Frank Pfenning (Ed.)

LNAI 4603

Automated Deduction – CADE-21

21st International Conference on Automated Deduction
Bremen, Germany, July 2007
Proceedings

Springer

Frank Pfenning (Ed.)

Automated Deduction – CADE-21

21st International Conference on Automated Deduction
Bremen, Germany, July 17-20, 2007
Proceedings

Springer

Series Editors

Jaime G. Carbonell, Carnegie Mellon University, Pittsburgh, PA, USA
Jörg Siekmann, University of Saarland, Saarbrücken, Germany

Volume Editor

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

Library of Congress Control Number: 2007930705

CR Subject Classification (1998): I.2.3, F.4.1, F.3, F.4, D.2.4

LNCS Sublibrary: SL 7 – Artificial Intelligence

ISSN 0302-9743
ISBN-10 3-540-73594-1 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-73594-6 Springer Berlin Heidelberg New York

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12089642 06/3180 5 4 3 2 1 0

Lecture Notes in Artificial Intelligence 4603

Edited by J. G. Carbonell and J. Siekmann

Subseries of Lecture Notes in Computer Science

Lecture Notes in Artificial Intelligence (LNAI)

Vol. 4612: I. Miguel, W. Ruml (Eds.), Abstraction, Reformulation, and Approximation. XI, 418 pages. 2007.

Vol. 4604: U. Priss, S. Polovina, R. Hill (Eds.), Conceptual Structures: Knowledge Architecture for Smart Applications. XII, 514 pages. 2007.

Vol. 4603: F. Pfenning (Ed.), Automated Deduction – CADE-21. XII, 522 pages. 2007.

Vol. 4597: P. Perner (Ed.), Advances in Data Mining. XI, 353 pages. 2007.

Vol. 4594: R. Bellazzi, A. Abu-Hanna, J. Hunter (Eds.), Artificial Intelligence in Medicine. XVI, 509 pages. 2007.

Vol. 4585: M. Kryszkiewicz, J.F. Peters, H. Rybinski, A. Skowron (Eds.), Rough Sets and Intelligent Systems Paradigms. XIX, 836 pages. 2007.

Vol. 4578: F. Masulli, S. Mitra, G. Pasi (Eds.), Applications of Fuzzy Sets Theory. XVIII, 693 pages. 2007.

Vol. 4573: M. Kauers, M. Kerber, R. Miner, W. Windsteiger (Eds.), Towards Mechanized Mathematical Assistants. XIII, 407 pages. 2007.

Vol. 4571: P. Perner (Ed.), Machine Learning and Data Mining in Pattern Recognition. XIV, 913 pages. 2007.

Vol. 4570: H.G. Okuno, M. Ali (Eds.), New Trends in Applied Artificial Intelligence. XXI, 1194 pages. 2007.

Vol. 4565: D.D. Schmorrow, L.M. Reeves (Eds.), Foundations of Augmented Cognition. XIX, 450 pages. 2007.

Vol. 4562: D. Harris (Ed.), Engineering Psychology and Cognitive Ergonomics. XXIII, 879 pages. 2007.

Vol. 4548: N. Olivetti (Ed.), Automated Reasoning with Analytic Tableaux and Related Methods. X, 245 pages. 2007.

Vol. 4539: N.H. Bshouty, C. Gentile (Eds.), Learning Theory. XII, 634 pages. 2007.

Vol. 4529: P. Melin, O. Castillo, L.T. Aguilar, J. Kacprzyk, W. Pedrycz (Eds.), Foundations of Fuzzy Logic and Soft Computing. XIX, 830 pages. 2007.

Vol. 4511: C. Conati, K. McCoy, G. Paliouras (Eds.), User Modeling 2007. XVI, 487 pages. 2007.

Vol. 4509: Z. Kobti, D. Wu (Eds.), Advances in Artificial Intelligence. XII, 552 pages. 2007.

Vol. 4496: N.T. Nguyen, A. Grzech, R.J. Howlett, L.C. Jain (Eds.), Agent and Multi-Agent Systems: Technologies and Applications. XXI, 1046 pages. 2007.

Vol. 4483: C. Baral, G. Brewka, J. Schlipf (Eds.), Logic Programming and Nonmonotonic Reasoning. IX, 327 pages. 2007.

