BRICS Research Series, 2000

August 7, 2003

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

References

[RS-00-52] **Abstract**, *PostScript*, *PDF*, *DVI*.
Claude Crpeau, Frdric Lgar, and Louis Salvail. *How to Convert a Flavor of Quantum Bit Commitment*. December 2000. 24 pp. Appears in Pfitzmann, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '01 Proceedings, LNCS 2045, 2001, pages 60–77.

[RS-00-51] **Abstract**, *PostScript*, *PDF*, *DVI*.
Peter D. Mosses. *CASL for CafeOBJ Users*. December 2000. 25 pp. Appears in Futatsugi, Nakagawa and Tamai, editors, *CAFE: An Industrial-Strength Algebraic Formal Method*, 2000, chapter 6, pages 121–144.

[RS-00-50] **Abstract**, *PostScript*, *PDF*, *DVI*.
Peter D. Mosses. *Modularity in Meta-Languages*. December 2000. 19 pp. Appears in Despeyroux, editor, *2nd Workshop on Logical Frameworks and Meta-Languages*, LFM '00 Proceedings, 2000, pages 1–18.

[RS-00-49] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *Higher Order Reverse Mathematics*. December 2000. 18 pp. To appear in S. G. Simpson (ed.), *Reverse Mathematics*.

[RS-00-48] **Abstract**, *PostScript*, *PDF*, *DVI*.
Marcin Jurdziński and Jens Vge. *A Discrete Stratety Improvement Algorithm for Solving Parity Games*. December 2000. 31 pp. Extended abstract appears in Emerson and Sistla, editors, *Computer-Aided Verification: 12th International Conference*, CAV '00 Proceedings, LNCS 1855, 2000, pages 202–215.

[RS-00-47] **Abstract**, *PostScript*, *PDF*, *DVI*.
Lasse R. Nielsen. *A Denotational Investigation of Defunctionalization*. December 2000. 50 pp. Presented at *16th Workshop on the Mathematical Foundations of Programming Semantics*, MFPS '00 (Hoboken, New Jersey, USA, April 13–16, 2000).

[RS-00-46] Zhe Yang. *Reasoning About Code-Generation in Two-Level Languages*. December 2000.

[RS-00-45] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Mads J. Jurik. *A Generalisation, a Simplification and some Applications of Paillier's Probabilistic Public-Key System*. December 2000. 18 pp. Appears in Kim, editor, *Fourth International Workshop on Practice and Theory in Public Key Cryptography*, PKC '01 Proceedings, LNCS 1992, 2001, pages 119–136. This revised and extended report supersedes the earlier BRICS report RS-00-5.

[RS-00-44] **Abstract**, *PostScript*, *PDF*, *DVI*.
Bernd Grobauer and Zhe Yang. *The Second Futamura Projection for Type-Directed Partial Evaluation*. December 2000. Appears in *Higher-Order and Symbolic Computation* 14(2–3):173–219 (2001). This revised and extended report supersedes the earlier BRICS report RS-99-40 which in turn was an extended version of Lawall, editor, *ACM SIGPLAN Workshop on Partial Evaluation and Semantics-Based Program Manipulation*, PEPM '00 Proceedings, 2000, pages 22–32.

[RS-00-43] **Abstract**, *PostScript*, *PDF*.
Claus Brabrand, Anders Mller, Mikkel Ricky Christensen, and Michael I. Schwartzbach. *PowerForms: Declarative Client-Side Form Field Validation*. December 2000. 21 pp. Appears in *World Wide Web Journal*, 4(3), 2000.

[RS-00-42] **Abstract**, *PostScript*, *PDF*.
Claus Brabrand, Anders Mller, and Michael I. Schwartzbach. *The* `<bigwig>` *Project*. December 2000. 25 pp. To appear in ACM Transactions on Internet Technology, 2002.

[RS-00-41] **Abstract**, *PostScript*, *PDF*, *DVI*.
Nils Klarlund, Anders Mller, and Michael I. Schwartzbach. *The DSD Schema Language and its Applications*. December 2000. 32 pp. Appears in *Automated Software Engineering*, 9(3):285–319,2002. Shorter version appears in Heimdahl, editor, *3rd ACM SIGSOFT Workshop on on Formal Methods in Software Practice*, FMSP '00 Proceedings, 2000 , pages 101–111.

