LNCS 4639

Erzsébet Csuhaj-Varjú
Zoltán Ésik (Eds.)

Fundamentals of Computation Theory

16th International Symposium, FCT 2007
Budapest, Hungary, August 2007
Proceedings

Springer

Erzsébet Csuhaj-Varjú
Zoltán Ésik (Eds.)

Fundamentals of Computation Theory

16th International Symposium, FCT 2007
Budapest, Hungary, August 27-30, 2007
Proceedings

Springer

Volume Editors

Erzsébet Csuhaj-Varjú
Hungarian Academy of Sciences
Computer and Automation Research Institute
Budapest, Hungary
E-mail: csuhaj@sztaki.hu

Zoltán Ésik
University of Szeged
Department of Computer Science
Szeged, Hungary
E-mail: ze@inf.u-szeged.hu

Library of Congress Control Number: 2007932400

CR Subject Classification (1998): F.1, F.2, F.4.1, I.3.5, G.2

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

ISSN 0302-9743
ISBN-10 3-540-74239-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-74239-5 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: 12108152 06/3180 5 4 3 2 1 0

Lecture Notes in Computer Science 4639

Preface

The Symposium on Fundamentals of Computation Theory was established in 1977 for researchers interested in all aspects of theoretical computer science, in particular in algorithms, complexity, and formal and logical methods. It is a biennial conference, which has previously been held in Poznan (1977), Wendisch-Rietz (1979), Szeged (1981), Borgholm (1983), Cottbus (1985), Kazan (1987), Szeged (1989), Gosen-Berlin (1991), Szeged (1993), Dresden (1995), Kraków (1997), Iasi (1999), Riga (2001), Malmö (2003), and Lübeck (2005).

The 16th International Symposium on Fundamentals of Computation Theory (FCT 2007) was held in Budapest, August 27–30, 2007, and was jointly organized by the Computer and Automation Research Institute of the Hungarian Academy of Sciences and the Institute of Computer Science, University of Szeged.

The suggested topics of FCT 2007 included, but were not limited to, automata and formal languages, design and analysis of algorithms, computational and structural complexity, semantics, logic, algebra and categories in computer science, circuits and networks, learning theory, specification and verification, parallel and distributed systems, concurrency theory, cryptography and cryptographic protocols, approximation and randomized algorithms, computational geometry, quantum computation and information, and bio-inspired computation.

The Programme Committee invited lectures from Ahmed Bouajjani (Paris), Oscar H. Ibarra (Santa Barbara), László Lovász (Budapest), and Philip J. Scott (Ottawa) and, from the 147 submissions, selected 39 papers for presentation at the conference and inclusion in the proceedings. This volume contains the texts or the abstracts of the invited lectures and the texts of the accepted papers.

We would like to thank the members of the Programme Committee for the evaluation of the submissions and their subreferees for their excellent cooperation in this work. We are grateful to the contributors to the conference, in particular to the invited speakers for their willingness to present interesting new developments.

Finally, we thank Zsolt Gazdag and Szabolcs Iván for their technical assistance during the preparation of these proceedings, and all those whose work behind the scenes contributed to this volume.

June 2007

Erzsébet Csuhaj-Varjú
Zoltán Ésik

Organization

Programme Committee

Jiri Adámek (Braunschweig, Germany)
Giorgio Ausiello (Rome, Italy)
Jean Berstel (Marne-la-Vallée, France)
Flavio Corradini (Camerino, Italy)
Erzsébet Csuhaj-Varjú (Budapest, Hungary), co-chair
Zoltán Ésik (Szeged, Hungary), co-chair
Jozef Gruska (Brno, Czech Republic)
Masahito Hasegawa (Kyoto, Japan)
Juraj Hromkovic (Zurich, Switzerland)
Anna Ingólfsdóttir (Reykjavik, Iceland)
Masami Ito (Kyoto, Japan)
Frédéric Magniez (Paris, France)
Catuscia Palamidessi (Palaiseau, France)
Gheorghe Păun (Bucharest, Romania and Seville, Spain)
Jean-Éric Pin (Paris, France)
Alexander Rabinovich (Tel-Aviv, Israel)
R. Ramanujam (Chennai, India)
Wojciech Rytter (Warsaw, Poland)
Arto Salomaa (Turku, Finland)
David A. Schmidt (Manhattan, KS, USA)
Alex Simpson (Edinburgh, UK)
Michael Sipser (Cambridge, MA, USA)
Colin Stirling (Edinburgh, UK)
Howard Straubing (Chestnut Hill, MA, USA)
György Turán (Chicago, IL, USA)
Thomas Wilke (Kiel, Germany)

