July 25, 2008

David Zuckerman

Department of Computer Science
University of Texas at Austin
1 University Station C0500
Austin, TX 78712

Email: diz@cs.utexas.edu
URL: http://www.cs.utexas.edu/~diz
Phone: (512) 471-9729
Fax: (512) 471-8885

Research Interests

The role of randomness in computation, pseudorandomness, complexity theory, approximability, coding theory, cryptography, distributed computing, random walks.

Professional Experience

University of Texas at Austin, Department of Computer Science
Professor, September 2003 - present;
Associate Professor (tenured), September 1998 - August 2003;
Assistant Professor, January 1994 - August 1998.

Harvard University, Radcliffe Institute for Advanced Study and DEAS
Radcliffe Fellow, Guggenheim Fellow, and Visiting Scholar, July 2004 - June 2005.

University of California at Berkeley, Computer Science Division
Visiting Scholar and Visiting MacKay Lecturer, January 1999 - December 2000.

Hebrew University of Jerusalem, Institute for Computer Science
Lady Davis Postdoctoral Fellow, October 1993 - December 1993.

Massachusetts Institute of Technology, Laboratory for Computer Science
NSF Mathematical Sciences Postdoctoral Fellow, September 1991 - September 1993.

Education

University of California at Berkeley
Ph.D. in Computer Science, 1991.
Thesis title: Computing Efficiently Using General Weak Random Sources;
Advisor: Umesh V. Vazirani.
AT&T Bell Laboratories Fellowship, NSF Graduate Fellowship.

Harvard University
A.B. in Mathematics, summa cum laude, 1987.

Major Honors and Awards

Guggenheim Fellowship, 2004-05.

Radcliffe Institute for Advanced Study Fellowship, 2004-05.

David and Lucile Packard Fellowship for Science and Engineering, 1996-2006

Alfred P. Sloan Research Fellowship, 1996-2000

NSF Young Investigator Award, 1994-2000

Machtey Award (Best Student Paper Award), FOCS, 1990
Co-winner for "General Weak Random Sources."

William Lowell Putnam Mathematical Competition
1986: Putnam Fellow – scored among top 6 in nation.
1985: Scored 8th highest in nation.

Other Grants

Texas Higher Education Coordinating Board, Advanced Research Projects, 2008-10
Randomness Extraction and Distributed Computing

National Science Foundation, 2006-09
Randomness Extraction and Applications

National Science Foundation, 2003-06
Pseudorandomness, Codes, and Cryptography

National Science Foundation, 2000-04
Pseudorandomness and Fault Tolerance

University Research Institute Summer Research Award, 1994
Investigating Whether Randomness is Necessary for Computation

Editorial Boards

ACM Transactions on Computation Theory, 2008 - present

Theory of Computing, 2005 - present

SIAM Journal on Discrete Mathematics, 2003 - present

Program Committees

23rd Annual IEEE Conference on Computational Complexity (CCC), 2008

46th Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2005

41st Annual IEEE Symposium on Foundations of Computer Science (FOCS), 2000

29th Annual ACM Symposium on Theory of Computing (STOC), 1997

1st International Symposium on Randomization and Approximating Techniques in Computer Science (RANDOM), 1997

11th Annual IEEE Conference on Computational Complexity (CCC), 1996

Organizing Committees

Principal Organizer, DIMACS Workshop *Pseudorandomness and Explicit Combinatorial Constructions*, Rutgers University, October, 1999

4th Annual German-American Frontiers of Science Symposium, 1998

Ph.D. Advisees

Jesse Kamp (Ph.D., 2007), Anindya Patthak (Ph.D., 2007), Anup Rao (Ph.D., 2007), Xin Li (in progress), Raghu Meka (in progress).

Postdocs Sponsored

Tugkan Batu (2003-04), Amnon Ta-Shma (1999-2000), Alex Russell (1997-99).

Courses Taught

Graduate courses
Approximation Algorithms, Combinatorics and Graph Theory, Polynomials and Computation, Pseudorandomness, Pseudorandomness and Cryptography, Randomized Algorithms, Randomness and Computation, Theory of Computation.

