

Volker Diekert
Mikhail V. Volkov
Andrei Voronkov (Eds.)

LNCS 4649

Computer Science – Theory and Applications

Second International Symposium
on Computer Science in Russia, CSR 2007
Ekaterinburg, Russia, September 2007, Proceedings

Volker Diekert Mikhail V. Volkov
Andrei Voronkov (Eds.)

Computer Science – Theory and Applications

Second International Symposium
on Computer Science in Russia, CSR 2007
Ekaterinburg, Russia, September 3-7, 2007
Proceedings

Volume Editors

Volker Diekert
Universität Stuttgart
Institut für Formale Methoden der Informatik
Universitätsstr. 38, 70569 Stuttgart, Germany
E-mail: diekert@fmi.uni-stuttgart.de

Mikhail V. Volkov
Ural State University
Department of Algebra and Discrete Mathematics
Faculty of Mathematics and Mechanics
Lenina 51, 620083 Ekaterinburg, Russia
E-mail: Mikhail.Volkov@usu.ru

Andrei Voronkov
University of Manchester
School of Computer Science
Kilburn Building, Oxford Road, Manchester, M13 9PL, UK
E-mail: andrej@voronkov.com

Library of Congress Control Number: 2007933004

CR Subject Classification (1998): F.1.1-2, F.2.1-2, F.4.1, I.2.6, J.3

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

ISSN	0302-9743
ISBN-10	3-540-74509-2 Springer Berlin Heidelberg New York
ISBN-13	978-3-540-74509-9 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: 12113064 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 2nd International Symposium on Computer Science in Russia (CSR 2007) was held September 3–7 in Ekaterinburg, Russia, hosted by Ural State University. CSR 2007 was the second event in a series of regular international meetings that started with CSR 2006 in St. Petersburg (see LNCS 3967). The symposium was organized under the auspices of the European Association for Theoretical Computer Science.

The symposium was composed of two tracks: Theory and Applications/Technology. The opening lecture was given by Yuri Gurevich and other invited lectures were given by Scott Aaronson, Rajeev Alur, Peter Druschel, Ziyad Hanna, Bertrand Meyer, Alexei Miasnikov, Geraud Senizergues, and Geoff Sutcliffe. This volume contains the accepted papers of both tracks and the abstracts of seven invited presentations.

The scope of proposed topics for the symposium was quite broad and covered many areas of computer science and its applications. We received 95 submissions, the contributors being from 24 countries. Each submission was reviewed by at least three Program Committee members. The committee decided to accept 34 papers. The reviewing process as well as the preparation of this volume were efficiently supported by the EasyChair conference system.

The following satellite events were collocated with CSR 2007:

- Workshop on Computational Complexity and Decidability in Algebra
- Workshop on Infinite Words, Automata and Dynamics
- Russian Summer School in Information Retrieval

We thank our sponsors: Microsoft Research, Russian Foundation for Basic Research, SKB Kontur, Ural State University, and Yandex.

Yandex, the largest resource on the Russian Internet, established the Yandex the Best Paper Awards and Yandex Best Student Paper Awards for the CSR series. The inauguration of the Yandex Awards formed a part of the Business Meeting of CSR 2007 along with the presentations of the first awarded papers. The following three papers were selected by the Program Committee:

- “Conjunctive grammars over a unary alphabet: undecidability and unbounded growth” by Artur Jez and Alexander Okhotin — Best Paper in the Theory Track
- “Estimation of the click volume by large-scale regression analysis” by Yuri Lifshits and Dirk Nowotka — Best Paper in the Applications and Technology Track
- “A fast algorithm for path 2-packing problem” by Maxim Babenko — Best Student Paper

We thank the local Organizing Committee (co-chaired by Vladimir Tretjakov, President of Ural State University, and Vitaly Berdyshev, Director of Mathematics and Mechanics Institute of the Ural Branch of the Russian Academy of Sciences), especially Svetlana Goldberg, Grigoriy Povarov, and Elena Pribavkina.