Vol. 4482: A. An, J. Stefanowski, S. Ramanna, C.J. Butz, W. Pedrycz, G. Wang (Eds.), Rough Sets, Fuzzy Sets, Data Mining and Granular Computing. XIV, 585 pages. 2007.

Vol. 4481: J. Yao, P. Lingras, W.-Z. Wu, M. Szczuka, N.J. Cercone, D. Ślęzak (Eds.), Rough Sets and Knowledge Technology. XIV, 576 pages. 2007.

Vol. 4476: V. Gorodetsky, C. Zhang, V.A. Skormin, L. Cao (Eds.), Autonomous Intelligent Systems: Multi-Agents and Data Mining. XIII, 323 pages. 2007.

Vol. 4452: M. Fasli, O. Shehory (Eds.), Agent-Mediated Electronic Commerce. VIII, 249 pages. 2007.

Vol. 4451: T.S. Huang, A. Nijholt, M. Pantic, A. Pentland (Eds.), Artifical Intelligence for Human Computing. XVI, 359 pages. 2007.

Vol. 4438: L. Maicher, A. Sigel, L.M. Garshol (Eds.), Leveraging the Semantics of Topic Maps. X, 257 pages. 2007.

Vol. 4429: R. Lu, J.H. Siekmann, C. Ullrich (Eds.), Cognitive Systems. X, 161 pages. 2007.

Vol. 4426: Z.-H. Zhou, H. Li, Q. Yang (Eds.), Advances in Knowledge Discovery and Data Mining. XXV, 1161 pages. 2007.

Vol. 4411: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), Programming Multi-Agent Systems. XIV, 249 pages. 2007.

Vol. 4410: A. Branco (Ed.), Anaphora: Analysis, Algorithms and Applications. X, 191 pages. 2007.

Vol. 4399: T. Kovacs, X. Llorà, K. Takadama, P.L. Lanzi, W. Stolzmann, S.W. Wilson (Eds.), Learning Classifier Systems. XII, 345 pages. 2007.

Vol. 4390: S.O. Kuznetsov, S. Schmidt (Eds.), Formal Concept Analysis. X, 329 pages. 2007.

Vol. 4389: D. Weyns, H.V.D. Parunak, F. Michel (Eds.), Environments for Multi-Agent Systems III. X, 273 pages. 2007.

Vol. 4384: T. Washio, K. Satoh, H. Takeda, A. Inokuchi (Eds.), New Frontiers in Artificial Intelligence. IX, 401 pages. 2007.

Vol. 4371: K. Inoue, K. Satoh, F. Toni (Eds.), Computational Logic in Multi-Agent Systems. X, 315 pages. 2007.

Vol. 4369: M. Umeda, A. Wolf, O. Bartenstein, U. Geske, D. Seipel, O. Takata (Eds.), Declarative Programming for Knowledge Management. X, 229 pages. 2006.

Vol. 4342: H. de Swart, E. Orłowska, G. Schmidt, M. Roubens (Eds.), Theory and Applications of Relational Structures as Knowledge Instruments II. X, 373 pages. 2006.

Vol. 4335: S.A. Brueckner, S. Hassas, M. Jelasity, D. Yamins (Eds.), Engineering Self-Organising Systems. XII, 212 pages. 2007.

Vol. 4334: B. Beckert, R. Hähnle, P.H. Schmitt (Eds.), Verification of Object-Oriented Software. XXIX, 658 pages. 2007.

Vol. 4333: U. Reimer, D. Karagiannis (Eds.), Practical Aspects of Knowledge Management. XII, 338 pages. 2006.

Vol. 4327: M. Baldoni, U. Endriss (Eds.), Declarative Agent Languages and Technologies IV. VIII, 257 pages. 2006.

Vol. 4314: C. Freksa, M. Kohlhase, K. Schill (Eds.), KI 2006: Advances in Artificial Intelligence. XII, 458 pages. 2007.

Vol. 4304: A. Sattar, B.-h. Kang (Eds.), AI 2006: Advances in Artificial Intelligence. XXVII, 1303 pages. 2006.

Vol. 4303: A. Hoffmann, B.-h. Kang, D. Richards, S. Tsumoto (Eds.), Advances in Knowledge Acquisition and Management. XI, 259 pages. 2006.

