BRICS Research Series, 2001

August 5, 2003

This document is also available as *PostScript* and *DVI*.

References

[RS-01-55] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Damian and Olivier Danvy. *A Simple CPS Transformation of Control-Flow Information*. December 2001. 18 pp. Appears in *Logic Journal of the IGPL*, 10(2):501–515, 2002.

[RS-01-54] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Damian and Olivier Danvy. *Syntactic Accidents in Program Analysis: On the Impact of the CPS Transformation*. December 2001. 41 pp. To appear in the *Journal of Functional Programming*. This report supersedes the earlier BRICS report RS-00-15.

[RS-01-53] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik and Masami Ito. *Temporal Logic with Cyclic Counting and the Degree of Aperiodicity of Finite Automata*. December 2001. 31 pp.

[RS-01-52] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jens Groth. *Extracting Witnesses from Proofs of Knowledge in the Random Oracle Model*. December 2001. 23 pp.

[RS-01-51] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *On Weak Markov's Principle*. December 2001. 10 pp. Appears in *Mathematical Logic Quarterly*, 48(suppl. 1):59–65, 2002.

[RS-01-50] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jiř Srba. *Note on the Tableau Technique for Commutative Transition Systems*. December 2001. 19 pp. Appears in Nielsen and Engberg, editors, *Foundations of Software Science and Computation Structures*, FoSSaCS '02 Proceedings, LNCS 2303, 2002, pages 387–401.

[RS-01-49] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Lasse R. Nielsen. *A First-Order One-Pass CPS Transformation*. December 2001. 21 pp. To appear in *Theoretical Computer Science*. Extended version of a paper appearing in Nielsen

and Engberg, editors, *Foundations of Software Science and Computation Structures*, FoSSaCS '02 Proceedings, LNCS 2303, 2002, pages 98–113.

[RS-01-48] **Abstract**, *PostScript*, *PDF*, *DVI*.
Mogens Nielsen and Frank D. Valencia. *Temporal Concurrent Constraint Programming: Applications and Behavior*. December 2001. 36 pp. Appears in Brauer, Ehrig, Karhumki and Salomaa, editors, *Formal and Natural Computing*, LNCS 2300, 2001, pages 298–321.

[RS-01-47] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jesper Buus Nielsen. *Non-Committing Encryption is Too Easy in the Random Oracle Model*. December 2001. 20 pp.

[RS-01-46] **Abstract**, *PostScript*, *PDF*, *DVI*.
Lars Kristiansen. *The Implicit Computational Complexity of Imperative Programming Languages*. November 2001. 46 pp.

[RS-01-45] **Abstract**, *PostScript*, *PDF*.
Ivan B. Damgrd and Gudmund Skovbjerg Frandsen. *An Extended Quadratic Frobenius Primality Test with Average Case Error Estimates*. November 2001. 43 pp.

[RS-01-44] **Abstract**, *PostScript*, *PDF*.
M. Oliver Mller, Harald Rue, and Maria Sorea. *Predicate Abstraction for Dense Real-Time Systems*. November 2001. 27 pp. Appears in Asarin, Maler and Yovine, editors, *Workshop on Theory and Practice of Timed Systems*, TPTS '02 Proceedings, ENTCS 65(6), 2002.

[RS-01-43] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Jesper Buus Nielsen. *From Known-Plaintext Security to Chosen-Plaintext Security*. November 2001. 18 pp.

[RS-01-42] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik and Werner Kuich. *Rationally Additive Semirings*. November 2001. 11 pp. Appears in *Journal of Universal Computer Science*, 8(2):173–183, 2002.

[RS-01-41] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Jesper Buus Nielsen. *Perfect Hiding and Perfect Binding Universally Composable Commitment Schemes with Constant Expansion Factor*. October 2001. 43 pp. Appears in Yung, editor, *Advances in Cryptology: 22nd Annual International Cryptology Conference*, CRYPTO '02 Proceedings, LNCS 2442, 2002, pages 581–596.

[RS-01-40] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Damian and Olivier Danvy. *CPS Transformation of Flow Information, Part II: Administrative Reductions*. October 2001. 9 pp. To appear in the *Journal of Functional Programming*. Superseeded by the BRICS report RS-02-36.

[RS-01-39] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Mayer Goldberg. *There and Back Again*. October 2001. 14 pp. To appear in the proceedings of the 2002 ACM SIGPLAN International Conference on Functional Programming.

[RS-01-38] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik. *Free De Morgan Bisemigroups and Bisemilattices*. October 2001. 13 pp. To appear in the journal *Algebra Colloquium*.