Steering Committee

Bogdan S. Chlebus (Warsaw, Poland and Denver, USA)
Zoltán Ésik (Szeged, Hungary)
Marek Karpinski (Bonn, Germany), chair
Andrzej Lingas (Lund, Sweden)
Miklos Santha (Paris, France)
Eli Upfal (Providence, RI, USA)
Ingo Wegener (Dortmund, Germany)

Additional Referees

Scott Aaronson
Farid Ablayev
Luca Aceto
Dimitris Achlioptas
Ruben Agadzanyan
Jean-Paul Allouche
Roberto Amadio
Amihood Amir
Ricardo Baeza-Yates
Nikhil Bansal
Franco Barbanera
David A. Mix Barrington
Ezio Bartocci
Ingo Battenfeld
Paweł Baturo
Maurice H. ter Beek
Radim Bělohlávek
Dietmar Berwanger
Amitava Bhattacharya
Yngvi Björnsson
Zoltán Blázsik
Luc Boasson
Hans-Joachim Böckenhauer
Andreas Brandstädt
Diletta Cacciagrano
Nicola Cannata
Silvio Capobianco
Venanzio Capretta
Olivier Carton
Matteo Cavaliere
Sourav Chakraborty
Jean-Marc Champarnaud
Arkadev Chattopadhyay
Parimal P. Chaudhuri
Vincent Conitzer
José R. Correa
Bruno Courcelle
Pierluigi Crescenzi
Maxime Crochemore
Stefan Dantchev
Bhaskar DasGupta
Jürgen Dassow
Clelia De Felice
Camil Demetrescu
Mariangiola Dezani-Ciancaglini
Michael Domaratzki
Alberto Peinado Domínguez
Manfred Droste
Stefan Dziembowski
Bruno Escoffier
Olivier Finkel
Maurizio Gabbrielli
Peter Gacs
Ricard Gavaldà
Blaise Genest
Robert Gilman
Amy Glen
Judy Goldsmith
Éva Gombás
Martin Grohe
Jiong Guo
Dan Gutfreund
Michel Habib
Vesa Halava
Bjarni V. Halldórsson
Magnús M. Halldórsson
Joseph Y. Halpern
Laszlo Hars
Reinhold Heckmann
Yoram Hirshfeld
Petr Hliněný
Štěpán Holub
Hendrik Jan Hoogeboom
Tamás Horváth
Brian Howard
Mihály Hujter
Mathilde Hurand
Atsushi Igarashi
Lucian Ilie
Csanád Imreh
Chuzo Iwamoto
Klaus Jansen
Emmanuel Jeandel
Yoshihiko Kakutani
Haim Kaplan
Marc Kaplan
Christos Kapoutsis
Juhani Karhumäki
Marek Karpinski
Shin-ya Katsumata
Zurab Khasidashvili
Jürgen Koslowski
Łukasz Kowalik
Mirek Kowaluk
Richard Kralovic
Manfred Kudlek
Werner Kuich
Arvind Kumar
Michal Kunc
Sonia L'Innocente
Anna Labella
Marie Lalire
Sophie Laplante
Peeter Laud
Troy Lee
Stefano Leonardi
Tal Lev-Ami
Nutan Limaye
Kamal Lodaya
Christof Löding
Sylvain Lombardy
Elena Losievskaja
Jack Lutz
Meena Mahajan
Sebastian Maneth
Pierre McKenzie
Paul-André Melliès
Massimo Merro
Antoine Meyer
Mehdi Mhalla
Sounaka Mishra
Tobias Mömke
Raúl Montes-de-Oca
Fabien de Montgolfier
Kenichi Morita