June 2007

Volker Diekert
Mikhail Volkov
Andrei Voronkov

Conference Organization

Program Committee

Theory Track

Eric Allender	Rutgers University, USA
Sergei Artemov	City University of New York, USA
Eugene Asarin	Université Paris-7, France
Lev Beklemishev	Steklov Institute/Moscow, Russia
Andrei Bulatov	Simon Fraser University, Canada
Evgeny Dantsin	Roosevelt University, USA
Volker Diekert (Chair)	Universität Stuttgart, Germany
Anna Frid	Sobolev Institute/Novosibirsk, Russia
Paul Gastin	ENS de Cachan, France
Joachim von zur Gathen	Universität Paderborn, Germany
Andrew Goldberg	Microsoft Research, USA
Erich Graedel	Universität Aachen, Germany
Dima Grigoriev	CRNS, IRMAR, Rennes, France
Yuri Gurevich	Microsoft Research, USA
Tero Harju	University of Turku, Finland
Edward Hirsch	Steklov Institute/St.Petersburg, Russia
Peter Hoyer	University of Calgary, Canada
Michael Kaminski	Technion – Israel Institute of Technology, Israel
Yuri Matiyasevich	Steklov Institute/St.Petersburg, Russia
Pierre McKenzie	Université de Montréal, Canada
Alexander Razborov	IAS, USA and Steklov Institute/Moscow, Russia
Victor Selivanov	Novosibirsk State Pedagogical University, Russia
Alexander Shen	LIF Marseille, France and IITP Moscow, Russia
Denis Thérien	McGill University, Canada

Applications and Technology Track

Dines Bjørner	The Technical University of Denmark, Denmark
Nikolaj Bjørner	Microsoft Research, USA
Stéphane Bressan	National University of Singapore, Singapore
Gabriel Ciobanu	Institute of Computer Science of Iasi, Romania
Leonid Kalinichenko	IPI Moscow, Russia
Laura Kovacs	RISC Linz, Austria
Torben Ægidius Mogensen	University of Copenhagen, Denmark
Alexandre Petrenko	CRIM, Montréal, Canada
Sibylle Schupp	Chalmers University of Technology, Sweden
Oleg Sokolski	University of Pennsylvania, USA
Helmut Veith	Technische Universität München, Germany
Andrey Voronkov (Chair)	University of Manchester, UK

Conference Chair

Mikhail Volkov

Ural State University, Russia

Steering Committee for CSR Conferences

Anna Frid

Edward Hirsch

Juhani Karhumäki

Mikhail Volkov

Sobolev Institute/Novosibirsk, Russia

Steklov Institute/St.Petersburg, Russia

University of Turku, Finland

Ural State University, Russia

Referees

Bogdan Aman

Sergei Avgustinovich

Maxim Babenko

Reuven Bar-Yehuda

Eli Ben-Sasson

Daniel Berend

Therese Biedl

Markus Blaeser

Cosmin Bonchis

Sergiy Boroday

Mark Braverman

Olivier Carton

Julien Cassaigne

Steve Chain

Arkadev Chattopadhyay

Rafi Chen

Christian Choffrut

Maria Chudnovsky

Veronique Cortier

Felipe Cucker

Arnaud Dury

Henning Fernau

Hasham Hallal

May Haydar

Dmitry Itsykson

Ethan Jackson

Stasys Jukna

Jarkko Kari

Dmitry Karpov

Stefan Katzenbeisser

Olga Kharlampovich

Boris Konev

Levente Kovacs

Steve Kremer

Manfred Kufleitner

Stefan Kugele

Alexander Kulikov

Orna Kupferman

Roman Kuznets

Fribourg Laurent

Leonid Levin

Ming Li

Yury Lifshits

Alexis Maciel

Guillaume Malod

Bernard Mans

Larry Moss

Frantisek Mraz

Sergey Nikolenko

Dirk Nowotka

Friedrich Otto

Eric Pacuit

Alexei Pastor

Mati Pentus

Holger Petersen

Martin Platek

Igor Potapov

Artem Pyatkin

Christian Reitwiessner

Maurice Rojas

Samer Salame
Rahul Santhanam
John E. Savage
Uwe Schöning
Bart Selman
Rocco Servedio
Jeffrey Shallit
Evgeny Skvortsov
Anatol Slissenko
Andreas Steininger
Sergey Stupnikov
Alexei Talambutsa

Suguru Tamaki
Tony Tan
Michael Tautschnig
Pascal Tesson
Thomas Thierauf
Avraham Trahtman
Nikolay Vereshchagin
Volodya Vovk
Klaus Wagner
Derry Wijaya
Alexander Wolpert

Sponsors

Microsoft Research
Russian Foundation for Basic Research
SKB Kontur
Ural State University
Yandex
ZAO Spectralus

Lecture Notes in Computer Science

For information about Vols. 1–4560

please contact your bookseller or Springer

Vol. 4708: L. Kučera, A. Kučera (Eds.), *Mathematical Foundations of Computer Science 2007*. XVIII, 764 pages. 2007.

