Alexander A. Razborov

Personal data

Born on Feb 16, 1963 in the town Belovo, USSR.

Education

- 1985-87: graduate student at the Steklov Mathematical Institute, Moscow. Advisor: Prof. S.I.Adian.
- 1980-85: undergraduate student of the Moscow University, Department of Mechanics and Mathematics.

Degrees

- 1991: doctoral thesis, Lower bounds in the Boolean Complexity.
- 1987: PhD, On systems of equations in free groups.

Employment

- 2008-current: Andrew MacLeish Distinguished Service Professor, University of Chicago.
- 2000-2008: Principal Researcher, Steklov Mathematical Institute.
- 1991-2000: Leading Researcher, Steklov Mathematical Institute.
- 1987-1991: Researcher, Steklov Mathematical Institute.

Part-time positions

- 2008-current: Principal Researcher, Steklov Mathematical Institute.
- 2008-current: Resident Adjoint Professor, Toyota Technological Institute at Chicago.

Visiting positions

• 2003-2008: Visiting Professor, Institute for Advanced Study, Princeton

- 2000-2003: Member, Institute for Advanced Study, Princeton
- 1999-2000: Visiting Researcher, Department of Computer Science, Princeton University
- 1993-1994: Member, Institute for Advanced Study, Princeton

Honors

- 2013: David P. Robbins Prize of the American Mathematical Society.
- 2007: Göedel Prize of the European Association for Theoretical Computer Science and the Special Interest Group on Algorithms and Computation Theory of the Association for Computing Machinery.
- 1990: Rolf Nevanlinna Prize of the International Mathematical Union.

Membership

- 2020: American Academy of Arts and Sciences
- 2000: corresponding member of the Russian Academy of Science
- 1993: Academia Europea

Editorial Boards

- Forum of Mathematics (Π and Σ).
- Sbornik: Mathematics
- Combinatorica.
- Computational Complexity.
- Combinatorics, Probability and Computing.
- Moscow Journal of Combinatorics and Number Theory
- Lobachevskii Journal of Mathematics

Steering Committee

• Computer Science Symposium in Russia, 2012-current

Program Committees

- Computational Complexity Conference 2021
- International Conference "Computer Science Symposium in Russia" 2021
- Oberwolfach workshop "Proof Complexity and Beyond" 2017
- Innovations in Theoretical Computer Science Conference 2017
- Association for Symbolic Logic North American Annual Meeting 2015
- International Conference "Computer Science Symposium in Russia" 2015
- International Conference "Computer Science Symposium in Russia" 2014
- International Colloquium on Automata, Languages and Programming 2013
- International Conference "Computer Science Symposium in Russia" 2013
- International Conference "Computer Science Symposium in Russia" 2012
- International Conference "Computer Science Symposium in Russia" 2011
- IEEE Conference on Computational Complexity 2009
- International Conference on Logic for Programming, Artificial intelligence, and Reasoning 2008
- International Conference "Computer Science Symposium in Russia" 2008 chair of Theory Track

- Symposium on Foundations of Computer Science 2007
- International Conference "Computer Science Symposium in Russia" 2007
- Workshop on Logic, Language, Information and Computation 2007
- 13th International Congress of Logic, Methodology and Philosophy of Science 2007
- International Conference "Computer Science Symposium in Russia" 2006
- 2nd International Conference "Methods of logic in mathematics" 2005
- International Conference Dedicated to the 100th Anniversary of P.S.Novikov 2001
- Workshop on Circuit and Proof Complexity 2001
- Workshop on Complexity of Proofs and Computations 2000
- Logic Colloquium 2000
- Computational Complexity 2000
- Computer Science Logic 1998
- Workshop on Complexity Theory 1997
- Random97 conference
- Computer Science Logic 1994

Current students

- L. Coregliano
- S. Pang
- T. Papamakarios
- D. Quintana

Former students

- A. Nogin.
- O. Verbitsky (jointly with S. I. Adian).
- M. Alekhnovich (undergraduate)
- V. Podolski (undergraduate)
- R. Kulkarni (jointly with J. Simon)
- Y. Li
- P. Hatami