Mohammad Reza Mousavi
František Mráz
Marcin Mucha
Loránd Muzamel
Kedar Namjoshi
Sebastian Nanz
Zoltán L. Németh
Jean Néraud
Frank Neven
Brian Nielsen
Vivek Nigam
Hidenosuke Nishio
Mitsunori Ogihara
Yoshio Okamoto
Alexander Okhotin
Carlos Olarte
Bernhard Ömer
Marion Oswald
Sang-il Oum
Prakash Panangaden
Madhusudan Parthasarathy
Pawel Parys
Ion Petre
Wojciech Plandowski
Martin Plesch
Andrea Polini
Sanjiva Prasad
Pavel Pudlák
Tomasz Radzik
Stanisław P. Radziszowski
George Rahonis
Klaus Reinhardt
Eric Rémila
Vladimir Rogojin
Andrea Roli
Martin Rötteler
Michel de Rougemont
Michaël Rusinowitch
Jan Rutten
Marie-France Sagot
Miklos Santha
Jayalal Sarma
Benoît Saussol
Marcus Schaefer
Manfred Schimmler
Sebastian Seibert
Olivier Serre
Ehud Shapiro
Jeong Seop Sim
Sunil Simon
Jerzy Skurczyński
Michiel Smid
Jiří Srba
George Steiner
S. P. Suresh
Mario Szegedy
Luca Tesei
Carlo Toffalori
Masafumi Toyama
Vladimir Trifonov
Angelo Troina
Tomasz Truderung
Zsolt Tuza
Sándor Vágvölgyi
Frank D. Valencia
Leslie Valiant
Moshe Vardi
György Vaszil
Laurent Viennot
S. Vijayakumar
Leonardo Vito
Heiko Vogler
Laurent Vuillon
Bill Wadge
Magnus Wahlstrom
Thomas Worsch
Peng Wu
Yasushi Yamashita
Mihalis Yannakakis
Shoji Yuen
Eugen Zălinescu
Mario Ziman

Lecture Notes in Computer Science

For information about Vols. 1–4546

please contact your bookseller or Springer

Vol. 4671: V. Malyshkin (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. 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. 4634: H.R. Nielson, G. Filé (Eds.), Static Analysis. XI, 469 pages. 2007.

Vol. 4632: R. Alhajj, H. Gao, X. Li, J. Li, O.R. Zaïane (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. Mossakoski, U. Mantanari, M. Haveraaen (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.), ECOOP 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. Hämäläinen (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. Lelieveldt (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.

Vol. 4560: N. Aykin (Ed.), Usability and Internationalization, Part II. XVIII, 576 pages. 2007.

Vol. 4559: N. Aykin (Ed.), Usability and Internationalization, Part I. XVIII, 661 pages. 2007.

Vol. 4558: M.J. Smith, G. Salvendy (Eds.), Human Interface and the Management of Information, Part II. XXIII, 1162 pages. 2007.

Vol. 4557: M.J. Smith, G. Salvendy (Eds.), Human Interface and the Management of Information, Part I. XXII, 1030 pages. 2007.

Vol. 4556: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part III. XXII, 1020 pages. 2007.

Vol. 4555: C. Stephanidis (Ed.), Universal Access in Human-Computer Interaction, Part II. XXII, 1066 pages. 2007.

Vol. 4554: C. Stephanidis (Ed.), Universal Acess in Human Computer Interaction, Part I. XXII, 1054 pages. 2007.

Vol. 4553: J.A. Jacko (Ed.), Human-Computer Interaction, Part IV. XXIV, 1225 pages. 2007.

Vol. 4552: J.A. Jacko (Ed.), Human-Computer Interaction, Part III. XXI, 1038 pages. 2007.

Vol. 4551: J.A. Jacko (Ed.), Human-Computer Interaction, Part II. XXIII, 1253 pages. 2007.

Vol. 4550: J.A. Jacko (Ed.), Human-Computer Interaction, Part I. XXIII, 1240 pages. 2007.

