorithms for the Construction and Analysis of Systems

19th International Conference, TACAS 2013
Held as Part of the European Joint Conferences
on Theory and Practice of Software, ETAPS 2013
Rome, Italy, March 16-24, 2013
Proceedings

Springer

Volume Editors

Nir Piterman
University of Leicester
Department of Computer Science
University Road, LE1 7RH Leicester, UK
E-mail: nir.piterman@le.ac.uk

Scott A. Smolka
Stony Brook University
Department of Computer Science
Stony Brook, NY 11794-4400, USA
E-mail: sas@cs.sunysb.edu

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-36741-0 e-ISBN 978-3-642-36742-7
DOI 10.1007/978-3-642-36742-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2013932470

CR Subject Classification (1998): F.3.1-2, D.2.4-5, F.2.2, D.3.1, D.3.3, D.1.1, F.1.1-3, C.3

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Foreword

ETAPS 2013 is the sixteenth instance of the European Joint Conferences on Theory and Practice of Software. ETAPS is an annual federated conference that was established in 1998 by combining a number of existing and new conferences. This year it comprised six sister conferences (CC, ESOP, FASE, FOSSACS, POST, TACAS), 20 satellite workshops (ACCAT, AiSOS, BX, BYTECODE, CerCo, DICE, FESCA, GRAPHITE, GT-VMT, HAS, Hot-Spot, FSS, MBT, MEALS, MLQA, PLACES, QAPL, SR, TERMGRAPH and VSSE), three invited tutorials (*e-education*, by John Mitchell; *cyber-physical systems*, by Martin Fränzle; and *e-voting* by Rolf Küsters) and eight invited lectures (excluding those specific to the satellite events).

The six main conferences received this year 627 submissions (including 18 tool demonstration papers), 153 of which were accepted (6 tool demos), giving an overall acceptance rate just above 24%. (ETAPS 2013 also received 11 submissions to the software competition, and 10 of them resulted in short papers in the TACAS proceedings). Congratulations therefore to all the authors who made it to the final programme! I hope that most of the other authors will still have found a way to participate in this exciting event, and that you will all continue to submit to ETAPS and contribute to making it the best conference on software science and engineering.

The events that comprise ETAPS address various aspects of the system development process, including specification, design, implementation, analysis, security and improvement. The languages, methodologies and tools that support these activities are all well within its scope. Different blends of theory and practice are represented, with an inclination towards theory with a practical motivation on the one hand and soundly based practice on the other. Many of the issues involved in software design apply to systems in general, including hardware systems, and the emphasis on software is not intended to be exclusive.

ETAPS is a confederation in which each event retains its own identity, with a separate Programme Committee and proceedings. Its format is open-ended, allowing it to grow and evolve as time goes by. Contributed talks and system demonstrations are in synchronised parallel sessions, with invited lectures in plenary sessions. Two of the invited lectures are reserved for 'unifying' talks on topics of interest to the whole range of ETAPS attendees. The aim of cramming all this activity into a single one-week meeting is to create a strong magnet for academic and industrial researchers working on topics within its scope, giving them the opportunity to learn about research in related areas, and thereby to foster new and existing links between work in areas that were formerly addressed in separate meetings.

ETAPS 2013 was organised by the *Department of Computer Science of 'Sapienza' University of Rome*, in cooperation with

- ▷ European Association for Theoretical Computer Science (EATCS)
- ▷ European Association for Programming Languages and Systems (EAPLS)
- ▷ European Association of Software Science and Technology (EASST).

The organising team comprised:

General Chair:	*Daniele Gorla;*
Conferences:	*Francesco Parisi Presicce;*
Satellite Events:	*Paolo Bottoni* and *Pietro Cenciarelli;*
Web Master:	*Igor Melatti;*
Publicity:	*Ivano Salvo;*
Treasurers:	*Federico Mari* and *Enrico Tronci.*

Overall planning for ETAPS conferences is the responsibility of its Steering Committee, whose current membership is:

Vladimiro Sassone (Southampton, chair), Martín Abadi (Santa Cruz), Erika Ábrahám (Aachen), Roberto Amadio (Paris 7), Gilles Barthe (IMDEA-Software), David Basin (Zürich), Saddek Bensalem (Grenoble), Michael O'Boyle (Edinburgh), Giuseppe Castagna (CNRS Paris), Albert Cohen (Paris), Vittorio Cortellessa (L'Aquila), Koen De Bosschere (Gent), Ranjit Jhala (San Diego), Matthias Felleisen (Boston), Philippa Gardner (Imperial College London), Stefania Gnesi (Pisa), Andrew D. Gordon (MSR Cambridge and Edinburgh), Daniele Gorla (Rome), Klaus Havelund (JLP NASA Pasadena), Reiko Heckel (Leicester), Holger Hermanns (Saarbrücken), Joost-Pieter Katoen (Aachen), Paul Klint (Amsterdam), Jens Knoop (Vienna), Steve Kremer (Nancy), Gerald Lüttgen (Bamberg), Tiziana Margaria (Potsdam), Fabio Martinelli (Pisa), John Mitchell (Stanford), Anca Muscholl (Bordeaux), Catuscia Palamidessi (INRIA Paris), Frank Pfenning (Pittsburgh), Nir Piterman (Leicester), Arend Rensink (Twente), Don Sannella (Edinburgh), Zhong Shao (Yale), Scott A. Smolka (Stony Brook), Gabriele Taentzer (Marburg), Tarmo Uustalu (Tallinn), Dániel Varró (Budapest) and Lenore Zuck (Chicago).

The ordinary running of ETAPS is handled by its management group comprising: Vladimiro Sassone (chair), Joost-Pieter Katoen (deputy chair and publicity chair), Gerald Lüttgen (treasurer), Giuseppe Castagna (satellite events chair), Holger Hermanns (liaison with local organiser) and Gilles Barthe (industry liaison).

I would like to express here my sincere gratitude to all the people and organisations that contributed to ETAPS 2013, the Programme Committee chairs and members of the ETAPS conferences, the organisers of the satellite events, the speakers themselves, the many reviewers, all the participants, and Springer-Verlag for agreeing to publish the ETAPS proceedings in the ARCoSS subline.

Last but not least, I would like to thank the organising chair of ETAPS 2013, Daniele Gorla, and his Organising Committee, for arranging for us to have ETAPS in the most beautiful and historic city of Rome.

My thoughts today are with two special people, profoundly different for style and personality, yet profoundly similar for the love and dedication to our discipline, for the way they shaped their respective research fields, and for the admiration and respect that their work commands. Both are role-model computer scientists for us all.

ETAPS in Rome celebrates *Corrado Böhm*. Corrado turns 90 this year, and we are just so lucky to have the chance to celebrate the event in Rome, where he has worked since 1974 and established a world-renowned school of computer scientists. Corrado has been a pioneer in research on programming languages and their semantics. Back in 1951, years before FORTRAN and LISP, he defined and implemented a *metacircular compiler* for a programming language of his invention. The compiler consisted of just 114 instructions, and anticipated some modern list-processing techniques.

Yet, Corrado's claim to fame is asserted through the breakthroughs expressed by the *Böhm-Jacopini Theorem* (CACM 1966) and by the invention of *Böhm-trees*. The former states that any algorithm can be implemented using only sequencing, conditionals, and while-loops over elementary instructions. Böhm trees arose as a convenient data structure in Corrado's milestone proof of the decidability inside the λ-calculus of the equivalence of terms in β-η-normal form.

Throughout his career, Corrado showed exceptional commitment to his roles of researcher and educator, fascinating his students with his creativity, passion and curiosity in research. Everybody who has worked with him or studied under his supervision agrees that he combines an outstanding technical ability and originality of thought with great personal charm, sweetness and kindness. This is an unusual combination in problem-solvers of such a high calibre, yet another reason why we are ecstatic to celebrate him. *Happy birthday from ETAPS, Corrado!*

ETAPS in Rome also celebrates the life and work of *Kohei Honda*. Kohei passed away suddenly and prematurely on December 4th, 2012, leaving the saddest gap in our community. He was a dedicated, passionate, enthusiastic scientist and –more than that!– his enthusiasm was contagious. Kohei was one of the few theoreticians I met who really succeeded in building bridges between theoreticians and practitioners. He worked with W3C on the standardisation of web services choreography description languages (WS-CDL) and with several companies on *Savara* and *Scribble*, his own language for the description of application-level protocols among communicating systems.