Plenary and invited talks

- 8th European Congress of Mathematicians, Portoroz, 2020 (re-scheduled for 2021)
- 14th Latin American Theoretical Informatics Symposium, Sao Paolo, 2020 (January 2021, online), *Theons and Quasirandomness*
- Association for Symbolic Logic North American Annual Meeting, Irvine, 2020 (cancelled)
- Workshop on Proof Complexity, Banff, Canada, 2020, *Hardness Con*densation
- Steklov International Mathematical Center, inaugural conference, Moscow, 2019, *Limits of Combinatorial Objects*
- Symposium on 50 Years of Complexity theory in Honor of Stephen Cook, Toronto, 2019, *P*, *NP* and *Proof Complexity*
- ICERM workshop on Real Algebraic Geometry and Optimization, Providence, 2018, *The Tale of One Variety (And Its Family)*.
- Clay Institute workshop on Complexity Theory, Oxford, 2018, Grand Challenges in Complexity Theory through the Lens of Proof Theory

- Building Bridges II Conference, Budapest, 2018, Semantic Limits of Combinatorial Objects
- VIII RASA-USA conference, Chicago, 2017, Solving Satisfiability
- Avi is 60 Conference, Princeton, 2016, Propositional Proof Complexity: Fifteen (or so) Years After
- Computability in Europe, Bucharest, 2015, Complexity of Propositional Proofs
- Stockholm Mathematics Centre Colloquium, 2015, Continuous Combinatorics
- Crystals, Quasicrystals and Random Networks Workshop (ICERM), Providence, 2015, Syntactic Methods in Continuous Combinatorics
- Probabilistic and Extremal Combinatorics Workshop (IMA), Minneapolis, 2014, Flag Algebras: an Interim Report
- Mathematics in Armenia: Advances and Perspectives, Tsaghkadzor, 2013, *Flag Algebras*
- EXCILL2: Extremal Combinatorics at Illinois (plenary lecture), 2013, Flag Algebras: an Interim Report
- Indiana University Turing Symposium (keynote lecture), 2012, *Flag Algebras*
- 8th Annual Graduate Student Combinatorics Conference (keynote lecture), Urbana-Champaign, 2012, *Topics in Extremal Combinatorics*
- Saint Petersburg Mathematical Society, 2011, Flag Algebras
- Aisenstadt Lectures, Montreal, 2010 (various topics)
- 5th International Computer Science Symposium in Russia (opening lecture), Kazan, 2010, Complexity of Propositional Proofs
- Twenty-first annual Gödel Lecture, Association for Symbolic Logic North American Annual Meeting, Washington DC, 2010

- Barriers in Complexity Theory Workshop, Princeton, 2009, Somewhat Impartial Survey of Results in Circuit Complexity
- Association for Symbolic Logic North American Annual Meeting, Notre Dame University, 2009, *Flag Algebras*
- Midwest Model Theory Meeting, Notre Dame University, 2008, *Flag Algebras*
- China Theory Week, Beijing, 2007, Complexity of Propositional Proofs
- Workshop on Computational, Descriptive and Proof Complexity, and Algorithms, Moscow, 2007, Grand Challenges of Proof Complexity
- Symposium on Logical Foundations of Computer Science, New York, 2007, Natural Proofs: Ten Years After
- Pacific Institute for the Matematical Sciences, 10th Anniversary Lecture, Vancouver, 2006, *Feasible Proofs and Computations*
- European Mathematical Society weekend, Prague, 2004, *Feasible Proofs* and Computations.
- Joint meeting of 31st International Colloquium on Automata, Languages and Programming and 19th Annual IEEE Symposium on Logic in Computer Science, Turku, 2004, *Feasible Proofs and Computations: Partnership and Fusion*.
- International Workshop on Logic and Complexity in Computer Science Dedicated to the 60th Anniversary of A. Slissenko, Paris, 2001, *Proof Complexity of pigeonhole principles*.
- 5th Developments of Language Theory Conference, Vienna, 2001, *Propositional Proof Complexity*.
- International Conference Dedicated to the 100th Anniversary of P.S.Novikov, Moscow, 2001, *Complexity of Propositional Proofs*.
- Alfred Tarsky lectures, Berkeley, 2000.
- Vision in Mathematics, Tel-Aviv, 1999, Complexity of Proofs and Computations.

