Curriculam Vitae

MANINDRA AGRAWAL, *N. Rama Rao Chair Professor*

Department of Computer Science and Engineering
Indian Institute of Technology
Kanpur 208016, INDIA

Academic Degrees

- B. Tech in Computer Science and Engineering, IIT Kanpur, 1986.
- Ph.D. in Computer Science, IIT Kanpur, 1991.

Employment

[1/03–present] N. Rama Rao Chair Professor, Department of Computer Science and Engineering, IIT Kanpur.

[7/04–6/05] Distinguished Visiting Professor, Department of Computer Science, National University of Singapore, Singapore.

[6/03–6/04] Member, School of Mathematics, Institute for Advanced Studies, Princeton, USA.

[9/01–12/02] Professor, Department of Computer Science and Engineering, IIT Kanpur.

[12/99–8/01] Associate Professor, Department of Computer Science and Engineering, IIT Kanpur.

[8/96–11/99] Assistant Professor, Department of Computer Science and Engineering, IIT Kanpur.

[7/95–7/96] Humblodt Fellow, University of Ulm, Ulm, Germany.

[3/93–6/95] Fellow, School of Mathematics, SPIC Science Foundation, Madras.

[1/92–2/93] Research Associate, Department of Computer Science and Engineering, IIT Kanpur.

Awards

- H. K. Firodia Award, 2011.
- Humboldt Prize, 2011.
- TWAS Prize in Mathematics, 2011.
- Rajib Goyal Prize, 2010.
- P. C. Mahalanobis Birth Centenary Award, 2009.
- G. D. Birla Award for Scientific Research, 2009.
- Infosys Mathematics Prize, 2008.
- Fulkerson Prize for the paper "PRIMES is in P", 2006.
- Gödel Prize for the paper "PRIMES is in P", 2006.
- Dr Meghnad Saha award (UGC) in Mathematical Sciences, 2003.
- ICTP (Internatinal Centre for Theoretical Physics, Trieste) prize, 2003.
- Shanti Swarup Bhatnagar award in Mathematical Sciences, 2003.
- Distinguished Alumnus award by Indian Institute of Technology, Kanpur, 2003.
- The Clay Research Award by Clay Mathematics Institute, Boston, 2002.
- The Young Scientist Award by the UP Council for Science and Technology, 2000.
- The Young Engineer Award by the Indian National Academy of Engineering, 1998.

Fellowships

- J. C. Bose Fellowship for the period 2006-2015.
- Fellow of Indian National Science Academy.
- Fellow of Indian Academy of Sciences.
- Fellow of Indian National Academy of Engineering.
- Fellow of The National Academy of Sciences.

Professional Activities

- Editor, Computability journal (IOS Press).
- Editor, Theory of Computing journal (online journal published at university of Chicago).
- Member, Conference Committee, Conference on Computational Complexity, 2009-11.
- Program committee chair for the 20th IEEE Conference on Computational Complexity, July 2006, Prague, Czech Republic.

- Program committee co-chair for the 22nd Foundations of Software Technology and Theoretical Computer Science conference, December 2002, Kanpur.
- Served on the program committees of several conferences: CCC, FOCS, FSTTCS, AsiaCrypt, TAMC etc.

Publications

Book Chapters

1. *The Discrete Time Behavior of Restricted Linear Hybrid Automata* (with F. Stephan, P. S. Thiagarajan, S. Yang), Modern Applications of Automata Theory, World Scientific, pages 437–453, 2012.

2. *The Isomorphism Conjecture for NP*, Computability in Context: Computation and Logic in Real World, Editors: Barry Cooper and Andrea Sorbi, World Scientific, pages 19–48, 2011.

3. *Classifying Polynomials and Identity Testing* (with R. Saptharishi), Current Trends in Science (Platinum Jubilee Special, Indian Academy of Sciences), pages 149–162, 2009.

Journal Papers

1. *The Isomorphism Conjecture for Constant Depth Reductions*, Journal of Computer and Systems Sciences (special issue on Karp's Kyoto Prize), volume 77(1), pages 3–13, 2011.

2. *PRIMES is in P* (with N. Kayal and N. Saxena), Annals of Mathematics, volume 160(2), pages 781–793, 2004.

3. *Primality and Identity Testing via Chinese Remaindering* (with S. Biswas), Journal of the ACM, volume 50(4), pages 429–443, 2003.

4. *For Completeness, Sublogarithmic Space is No Space*, Information Processing Letters, volume 82, pages 321–325, 2002.

5. *The Satisfiability Problem for Probabilistic Ordered Branching Programs* (with T. Thierauf), Theory of Computing Systems, volume 34, pages 471–487, 2001.

6. *Reducing the Complexity of Reductions* (with E. Allender, R. Impagliazzo, T. Pitassi, and S. Rudich), Journal of Computational Complexity, volume 10, pages 117–138, 2001.