Vol. 4705: O. Gervasi, M. Gavrilova (Eds.), *Computational Science and Its Applications – ICCSA 2007*, Part I. XLIV, 1169 pages. 2007.

Vol. 4697: L. Choi, Y. Paek, S. Cho (Eds.), *Advances in Computer Systems Architecture*. XIII, 400 pages. 2007.

Vol. 4685: D.J. Veit, J. Altmann (Eds.), *Grid Economics and Business Models*. XIII, 201 pages. 2007.

Vol. 4682: D.-S. Huang, L. Heutte, M. Loog (Eds.), *Advanced Intelligent Computing Theories and Applications*. XXVII, 1373 pages. 2007. (Sublibrary LNAI).

Vol. 4681: D.-S. Huang, L. Heutte, M. Loog (Eds.), *Advanced Intelligent Computing Theories and Applications*. XXVI, 1379 pages. 2007.

Vol. 4679: A.L. Yuille, S.-C. Zhu, D. Cremers, Y. Wang (Eds.), *Energy Minimization Methods in Computer Vision and Pattern Recognition*. XII, 494 pages. 2007.

Vol. 4673: W.G. Kropatsch, M. Kampel, A. Hanbury (Eds.), *Computer Analysis of Images and Patterns*. XX, 1006 pages. 2007.

Vol. 4671: V. Malyshev (Ed.), *Parallel Computing Technologies*. XIV, 635 pages. 2007.

Vol. 4660: S. Džeroski, J. Todorovski (Eds.), *Computational Discovery of Scientific Knowledge*. X, 327 pages. 2007. (Sublibrary LNAI).

Vol. 4651: F. Azevedo, P. Barahona, F. Fages, F. Rossi (Eds.), *Recent Advances in Constraints*. VIII, 185 pages. 2007. (Sublibrary LNAI).

Vol. 4649: V. Diekert, M.V. Volkov, A. Voronkov (Eds.), *Computer Science – Theory and Applications*. XIII, 420 pages. 2007.

Vol. 4647: R. Martin, M. Sabin, J. Winkler (Eds.), *Mathematics of Surfaces*. XII. IX, 509 pages. 2007.

Vol. 4645: R. Giancarlo, S. Hannenhalli (Eds.), *Algorithms in Bioinformatics*. XIII, 432 pages. 2007. (Sublibrary LNBI).

Vol. 4643: M.-F. Sagot, M.E.M.T. Walter (Eds.), *Advances in Bioinformatics and Computational Biology*. XII, 177 pages. 2007. (Sublibrary LNBI).

Vol. 4639: E. Csuhaj-Varjú, Z. Ésik (Eds.), *Fundamentals of Computation Theory*. XIV, 508 pages. 2007.

Vol. 4637: C. Kruegel, R. Lippmann, A. Clark (Eds.), *Recent Advances in Intrusion Detection*. XII, 338 pages. 2007.

Vol. 4635: B. Kocinov, D.C. Richardson, T.R. Roth-Berghofer, L. Vieu (Eds.), *Modeling and Using Context*. XIV, 574 pages. 2007. (Sublibrary LNAI).

Vol. 4634: H.R. Nielson, G. Filé (Eds.), *Static Analysis*. XI, 469 pages. 2007.

Vol. 4633: M. Kamel, A. Campilho (Eds.), *Image Analysis and Recognition*. XII, 1312 pages. 2007.

Vol. 4632: R. Alhajj, H. Gao, X. Li, J. Li, O.R. Zaiane (Eds.), *Advanced Data Mining and Applications*. XV, 634 pages. 2007. (Sublibrary LNAI).

Vol. 4628: L.N. de Castro, F.J. Von Zuben, H. Knidel (Eds.), *Artificial Immune Systems*. XII, 438 pages. 2007.

Vol. 4627: M. Charikar, K. Jansen, O. Reingold, J.D.P. Rolim (Eds.), *Approximation, Randomization, and Combinatorial Optimization*. XII, 626 pages. 2007.