Undergraduate courses
Analysis of Programs, Cryptography, Theory of Computation.

Featured Invited Talks

IBM Research/NYU/Columbia Theory Day, April, 2005
"Linear Degree Extractors and the Inapproximability of Max Clique and Chromatic Number."

DIMACS Workshop on Computational Complexity, Entropy, and Statistical Physics, Rutgers University, December, 2001
"Computational Complexity and Entropy."

DIMACS Workshop on Codes and Complexity, Rutgers University, December, 2001
"Codes in Theoretical Computer Science."

6th Scandinavian Workshop on Algorithm Theory, Stockholm, Sweden, July, 1998
"Extractors for Weak Random Sources and their Applications."

Selected Other Invited Talks

BIRS Workshop "Recent Advances in Computational Complexity", Banff, August, 2006
"Deterministic Extractors for Small Space Sources."

SIAM Conference on Discrete Mathematics, Victoria, Canada, June, 2006
"Deterministic Extractors for Small Space Sources."

Visions Lecture, University of Texas at Austin, November, 2004
"Extracting Randomness: Past and Future."

Radcliffe Institute for Advanced Study, Cambridge, October, 2004
"The Power of Randomness in Computation."

IPAM Workshop on Automorphic Forms, Group Theory and Graph Expansion, Los Angeles, February, 2004
"Some Successes and Failures of Algebra in Constructing Extractors."

Complexity Theory Meeting, Oberwolfach, Germany, November, 2000
"Extractors, Codes, and Polynomials."

MacKay Lectures, University of California at Berkeley, February-March, 2000
Three Lectures on Pseudorandomness, Expanders, and Extractors

Complexity Theory Meeting, Oberwolfach, Germany, November, 1998
"Advances in Perfect Information Leader Election."

DIMACS Workshop "Microsurveys in Discrete Probability", Princeton University, June, 1997
"Extractors and their Applications."

Institute for Mathematics and its Applications Workshop on Emerging Applications of Number Theory, Minneapolis, July, 1996
"Constructing Expanders that Beat the Eigenvalue Bound."

AMS Special Session on Probability and Combinatorics, Joint Mathematics Meetings, San Francisco, January, 1995
"Diminishing our Reliance on Randomness in Computation."

Orsay Workshop on Randomized Algorithms, Orsay, France, October, 1994
"Computing With Very Weak Random Sources."

Publications

Randomness Extractors and Applications

- Y. Kalai, X. Li, A. Rao and D. Zuckerman, "Network extractor protocols," *40th Annual IEEE Symposium on Foundations of Computer Science*, 2008.
- A. Rao and D. Zuckerman, "Extractors for three uneven-length sources," *12th International Workshop on Randomization and Computation (RANDOM)*, 2008.
- D. Zuckerman, "Linear degree extractors and the inapproximability of Max Clique and Chromatic Number," *Theory of Computing*, 3 (2007): 103-128. Preliminary version in *38th Annual ACM Symposium on Theory of Computing*, 2006, pp. 681-690.
- J. Kamp, A. Rao, S. Vadhan, and D. Zuckerman, "Deterministic extractors for small space sources," *38th Annual ACM Symposium on Theory of Computing*, 2006, pp. 691-700.
- J. Kamp and D. Zuckerman, "Deterministic extractors for bit-fixing sources and exposure-resilient cryptography," *SIAM Journal on Computing*, 36 (2006): 1231-1247. Preliminary version in *44th Annual IEEE Symposium on Foundations of Computer Science*, 2003, pp. 92-101.
- A. Ta-Shma, D. Zuckerman, and S. Safra, "Extractors from Reed-Muller codes," *Journal of Computer and System Sciences*, 72 (2006): 786-812. Special issue on FOCS 2001. Preliminary version in *42nd Annual IEEE Symposium on Foundations of Computer Science*, 2001, pp. 638-647.
- A. Ta-Shma and D. Zuckerman, "Extractor codes," *IEEE Transactions on Information Theory*, 50 (2004): 3015-3025. Preliminary version in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 193-199.
- A. Ta-Shma, C. Umans, and D. Zuckerman, "Lossless condensers, unbalanced expanders, and extractors," *Combinatorica*, 27 (2007): 213-240. Preliminary version in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 143-152.
- O. Goldreich and D. Zuckerman, "Another proof that BPP $\subseteq$ PH (and more)," *Electronic Colloquium on Computational Complexity*, Technical Report TR97-045, 1997.
- D. Zuckerman, "Randomness-optimal oblivious sampling," *Random Structures & Algorithms*, 11 (1997): 345-367. Preliminary version, entitled "Randomness-optimal sampling, extractors, and constructive leader election," in *28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 286-295.
- A. Srinivasan and D. Zuckerman, "Computing with very weak random sources," *SIAM Journal on Computing*, 28 (1999): 1433-1459. Preliminary version in *35th Annual IEEE Symposium on Foundations of Computer Science*, 1994, pp. 264-275.
- A. Wigderson and D. Zuckerman, "Expanders that beat the eigenvalue bound: explicit construction and applications," *Combinatorica*, 19 (1999): 125-138. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 245-251.
- N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, 52 (1996): 43-52. Special issue on STOC 1993. Preliminary version, entitled "More deterministic simulation in Logspace," in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 235-244.
- D. Zuckerman, "Simulating BPP using a general weak random source," *Algorithmica*, 16 (1996): 367-391. Special issue on randomized algorithms. Preliminary version in *32nd Annual IEEE Symposium on Foundations of Computer Science*, 1991, pp. 79-89.
- D. Zuckerman, "General weak random sources," *31st Annual IEEE Symposium on Foundations of Computer Science*, 1990, pp. 534-543. For journal version, see improved results in "Simulating BPP using a general weak random source."

