Frank Pfenning (Ed.)

LNCS 4098

Term Rewriting and Applications

17th International Conference, RTA 2006
Seattle, WA, USA, August 2006
Proceedings

Springer

Frank Pfenning (Ed.)

Term Rewriting and Applications

17th International Conference, RTA 2006
Seattle, WA, USA, August 12-14, 2006
Proceedings

Springer

Volume Editor

Frank Pfenning
Carnegie Mellon University
Department of Computer Science
Pittsburgh, PA 15213-3891, USA
E-mail: fp@cs.cmu.edu

Library of Congress Control Number: 2006929604

CR Subject Classification (1998): F.4, F.3.2, D.3, I.2.2-3, I.1

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

ISSN 0302-9743
ISBN-10 3-540-36834-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-36834-2 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 11805618 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 4098

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

Editorial Board

Preface

This volume contains the proceedings of the 17th International Conference on Rewriting Techniques and Applications, which was held on August 12–14, 2006 in Seattle, Washington, as part of of the 4th Federated Logic Conference (FLoC). RTA is the major forum for the presentation of research on all aspects of rewriting. Previous RTA conferences took place in Dijon (1985), Bordeaux (1987), Chapel Hill (1989), Como (1991), Montreal (1993), Kaiserslautern (1995), New Brunswick (1996), Sitges (1997), Tsukuba (1998), Trento (1999), Norwich (2000), Utrecht (2001), Copenhagen (2002), Valencia (2003), Aachen (2004), and Nara (2005).

A total of 23 regular papers and 4 system descriptions were selected for presentation from 52 submissions. Each paper was reviewed by at least 4 members of the Program Committee, with the help of 115 external referees. The committee decided to give the Best Paper Award for RTA 2006 to the contribution "Termination of String Rewriting with Matrix Interpretations" by Dieter Hofbauer and Johannes Waldmann for their original and powerful application of SAT solving in proving termination.

I would like to thank all the members of the Program Committee for their diligent, careful, and timely work and thoughtful deliberation, and Andrei Voronkov for providing the EasyChair system which greatly facilitated the reviewing process, the electronic Program Committee meeting, and the preparation of the program and the proceedings.

In addition to contributed papers, the program contained a FLoC plenary talk by Randal Bryant and two invited talks by Javier Esparza and Jürgen Giesl. I would like to thank the invited speakers not only for their presentations, but also for contributing abstracts or full papers to the proceedings.

RTA also sponsored a number of workshops held during FLoC, on the topics of Higher-Order Rewriting (HOR), Rule-Based Programming (RULE), Unification (UNIF), Reduction Strategies in Rewriting and Programming (WRS), Termination (WST), and a meeting of the IFIP Working Group 1.6 on Term Rewriting.

Many people helped to make RTA 2006 a success. I am particularly grateful to Ashish Tiwari, who took on the dual role of Conference Chair and RTA Workshop Chair, Ralf Treinen, the Publicity Chair, and Thomas Ball, Gopal Gupta, Jakob Rehof, and Moshe Vardi from the FLoC Organizing Committee who did an incredible amount of work in the arrangements for RTA and FLoC.

May 2006 Frank Pfenning

Conference Organization

Program Chair

Frank Pfenning	Carnegie Mellon University

Program Committee

Zena Ariola	University of Oregon
Franz Baader	Technical University Dresden
Gilles Dowek	École Polytechnique and INRIA
Guillem Godoy	Technical University of Catalonia
Deepak Kapur	University of New Mexico
Delia Kesner	University Paris 7
Denis Lugiez	University of Provence
Claude Marché	University Paris-Sud
Frank Pfenning	Carnegie Mellon University
Ashish Tiwari	SRI International
Yoshihito Toyama	Tohoku University
Eelco Visser	Utrecht University
Hans Zantema	Eindhoven University of Technology

