

Sergei N. Artemov
Anil Nerode (Eds.)

LNCS 4514

Logical Foundations of Computer Science

International Symposium, LFCS 2007
New York, NY, USA, June 2007
Proceedings



Springer

TP3-53
L687
2007

Sergei N. Artemov Anil Nerode (Eds.)

Logical Foundations of Computer Science

International Symposium, LFCS 2007
New York, NY, USA, June 4-7, 2007
Proceedings



 Springer



E2007003257

Volume Editors

Sergei N. Artemov
CUNY Graduate Center
Computer Science
365 Fifth Ave., New York City, NY 10016, USA
E-mail: Sartemov@gc.cuny.edu

Anil Nerode
Cornell University
Department of Mathematics
545 Malott Hall, Ithaca NY 14853, USA
E-mail: anil@math.cornell.edu

Library of Congress Control Number: 2007927056

CR Subject Classification (1998): F.4.1, F.4, F.3, I.2.2-4

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

ISSN 0302-9743
ISBN-10 3-540-72732-9 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-72732-3 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 2007
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12067930 06/3180 5 4 3 2 1 0

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

Preface

The Symposium on Logical Foundations of Computer Science series provides a forum for the fast-growing body of work in the logical foundations of computer science, e.g., those areas of fundamental theoretical logic related to computer science. The LFCS series began with “Logic at Botik,” Pereslavl-Zalessky, 1989, which was co-organized by Albert R. Meyer (MIT) and Michael Taitslin (Tver). After that, organization passed to Anil Nerode.

Currently, LFCS is governed by a Steering Committee consisting of Anil Nerode, Cornell (General Chair); Stephen Cook, Toronto; Dirk van Dalen, Utrecht; Yuri Matiyasevich, St. Petersburg; John McCarthy, Stanford; J. Alan Robinson, Syracuse; Gerald Sacks, Harvard; and Dana Scott, Carnegie-Mellon.

The 2007 Symposium on Logical Foundations of Computer Science took place in New York, USA at the Graduate Center of the City University of New York during June 4 - 7. This volume contains the extended abstracts of talks selected by the Program Committee for presentation at LFCS 2007.

The scope of the symposium is broad and contains constructive mathematics and type theory; logical foundations of programming; logical aspects of computational complexity; logic programming and constraints; automated deduction and interactive theorem proving; logical methods in protocol and program verification; logical methods in program specification and extraction; domain theory logics; logical foundations of database theory; equational logic and term rewriting; lambda and combinatory calculi; categorical logic and topological semantics; linear logic; epistemic and temporal logics; intelligent and multiple agent system logics; logics of proof and justification; nonmonotonic reasoning; logic in game theory and social software; logic of hybrid systems; distributed system logics; system design logics; other logics in computer science.

We thank the authors and reviewers for their contributions. We acknowledge the support of the Graduate Center of the City University of New York, the Mid-Atlantic Mathematical Logic Seminar, the New York Logic Colloquium, and the CUNY Computer Science Colloquium.

We are grateful to Evan Goris, Bryan Renne, and Roman Kuznets for preparing this volume for Springer.

March 2007

Anil Nerode
Sergei Artemov

Organization

Steering Committee

Stephen Cook (Toronto)
Dirk van Dalen (Utrecht)
Yuri Matiyasevich (St. Petersburg)
John McCarthy (Stanford)
Anil Nerode (Cornell) - General Chair
J. Alan Robinson (Syracuse)
Gerald Sacks (Harvard)
Dana Scott (Carnegie-Mellon)

Program Committee

Samson Abramsky (Oxford)
Sergei Artemov (New York) - PC Chair
Matthias Baaz (Vienna)
Lev Beklemishev (Moscow)
Andreas Blass (Ann Arbor)
Lenore Blum (Carnegie-Mellon)
Samuel Buss (San Diego)
Thierry Coquand (Göteborg)
Ruy de Queiroz (Recife, Brazil)
Denis Hirschfeldt (Chicago)
Bakhadyr Khoussainov (Auckland)
Yves Lafont (Marseille)
Joachim Lambek (McGill)
Daniel Leivant (Indiana)
Victor Marek (Kentucky)
Anil Nerode (Cornell) - General LFCS Chair
Philip Scott (Ottawa)
Anatol Slissenko (Paris)
Alex Simpson (Edinburgh)
V.S. Subrahmanian (Maryland)
Michael Rathjen (Leeds)
Alasdair Urquhart (Toronto)

