BRICS Research Series, 1998

August 5, 2003

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

References

[RS-98-55] **Abstract**, *PostScript*, *PDF*, *DVI*.
Andrew D. Gordon, Paul D. Hankin, and Sren B. Lassen. *Compilation and Equivalence of Imperative Objects (Revised Report)*. December 1998. iv+75 pp. This is a revision of Technical Report 429, University of Cambridge Computer Laboratory, June 1997, and the earlier BRICS report RS-97-19, July 1997. Appears in *Journal of Functional Programming*, 9(4):373-427, 1999, and Ramesh and Sivakumar, editors, *Foundations of Software Technology and Theoretical Computer Science: 17th Conference*, FST&TCS '97 Proceedings, LNCS 1346, 1997, pages 74–87.

[RS-98-54] Olivier Danvy and Ulrik P. Schultz. *Lambda-Dropping: Transforming Recursive Equations into Programs with Block Structure*. December 1998. 55 pp. This report is superseded by the later report BRICS RS-99-27.

[RS-98-53] **Abstract**, *PostScript*, *PDF*.
Julian C. Bradfield. *Fixpoint Alternation: Arithmetic, Transition Systems, and the Binary Tree*. December 1998. 20 pp. Appears in *Theoretical Informatics and Applications*, 33:341–356, 1999.

[RS-98-52] **Abstract**, *PostScript*, *PDF*, *DVI*.
Josva Kleist and Davide Sangiorgi. *Imperative Objects and Mobile Processes*. December 1998. 22 pp. Appears in Gries and de Roever, editors, *IFIP Working Conference on Programming Concepts and Methods*, PROCOMET '98 Proceedings, 1998, pages 285–303.

[RS-98-51] **Abstract**, *PostScript*, *PDF*.
Peter Krogsgaard Jensen. *Automated Modeling of Real-Time Implementation*. December 1998. 9 pp. Appears in *The 13th IEEE Conference on Automated Software Engineering*, ASE '98 Doctoral Symposium Proceedings, 1998, pages 17–20.

[RS-98-50] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto and Anna Inglfsdttir. *Testing Hennessy-Milner Logic with Recursion*. December 1998. 15 pp. Appears in Thomas,

editor, *Foundations of Software Science and Computation Structures: Second International Conference*, FoSSaCS '99 Proceedings, LNCS 1578, 1999, pages 41–55.

[RS-98-49] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Willem Jan Fokkink, and Anna Inglfsdttir. *A Cook's Tour of Equational Axiomatizations for Prefix Iteration*. December 1998. 14 pp. Appears in Nivat, editor, *Foundations of Software Science and Computation Structures: First International Conference*, FoSSaCS '98 Proceedings, LNCS 1378, 1998, pages 20–34.

[RS-98-48] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Patricia Bouyer, Augusto Burgueo, and Kim G. Larsen. *The Power of Reachability Testing for Timed Automata*. December 1998. 12 pp. Appears in Arvind and Ramanujam, editors, *Foundations of Software Technology and Theoretical Computer Science: 18th Conference*, FST&TCS '98 Proceedings, LNCS 1530, 1998, pages 245–256.

[RS-98-47] **Abstract**, *PostScript*, *PDF*.
Gerd Behrmann, Kim G. Larsen, Justin Pearson, Carsten Weise, and Wang Yi. *Efficient Timed Reachability Analysis using Clock Difference Diagrams*. December 1998. 13 pp. Appears in Halbwachs and Peled, editors, *Computer-Aided Verification: 11th International Conference*, CAV '99 Proceedings, LNCS 1633, 1999, pages 341–353.

[RS-98-46] **Abstract**, *PostScript*, *PDF*.
Kim G. Larsen, Carsten Weise, Wang Yi, and Justin Pearson. *Clock Difference Diagrams*. December 1998. 18 pp. Presented at *10th Nordic Workshop on Programming Theory*, NWPT '10 Abstracts, Turku Centre for Computer Science TUCS General Publications 11, 1998. Appears in *Nordic Journal of Computing*, 6(3):271–298, 1999.