[RS-00-40] **Abstract**, *PostScript*, *PDF*.
Nils Klarlund, Anders Mller, and Michael I. Schwartzbach. *MONA Implementation Secrets*. December 2000. 19 pp. Appears in *International Journal of Foundations of Computer Science*, 13(4):571–586, 2002. Shorter version appears in Yu and Păum, editors, *Fifth International Conference on Implementation and Application of Automata*, CIAA '00 Pre-Proceedings, LNCS 2088, 2001, pages 182–194.

[RS-00-39] **Abstract**, *PostScript*, *PDF*.
Anders Mller and Michael I. Schwartzbach. *The Pointer Assertion*

Logic Engine. December 2000. 23 pp. Appears in *ACM SIGPLAN Conference on Programming Language Design and Implementation*, PLDI '01 Proceedings, 2001 pp. 221–231.

[RS-00-38] **Abstract**, *PostScript*, *PDF*.
Bertrand Jeannet. *Dynamic Partitioning in Linear Relation Analysis: Application to the Verification of Synchronous Programs*. December 2000. 44 pp.

[RS-00-37] **Abstract**, *PostScript*, *PDF*.
Thomas S. Hune, Kim G. Larsen, and Paul Pettersson. *Guided Synthesis of Control Programs for a Batch Plant using* UPPAAL. December 2000. 29 pp. Appears in Lai, editor, *International Workshop in Distributed Systems Validation and Verification. Held in conjunction with 20th IEEE International Conference on Distributed Computing Systems (ICDCS '2000)*, DSVV '00 Proceedings, 2000, pages E15–E22 and *Nordic Journal of Computing*, 8(1):43–64, 2001.

[RS-00-36] **Abstract**, *PostScript*, *PDF*, *DVI*.
Rasmus Pagh. *Dispersing Hash Functions*. December 2000. 18 pp. Preliminary version appeared in Rolim, editor, *4th International Workshop on Randomization and Approximation Techniques in Computer Science*, RANDOM '00, Proceedings in Informatics, 2000, pages 53–67.

[RS-00-35] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Lasse R. Nielsen. *CPS Transformation of Beta-Redexes*. December 2000. 12 pp. Appears in Sabry, editor, *3rd ACM SIGPLAN Workshop on Continuations*, CW '01 Proceedings, Association for Computing Machinery (ACM) SIGPLAN Technical Report 545, 2001, pages 35–39.

[RS-00-34] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Morten Rhiger. *A Simple Take on Typed Abstract Syntax in Haskell-like Languages*. December 2000. 25 pp. Appears in Kuchen and Ueda, editors, *Fifth International Symposium on Functional and Logic Programming*, FLOPS '01 Proceedings, LNCS 2024, 2001, pages 343–358.

[RS-00-33] **Abstract**, *PostScript*, *PDF*, *DVI*.
Olivier Danvy and Lasse R. Nielsen. *A Higher-Order Colon Translation*. December 2000. 17 pp. Appears in Kuchen and Ueda, editors, *Fifth International Symposium on Functional and Logic Programming*, FLOPS '01 Proceedings, LNCS 2024, 2001, pages 78–91.

[RS-00-32] **Abstract**, *PostScript*, *PDF*, *DVI*.
John C. Reynolds. *The Meaning of Types — From Intrinsic to Extrinsic Semantics*. December 2000. 35 pp. A shorter version of this report describing a more limited language appears in Annabelle McIver and Carroll Morgan (eds.) *Essays on Programming Methodology*, Springer-Verlag, New York, 2001.

[RS-00-31] **Abstract**, *PostScript*, *PDF*.
Bernd Grobauer and Julia L. Lawall. *Partial Evaluation of Pattern Matching in Strings, revisited*. November 2000. 48 pp. Appears in *Nordic Journal of Computing*, 8(4):437–462, 2001.

[RS-00-30] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Maciej Koprowski. *Practical Threshold RSA Signatures Without a Trusted Dealer*. November 2000. 14 pp. Appears in Pfitzmann, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '01 Proceedings, LNCS 2045, 2001, pages 152–165.

[RS-00-29] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luigi Santocanale. *The Alternation Hierarchy for the Theory of μ-lattices*. November 2000. 44 pp. Extended abstract appears in *Abstracts from the International Summer Conference in Category Theory*, CT2000, Como, Italy, July 16–22, 2000. Appears in *Theory and Applications of Categories*, 9:166–197, 2002.

[RS-00-28] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luigi Santocanale. *Free μ-lattices*. November 2000. 51 pp. Short abstract appeared in *Proceedings of Category Theory 99*, Coimbra, Portugal, July 19–24, 1999. Full version appears in the Journal of Pure and Applied Algebra, 168/2-3, pp. 227-264.