[RS-01-37] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ronald Cramer and Victor Shoup. *Universal Hash Proofs and a Paradigm for Adaptive Chosen Ciphertext Secure Public-Key Encryption*. October 2001. 34 pp.

[RS-01-36] **Abstract**, *PostScript*, *PDF*.
Gerth Stlting Brodal, Rolf Fagerberg, and Riko Jacob. *Cache Oblivious Search Trees via Binary Trees of Small Height*. October 2001. 20 pp. Appears in Eppstein, editor, *The Thirteenths Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '02 Proceedings, 2002, pages 39–48.

[RS-01-35] **Abstract**, *PostScript*, *PDF*, *DVI*.
Mayer Goldberg. *A General Schema for Constructing One-Point Bases in the Lambda Calculus*. September 2001. 8 pp.

[RS-01-34] **Abstract**, *PostScript*, *PDF*.
Flemming Friche Rodler and Rasmus Pagh. *Fast Random Access to Wavelet Compressed Volumetric Data Using Hashing*. August 2001. 31 pp. To appear in *ACM Transactions on Graphics*.

[RS-01-33] **Abstract**, *PostScript*, *PDF*.
Rasmus Pagh and Flemming Friche Rodler. *Lossy Dictionaries*. August 2001. 14 pp. Short version appears in Meyer auf der Heide, editor, *9th Annual European Symposium on Algorithms*, ESA '01 Proceedings, LNCS 2161, 2001, pages 300–311.

[RS-01-32] **Abstract**, *PostScript*, *PDF*.
Rasmus Pagh and Flemming Friche Rodler. *Cuckoo Hashing*. August 2001. 21 pp. Short version appears in Meyer auf der Heide, editor, *9th Annual European Symposium on Algorithms*, ESA '01 Proceedings, LNCS 2161, 2001, pages 121–133.

[RS-01-31] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Lasse R. Nielsen. *Syntactic Theories in Practice*. July 2001. 37 pp. Extended version of an article to appear in the informal proceedings of the *Second International Workshop on Rule-Based Programming*, RULE 2001 (Firenze, Italy, September 4, 2001). Superseeded by the BRICS report RS-02-4.

[RS-01-30] **Abstract**, *PostScript*, *PDF*, *DVI*.
Lasse R. Nielsen. *A Selective CPS Transformation*. July 2001. 24 pp. Appears in Brookes and Mislove, editors, *27th Annual Conference on the Mathematical Foundations of Programming Semantics*,

MFPS '01 Proceedings, ENTCS 45, 2001. A preliminary version appeared in Brookes and Mislove, editors, *17th Annual Conference on Mathematical Foundations of Programming Semantics*, MFPS '01 Preliminary Proceedings, BRICS Notes Series NS-01-2, 2001, pages 201–222.

[RS-01-29] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy, Bernd Grobauer, and Morten Rhiger. *A Unifying Approach to Goal-Directed Evaluation*. July 2001. 23 pp. Appears in *New Generation Computing*, 20(1):53–73, November 2001. A preliminary version appeared in Taha, editor, *2nd International Workshop on Semantics, Applications, and Implementation of Program Generation*, SAIG '01 Proceedings, LNCS 2196, 2001, pages 108–125.

[RS-01-28] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Zoltn sik, and Anna Inglfsdttir. *A Fully Equational Proof of Parikh's Theorem*. June 2001. 28 pp. Appears in *RAIRO, Theoretical Informatics and Applications*, 36(2):129–153, 2002, special issue devoted to selected papers from FICS 2001 (A. Labella ed.).

[RS-01-27] **Abstract**, *PostScript*, *PDF*, *DVI*.
Mario Jos Cccamo and Glynn Winskel. *A Higher-Order Calculus for Categories*. June 2001. 24 pp. Appears in Boulton and Jackson, editors, *Theorem Proving in Higher Order Logics: 14th International Conference*, TPHOLs '01 Proceedings, LNCS 2152, 2001, pages 136–153.

[RS-01-26] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrik Frendrup and Jesper Nyholm Jensen. *A Complete Axiomatization of Simulation for Regular CCS Expressions*. June 2001. 18 pp.

[RS-01-25] **Abstract**, *PostScript*, *PDF*, *DVI*.
Bernd Grobauer. *Cost Recurrences for DML Programs*. June 2001. 51 pp. Extended version of a paper appearing in Leroy, editor, *Proceedings of the 6th ACM SIGPLAN International Conference on Functional Programming*, 2001, pages 253–264.

