Lecture Notes in Computer Science 4134

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

Editorial Board

David Hutchison
Lancaster University, UK

Takeo Kanade
Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler
University of Surrey, Guildford, UK

Jon M. Kleinberg
Cornell University, Ithaca, NY, USA

Friedemann Mattern
ETH Zurich, Switzerland

John C. Mitchell
Stanford University, CA, USA

Moni Naor
Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz
University of Bern, Switzerland

C. Pandu Rangan
Indian Institute of Technology, Madras, India

Bernhard Steffen
University of Dortmund, Germany

Madhu Sudan
Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos
University of California, Los Angeles, CA, USA

Doug Tygar
University of California, Berkeley, CA, USA

Moshe Y. Vardi
Rice University, Houston, TX, USA

Gerhard Weikum
Max-Planck Institute of Computer Science, Saarbruecken, Germany

Kwangkeun Yi (Ed.)

Static Analysis

13th International Symposium, SAS 2006
Seoul, Korea, August 29-31, 2006
Proceedings

Springer

Volume Editor

Kwangkeun Yi
Seoul National University
School of Computer Science and Engineering
Seoul 151-744, Korea
E-mail: kwang@ropas.snu.ac.kr

Library of Congress Control Number: 2006931004

CR Subject Classification (1998): D.3.2-3, F.3.1-2, D.2.8, F.4.2, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-540-37756-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-37756-6 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media

springer.com

© Springer-Verlag Berlin Heidelberg 2006
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11823230 06/3142 5 4 3 2 1 0

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 applicational advances in the area.

This volume contains the proceedings of the 13th International Static Analysis Symposium (SAS 2006), which was held 29-31 August 2006 at Seoul National University, Seoul, Korea. A total of 80 papers were submitted; the Program Committee held a 6-day long online discussion, during which they selected 23 papers. The selection was based on scientific quality, originality and relevance to the scope of SAS. Almost all submissions were reviewed by three (or more) PC members with the help of external reviewers.

In addition to the 23 accepted papers, this volume also contains abstracts of talks given by three invited speakers: Manuvir Das (Microsoft), Peter O'Hearn (Queen Mary, University of London), and Hongseok Yang (Seoul National University).

On behalf of the Program Committee, I would like to thank all of the authors who submitted papers. I would also like to thank the members of the Program Committee for their thorough reviews and dedicated involvement during the paper selection process, and all the external reviewers for their invaluable contributions. I would also like to thank the Steering Committee for their help and advice. Last but not least, I would like to thank Deokhwan Kim for his help in preparing this volume and in maintaining the on-line conference system, and Hyunjun Eo for the local arrangements.

June 2006 Kwangkeun Yi

Organization

Program Chair

Kwangkeun Yi	Seoul National University, Korea

Program Committee

Anindya Banerjee	Kansas State Univ., USA
Wei-Ngan Chin	National Univ. of Singapore, Singapore
Patrick Cousot	École Normale Supérieure, France
Roberto Giacobazzi	Univ. of Verona, Italy
Chris Hankin	Imperial College, UK)
Luddy Harrison	Univ. of Illinois at Urbana-Champaign, USA
Naoki Kobayashi	Tohoku Univ., Japan
Oukseh Lee	Hanyang Univ., Korea
Alan Mycroft	Univ. of Cambridge, UK
Kedar Namjoshi	Bell Labs., USA
Jens Palsberg	Univ. of California L.A., USA
Andreas Podelski	Max-Planck-Institut, Germany
Ganesan Ramalingam	IBM T.J.Watson Research, USA
Radu Rugina	Cornell Univ., USA
Harald Søndergaard	Univ. of Melbourne, Australia
Zhendong Su	Univ. of California Davis, USA
Reinhard Wilhelm	Univ. des Saarlandes, Germany

Steering Committee

Patrick Cousot	École Normale Supérieure, Paris, France
Giberto Filé	Univ. of Padova, Italy
David Schmidt	Kansas State Univ., USA

External Referees

Stefan Andrei	Julien Bertrane	Philppe Clauss
Roberto Bagnara	Silvia Breu	Christopher L. Conway
Joerg Bauer	Satish Chandra	Florin Craciun
Josh Berdine	Taehyoung Choi	Dennis Dams

Manuvir Das
William Deng
Olivia Rossi Doria
Manuel Fahndrich
Jerome Feret
John Field
Patrice Godefroid
Alexey Gotsman
Daniel Grund
Sumit Gulwani
Sebastian Hack
Atsushi Igarashi
François Irigoin
Bertrand Jeannet
Lingxiao Jiang
Jens Knoop
Roman Manevich
Isabella Mastroeni
Laurent Mauborgne
Benoit Meister
Alessio Merlo
Antoine Miné
Ghassan Misherghi
Anders Moller
David Monniaux
Huu Hai Nguyen
Ron Olsson
Corneliu Popeea
Shengchao Qin
Komondoor Raghavan
Venkatesh P. Ranganath
Francesco Ranzato
Jan Reineke
Noam Rinetzky
Xavier Rival
Mooly Sagiv
Hiroyuki Sato
Peter Schachte
David A. Schmidt
Hiroyuk Seki
Damien Sereni
Jakob Grue Simonsen
Jeremy Singer
Fausto Spoto
Bjarne Steensgard
Peter Stuckey
Kohei Suenaga
Eijiro Sumii
Yoshinori Tanabe
Stephan Thesing
Salvatore La Torre
Hiroshi Unno
Eben Upton
Martin Vechev
Bjoern Wachter
Gary Wassermann
Bernd Westphal
Thomas Wies
Jingling Xue
Eran Yahav
Enea Zaffanella
Damiano Zanardini

Sponsoring Institutions

Seoul National University
Korea Information Science Society (KISS)
KISS Special Interest Group on Programming Languages (SIGPL)

In Memoriam: Alain Deutsch (1965-2006)

It is with great sadness that we must note the untimely death of Alain Deutsch, one of the foremost researchers in static analysis.