Vol. 4293: A. Gelbukh, C.A. Reyes-Garcia (Eds.), MICAI 2006: Advances in Artificial Intelligence. XXVIII, 1232 pages. 2006.

Vol. 4289: M. Ackermann, B. Berendt, M. Grobelnik, A. Hotho, D. Mladenič, G. Semeraro, M. Spiliopoulou, G. Stumme, V. Svátek, M. van Someren (Eds.), Semantics, Web and Mining. X, 197 pages. 2006.

Vol. 4285: Y. Matsumoto, R.W. Sproat, K.-F. Wong, M. Zhang (Eds.), Computer Processing of Oriental Languages. XVII, 544 pages. 2006.

Vol. 4274: Q. Huo, B. Ma, E.-S. Chng, H. Li (Eds.), Chinese Spoken Language Processing. XXIV, 805 pages. 2006.

Vol. 4265: L. Todorovski, N. Lavrač, K.P. Jantke (Eds.), Discovery Science. XIV, 384 pages. 2006.

Vol. 4264: J.L. Balcázar, P.M. Long, F. Stephan (Eds.), Algorithmic Learning Theory. XIII, 393 pages. 2006.

Vol. 4259: S. Greco, Y. Hata, S. Hirano, M. Inuiguchi, S. Miyamoto, H.S. Nguyen, R. Słowiński (Eds.), Rough Sets and Current Trends in Computing. XXII, 951 pages. 2006.

Vol. 4253: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part III. XXXII, 1301 pages. 2006.

Vol. 4252: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part II. XXXIII, 1335 pages. 2006.

Vol. 4251: B. Gabrys, R.J. Howlett, L.C. Jain (Eds.), Knowledge-Based Intelligent Information and Engineering Systems, Part I. LXVI, 1297 pages. 2006.

Vol. 4248: S. Staab, V. Svátek (Eds.), Managing Knowledge in a World of Networks. XIV, 400 pages. 2006.

Vol. 4246: M. Hermann, A. Voronkov (Eds.), Logic for Programming, Artificial Intelligence, and Reasoning. XIII, 588 pages. 2006.

Vol. 4223: L. Wang, L. Jiao, G. Shi, X. Li, J. Liu (Eds.), Fuzzy Systems and Knowledge Discovery. XXVIII, 1335 pages. 2006.

Vol. 4213: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Knowledge Discovery in Databases: PKDD 2006. XXII, 660 pages. 2006.

Vol. 4212: J. Fürnkranz, T. Scheffer, M. Spiliopoulou (Eds.), Machine Learning: ECML 2006. XXIII, 851 pages. 2006.

Vol. 4211: P. Vogt, Y. Sugita, E. Tuci, C.L. Nehaniv (Eds.), Symbol Grounding and Beyond. VIII, 237 pages. 2006.

Vol. 4203: F. Esposito, Z.W. Raś, D. Malerba, G. Semeraro (Eds.), Foundations of Intelligent Systems. XVIII, 767 pages. 2006.

Vol. 4201: Y. Sakakibara, S. Kobayashi, K. Sato, T. Nishino, E. Tomita (Eds.), Grammatical Inference: Algorithms and Applications. XII, 359 pages. 2006.

Vol. 4200: I.F.C. Smith (Ed.), Intelligent Computing in Engineering and Architecture. XIII, 692 pages. 2006.

Vol. 4198: O. Nasraoui, O. Zaïane, M. Spiliopoulou, B. Mobasher, B. Masand, P.S. Yu (Eds.), Advances in Web Mining and Web Usage Analysis. IX, 177 pages. 2006.

Vol. 4196: K. Fischer, I.J. Timm, E. André, N. Zhong (Eds.), Multiagent System Technologies. X, 185 pages. 2006.

Vol. 4188: P. Sojka, I. Kopeček, K. Pala (Eds.), Text, Speech and Dialogue. XV, 721 pages. 2006.

Vol. 4183: J. Euzenat, J. Domingue (Eds.), Artificial Intelligence: Methodology, Systems, and Applications. XIII, 291 pages. 2006.

Vol. 4180: M. Kohlhase, OMDoc – An Open Markup Format for Mathematical Documents [version 1.2]. XIX, 428 pages. 2006.

Vol. 4177: R. Marín, E. Onaindía, A. Bugarín, J. Santos (Eds.), Current Topics in Artificial Intelligence. XV, 482 pages. 2006.