Other Pseudorandomness and Explicit Constructions

- M. Saks, A. Srinivasan, S. Zhou, and D. Zuckerman, "Low discrepancy sets yield approximate min-wise independent permutation families," *Information Processing Letters*, 73 (2000): 29-32. Preliminary version in *3rd International Workshop on Randomization and Approximation Techniques in Computer Science*, volume 1671 of Springer-Verlag *Lecture Notes in Computer Science*, 1999, pp. 11-15.
- N. Linial, M. Luby, M. Saks, and D. Zuckerman, "Efficient construction of a small hitting set for combinatorial rectangles in high dimension," *Combinatorica*, 17 (1997): 215-234. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 258-267.
- R. Impagliazzo and D. Zuckerman, "How to recycle random bits," *30th Annual IEEE Symposium on Foundations of Computer Science*, 1989, pp. 248-253.

Coding Theory and Compression

- P. Gopalan, A.R. Klivans, and D. Zuckerman, "List-decoding Reed-Muller codes over small fields," *40th Annual ACM Symposium on Theory of Computing*, 2008.
- C.S. Jutla, A.C. Patthak, A. Rudra, and D. Zuckerman, "Testing Low-Degree Polynomials Over Prime Fields," *Random Structures & Algorithms*, to appear. Preliminary version in *45th Annual IEEE Symposium on Foundations of Computer Science*, 2004, pp. 423-432.
- L. Trevisan, S. Vadhan, and D. Zuckerman, "Compression of Samplable Sources," *Computational Complexity*, 14 (2005), pp. 186-227 . Special issue on CCC 2004. Preliminary version in *19th Annual IEEE Conference on Computational Complexity*, 2004, pp. 1-14.
- V. Guruswami, J. Hastad, M. Sudan, and D. Zuckerman, "Combinatorial bounds for list decoding," *IEEE Transactions on Information Theory*, 48 (2002), pp. 1021-1034. Preliminary version in *38th Annual Allerton Conference on Communication, Control, and Computing*, 2000, pp. 603-612.
- L.J. Schulman and D. Zuckerman, "Asymptotically good codes correcting insertions, deletions and transpositions," *IEEE Transactions on Information Theory*, 45 (1999), pp. 2552-2557. Preliminary version in *8th ACM-SIAM Symposium on Discrete Algorithms*, 1997, pp. 669-674.
- J. Blomer, M. Kalfane, M. Karpinski, R. Karp, M. Luby, and D. Zuckerman, "An XOR-based erasure-resilient coding scheme," *ICSI Technical Report No. TR-95-048*, 1995.