Among Kohei's milestone research, I would like to mention his 1991 epochmaking paper at ECOOP (with M. Tokoro) on the treatment of asynchrony in message passing calculi, which has influenced all process calculi research since. At ETAPS 1998 he introduced (with V. Vasconcelos and M. Kubo) a new concept in type theories for communicating processes: it came to be known as '*session types*,' and has since spawned an entire research area, with practical and multidisciplinary applications that Kohei was just starting to explore.

Kohei leaves behind him enormous impact, and a lasting legacy. He is irreplaceable, and I for one am proud to have been his colleague and glad for the opportunity to arrange for his commemoration at ETAPS 2013.

My final ETAPS '*Foreword*' seems like a good place for a short reflection on ETAPS, what it has achieved in the past few years, and what the future might have in store for it.

On April 1st, 2011 in Saarbrücken, we took a significant step towards the consolidation of ETAPS: the establishment of *ETAPS e.V.* This is a *non-profit association* founded under German law with the immediate purpose of supporting the conference and the related activities. ETAPS e.V. was required for practical reasons, e.g., the conference needed (to be represented by) a legal body to better support authors, organisers and attendees by, e.g., signing contracts with service providers such as publishers and professional meeting organisers. Our ambition is however to make of '*ETAPS the association*' more than just the organisers of '*ETAPS the conference*'. We are working towards finding a voice and developing a range of activities to support our scientific community, in cooperation with the relevant existing associations, learned societies and interest groups. The process of defining the structure, scope and strategy of ETAPS e.V. is underway, as is its first ever membership campaign. For the time being, ETAPS e.V. has started to support community-driven initiatives such as open access publications (LMCS and EPTCS) and conference management systems (Easychair), and to cooperate with cognate associations (European Forum for ICT).

After two successful runs, we continue to support POST, *Principles of Security and Trust*, as a candidate to become a permanent ETAPS conference. POST was the first addition to our main programme since 1998, when the original five conferences met together in Lisbon for the first ETAPS. POST resulted from several smaller workshops and informal gatherings, supported by IFIP WG 1.7, and combines the practically important subject of security and trust with strong technical connections to traditional ETAPS areas. POST is now attracting interest and support from prominent scientists who have accepted to serve as PC chairs, invited speakers and tutorialists. I am very happy about the decision we made to create and promote POST, and to invite it to be a part of ETAPS.

Considerable attention was recently devoted to our *internal processes* in order to streamline our procedures for appointing Programme Committees, choosing invited speakers, awarding prizes and selecting papers; to strengthen each member conference's own Steering Group, and, at the same time, to strike a balance between these and the ETAPS Steering Committee. A lot was done and a lot remains to be done.

We produced a *handbook* for local organisers and one for PC chairs. The latter sets out a code of conduct that all the people involved in the selection of papers, from PC chairs to referees, are expected to adhere to. From the point of view of the authors, we adopted a *two-phase submission* protocol, with fixed deadlines in the first week of October. We published a *confidentiality policy* to

set high standards for the handling of submissions, and a *republication policy* to clarify what kind of material remains eligible for submission to ETAPS after presentation at a workshop. We started an *author rebuttal phase*, adopted by most of the conferences, to improve the author experience. It is important to acknowledge that – regardless of our best intentions and efforts – the quality of reviews is not always what we would like it to be. To remain true to our commitment to the authors who elect to submit to ETAPS, we must endeavour to improve our standards of refereeing. The rebuttal phase is a step in that direction and, according to our experience, it seems to work remarkably well at little cost, provided both authors and PC members use it for what it is. ETAPS has now reached a healthy paper acceptance rate around the 25% mark, essentially uniformly across the six conferences. This seems to me to strike an excellent balance between being selective and being inclusive, and I hope it will be possible to maintain it even if the number of submissions increases.