Additional Reviewers

Alexandru Baltag
Jan Broersen

VIII Organization

Arnaud Carayol
Walter Carnielli
Robin Cockett
Melvin Fitting
Rosalie Iemhoff
Max Kanovich
Vladimir Krupski
Larisa Maksimova
Joao Marcos
Edwin Mares
Joel Oaknine
Rohit Parikh
Valery Plisko
Jeffrey Remmel
Andre Scedrov
Sven Schewe
Subash Shankar
Valentin Shehtman
Mirek Truszczyński
Sergei Tupailo
James Worrell

Lecture Notes in Computer Science

For information about Vols. 1–4393

please contact your bookseller or Springer

- Vol. 4523: Y.-H. Lee, H.-N. Kim, J. Kim, Y. Park, L.T. Yang, S.W. Kim (Eds.), *Embedded Software and Systems*. XIX, 829 pages. 2007.
- Vol. 4517: F. Boavida, E. Monteiro, S. Mascolo, Y. Koucheryavy (Eds.), *Wired/Wireless Internet Communications*. XIV, 382 pages. 2007.
- Vol. 4515: M. Naor (Ed.), *Advances in Cryptology - EUROCRYPT 2007*. XIII, 591 pages. 2007.
- Vol. 4514: S.N. Artemov, A. Nerode (Eds.), *Logical Foundations of Computer Science*. XI, 513 pages. 2007.
- Vol. 4510: P. Van Hentenryck, L. Wolsey (Eds.), *Integration of AI and OR Techniques in Constraint Programming for Combinatorial Optimization Problems*. X, 391 pages. 2007.
- Vol. 4509: Z. Kobti, D. Wu (Eds.), *Advances in Artificial Intelligence*. XII, 552 pages. 2007. (Sublibrary LNAI).
- Vol. 4506: D. Zeng, I. Gotham, K. Komatsu, C. Lynch, M. Thurmond, D. Madigan, B. Lober, J. Kvach, H. Chen (Eds.), *Intelligence and Security Informatics: Biosurveillance*. XI, 234 pages. 2007.
- Vol. 4504: J. Huang, R. Kowalczyk, Z. Maamar, D. Martin, I. Müller, S. Stoutenburg, K.P. Sycara (Eds.), *Service-Oriented Computing: Agents, Semantics, and Engineering*. X, 175 pages. 2007.
- Vol. 4493: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), *Advances in Neural Networks – ISNN 2007, Part III*. XXXVI, 1215 pages. 2007.
- Vol. 4492: D. Liu, S. Fei, Z. Hou, H. Zhang, C. Sun (Eds.), *Advances in Neural Networks – ISNN 2007, Part II*. XXVII, 1321 pages. 2007.
- Vol. 4491: D. Liu, S. Fei, Z.-G. Hou, H. Zhang, C. Sun (Eds.), *Advances in Neural Networks – ISNN 2007, Part I*. LIV, 1365 pages. 2007.
- Vol. 4490: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), *Computational Science – ICCS 2007, Part IV*. XXXVII, 1211 pages. 2007.
- Vol. 4489: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), *Computational Science – ICCS 2007, Part III*. XXXVII, 1257 pages. 2007.
- Vol. 4488: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), *Computational Science – ICCS 2007, Part II*. XXXV, 1251 pages. 2007.
- Vol. 4487: Y. Shi, G.D. van Albada, J. Dongarra, P.M.A. Sloot (Eds.), *Computational Science – ICCS 2007, Part I*. LXXXI, 1275 pages. 2007.
- Vol. 4486: M. Bernardo, J. Hillston (Eds.), *Formal Methods for Performance Evaluation*. VII, 469 pages. 2007.
- Vol. 4484: J.-Y. Cai, S.B. Cooper, H. Zhu (Eds.), *Theory and Applications of Models of Computation*. XIII, 772 pages. 2007.
- Vol. 4483: C. Baral, G. Brewka, J. Schlipf (Eds.), *Logic Programming and Nonmonotonic Reasoning*. IX, 327 pages. 2007. (Sublibrary LNAI).
- 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. (Sublibrary LNAI).
- 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. (Sublibrary LNAI).
- Vol. 4480: A. LaMarca, M. Langheinrich, K.N. Truong (Eds.), *Pervasive Computing*. XIII, 369 pages. 2007.
- Vol. 4479: I.F. Akyildiz, R. Sivakumar, E. Ekici, J.C.d. Oliveira, J. McNair (Eds.), *NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet*. XXVII, 1252 pages. 2007.
- Vol. 4472: M. Haindl, J. Kittler, F. Roli (Eds.), *Multiple Classifier Systems*. XI, 524 pages. 2007.
- Vol. 4471: P. Cesar, K. Choriantopoulos, J.F. Jensen (Eds.), *Interactive TV: a Shared Experience*. XIII, 236 pages. 2007.
- Vol. 4470: Q. Wang, D. Pfahl, D.M. Raffo (Eds.), *Software Process Dynamics and Agility*. XI, 346 pages. 2007.
- Vol. 4464: E. Dawson, D.S. Wong (Eds.), *Information Security Practice and Experience*. XIII, 361 pages. 2007.
- Vol. 4463: I. Mändou, A. Zelikovsky (Eds.), *Bioinformatics Research and Applications*. XV, 653 pages. 2007. (Sublibrary LNBI).
- Vol. 4462: D. Sauveron, K. Markantonakis, A. Bilas, J.-J. Quisquater (Eds.), *Information Security Theory and Practices*. XII, 255 pages. 2007.
- Vol. 4459: C. Cérin, K.-C. Li (Eds.), *Advances in Grid and Pervasive Computing*. XVI, 759 pages. 2007.
- Vol. 4453: T. Speed, H. Huang (Eds.), *Research in Computational Molecular Biology*. XVI, 550 pages. 2007. (Sublibrary LNBI).
- Vol. 4452: M. Fasli, O. Shehory (Eds.), *Agent-Mediated Electronic Commerce*. VIII, 249 pages. 2007. (Sublibrary LNAI).
- Vol. 4451: T.S. Huang, A. Nijholt, M. Pantic, A. Pentland (Eds.), *Artificial Intelligence for Human Computing*. XVI, 359 pages. 2007. (Sublibrary LNAI).
- Vol. 4450: T. Okamoto, X. Wang (Eds.), *Public Key Cryptography – PKC 2007*. XIII, 491 pages. 2007.
- Vol. 4448: M. Giacobini et al. (Ed.), *Applications of Evolutionary Computing*. XXIII, 755 pages. 2007.
- Vol. 4447: E. Marchiori, J.H. Moore, J.C. Rajapakse (Eds.), *Evolutionary Computation, Machine Learning and Data Mining in Bioinformatics*. XI, 302 pages. 2007.

