

Madhu Sudan

MIT, CSAIL
The Stata Center, 32-G640
32 Vassar Street
Cambridge, MA 02139, USA
Tel: (617) 253-9680
email: madhu@mit.edu
<http://theory.csail.mit.edu/~madhu>

Last updated: August 23, 2007

Areas of Special Interests

Theoretical Computer Science, Algorithms, Computational Complexity, Coding Theory, Optimization.

Ph.D. Title

Efficient Checking of Polynomials and Proofs and the Hardness of Approximations.

Educational Background

Ph.D. Computer Science; University of California at Berkeley, 1992
B.Tech. Computer Science; Indian Institute of Technology at New Delhi, 1987

Work Experience

1990 Summer Student Researcher at IBM Almaden Research Center
1992-1997 Research Staff Member, IBM Thomas J. Watson Research Center
Mathematical Sciences Department
Sept. 1997 - Dec. 2002 Associate Professor, Massachusetts Institute of Technology
Department of Electrical Engineering and Computer Science
Jan. 2003 - Jan. 2005 Professor, MIT EECS.
Feb. 2005 - Fujitsu Chair Professor, MIT EECS
July 2005 - Danny Lewin Outstanding Professor, MIT EECS

Awards

Sakrison Memorial Award (Ph.D. Thesis, EECS, Berkeley)	1993
ACM Doctoral Dissertation Award	1993
Sloan Foundation Fellowship	1998
NSF Career Award	1999
Information Theory Paper Award	2000
Gödel Prize	2001
Nevanlinna Prize	2002
Felicitaton, Indian Assoc. Computing Research	2002
Distinguished Alumnus Award, University of California at Berkeley, CS Division	2003
Radcliffe Fellowship	2003-2004
Distinguished Alumnus Award, Indian Institute of Technology at New Delhi	2004
Guggenheim Fellowship	2005-2006

Current Organization Membership: ACM, IEEE, SIAM, AMS

Professional Service:

<u>Activity</u>	<u>Beginning</u>	<u>Ending</u>
Journal activities		
<u>Editor</u> , SIAM Journal on Discrete Mathematics	1997	2002
<u>Editor</u> , SIAM Journal on Computing	2000	current
<u>Editor</u> , Information and Computation	2000	2006
<u>Guest Editor</u> , Journal of Computer and System Sciences, Special issue devoted to papers from <i>Complexity '2001</i>	May 2001	May 2002
<u>Editor</u> , Journal of the ACM	2003	current
<u>Guest Co-Editor</u> , SIAM Journal on Computing, Special Issue on <i>Randomness and Complexity</i>	May 2004	May 2006
<u>Editor-in-chief</u> , Foundations and Trends in Theoretical Computer Science	June 2004	present
<u>Associate Editor</u> , IEEE Transactions on Information Theory	2005	2006
Conference Program Committee Activities		
<u>Chair</u> , Program Committee, <i>Complexity 2001</i> , IEEE Conference on Computational Complexity	2001	2001
<u>Chair</u> , Program Committee, <i>FOCS 2003</i> , IEEE Symposium on Foundations of Computer Science	November 2002	November 2003
<u>Member</u> , Program Committee, <i>STOC '95</i> , ACM Symposium on Theory of Computing	May 1995	
<u>Member</u> , Program Committee, <i>FOCS '97</i> , IEEE Symposium on Foundations of Computer Science	October 1997	
<u>Member</u> , Program Committee, <i>SODA '98</i> , ACM-SIAM Symposium on Discrete Algorithms	January 1998	
<u>Member</u> , Program Committee, <i>RANDOM '98</i> , Workshop on Randomization and Approximation	October 1998	
<u>Member</u> , Program Committee, <i>COCOON '99</i> , International Computing and Combinatorics Conference	July 1999	
<u>Member</u> , Program Committee, <i>FCT '99</i> , Int'l Symposium on Fundamentals of Computing Theory	September 1999	
<u>Member</u> , Program Committee, <i>FOCS '2001</i> , IEEE Symposium on Foundations of Computer Science	October 2001	
<u>Member</u> , Program Committee, <i>FSTTCS '2001</i> , Foundations of Software Technology and Theoretical CS	December 2001	
<u>Member</u> , Program Committee, <i>STOC '2006</i> , ACM Symposium on Theory of Computing	May 2006	
<u>Member</u> , Program Committee, <i>ISIT '2006</i> , International Symposium on Information Theory	July 2006	
<u>Member</u> , Program Committee, <i>CCC '2006</i> , IEEE Conference on Computational Complexity	July 2006	
<u>Member</u> , Program Committee, <i>RANDOM '2006</i> , 10th Annual Workshop on Randomization and Computation	August 2006	
<u>Member</u> , Program Committee, <i>EuroComb '2007</i> , European Conf. Combinatorics, Graph theory, Applications	March 2007	

Steering Committees

<u>Member of Scientific Board</u> , Electronic Colloquium on Computational Complexity	1994	present
<u>Conference Committee Member</u> , IEEE Conference on Computational Complexity	1999	2002

Other activities

<u>Chair</u> , Session on Approximation Algorithms 16th Mathematical Programming Symposium	June 1994	
<u>Co-organizer</u> , Dagstuhl Workshop on Combinatorial Optimization Problems	January 2000	
<u>Co-organizer</u> , IAS Workshop on Asymptotic and Computational Aspects of Coding Theory	March 2001	
<u>Member</u> , Committee on Fundamentals of Computer Science, Computer Science and Telecommunications Board, National Academies of Sciences	January 2001	December 2002
<u>Panelist</u> , NSF Workshop on the interface between Information Theory and Computer Science	2003	2003
<u>Co-organizer</u> , IMA special thematic year (2006-2007) on Algebraic Geometry and its Applications	March 2003	June 2007
<u>Co-organizer</u> , Oberwolfach meeting on Complexity Theory	May 2003	May 2003
<u>Co-organizer</u> , Radcliffe Symposium on Privacy and Security: Technology, Policy and Society	September 2003	March 2004
<u>Co-organizer</u> , Banff International Research Station Workshop on Advances in Complexity Theory	April 2004	July 2004
<u>Co-moderator</u> , ACM Computing Research Repository (CoRR), Information Theory Section	April 2004	present
<u>Co-organizer</u> , Oberwolfach meeting on Complexity Theory	June 2005	June 2005
<u>Member</u> , SIGACT Committee on TCS Funding	June 2005	June 2007
<u>Co-organizer</u> , Banff International Research Station Workshop on Advances in Complexity Theory	May 2006	August 2006
<u>Co-organizer</u> , IMA Workshop on Complexity, Coding, and Communications	June 2006	April 2007
<u>Co-organizer</u> , Oberwolfach meeting on Complexity Theory	June 2007	June 2007