- Collegium Logicum, Vienna, 1998, Complexity of Resolution Proofs.
- Logic Colloquium, Prague, 1998, Complexity of Resolution Proofs.
- Proof Theory and Complexity, Aarhus, 1998, Lower Bounds for Algebraic Proof Systems.
- Paul Erdös Lectures, Jerusalem, 1998.
- Coxeter Lectures, Fields Institute, Toronto, 1998.
- 23rd International Colloquium on Automata, Languages and Programming, Paderborn, 1996, Lower bounds for propositional proofs and independence results in Bounded Arithmetic.
- DIMACS Distinguished Lectures Series, Rutgers University, 1996, Lower bounds for propositional proofs and independence results in Bounded Arithmetic.
- Mathematical Foundations of Computer Science, Prague, 1995, Lower Bounds for Propositional Proofs and Independence Results in Bounded Arithmetic.
- The seventh International Conference on Random Structures and Algorithms, Atlanta, 1995, *Pseudorandom Function Generators in Proof Theory and Complexity Theory*.
- Workshop on Geometrical and Combinatorial Methods in the Group Theory, Edinburgh, 1993, On systems of equations in free groups.
- SWAT 92, Helsinki, 1992, On small depth threshold circuits.
- Feasible Mathematics II, Cornell University, 1992, Bounded arithmetic and lower bounds in Boolean complexity.
- 8th Foundamentals of Complexity Theory, Gosen, 1991, Lower bounds for deterministic and nondeterministic branching programs.
- International Congress of Mathematicians at Berkeley, 1986, Lower Bounds for Monotone Complexity of Boolean Functions.

Journal Publications

- A. A. Razborov. On systems of equations in a free group. Izvestiya AN SSSR, ser. matem., 48(4):779–832, 1984. English Translation in Math. USSR Izvestiya, 25(1):115-162, 1985.
- [2] A. A. Razborov. Lower bounds for the monotone complexity of some boolean functions. *Doklady Academii Nauk SSSR*, 281(4):798–801, 1985.
 English Translation in *Soviet Math. Dokl.*, 31:354-357, 1985.
- [3] A. A. Razborov. Lower bounds of monotone complexity of the logical permanent function. *Matematicheskie Zametki*, 37(6):887–900, 1985.
 English Translation in *Mathem. Notes of the Academy of Sci. of the* USSR, 37:485-493, 1985.
- [4] A. Razborov. Lower bounds on the size of bounded-depth networks over a complete basis with logical addition. *Mathematical Notes of the Academy of Sciences of the USSR*, 41(4):598–607, 1987. English translation in 41:4, pages 333-338.
- [5] S. I. Adian and A. A. Razborov. Periodical groups and Li algebras. Russian Mathematical Surveys, 42(2):3–68, 1987.
- [6] A. Razborov. The gap between the chromatic number of a graph and the rank of its adjacency matrix is superlinear. *Discrete Mathematics*, 108:393–396, 1992.
- [7] A. Razborov. On the distributional complexity of disjointness. *Theoretical Computer Science*, 106:385–390, 1992.
- [8] A. Razborov. Kolmogorov and the complexity of algorithms. Bull. London. Math. Soc., 22:79–82, 1990.
- [9] A. Razborov. Lower bounds on the size of switching-and-rectifier networks for symmetric Boolean functions. *Mathematical Notes of the Academy of Sciences of the USSR*, 48(6):79–91, 1990.
- [10] A. Razborov. Applications of matrix methods to the theory of lower bounds in computational complexity. *Combinatorica*, 10(1):81–93, 1990.
- [11] M.S. Paterson and A. A. Razborov. The set of minimal braids is co-NPcomplete. Journal of Algorithms, 12:393–408, 1991.