[RS-98-45] **Abstract**, *PostScript*, *PDF*.
Morten Vadskr Jensen and Brian Nielsen. *Real-Time Layered Video Compression using SIMD Computation*. December 1998. 37 pp. Appears in Zinterhof, Vajtersic and Uhl, editors, *Parallel Computing: Fourth International ACPC Conference*, ACPC '99 Proceedings, LNCS 1557, 1999, pages 377–387.

[RS-98-44] **Abstract**, *PostScript*, *PDF*.
Brian Nielsen and Gul Agha. *Towards Re-usable Real-Time Objects*. December 1998. 36 pp. Appears in *The Annals of Software Engineering*, 7:257–282, 1999.

[RS-98-43] **Abstract**, *PostScript*, *PDF*, *DVI*.
Peter D. Mosses. *CASL: A Guided Tour of its Design*. December 1998. 31 pp. Appears in Fiadeiro, editor, *Recent Trends in Algebraic Development Techniques: 13th Workshop*, WADT '98 Selected Papers, LNCS 1589, 1999, pages 216–240.

[RS-98-42] **Abstract**, *PostScript*, *PDF*, *DVI*.
Peter D. Mosses. *Semantics, Modularity, and Rewriting Logic*. December 1998. 20 pp. Appears in Kirchner and Kirchner, editors, *International Workshop on Rewriting Logic and its Applications*, WRLA '98 Proceedings, ENTCS 15, 1998.

[RS-98-41] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *The Computational Strength of Extensions of Weak Knig's Lemma*. December 1998. 23 pp.

[RS-98-40] **Abstract**, *PostScript*, *PDF*, *DVI*.
Henrik Reif Andersen, Colin Stirling, and Glynn Winskel. *A Compositional Proof System for the Modal μ-Calculus*. December 1998. 29 pp. Extended abstract appears in *Ninth Annual IEEE Symposium on Logic in Computer Science*, LICS '94 Proceedings, 1994, pages 144–153. Superseeds the earlier BRICS Report RS-94-34.

[RS-98-39] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Fridlender. *An Interpretation of the Fan Theorem in Type Theory*. December 1998. 15 pp. Appears in Altenkirch, Naraschewski and Reus, editors, *International Workshop on Types for Proofs and Programs 1998*, TYPES '98 Selected Papers, LNCS 1657, 1999, pages 93–105.

[RS-98-38] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Fridlender and Mia Indrika. *An n-ary* `zipWith` *in Haskell*. December 1998. 12 pp.

[RS-98-37] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd, Joe Kilian, and Louis Salvail. *On the (Im)possibility of Basing Oblivious Transfer and Bit Commitment on Weakened Security Assumptions*. December 1998. 22 pp. Appears in Stern, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '99 Proceedings, LNCS 1592, 1999, pages 56–73.

[RS-98-36] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ronald Cramer, Ivan B. Damgrd, Stefan Dziembowski, Martin Hirt, and Tal Rabin. *Efficient Multiparty Computations with Dishonest Minority*. December 1998. 19 pp. Appears in Stern, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '99 Proceedings, LNCS 1592, 1999, pages 311–326.

[RS-98-35] **Abstract**.
Olivier Danvy and Zhe Yang. *An Operational Investigation of the CPS Hierarchy*. December 1998. Extended version of a paper appearing in Swierstra, editor, *Programming Languages and Systems: Eighth European Symposium on Programming*, ESOP '99 Proceedings, LNCS 1576, 1999, pages 224–242.

[RS-98-34] **Abstract**, *PostScript*, *PDF*, *DVI*.
Peter G. Binderup, Gudmund Skovbjerg Frandsen, Peter Bro Miltersen, and Sven Skyum. *The Complexity of Identifying Large Equivalence Classes*. December 1998. Appears in *Fundamenta Informaticae*, 38:17–29.