Vol. 4549: J. Aspnes, C. Scheideler, A. Arora, S. Madden (Eds.), Distributed Computing in Sensor Systems. XIII, 417 pages. 2007.

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

Vol. 4547: C. Carlet, B. Sunar (Eds.), Arithmetic of Finite Fields. XI, 355 pages. 2007.

¥689.00元

Table of Contents

Invited Lectures

Contributions

Rewriting Systems with Data
A Framework for Reasoning About Systems with Unbounded Structures over Infinite Data Domains*

Ahmed Bouajjani[1], Peter Habermehl[1,2], Yan Jurski[1], and Mihaela Sighireanu[1]

[1] LIAFA, CNRS & U. Paris 7, Case 7014, 2 place Jussieu, 75251 Paris 05, France
[2] LSV, CNRS & ENS Cachan, 61 av Président Wilson, 94235 Cachan, France

Abstract. We introduce a uniform framework for reasoning about infinite-state systems with unbounded control structures and unbounded data domains. Our framework is based on constrained rewriting systems on words over an infinite alphabet. We consider several rewriting semantics: factor, prefix, and multiset rewriting. Constraints are expressed in a logic on such words which is parametrized by a first-order theory on the considered data domain. We show that our framework is suitable for reasoning about various classes of systems such as recursive sequential programs, multithreaded programs, parametrized and dynamic networks of processes, etc. Then, we provide generic results (1) for the decidability of the satisfiability problem of the fragment $\exists^*\forall^*$ of this logic provided that the underlying logic on data is decidable, and (2) for proving inductive invariance and for carrying out Hoare style reasoning within this fragment. We also show that the reachability problem is decidable for a class of prefix rewriting systems with integer data.

1 Introduction

Software verification requires in general reasoning about infinite-state models. The sources of infinity in software models are multiple. They can be related for instance to the complex control these system may have due, e.g., to recursive procedure calls, communication through fifo channels, dynamic creation of concurrent processes, or the consideration of a parametric number of parallel processes. Other important sources of infinity are related to the manipulation of variables and (dynamic) data structures ranging over infinite data domains such as integers, reals, arrays, heap structures like lists and trees, etc.

In the last few years, a lot of effort has been devoted to the development of theoretical frameworks for the formal modeling and the automatic analysis of several classes of software systems. Rewriting systems (on words or terms), as well as related automata-based frameworks, have been shown to be adequate for reasoning about various classes of systems such as recursive programs, multithreaded programs, parametrized or dynamic networks of identical processes, communicating systems through fifo-channels, etc. (see, e.g., [11,4,13] for survey

* Partially supported by the French ANR project ACI-06-SETI-001.

E. Csuhaj-Varjú and Z. Ésik (Eds.): FCT 2007, LNCS 4639, pp. 1–22, 2007.

papers). These works address in general the problem of handling systems with complex control structures, but where the manipulated data range of finite domains, basically booleans. Other existing works address the problem of handling models with finite control structures, but which manipulate variables over infinite data domains such as counters, clocks, etc., or unbounded data structures (over finite alphabets) such as stacks, queues, limited forms of heap memory (e.g., lists, trees), etc. [2,14,29,8,6,26,25,27,12,15]. Notice that the boundary between systems with infinite control and systems with infinite data is not sharp. For instance, recursive programs can be modeled as prefix rewrite systems which are equivalent to pushdown systems, and (classes of) multithreaded programs can be modeled using multiset rewrite systems which are equivalent to Petri nets and to vector addition systems (a particular class of counter machines).

As already said, in all the works mentionned above, only one source of infinity is taken into account (while the others are either ignored or abstracted away). Few works dealing with different sources of infinity have been carried out nevertheless, but the research on this topic is still in its emerging phase [5,1,21,19,17,3,16]. In this paper, we propose a uniform framework for reasoning about infinite-state systems with both unbounded control structures and unbounded data domains. Our framework is based on word rewriting systems over infinite alphabets where each element is composed from a label over a finite set of symbols and a vector of data in a potentially infinite domain. Words over such an alphabet are called data words and rewriting systems on such words are called data word rewriting systems (DWRS for short). A DWRS is a set of rewriting rules with constraints on the data carried by the elements of the words.