- Vol. 4446: C. Cotta, J. van Hemert (Eds.), *Evolutionary Computation in Combinatorial Optimization*. XII, 241 pages. 2007.
- Vol. 4445: M. Ebner, M. O'Neill, A. Ekárt, L. Vanneschi, A.I. Esparcia-Alcázar (Eds.), *Genetic Programming*. XI, 382 pages. 2007.
- Vol. 4444: T. Reps, M. Sagiv, J. Bauer (Eds.), *Program Analysis and Compilation, Theory and Practice*. X, 361 pages. 2007.
- Vol. 4443: R. Kotagiri, P.R. Krishna, M. Mohania, E. Nantajeewarawat (Eds.), *Advances in Databases: Concepts, Systems and Applications*. XXI, 1126 pages. 2007.
- Vol. 4440: B. Liblit, *Cooperative Bug Isolation*. XV, 101 pages. 2007.
- Vol. 4439: W. Abramowicz (Ed.), *Business Information Systems*. XV, 654 pages. 2007.
- Vol. 4438: L. Maicher, A. Sigel, L.M. Garshol (Eds.), *Leveraging the Semantics of Topic Maps*. X, 257 pages. 2007. (Sublibrary LNAI).
- Vol. 4433: E. Şahin, W.M. Spears, A.F.T. Winfield (Eds.), *Swarm Robotics*. XII, 221 pages. 2007.
- Vol. 4432: B. Beliczynski, A. Dzieliński, M. Iwanowski, B. Ribeiro (Eds.), *Adaptive and Natural Computing Algorithms, Part II*. XXVI, 761 pages. 2007.
- Vol. 4431: B. Beliczynski, A. Dzieliński, M. Iwanowski, B. Ribeiro (Eds.), *Adaptive and Natural Computing Algorithms, Part I*. XXV, 851 pages. 2007.
- Vol. 4430: C.C. Yang, D. Zeng, M. Chau, K. Chang, Q. Yang, X. Cheng, J. Wang, F.-Y. Wang, H. Chen (Eds.), *Intelligence and Security Informatics*. XII, 330 pages. 2007.
- Vol. 4429: R. Lu, J.H. Siekmann, C. Ullrich (Eds.), *Cognitive Systems*. X, 161 pages. 2007. (Sublibrary LNAI).
- Vol. 4427: S. Uhlig, K. Papagiannaki, O. Bonaventure (Eds.), *Passive and Active Network Measurement*. XI, 274 pages. 2007.
- Vol. 4426: Z.-H. Zhou, H. Li, Q. Yang (Eds.), *Advances in Knowledge Discovery and Data Mining*. XXV, 1161 pages. 2007. (Sublibrary LNAI).
- Vol. 4425: G. Amati, C. Carpineto, G. Romano (Eds.), *Advances in Information Retrieval*. XIX, 759 pages. 2007.
- Vol. 4424: O. Grumberg, M. Huth (Eds.), *Tools and Algorithms for the Construction and Analysis of Systems*. XX, 738 pages. 2007.
- Vol. 4423: H. Seidl (Ed.), *Foundations of Software Science and Computational Structures*. XVI, 379 pages. 2007.
- Vol. 4422: M.B. Dwyer, A. Lopes (Eds.), *Fundamental Approaches to Software Engineering*. XV, 440 pages. 2007.
- Vol. 4421: R. De Nicola (Ed.), *Programming Languages and Systems*. XVII, 538 pages. 2007.
- Vol. 4420: S. Krishnamurthi, M. Odersky (Eds.), *Compiler Construction*. XIV, 233 pages. 2007.
- Vol. 4419: P.C. Diniz, E. Marques, K. Bertels, M.M. Fernandes, J.M.P. Cardoso (Eds.), *Reconfigurable Computing: Architectures, Tools and Applications*. XIV, 391 pages. 2007.