Vol. 4626: R.O. Weber, M.M. Richter (Eds.), *Case-Based Reasoning Research and Development*. XIII, 534 pages. 2007. (Sublibrary LNAI).

Vol. 4624: T. Mossakowski, U. Montanari, M. Haverlaan (Eds.), *Algebra and Coalgebra in Computer Science*. XI, 463 pages. 2007.

Vol. 4622: A. Menezes (Ed.), *Advances in Cryptology - CRYPTO 2007*. XIV, 631 pages. 2007.

Vol. 4619: F. Dehne, J.-R. Sack, N. Zeh (Eds.), *Algorithms and Data Structures*. XVI, 662 pages. 2007.

Vol. 4618: S.G. Akl, C.S. Calude, M.J. Dinneen, G. Rozenberg, H.T. Wareham (Eds.), *Unconventional Computation*. X, 243 pages. 2007.

Vol. 4617: V. Torra, Y. Narukawa, Y. Yoshida (Eds.), *Modeling Decisions for Artificial Intelligence*. XII, 502 pages. 2007. (Sublibrary LNAI).

Vol. 4616: A. Dress, Y. Xu, B. Zhu (Eds.), *Combinatorial Optimization and Applications*. XI, 390 pages. 2007.

Vol. 4615: R. de Lemos, C. Gacek, A. Romanovsky (Eds.), *Architecting Dependable Systems IV*. XIV, 435 pages. 2007.

Vol. 4613: F.P. Preparata, Q. Fang (Eds.), *Frontiers in Algorithmics*. XI, 348 pages. 2007.

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

Vol. 4611: J. Indulska, J. Ma, L.T. Yang, T. Ungerer, J. Cao (Eds.), *Ubiquitous Intelligence and Computing*. XXIII, 1257 pages. 2007.

Vol. 4610: B. Xiao, L.T. Yang, J. Ma, C. Muller-Schloer, Y. Hua (Eds.), *Autonomic and Trusted Computing*. XVIII, 571 pages. 2007.

Vol. 4609: E. Ernst (Ed.), *ECOOOP 2007 – Object-Oriented Programming*. XIII, 625 pages. 2007.

Vol. 4608: H.W. Schmidt, I. Crnkovic, G.T. Heineman, J.A. Stafford (Eds.), *Component-Based Software Engineering*. XII, 283 pages. 2007.