Principal Lectures and Addresses

- Courses, mini-courses, lecture series
 - One week course on *Coding Theory in Modern Computational Complexity*, Barbados, March 2006.
 - Four week course on *Probabilistic Checking of Proofs* at the Scuola Normale Superiore, organized by the Scuola Matematica Interuniversitaria, Cortona, Italy, July 2005.
 - Mini-course on *Coding Theory* at the Estonian Winter School in Computer Science, Palmse, Estonia, March 2004.
 - Mini-course on *Coding Theory* at the IBM Almaden Research Center, November 2000.
 - Mini-course on *Probabilistic Checking of Proofs*, Part of Graduate Summer School on Computational Complexity organized by the Park City Mathematical Institute at the Institute for Advanced Study, Princeton, New Jersey, July-August, 2000.
 - Mini-course on *Coding Theory* at the IBM Thomas J. Watson Research Center, January 2000.
 - Lecture series on *Probabilistic verification of proofs* at the Fields Institute, Toronto, April 1998.

- Lecture series at the school on *Approximate Solutions to Hard Combinatorial Optimization Problems* at the CISM, Udine, Italy, September 1996.
 - Lecture series on *Approximability of Optimization Problems* at the IBM Tokyo Research Laboratory, March 1996.
 - Lecture series on *Hardness of Approximation Problems* at the IBM Almaden Research Center, October 1995.
 - Mini-course on *Hardness of Approximation Problems* at the University of Toronto, February 1993.
- Invited seminars
 - Workshop in honor of Tom Høholdt’s 60th Birthday, Lyngby, Denmark, June 2005.
 - Plenary speaker, *Information Theory Workshop*, San Antonio, Texas, October, 2004.
 - Oberwolfach Meetings on *Coding Theory*, Germany, May 2000, and December 2003.
 - Plenary speaker, Winter meeting of the Canadian Mathematical Society, December 6, 2003.
 - Plenary speaker, Annual meeting of the German Mathematical Society, September 30, 2003.
 - New York Theory Day, May 2003.
 - Nevanlinna Prize Lecture, International Congress of Mathematicians, Beijing, 23 August 2002.
 - Workshop on Information Theory in honor of Philippe Delsarte’s 60th Birthday at Universite Catholique du Louvain, Belgium, 31 May 2002.
 - Erdős Memorial Lecture Series, Hebrew University, Jerusalem, 14-20 March 2002.
 - Invited speaker at Applied Algebra, Algebraic Algorithms, and Error-correcting codes (AAECC’01), Melbourne, 26-30 November, 2001.
 - Invited Tutorial on *Coding theory* at IEEE Symposium on Foundations of Computer Science, Las Vegas, 14-17 October, 2001.
 - Oberwolfach Meetings on *Complexity Theory*, Germany, 1994, 1996, and 2000.
 - Invited speaker, Symposium on Discrete Mathematics 2000, Technische Universität, München, 5-6 October 2000.
 - Keynote plenary invited speaker at the International Conference IFIP TCS 2000, Sendai, Japan, August 2000.
 - Invited speaker, DIMACS Workshop on Computing Approximate Solutions to NP-hard Problems, Princeton, New Jersey, February 20-22, 2000.
 - Invited speaker, RANDOM ’99, Third International Workshop on Randomization and Approximation Techniques in Computer Science, Berkeley, California, August 1999.
 - International Congress of Mathematicians, Berlin, August 1998.
 - Foundations of Software Technology and Theoretical Computer Science, Kharagpur, December 1997.
 - Workshop in honor of Michael Rabin’s 65th Birthday, Jerusalem, June 1997.
 - Israeli Theory Seminar, Tel Aviv, April 1994 and January 1997.
 - Seminar on Complexity in honor of Shmuel Winograd’s 60th Birthday at IBM Yorktown Heights, May 1996.
 - *20th Theory Day*, Columbia University, 1992.
 - *Bay Area Theory Seminar*, Berkeley, 1990.

Courses taught

Summary

<u>Term</u>	<u>Subject</u>	<u>Title</u>	<u>Role</u>
ST93	*Columbia U.*	Hardness of Approximations	Lectures
FT97	6.046	Analysis of Algorithms	Recitations + Lectures (w. S. Goldwasser)
FT97		Complexity seminar	Seminar (w. S. Goldwasser)
ST98	6.001	Structure and Interpretation of Computer Programs	Recitations
ST98		Complexity seminar	Seminar
FT98	6.966	Algebra and Computation	Lectures + Development
ST99		Complexity seminar	Seminar
FT99	6.893	Approximability of Optimization Problems	Lectures + Development
ST00	6.045	Automata, Computability, and Intractability	Lectures
FT00	6.046	Introduction to Algorithms	Lectures (w. S. Teller)
FT00	6.897	Complexity Seminar	Seminar
ST01	6.046	Introduction to Algorithms	Lectures (w. P. Indyk)
FT01	6.897	Algorithmic Coding Theory	Lectures + Development
ST02	6.841	Advanced Complexity Theory	Lectures
FT02	6.896	Essential Coding Theory	Lectures + Development
ST03	6.841	Advanced Complexity Theory	Lectures
FT04	6.895	Essential Coding Theory	Lectures
ST05	6.841	Advanced Complexity Theory	Lectures
FT05	6.885	Algebra and Computation	Lectures
ST06	6.441	Transmission of Information	Lectures
FT06	6.885	Introduction to Algorithms	Lectures (w. E. Demaine)
ST07	6.841	Advanced Complexity Theory	Lectures
ST07	6.899	Advanced Seminar in Complexity and Cryptography	Seminar

Theses Supervised by Madhu Sudan

Engineer's Theses

- Hon, Kenneth, S., "Design of Prototype Real-Time Broadcast System over the Internet," January 1998.
- Feng, Yuan, "Analysis and Implementation of Generic MPEG Header and Transport Decoders," May 1999.
- Krevat, Elie, "Scheduling Algorithms to improve utilization in Toroidal Interconnected Systems", May 2003.
- Preda, Daniel, "Quantum Communication Complexity Revisited", May 2003.

