# Curriculam Vitae

**MANINDRA AGRAWAL**, 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

[**1/18–present**] Professor, Department of Computer Science and Engineering, IIT Kanpur.

[**1/03–12/17**] 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

- Goyal Prize, 2017
- NASI-Reliance Platinum Jubilee Award, 2015
- ACCS-CDAC Foundation Award, 2014
- Padma Shri, 2013
- H. K. Firodia Award, 2011
- Humboldt Forscheungpreis, 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, 2006
- Gödel Prize, 2006
- Dr Meghnad Saha award 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

- Foreign Associate of the US National Academy of Sciences.
- Fellow of The World Academy of Sciences.
- 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.
- J. C. Bose Fellowship for the period 2006-2015.

# Professional and Administrative Activities

## Administrative Experience

- Deputy Director, IIT Kanpur, 2017-19.
- Dean of Faculty Affairs, IIT Kanpur, 2013-15.
- Dean of Resource Planning and Generation, IIT Kanpur, 2011-12.
- Head, Department of Computer Science and Engineering, IIT Kanpur, 2006-10.

## Membership of Committees

- Member, Governing Council, Indian Statistical Institute, 2016-22.
- Vice President, Indian Academy of Sciences, 2016-21.
- Chairman, SERB PAC on EE-CE, 2018-21.
- Chairperson, INSPIRE Committee for Mathematical Sciences, 2016-20.
- Member, National Board of Higher Mathematics, 2015-19.
- Member, Governing Council, Indian National Science Academy, 2016-18.
- Member, Board of Governors, IISER Bhopal, 2009-2017.
- Member, Board of Governors, NISER Bhubaneswar, 2015-17.
- Member, Governing Council, Indian Academy of Engineering, 2014-15.
- Member, Board of Management, IIIT Allahabad, 2013-2015.
- Memeber, Science and Engineering Research Board, 2012-14.

## Editorships and Program Committees

- 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, Prague, Czech Republic, 2006.
- Program committee co-chair for the 22nd Foundations of Software Technology and Theoretical Computer Science conference, Kanpur, 2002.
- Served on the program committees of several conferences: CCC, FOCS, FSTTCS, AsiaCrypt, TAMC etc.

## Major Projects

| Project Name | Role | Funding Agency | Duration | Funding (in Rs Cr) |
|---|---|---|---|---|
| Technology Innovation Hub in Cybersecurity | Project Director | DST | 2020-24 | 170 |
| Center of Excellence for Defense Corridor | PI | GoUP | 2019-23 | 50 |
| National Blockchain Project | PI | NSCS | 2018-23 | 33 |
| Cyber Security Center for Critical Infrastructure | PI | SERB | 2017-23 | 16 |

# 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, 2012: 473–453.

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

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

## Journal Papers

1. *Modeling the spread of SARS-CoV-2 pandemic - Impact of lockdowns & interventions* (with M. Kanitkar and M. Vidyasagar) Indian Journal of Medical Research, volume 153, 2021: 175–181.

2. *Bootstrapping Variables in Algebraic Circuits* (with S. Ghosh, and N. Saxena) PNAS, volume 116 (17), 2019: 8107–8118.

3. *The Query Complexity of a Permutation-Based Variant of Mastermind* (with P. Afshani, B. Doerr, C. Doerr, K. G. Larsen, and K. Melhorn) Discrete Applied Mathematics, volume 260, 2019: 28–50.

4. *On the Optimality of Lattices for the Coppersmith Technique* (with Y. Aono, T. Satoh, and O. Watanabe) Applied Algebra in Engineering, Communication and Computing, volume 29(2), 2018: 169–195.

5. *Dimension, Pseudorandomness, and Extraction of Pseudorandomness* (with D. Chakraborty, D. Das, and S. Nandkumar) Computability, volume 6(3), 2017: 277–305.

6. *Jacobian Hits Circuits: Hitting Sets, Lower Bounds for Depth-D Occur-k Formulas and Depth-3 Transcendence Degree-k Circuits* (with C. Saha, R. Saptharishi, and N. Saxena) SIAM Journal of Computing, volume 45(4), 2016: 1533–1562.

7. *Hitting Sets for ROABP and Sum of Set-Multilinear Circuits* (with R. Gurjar, A. Korwar, and N. Saxena) SIAM Journal of Computing, volume 44(3), 2015: 669–697.

8. *Approximate Verification of the Symbolic Dynamics of Markov Chains* (with S. Akshay, Blaise Genest, and P. S. Thiagarajan), Journal of the ACM, volume 62(1), 2015: 2.1–2.34.

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

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

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

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

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

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

15. *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.

16. *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, 2000: 395–421.

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

18. *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, 1999: 127–143.

19. *DSPACE(n) $\overset{?}{=}$ 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), 1997: 383–392.

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

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

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

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

24. *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), 1996: 267–282.

25. *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), 1996: 155–160.

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

## Invited Papers

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

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

3. *Proving Lower Bounds via Pseudo-random Generators*, in proceedings of the 25th FSTTCS Conference, LNCS 3821, 2005: 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, LNCS 3404, 2005: 1–17.

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

## Refereed Conference Papers

1. *SUTRA: An Approach to Modelling Pandemics with Undetected (Asymptomatic) Patients, and Applications to COVID-19* (with M. Kanitkar and M. Vidyasagar), in proceedings of 60th IEEE Conference on Decision and Control (CDC), 2021: 3531.

2. *Bootstrapping Variables in Algebraic Circuits* (with S. Ghosh and N. Saxena), in proceedings of 50th Symposium on Theory of Computing (STOC), 2018: 1166-1179.

3. *Integer Factoring Using Small Algebraic Dependencies* (with Nitin Saxena, Shubham Srivastava), in proceedings of 41st Mathematical Foundations of Computer Science (MFCS), 2016: 1–14.

4. *Dimension, Pseudorandomness and Extraction of Pseudorandomness* (with Diptarka Chakravarti, Satyadev Nandkumar), in proceedings of 35th annual conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS), 2015: 221–235.

5. *The Query Complexity of Finding a Hidden Permutation* (with Peyman Afshani, Benjamin Doerr, Carola Doerr, Kasper Green Larsen, Kurt Mehlhorn), Space-Efficient Data Structures, Streams, and Algorithms, 2013: 1–13.

6. *Quasi-polynomial hitting sets for set depth-D formulas* (with C. Saha and N. Saxena), in proceedings of 45th Symposium on Theory of Computing (STOC), 2013: 321–330.

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

8. *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: 55–64.

9. *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: 599–614.

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

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

12. *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, LNCS 4393, 2007: 489–499.

13. *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, LNCS 3927, 2006: 4–18.

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

15. *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, LNCS 3414, 2005: 55–69.

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

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

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

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

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

21. *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: 202–209.

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

23. *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: 134–148.

24. *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: 730–738.

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

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

27. *An Isomorphism Theorem for Circuit Complexity* (with E. Allender), in proceedings of the eleventh IEEE Conference on Computational Complexity, Philadelphia, 1996: 2–12.

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

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

30. *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: 264–276.

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

32. *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: 24–30.

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

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

35. *NP-hard Sets and Creativeness Over Constant Time Languages*, in proceedings of the eleventh FST &T̃CS, Delhi, LNCS 560, 1991: 224–241.