The framework we propose allows to consider different rewriting semantics and different theories on data, and allows also to apply in a generic way decision procedures and analysis techniques. The rewriting semantics we consider are either the factor rewriting semantics (which consists in replacing any factor in the word corresponding to the left hand side or a rule by the right hand side), as well as the prefix and the multiset rewriting semantics. The constraints in the rewriting systems are expressed in a logic called DWL which is an extension of the monadic first-order theory of the natural ordering on positive integers (corresponding to positions on the word) with a theory on data allowing to express the constraints on the data values at each position of the word. The theory on data, which is a parameter of the logic DWL, can be any fist-order theory such as Presburger arithmetics, or the first-order theory on reals.

We show that this framework is expressive enough to model various classes of infinite-state systems. Prefix rewriting systems are used to model recursive programs with global and local variables over infinite data domains. Factor rewriting systems are used for modeling parametrized networks of processes with a linear topology (i.e., there is a total ordering between the identities of the processes). This is for instance the case of various parallel and/or distributed algorithms. (We give as an example a model for the Lamport's Bakery algorithm for mutual exclusion.) Multiset rewriting systems can be used for modeling multithreaded programs or dynamic/parametrized networks where the information about identities of processes is not relevant. This is the case for various systems such as cache coherence protocols (see, e.g., [23]).

We address the decidability of the satisfiability problem of the logic DWL. We show that this problem is undecidable for very weak theories on data already for the fragment of $\forall^*\exists^*$ formulas. On the other hand, we prove the generic result that whenever the underlying theory on data has a decidable satisfiability problem, the fragment of $\exists^*\forall^*$ formulas of DWL has also a decidable satisfiability problem.

Then, we address the issue of automatic analysis of DWRS models. We provide two kinds of results. First, we consider the problem of carrying out post and pre condition reasoning based on computing immediate successors and immediate predecessors of sets of configurations. We prove, again in a generic way, that the fragment of $\exists^*\forall^*$ formulas in DWL is effectively closed under the computation of post and pre images by rewriting systems with constraints in $\exists^*\forall^*$. We show how this result, together with the decidability result of the satisfiability problem in $\exists^*\forall^*$, can be used for deciding whether a given assertion is an inductive invariant of a system, or whether the specification of an action is coherent, that is, the execution of an action starting from the pre condition leads to configurations satisfying the post condition. The framework we present here generalizes the one we introduced recently in [16] based on constrained multiset rewriting systems. Our generalization to word factor and prefix rewriting systems allows to deal in a uniform and natural way with a wider class of systems where reasoning about linearly ordered structures is needed.

Finally, we consider the problem of solving the reachability problem for a subclass of DWRS. We provide a new decidability result of this problem for the class of context-free prefix rewriting systems (i.e., where the left hand side of each rule is of size 1) over the data domain of integers with difference constraints. (Extensions of this class lead to undecidabilty.) This results generalizes a previous result we have established few years ago in [17] for a more restricted class of systems where not all difference constraints were allowed.

Related work: Regular model checking has been defined as a uniform framework for reasoning about infinite-state systems [29,28,18,4]. However, this framework is based on finite-state automata and transducers over finite alphabets which does not allow to deal in a simple and natural way with systems with both unbounded control and data domains. The same holds for similar frameworks based on word/tree rewriting systems over a finite alphabet (e.g., [11,13]).

Works on the analysis of models for systems with two sources of infinity such as networks of infinite-stat processes are not very numerous in the literature. In [5], the authors consider the case of networks of 1-clock timed systems and show that the verification problem for a class of safety properties is decidable under some restrictions on the used constraints. Their approach has been extended in [21,19] to a particular class of multiset rewrite systems with constraints (see also [3] for recent developments of this approach). In [17], we have considered the case of prefix rewrite systems with integer data which can be seen as models of recursive programs with one single integer parameter. Again, under some