Master's Theses

- Dodis, Yevgeniy, "Space-Time Tradeoffs for Graph Properties," May 1998.
- Sherman, Alexander, "Distributed Web Caching System with Consistent Hashing," February 1999.
- Guruswami, Venkatesan, "Query-Efficient Checking of Proofs and Improved PCP Characterizations of NP," May 1999.
- Harsha, Praladh, "Small PCPs with low query complexity," May 2000.
- Shelat, Abhi, "Evaluating Grammar-Based Data Compression Algorithm", August 2001.
- Smith, Adam, "Multi-party Quantum Computation", August 2001.
- Grigorescu, Elena, "Local decoding and testing of Homomorphisms", August 2006.
- Kopparty, Swastik, "The list-decoding radius for Reed-Solomon codes," August 2006.

Doctoral Theses, Reader

- Khanna, Sanjeev, "A Structural View of Approximation," Stanford University, August 1996.
- Alimonti, Paola, "Local Search and approximability of MAX SNP problems," University of Rome, September 1997.
- Micciancio, Daniele, "On the Hardness of the Shortest Vector Problem," MIT, September 1998.
- Sahai, Amit, "Frontiers in Zero Knowledge", MIT, September 2000.
- Ramzan, Zufikar, "A Study of Luby-Rackoff Ciphers", MIT, January 2001.
- Reyzin, Leonid, "Zero-knowledge without public keys", MIT, May 2001.
- Nielsen, Rasmus Refslund, "List-decoding of Linear Block Codes", Denmark Technical University, Lyngby, Denmark, November 2001.
- Forster, Jürgen, "Some Results Concerning Arrangements of Half Spaces and Relative Loss Bounds", Universitat Bochum, February 2002.
- Lysyanskaya, Anna, "Signature Schemes and Applications to Cryptographic Protocol Design," May 2002.
- Raskhodnikova, Sofya, "Property Testing: Theory and Applications," May 2003.
- Feldman, Jonathan, "Decoding Error-Correcting Codes via Linear Programming," May 2003.

- Bazzi, Louay, “Error Correcting Codes Minimum Distance versus: Encoding Complexity, Symmetry, and Pseudo-randomness”, August 2003.
- Chan, Albert, “A Framework for Low-Complexity Iterative Interference Cancellation in Communication Systems,” June 2004.
- Newman, Alantha, “Algorithms for String and Graph Layout,” August 2004.
- Immorlica, Nicole, “Computing with Strategic Inputs,” June 2005.
- Kleinberg, Robert David, “Online Decision Problems with Large Strategy Sets,” June 2005.
- shelat, abhi, “Etudes in Zero-Knowledge”, December 2005.
- Bădoiu, Mihai, “Algorithmic Embeddings”, May 2006.
- Pass, Rafael, “A Precise Computational Approach to Knowledge”, May 2006.
- Rademacher, Luis, “Dispersion of Mass and the Complexity of Geometric Problems,” May 2007.
- Kelner, Jonathan A., “New Geometric Techniques for Linear Programming and Graph Partitioning”, (for formal reasons, I was listed as co-advisor at the behest of the principal advisor Dan Spielman, Yale University), MIT, September 2006.
- Akavia, Adi, Expected Summer 2007.

Ph.D. Supervision (Completed)

- Dodis, Yevgeniy, “Exposure-Resilient Cryptography,” MIT, August 2000.
- Guruswami, Venkatesan, “List-decoding of Error-Correcting Codes” MIT, August 2001.
- Lehman, Eric, “Approximation Algorithms for Grammar-based Data Compression”, MIT, January 2002.
- O’Donnell, Ryan William, “Computational Applications of Noise Sensitivity”, MIT, June 2003.
- Alekhnovitch, Mikhail, “Propositional Proof Systems: Efficiency and Automatizability”, MIT, June 2003.
- Smith, Adam Davison, “Maintaining Secrecy when Information Leakage is Unavoidable”, MIT, June 2004.
- Harsha, Prahladh, “Robust PCPs of Proximity and Shorter PCPs”, MIT, August 2004.
- Lehman, April Rasala, “Network Coding”, MIT, January 2005.

Ph.D. Supervision (Current)

- Yekhanin, Sergey, 4th year.
- Chen, Victor, 3rd year.
- Grigorescu, Elena, 3rd year.
- Kopparty, Swastik, 3rd year.
- Juba, Brendan, 2nd year.
- Rossman, Benjamin, 2nd year.

Post-Doctoral Supervision

- Trevisan, Luca: September 1997 - August 1998.
- Vadhan, Salil: September 1999 - August 2000.
- Engebretsen, Lars: September 2000 - August 2001.
- Ben-Sasson, Eli: September 2001 - August 2003.
- Shpilka, Amir: August 2002 - July 2003.
- Chuzhoy, Julia: August 2004 - July 2006.

Publications

1. Books and Book Chapters.

1. Madhu Sudan. **Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems**. ACM Distinguished Theses. Lecture Notes in Computer Science, no. 1001, Springer, 1996.
2. Nadia Creignou, Sanjeev Khanna, and Madhu Sudan. **Complexity Classifications of Boolean Constraint Satisfaction Problems**. SIAM Press, Philadelphia, PA, USA, March 2001.
3. Madhu Sudan. Chapter on “Cryptography” in **Computer Science: Reflections on the Field, Reflections from the Field**, Mary Shaw (Chair), pages 144–150, The National Academies Press, Washington D.C., 2004.
4. Madhu Sudan. Chapter on “Probabilistically checkable proofs”, in **Computational Complexity Theory**, Steven Rudich and Avi Wigderson (Eds.), pages 349–389, IAS/Park City Mathematics Series, volume 10, American Mathematical Society, 2004.
5. Madhu Sudan. Chapter on “Reliable Transmission of Information”, in **Princeton Companion to Mathematics**, Tim Gowers (Ed.), pages ???, Princeton University Press (expected 2007).