ETAPS signed a favourable three-year publication contract with Springer for publication in the ARCoSS subline of LNCS. This was the result of lengthy negotiations, and I consider it a good achievement for ETAPS. Yet, publication of its proceedings is possibly the hardest challenge that ETAPS – and indeed most computing conferences – currently face. I was invited to represent ETAPS at a most interesting Dagstuhl Perspective Workshop on the '*Publication Culture in Computing Research*' (seminar 12452). The paper I gave there is available online from the workshop proceedings, and illustrates three of the views I formed also thanks to my experience as chair of ETAPS, respectively on open access, bibliometrics, and the roles and relative merits of conferences versus journal publications. Open access is a key issue for a conference like ETAPS. Yet, in my view it does not follow that we can altogether dispense with publishers – be they commercial, academic, or learned societies – and with their costs. A promising way forward may be based on the '*author-pays*' model, where publications fees are kept low by resorting to learned-societies as publishers. Also, I believe it is ultimately in the interest of our community to de-emphasise the perceived value of conference publications as viable – if not altogether superior – alternatives to journals. A large and ambitious conference like ETAPS ought to be able to rely on quality open-access journals to cover its entire spectrum of interests, even if that means promoting the creation of a new journal.

Due to its size and the complexity of its programme, hosting ETAPS is an increasingly challenging task. Even though excellent candidate *locations* keep being volunteered, in the longer run it seems advisable for ETAPS to provide more support to local organisers, starting e.g., by taking direct control of the organisation of satellite events. Also, after sixteen splendid years, this may be a good time to start thinking about exporting ETAPS to other continents. The US East Coast would appear to be the obvious destination for a first ETAPS outside Europe.

The strength and success of ETAPS comes also from presenting – regardless of the natural internal differences – a homogeneous interface to authors and participants, i.e., to look like one large, coherent, well-integrated conference

rather than a mere co-location of events. I therefore feel it is vital for ETAPS to regulate the centrifugal forces that arise naturally in a 'union' like ours, as well as the legitimate aspiration of individual PC chairs to run things their way. In this respect, we have large and solid foundations, alongside a few relevant issues on which ETAPS has not yet found agreement. They include, e.g., submission by PC members, rotation of PC memberships, and the adoption of a rebuttal phase. More work is required on these and similar matters.

January 2013

Vladimiro Sassone
ETAPS SC Chair
ETAPS e.V. President

Preface

This volume contains the proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. TACAS 2013 took place during March 18–21, 2013, in the eternal city of Rome, Italy.It was part of the 16th European Joint Conference on Theory and Practice of Software (ETAPS 2013).

TACAS is a forum for researchers, developers, and users interested in rigorously based tools and algorithms for the construction and analysis of systems. The research areas covered by TACAS include, but are not limited to, formal methods, software and hardware verification, static analysis, programming languages, software engineering, real-time systems, communication protocols, and biological systems. TACAS provides a venue where common problems, heuristics, algorithms, data structures, and methodologies in these areas can be discussed and explored.

Following a debut in 2012, TACAS 2013 solicited four kinds of papers, including three types of full-length papers (15 pages), as well as short tool demonstration papers (6 pages):

- Research papers – papers describing novel research on topics included in the remit of TACAS.
- Case study papers – papers reporting on case studies (preferably in a "real life" setting), describing methodologies and approaches used.
- Regular tool papers – papers describing a tool (either completely new, new component, or existing) and focusing on engineering aspects of the tool (including, e.g., software architecture, data structures, and algorithms).
- Tool demonstration papers – papers focusing on the usage aspects of tools relevant to the above-mentioned topics.

This year, TACAS attracted a total of 172 paper submissions, divided into 130 research papers, 15 regular tool papers, 9 case study papers, and 18 tool demonstration papers. Each submission was refereed by at least three reviewers, who evaluated the papers, commented on them, and in many cases suggested improvements and enhancements. The reviewing process was followed by an online Program Committee discussion. As a result of the discussion, 42 papers were accepted for presentation at the conference: 32 research papers, 1 case study paper, 3 regular tool papers, and 6 tool demonstration papers.

TACAS 2013 marked the second time that the Competition on Software Verification was associated with TACAS. This volume includes an overview of the competition results, and short papers describing 10 of the 11 tools that participated in the competition. These papers were reviewed by a separate Program Committee and each paper was refereed by at least three reviewers. Competition results were presented at the conference by Dirk Beyer, the Competition Chair, and the verifiers were presented by the participating teams.