- Vol. 4607: L. Baresi, P. Fraternali, G.-J. Houben (Eds.), *Web Engineering*. XVI, 576 pages. 2007.
- Vol. 4606: A. Pras, M. van Sinderen (Eds.), *Dependable and Adaptable Networks and Services*. XIV, 149 pages. 2007.
- Vol. 4605: D. Papadias, D. Zhang, G. Kollios (Eds.), *Advances in Spatial and Temporal Databases*. X, 479 pages. 2007.
- Vol. 4604: U. Priss, S. Polovina, R. Hill (Eds.), *Conceptual Structures: Knowledge Architectures for Smart Applications*. XII, 514 pages. 2007. (Sublibrary LNAI).
- Vol. 4603: F. Pfenning (Ed.), *Automated Deduction – CADE-21*. XII, 522 pages. 2007. (Sublibrary LNAI).
- Vol. 4602: S. Barker, G.-J. Ahn (Eds.), *Data and Applications Security XXI*. X, 291 pages. 2007.
- Vol. 4600: H. Comon-Lundh, C. Kirchner, H. Kirchner (Eds.), *Rewriting, Computation and Proof*. XVI, 273 pages. 2007.
- Vol. 4599: S. Vassiliadis, M. Berekovic, T.D. Hämmäläinen (Eds.), *Embedded Computer Systems: Architectures, Modeling, and Simulation*. XVIII, 466 pages. 2007.
- Vol. 4598: G. Lin (Ed.), *Computing and Combinatorics*. XII, 570 pages. 2007.
- Vol. 4597: P. Perner (Ed.), *Advances in Data Mining*. XI, 353 pages. 2007. (Sublibrary LNAI).
- Vol. 4596: L. Arge, C. Cachin, T. Jurdziński, A. Tarlecki (Eds.), *Automata, Languages and Programming*. XVII, 953 pages. 2007.
- Vol. 4595: D. Bošnački, S. Edelkamp (Eds.), *Model Checking Software*. X, 285 pages. 2007.
- Vol. 4594: R. Bellazzi, A. Abu-Hanna, J. Hunter (Eds.), *Artificial Intelligence in Medicine*. XVI, 509 pages. 2007. (Sublibrary LNAI).
- Vol. 4592: Z. Kedad, N. Lammari, E. Métais, F. Meziane, Y. Rezgui (Eds.), *Natural Language Processing and Information Systems*. XIV, 442 pages. 2007.
- Vol. 4591: J. Davies, J. Gibbons (Eds.), *Integrated Formal Methods*. IX, 660 pages. 2007.
- Vol. 4590: W. Damm, H. Hermanns (Eds.), *Computer Aided Verification*. XV, 562 pages. 2007.
- Vol. 4589: J. Münch, P. Abrahamsson (Eds.), *Product-Focused Software Process Improvement*. XII, 414 pages. 2007.
- Vol. 4588: T. Harju, J. Karhumäki, A. Lepistö (Eds.), *Developments in Language Theory*. XI, 423 pages. 2007.
- Vol. 4587: R. Cooper, J. Kennedy (Eds.), *Data Management*. XIII, 259 pages. 2007.
- Vol. 4586: J. Pieprzyk, H. Ghodosi, E. Dawson (Eds.), *Information Security and Privacy*. XIV, 476 pages. 2007.
- Vol. 4585: M. Kryszkiewicz, J.F. Peters, H. Rybinski, A. Skowron (Eds.), *Rough Sets and Intelligent Systems Paradigms*. XIX, 836 pages. 2007. (Sublibrary LNAI).
- Vol. 4584: N. Karssemeijer, B. Believeltd (Eds.), *Information Processing in Medical Imaging*. XX, 777 pages. 2007.
- Vol. 4583: S.R. Della Rocca (Ed.), *Typed Lambda Calculi and Applications*. X, 397 pages. 2007.
- Vol. 4582: J. Lopez, P. Samarati, J.L. Ferrer (Eds.), *Public Key Infrastructure*. XI, 375 pages. 2007.
- Vol. 4581: A. Petrenko, M. Veanes, J. Tretmans, W. Grieskamp (Eds.), *Testing of Software and Communicating Systems*. XII, 379 pages. 2007.
- Vol. 4580: B. Ma, K. Zhang (Eds.), *Combinatorial Pattern Matching*. XII, 366 pages. 2007.
- Vol. 4579: B. M. Hämmerli, R. Sommer (Eds.), *Detection of Intrusions and Malware, and Vulnerability Assessment*. X, 251 pages. 2007.
- Vol. 4578: F. Masulli, S. Mitra, G. Pasi (Eds.), *Applications of Fuzzy Sets Theory*. XVIII, 693 pages. 2007. (Sublibrary LNAI).
- Vol. 4577: N. Sebe, Y. Liu, Y.-t. Zhuang, T.S. Huang (Eds.), *Multimedia Content Analysis and Mining*. XIII, 513 pages. 2007.
- Vol. 4576: D. Leivant, R. de Queiroz (Eds.), *Logic, Language, Information and Computation*. X, 363 pages. 2007.
- Vol. 4575: T. Takagi, T. Okamoto, E. Okamoto, T. Okamoto (Eds.), *Pairing-Based Cryptography – Pairing 2007*. XI, 408 pages. 2007.
- Vol. 4574: J. Derrick, J. Vain (Eds.), *Formal Techniques for Networked and Distributed Systems – FORTE 2007*. XI, 375 pages. 2007.
- Vol. 4573: M. Kauers, M. Kerber, R. Miner, W. Windsteiger (Eds.), *Towards Mechanized Mathematical Assistants*. XIII, 407 pages. 2007. (Sublibrary LNAI).
- Vol. 4572: F. Stajano, C. Meadows, S. Capkun, T. Moore (Eds.), *Security and Privacy in Ad-hoc and Sensor Networks*. X, 247 pages. 2007.
- Vol. 4571: P. Perner (Ed.), *Machine Learning and Data Mining in Pattern Recognition*. XIV, 913 pages. 2007. (Sublibrary LNAI).
- Vol. 4570: H.G. Okuno, M. Ali (Eds.), *New Trends in Applied Artificial Intelligence*. XXI, 1194 pages. 2007. (Sublibrary LNAI).
- Vol. 4569: A. Butz, B. Fisher, A. Krüger, P. Olivier, S. Owada (Eds.), *Smart Graphics*. IX, 237 pages. 2007.
- Vol. 4568: T. Ishida, S. R. Fussell, P. T. J. M. Vossen (Eds.), *Intercultural Collaboration*. XIII, 395 pages. 2007.
- Vol. 4566: M.J. Dainoff (Ed.), *Ergonomics and Health Aspects of Work with Computers*. XVIII, 390 pages. 2007.
- Vol. 4565: D.D. Schmorrow, L.M. Reeves (Eds.), *Foundations of Augmented Cognition*. XIX, 450 pages. 2007. (Sublibrary LNAI).
- Vol. 4564: D. Schuler (Ed.), *Online Communities and Social Computing*. XVII, 520 pages. 2007.
- Vol. 4563: R. Shumaker (Ed.), *Virtual Reality*. XXII, 762 pages. 2007.
- Vol. 4562: D. Harris (Ed.), *Engineering Psychology and Cognitive Ergonomics*. XXIII, 879 pages. 2007. (Sublibrary LNAI).
- Vol. 4561: V.G. Duffy (Ed.), *Digital Human Modeling*. XXIII, 1068 pages. 2007.