2. Papers in refereed journals.

1. Peter Gemmell and Madhu Sudan, “Highly resilient correctors for multivariate polynomials,” *Information Processing Letters*, 43(4): 169–174, September 1992.
2. Marshall Bern, Daniel H. Greene, Arvind Raghunathan, and Madhu Sudan, “Online algorithms for locating checkpoints,” *Algorithmica*, 11(1): 33–52, January 1994.
3. Rajeev Motwani and Madhu Sudan, “Computing roots of graphs is hard,” *Discrete Applied Mathematics*, 54(1):81–88, September 1994.
4. Ronitt Rubinfeld and Madhu Sudan, “Robust characterizations of polynomials with applications to program testing,” *SIAM Journal on Computing*, 25(2):252–271, April 1996.
5. Alok Aggarwal, Amotz Bar-Noy, Don Coppersmith, Rajeev Ramaswami, Baruch Schieber, and Madhu Sudan, “Efficient routing algorithms in optical networks,” *Journal of the ACM*, 43(6):973–1001, November 1996.
6. Andres Albanese, Johannes Blömer, Jeff Edmonds, Michael Luby, and Madhu Sudan, “Priority encoding transmission,” *IEEE Transactions on Information Theory*, Special Issue on Codes and Complexity, 42(6): 1737–1744, November 1996.
7. Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan, “Linearity testing over characteristic two,” *IEEE Transactions on Information Theory*, Special Issue on Codes and Complexity, 42(6): 1781–1795, November 1996.
8. Madhu Sudan, “Decoding of Reed Solomon codes beyond the error-correction bound,” *Journal of Complexity*, special issue dedicated to Shmuel Winograd, 13(1): 180–193, March 1997.
9. Guy Even, Joseph (Seffi) Naor, Baruch Schieber, and Madhu Sudan, “Approximating minimum feedback sets and multicuts in directed graphs,” *Algorithmica*, 20(2): 151–174, February 1998.
10. David Karger, Rajeev Motwani, and Madhu Sudan, “Approximate graph coloring by semidefinite programming,” *Journal of the ACM*, 45(2): 246–265, March 1998.
11. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy, “Proof verification and the hardness of approximation problems,” *Journal of the ACM*, 45(3): 501–555, May 1998.
12. Mihir Bellare, Oded Goldreich, and Madhu Sudan, “Free bits, PCP and non-approximability — towards tight results,” *SIAM Journal on Computing*, 27(3): 804–915, June 1998.
13. Amotz Bar-Noy, Alain Mayer, Baruch Schieber, and Madhu Sudan, “Guaranteeing fair service to persistent dependent tasks,” *SIAM Journal on Computing*, 27(4): 1168–1189, August 1998.

14. Sanjeev Khanna, Rajeev Motwani, Madhu Sudan, and Umesh Vazirani, “On syntactic versus computational views of approximability,” *SIAM Journal on Computing*, 28(1): 164–191, February 1999.
15. Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan, “Reconstructing algebraic functions from mixed data,” *SIAM Journal on Computing*, 28(2): 487–510, April 1999.
16. Benny Chor and Madhu Sudan. “A geometric approach to betweenness,” *SIAM Journal on Discrete Mathematics*, 11(4): 511–523, November 1998.
17. Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, “Private information retrieval,” *Journal of the ACM* 45(6): 965–981, November 1998.
18. Venkatesan Guruswami and Madhu Sudan, “Improved decoding of Reed-Solomon codes and algebraic-geometric codes,” *IEEE Transactions on Information Theory*, 45(6): 1757–1767, September 1999.
19. Oded Goldreich and Madhu Sudan, “Computational indistinguishability: A sample hierarchy,” *Journal of Computer and System Sciences*, 59(2): 253–269, October 1999.
20. Oded Goldreich, Dana Ron, and Madhu Sudan, “Chinese remaindering with errors,” *IEEE Transactions on Information Theory*, 46(4): 1330–1338, July 2000.
21. Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan, “Learning polynomials with queries: The highly noisy case,” *SIAM Journal on Discrete Mathematics*, 13(4): 535–570, November 2000.
22. Prahladh Harsha and Madhu Sudan, “Small PCPs with low query complexity,” *Computational Complexity*, 9(3-4): 157–201, 2000.
23. Luca Trevisan, Gregory B. Sorkin, Madhu Sudan, and David P. Williamson, “Gadgets, approximation, and linear programming,” *SIAM Journal on Computing*, 29(6): 2074–2097, December 2000.
24. Allan Borodin, Jon Kleinberg, Prabhakar Raghavan, Madhu Sudan, and David P. Williamson, “Adversarial queueing theory,” *Journal of the ACM*, 48(1): 13–38, January 2001.
25. Madhu Sudan, Luca Trevisan, and Salil Vadhan, “Pseudorandom generators without the XOR Lemma,” *Journal of Computer and System Sciences*, 62(2): 236–266, March 2001.
26. Sanjeev Khanna, Madhu Sudan, Luca Trevisan, and David P. Williamson, “The approximability of constraint satisfaction problems,” *SIAM Journal on Computing*, 30(6): 1863–1920, March 2001.
27. Venkatesan Guruswami and Madhu Sudan, “On representations of algebraic-geometric codes,” *IEEE Transactions on Information Theory*, 47(4): 1610–1613, May 2001.
28. Yonatan Aumann, Johan Håstad, Michael O. Rabin, and Madhu Sudan, “Linear consistency testing,” *Journal of Computer and System Sciences*, 62(4): 589–607, July 2001.
29. Ronald Fagin, Anna Karlin, Jon Kleinberg, Prabhakar Raghavan, Sridhar Rajagopalan, Ronitt Rubinfeld, Madhu Sudan, and Andrew Tomkins, “Random walks with “Back Buttons”,” *Annals of Applied Probability*, 11(3): 810–862, 2001.
30. Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman, “Combinatorial bounds for list decoding,” *IEEE Transactions on Information Theory*, 48(5):1021–1034, May 2002.
31. Venkatesan Guruswami, Johan Håstad, and Madhu Sudan, “Hardness of approximate hypergraph coloring,” *SIAM Journal on Computing*, 31(6):1663–1686, 2002.
32. Ilya Dumer, Daniele Micciancio, and Madhu Sudan, “Hardness of approximating the minimum distance of a linear code,” *IEEE Transactions on Information Theory*, 49(1):22–37, January 2003.
33. Sanjeev Arora and Madhu Sudan, “Improved low degree testing and its applications,” *Combinatorica*, 23(3):365–426, July 2003.
34. Ari Juels and Madhu Sudan, “A Fuzzy Vault Scheme,” *Designs, Codes and Cryptography*, 38(2):237–257, February 2006.
35. Lars Engebretsen and Madhu Sudan, “Harmonic broadcasting is bandwidth-optimal assuming constant bit rate,” *Networks*, 47(3):172–177, February 2006.