In addition to refereed contributions, the program included an invited talk by Orna Grumberg. TACAS took place in an exciting and vibrant scientific atmosphere, consisting of five other sister conferences (CC, ESOP, FASE, FoSSaCS, and Post), with (sometimes) overlapping scientific fields of interest, their invited speakers, and the ETAPS unifying speakers Gilles Barthe and Cédric Fournet.

We would like to thank all of the authors who submitted papers to TACAS 2013, the Program Committee members, and additional reviewers, without whom TACAS would not have been such a success. We would especially like to thank Claude Marche for his invaluable help as TACAS Tool Chair. We also benefited greatly from the EasyChair conference management system, which we used to run the Program Commitee discussion and to handle the submission, review, and proceedings preparation process. Finally, we would like to thank the TACAS Steering Committee, the ETAPS Steering Committee, and the ETAPS Organizing Committee chaired by Daniele Gorla, who made ETAPS 2013 such a memorable event.

January 2013

Nir Piterman
Scott Smolka

Organization

Steering Committee

Rance Cleaveland	University of Maryland, USA
Kim Guldstrand Larsen	Aalborg University, Denmark
Joost-Pieter Katoen	RWTH Aachen University, Germany
Bernhard Steffen	TU Dortmund, Germany
Lenore Zuck	University of Illinois in Chicago, USA

Program Committee

Erika Abraham	RWTH Aachen University, Germany
Marsha Chechik	University of Toronto, Canada
Rance Cleaveland	University of Maryland, USA
Leonardo De Moura	Microsoft Research, USA
Cindy Eisner	IBM Research - Haifa, Israel
Cédric Fournet	Microsoft, UK
Dimitra Giannakopoulou	NASA Ames, USA
Susanne Graf	VERIMAG (CNRS and Grenoble University), France
Kim Guldstrand Larsen	Aalborg University, Denmark
Klaus Havelund	NASA JPL, USA
Laurie Hendren	McGill University, Canada
Gerard Holzmann	NASA JPL, USA
Michael Huth	Imperial College London, UK
Paola Inverardi	Università dell'Aquila, Italy
Joost-Pieter Katoen	RWTH Aachen University, Germany
Panagiotis Katsaros	Aristotle University of Thessaloniki, Greece
Hillel Kugler	Microsoft Research, UK
Barbara König	Universität Duisburg-Essen, Germany
Axel Legay	IRISA/INRIA, Rennes, France
Claude Marche	INRIA, France
Tobias Nipkow	TU Munich, Germany
Gethin Norman	University of Glasgow, UK
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Nir Piterman	University of Leicester, UK
Mooly Sagiv	Tel Aviv University, Israel
Natasha Sharygina	University of Lugano, Switzerland
Scott Smolka	State University of New York, USA

Bernhard Steffen	TU Dortmund, Germany
Cesare Tinelli	The University of Iowa, USA
Verena Wolf	Saarland University, Germany
Lenore Zuck	University of Illinois in Chicago, USA

Program Committee for Competition on Software Verification

Dirk Beyer	University of Passau, Germany
Lucas Cordeiro	Universidade Federal do Amazonas, Brazil
Bernd Fischer	University of Southampton, UK
Arie Gurfinkel	SEI, USA
Matthias Heizmann	University of Freiburg, Germany
Stefan Löwe	University of Passau, Germany
Vadim Mutilin	ISP RAS, Russian Federation
Andrey Rybalchenko	TU Munich, Germany
Carsten Sinz	Karlsruhe Institute of Technology, Germany
Jiri Slaby	Masaryk University, Czech Republic
Tomáš Vojnar	Brno University of Technology, Czech Republic
Philipp Wendler	University of Passau, Germany

Additional Reviewers

Abdeddaïm, Yasmina	Bobot, François	D'Silva, Vijay
Albarghouthi, Aws	Bollig, Benedikt	de Boer, Pieter-Tjerk
Alberti, Francesco	Bolton, Matthew	Dehnert, Christian
Aleksandrowicz, Gadi	Bonakdarpour, Borzoo	Delahaye, Benoit
Andreychenko, Aleksandr	Bouajjani, Ahmed	Deshpande, Tushar
Autili, Marco	Boyer, Benoît	Deters, Morgan
Bacci, Giovanni	Bozga, Marius	Eades Iii, Harley
Balasubramanian, Daniel	Bozzelli, Laura	Efraimidis, Pavlos
Banach, Richard	Bruggink, Harrie Jan Sander	Fahrenberg, Uli
Barringer, Howard	Brumley, David	Fedyukovich, Grigory
Bartocci, Ezio	Bøgholm, Thomas	Feo, Sergio
Ben-David, Shoham	Chatzieleftheriou, George	Fisman, Dana
Bensalem, Saddek	Chen, Xin	Florian, Mihai
Bhaduri, Purandar	Chen, Yu-Fang	Fontana, Peter
Bjørner, Nikolaj	Chockler, Hana	Fränzle, Martin
Blanchette, Jasmin Christian	Copty, Fady	Fu, Hongfei
Blume, Christoph	Corzilius, Florian	Ganesh, Vijay