Vol. 4160: M. Fisher, W. van der Hoek, B. Konev, A. Lisitsa (Eds.), Logics in Artificial Intelligence. XII, 516 pages. 2006.

Vol. 4155: O. Stock, M. Schaerf (Eds.), Reasoning, Action and Interaction in AI Theories and Systems. XVIII, 343 pages. 2006.

Vol. 4149: M. Klusch, M. Rovatsos, T.R. Payne (Eds.), Cooperative Information Agents X. XII, 477 pages. 2006.

Vol. 4140: J.S. Sichman, H. Coelho, S.O. Rezende (Eds.), Advances in Artificial Intelligence - IBERAMIA-SBIA 2006. XXIII, 635 pages. 2006.

Vol. 4139: T. Salakoski, F. Ginter, S. Pyysalo, T. Pahikkala (Eds.), Advances in Natural Language Processing. XVI, 771 pages. 2006.

Vol. 4133: J. Gratch, M. Young, R. Aylett, D. Ballin, P. Olivier (Eds.), Intelligent Virtual Agents. XIV, 472 pages. 2006.

Vol. 4130: U. Furbach, N. Shankar (Eds.), Automated Reasoning. XV, 680 pages. 2006.

Vol. 4120: J. Calmet, T. Ida, D. Wang (Eds.), Artificial Intelligence and Symbolic Computation. XIII, 269 pages. 2006.

¥689.00元

Preface

This volume contains the proceedings of the 21st International Conference on Automated Deduction, which was held July 17–20, 2007 at the Jacobs University in Bremen, Germany. CADE is the major forum for the presentation of research in all aspects of automated deduction. There were also a number of affiliated workshops on the days preceding CADE, which helped to make the conference a success.

A total of 28 regular papers and 6 system descriptions were selected for presentation from 64 submissions. Each submission was reviewed by at least 4 members of the Program Committee, with the help of 115 external referees. I would like to thank all the members of the Program Committee for their diligent, careful, and timely work and thoughtful deliberations, and Andrei Voronkov for providing the EasyChair system which greatly facilitated the reviewing process, the electronic Program Committee meeting, and the preparation of the proceedings.

In addition to the contributed papers, the program contained four invited talks by Peter Baumgartner, Rustan Leino, Colin Stirling, and Ashish Tiwari. I would like to thank the invited speakers not only for their presentations, but also for contributing abstracts or full papers to the proceedings.

During the conference, the 2007 Herbrand Award for Distinguished Contributions to Automated Reasoning was given to Alan Bundy in recognition of his outstanding contributions to proof planning and inductive theorem proving, as well as to many other areas of automated reasoning and artificial intelligence.

Many people helped to make CADE-21 a success. I am particularly grateful to Michael Kohlhase (Conference Chair), Christoph Benzmüller (Workshop Chair), Amy Felty (CADE Secretary and Publicity Chair), Geoff Sutcliffe (CASC Chair), and all the individual workshop organizers.

May 2007

Frank Pfenning

Conference Organization

Program Chair

Frank Pfenning	Carnegie Mellon University

Program Committee

David Basin	ETH Zürich
Christoph Benzmüller	The University of Cambridge
Maria Paola Bonacina	Università degli Studi di Verona
Simon Colton	Imperial College London
Gilles Dowek	École Polytechnique
Rajeev Goré	Australian National University
Jean Goubault-Larrecq	ENS Cachan
Reiner Hähnle	Chalmers University of Technology
John Harrison	Intel Corporation
Michael Kohlhase	Jacobs University Bremen
Dale Miller	INRIA-Futurs and École Polytechnique
Tobias Nipkow	Technical University Munich
Hans de Nivelle	University of Wroclaw
Albert Oliveras	Technical University of Catalonia
Frank Pfenning	Carnegie Mellon University
Ulrike Sattler	University of Manchester
Manfred Schmidt-Schauß	University of Frankfurt
Cesare Tinelli	University of Iowa
Andrei Voronkov	University of Manchester
Toby Walsh	National ICT Australia and University of New South Wales