[RS-98-33] **Abstract**, *PostScript*, *PDF*, *DVI*.
Hans Httel, Josva Kleist, Uwe Nestmann, and Massimo Merro. *Migration = Cloning ; Aliasing (Preliminary Version)*. December 1998. 40 pp. Appears in Cardelli, editor, *Foundations of Object-Oriented Languages: 6th International Conference*, FOOL6 Informal Proceedings, 1999.

[RS-98-32] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jan Camenisch and Ivan B. Damgrd. *Verifiable Encryption and Applications to Group Signatures and Signature Sharing*. December 1998. 18 pp. Appears in Okamoto, editor, *Advances in Cryptology: Sixth ASIACRYPT Conference on the Theory and Applications of Cryptologic Techniques*, ASIACRYPT '00 Proceedings, LNCS 1976, 2000, pages 331–345.

[RS-98-31] **Abstract**, *PostScript*, *PDF*, *DVI*.
Glynn Winskel. *A Linear Metalanguage for Concurrency*. November 1998. 21 pp. Appears in Haeberer, editor, *Algebraic Methodology and Software Technology: 7th International Conference*, AMAST '98 Proceedings, LNCS 1548, 1999, pages 42–58.

[RS-98-30] **Abstract**, *PostScript*, *PDF*, *DVI*.
Carsten Butz. *Finitely Presented Heyting Algebras*. November 1998. 30 pp.

[RS-98-29] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jan Camenisch and Markus Michels. *Proving in Zero-Knowledge that a Number is the Product of Two Safe Primes*. November 1998. 19 pp. Appears in Stern, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '99 Proceedings, LNCS 1592, 1999, pages 106–121.

[RS-98-28] **Abstract**, *PostScript*, *PDF*.
Rasmus Pagh. *Low Redundancy in Dictionaries with $O(1)$ Worst Case Lookup Time*. November 1998. 15 pp. Journal version in *SIAM Journal on Computing* 31:353–363, 2001, and proceedings version in van Emde Boas, Wiedermann and Nielsen, editors, *26th International Colloquium on Automata, Languages, and Programming*, ICALP '99 Proceedings, LNCS 1644, 1999, pages 595–604.

[RS-98-27] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jan Camenisch and Markus Michels. *A Group Signature Scheme Based on an RSA-Variant*. November 1998. 18 pp. Preliminary version appeared in Ohta and Pei, editors, *Advances in Cryptology: Fourth ASIACRYPT Conference on the Theory and Applications of*

Cryptologic Techniques, ASIACRYPT '98 Proceedings, LNCS 1514, 1998, pages 160–174.

[RS-98-26] **Abstract**, *PostScript*, *PDF*, *DVI*.
Paola Quaglia and David Walker. *On Encoding $p\pi$ in $m\pi$*. October 1998. 27 pp. Full version of paper appearing in Arvind and Ramanujam, editors, *Foundations of Software Technology and Theoretical Computer Science: 18th Conference*, FST&TCS '98 Proceedings, LNCS 1530, 1998, pages 42–53.

[RS-98-25] **Abstract**, *PostScript*, *PDF*, *DVI*.
Devdatt P. Dubhashi. *Talagrand's Inequality in Hereditary Settings*. October 1998. 22 pp.

[RS-98-24] **Abstract**, *PostScript*, *PDF*, *DVI*.
Devdatt P. Dubhashi. *Talagrand's Inequality and Locality in Distributed Computing*. October 1998. 14 pp Appears in Luby, Rolim and Serna, editors, *Randomization and Approximation Techniques in Computer Science: Second International Workshop: Second International Workshop*, RANDOM '98 Proceedings, LNCS 1518, 1998, pages 60–70.