Garrison, Bill
Grechanik, Mark
Gretz, Friedrich
Griggio, Alberto
Gurfinkel, Arie
Haller, Leopold
Han, Tingting
Hansen, Henri
Harkjær Møller, Mikael
Heinen, Jonathan
Heljanko, Keijo
Howar, Falk
Hyvärinen, Antti
Hölzl, Johannes
Iosif, Radu
Isberner, Malte
Ivrii, Alexander
Jaeger, Manfred
Jansen, Christina
Jansen, Nils
Jegourel, Cyrille
Jovanovic, Dejan
Jung, Yungbum
Kerstan, Henning
Kidd, Nicholas
Kiefer, Stefan
Komuravelli, Anvesh
Krüger, Thilo
Kupferman, Orna
Küpper, Sebastian
Laarman, Alfons
Lamprecht, Anna-Lena
Langerak, Rom
Lee, Adam
Loup, Ulrich
Luckow, Kasper
Manevich, Roman
Mardare, Radu
Margalit, Oded
Markey, Nicolas
Merten, Maik
Michael, Maged
Mikeev, Linar
Mikucionis, Marius
Miller, Alice
Mogavero, Fabio
Monniaux, David
Moy, Matthieu
Musial, Peter
Møller, Anders
Namjoshi, Kedar
Naujokat, Stefan
Nestmann, Uwe
Neubauer, Johannes
Neuhäußer, Martin R.
Nevo, Ziv
Nickovi, Dejan
Noll, Thomas
Oe, Duckki
Olesen, Mads C.
Pai, Ganesh
Parker, David
Pelliccione, Patrizio
Person, Suzette
Potet, Marie-Laure
Poulsen, Danny Bøgsted
Pradella, Matteo
Pulungan, Reza
Quinton, Sophie
Rajan, Hridesh
Ranzato, Francesco
Ravn, Anders
Raymond, Pascal
Reger, Giles
Reineke, Jan
Reynolds, Andrew
Rinetzky, Noam
Rojas, José Miguel
Rollini, Simone Fulvio
Rozier, Kristin Yvonne
Ruah, Sitvanit
Rungta, Neha
Rydeheard, David
Rüthing, Oliver
Sadre, Ramin
Saidi, Hassen
Salay, Rick
Samanta, Roopsha
Schmalz, Matthias
Schneider-Kamp, Peter
Schubert, Tobias
Schulze, Christoph
Schwoon, Stefan
Sery, Ondrej
Shacham, Ohad
Shafiei, Nastaran
Sher, Falak
Simon, Axel
Sims, Steve
Sinha, Nishant
Spieler, David
Sproston, Jeremy
Srba, Jiri
Srivathsan, Baluguru
Stachtiari, Emmanouela
Stoelinga, Mariëlle I.A.
Stoller, Scott
Stückrath, Jan
Suter, Philippe
Telek, Miklos
Tivoli, Massimo
Tkachuk, Oksana
Vafeiadis, Viktor
van Breugel, Franck
van de Pol, Jaco
Veksler, Tatyana
Viswanathan, Mahesh
von Styp, Sabrina
Wang, Bow-Yaw
Wimmer, Ralf
Windmüller, Stephan
Yang, Bow-Yaw
Yang, Guowei
Yang, Junxing
Yorav, Karen
Yue, Haidi
Zhang, Lijun
Ziv, Avi
Zuliani, Paolo

Additional Reviewers for Competition on Software Verification

Falke, Stephan Mandrykin, Mikhail Zakharov, Ilya

SAT-Based Model Checking: Interpolation, IC3 and beyond (Invited Talk)

Orna Grumberg

Computer Science Department, The Technion, Haifa, Israel

Model checking [3] is an automatic approach to formally verifying that a given system satisfies a given specification. The system to be verified is modelled as a finite state machine and the specification is described using temporal logic. Model checking algorithms are typically based on an exploration of the model state space while searching for violations of the specification. In spite of its great success in verifying hardware and software systems, the applicability of model checking is impeded by its high space and time requirements. This is referred to as the *state explosion problem*.