Table of Contents

Proving Church's Thesis (Invited Talk)	1
<i>Yuri Gurevich</i>	
The Limits of Quantum Computers (Invited Talk)	4
<i>Scott Aaronson</i>	
Marrying Words and Trees (Invited Talk)	5
<i>Rajeev Alur</i>	
TPTP, TSTP, CASC, etc. (Invited Talk)	6
<i>Geoff Sutcliffe</i>	
Abstract Modeling and Formal Verification of Microprocessors (Invited Talk)	23
<i>Ziyad Hanna</i>	
Sequences of Level 1, 2, 3, . . . , k , . . . (Invited Talk)	24
<i>Géraud Sénizergues</i>	
Timers and Proximities for Mobile Ambients	33
<i>Bogdan Aman and Gabriel Ciobanu</i>	
Pushing Random Walk Beyond Golden Ratio	44
<i>Ehsan Amiri and Evgeny Skvortsov</i>	
Reversible Machine Code and Its Abstract Processor Architecture	56
<i>Holger Bock Azelsen, Robert Glück, and Tetsuo Yokoyama</i>	
A Fast Algorithm for Path 2-Packing Problem	70
<i>Maxim A. Babenko</i>	
Decidability of Parameterized Probabilistic Information Flow	82
<i>Danièle Beauquier, Marie Duflot, and Yury Lifshits</i>	
Inverting Onto Functions and Polynomial Hierarchy	92
<i>Harry Buhrman, Lance Fortnow, Michal Koucký, John D. Rogers, and Nikolay Vereshchagin</i>	
Proved-Patterns-Based Development for Structured Programs	104
<i>Dominique Cansell and Dominique Méry</i>	
Planarity, Determinants, Permanents, and (Unique) Matchings	115
<i>Samir Datta, Raghav Kulkarni, Nutan Limaye, and Meena Mahajan</i>	

Equivalence Problems for Circuits over Sets of Natural Numbers	127
<i>Christian Glaßer, Katrin Herr, Christian Reitwießner, Stephen Travers, and Matthias Waldherr</i>	
Bouillon: A Wiki-Wiki Social Web	139
<i>Victor Grishchenko</i>	
A PDL-Like Logic of Knowledge Acquisition	146
<i>Bernhard Heinemann</i>	
Resource Placement in Networks Using Chromatic Sets of Power Graphs	158
<i>Navid Imani, Hamid Sarbazi-Azad, and Selim G. Akl</i>	
Conjunctive Grammars over a Unary Alphabet: Undecidability and Unbounded Growth	168
<i>Artur Jež and Alexander Okhotin</i>	
Ruling Out Polynomial-Time Approximation Schemes for Hard Constraint Satisfaction Problems	182
<i>Peter Jonsson, Andrei Krokhin, and Fredrik Kuivinen</i>	
New Bounds for MAX-SAT by Clause Learning	194
<i>Alexander S. Kulikov and Konstantin Kutzkov</i>	
Towards Hierarchical Clustering (Extended Abstract)	205
<i>Mark Sh. Levin</i>	
Estimation of the Click Volume by Large Scale Regression Analysis	216
<i>Yury Lifshits and Dirk Nowotka</i>	
Maximal Intersection Queries in Randomized Graph Models	227
<i>Benjamin Hoffmann, Yury Lifshits, and Dirk Nowotka</i>	
A Note on Specialization of Interpreters	237
<i>Alexei Lisitsa and Andrei P. Nemytykh</i>	
Efficient Computation in Groups Via Compression	249
<i>Markus Lohrey and Saul Schleimer</i>	
Constructing a Secret Binary Partition of a Digital Image Robust to a Loss of Synchronization	259
<i>Alexei Lysenko</i>	
On the Complexity of Matrix Rank and Rigidity	269
<i>Meena Mahajan and Jayalal Sarma M.N.</i>	
On the Usage of Clustering for Content Based Image Retrieval	281
<i>Jorge R. Manjarrez Sanchez, Jose Martinez, and Patrick Valduriez</i>	