- [12] A. Borodin, A. Razborov, and R. Smolensky. On lower bounds for read-k times branching programs. Computational Complexity, 3(1):1–18, 1993.
- [13] M. Goldmann, J. Hastad, and A. Razborov. Majority gates vs. general weighted threshold gates. *Computational Complexity*, 2:277–300, 1992.
- [14] J. Hastad, A. Razborov, and A. Yao. On the shrinkage exponent for read-once formulae. *Theoretical Computer Science*, 141:269–282, 1995.
- [15] A. Razborov and A. Wigderson. $n^{\Omega(\log n)}$ lower bounds on the size of depth 3 threshold circuits with AND gates at the bottom. *Information Processing Letters*, 45:303–307, 1993.
- [16] A. Razborov, E. Szemerédi, and A. Wigderson. Constructing small sets that are uniform in arithmetic progressions. *Combinatorics, Probability* and Computing, 2:513–518, 1993.
- [17] A. Razborov. On the parameterization of solutions for equations in free groups. International Journal of Algebra and Computation, 3(3):251– 273, 1993.
- [18] A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of Bounded Arithmetic. *Izvestiya of the RAN*, 59(1):201–222, 1995. See also *Izvestiya: Mathematics 59:1*, 205-227.
- [19] A. Razborov and S. Rudich. Natural proofs. Journal of Computer and System Sciences, 55(1):24–35, 1997.
- [20] S. Buss, R. Impagliazzo, J. Krajiček, P. Pudlák, A. Razborov, and J. Sgall. Proof complexity in algebraic systems and bounded depth Frege systems with modular counting. *Computational Complexity*, 6(3):256– 298, 1996/1997.
- [21] S. Jukna and A. Razborov. Neither reading few bits twice nor reading illegally helps much. *Discrete Applied Mathematics*, 85(3):223–238, 1998.
- [22] A. Razborov, A. Wigderson, and A. Yao. Read-once branching programs, rectangular proofs of the pigeonhole principle and the transversal calculus. *Combinatorica*, 22(4):555–574, 2002.
- [23] A. Razborov. Lower bounds for the polynomial calculus. Computational Complexity, 7:291–324, 1998.

- [24] B. Kashin and A. Razborov. Improved lower bounds on the rigidity of Hadamard matrices. *Matematicheskie Zametki*, 63(4):535–540, 1998.
- [25] S. Jukna, A. Razborov, P. Savicky, and I. Wegener. On P versus $NP \cap co NP$ for decision trees and read-once branching programs. Computational Complexity, 8(4):357–370, 1999.
- [26] D. Grigoriev and A. Razborov. Exponential complexity lower bounds for depth 3 arithmetic circuits in algebras of functions over finite fields. *Applicable Algebra in Engineering, Communication and Computing*, 10(6):465–487, 2000.
- [27] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Space complexity in propositional calculus. *SIAM Journal on Computing*, 31(4):1184–1211, 2002.
- [28] M. Alekhnovich, E. Ben-Sasson, A. Razborov, and A. Wigderson. Pseudorandom generators in propositional proof complexity. *SIAM Journal* on Computing, 34(1):67–88, 2004.
- [29] M. Alekhnovich and A. Razborov. Lower bounds for the polynomial calculus: non-binomial case. Proceedings of the Steklov Institute of Mathematics, 242:18–35, 2003.
- [30] A. Razborov. Resolution lower bounds for the weak functional pigeonhole principle. *Theoretical Computer Science*, 303(1):233–243, 2003.
- [31] A. Razborov. Resolution lower bounds for perfect matching principles. Journal of Computer and System Sciences, 69(1):3–27, 2004.
- [32] A. Razborov. Quantum communication complexity of symmetric predicates. Izvestiya of the Russian Academy of Science, Mathematics, 67(1):159–176, 2003.
- [33] A. Razborov. An upper bound on the threshold quantum decoherence rate. *Quantum Computation and Information*, 4(3):222–228, 2004.
- [34] A. Razborov. Guessing more secrets via list decoding. Internet Mathematics, 2(1):21–30, 2005.
- [35] V. Lifschitz and A. Razborov. Why are there so many loop formulas? ACM Transactions on Computational Logic, 7(2):261–268, 2006.