36. Oded Goldreich and Madhu Sudan, “Locally testable codes and PCPs of almost-linear length,” *Journal of the ACM*, **53**(4):558–655, July 2006.
 37. Eli Ben-Sasson and Madhu Sudan, “Robust locally testable codes and products of codes,” *Random Structure and Algorithms*, **28**(4): 387–402, July 2006.
3. Papers in refereed conferences.
1. Marshall Bern, Daniel H. Greene, Arvind Raghunathan, and Madhu Sudan, “Online algorithms for locating checkpoints,” *Proceedings of the Twenty Second Annual ACM Symposium on Theory of Computing*, pages 359–368, Baltimore, Maryland, 14–16 May 1990.
 2. Peter Gemmell, Richard Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson, “Self-testing/correcting for polynomials and for approximate functions,” *Proceedings of the Twenty Third Annual ACM Symposium on Theory of Computing*, pages 32–42, New Orleans, Louisiana, 6–8 May 1991.
 3. Ronitt Rubinfeld and Madhu Sudan, “Self-testing polynomial functions efficiently and over rational domains,” *Proceedings of the Third Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 23–32, Orlando, Florida, 27–29 January 1992.
 4. Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy, “Proof verification and hardness of approximation problems,” *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*, pages 14–23, Pittsburgh, Pennsylvania, 24–27 October 1992.
 5. Sigal Ar, Richard J. Lipton, Ronitt Rubinfeld, and Madhu Sudan, “Reconstructing algebraic functions from mixed data,” *Proceedings of the 33rd Annual Symposium on Foundations of Computer Science*, pages 503–512, Pittsburgh, Pennsylvania, 24–27 October 1992.
 6. Alok Aggarwal, Amotz Bar-Noy, Don Coppersmith, Rajeev Ramaswami, Baruch Schieber, and Madhu Sudan, “Efficient routing and scheduling algorithms for optical networks,” *Proceedings of the Fifth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 412–423, Philadelphia, Pennsylvania, 23–25 January 1994.
 7. Avrim Blum, Prasad Chalasani, Don Coppersmith, Bill Pulleyblank, Prabhakar Raghavan, and Madhu Sudan, “The minimum latency problem,” *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, pages 163–171, Montreal, Quebec, Canada, 23–25 May 1994.
 8. Mihir Bellare and Madhu Sudan, “Improved non-approximability results,” *Proceedings of the Twenty-Sixth Annual ACM Symposium on the Theory of Computing*, pages 184–193, Montreal, Quebec, Canada, 23–25 May 1994.
 9. David Karger, Rajeev Motwani, and Madhu Sudan, “Approximate graph coloring by semidefinite programming,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 2–13, Santa Fe, New Mexico, 20–22 November 1994.
 10. Christos Papadimitriou, Prabhakar Raghavan, Madhu Sudan, and Hisao Tamaki, “Motion planning on a graph,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 511–520, Santa Fe, New Mexico, 20–22 November 1994.
 11. Andres Albanese, Johannes Blömer, Jeff Edmonds, Michael Luby, and Madhu Sudan, “Priority encoding transmission,” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 604–612, Santa Fe, New Mexico, 20–22 November 1994.
 12. Sanjeev Khanna, Rajeev Motwani, Madhu Sudan, and Umesh Vazirani, “On syntactic versus computational views of approximability” *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 819–830, Santa Fe, New Mexico, 20–22 November 1994.
 13. Katalin Friedl and Madhu Sudan, “Some improvements to total degree tests,” *Proceedings of the 3rd Annual Israel Symposium on Theory of Computing and Systems*, pages 190–198, Tel Aviv, Israel, 4–6 January 1995.

14. Amotz Bar-Noy, Alain Mayer, Baruch Schieber, and Madhu Sudan, "Guaranteeing fair service to persistent dependent tasks," Proceedings of the Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 243-252, San Francisco, California, 22-24 January 1995.
15. Benny Chor and Madhu Sudan, "A geometric approach to betweenness," Third European Symposium on Algorithms, Lecture Notes in Computer Science v. 979, pages 227-239, Corfu, Greece, September 1995.
16. Guy Even, Joseph (Seffi) Naor, Baruch Schieber, and Madhu Sudan, "Approximating minimum feedback sets and multicuts in directed graphs," Proceedings of the 4th MPS Conference on Integer Programming and Combinatorial Optimization, Copenhagen, Denmark, Lecture Notes in Computer Science, v. 920, pages 14-24, 29-31 May 1995.
17. Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan, "Private information retrieval," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 41-50, Milwaukee, Wisconsin, 23-25 October 1995.
18. Oded Goldreich, Ronitt Rubinfeld, and Madhu Sudan, "Learning polynomials with queries: The highly noisy case," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 294-303, Milwaukee, Wisconsin, 23-25 October 1995.
19. Mihir Bellare, Oded Goldreich, and Madhu Sudan, "Free bits, PCPs and non-approximability - towards tight results," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 422-431, Milwaukee, Wisconsin, 23-25 October 1995.
20. Mihir Bellare, Don Coppersmith, Johan Håstad, Marcos Kiwi, and Madhu Sudan, "Linearity testing in characteristic two," Proceedings of the 36th Annual Symposium on Foundations of Computer Science, pages 432-441, Milwaukee, Wisconsin, 23-25 October 1995.
21. Allan Borodin, Jon Kleinberg, Prabhakar Raghavan, Madhu Sudan, and David P. Williamson, "Adversarial queueing theory," Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, pages 376-385, Philadelphia, Pennsylvania, 22-24 May 1996.
22. Madhu Sudan, "Maximum likelihood decoding of Reed Solomon codes," Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pages 164-172, Burlington, Vermont, 14-16 October 1996.
23. Luca Trevisan, Gregory B. Sorkin, Madhu Sudan, and David P. Williamson, "Gadgets, approximation, and linear programming," Proceedings of the 37th Annual Symposium on Foundations of Computer Science, pages 617-626, Burlington, Vermont, 14-16 October 1996.
24. Sanjeev Khanna, Madhu Sudan, and David P. Williamson, "A complete classification of the approximability of maximization problems derived from Boolean constraint satisfaction," Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 11-20, El Paso, Texas, 4-6 May 1997.
25. Sanjeev Arora and Madhu Sudan, "Improved low degree testing and its applications," Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing, pages 485-495, El Paso, Texas, 4-6 May 1997.
26. Sanjeev Khanna, Madhu Sudan, and Luca Trevisan, "Constraint satisfaction: The approximability of minimization problems," Proceedings of the 12th Annual IEEE Conference on Computational Complexity, pages 282-296, Ulm, Germany, 24-27 June, 1997.
27. Oded Goldreich and Madhu Sudan, "Computational indistinguishability: A sample hierarchy," Proceedings of the Thirteenth Annual IEEE Symposium on Computational Complexity, pages 24-33, Buffalo, New York, 15-18 June, 1998.
28. Venkatesan Guruswami, Daniel Lewin, Madhu Sudan, and Luca Trevisan, "A tight characterization of NP with 3-query PCPs," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 8-17, Palo Alto, California, 8-11 November, 1998.
29. Madhu Sudan and Luca Trevisan, "Probabilistically checkable proofs with low amortized query complexity," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 18-27, Palo Alto, California, 8-11 November, 1998.