- Vol. 4418: A. Gagalowicz, W. Philips (Eds.), *Computer Vision/Computer Graphics Collaboration Techniques*. XV, 620 pages. 2007.
- Vol. 4416: A. Bemporad, A. Bicchi, G. Buttazzo (Eds.), *Hybrid Systems: Computation and Control*. XVII, 797 pages. 2007.
- Vol. 4415: P. Lukowicz, L. Thiele, G. Tröster (Eds.), *Architecture of Computing Systems - ARCS 2007*. X, 297 pages. 2007.
- Vol. 4414: S. Hochreiter, R. Wagner (Eds.), *Bioinformatics Research and Development*. XVI, 482 pages. 2007. (Sublibrary LNBI).
- Vol. 4412: F. Stajano, H.J. Kim, J.-S. Chae, S.-D. Kim (Eds.), *Ubiquitous Convergence Technology*. XI, 302 pages. 2007.
- Vol. 4411: R.H. Bordini, M. Dastani, J. Dix, A.E.F. Seghrouchni (Eds.), *Programming Multi-Agent Systems*. XIV, 249 pages. 2007. (Sublibrary LNAI).
- Vol. 4410: A. Branco (Ed.), *Anaphora: Analysis, Algorithms and Applications*. X, 191 pages. 2007. (Sublibrary LNAI).
- Vol. 4409: J.L. Fiadeiro, P.-Y. Schobbens (Eds.), *Recent Trends in Algebraic Development Techniques*. VII, 171 pages. 2007.
- Vol. 4407: G. Puebla (Ed.), *Logic-Based Program Synthesis and Transformation*. VIII, 237 pages. 2007.
- Vol. 4406: W. De Meuter (Ed.), *Advances in Smalltalk*. VII, 157 pages. 2007.
- Vol. 4405: L. Padgham, F. Zambonelli (Eds.), *Agent-Oriented Software Engineering*. VII. XII, 225 pages. 2007.
- Vol. 4403: S. Obayashi, K. Deb, C. Poloni, T. Hiroyasu, T. Murata (Eds.), *Evolutionary Multi-Criterion Optimization*. XIX, 954 pages. 2007.
- Vol. 4401: N. Guelfi, D. Buchs (Eds.), *Rapid Integration of Software Engineering Techniques*. IX, 177 pages. 2007.
- Vol. 4400: J.F. Peters, A. Skowron, V.W. Marek, E. Orłowska, R. Słowiński, W. Ziarko (Eds.), *Transactions on Rough Sets VII, Part II*. X, 381 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. (Sublibrary LNAI).
- Vol. 4398: S. Marchand-Maillet, E. Bruno, A. Nürnberger, M. Detyniecki (Eds.), *Adaptive Multimedia Retrieval: User, Context, and Feedback*. XI, 269 pages. 2007.
- Vol. 4397: C. Stephanidis, M. Pieper (Eds.), *Universal Access in Ambient Intelligence Environments*. XV, 467 pages. 2007.
- Vol. 4396: J. García-Vidal, L. Cerdà-Alabern (Eds.), *Wireless Systems and Mobility in Next Generation Internet*. IX, 271 pages. 2007.
- Vol. 4395: M. Daydé, J.M.L.M. Palma, Á.L.G.A. Coutinho, E. Pacitti, J.C. Lopes (Eds.), *High Performance Computing for Computational Science - VEC- PAR 2006*. XXIV, 721 pages. 2007.
- Vol. 4394: A. Gelbukh (Ed.), *Computational Linguistics and Intelligent Text Processing*. XVI, 648 pages. 2007.

