Lecture Notes in Computer Science 6887

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

Editorial Board

David Hutchison, UK
Josef Kittler, UK
Alfred Kobsa, USA
John C. Mitchell, USA
Oscar Nierstrasz, Switzerland
Bernhard Steffen, Germany
Demetri Terzopoulos, USA
Gerhard Weikum, Germany
Takeo Kanade, USA
Jon M. Kleinberg, USA
Friedemann Mattern, Switzerland
Moni Naor, Israel
C. Pandu Rangan, India
Madhu Sudan, USA
Doug Tygar, USA

Advanced Research in Computing and Software Science

Subline of Lectures Notes in Computer Science

Subline Series Editors

Giorgio Ausiello, *University of Rome 'La Sapienza', Italy*
Vladimiro Sassone, *University of Southampton, UK*

Subline Advisory Board

Susanne Albers, *University of Freiburg, Germany*
Benjamin C. Pierce, *University of Pennsylvania, USA*
Bernhard Steffen, *University of Dortmund, Germany*
Madhu Sudan, *Microsoft Research, Cambridge, MA, USA*
Deng Xiaotie, *City University of Hong Kong*
Jeannette M. Wing, *Carnegie Mellon University, Pittsburgh, PA, USA*

Eran Yahav (Ed.)

Static Analysis

18th International Symposium, SAS 2011
Venice, Italy, September 14-16, 2011
Proceedings

Springer

Volume Editor

Eran Yahav
Technion
Computer Science Department
Technion City
Haifa 32000, Israel
E-mail: yahave@cs.technion.ac.il

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-23701-0 e-ISBN 978-3-642-23702-7
DOI 10.1007/978-3-642-23702-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2011935065

CR Subject Classification (1998): D.2, F.3, D.3, D.2.4, F.4.1, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2011
This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.
The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

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)

Preface

Static analysis is increasingly recognized as a fundamental tool for program verification, bug detection, compiler optimization, program understanding, and software maintenance. The series of Static Analysis Symposia has served as the primary venue for presentation of theoretical, practical, and application advances in the area.

This volume contains the proceedings of the 18th International Static Analysis Symposium (SAS 2011), which was held September 14–16, 2011, in Venice, Italy. Previous symposia were held in Perpignan, France (2010); Los Angeles, USA (2009); Valencia, Spain (2008); Kongens Lyngby, Denmark (2007); Seoul, South Korea (2006); London, UK (2005); Verona, Italy (2004); San Diego, USA (2003); Madrid, Spain (2002); Paris, France (2001); Santa Barbara, USA (2000); Venice, Italy (1999); Pisa, Italy (1998); Paris, France (1997); Aachen, Germany (1996); Glasgow, UK (1995); and Namur, Belgium (1994).

The 18th International Static Analysis Symposium (SAS 2011), was held together with three affiliated Workshops: NSAD 2011 (The Third Workshop on Numerical and Symbolic Abstract Domains), SASB (Second Workshop on Static Analysis and Systems Biology) on September 13, 2011, and TAPAS 2010 (Tools for Automatic Program AnalysiS) on September 17, 2011.

There were 67 submissions. Each submission was reviewed by at least four Program Committee members. The committee decided to accept 22 papers.

In addition to the 22 contributed papers, the program included five invited talks by Jérôme Feret (Ecole Normale Superieure, France), Daniel Kaestner (AbsInt, Germany), Ken McMillan (Microsoft Research, USA), John Mitchell (Stanford, USA), and Sriram Rajamani (Microsoft Research, India).

On behalf of the Program Committee, I would like to thank all the external referees for their participation in the reviewing process. We are grateful to our generous sponsors, to all the members of the Organizing Committee in Venice for their hard work, and to the EasyChair team for the use of their system.

September 2011 Eran Yahav

Conference Organization

General Chairs

Gilberto Filè	University of Padova, Italy
Mooly Sagiv	Tel Aviv University, Israel

Program Chair

Eran Yahav	Technion, Israel

Program Committee

Anindya Banerjee	IMDEA Software Institute, Spain
Michele Bugliesi	Università Cà Foscari, Italy
Byron Cook	Microsoft Research, UK
Radhia Cousot	École Normale Supérieure and CNRS, France
Roberto Giacobazzi	University of Verona, Italy
Sumit Gulwani	Microsoft Research, USA
Chris Hankin	Imperial College London, UK
Naoki Kobayashi	Tohoku University, Japan
Viktor Kuncak	EPFL, Switzerland
Ondrej Lhotak	University of Waterloo, Canada
Matthieu Martel	Université de Perpignan, France
Antoine Miné	École Normale Supérieure and CNRS, France
George Necula	UC Berkeley, USA
Ganesan Ramalingam	Microsoft Research, India
Francesco Ranzato	University of Padova, Italy
Thomas Reps	University of Wisconsin, USA
Noam Rinetzky	Queen Mary University of London, UK
Helmut Seidl	University of Munich, Germany
Zhendong Su	University of California, Davis, USA
Hongseok Yang	University of Oxford, UK

Organizing Committee

Alberto Carraro	Università Cà Foscari
Nicoletta Cocco	Università Cà Foscari
Sabina Rossi	Università Cà Foscari, Chair
Silvia Crafa	University of Padova

Steering Committee

Patrick Cousot	École Normale Supérieure, France and New York University, USA
Radhia Cousot	École Normale Supérieure and CNRS, France
Roberto Giacobazzi	University of Verona, Italy
Gilberto Filè	University of Padova, Italy
Manuel Hermenegildo	IMDEA Software Institute, Spain
David Schmidt	Kansas State University, USA