[RS-98-23] **Abstract**, *PostScript*, *PDF*, *DVI*.
Devdatt P. Dubhashi. *Martingales and Locality in Distributed Computing*. October 1998. 19 pp. Appears in Arvind and Ramanujam, editors, *Foundations of Software Technology and Theoretical Computer Science: 18th Conference*, FST&TCS '98 Proceedings, LNCS 1530, 1998, pages 174–185.

[RS-98-22] **Abstract**, *PostScript*, *PDF*, *DVI*.
Gian Luca Cattani, John Power, and Glynn Winskel. *A Categorical Axiomatics for Bisimulation*. September 1998. ii+21 pp. Appears in Sangiorgi and de Simone, editors, *Concurrency Theory: 9th International Conference*, CONCUR '98 Proceedings, LNCS 1466, 1998, pages 581–596.

[RS-98-21] **Abstract**, *PostScript*, *PDF*, *DVI*.
John Power, Gian Luca Cattani, and Glynn Winskel. *A Representation Result for Free Cocompletions*. September 1998. 16 pp. Appears in *Journal of Pure and Applied Algebra*, 151(3):273–286 (2000).

[RS-98-20] **Abstract**, *PostScript*, *PDF*, *DVI*.
Sren Riis and Meera Sitharam. *Uniformly Generated Submodules of Permutation Modules*. September 1998. 35 pp. Appears in *Annals of Pure and Applied Algebra*, 160(3):285–318, 2001.

[RS-98-19] **Abstract**, *PostScript*, *PDF*, *DVI*.
Sren Riis and Meera Sitharam. *Generating Hard Tautologies Using Predicate Logic and the Symmetric Group*. September 1998. 13 pp. Abstract appears in *Logic Journal of IGPL*, a special section devoted *the 5th Workshop on Logic, Language, Information and Computation*, WoLLIC '98 (So Paulo, Brazil, July 28–31, 1998), pages 936–937. Full version appears in *Logic Journal of the IGPL*, 8(6):787–795, 2000.

[RS-98-18] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *Things that can and things that can't be done in PRA*. September 1998. 24 pp. Appeared in *Annals of Pure and Applied Logic*, 102(3):223-245, 2000.

[RS-98-17] **Abstract**, *PostScript*, *PDF*, *DVI*.
Roberto Bruni, Jos Meseguer, Ugo Montanari, and Vladimiro Sassone. *A Comparison of Petri Net Semantics under the Collective Token Philosophy*. September 1998. 20 pp. Appears in Hsiang and Ohori, editors, *Fourth Asian Computing Science Conference*, ASIAN '98 Proceedings, LNCS 1538, 1998, pages 225–244.

[RS-98-16] Stephen Alstrup, Thore Husfeldt, and Theis Rauhe. *Marked Ancestor Problems*. September 1998. Extended abstract appears in Motwani, editor, *39th Annual Symposium on Foundations of Computer Science*, FOCS '98 Proceedings, 1998, pages 534–543.

[RS-98-15] **Abstract**, *PostScript*, *PDF*.
Jung-taek Kim, Kwangkeun Yi, and Olivier Danvy. *Assessing the Overhead of ML Exceptions by Selective CPS Transformation*. September 1998. 31 pp. Appears in the proceedings of the *1998 ACM SIGPLAN Workshop on ML*, Baltimore, Maryland, September 26, 1998, pages 103–114.

[RS-98-14] **Abstract**, *PostScript*, *PDF*, *DVI*.
Sandeep Sen. *The Hardness of Speeding-up Knapsack*. August 1998. 6 pp.

[RS-98-13] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Morten Rhiger. *Compiling Actions by Partial Evaluation, Revisited*. June 1998. 25 pp. Earlier version appears in Vain, editor, *9th Nordic Workshop on Programming Theory*, NWPT '9 Proceedings, Estonian Academy of Sciences Series, 1997.