Conference Chair

Ashish Tiwari	SRI International

RTA Steering Committee

Robert Nieuwenhuis	Technical University of Catalonia
Ralf Treinen	ENS Cachan, *Publicity Chair*
Jürgen Giesl	RWTH Aachen, *Chair*
Delia Kesner	University Paris 7
Vincent van Oostrom	Utrecht University
Ashish Tiwari	SRI International

FLoC Sponsors

Cadence
IBM
Microsoft Research

NEC
The John von Neumann Minerva Center
for the Development of Reactive Systems

FLoC Organizing Committee

Thomas Ball
Armin Biere
Sandro Etalle
Gopal Gupta
John Harrison
Manuel Hermenegildo
Lydia Kavraki
Stephan Kreutzer
Jacob Rehof
Nicole Schweikardt
Ashish Tiwari
Mirek Truszczynski
Moshe Y. Vardi
Margus Veanes

External Reviewers

Cuihtlauac Alvarado
Takahito Aoto
Albert Atserias
Patrick Baillot
Frédéric Blanqui
Eduardo Bonelli
Bernd Brassel
Martin Bravenboer
Pierre Castéran
Taolue Chen
Manuel Clavel
Thomas Colcombet
Evelyne Contejean
Jim Cordy
Solange Coupet-Grimal
Marcel Crabbé
Jeremy Dawson
Marie Duflot
Irène Durand
Joerg Endrullis
Stephan Falke
Berndt Farwer
Jean-Christophe Filliâtre
Robby Findler
Bernd Fischer
Julien Forest
Kim Gabarro
John Gallagher
Thomas Genet
Benny K. George
Silvio Ghilardi
Jürgen Giesl
Guillem Godoy
Bernhard Gramlich
Thomas Hallgren
Michael Hanus
Ryu Hasegawa
Sebastien Hemon
Joe Hendrix
Nao Hirokawa
Dieter Hofbauer
Martin Hofmann
Florent Jacquemard
Wolfram Kahl
Kentaro Kikuchi
Jan Willem Klop
Adam Koprowski
Masahito Kurihara
Pascal Lafourcade
Ugo dal Lago
Stéphane Lengrand
Jean-Jacques Lévy
Jordi Levy
Salvador Lucas
Bas Luttik
Ian Mackie
John Maraist
Luc Maranget
Massimo Marchiori
Ralph Matthes
Michel Mauny
Richard Mayr
Paul-André Melliès
Aart Middeldorp
Oege de Moor
Barbara Morawska
Sara Negri
Monica Nesi
Joachim Niehren
Robert Nieuwenhuis
Mizuhito Ogawa
Vincent van Oostrom
Vincent Padovani
Emir Pasalic
Adolfo Piperno
Emmanuel Polonowski
Jack M. Pullikottil
Femke van Raamsdonk
Jason Reed
Enric Rodríguez-Carbonell
Albert Rubio
Michel de Rougemont
Michael Rusinowitch

Amr Sabry
Masahiko Sakai
Hideki Sakurada
Luigi Santocanale
Manfred Schmidt-Schauß
Aleksy Schubert
Klaus Schulz
Peter Sestoft
Sandeep K. Shukla
Mark-Oliver Stehr
Sorin Stratulat
Toshinori Takai
Jean-Marc Talbot
René Thiemann
Andrew Tolmach
Ralf Treinen
Xavier Urbain
Christian Urban
Kumar Neeraj Verma
René Vestergaard
Luca Viganò
Laurent Vigneron
Mateu Villaret
Jérôme Vouillon
Johannes Waldmann
Daria Walukiewicz-Chrzaszcz
Andreas Weiermann
Benjamin Werner
Hongwei Xi
Toshiyuki Yamada
Ting Zhang
Calogero G. Zarba

Author Index

Lecture Notes in Computer Science

For information about Vols. 1–3992

please contact your bookseller or Springer

Vol. 4127: E. Damiani, P. Liu (Eds.), Data and Applications Security XX. X, 319 pages. 2006.