The introduction of SAT-based model checking algorithms [1, 8, 6, 9, 2] significantly increases the size of the systems that can be model checked. In its early days SAT-based model checking was used mostly for bug hunting. The introduction of *interpolation* enabled an efficient complete algorithm, referred to as Interpolation-based model checking (ITP) [6]. ITP uses interpolation to extract an over-approximation of a set of reachable states from a proof of unsatisfiability generated by a SAT-solver. The set of reachable states computed by the reachability analysis is used by ITP to check if a system M satisfies a safety property AGp.

In [2] an alternative SAT-based algorithm, called IC3, is introduced. Similarly to ITP, IC3 also computes over-approximations of sets of reachable states. However, ITP unrolls the model in order to obtain more precise approximations. In many cases, this is a bottleneck of the approach. IC3, on the other hand, improves the precision of the approximations by performing many local checks that do not require unrolling.

Here, we survey several approaches to enhancing SAT-based model checking. One approach, detailed in [9], uses *interpolation sequence* [5, 7] rather than interpolation in order to obtain a more precise over-approximation of the set of reachable states.

The other approach, described in [10], integrates lazy abstraction with IC3 in order to achieve scalability. *Lazy abstraction* [4, 7], originally developed for software model checking, is a specific type of abstraction that allows hiding different model details at different steps of the verification. We find the IC3 algorithm most suitable for lazy abstraction since its state traversal is performed by means of *local* reachability checks, each involving only two consecutive sets. A different abstraction can therefore be applied in each of the local checks.

References

1. Biere, A., Cimatti, A., Clarke, E., Zhu, Y.: Symbolic Model Checking without BDDs. In: Cleaveland, W.R. (ed.) TACAS/ETAPS 1999. LNCS, vol. 1579, pp. 193–207. Springer, Heidelberg (1999)
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. Clarke, E.C., Grumberg, O., Peled, D.: Model Checking. MIT Press (1999)
4. Henzinger, T., Jhala, R., Majumdar, R.: Lazy abstraction. In: POPL (2002)
5. Jhala, R., McMillan, K.L.: Interpolant-Based Transition Relation Approximation. In: Etessami, K., Rajamani, S.K. (eds.) CAV 2005. LNCS, vol. 3576, pp. 39–51. Springer, Heidelberg (2005)
6. McMillan, K.L.: Interpolation and SAT-Based Model Checking. In: Hunt Jr., W.A., Somenzi, F. (eds.) CAV 2003. LNCS, vol. 2725, pp. 1–13. Springer, Heidelberg (2003)
7. McMillan, K.L.: Lazy Abstraction with Interpolants. In: Ball, T., Jones, R.B. (eds.) CAV 2006. LNCS, vol. 4144, pp. 123–136. Springer, Heidelberg (2006)
8. Sheeran, M., Singh, S., Stålmarck, G.: Checking Safety Properties Using Induction and a SAT-Solver. In: Johnson, S.D., Hunt Jr., W.A. (eds.) FMCAD 2000. LNCS, vol. 1954, pp. 108–125. Springer, Heidelberg (2000)
9. Vizel, Y., Grumberg, O.: Interpolation-sequence based model checking. In: FMCAD (2009)
10. Vizel, Y., Grumberg, O., Shoham, S.: Lazy abstraction and SAT-based reachability in hardware model checking. In: FMCAD (2012)

Table of Contents

Games and Synthesis

Process Algebra

Pushdown Systems Boolean/Integer Programs

Runtime Verification and Model Checking

Concurrency

Learning and Abduction

Timed Automata

Security and Access Control

Frontiers (Graphics and Quantum)

Functional Programs and Types

Tool Demonstrations

Explicit-State Model Checking

Büchi Automata

Competition on Software Verification