- [36] A. Razborov. Flag algebras. Journal of Symbolic Logic, 72(4):1239–1282, 2007.
- [37] A. Razborov and S. Yekhanin. An $\Omega(n^{1/3})$ lower bound for bilinear group based private information retrieval. *Theory of Computing*, 3:221–238, 2007.
- [38] M. Alekhnovich and A. Razborov. Resolution is not automatizable unless W[P] is tractable. SIAM Journal on Computing, 38(4):1347–1363, 2008.
- [39] A. Razborov. On the minimal density of triangles in graphs. Combinatorics, Probability and Computing, 17(4):603–618, 2008.
- [40] A. Razborov. A simple proof of Bazzi's theorem. ACM Transactions on Computation Theory, 1(1), 2009.
- [41] V. Guruswami, J. Lee, and A. Razborov. Almost euclidean subspaces of ℓ_1^N via expander codes. *Combinatorica*, 30(1):47–68, 2010.
- [42] A. Razborov and A. Sherstov. The sign-rank of AC⁰. SIAM Journal on Computing, 39(5):1833–1855, 2010.
- [43] A. Razborov. On 3-hypergraphs with forbidden 4-vertex configurations. SIAM Journal on Discrete Mathematics, 24(3):946–963, 2010.
- [44] F. Eisenbrand, N. Hähnle, A. Razborov, and T. Rothvoß. Diameter of polyhedra: Limits of abstraction. *Mathematics of Operations Research*, 35:786–794, 2010.
- [45] A. Razborov. On the Fon-der-Flaass interpretation of extremal examples for Turan's (3,4)-problem. Proceedings of the Steklov Institute of Mathematics, 274:247–266, 2011.
- [46] M. Alekhnovich and A. Razborov. Satisfiability, branch-width and Tseitin tautologies. Computational Complexity, 20:649–678, 2011.
- [47] O. Beyersdorff, N. Galesi, M. Lauria, and A. Razborov. Parameterized bounded-depth Frege is not optimal. ACM Transactions on Computation Theory, 7, article 7, 2012.

- [48] Hatami H, J. Hladky, D. Kral, S. Norin, and A. Razborov. Non-threecolorable common graphs exist. *Combinatorics, Probability and Computing*, 21(5):734–742, 2012.
- [49] Hatami H, J. Hladky, D. Kral, S. Norin, and A. Razborov. On the number of pentagons in triangle-free graphs. *Journal of Combinatorial Series, ser. A*, 120(3):722–732, 2013.
- [50] A. Razborov. On the Caccetta-Haggkvist conjecture with forbidden subgraphs. *Journal of Graph Theory*, 74(2):236–248, 2013.
- [51] A. Razborov. On Turan's (3,4)-problem with forbidden configurations. Matematicheskie Zametki, 95(2):271–281, 2014.
- [52] A. Razborov and E. Viola. Real advantage. ACM Transactions on Computation Theory, 5:article 7, 2013.
- [53] A. Razborov. A product theorem in free groups. Annals of Mathematics, 179(2):405–429, 2014.
- [54] A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. Annals of Mathematics, 181(3):415-472, 2015.
- [55] A. Razborov. A new kind of tradeoffs in propositional proof complexity. Journal of the ACM, 62(3):article 16, 2016.
- [56] Y. Li, A. Razborov, and B. Rossmann. On the AC⁰ complexity of subgraph isomorphism. SIAM Journal on Computing, 46(3):936–971, 2017.
- [57] L. Coregliano and A. Razborov. On the density of transitive torunaments. Journal of Graph Theory, 85(1):12–21, 2017.
- [58] A. Razborov. On the width of semi-algebraic proofs and algorithms. Mathematics of Operation Research, 42(4):1106–1134, 2017.
- [59] O. Pikhurko and A. Razborov. Asymptotic structure of graphs with the minimum number of triangles. *Combinatorics, Probability and Comput*ing, 26(1):138–160, 2017.
- [60] A. Razborov. On space and depth in resolution. Computational Complexity, 27(3):511–559, 2018.

Conference Proceedings, Collections etc.: original results not (yet) published in journals

- A. A. Razborov. Bounded-depth formulae over {∧, ⊕} and some combinatorial problems. In S. I. Adian, editor, *Problems of Cybernetics. Complexity Theory and Applied Mathematical Logic*, pages 149–166. VINITI, Moscow, 1988. In Russian.
- [2] A. Razborov. On the method of approximation. In Proceedings of the 21st ACM Symposium on Theory of Computing, pages 167–176, 1989.
- [3] A. Razborov. On submodular complexity measures. In M. S. Paterson, editor, Boolean Function Complexity. London Math. Soc., Lecture Note Series 169, pages 76–83. Cambridge University Press, 1992.
- [4] A. Razborov. An equivalence between second order bounded domain bounded arithmetic and first order bounded arithmetic. In P. Clote and J. Krajiček, editors, Arithmetic, Proof Theory and Computational Complexity, pages 247–277. Oxford University Press, 1992.
- [5] A. Razborov. Bounded Arithmetic and lower bounds in Boolean complexity. In P. Clote and J. Remmel, editors, *Feasible Mathematics II. Progress in Computer Science and Applied Logic, vol.* 13, pages 344–386. Birkhaüser, 1995.
- [6] J. Nordström and A. Razborov. On minimal unsatisfiability and timespace trade-offs for k-DNF resolution. In *Proceedings of the 38th International Colloquium on Automata, Languages and Programming*, pages 642–653, 2011.
- [7] A. Atserias, I. Bonacina, S. Rezende, M. Lauria, J. Nordström, and A. Razborov. Clique is hard on average for regular resolution. In *Pro*ceedings of the 50th ACM Symposium on the Theory of Computing, pages 866–877, 2018.