Vol. 4098: F. Pfenning (Ed.), Term Rewriting and Applications. XIII, 415 pages. 2006.

Vol. 4090: S. Spaccapietra, K. Aberer, P. Cudré-Mauroux (Eds.), Journal on Data Semantics VI. XI, 211 pages. 2006.

Vol. 4079: S. Etalle, M. Truszczyński (Eds.), Logic Programming. XIV, 474 pages. 2006.

Vol. 4077: M.-S. Kim, K. Shimada (Eds.), Advances in Geometric Modeling and Processing. XVI, 696 pages. 2006.

Vol. 4076: F. Hess, S. Pauli, M. Pohst (Eds.), Algorithmic Number Theory. X, 599 pages. 2006.

Vol. 4075: U. Leser, F. Naumann, B. Eckman (Eds.), Data Integration in the Life Sciences. XI, 298 pages. 2006. (Sublibrary LNBI).

Vol. 4074: M. Burmester, A. Yasinsac (Eds.), Secure Mobile Ad-hoc Networks and Sensors. X, 193 pages. 2006.

Vol. 4073: A. Butz, B. Fisher, A. Krüger, P. Olivier (Eds.), Smart Graphics. XI, 263 pages. 2006.

Vol. 4072: M. Harders, G. Székely (Eds.), Biomedical Simulation. XI, 216 pages. 2006.

Vol. 4071: H. Sundaram, M. Naphade, J.R. Smith, Y. Rui (Eds.), Image and Video Retrieval. XII, 547 pages. 2006.

Vol. 4069: F.J. Perales, R.B. Fisher (Eds.), Articulated Motion and Deformable Objects. XV, 526 pages. 2006.

Vol. 4068: H. Schärfe, P. Hitzler, P. Øhrstrøm (Eds.), Conceptual Structures: Inspiration and Application. XI, 455 pages. 2006. (Sublibrary LNAI).

Vol. 4067: D. Thomas (Ed.), ECOOP 2006 – Object-Oriented Programming. XIV, 527 pages. 2006.

Vol. 4066: A. Rensink, J. Warmer (Eds.), Model Driven Architecture – Foundations and Applications. XII, 392 pages. 2006.

Vol. 4065: P. Perner (Ed.), Advances in Data Mining. XI, 592 pages. 2006. (Sublibrary LNAI).

Vol. 4064: R. Büschkes, P. Laskov (Eds.), Detection of Intrusions and Malware & Vulnerability Assessment. X, 195 pages. 2006.

Vol. 4063: I. Gorton, G.T. Heineman, I. Crnkovic, H.W. Schmidt, J.A. Stafford, C.A. Szyperski, K. Wallnau (Eds.), Component-Based Software Engineering. XI, 394 pages. 2006.

Vol. 4062: G. Wang, J.F. Peters, A. Skowron, Y. Yao (Eds.), Rough Sets and Knowledge Technology. XX, 810 pages. 2006. (Sublibrary LNAI).

Vol. 4061: K. Miesenberger, J. Klaus, W. Zagler, A. Karshmer (Eds.), Computers Helping People with Special Needs. XXIX, 1356 pages. 2006.

Vol. 4060: K. Futatsugi, J.-P. Jouannaud, J. Meseguer (Eds.), Algebra, Meaning and Computation. XXXVIII, 643 pages. 2006.

Vol. 4059: L. Arge, R. Freivalds (Eds.), Algorithm Theory – SWAT 2006. XII, 436 pages. 2006.

Vol. 4058: L.M. Batten, R. Safavi-Naini (Eds.), Information Security and Privacy. XII, 446 pages. 2006.

Vol. 4057: J.P. W. Pluim, B. Likar, F.A. Gerritsen (Eds.), Biomedical Image Registration. XII, 324 pages. 2006.

Vol. 4056: P. Flocchini, L. Gąsieniec (Eds.), Structural Information and Communication Complexity. X, 357 pages. 2006.