¥689.00元

Table of Contents

Justified and Common Knowledge: Limited Conservativity	1
<i>Evangelia Antonakos</i>	
The Intensional Lambda Calculus	12
<i>Sergei Artemov and Eduardo Bonelli</i>	
Generalized Non-deterministic Matrices and (n,k)-ary Quantifiers	26
<i>Arnon Avron and Anna Zamansky</i>	
Elementary Differential Calculus on Discrete and Hybrid Structures	41
<i>Howard A. Blair, David W. Jakel, Robert J. Irwin, and Angel Rivera</i>	
Weighted Distributed Systems and Their Logics	54
<i>Benedikt Bollig and Ingmar Meinecke</i>	
Weighted O-Minimal Hybrid Systems Are More Decidable Than Weighted Timed Automata!	69
<i>Patricia Bouyer, Thomas Brihaye, and Fabrice Chevalier</i>	
On Decidability and Expressiveness of Propositional Interval Neighborhood Logics	84
<i>Davide Bresolin, Valentin Goranko, Angelo Montanari, and Guido Sciavicco</i>	
Reasoning About Sequences of Memory States	100
<i>Rémi Brochenin, Stéphane Demri, and Etienne Lozes</i>	
Cut Elimination in Deduction Modulo by Abstract Completion	115
<i>Guillaume Burel and Claude Kirchner</i>	
Density Elimination and Rational Completeness for First-Order Logics	132
<i>Agata Ciabattoni and George Metcalfe</i>	
Extracting the Resolution Algorithm from a Completeness Proof for the Propositional Calculus	147
<i>Robert Constable and Wojciech Moczyłowski</i>	
Topological Semantics and Bisimulations for Intuitionistic Modal Logics and Their Classical Companion Logics	162
<i>J.M. Davoren</i>	
A Decidable Temporal Logic of Repeating Values	180
<i>Stéphane Demri, Deepak D'Souza, and Régis Gascon</i>	

Model Checking Knowledge and Linear Time: PSPACE Cases	195
<i>Kai Engelhardt, Peter Gammie, and Ron van der Meyden</i>	
Realizations and LP	212
<i>Melvin Fitting</i>	
Successive Abstractions of Hybrid Automata for Monotonic CTL Model Checking	224
<i>R. Gentilini, K. Schneider, and B. Mishra</i>	
Explicit Proofs in Formal Provability Logic	241
<i>Evan Goris</i>	
A Synthesis Algorithm for Hybrid Systems	254
<i>Srikanth Gottipati and Anil Nerode</i>	
Including the Past in ‘Topologic’	269
<i>Bernhard Heinemann</i>	
A Note on Rewriting Proofs and Fibonacci Numbers	284
<i>Max Kanovich</i>	
On Complexity of Ehrenfeucht-Fraïssé Games	293
<i>Bakhadyr Khoussainov and Jiamou Liu</i>	
The Law of the Iterated Logarithm for Algorithmically Random Brownian Motion	310
<i>Bjørn Kjos-Hanssen and Anil Nerode</i>	
Hypersequent Calculus for Intuitionistic Logic with Classical Atoms	318
<i>Hidenori Kurokawa</i>	
Proof Identity for Classical Logic: Generalizing to Normality	332
<i>Roman Kuznets</i>	
On the Constructive Dedekind Reals: Extended Abstract	349
<i>Robert S. Lubarsky and Michael Rathjen</i>	
Verifying Balanced Trees	363
<i>Zohar Manna, Henny B. Sipma, and Ting Zhang</i>	
Compactness Properties for Stable Semantics of Logic Programs	379
<i>Victor W. Marek and Jeffrey B. Remmel</i>	
Uniform Circuits, & Boolean Proof Nets	401
<i>Virgile Mogbil and Vincent Rahli</i>	
Finite Automata Presentable Abelian Groups	422
<i>André Nies and Pavel Semukhin</i>	

Embeddings into Free Heyting Algebras and Translations into Intuitionistic Propositional Logic	437
<i>Michael O'Connor</i>	
Some Puzzles About Probability and Probabilistic Conditionals	449
<i>Rohit Parikh</i>	
A Temporal Dynamic Logic for Verifying Hybrid System Invariants	457
<i>André Platzer</i>	
Multiplexor Categories and Models of Soft Linear Logic	472
<i>Brian F. Redmond</i>	
Until-Since Temporal Logic Based on Parallel Time with Common Past. Deciding Algorithms	486
<i>V. Rybakov</i>	
Total Public Announcements	498
<i>David Steiner and Thomas Studer</i>	
Author Index	513

Justified and Common Knowledge: Limited Conservativity

Evangelia Antonakos

CUNY Graduate Center
Ph.D. Program in Mathematics
365 Fifth Avenue
New York, NY 10016, USA
Eva@Antonakos.net

Abstract. We consider the relative strengths of three formal approaches to public knowledge: “any fool” knowledge by McCarthy (1970), Common Knowledge by Halpern and Moses (1990), and Justified Knowledge by Artemov (2004). Specifically, we show that epistemic systems with the Common Knowledge modality C are conservative with respect to Justified Knowledge systems on formulas $\chi \wedge C\varphi \rightarrow \psi$, where χ, φ , and ψ are C -free.