Conference Chair

Michael Kohlhase	Jacobs University Bremen

Workshop Chair

Christoph Benzmüller	The University of Cambridge

System Competition

Geoff Sutcliffe	University of Miami

External Reviewers

Wolfgang Ahrendt
Anbulagan
Flemming Andersen
Serge Autexier
David Baelde
Marc Bezem
Jesse Bingham
Magnus Björk
Richard Bonichon
Achim Brucker
Richard Bubel
Linda Buisman
Elie Bursztein
Amine Chaieb
Ching-Tsun Chou
Koen Claessen
Hubert Comon-Lundh
Cas Cremers
Jeremy Dawson
Christian Dax
Anatoli Degtyarev
Louise Dennis
Francesco Donini
Mnacho Echenim
Amy Felty
Christian Fermueller
Maribel Fernandez
Jean-Christophe Filliatre
Alexander Fuchs
Murdoch Gabbay
Didier Galmiche
Silvio Ghilardi
Martin Giese
Juergen Giesl
Birte Glimm
Guillem Godoy
Amit Goel
Jeremy Gow
Bernhard Gramlich
Jim Grundy
Olivier Hermant
Jan Hladik
Ullrich Hustadt
Dieter Hutter
Paul Jackson
Felix Klaedtke
Gerwin Klein
Konstantin Korovin
Laura Kovacs
Alexander Krauss
Sava Krstic
Oliver Kullmann
Hermann Lehner
Christopher Lynch
Michael Maher
Maarten Marx
Fabio Massacci
Laurent Mauborgne
Stefan Maus
William McCune
Jia Meng
Tommie Meyer
Aart Middeldorp
Jean-Francois Monin
Boris Motik
Normen Mueller
Cesar Munoz
Juan Antonio Navarro Perez
Linh Nguyen
Joachim Niehren
Robert Nieuwenhuis
Immanuel Normann
Michael Norrish
Jens Otten
Peter Patel-Schneider
Christine Paulin-Mohring
Larry Paulson
Andrew Pitts
Randy Pollack
Florian Rabe
Silvio Ranise
Christophe Ringeissen
Enric Rodriguez-Carbonell
Philipp Ruemmer
Michael Rusinowitch
David Sabel
Alexis Saurin
Gerhard Schellhorn
Marvin Schiller
Norbert Schirmer
Lutz Schröder
Stephan Schulz
Jan Schwinghammer
Rob Shearer
Andrew Slater
Viorica Sofronie-Stokkermans
Volker Sorge
Christoph Sprenger
Graham Steel
Werner Stephan
Lutz Strassburger
Murali Talupur
Dmitry Tsarkov
Tarmo Uustalu
David Wahlstedt
Angela Wallenburg
Makarius Wenzel
Freek Wiedijk
Claus-Peter Wirth
Burkhard Wolff
Jin Yang
Calogero Zarba
Evgeny Zolin
Roland Zumkeller

Table of Contents

Session 6. Satisfiability Modulo Theories

Session 7. Induction, Rewriting, and Polymorphism

Session 8. First-Order Logic

Session 9. Invited Talk: K. Rustan M. Leino

Session 10. Model Checking and Verification

Session 11. Invited Talk: Peter Baumgartner

Session 12. Termination

Session 13. Tableaux and First-Order Systems

Games, Automata and Matching

Colin Stirling

School of Informatics
University of Edinburgh
cps@inf.ed.ac.uk

Higher-order matching is the problem given $t = u$ where t, u are terms of simply typed λ-calculus and u is closed, is there a substitution θ such that $t\,\theta$ and u have the same normal form with respect to $\beta\eta$-equality: can t be pattern matched to u? The problem was conjectured to be decidable by Huet [4]. Loader showed that it is undecidable when β-equality is the same normal form by encoding λ-definability as matching [6].

In previous work, we confirm Huet's conjecture [12]: a full (and very complicated) proof is in the long version of [12] available from the author's web page. It first appeals to Padovani's and Schubert's reduction of matching to the conceptually simpler (dual) interpolation problem [9,8]. It is then inspired by model-checking games (such as in [10]) where a model, a transition graph, is traversed relative to a property and players make choices at appropriate positions. We define a game where the model is a closed λ-term t and play moves around it relative to a (dual) interpolation problem P. The game captures the dynamics of β-reduction on t without changing it (using substitution). Unlike standard model-checking games, play may arbitrarily jump around a term because of binding. The principal virtue of the game is that small pieces of a solution term can be understood in terms of their subplays and how they, thereby, contribute to solving the problem P. Simple transformations on terms are defined and combinatorial properties shown. Decidability of matching follows from the *small model property*: if there is a solution to a problem then there is a small solution to it. The proof of this property uses "unfolding" a λ-term with respect to game playing, analogous to unravelling a transition system in modal logic, followed by its inverse refolding.