Vol. 4055: J. Lee, J. Shim, S.-g. Lee, C. Bussler, S. Shim (Eds.), Data Engineering Issues in E-Commerce and Services. IX, 290 pages. 2006.

Vol. 4054: A. Horváth, M. Telek (Eds.), Formal Methods and Stochastic Models for Performance Evaluation. VIII, 239 pages. 2006.

Vol. 4053: M. Ikeda, K.D. Ashley, T.-W. Chan (Eds.), Intelligent Tutoring Systems. XXVI, 821 pages. 2006.

Vol. 4052: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part II. XXIV, 603 pages. 2006.

Vol. 4051: M. Bugliesi, B. Preneel, V. Sassone, I. Wegener (Eds.), Automata, Languages and Programming, Part I. XXIII, 729 pages. 2006.

Vol. 4049: S. Parsons, N. Maudet, P. Moraitis, I. Rahwan (Eds.), Argumentation in Multi-Agent Systems. XIV, 313 pages. 2006. (Sublibrary LNAI).

Vol. 4048: L. Goble, J.-J.C.. Meyer (Eds.), Deontic Logic and Artificial Normative Systems. X, 273 pages. 2006. (Sublibrary LNAI).

Vol. 4047: M. Robshaw (Ed.), Fast Software Encryption. XI, 434 pages. 2006.

Vol. 4046: S.M. Astley, M. Brady, C. Rose, R. Zwiggelaar (Eds.), Digital Mammography. XVI, 654 pages. 2006.

Vol. 4045: D. Barker-Plummer, R. Cox, N. Swoboda (Eds.), Diagrammatic Representation and Inference. XII, 301 pages. 2006. (Sublibrary LNAI).

Vol. 4044: P. Abrahamsson, M. Marchesi, G. Succi (Eds.), Extreme Programming and Agile Processes in Software Engineering. XII, 230 pages. 2006.

Vol. 4043: A.S. Atzeni, A. Lioy (Eds.), Public Key Infrastructure. XI, 261 pages. 2006.

Vol. 4042: D. Bell, J. Hong (Eds.), Flexible and Efficient Information Handling. XVI, 296 pages. 2006.

Vol. 4041: S.-W. Cheng, C.K. Poon (Eds.), Algorithmic Aspects in Information and Management. XI, 395 pages. 2006.

Vol. 4040: R. Reulke, U. Eckardt, B. Flach, U. Knauer, K. Polthier (Eds.), Combinatorial Image Analysis. XII, 482 pages. 2006.

Vol. 4039: M. Morisio (Ed.), Reuse of Off-the-Shelf Components. XIII, 444 pages. 2006.

Vol. 4038: P. Ciancarini, H. Wiklicky (Eds.), Coordination Models and Languages. VIII, 299 pages. 2006.

Vol. 4037: R. Gorrieri, H. Wehrheim (Eds.), Formal Methods for Open Object-Based Distributed Systems. XVII, 474 pages. 2006.

Vol. 4036: O. H. Ibarra, Z. Dang (Eds.), Developments in Language Theory. XII, 456 pages. 2006.

Vol. 4035: T. Nishita, Q. Peng, H.-P. Seidel (Eds.), Advances in Computer Graphics. XX, 771 pages. 2006.

Vol. 4034: J. Münch, M. Vierimaa (Eds.), Product-Focused Software Process Improvement. XVII, 474 pages. 2006.

Vol. 4033: B. Stiller, P. Reichl, B. Tuffin (Eds.), Performability Has its Price. X, 103 pages. 2006.

Vol. 4032: O. Etzion, T. Kuflik, A. Motro (Eds.), Next Generation Information Technologies and Systems. XIII, 365 pages. 2006.

Vol. 4031: M. Ali, R. Dapoigny (Eds.), Innovations in Applied Artificial Intelligence. XXIII, 1353 pages. 2006. (Sublibrary LNAI).