Keywords: justified knowledge, common knowledge, Artemov, conservative.

1 Multi-agent Logics

The logics T_n , $S4_n$, and $S5_n$ are logics in which each of the finitely many (n) agents has a knowledge operator K_i which is T , or $S4$, or $S5$ respectively. We only consider cases where all agents’ modalities are of the same logical strength.

Definition 1. *The formal systems for T_n , $S4_n$, and $S5_n$ are as follows:*

Propositional Logic plus for K_i , $i = 1, 2, \dots, n$ we have

Axioms for $S4_n$:

$K : K_i(\varphi \rightarrow \psi) \rightarrow (K_i\varphi \rightarrow K_i\psi)$	each agent can do <i>modus ponens</i>
$T : K_i\varphi \rightarrow \varphi$	agents can know only true propositions
$4 : K_i\varphi \rightarrow K_iK_i\varphi$	agents have positive introspection

Rules:

Necessitation: $\vdash \varphi \Rightarrow \vdash K_i\varphi$, for $i = 1, 2, \dots, n$

For T_n , omit the final axiom.

For $S5_n$, add negative introspection: $\neg K_i\varphi \rightarrow K_i\neg K_i\varphi$.

Definition 2. *Kripke models for $S4_n$: $M = \langle W, R_1, R_2, \dots, R_n, \Vdash \rangle$ where*

- W is a non-empty set of worlds
- $R_i \subseteq W \times W$ is agent i ’s accessibility relation. R_i is reflexive and transitive.

• $\Vdash \subseteq W \times Var$ where Var is the set of propositional variables. The forcing relation \Vdash is naturally extended to all formulas so that R_i corresponds to K_i :

$$M, u \Vdash K_i \varphi \Leftrightarrow (\forall v \in M)[uR_i v \rightarrow M, v \Vdash \varphi] .$$

For T_n -models, each R_i is reflexive while for $S5_n$ -models, each R_i is an equivalence relation.

Theorem 1. T_n , $S4_n$, and $S5_n$ are sound and complete with respect to their models (cf. [10]).

Multi-agent systems are enhanced by the addition of modalities which take into account shared or public knowledge of agents. Three such modalities C , J , and O will be discussed, all of which model variations of public information. We will compare their logical strengths, semantics, and complexity and will see why Justified Knowledge (J) systems are sufficient to solve classical epistemic scenarios, a role usually designated for Common Knowledge (C).

2 Common Knowledge

The most recognized concept of public knowledge is common knowledge, and the literature addressing it, both philosophical and mathematical, is vast. The initial investigation was philosophical: Lewis's book [15] on convention. The intuition behind the informal definition of common knowledge below derives from Aumann's oft-cited [5], where it was used in the context of agents having common priors. McCarthy's 'any fool' operator of 1970 ([10], p. 13) is closely related to common knowledge and his systems in [16] (see section 4 of this paper) may be the first to address it axiomatically. Rigorous work on common knowledge in the context of multi-agent systems was done by Halpern and Moses in [13] (an expansion of a 1984 work of the same title) and Lehmann [14]. Much of the work by Halpern and Moses appears in [10]. Common knowledge continues to be actively investigated.

Informally, the epistemic operator $C\varphi$, to be read ' φ is common knowledge,' can be given as infinite conjunction:

$$C\varphi \leftrightarrow \varphi \wedge E\varphi \wedge EE\varphi \wedge EEE\varphi \wedge E^4\varphi \wedge \dots \wedge E^n\varphi \wedge \dots \quad (1)$$

where $E\varphi = K_1\varphi \wedge K_2\varphi \wedge \dots \wedge K_n\varphi$ ('everyone knows φ ') and K_i is an individual agent's knowledge operator corresponding to T , $S4$ or $S5$ as appropriate. One formal characterization which [10] and [7] take is via the Fixed Point Axiom

$$C\varphi \leftrightarrow E(\varphi \wedge C\varphi) \quad (2)$$

and the Induction Rule

$$\frac{\varphi \rightarrow E(\varphi \wedge \psi)}{\varphi \rightarrow C\psi} \quad (3)$$

yielding Common Knowledge to be the greatest fixed point solution to $X \leftrightarrow E(\varphi \wedge X)$ [10]. Common Knowledge does not take into account the means by

which the knowledge is acquired. As we will see, this is in contrast to Justified Knowledge. The distinction between the infinite conjunction, the fixed point axiom, and how common knowledge is achieved is addressed in [6]. [12] too, provides a survey with examples but does not include a distinct formalism. There is also an equivalent axiomatic formulation of common knowledge which replaces the induction rule with the induction axiom in [17], which, for technical convenience, we will use.