In the talk our interest is with a different, although related, question: can we independently characterize the set of *all* solution terms to an interpolation problem? Part of the hope is that this may lead to a simpler proof of decidability of matching. Again, we start with the term checking game. However, we slightly reformulate it and show that it underpins an automata-theoretic characterization relative to *resource*: given a problem P, a finite set of variables and constants the (possibly infinite) set of terms that are built from those components and that solve P is regular. The characterization uses standard bottom-up tree automata. The states of the automaton are built from abstractions of sequences of moves in the game. The automaton construction works for all orders. Comon and Jurski define tree automata that characterize all solutions to a 4th-order problem [2]. The states of their automata appeal to Padovani's observational equivalence classes of terms [8]. To define the states of their automata at higher-orders, one

F. Pfenning (Ed.): CADE 2007, LNAI 4603, pp. 1–2, 2007.

would need to solve the problem of how to quotient the potentially infinite set of terms into their respective finite observational equivalence classes: however, as Padovani shows this problem is, in fact, equivalent to the matching problem itself. Ong shows decidability of monadic second-order logic of the tree generated by an arbitrary higher-order scheme [7]. The proof uses a game-semantic characterization of a scheme as an infinite λ-term. A property, expressed as an alternating parity tree automaton, of the tree has to be transferred to the infinite term. A key ingredient of the transition from game to automaton is Ong's abstraction "variable profile" that captures a sequence of back-and-forth play jumping in a term which is also central to our analysis.

References

1. Comon, H., Dauchet, M., Gilleron, R., Jacquemard, F., Lugiez, D., Tison, S., Tommasi, M.: Tree Automata Techniques and Applications. Draft Book (2002) `http://l3ux02.univ-lille3.fr/tata/`
2. Comon, H., Jurski, Y.: Higher-order matching and tree automata. In: Nielsen, M. (ed.) CSL 1997. LNCS, vol. 1414, pp. 157–176. Springer, Heidelberg (1998)
3. Dowek, G.: Higher-order unification and matching. In: Robinson, A., Voronkov, A. (ed.) Handbook of Automated Reasoning, vol. 2, pp. 1009–1062, North-Holland (2001)
4. Huet, G.: Rèsolution d'èquations dans les langages d'ordre 1, 2, ... ω. Thèse de doctorat d'ètat, Universitè Paris VII (1976)
5. Jung, A., Tiuryn, J.: A new characterisation of lambda definability. In: Bezem, M., Groote, J.F. (eds.) TLCA 1993. LNCS, vol. 664, pp. 245–257. Springer, Heidelberg (1993)
6. Loader, R.: Higher-order β-matching is undecidable. Logic Journal of the IGPL 11(1), 51–68 (2003)
7. Ong, C.-H.L.: On model-checking trees generated by higher-order recursion schemes. In: Procs LICS, pp. 81–90 (Longer version available from Ong's web page) (2006)
8. Padovani, V.: Decidability of fourth-order matching. Mathematical Structures in Computer Science 10(3), 361–372 (2001)
9. Schubert, A.: Linear interpolation for the higher-order matching problem. In: Bidoit, M., Dauchet, M. (eds.) CAAP 1997, FASE 1997, and TAPSOFT 1997. LNCS, vol. 1214, pp. 441–452. Springer, Heidelberg (1997)
10. Stirling, C.: Modal and Temporal Properties of Processes. In: Texts in Computer Science, Springer, Heidelberg (2001)
11. Stirling, C.: Higher-order matching and games. In: Ong, L. (ed.) CSL 2005. LNCS, vol. 3634, pp. 119–134. Springer, Heidelberg (2005)
12. Stirling, C.: A game-theoretic approach to deciding higher-order matching. In: Bugliesi, M., Preneel, B., Sassone, V., Wegener, I. (eds.) ICALP 2006. LNCS, vol. 4052, pp. 348–359. Springer, Heidelberg (2006)

Formalization of Continuous Probability Distributions

Osman Hasan and Sofiène Tahar

Dept. of Electrical & Computer Engineering, Concordia University
1455 de Maisonneuve W., Montreal, Quebec, H3G 1M8, Canada
{o_hasan,tahar}@ece.concordia.ca