Performance Modeling of Wormhole Hypermeshes Under Hotspot Traffic	290
<i>Reza Moraveji, Hamid Sarbazi-Azad, Abbas Nayebi, and Keyvan Navi</i>	
Application of Modified Coloured Petri Nets to Modeling and Verification of SDL Specified Communication Protocols	303
<i>Valery A. Nepomniaschy, Gennady I. Alekseev, Victor S. Argirov, Dmitri M. Beloglazov, Alexander V. Bystrov, Eugene A. Chetvertakov, Tatiana G. Churina, Sergey P. Mylnikov, and Ruslan M. Novikov</i>	
Symmetry of Information and Nonuniform Lower Bounds	315
<i>Sylvain Perifel</i>	
Perceptrons of Large Weight	328
<i>Vladimir V. Podolskii</i>	
A Padding Technique on Cellular Automata to Transfer Inclusions of Complexity Classes	337
<i>Victor Poupet</i>	
Kolmogorov Complexity, Lovász Local Lemma and Critical Exponents	349
<i>Andrey Yu. Rumyantsev</i>	
Generic Complexity of Presburger Arithmetic	356
<i>Alexander N. Rybalov</i>	
Everywhere α -Repetitive Sequences and Sturmian Words	362
<i>Kalle Saari</i>	
Timed Traces and Strand Spaces	373
<i>Robin Sharp and Michael R. Hansen</i>	
On Empirical Meaning of Randomness with Respect to a Real Parameter	387
<i>Vladimir V'yugin</i>	
An Efficient Algorithm for Zero-Testing of a Lacunary Polynomial at the Roots of Unity	397
<i>Sergey P. Tarasov and Mikhail N. Vyalyi</i>	
Generic Complexity of Undecidable Problems	407
<i>Alexei Myasnikov</i>	
Author Index	419

Proving Church's Thesis

(Abstract)

Yuri Gurevich

Microsoft Research

The talk reflects recent joint work with Nachum Dershowitz [4].

In 1936, Church suggested that the recursive functions, which had been defined by Gödel earlier that decade, adequately capture the intuitive notion of a computable (“effectively calculable”) numerical function¹ [2]. Independently Turing argued that, for strings-to-strings functions, the same goal is achieved by his machines [11].

The modern form of Church's thesis is due to Church's student Kleene. It asserts that every computable numerical partial function is partial recursive. (Originally Church spoke of total functions.)

Kleene thought that the thesis was unprovable: “Since our original notion of effective calculability... is a somewhat vague intuitive one, the thesis cannot be proved” [7]. But he presented evidence in favor of the thesis. By far the strongest argument was Turing's analysis [11] of “the sorts of operations which a human computer could perform, working according to preassigned instructions” [7]. The argument convinced Gödel who thought the idea “that this really is the correct definition of mechanical computability was established beyond any doubt by Turing” [5].

Moreover, Gödel has been reported to have thought “that it might be possible ... to state a set of axioms which would embody the generally accepted properties of [effective calculability], and to do something on that basis” [3]. As explained by Shoenfield [10]:

It may seem that it is impossible to give a proof of Church's Thesis. However, this is not necessarily the case. ... In other words, we can write down some axioms about computable functions which most people would agree are evidently true. It might be possible to prove Church's Thesis from such axioms. ... However, despite strenuous efforts, no one has succeeded in doing this (although some interesting partial results have been obtained).