30. Venkatesan Guruswami and Madhu Sudan, "Improved decoding of Reed-Solomon and algebraic-geometric codes," Proceedings of the 39th Annual Symposium on Foundations of Computer Science, pages 28-37, Palo Alto, California, 8-11 November, 1998.
31. Oded Goldreich, Dana Ron, and Madhu Sudan, "Chinese remaindering with errors," Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, pages 225-234, Atlanta, Georgia, 1-4 May 1999.
32. Madhu Sudan, Luca Trevisan, and Salil Vadhan, "Pseudorandom generators without the XOR lemma," Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing, pages 537-546, Atlanta, Georgia, 1-4 May 1999.
33. Yonatan Aumann, Johan Håstad, Michael O. Rabin, and Madhu Sudan, "Linear consistency testing," Randomization, Approximation and Combinatorial Optimization, D. Hochbaum et al. (Eds), Proceedings of the 3rd International Workshop on Randomization and Approximation Techniques in Computer Science, Berkeley, California, 8-11 August 1999, Lecture Notes in Computer Science, vol. 1671, Springer, Berlin, pages 109-120, 1999.
34. Ilya Dumer, Daniele Micciancio, and Madhu Sudan, "Hardness of approximating the minimum distance of a linear code," Proceedings of the 40th Annual Symposium on Foundations of Computer Science, pages 475-484, New York City, New York, 17-19 October, 1999.
35. Venkatesan Guruswami and Madhu Sudan, "List decoding algorithms for certain concatenated codes," Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pages 181-190, Portland, Oregon, 21-23 May 2000.
36. Ronald Fagin, Anna Karlin, Jon Kleinberg, Prabhakar Raghavan, Sridhar Rajagopalan, Ronitt Rubinfeld, Madhu Sudan, and Andrew Tomkins, "Random walks with "Back Buttons"," Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing, pages 484-493, Portland, Oregon, 21-23 May 2000.
37. Venkatesan Guruswami and Madhu Sudan, "On representations of algebraic-geometric codes for list decoding," Proceedings of the 8th Annual European Symposium on Algorithms, pages 244-255, Saarbrücken, Germany, September 5-8, 2000.
38. Venkatesan Guruswami, Johan Håstad, and Madhu Sudan, "Hardness of approximate hypergraph coloring," Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pages 149-158, Redondo Beach, California, 12-14 November, 2000.
39. Venkatesan Guruswami, Amit Sahai, and Madhu Sudan, "'Soft-decision" decoding of Chinese remainder codes," Proceedings of the 41st Annual Symposium on Foundations of Computer Science, pages 159-168, Redondo Beach, California, 12-14 November, 2000.
40. Prahladh Harsha and Madhu Sudan, "Small PCPs with low query complexity," *STACS 2001*, Afonso Ferreira and Horst Reichel (Eds.), Proceedings of the 18th Annual Symposium on Theoretical Aspects of Computer Science, Dresden, Germany, 15-17 February 2001. Lecture Notes in Computer Science, vol. 2010, Springer, Berlin, pages 327-338, 2001.
41. Noga Alon, Venkatesan Guruswami, Tali Kaufman, and Madhu Sudan, "Guessing secrets efficiently via list decoding," Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 254-262, San Francisco, California, 6-8 January 2002.
42. Lars Engebretsen and Madhu Sudan, "Harmonic broadcasting is optimal," Proceedings of the Thirteenth Annual ACM-SIAM Symposium on Discrete Algorithms, pages 431-432, San Francisco, California, 6-8 January 2002.
43. Venkatesan Guruswami and Madhu Sudan, "Decoding concatenated codes using soft information", Proceedings of the Seventeenth Annual IEEE Conference on Computational Complexity, pages 148-157, Montreal, Canada, 21-24 May, 2002.
44. Ari Juels and Madhu Sudan, "A fuzzy vault scheme", Proceedings of the IEEE International Symposium on Information Theory, A. Lapidoth and E. Teletar, Eds., page 408, Lausanne, Switzerland, 30 June - 5 July, 2002.

45. Oded Goldreich and Madhu Sudan, “Locally testable codes and PCPs of almost-linear length”, Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science, pages 13–22, Vancouver, Canada, 16–19 November, 2002.
46. Don Coppersmith and Madhu Sudan. “Reconstructing curves in three (and higher) dimensional spaces from noisy data.” Proceedings of the Thirty Fifth Annual ACM Symposium on Theory of Computing, pages 136–142, San Diego, California, 9–11 June 2003.
47. Eli Ben-Sasson, Madhu Sudan, Salil Vadhan, and Avi Wigderson. “Randomness-efficient low degree tests and short PCPs via ϵ -biased sets”, Proceedings of the Thirty Fifth Annual ACM Symposium on Theory of Computing, pages 612–621, San Diego, California, 9–11 June 2003.
48. Eli Ben-Sasson, Oded Goldreich, and Madhu Sudan. “Bounds on 2-query codeword testing”, In Sanjeev Arora, Klaus Jansen, Jos D. P. Rolim, Amit Sahai (Eds.): Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 6th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2003 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2003, Princeton, NY, USA, August 24–26, 2003. Lecture Notes in Computer Science 2764 Springer 2003, ISBN 3-540-40770-7, pages 216–227.
49. Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. “Robust PCPs of proximity, shorter PCPs and applications to coding”, Proceedings of the Thirty Sixth Annual ACM Symposium on Theory of Computing, pages 1–10, Chicago, Illinois, June 13–15, 2004.
50. Eli Ben-Sasson and Madhu Sudan. “Robust locally testable codes and products of codes”, In Klaus Jansen, Sanjeev Khanna, Jos D. P. Rolim, and Dana Ron (Eds.): Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 7th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2004 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2004, Radcliffe Institute, Cambridge, MA, USA, August 22–24, 2004, pages 286–297.
51. Silvio Micali, Chris Peikert, Madhu Sudan, and David A. Wilson. Optimal error-correction against computationally bounded noise. Second Annual Theory of Cryptography Conference, pages 1–16, MIT, Cambridge, Massachusetts, February 10–12, 2005.
52. Eli Ben-Sasson and Madhu Sudan. “Simple PCPs with Poly-log Rate and Query Complexity”, Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 266–275, Baltimore, Maryland, May 22–24, 2005.
53. Gagan Aggarwal, Amos Fiat, Andrew Goldberg, Jason Hartline, Nicole Immorlica, and Madhu Sudan. “Derandomization of Auctions”, Proceedings of the Thirty Seventh Annual ACM Symposium on Theory of Computing, pages 619–625, Baltimore, Maryland, May 22–24, 2005.
54. Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. “Short PCPs verifiable in polylogarithmic time”, Proceedings of the Twelfth Annual IEEE Conference on Computational Complexity, pages 120–134, San Jose, California, June 12–15, 2005.
55. Shafi Goldwasser, Madhu Sudan, and Vinod Vaikuntanathan, “Distributed Computing with Imperfect Randomness”, Proceedings of DISC 2005, Cracow, Poland, September 26–29, 2005, Springer Lecture Notes in Computer Science, volume 3724, pages 288–302, 2005.
56. Irit Dinur, Madhu Sudan, and Avi Wigderson, “Robust local testability of tensor products of LDPC codes”, Proceedings of APPROX-RANDOM 2006, Barcelona, Spain, Springer Lecture Notes in Computer Science, vol. 4110, pages 304–315, 2006.
57. Elena Grigorescu, Swastik Kopparty, and Madhu Sudan, “Local decoding and testing for homomorphisms”, Proceedings of APPROX-RANDOM 2006, Barcelona, Spain, Springer Lecture Notes in Computer Science, vol. 4110, pages 375–385, 2006.