Vol. 4029: L. Rutkowski, R. Tadeusiewicz, L.A. Zadeh, J. Zurada (Eds.), Artificial Intelligence and Soft Computing – ICAISC 2006. XXI, 1235 pages. 2006. (Sublibrary LNAI).

Vol. 4027: H.L. Larsen, G. Pasi, D. Ortiz-Arroyo, T. Andreasen, H. Christiansen (Eds.), Flexible Query Answering Systems. XVIII, 714 pages. 2006. (Sublibrary LNAI).

Vol. 4026: P.B. Gibbons, T. Abdelzaher, J. Aspnes, R. Rao (Eds.), Distributed Computing in Sensor Systems. XIV, 566 pages. 2006.

Vol. 4025: F. Eliassen, A. Montresor (Eds.), Distributed Applications and Interoperable Systems. XI, 355 pages. 2006.

Vol. 4024: S. Donatelli, P. S. Thiagarajan (Eds.), Petri Nets and Other Models of Concurrency - ICATPN 2006. XI, 441 pages. 2006.

Vol. 4021: E. André, L. Dybkjær, W. Minker, H. Neumann, M. Weber (Eds.), Perception and Interactive Technologies. XI, 217 pages. 2006. (Sublibrary LNAI).

Vol. 4020: A. Bredenfeld, A. Jacoff, I. Noda, Y. Takahashi (Eds.), RoboCup 2005: Robot Soccer World Cup IX. XVII, 727 pages. 2006. (Sublibrary LNAI).

Vol. 4019: M. Johnson, V. Vene (Eds.), Algebraic Methodology and Software Technology. XI, 389 pages. 2006.

Vol. 4018: V. Wade, H. Ashman, B. Smyth (Eds.), Adaptive Hypermedia and Adaptive Web-Based Systems. XVI, 474 pages. 2006.

Vol. 4017: S. Vassiliadis, S. Wong, T.D. Hämäläinen (Eds.), Embedded Computer Systems: Architectures, Modeling, and Simulation. XV, 492 pages. 2006.

Vol. 4016: J.X. Yu, M. Kitsuregawa, H.V. Leong (Eds.), Advances in Web-Age Information Management. XVII, 606 pages. 2006.

Vol. 4014: T. Uustalu (Ed.), Mathematics of Program Construction. X, 455 pages. 2006.

Vol. 4013: L. Lamontagne, M. Marchand (Eds.), Advances in Artificial Intelligence. XIII, 564 pages. 2006. (Sublibrary LNAI).

Vol. 4012: T. Washio, A. Sakurai, K. Nakajima, H. Takeda, S. Tojo, M. Yokoo (Eds.), New Frontiers in Artificial Intelligence. XIII, 484 pages. 2006. (Sublibrary LNAI).

Vol. 4011: Y. Sure, J. Domingue (Eds.), The Semantic Web: Research and Applications. XIX, 726 pages. 2006.

Vol. 4010: S. Dunne, B. Stoddart (Eds.), Unifying Theories of Programming. VIII, 257 pages. 2006.

Vol. 4009: M. Lewenstein, G. Valiente (Eds.), Combinatorial Pattern Matching. XII, 414 pages. 2006.

Vol. 4008: J.C. Augusto, C.D. Nugent (Eds.), Designing Smart Homes. XI, 183 pages. 2006. (Sublibrary LNAI)

Vol. 4007: C. Àlvarez, M. Serna (Eds.), Experimental Algorithms. XI, 329 pages. 2006.

Vol. 4006: L.M. Pinho, M. González Harbour (Eds.), Reliable Software Technologies – Ada-Europe 2006. XII 241 pages. 2006.

Vol. 4005: G. Lugosi, H.U. Simon (Eds.), Learning Theory. XI, 656 pages. 2006. (Sublibrary LNAI).

Vol. 4004: S. Vaudenay (Ed.), Advances in Cryptology - EUROCRYPT 2006. XIV, 613 pages. 2006.