We will demonstrate that, under certain very natural hypotheses regarding algorithmic activity, called the “Sequential Postulates” [6], Church's Thesis is in fact provable. In brief, the postulates say the following.

I. Sequential Time. *An algorithm determines a sequence of “computational” states for each valid input.*

¹ For brevity we use the term numerical function to mean a function from natural numbers to natural numbers.

- II. Abstract State.** *The states of a computational sequence can be arbitrary (first-order) structures.*
- III. Bounded Exploration.** *The transitions from state to state in the sequence are governed by a finite description.*

For precise formulation of the three postulates see the article [6]. With Bounded Exploration, an algorithm computes in “steps of limited complexity”, as demanded by Kolmogorov [8]. This postulate thereby answers Kolmogorov’s implicit question: What does it mean to bound the complexity of each individual step?

The postulates are justified in the article [6]. On this ground, a (sequential) algorithm is defined there as any object satisfying the three postulates. One may worry that this definition is too liberal. To this end, the article proves that (sequential) abstract state machines, introduced earlier by the author, satisfy the three postulates, and that, for every algorithm, there is an abstract state machine that emulates the algorithm.

To focus on numerical algorithms, we add the following postulate:

- IV.** *Only basic arithmetic operations are available initially.*

Algorithms satisfying postulate IV will be called numerical.

We will show that Church’s Thesis provably follows from these four postulates.

Theorem 1. *Any numerical partial function is computed by a numerical algorithm if and only if it is partial recursive.*

Thus, to the extent that one might entertain the notion that there exist non-recursive effective functions, one must reject one or more of these postulates. In a similar way, we can prove Turing’s thesis from postulates I–III and a postulate.

- V.** *Only basic string operations are available initially.*

Theorem 1 generalizes to the case when oracles are present. If only oracle functions are available initially, postulates I–III suffice. No additional postulates are needed.

Our goal in this work has been to remedy the situation described thus by Montague [9]: “Discussion of Church’s thesis has suffered for lack of a precise general framework within which it could be conducted.” We show how the Sequential ASM Postulates provide just such a framework. As we mentioned, Gödel surmised that Church’s Thesis may follow from appropriate axioms of computability. But, as far as we can ascertain, no complete axiomatization has previously been presented in the literature. In fact, the challenge of proving Church’s Thesis is first in Shore’s list of “pie-in-the-sky problems” for the twenty-first century [1].

References

1. Buss, S.R., Kechris, A.A., Pillay, A., Shore, R.A.: Prospects for mathematical logic in the twenty-first century. *Bulletin of Symbolic Logic* 7(2), 169–196 (2001)
2. Church, A.: An unsolvable problem of elementary number theory. *American Journal of Mathematics* 58, 345–363 (1936)
3. Davis, M.: Why Gödel didn't have Church's thesis. *Information and Control* 54, 3–24 (1982)
4. Dershowitz, N., Gurevich, Y.: A natural axiomatization of Church's thesis (to appear)
5. Gödel, K.: Kurt Gödel: Collected Works. In: Feferman, S. (ed.) *Unpublished essays and lectures*, vol. III, p. 168. Oxford University Press, Oxford (1995)
6. Gurevich, Y.: Sequential abstract state machines capture sequential algorithms. *ACM Transactions on Computational Logic* 1, 77–111 (2000)
7. Kleene, S.C.: *Introduction to Metamathematics*, North Holland, Amsterdam (1952)
8. Kolmogorov, A. N.: O ponyatii algoritma (On the concept of algorithm), *Uspekhi Matematicheskikh Nauk*, vol. 8(4), pp. 175–176 (1953) (in Russian). An English translation is In: Uspensky, V.A., Semenov, A.L.: *Algorithms: Main Ideas and Applications*, pp. 18–19. Kluwer (1993)
9. Montague, R.: Towards a general theory of computability. *Synthese* 12(4), 429–438 (1960)
10. Shoenfield, J.R.: *Recursion Theory*. *Lecture Notes in Logic*, vol. 1. Springer, New York (1991)
11. Turing, A.M.: On computable numbers, with an application to the Entscheidungsproblem. In: *Proceedings of the London Mathematical Society*, vol. 42, pp. 230–265, 1936–37. Corrections in vol. 43, pp. 544–546 (1937)