4. Invited (unrefereed) papers.

1. Madhu Sudan, “On the role of algebra in the efficient verification of proofs,” Workshop of Algebraic Methods in Complexity Theory (AMCOT), Indian Institute of Mathematical Sciences, Chennai, India, December 1994.
 2. Jonathan Hosking, Edwin Pednault, and Madhu Sudan, “A statistical perspective on data mining,” *Future Generation Computer Systems*, Special Issue on Data Mining, 13(2-3): 117–134, November 1997.
 3. Madhu Sudan, “Decoding Reed-Solomon codes beyond the error-correction diameter,” *Proceedings of the 35th Annual Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, pages 215–224, 29 September – 1 October, 1997.
 4. Madhu Sudan, “Algorithmic issues in coding theory,” *Proceedings of the 17th Annual Conference on Foundations of Software Technology and Theoretical Computer Science*, Kharagpur, India, 18-20 December, 1997. S. Ramesh and G. Sivakumar (Eds.) *Lecture Notes in Computer Science*, 1346:184–199, Springer, Berlin, 1997.
 5. Madhu Sudan, “Probabilistic verification of proofs,” *Proceedings of the International Congress of Mathematicians*, Berlin 1998, August 18–27, *Documenta Mathematica*, Extra Volume ICM 1998, III, 461–470.
 6. Madhu Sudan, “List decoding: Algorithms and applications,” *SIGACT News*, Volume 31, Number 1, pp. 16–27, March 2000 (Whole Number 114).
 7. Madhu Sudan, “List decoding: Algorithms and applications,” *Proceedings of the International Conference IFIP TCS 2000*, Sendai, Japan, 17-19 August, 2000. In *Lecture Notes in Computer Science*, Volume 1872, J. van Leeuwen, O. Watanabe, M. Hagiya, P.D. Mosses, T. Ito (Eds.), Springer, pages 25–41, August 2000.
 8. Venkatesan Guruswami, Johan Håstad, Madhu Sudan, and David Zuckerman, “Combinatorial bounds for list decoding,” *Proceedings of the 38th Annual Allerton Conference on Communication, Control and Computing*, pages 603–612, Monticello, Illinois, 4-6 October, 2000.
 9. Madhu Sudan, “Coding theory: Tutorial & Survey,” *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 36–53, Las Vegas, Nevada, 14-17 October 2001.
 10. Madhu Sudan, “Ideal error-correcting codes: Unifying algebraic and number-theoretic algorithms,” *Proceedings of AAEECC-14, the Fourteenth Symposium on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes*, Melbourne, Australia, 26-30 November 2001. In *Lecture Notes in Computer Science*, Volume 2227, Serdar Boztaş and Igor E. Shparlinksi (Eds.), Springer, pages 36–45, November 2001.
 11. Nadia Creignou, Sanjeev Khanna, and Madhu Sudan, “Complexity classifications of Boolean constraint satisfaction problems”, *SIGACT News*, Volume 32, Number 4, Whole Number 121, *Complexity Theory Column* 34, pages 24-33, December 2001.
 12. Venkatesan Guruswami and Madhu Sudan, “Reflections on “Improved Decoding of Reed-Solomon and Algebraic-Geometric Codes””, *IEEE Information Theory Society Newsletter*, Volume 52, Number 1, ISSN 1059-2362, pages 6-12, March 2002.
 13. Madhu Sudan, “Quick and Dirty Refereeing?”, *Science*, Volume 301, pages 1191–1192, 29 August 2003.
 14. Jaikumar Radhakrishnan and Madhu Sudan, “On Dinur’s proof of the PCP theorem,” *Bulletin of the AMS* (to appear).
 15. Madhu Sudan, “Modelling Errors and Recovery for Communication,” *Proceedings of LATIN 2006*, Valdivia, Chile, Springer *Lecture Notes in Computer Science*, volume 3887, pages 25–25, 2006.
5. Technical reports
1. Milena Mihail and Madhu Sudan, “Connectivity properties of matroids,” Technical Report, Computer Science Division, University of California at Berkeley, CSD-91-662, 1991.

2. Sanjeev Khanna and Madhu Sudan, "The optimization complexity of constraint satisfaction problems," Technical Note, Stanford University, Computer Science Department, CS-TN-96-29, January 1996.
 3. Oded Goldreich, Madhu Sudan, and Luca Trevisan, "From logarithmic advice to single-bit advice," Electronic Colloquium on Computational Complexity (ECCC), TR04-093, November 2004.
6. Seminars: Approximately 180 invited seminars.