Vol. 4003: Y. Koucheryavy, J. Harju, V.B. Iversen (Eds.) Next Generation Teletraffic and Wired/Wireless Advanced Networking. XVI, 582 pages. 2006.

Vol. 4001: E. Dubois, K. Pohl (Eds.), Advanced Information Systems Engineering. XVI, 560 pages. 2006.

Vol. 3999: C. Kop, G. Fliedl, H.C. Mayr, E. Métais (Eds.) Natural Language Processing and Information Systems XIII, 227 pages. 2006.

Vol. 3998: T. Calamoneri, I. Finocchi, G.F. Italiano (Eds.), Algorithms and Complexity. XII, 394 pages 2006.

Vol. 3997: W. Grieskamp, C. Weise (Eds.), Formal Approaches to Software Testing. XII, 219 pages. 2006.

Vol. 3996: A. Keller, J.-P. Martin-Flatin (Eds.), Self-Managed Networks, Systems, and Services. X, 185 pages. 2006.

Vol. 3995: G. Müller (Ed.), Emerging Trends in Information and Communication Security. XX, 524 pages 2006.

Vol. 3994: V.N. Alexandrov, G.D. van Albada, P.M.A Sloot, J. Dongarra, Computational Science – ICCS 2006 Part IV. XXXV, 1096 pages. 2006.

Vol. 3993: V.N. Alexandrov, G.D. van Albada, P.M.A Sloot, J. Dongarra, Computational Science – ICCS 2006 Part III. XXXVI, 1136 pages. 2006.

Table of Contents

FLoC Plenary Talk

Session 1. Constraints and Optimization

Session 2. Equational Reasoning

Session 3. System Verification

Invited Talk

Session 4. Lambda Calculus

Session 5. Theorem Proving

Session 6. System Descriptions

Invited Talk

Session 7. Termination

Session 8. Higher-Order Rewriting and Unification

Formal Verification of Infinite State Systems Using Boolean Methods*

Randal E. Bryant

School of Computer Science, Carnegie Mellon University, Pittsburgh, PA
Randy.Bryant@cs.cmu.edu

Most successful automated formal verification tools are based on a bit-level model of computation, where a set of Boolean state variables encodes the system state. Using powerful inference engines, such as Binary Decision Diagrams (BDDs) and Boolean satisfiability (SAT) checkers, symbolic model checkers and similar tools can analyze all possible behaviors of very large, finite-state systems.

For many hardware and software systems, we would like to go beyond bit-level models to handle systems that are truly infinite state, or that are better modeled as infinite-state systems. Examples include programs manipulating integer data, concurrency protocols involving arbitrary numbers of processes, and systems containing buffers where the sizes are described parametrically.

Historically, much of the effort in verifying such systems involved automated theorem provers, requiring considerable guidance and expertise on the part of the user. We would like to devise approaches for these more expressive system models that retain the desirable features of model checking, such as the high degree of automation and the ability to generate counterexamples.

We have developed UCLID [1], a prototype verifier for infinite-state systems. The UCLID modeling language extends that of SMV [9], a bit-level model checker, to include state variables that are integers, as well as functions mapping integers to integers and integers to Booleans. Functional state variables can be used to define array and memory structures, including arrays of identical processes, FIFO buffers, and content-addressable memories.

System operation is defined in UCLID in terms of the initial values and next-state functions of the state variables. Integer operations include linear arithmetic and relational operations. Functions can be defined using uninterpreted function symbols, as well as via a restricted form of lambda expression. The underlying logic is reasonably expressive, yet it still permits a decision procedure that translates the formula into propositional logic and then uses a SAT solver [7].

UCLID supports multiple forms of verification, requiring different levels of sophistication in the handling of quantifiers. All styles verify that a safety property of the form $\forall \mathcal{X} P(s)$ holds for some set of system states s, where $\mathcal{X}$ denotes a set of integer *index variables*. Index variables can be used to express universal properties for all elements in an array of identical processes, all entries in a FIFO buffer, etc.