[RS-00-27] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik and Werner Kuich. *Inductive *-Semirings*. October 2000. 34 pp. To appear in *Theoretical Computer Science*.

[RS-00-26] **Abstract**, *PostScript*, *PDF*.
František Čapkovič. *Modelling and Control of Discrete Event Dynamic Systems*. October 2000. 58 pp.

[RS-00-25] **Abstract**, *PostScript*, *PDF*, *DVI*.
Zoltn sik. *Continuous Additive Algebras and Injective Simulations of Synchronization Trees*. September 2000. 41 pp. Appears in *Journal of Logic and Computation*, 12(2):271–300, 2002.

[RS-00-24] **Abstract**, *PostScript*, *PDF*.
Claus Brabrand and Michael I. Schwartzbach. *Growing Languages with Metamorphic Syntax Macros*. September 2000. 22 pp. Appears in Thiemann, editor, *ACM SIGPLAN Workshop on Partial Evaluation and Semantics-Based Program Manipulation*, PEPM '02 Proceedings, 2002, pages 31–40.

[RS-00-23] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Anna Inglfsdttir, Mikkel Lykke Pedersen, and Jan Poulsen. *Characteristic Formulae for Timed Automata*. September 2000. 23 pp. Appears in *RAIRO, Theoretical Informatics and Applications* 34(6), pp. 565–584.

[RS-00-22] **Abstract**, *PostScript*, *PDF*.
Thomas S. Hune and Anders B. Sandholm. *Using Automata in Control Synthesis — A Case Study*. September 2000. 20 pp. Appears in Maibaum, editor, *Fundamental Approaches to Software Engineering: Third International Conference*, FASE '00 Proceedings, LNCS 1783, 2000, pages 349–362.

[RS-00-21] **Abstract**, *PostScript*, *PDF*.
M. Oliver Mller and Rajeev Alur. *Heuristics for Hierarchical Partitioning with Application to Model Checking*. August 2000. 30 pp. A shorter version appears in Margaria and Melham, editors, *Correct Hardware Design and Verification Methods, 11th IFIP WG 10.5 Advanced Research Working Conference*, CHARME '01 Proceedings, LNCS 2144, 2001, pages 71–85.

[RS-00-20] **Abstract**, *PostScript*, *PDF*, *DVI*.
Luca Aceto, Willem Jan Fokkink, and Anna Inglfsdttir. *2-Nested Simulation is not Finitely Equationally Axiomatizable*. August 2000. 13 pp. Appears in Ferreira and Reichel, editors, *18th Annual Symposium on Theoretical Aspects of Computer Science*, STACS '01 Proceedings, LNCS 2010, 2001, pages 39–50.

[RS-00-19] **Abstract**, *PostScript*, *PDF*, *DVI*.
Vinodchandran N. Variyam. *A Note on* $\mathbf{NP} \cap \mathbf{coNP}$/poly. August 2000. 7 pp.

[RS-00-18] **Abstract**, *PostScript*, *PDF*, *DVI*.
Federico Crazzolara and Glynn Winskel. *Language, Semantics, and Methods for Cryptographic Protocols*. August 2000. ii+42 pp.

[RS-00-17] **Abstract**, *PostScript*, *PDF*.
Thomas S. Hune. *Modeling a Language for Embedded Systems in Timed Automata*. August 2000. 26 pp. Earlier version entitled *Modelling a Real-Time Language* appeared in Gnesi and Latella, editors, *Fourth International ERCIM Workshop on Formal Methods for Industrial Critical Systems*, FMICS '99 Proceedings of the FLoC Workshop, 1999, pages 259–282.

[RS-00-16] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jiř Srba. *Complexity of Weak Bisimilarity and Regularity for BPA and BPP*. June 2000. 20 pp. To appear in Aceto and Victor, editors, *Expressiveness in Concurrency: 7th International Workshop*, EXPRESS '00 Proceedings, ENTCS 39(1), 2000.

[RS-00-15] **Abstract**, *PostScript*, *PDF*, *DVI*.
Daniel Damian and Olivier Danvy. *Syntactic Accidents in Program Analysis: On the Impact of the CPS Transformation*. June 2000. 26 pp. Extended version of an article appearing in Wadler, editor, *Proceedings of the fifth ACM SIGPLAN International Conference on Functional Programming*, 2000, pages 209–220. To appear in *Journal of Functional Programming*.

[RS-00-14] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ronald Cramer, Ivan B. Damgrd, and Jesper Buus Nielsen. *Multiparty Computation from Threshold Homomorphic Encryption*. June 2000. ii+38 pp. Appears in Pfitzmann, editor, *Advances in Cryptology: International Conference on the Theory and Application of Cryptographic Techniques*, EUROCRYPT '01 Proceedings, LNCS 2045, 2001, pages 280–300.