Abstract. Continuous probability distributions are widely used to mathematically describe random phenomena in engineering and physical sciences. In this paper, we present a methodology that can be used to formalize any continuous random variable for which the inverse of the cumulative distribution function can be expressed in a closed mathematical form. Our methodology is primarily based on the Standard Uniform random variable, the classical cumulative distribution function properties and the Inverse Transform method. The paper includes the higher-order-logic formalization details of these three components in the HOL theorem prover. To illustrate the practical effectiveness of the proposed methodology, we present the formalization of Exponential, Uniform, Rayleigh and Triangular random variables.

1 Introduction

Theorem proving [7] is an interactive verification approach that can be used to prove mathematical theorems in a computer based environment. Due to its inherent soundness, theorem proving is capable of providing precise answers and is thus more powerful than testing or simulation-based system analysis techniques. In this paper, we propose to perform probabilistic analysis within the environment of a higher-order-logic theorem prover in order to overcome the inaccuracy and enormous CPU time requirement limitations of state-of-the-art simulation based probabilistic analysis approaches.

The foremost criteria for constructing a theorem-proving based probabilistic analysis framework is to be able to formalize the commonly used random variables in higher-order logic. This formalized library of random variables can be utilized to express random behavior exhibited by systems and the corresponding probabilistic properties can then be proved within the sound environment of an interactive theorem prover. Random variables are basically functions that map random events to numbers and they can be expressed in a computerized environment as probabilistic algorithms. In his PhD thesis, Hurd [14] presented a methodology for the verification of probabilistic algorithms in the higher-order-logic (HOL) theorem prover [8]. Hurd was also able to formalize a few discrete random variables and verify their corresponding distribution properties. On the

F. Pfenning (Ed.): CADE 2007, LNAI 4603, pp. 3–18, 2007.

other hand, to the best of our knowledge, no higher-order-logic formalization of continuous random variables exists in the open literature so far.

In this paper, we propose a methodology for the formalization of continuous random variables in HOL. Our methodology utilizes Hurd's formalization framework and is based on the concept of the nonuniform random number generation [5], which is the process of obtaining random variates of arbitrary distributions using a Standard Uniform random number generator. The main advantage of this approach is that we only need to formalize one continuous random variable from scratch, i.e., the Standard Uniform random variable, which can be used to model other continuous random variables by formalizing the corresponding nonuniform random number generation method.

Based on the above methodology, we now present a framework, illustrated in Figure 1, for the formalization of continuous probability distributions for which the inverse of the *Cumulative Distribution Function* (CDF) can be represented in a closed mathematical form. Firstly, we formally specify the Standard Uniform random variable and verify its correctness by proving the corresponding CDF and measurability properties. The next step is the formalization of the CDF and the verification of its classical properties. Then we formally specify the mathematical concept of the inverse function of a CDF. This formal specification, along with the formalization of the Standard Unform random variable and the CDF properties, can be used to formally verify the correctness of the *Inverse Transform Method* (ITM) [5], which is a well known nonuniform random generation technique for generating nonuniform random variates for continuous probability distributions for which the inverse of the CDF can be represented in a closed mathematical form. At this point, the formalized Standard Uniform random variable can be used to formally specify any such continuous random variable and its corresponding CDF can be verified using the ITM.

The rest of the paper is organized as follows: In Section 2, we briefly review Hurd's methodology for the verification of probabilistic algorithms in HOL. The next three sections of this paper present the HOL formalization of the three major steps given in Figure 1, i.e., the Standard Uniform random variable, the CDF and the ITM. In Section 6, we utilize the proposed framework of Figure

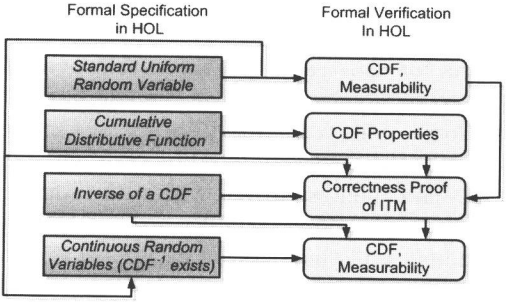

Fig. 1. Proposed Formalization Framework