7. *Characterizing Small Space and Small Depth Classes by Operators of Higher Types* (with E. Allender, S. Dutta, H. Vollmer, C. Wanger), Chicago Journal on Theoretical Computer Science,
`http://www.cs.uchicago.edu/research/publications/cjtcs/`, 2000.

8. *On TC^0, AC^0, and Arithmetic Circuits* (with E. Allender and S. Dutta), the special issue of the Journal of Computer and System Sciences on the twelfth Conference on Computational Complexity, volume 60, pages 395–421, 2000.

9. *The Formula Isomorphism Problem* (with T. Thierauf), SIAM Journal on Computing, volume 30(3), pages 990–1009, 2000.

10. *Reductions in Circuit Complexity: An Isomorphism Theorem and a Gap Theorem* (with E. Allender and S. Rudich), the special issue of the Journal of Computer and System Sciences on the eleventh Conference on Computational Complexity, volume 57, pages 127–143, 1999.

11. *DSPACE(n) $\stackrel{?}{=}$ NSPACE(n): A Degree Theoretic Characterization*, the special issue of the Journal of Computer and Systems Sciences on the tenth Structure in Complexity Theory conference, volume 54(3), pages 383–392, 1997.

12. *A Note on Decision versus Search for Graph Automorphism* (with V. Arvind), Information and Computation 131(2), pages 179–189, 1996.

13. *NP-creative Sets: A New Class of Creative Sets in NP* (with S. Biswas), Mathematical Systems Theory 29, pages 487–505, 1996.

14. *Quasi-linear Truth-table Reductions to P-selective Sets* (with V. Arvind), Theoretical Computer Science 158, pages 361–370, 1996.

15. *Geometric Sets of Low Information Content* (with V. Arvind), Theoretical Computer Science 158, pages 193–220, 1996.

16. *On the Isomorphism Conjecture for Weak Reducibilities*, the special issue of the Journal of Computer and Systems Sciences on the ninth Structure in Complexity Theory conference, volume 53(2), pages 267–282, 1996.

17. *Polynomial Isomorphism of 1-L-Complete Sets* (with S. Biswas), the special issue of the journal of Computer and Systems Sciences on the eighth Structure in Complexity Theory conference, volume 53(2), pages 155-160, 1996.

18. *On the Isomprphism Conjecture for 2DFA Reductions* (with S. Venkatesh), Intl. Journal on Foundations of Computer Science 7(4), pages 339–352, 1996.

Invited Papers

1. *On the Arithmetic Complexity of Euler Function*, in proceedings of the 6th International Computer Science Symposium in Russia, 2011, LNCS 6651, pp 43–49.

2. *Primality Tests Based on Fermat's Little Theorem*, in proceedings of the 8th ICDCN Conference, 2006, LNCS 4308, pp 288–293.

3. *Proving Lower Bounds via Pseudo-random Generators*, in proceedings of the 25th FSTTCS Conference, 2005, LNCS 3821, pp 92–105.

4. *Automorphisms of Finite Rings and Applications to Complexity of Problems* (with N. Saxena), in proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science, Stuttgart, 2005, LNCS 3404, pp 1–17.

5. *On Derandomizing Tests for Certain Polynomial Identities*, in proceedings of the 18th IEEE Conference on Computational Complexity, Aarhus, 2003, pp 355–359.

Refereed Conference Papers

1. *On the Optimality of Lattices for the Coppersmith Technique* (with Y. Aono, T. Satoh, O. Watanabe), in proceedings of 17th Australasian Conference on Information Security and Privacy (ACISP), 2012, pp 376–389.

2. *Verification of the Symbolic Dynamics of Markov Chains* (with S. Akshay, B. Genest, P. S. Thiagarajan), in proceedings of 27th Symposium on Logic in Computer Science (LICS), 2012, pp 55–64.

3. *Jacobian hit circuits: Hitting sets, lower bounds for depth-D occur-k formulas and depth-3 transcendence degree-k circuits* (with Chandan Saha, Ramprasad Saptharishi, Nitin Saxena), in proceedings of 44th Symposium on Theory of Computing (STOC), 2012, pp 599–614.

4. *One-Way Functions and the Berman-Hartmanis Conjecture* (with O. Watanabe), in proceedings of 24th Conference on Computational Complexity (CCC), 2009, pp 194–202.

5. *Arithmetic Circuits: A Chasm at Depth Four* (with V Vinay), in proceedings of 49th Foundations of Computer Science conference (FOCS), 2008, pp 48–53.

6. *The Polynomially Bounded Perfect Matching Problem is in NC^2* (with T. M. Hoang and T. Thierauf), in proceedings of 24th Symposium on Theoretical Aspects of Computer Science, 2007, LNCS 4393, pp 489–499.