Professional Statement

My primary area of research is the study of the complexity of computational problems. My main technical works focus on the design of probabilistic methods for verification of algebraic identities. The ensuing methods have applications to a wide collection of areas including: Program verification, Proof checking, Combinatorial optimization, Coding theory and Complexity theory; and I maintain an active interest in all the above areas. My most significant work in the area of proof checking was in [1] where we gave the first "Probabilistically checkable proof system" (PCP) which allowed a probabilistic verifier to verify proofs of arbitrary mathematical statements by just looking at a constant number of bits of the proof. Specifically, this result showed that mathematical theorems and proofs have a verifier (a computational entity) that has a robust verification guarantee. Every true theorem can be proven so that the verifier always accepts. But incorrect theorems have no proofs that the verifier will accept with probability more than half. And the verifier achieves all this while examining only a constant number of bits of the proof.

The result described above is a fundamental statement about the power of randomness in mathematical logic. Additionally it provides in principle at least, ways in which computer programs can certify they have run correctly: The statement that they have computed the correct output for a given input, is the "theorem"; the proof is derived from the transcript of the program's computations; and the verifier does not need to look at the whole transcript to verify correctness.

However the most important and immediate consequence of the above described result is that it provides powerful insights into our ability to solve central combinatorial optimization problems, approximately. Optimization problems computational problems where the goal is to find schedules of task that minimize some cost or maximize some profit. The PCP construction described above, in a perverse twist of logic, ends up implying that for many well-studied and central optimization problems including versions of the famed Travelling Salesman Problem, finding near-optimal solutions is as hard computationally as finding optimal solutions.

A key technical component in the above-mentioned PCP construction was my prior work on "robust characterizations of polynomial functions" [2], where we gave a "tester", or a highly efficient algorithm, to test the proximity of a multivariate function to the class of polynomials of a specified degree.

In the years since, I have been focusing on all aspects of the above results:

1. The design of efficient methods to verify algebraic identities and the study of the mathematical foundations of such tests.
2. The identification of important parameters in PCPs and design of optimal PCPs with respect to these parameters.
3. Tight (in)-approximability results for central optimization problems and a new look at optimization problems.

The papers [3,4,5] are some of the milestones in these directions of research.

My more recent works have been taking on a new direction: The development of new algorithms for "list-decoding of algebraic codes." This sequence of works started in [6] where we gave a new algorithm to decode a basic and commonly-used family of error-correcting codes, called Reed-Solomon codes. The new algorithm corrected far more errors for codes of low-rate than any of the classical algorithms. Subsequently, in [7], even the requirement that the code be of low-rate was removed. Consequently, we now have algorithms that correct far more errors than the classical methods for every possible choice of the rate parameter (while for no choice of the rate, had there been an improvement since the classical algorithm was developed in 1960). The impact of this work is widespread: It has revitalized interest in algebraic codes with numerous works re-examining their combinatorial performance and improving the efficiency of the various steps of the algorithm given in [7]. Furthermore, numerous applications of this result have been derived in Complexity theory and Cryptography.

The works described above have been recipients of, or cited in various awards. The work on PCPs was first reported in my Ph.D. thesis from U.C. Berkeley and received the ACM Doctoral Dissertation Award (1993).

The research paper where the result was reported (authored with S. Arora, C. Lund, R. Motwani, and M. Szegedy) was a co-recipient for the 2001 Godel Prize awarded by the ACM SIGACT for outstanding journal paper in the field of theoretical computer science. The work on list-decoding was awarded the analogous prize in the information theory community, namely the IEEE Information Theory Paper Prize (2000). The works in this direction are also part of a Ph.D. thesis, by Venkatesan Guruswami at MIT, which is a co-winner of this year's MIT Sprowls Prize (best dissertations in EECS) and is currently a contender for the ACM award. Finally both streams of work were cited in the Nevanlinna Prize that I received this year at the International Congress of Mathematicians. The Nevanlinna Prize is awarded once every four years for outstanding work by a young research in the mathematics of information and computer science (interpreted broadly). The award is patterned after the Fields Medal in mathematics and awarded at the same ceremony.

The works described above have also been covered at varying levels in the popular press. The work on the PCP theorem received coverage from the New York Times, and was then extensively reported in the popular science press including Science, Science News, Discover, New Scientist. The work on error-correction of codes has received mentions in the SIAM News and Science News. There was also some description of the results informally in news reports describing the Nevanlinna Prize (in particular articles in the Hindu, the Indian Express, Salon.com, Science, the Times of India, Asian Age etc. gave some description of the results).

In addition to research in topics described above, I have also spent a fair amount of time and energy disseminating the fruits of our work to the MIT community, the Computer Science Theory community and to the rest of the world. In particular, I have given over a hundred and fifty seminar presentations around the world and have taught over ten courses/mini-courses on Approximation of Optimization Problems, Probabilistic Checking of Proofs, and Coding Theory at leading academic and research institutions around the world (not including the MIT courses). The audiences in these presentations have varied from general university wide audiences focussing on the general undergraduate population, to specialists in theoretical computer science. A high point in these presentations is a two minute clip in a WGBH educational video explaining the role of division in producing error-correcting codes to middle-school math. teachers. I am a strong believer in the power of mathematics when applied judiciously; and believe every intricate form of mathematics has a simple conceptual analog that can and ought to be explained to broad audiences so as to retain their interest in mathematics. Computer science, as the science of information and its manipulation, provides one of the richest domains for the applications of mathematics and this is what I hope to continue to exploit in my research.

I have also been a dedicated teacher at MIT and my course evaluations in "Introduction to Algorithms," (MIT 6.046) as well as "Automata, Computability, and Complexity" (MIT 6.045) reflect this. At the graduate level, I am currently developing three different courses: An introductory course on coding theory, where I am using my "outsider's" perspective to abstract the very high level themes in coding theory and presenting them to entry-level graduate students. I am also developing a course on algebra and its role on computation where I recapitulate main themes in algebra from an algorithmic perspective. Finally, I have been trying to develop an alternate view of combinatorial optimization from the perspective of approximation algorithms, and the study of their complexity. In each one of the cases, my course notes have attracted a fair amount of attention from peers as well as publishers interested in publishing texts based on the same.

References

1. S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy. JACM, 45(3), May 1998.
2. R. Rubinfeld and M. Sudan. SICOMP, 25(2), April 1996.
3. S. Arora and M. Sudan, Combinatorica (to appear).u
4. M. Bellare, O. Goldreich, M. Sudan. SICOMP, 27(3), June 1998.
5. S. Khanna, M. Sudan, L. Trevisan, D. P. Williamson. SICOMP, 30(6): 1863-1920, March 2001.
6. M. Sudan. J. Complexity, 13(1), March 1997.
7. V. Guruswami, M. Sudan. IEEE Transactions on Information Theory, 45(6), September 1999