Preprints, Submutted Manuscripts etc.

[1] A. A. Razborov. On rigid matrices. Manuscript in Russian, June 1989.

- [2] A. Razborov. On provably disjoint NP-pairs. Technical Report RS-94-36, Basic Research in Computer Science Center, Aarhus, Denmark, 1994. Available at http://www.brics.aau.dk/RS/94/36/BRICS-RS-94-36.ps.gz.
- [3] A. Razborov. Improved resolution lower bounds for the weak pigeonhole principle. Technical Report TR01-055, Electronic Colloquium on Computational Complexity, 2001.
- [4] D. Mubayi and A. Razborov. Polynomial to exponential transition in Ramsey theory. Technical Report 1901.06029 [math.CO], arXiv e-print, 2019, to appear in *Proceedings of the London Mathematical Society*.
- [5] L. Coregliano and A. Razborov. Semantic limits of dense combinatorial objects. Technical Report 1910.08797 [math.CO], arXiv e-print, 2019, to appear in *Russian Mathematical Surveys*.
- [6] N. Mull, S. Pang, and A. Razborov. On CDCL-based proof systems with the ordered decision strategy. Technical Report 1909.04135 [cs.LO], arXiv e-print, 2019.

Conference Proceedings: survey talks

- A. A. Razborov. Lower bounds for monotone complexity of boolean functions. In *Proceedings of the International Congress of Mathematicians*, volume 2, pages 1478–1487, Berkeley, California, USA, 1986. In Russian. For the English translation see *Amer. Math. Soc. Transl.*, 147(2):75-84, 1990.
- [2] S. I. Adian, A.A. Razborov, and N.N Repin. Upper and lower bounds for nilpotency classes of Lie algebras with Engel conditions. In *Group The*ory, Proceedings of the Singapore Group Theory Conference held at the National University of Singapore, June 8-19,1987, pages 57–75. Walter de Gruyter, 1989.
- [3] A. Razborov. Lower bounds for deterministic and nondeterministic branching programs. In *Proceedings of the 8th FCT, Lecture Notes in Computer Science*, 529, pages 47–60, New York/Berlin, 1991. Springer-Verlag.

- [4] A. Razborov. On small depth threshold circuits. In Proceedings of the SWAT 92, Lecture Notes in Computer Science, 621, pages 42–52, New York/Berlin, 1992. Springer-Verlag.
- [5] A. Razborov. On systems of equations in free groups. In Combinatorial and Geometric Group Theory, Edinburgh 1993. London Mathematical Society Lecture Note Series, 204, pages 269–283. Cambridge University Press, 1995.
- [6] A. Razborov. Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In F. Meyer auf der Heide and B. Monien, editors, *Proceedings of the 23rd ICALP, Lecture Notes in Computer Science*, 1099, pages 48–62, New York/Berlin, 1996. Springer-Verlag.
- [7] A. Razborov. Proof complexity of pigeonhole principles. In *Proceedings* of the 5th DLT, Lecture Notes in Computer Science, 2295, pages 100– 116, New York/Berlin, 2002. Springer-Verlag.
- [8] A. Razborov. Propositional proof complexity. Journal of the ACM, 50(1):80-82, 2003.
- [9] A. Razborov. Feasible proofs and computations: partnership and fusion. In Proceedings of the 31st International Colloquium, Lecture Notes in Computer Science, 3142, pages 8–14, New York/Berlin, 2004. Springer-Verlag. Also appeared in Proceedings of the 19th LICS conference.