Definition 3. T_n^C , $\mathsf{S4}_n^C$, and $\mathsf{S5}_n^C$ axiom systems:

Propositional Logic plus

Axioms:

T , $\mathsf{S4}$, or $\mathsf{S5}$ axioms for K_i , $i = 1, 2, \dots, n$, respectively;

K : $C(\varphi \rightarrow \psi) \rightarrow (C\varphi \rightarrow C\psi)$;

T : $C\varphi \rightarrow \varphi$;

$C\varphi \rightarrow E(C\varphi)$, where $E\varphi = K_1\varphi \wedge K_2\varphi \wedge \dots \wedge K_n\varphi$;

Induction Axiom: $\varphi \wedge C(\varphi \rightarrow E\varphi) \rightarrow C\varphi$.

Rules:

Necessitation: $\vdash \varphi \Rightarrow \vdash K_i\varphi$, for $i = 1, 2, \dots, n$

Necessitation: $\vdash \varphi \Rightarrow \vdash C\varphi$.

Definition 4. Models for T_n^C , $\mathsf{S4}_n^C$, and $\mathsf{S5}_n^C$: $M = \langle W, R_1, R_2, \dots, R_n, R_C, \Vdash \rangle$ where

- $M = \langle W, R_1, R_2, \dots, R_n, \Vdash \rangle$ is a T_n , $\mathsf{S4}_n$, or $\mathsf{S5}_n$ model, respectively
- $R_C = \left(\bigcup_{i=1}^n R_i \right)^*$, that is the transitive closure of all the agents' relations
- The forcing relation \Vdash is extended to all formulas so R_C corresponds to C :

$$M, u \Vdash C\varphi \Leftrightarrow (\forall v \in M)[uR_C v \rightarrow M, v \Vdash \varphi] .$$

Theorem 2. T_n^C , $\mathsf{S4}_n^C$, and $\mathsf{S5}_n^C$ are sound and complete with respect to their models (cf. [10], p. 70ff, [17], p. 47ff).

The agents' logic plays a role in determining the strength of the common knowledge operator C . In the systems defined above, C is always at least as strong as K_i . Showing that in T_n^C , $\mathsf{S4}_n^C$, and $\mathsf{S5}_n^C$, C satisfies the T , $\mathsf{S4}$, and $\mathsf{S5}$ axioms, respectively, is given as an exercise in [10], p. 93.

3 Justified Knowledge

Justified Knowledge was introduced by Artemov in [3,4] as the forgetful projection of the *evidence-based* knowledge represented by an appropriate adaptation of LP (Logic of Proofs). In LP systems ($\mathsf{T}_n\text{LP}$, $\mathsf{S4}_n\text{LP}$, $\mathsf{S5}_n\text{LP}$), each formula / subformula carries with it a proof term representing a particular proof of the formula / subformula from the axioms. Justified knowledge systems are ones in which all proofs are identified as one. Whereas $C\varphi$ asserts that φ is common

knowledge, $J\varphi$ asserts that φ is common knowledge arising from a proof of φ or some other agreed-upon acceptable set of evidences. Though the proof of φ is not explicitly presented with the assertion $J\varphi$, it is reproducible. This is the important Realization Theorem which provides an algorithm to reconstruct LP proof terms. For more details on this, the reader should consult [4].

As with the common knowledge logics, the construction of the justified knowledge logics T_n^J , $\mathsf{S4}_n^J$, and $\mathsf{S5}_n^J$ builds on the multi-agent logics. In C systems the agents' logic determines the strength of C while in J systems the strength of J is chosen independently to be weaker, stronger, or the same as that of the agents'. In the aforementioned logics, the modality J will be assumed to be $\mathsf{S4}$ unless otherwise specified.

Definition 5. T_n^J , $\mathsf{S4}_n^J$, and $\mathsf{S5}_n^J$ axiom systems:

Propositional Logic plus

Axioms:

T , $\mathsf{S4}$, or $\mathsf{S5}$ axioms for K_i , $i = 1, 2, \dots, n$;

$\mathsf{S4}$ axioms for J ;

Connection Principle: $J\varphi \rightarrow K_i\varphi$.