[RS-00-13] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ondřej Klma and Jiř Srba. *Matching Modulo Associativity and Idempotency is NP-Complete*. June 2000. 19 pp. Appeared in Nielsen and Rovan, editors, *Mathematical Foundations of Computer Science: 25th International Symposium*, MFCS '00 Proceedings, LNCS 1893, 2000, pages 456–466.

[RS-00-12] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *Intuitionistic Choice and Restricted Classical Logic*. May 2000. 9 pp. Appears in *Mathematical Logic Quaterly* vol 47, pp. 455-460, 2001,.

[RS-00-11] **Abstract**, *PostScript*, *PDF*, *DVI*.
Jakob Pagter. *On Ajtai's Lower Bound Technique for R-way Branching Programs and the Hamming Distance Problem*. May 2000. 18 pp.

[RS-00-10] **Abstract**, *PostScript*, *PDF*.
Stefan Dantchev and Sren Riis. *A Tough Nut for Tree Resolution*. May 2000. 13 pp.

[RS-00-9] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ulrich Kohlenbach. *Effective Uniform Bounds on the Krasnoselski-Mann Iteration*. May 2000. 34 pp. The material of this report appeared as two publications: 1) A Quantitative version of a theorem due to Borwein-Reich-Shafrir, Numer.Funct. Aanal.Optimiz. 22, pp. 641-656 (2001), 2) On the computational content of the Krasnoselski and Ishikawa fixed point theorems. In Blanck (et.al.) eds., CCA 2000, LNCS 2064, pp. 119-145 (2001).

[RS-00-8] **Abstract**, *PostScript*, *PDF*, *DVI*.
Nabil H. Mustafa and Aleksandar Pekeč. *Democratic Consensus and the Local Majority Rule*. May 2000. 38 pp.

[RS-00-7] **Abstract**.
Lars Arge and Jakob Pagter. *I/O-Space Trade-Offs*. April 2000. Appears in Halldrsson, editor, *7th Scandinavian Workshop on Algorithm Theory*, SWAT '98 Proceedings, LNCS 1851, 2000, pages 448–461.

[RS-00-6] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Jesper Buus Nielsen. *Improved Non-Committing Encryption Schemes based on a General Complexity Assumption*. March 2000. 24 pp. Appears in Bellare, editor, *Advances*

in Cryptology: 20th Annual International Cryptology Conference, CRYPTO '00 Proceedings, LNCS 1880, 2000, pages 433–451.

[RS-00-5] **Abstract**, *PostScript*, *PDF*, *DVI*.
Ivan B. Damgrd and Mads J. Jurik. *Efficient Protocols based on Probabilistic Encryption using Composite Degree Residue Classes*. March 2000. 19 pp.

[RS-00-4] **Abstract**, *PostScript*, *PDF*.
Rasmus Pagh. *A New Trade-off for Deterministic Dictionaries*. February 2000. Appears in Halldrsson, editor, *7th Scandinavian Workshop on Algorithm Theory*, SWAT '98 Proceedings, LNCS 1851, 2000, pages 22–31. Journal version in *Nordic Journal of Computing* 7(3):151–163, 2000 with the title *A Trade-Off for Worst-Case Efficient Dictionaries*.

[RS-00-3] **Abstract**, *PostScript*, *PDF*, *DVI*.
Fredrik Larsson, Paul Pettersson, and Wang Yi. *On Memory-Block Traversal Problems in Model Checking Timed Systems*. January 2000. 15 pp. Appears in Graf and Schwartzbach, editors, *Tools and Algorithms for The Construction and Analysis of Systems: 6th International Conference*, TACAS '00 Proceedings, LNCS 1785, 2000, pages 127–141.

[RS-00-2] **Abstract**, *PostScript*, *PDF*.
Igor Walukiewicz. *Local Logics for Traces*. January 2000. 30 pp. To appear in *Journal of Automata, Languages and Combinatorics*.

[RS-00-1] **Abstract**, *PostScript*, *PDF*, *DVI*.
Rune B. Lyngs and Christian N. S. Pedersen. *Pseudoknots in RNA Secondary Structures*. January 2000. 15 pp. Appears in Shamir, editor, *Fourth Annual International Conference on Computational Molecular Biology*, RECOMB '00 Proceedings, 2000, 201–209 and in *Journal of Computational Biology*, 7(3/4):409–427, 2000.