[RS-01-24] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik and Zoltn L. Nmeth. *Automata on Series-Parallel Biposets*. June 2001. 15 pp. Appears in Kuich, Rozenberg and Salomaa, editors, *5th International Conference, Developments in Language Theory*, DLT '01 Revised Papers, LNCS 2295, 2002, pages 217–227. Superseded by the later BRICS report RS-02-44.

[RS-01-23] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Lasse R. Nielsen. *Defunctionalization at Work*. June 2001. 45 pp. Extended version of an article appearing in Sndergaard, editor, *3rd International Conference on Principles and Practice of Declarative Programming*, PPDP '01 Proceedings, 2001, pages 162–174.

[RS-01-22] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik. *The Equational Theory of Fixed Points with Applications to Generalized Language Theory*. June 2001. 21 pp. Appears in Kuich, Rozenberg and Salomaa, editors, *5th International Conference, Developments in Language Theory*, DLT '01 Revised Papers, LNCS 2295, 2002,pages 21–36.

[RS-01-21] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Zoltn sik, and Anna Inglfsdttir. *Equational Theories of Tropical Semirings*. June 2001. 52 pp. To appear in *Theoretical Computer Science*. Extended abstracts of parts of this paper have appeared in Honsell and Miculan, editors, *Foundations of Software Science and Computation Structures*, FoSSaCS '01 Proceedings, LNCS 2030, 2001, pages 42–56 and in Gaubert and Loiseau, editors, *Workshop on Max-Plus Algebras and Their Applications to Discrete-Event Systems, Theoretical Computer Science, and Optimization*, MAX-PLUS '01 Proceedings, IFAC (International Federation of Automatic Control) IFAC Publications, 2001.

[RS-01-20] **Abstract**, *PostScript*, *PDF*, *DVI*.
Catuscia Palamidessi and Frank D. Valencia. *A Temporal Concurrent Constraint Programming Calculus*. June 2001. 31 pp. Appears in Walsh, editor, *7th International Conference on Principles and Practice of Constraint Programming*, CP '01 Proceedings, LNCS 2239, 2001, pages 302–316.

[RS-01-19] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jiř Srba. *On the Power of Labels in Transition Systems*. June 2001. 23 pp. Full and extended version of Larsen and Nielsen, editors, *Concurrency Theory: 12th International Conference*, CONCUR '01 Proceedings, LNCS 2154, 2001, pages 277–291.

[RS-01-18] **Abstract**, *PostScript*, *PDF*.
Katalin M. Hangos, Zsolt Tuza, and Anders Yeo. *Some Complexity Problems on Single Input Double Output Controllers*. May 2001. 27 pp.

[RS-01-17] **Abstract**, *PostScript*, *PDF*.
Claus Brabrand, Anders Mller, Steffan Olesen, and Michael I. Schwartzbach. *Language-Based Caching of Dynamically Generated HTML*. May 2001. 18 pp. Appears in *World Wide Web Journal*, 5(4):305–323, 2002.

[RS-01-16] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy, Morten Rhiger, and Kristoffer H. Rose. *Normalization by Evaluation with Typed Abstract Syntax*. May 2001. 9 pp. Appears in *Journal of Functional Programming*, 11(6):673–68, November 2000.

[RS-01-15] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luigi Santocanale. *A Calculus of Circular Proofs and its Categorical*

Semantics. May 2001. 30 pp. Appears in Nielsen and Engberg, editors, *Foundations of Software Science and Computation Structures*, FoSSaCS '02 Proceedings, LNCS 2303, 2002, pages 129–143.

[RS-01-14] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach and Paulo B. Oliva. *Effective Bounds on Strong Unicity in L_1-Approximation.* May 2001. 38 pp. A revised and numerically much improved version appeared in *Annals of Pure and Applied Logic*, 121:1–38, 2003. Extended extended abstract appears in Hofmann, editor, *3rd International Workshop on Implicit Computational Complexity*, ICC '01 Proceedings, BRICS Notes Series NS-01-3, 2001, pages 117–122.

[RS-01-13] **Abstract**, *PostScript*, *PDF*, *DVI*.
Federico Crazzolara and Glynn Winskel. *Events in Security Protocols.* April 2001. 30 pp. Appears in *8th ACM conference on Computer and Communications Security*, CCS '01 Proceedings, 2001, pages 96–105.

[RS-01-12] **Abstract**, *PostScript*, *PDF*, *DVI*.
Torben Amtoft, Charles Consel, Olivier Danvy, and Karoline Malmkjr. *The Abstraction and Instantiation of String-Matching Programs.* April 2001. 37 pp. Appears in Mogensen, Schmidt and Sudborough, editors, *The Essence of Computation: Complexity, Analysis*, Transformation, LNCS 2556, 2002, pages 332–357.