7. *Behavioural Approximations for Restricted Linear Differential Hybrid Automata* (with Y. Shaofa, F. Stephan, P. S. Thiagarajan), Ninth International Workshop on Hybrid Systems: Computation and Control, 2006, LNCS 3927, pp 4–18.

8. *Equivalence of F-Algebras and Cubic Forms* (with N. Saxena), in proceedings of 23rd Symposium on Theoretical Aspects of Computer Science, 2006, LNCS 3884, pp 115–126.

9. *The Discrete Time Behavior of Lazy Linear Hybrid Automata* (with P. S. Thiagarajan), in proceedings of the Eighth International Workshop on Hybrid Systems: Computation and Control, 2005, LNCS 3414, pp 55–69.

10. *Lazy Rectangular Hybrid Automata* (with P. S. Thiagarajan), in proceedings of the Seventh International Workshop on Hybrid Systems: Computation and Control, University of Pennsilvania, 2004, LNCS 2993, pp 1–15.

11. *Pseudo-random Generators and the Structure of Complete Degrees*, in proceedings of the 17th IEEE Conference on Computational Complexity, Montreal, 2002, pp 139–146.

12. *The First-order Isomorphism Theorem*, in proceedings of the 21st FST-TCS conference, Bangalore, 2001, LNCS 2245, pp 70–82.

13. *Hards Sets and Pseudo-random Generators for Constant Depth Circuits*, in proceedings of the 21st FST-TCS conference, Bangalore, 2001, LNCS 2245, pp 58–69.

14. *Towards Uniform AC^0-Isomorphisms*, in proceedings of the 16th IEEE Conference on Computational Complexity, Chicago, 2001, pp 13–20.

15. *Primality and Identity Testing via Chinese Remeindering* (with S. Biswas), in proceedings of the 40th Annual Symposium on Foundations of Computer Science, New York, 1999, pp 202–209.

16. *The Satisfiability Problem for Probabilistic Ordered Branching Programs* (with T. Thierauf), in proceedings of the 13th IEEE Conference on Computational Complexity, Buffalo, 1998, pp 233–240.

17. *On TC^0, AC^0, and Arithmetic Circuits* (with E. Allender, and S. Dutta), in proceedings of the 12th IEEE Conference on Computational Complexity, 1997, pp 134–148. Invited to the special issue of the journal of Computer and Systems Sciences on the conference.

18. *Reducing the Complexity of Reductions* (with E. Allender, R. Impagliazzo, T. Pitassi, and S. Rudich), in proceedings of the 29th ACM Symposium on Theory of Computing, 1997, pp 730–738.

19. *Pinpointing Computation with Modular Queries in the Boolean Hierarchy* (with R. Beigel and T. Thierauf), in proceedings of the sixteenth FST & TCS conference, Hyderabad, 1996, LNCS 1180, pp 322–334.

20. *The Boolean Isomorphism Problem* (with T. Thierauf), in proceedings of the 37th IEEE Symposium on Foundations of Computer Science, 1996, pp 422–430.

21. *An Isomorphism Theorem for Circuit Complexity* (with E. Allender), in proceedings of the eleventh IEEE Conference on Computational Complexity, Philadelphia, 1996, pp 2–12. Invited to the special issue of the journal of Computer and Systems Sciences on the conference.

22. *A Note on Decision versus Search for Graph Automorphism* (with V. Arvind), in proceedings of the eleventh IEEE Conference on Computational Complexity, Philadelphia, 1996, pp 236–241.

23. *DSPACE(n) $\stackrel{?}{=}$ NSPACE(n): A Degree Theoretic Characterization*, in proceedings of the tenth IEEE Structure in Complexity Theory Conference, Minneapolis, 1995, pp 315–323.

24. *Reductions of Self-reducible Sets to Depth-1 Weighted Threshold Circuit Classes, and Sparse Sets* (with V. Arvind), in proceedings of the tenth IEEE Structure in Complexity Theory Conference, Minneapolis, 1995, pp 264–276.

25. *On the Isomorphism Problem for Weak Reducibilities*, in proceedings of the ninth IEEE Structure in Complexity Theory Conference, Amsterdum, 1994, pp 338–355.

26. *Polynomial-time Truth-table Reductions to P-selective Sets* (with V. Arvind), in proceedings of the ninth IEEE Structure in Complexity Theory Conference, Amsterdam, 1994, pp 24–30.

27. *Polynomial Isomorphism of 1-L-Complete Sets* (with S. Biswas), in proceedings of the eighth IEEE Structure in Complexity Theory Conference, San Diego, 1993, pp 75–80.

28. *Universal Relations* (with S. Biswas), in proceedings of the seventh IEEE Structure in Complexity Theory Conference, Boston, 1992, pp 207–220.

29. *NP-hard Sets and Creativeness Over Constant Time Languages*, in proceedings of the eleventh FST &$\tilde{\text{T}}$CS, Delhi, 1991, LNCS 560, pp 224–241.