Distributed Computing, Cryptography, and Security

- R. Gradwohl, S. Vadhan, and D. Zuckerman, "Random selection with an adversarial majority." In *Proceedings of 26th Annual International Cryptology Conference (CRYPTO)*, Lecture Notes in Computer Science, volume 4117, 2006, pp. 409-426.
- D. Song, D. Zuckerman, and J.D. Tygar, "Expander graphs for digital stream authentication and robust overlay networks," *IEEE Symposium on Security and Privacy*, 2002, pp. 258–270.
- A. Russell, M. Saks, and D. Zuckerman, "Lower bounds for leader election and collective coin-flipping in the perfect information model," *SIAM Journal on Computing*, 31 (2002): 1645-1662. Preliminary version in *31st Annual ACM Symposium on Theory of Computing*, 1999, pp. 339-347.
- A. Russell and D. Zuckerman, "Perfect information leader election in $\log^* n + O(1)$ rounds," *Journal of Computer and System Sciences*, 63 (2001), pp. 612–626. Special issue on FOCS 1998. Preliminary version in *39th Annual IEEE Symposium on Foundations of Computer Science*, 1998, pp. 576-583.
- B. Ghosh, F.T. Leighton, B.M. Maggs, S. Muthukrishnan, C.G. Plaxton, R. Rajaraman, A.W. Richa, R.E. Tarjan, and D. Zuckerman, "Tight analyses of two local load balancing algorithms," *SIAM Journal on Computing*, 29 (1999): 29-64. Preliminary version in *27th Annual ACM Symposium on Theory of Computing*, 1995, pp. 548-558.

- E. Kushilevitz, Y. Mansour, M.O. Rabin, and D. Zuckerman, "Lower bounds for randomized mutual exclusion," *SIAM Journal on Computing*, 27 (1998), pp. 1550-1563. Preliminary version in *25th Annual ACM Symposium on Theory of Computing*, 1993, pp. 154-163.
- O. Goldreich, R. Impagliazzo, L. Levin, R. Venkatesan, and D. Zuckerman, "Security preserving amplification of hardness," *31st Annual IEEE Symposium on Foundations of Computer Science*, 1990, pp. 318-326.

Inapproximability

- D. Zuckerman, "On unapproximable versions of NP-complete problems," *SIAM Journal on Computing*, 25 (1996): 1293-1304. Preliminary version, entitled "NP-complete problems have a version that's hard to approximate," in *8th IEEE Conference on Structure in Complexity Theory*, 1993, pp. 305-312.
- N. Alon, U. Feige, A. Wigderson, and D. Zuckerman, "Derandomized graph products," *Computational Complexity*, 5 (1995), pp. 60-75.

Random Walks on Graphs

- P. Winkler and D. Zuckerman, "Multiple cover time," *Random Structures & Algorithms*, 9 (1996): 403-411.
- D. Zuckerman, "A technique for lower bounding the cover time," *SIAM Journal on Discrete Mathematics*, 5 (1992): 81-87. Preliminary version in *22nd Annual ACM Symposium on Theory of Computing*, 1990, pp. 254-259.
- D. Zuckerman, "On the time to traverse all edges of a graph," *Information Processing Letters*, 38 (1991): 335-337.
- D. Zuckerman, "Covering times of random walks on bounded degree trees and other graphs," *Journal of Theoretical Probability*, 2 (1989): 147-157.

Other Topics

- H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman, "Interaction in quantum communication," *IEEE Transactions on Information Theory*, 53 (2007): 1970-1982. Preliminary version, entitled "Interaction in quantum communication and the complexity of set disjointness," in *33rd Annual ACM Symposium on Theory of Computing*, 2001, pp. 124-133.
- M. Luby, A. Sinclair, and D. Zuckerman, "Optimal speedup of Las Vegas algorithms," *Information Processing Letters*, 47 (1993): 173-180. Preliminary version in *2nd Israel Symposium on Theory of Computing and Systems*, 1993, pp. 128-133.