From 1988 to 1992, Alain conducted his PhD research at Ecole Polytechnique, under the direction of Christian Queinnec and Patrick Cousot. His thesis, entitled *Modèles Opérationnels de Langage de Programmation et Représentations de Relations sur des Langages Rationnnels avec Application à la Détermination Statique de Propriétés de Partages Dynamiques de Données*, was a landmark work, employing abstract interpretation, temporal logic, and formal-language theory to produce powerful aliasing and lifetime analyses for data structures of programs in higher-order languages. Alain's development of "storeless semantics," where rational trees and right-regular equivalence relations are used in place of environments and stores to give access-path semantics to data structures, initiated a line of research that continues to this day.

Following post-doctoral studies at Carnegie-Mellon University, Alain joined INRIA Rocquencourt in 1993, where he continued his research in static analysis and published seminal papers in the Principles of Programming Languages (POPL) and Programming Language Design and Implementation (PLDI) conferences. With Patrick Cousot, he jointly supervised the PhD research of Bruno Blanchet.

Alain is perhaps best known for his efforts at Polyspace Technologies Company; at the time of his death, he was Polyspace's Chief Technical Officer. The company was an outgrowth of a project conducted by Alain and his colleagues at INRIA in 1996, where Alain's techniques were applied to a post-mortem analysis of the software of the Ariane 501 rocket. Their successes at error detection for the 501 and validation of the software of its successor, the Ariane 502, inspired Alain and Daniel Pilaud in 1999 to co-found Polyspace, a company dedicated to development of verification and validation tools for on-board, real-time software. At Polyspace, Alain helped produce a family of sophisticated tools that analyze annotation-free software to validate correct behavior in variable initialization, array indexing, arithmetic, type casts, and pointer deferencing — all the classic problems addressed by static analysis researchers, handled all together. Polyspace's tool set has been used with great success by companies in the aerospace, automotive, medical instrument, and defense industries, and the company has grown from a group of ten to a multi-national corporation with offices in France and the United States.

Above all, Alain was a brilliant, incredibly hard working, friendly, sympathetic individual. He will not be forgotten.

Table of Contents

Invited Talk

Unleashing the Power of Static Analysis 1
Manuvir Das

Session 1

Static Analysis in Disjunctive Numerical Domains 3
Sriram Sankaranarayanan, Franjo Ivančić, Ilya Shlyakhter, Aarti Gupta

Static Analysis of Numerical Algorithms 18
Eric Goubault, Sylvie Putot

Static Analysis of String Manipulations in Critical Embedded C Programs 35
Xavier Allamigeon, Wenceslas Godard, Charles Hymans

Session 2

Abstract Regular Tree Model Checking of Complex Dynamic Data Structures 52
Ahmed Bouajjani, Peter Habermehl, Adam Rogalewicz, Tomáš Vojnar

Structural Invariants 71
Ranjit Jhala, Rupak Majumdar, Ru-Gang Xu

Existential Label Flow Inference Via CFL Reachability 88
Polyvios Pratikakis, Jeffrey S. Foster, Michael Hicks

Session 3

Abstract Interpretation with Specialized Definitions 107
Germán Puebla, Elvira Albert, Manuel Hermenegildo

Underapproximating Predicate Transformers 127
David A. Schmidt

Combining Widening and Acceleration in Linear Relation Analysis 144
Laure Gonnord, Nicolas Halbwachs

Beyond Iteration Vectors: Instancewise Relational Abstract Domains 161
Pierre Amiranoff, Albert Cohen, Paul Feautrier

Invited Talk

Separation Logic and Program Analysis 181
Peter W. O'Hearn

Beyond Reachability: Shape Abstraction in the Presence of Pointer Arithmetic 182
Cristiano Calcagno, Dino Distefano, Peter W. O'Hearn, Hongseok Yang

Session 4

Specialized 3-Valued Logic Shape Analysis Using Structure-Based Refinement and Loose Embedding 204
Gilad Arnold

Recency-Abstraction for Heap-Allocated Storage 221
Gogul Balakrishnan, Thomas Reps

Interprocedural Shape Analysis with Separated Heap Abstractions 240
Alexey Gotsman, Josh Berdine, Byron Cook

Automated Verification of the Deutsch-Schorr-Waite Tree-Traversal Algorithm 261
Alexey Loginov, Thomas Reps, Mooly Sagiv

Invited Talk

Shape Analysis for Low-Level Code 280
Hongseok Yang

Session 5

Catching and Identifying Bugs in Register Allocation 281
Yuqiang Huang, Bruce R. Childers, Mary Lou Soffa

Certificate Translation for Optimizing Compilers 301
Gilles Barthe, Benjamin Grégoire, César Kunz, Tamara Rezk

Analysis of Low-Level Code Using Cooperating Decompilers 318
Bor-Yuh Evan Chang, Matthew Harren, George C. Necula

Session 6

Static Analysis for Java Servlets and JSP 336
Christian Kirkegaard, Anders Møller

Cryptographically-Masked Flows 353
Aslan Askarov, Daniel Hedin, Andrei Sabelfeld

Proving the Properties of Communicating Imperfectly-Clocked Synchronous Systems 370
Julien Bertrane

Session 7

Parametric and Termination-Sensitive Control Dependence 387
Feng Chen, Grigore Roşu

Memory Leak Analysis by Contradiction 405
Maksim Orlovich, Radu Rugina

Path-Sensitive Dataflow Analysis with Iterative Refinement 425
Dinakar Dhurjati, Manuvir Das, Yue Yang

Author Index 443