External Reviewers

Reynald Affeldt
Xavier Allamigeon
Gianluca Amato
Saswat Anand
Tycho Andersen
Domagoj Babic
Earl Barr
Matko Botincan
Olivier Bouissou
Jacob Burnim
Stefano Calzavara
Bor-Yuh Evan Chang
Alexandre Chapoutot
Swarat Chaudhuri
Hana Chockler
Patrick Cousot
Silvia Crafa
Ferruccio Damiani
Eva Darulova
Giorgio Delzanno
Alessandra Di Pierro
Dino Distefano
Mike Dodds
Matt Elder
Tayfun Elmas
Michael Emmi
Karine Even
Jérôme Feret
Pietro Ferrara
Mark Gabel
Pierre Ganty
Pierre-Loic Garoche
Denis Gopan
Nikos Gorogiannis
Alexey Gotsman
Radu Grigore
Guy Gueta
Tihomir Gvero
Christoph Haase
Raju Halder
Emmanuel Haucourt
Hossein Hojjat
Kazuhiro Inaba
Arnault Ioualalen
Swen Jacobs
Pierre Jouvelot
Andy King
Etienne Kneuss
Eric Koskinen
Joerg Kreiker
Sava Krstic
Michael Kuperstein
Taeho Kwon
Ali Sinan Köksal
Vincent Laviron
Matt Lewis
David Lo
Giuseppe Maggiore
Stephen Magill
Roman Manevich
Mark Marron
Damien Massé
Isabella Mastroeni
Laurent Mauborgne
Michael Monerau
David Monniaux

Mayur Naik
Do Thi Bich Ngoc
Durica Nikolic
Pavel Parizek
Nimrod Partush
Rasmus Lerchedahl Petersen
Carla Piazza
Ruzica Piskac
Sebastian Pop
Prathmesh Prabhu
Mohammad Raza
Guillaume Revy
Xavier Rival
Philipp Ruemmer
Sriram Sankaranarayanan
Hamadou Sardaouna
Francesca Scozzari
Ohad Shacham
Tushar Sharma
Rishabh Singh
Harald Søndergaard
Fausto Spoto
Manu Sridharan
Saurabh Srivastava
Christos Stergiou
Kohei Suenaga
Philippe Suter
Aditya Thakur
Hiroshi Unno
Martin Vechev
Jules Villard
Dimitrios Vytiniotis
Björn Wachter
Thomas Wies
Herbert Wiklicky
Liang Xu
Greta Yorsh
Enea Zaffanella
Florian Zuleger
Cameron Zwarich

Table of Contents

Widening and Interpolation 1
Kenneth L. McMillan

Program Analysis and Machine Learning: A Win-Win Deal 2
Aditya V. Nori and Sriram K. Rajamani

Program Analysis for Web Security 4
John C. Mitchell

Astrée: Design and Experience 5
Daniel Kästner

Formal Model Reduction 6
Jérôme Feret

Purity Analysis: An Abstract Interpretation Formulation 7
Ravichandhran Madhavan, Ganesan Ramalingam, and Kapil Vaswani

The Complexity of Abduction for Separated Heap Abstractions 25
Nikos Gorogiannis, Max Kanovich, and Peter W. O'Hearn

Efficient Decision Procedures for Heaps Using STRAND 43
P. Madhusudan and Xiaokang Qiu

The Flow-Insensitive Precision of Andersen's Analysis in Practice 60
Sam Blackshear, Bor-Yuh Evan Chang, Sriram Sankaranarayanan, and Manu Sridharan

Side-Effect Analysis of Assembly Code 77
Andrea Flexeder, Michael Petter, and Helmut Seidl

Directed Symbolic Execution 95
Kin-Keung Ma, Khoo Yit Phang, Jeffrey S. Foster, and Michael Hicks

Statically Validating Must Summaries for Incremental Compositional Dynamic Test Generation 112
Patrice Godefroid, Shuvendu K. Lahiri, and Cindy Rubio-González

On Sequentializing Concurrent Programs 129
Ahmed Bouajjani, Michael Emmi, and Gennaro Parlato

Verifying Fence Elimination Optimisations 146
Viktor Vafeiadis and Francesco Zappa Nardelli

An Efficient Static Trace Simplification Technique for Debugging Concurrent Programs 163
Jeff Huang and Charles Zhang

A Family of Abstract Interpretations for Static Analysis of Concurrent Higher-Order Programs 180
Matthew Might and David Van Horn

Abstract Domains of Affine Relations 198
Matt Elder, Junghee Lim, Tushar Sharma, Tycho Andersen, and Thomas Reps

Transitive Closures of Affine Integer Tuple Relations and Their Overapproximations 216
Sven Verdoolaege, Albert Cohen, and Anna Beletska

Logico-Numerical Abstract Acceleration and Application to the Verification of Data-Flow Programs 233
Peter Schrammel and Bertrand Jeannet

Invisible Invariants and Abstract Interpretation 249
Kenneth L. McMillan and Lenore D. Zuck

An Abstraction-Refinement Framework for Trigger Querying 263
Guy Avni and Orna Kupferman

Bound Analysis of Imperative Programs with the Size-Change Abstraction 280
Florian Zuleger, Sumit Gulwani, Moritz Sinn, and Helmut Veith

Satisfiability Modulo Recursive Programs 298
Philippe Suter, Ali Sinan Köksal, and Viktor Kuncak

Probabilistically Accurate Program Transformations 316
Sasa Misailovic, Daniel M. Roy, and Martin C. Rinard

Probabilistic Abstractions with Arbitrary Domains 334
Javier Esparza and Andreas Gaiser

Software Verification Using k-Induction 351
Alastair F. Donaldson, Leopold Haller, Daniel Kroening, and Philipp Rümmer

Using Bounded Model Checking to Focus Fixpoint Iterations 369
David Monniaux and Laure Gonnord

Author Index 387