[RS-98-12] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy. *Functional Unparsing*. May 1998. 7 pp. This report supersedes the earlier report BRICS RS-98-5. Extended version of an article appearing in *Journal of Functional Programming*, 8(6):621–625, 1998.

[RS-98-11] **Abstract**, *PostScript*, *PDF*, *DVI*.
Gudmund Skovbjerg Frandsen, Johan P. Hansen, and Peter Bro Miltersen. *Lower Bounds for Dynamic Algebraic Problems*. May 1998. 30 pp. Revised versions appears in Meinel and Tison, editors, *16th Annual Symposium on Theoretical Aspects of Computer Science Proceedings*, STACS '99 Proceedings, LNCS 1563, 1999, pages 362–372, and in *Information and Computation*, 171:333–349, 2001.

[RS-98-10] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jakob Pagter and Theis Rauhe. *Optimal Time-Space Trade-Offs for Sorting*. May 1998. 12 pp. Appears in Motwani, editor, *39th*

Annual Symposium on Foundations of Computer Science, FOCS '98 Proceedings, 1998, pages 264–268.

[RS-98-9] **Abstract**, *PostScript*, *PDF*.
Zhe Yang. *Encoding Types in ML-like Languages (Preliminary Version)*. April 1998. 32 pp. Extended version of a paper appearing in Hudak and Queinnec, editors, *Proceedings of the third ACM SIGPLAN International Conference on Functional Programming*, 1998, pages 289–300.

[RS-98-8] **Abstract**, *PostScript*, *PDF*, *DVI*.
P. S. Thiagarajan and Jesper G. Henriksen. *Distributed Versions of Linear Time Temporal Logic: A Trace Perspective*. April 1998. 49 pp. Appears as a chapter of Reisig and Rozenberg, editors, *Lectures on Petri Nets I: Basic Models*, LNCS 1491, 1998, pages 643–681.

[RS-98-7] **Abstract**, *PostScript*, *PDF*, *DVI*.
Stephen Alstrup, Thore Husfeldt, and Theis Rauhe. *Marked Ancestor Problems (Preliminary Version)*. April 1998. 36 pp. Superseeded by RS-98-16. Extended abstract in Motwani, editor, *39th Annual Symposium on Foundations of Computer Science*, FOCS '98 Proceedings, 1998, pages 534–543.

[RS-98-6] **Abstract**, *PostScript*, *PDF*, *DVI*.
Kim Sunesen. *Further Results on Partial Order Equivalences on Infinite Systems*. March 1998. 48 pp.

[RS-98-5] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy. *Formatting Strings in ML*. March 1998. 3 pp. This report is superseded by the later report BRICS RS-98-12.

[RS-98-4] **Abstract**, *PostScript*, *PDF*.
Mogens Nielsen and Thomas S. Hune. *Timed Bisimulation and Open Maps*. February 1998. 27 pp. Appears in Brim, Gruska and Zlatuška, editors, *Mathematical Foundations of Computer Science: 23rd International Symposium*, MFCS '98 Proceedings, LNCS 1450, 1998, pages 378–387.

[RS-98-3] **Abstract**, *PostScript*, *PDF*, *DVI*.
Christian N. S. Pedersen, Rune B. Lyngs, and Jotun Hein. *Comparison of Coding DNA*. January 1998. 20 pp. Appears in Farach-Colton, editor, *Combinatorial Pattern Matching: 9th Annual Symposium*, CPM '98 Proceedings, LNCS 1448, 1998, pages 153–173.

[RS-98-2] Olivier Danvy. *An Extensional Characterization of Lambda-Lifting and Lambda-Dropping*. January 1998. This report is superseded by the later report BRICS RS-99-21.

[RS-98-1] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy. *A Simple Solution to Type Specialization*. January 1998. 10 pp. Appears in Larsen, Skyum and Winskel, editors, *25th International Colloquium on Automata, Languages, and Programming*, ICALP '98 Proceedings, LNCS 1443, 1998, pages 908–917.