The simplest form of *bounded property checking* allows the user to determine that property $\forall \mathcal{X} P(s)$ holds for all states reachable within a fixed number of steps k from an

* This research was supported by the Semiconductor Research Corporation, Contract RID 1029.001.

F. Pfenning (Ed.): RTA 2006, LNCS 4098, pp. 1–3, 2006.

initial state. Verifying such a property can be done by direct application of the decision procedure. In practice, the effort required to verify such a property grows exponentially in k, limiting the verification to around 10–20 steps. However, it provides a useful debugging tool. In our experience, most errors are detected by this approach.

Of course, it is important to verify that properties hold for all reachable states of the system. Unfortunately, the standard fixed-point methods for bit-level model checking do not work for infinite-state systems. In many cases, the system will not reach a fixed point within a bounded number of steps. Even for those that do, checking convergence is undecidable, and our efforts to implement incomplete methods for this task have had limited success [2].

To prove that property $\forall \mathcal{X} P(s)$ holds for all reachable states s, UCLID supports *inductive invariant* checking, where the user provides an invariant Q such that Q holds for all initial states, Q implies P, and any successor for a state satisfying Q must also satisfy Q. This latter condition requires proving the validity of a formula containing existentially quantified index variables. Although this problem is undecidable for our logic, we have successfully implemented an incomplete approach using quantifier instantiation [8].

A more automated technique is to derive an inductive invariant via *predicate abstraction* [4]. Predicate abstraction operates much like the fixed-point methods of symbolic model checking, but using the concretization and abstraction operations of abstract interpretation [3] on each step. We have generalized predicate abstraction to handle the indexed predicates supported by UCLID [6]. Each step requires quantifier elimination to eliminate the current state variables, much like the relational product step of symbolic model checking. We implement this step by performing SAT enumeration on the translated Boolean formula.

As a final level of automation, we can automatically discover a set of relevant predicates for predicate abstraction based on the property P and the next-state expressions for the state variables [5].

We have successfully verified a number of systems with UCLID, including out-of-order microprocessors, distributed cache protocols, and distributed synchronization protocols.

References

1. R. E. Bryant, S. K. Lahiri, and S. A. Seshia. Modeling and verifying systems using a logic of counter arithmetic with lambda expressions and uninterpreted functions. In E. Brinksma and K. G. Larsen, editors, *Computer-Aided Verification (CAV '02)*, LNCS 2404, pages 78–92, 2002.
2. R. E. Bryant, S. K. Lahiri, and S. A. Seshia. Convergence testing in term-level bounded model checking. In *Correct Hardware Design and Verification Methods (CHARME '03)*, LNCS, September 2003.
3. P. Cousot and R. Cousot. Abstract interpretation : a unified lattice model for the static analysis of programs by construction or approximation of fixpoints. In *Principles of Programming Languages (POPL '77)*, pages 238–252, 1977.
4. S. Graf and H. Saïdi. Construction of abstract state graphs with PVS. In O. Grumberg, editor, *Computer-Aided Verification (CAV '97)*, LNCS 1254, pages 72–83, 1997.

5. S. K. Lahiri and R. E. Bryant. Indexed predicate discovery for unbounded system verification. In *Computer-Aided Verification (CAV '04)*, LNCS 3114, pages 135–147, 2004.
6. S. K. Lahiri and R. E. Bryant. Indexed predicate abstraction. *ACM Transactions on Computational Logic*, To appear.
7. S. K. Lahiri and S. A. Seshia. The UCLID decision procedure. In *Computer-Aided Verification (CAV '04)*, LNCS 3114, pages 475–478, 2004.
8. S. K. Lahiri, S. A. Seshia, and R. E. Bryant. Modeling and verification of out-of-order microprocessors in UCLID. In M. D. Aagaard and J. W. O'Leary, editors, *Formal Methods in Computer-Aided Design (FMCAD '02)*, LNCS 2517, pages 142–159, 2002.
9. K. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1992.