Rules:

Necessitation for all K_i : $\vdash \varphi \Rightarrow \vdash K_i\varphi$;

Necessitation for J : $\vdash \varphi \Rightarrow \vdash J\varphi$.

Definition 6. Models for T_n^J , $\mathsf{S4}_n^J$, and $\mathsf{S5}_n^J$: $M = \langle W, R_1, R_2, \dots, R_n, R_J, \Vdash \rangle$ where

- $M = \langle W, R_1, R_2, \dots, R_n, \Vdash \rangle$ is a T_n , $\mathsf{S4}_n$, or $\mathsf{S5}_n$ model, respectively
- $R_J \subseteq W \times W$ is reflexive and transitive relation such that $R_J \supseteq \left(\bigcup_{i=1}^n R_i\right)^*$ (where $*$ is transitive closure)
- The forcing relation \Vdash is extended to all formulas so R_J corresponds to J :

$$M, u \Vdash J\varphi \Leftrightarrow (\forall v \in M)[uR_J v \rightarrow M, v \Vdash \varphi] .$$

Theorem 3. T_n^J , $\mathsf{S4}_n^J$, and $\mathsf{S5}_n^J$ are sound and complete with respect to their models, as shown in [4].

Recall that in common knowledge models, $R_C = \left(\bigcup_{i=1}^n R_i\right)^*$ and so $R_C \subseteq R_J$.

Thus in a context where we can compare the two, i.e. a hybrid model with both R_C and R_J , it seems (if φ contains no J s) $J\varphi \Rightarrow C\varphi$ but not vice versa. More formally, we have the following proposition.

Definition 7. Let φ^* be φ with each instance of a J replaced by a C .

Proposition 1. $(\mathsf{S4}_n^J)^* \subset \mathsf{S4}_n^C$ but $(\mathsf{S4}_n^J)^* \neq \mathsf{S4}_n^C$.

Proof. It needs to be shown that the $*$ -translation of each rule and axiom of $S4_n^J$ is provable in $S4_n^C$. Artemov shows this in [4] using the equivalent axiomatization of $S4_n^C$ from [10]. It is only the Induction Axiom of $S4_n^C$ which is not provable in $(S4_n^J)^*$, yielding the strict inclusion. \square

The case in which the J of $S5_n^J$ is an $S5$ modality, that is $S5_n^{J(S5)}$, is considered in [18] (where she names it $S5_nS5$). An $S5_n^{J(S5)}$ -model is like an $S5_n^J$ model except that R_J will now be an equivalence relation.

Corollary 1. *Let I.A. be the induction axiom. Then*

$$\begin{aligned} S4_n^C &\equiv (S4_n^J)^* + \text{I.A.} , \\ T_n^C &\equiv (T_n^J)^* + \text{I.A.} , \\ S5_n^C &\equiv (S5_n^{J(S5)})^* + \text{I.A.} . \end{aligned}$$

Proof. The strict inclusion of the J systems follows from Proposition 1 and noticing that C satisfies the 4 axiom in T_n^C and the 5 axiom in $S5_n^C$. When the induction axiom is added, the equivalence is clear. \square

Indeed, from Corollary 1, in any of the justified knowledge systems mentioned, $J\varphi \Rightarrow C\varphi^*$.

The evidence-based common knowledge semantics for J systems are further enriched by Artemov's Realization Theorem mentioned at the start of the section. This gives a constructive approach to recovering or realizing the full proof terms of the evidence-based knowledge systems.

Theorem 4 (Realization Theorem). *There is an algorithm that, given an $S4_n^J$ -derivation of a formula φ , retrieves an $S4_n\text{LP}$ -formula ψ , a realization of φ , such that φ is ψ° , where $^\circ$ replaces all proof terms with J , and $S4_n\text{LP}$ proves ψ .*

This theorem and a realization theorem for $S5_n^J$ (where J is an $S4$ -modality) is established in [4] while a realization theorem for $S5_n^{J(S5)}$ is given in [18].

Other major advantages to justified knowledge are

- proofs in $S4_n^J$ are normalizable ([4]), but those in $S4_n^C$ are not
- $S4_2^J$ is *PSPACE*-complete [9], whereas for $n \geq 2$, $S4_n^C$ is *EXPTIME*-complete [10].

These features have been exploited by Bryukhov in [8] to develop an automated theorem prover for $S4_n^J$. Justified Knowledge offers simpler, more constructive, and more automation-friendly approach to common knowledge.

4 Any Fool's Knowledge

McCarthy's model of common knowledge via "any fool knows" apparently goes back to roughly 1970 ([10], p. 13), though its first published appearance is in [16]. In this epistemic multi-agent system, the modality for each agent is denoted by S , with an additional virtual agent, "any fool" denoted by O . In [16] p. 2, whatever