[RS-01-11] **Abstract**, *PostScript*, *PDF*.
Alexandre David and M. Oliver Mller. *From* HUppaal *to* Uppaal*: A Translation from Hierarchical Timed Automata to Flat Timed Automata.* March 2001. 40 pp. Appears in Kutsche and Weber, editors, *Fundamental Approaches to Software Engineering: Fifth International Conference*, FASE '02 Proceedings, LNCS 2306, 2002, pages 218–232, with the title *Formal Verification of UML Statecharts with Real-Time Extensions.*

[RS-01-10] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Fridlender and Mia Indrika. *Do we Need Dependent Types?* March 2001. 6 pp. Appears in *Journal of Functional Programming*, 10(4):409–415, 2000. Superseeds BRICS Report RS-98-38.

[RS-01-9] **Abstract**, *PostScript*, *PDF*.
Claus Brabrand, Anders Mller, and Michael I. Schwartzbach. *Static Validation of Dynamically Generated HTML.* February 2001. 18 pp. Appears in Field and Snelting, editors, *ACM SIGPLAN-SIGSOFT Workshop on Program Analysis For Software Tools and Engineering*, PASTE '01 Proceedings, 2001, pages 38–45.

[RS-01-8] **Abstract**, *PostScript*, *PDF*.
Ulrik Frendrup and Jesper Nyholm Jensen. *Checking for Open Bisimilarity in the π-Calculus.* February 2001. 61 pp.

[RS-01-7] **Abstract**, *PostScript*, *PDF*, *DVI*.
Gregory Gutin, Khee Meng Koh, Eng Guan Tay, and Anders Yeo. *On the Number of Quasi-Kernels in Digraphs.* January 2001. 11 pp.

[RS-01-6] **Abstract**, *PostScript*, *PDF*, *DVI*.
Gregory Gutin, Anders Yeo, and Alexey Zverovich. *Traveling Salesman Should not be Greedy: Domination Analysis of Greedy-Type Heuristics for the TSP*. January 2001. 7 pp.

[RS-01-5] **Abstract**, *PostScript*, *PDF*.
Thomas S. Hune, Judi Romijn, Marille Stoelinga, and Frits W. Vaandrager. *Linear Parametric Model Checking of Timed Automata*. January 2001. 44 pp. Appears in Margaria and Yi, editors, *Tools and Algorithms for The Construction and Analysis of Systems: 7th International Conference*, TACAS '01 Proceedings, LNCS 2031, 2001, pages 174–188.

[RS-01-4] **Abstract**, *PostScript*, *PDF*.
Gerd Behrmann, Ansgar Fehnker, Thomas S. Hune, Kim G. Larsen, Paul Pettersson, and Judi Romijn. *Efficient Guiding Towards Cost-Optimality in* UPPAAL. January 2001. 21 pp. Appears in Margaria and Yi, editors, *Tools and Algorithms for The Construction and Analysis of Systems: 7th International Conference*, TACAS '01 Proceedings, LNCS 2031, 2001, pages 174–188.

[RS-01-3] **Abstract**, *PostScript*, *PDF*.
Gerd Behrmann, Ansgar Fehnker, Thomas S. Hune, Kim G. Larsen, Paul Pettersson, Judi Romijn, and Frits W. Vaandrager. *Minimum-Cost Reachability for Priced Timed Automata*. January 2001. 22 pp. Appears in Di Benedetto and Sangiovanni-Vincentelli, editors, *Hybrid Systems: Computation and Control, Fourth International Workshop*, HSCC '01 Proceedings, LNCS 2034, 2001, 147–161.

[RS-01-2] **Abstract**, *PostScript*, *PDF*, *DVI*.
Rasmus Pagh and Jakob Pagter. *Optimal Time-Space Trade-Offs for Non-Comparison-Based Sorting*. January 2001. ii+20 pp. Appears in Eppstein, editor, *The Thirteenths Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '02 Proceedings, 2002, pages 9–18.

[RS-01-1] **Abstract**, *PostScript*, *PDF*, *DVI*.
Gerth Stlting Brodal, Rolf Fagerberg, Christian N. S. Pedersen, and Anna stlin. *The Complexity of Constructing Evolutionary Trees Using Experiments*. January 2001. 28 pp. Appears in Orejas, Spirakis and Leeuwen, editors, *28th International Colloquium on Automata, Languages, and Programming*, ICALP '01 Proceedings, LNCS 2076, 2001, pages 140–151.