Scott Aaronson

Assistant Professor
Electrical Engineering and Computer Science
Massachusetts Institute of Technology
Cambridge, MA USA 02139
Room 32-G638
aaronson@csail.mit.edu
www.scottaaronson.com

April 24, 2008

Education

- **University of California, Berkeley (Berkeley, CA), 2000-2004**

  PhD in Computer Science.

  Thesis: *Limits on Efficient Computation in the Physical World.*

  Adviser: Umesh Vazirani.

- **Cornell University (Ithaca, NY), 1997-2000**

  B.Sc. in Computer Science with Honors (Minor in Mathematics).

- **Clarkson University (Potsdam, NY), 1996-1997**

  New York State G.E.D.

Postdoctoral Fellowships

- **University of Waterloo (Waterloo, Ontario), Institute for Quantum Computing, 2005-2007**
- **Institute for Advanced Study (Princeton, NJ), School of Mathematics, 2004-2005**

Awards

- Danny Lewin Best Student Paper Award of ACM Symposium on Theory of Computing for "Lower Bounds for Local Search by Quantum Arguments," 2004.

- Ronald V. Book Best Student Paper Award of IEEE Conference on Computational Complexity for "Limitations of Quantum Advice and One-Way Communication," 2004.
- Ronald V. Book Best Student Paper Award of IEEE Conference on Computational Complexity for "Quantum Certificate Complexity," 2003.
- David J. Sakrison Memorial Prize for PhD thesis (awarded annually for "a truly outstanding piece of research as documented in written form"), UC Berkeley, 2005.
- C. V. Ramamoorthy Distinguished Research Award for "Quantum Lower Bound for the Collision Problem," UC Berkeley, 2002.
- National Science Foundation Graduate Fellowship, UC Berkeley, 2001-2004.
- Telluride Association Residential Scholarship, Cornell University, 1998-2000.

Publications

- S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement, to appear in *Proceedings of IEEE Conference on Computational Complexity*, 2008. arXiv:0804.0802.
- S. Aaronson and A. Wigderson. Algebrization: A new barrier in complexity theory, to appear in *Proceedings of ACM STOC*, 2008. ECCC TR08-005.
- S. Aaronson. Quantum copy-protection, in preparation.
- S. Aaronson and J. Watrous. Closed timelike curves make classical and quantum computing equivalent, in preparation.
- S. Aaronson. The learnability of quantum states, *Proceedings of the Royal Society* A463(2088), 2007. ECCC TR06-106, quant-ph/0608142.
- S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice, *Theory of Computing* 3(7):129-157, 2007. Earlier version in *Proceedings of IEEE Conference on Computational Complexity*, pp. 115–128, 2007. ECCC TR06-055, quant-ph/0604056.
- S. Aaronson. QMA/qpoly is contained in PSPACE/poly: de-Merlinizing quantum protocols, *Proceedings of IEEE Conference on Computational Complexity*, 2006. ECCC TR03-057, quant-ph/0510230.
- S. Aaronson. Oracles are subtle but not malicious, *Proceedings of IEEE Conference on Computational Complexity*, 2006. ECCC TR05-040, cs.CC/0504048.
- S. Aaronson. NP-complete problems and physical reality, *ACM SIGACT News* Complexity Theory Column, March 2005. ECCC TR05-026, quant-ph/0502072.
- S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time, *Proceedings of the Royal Society A*, 461(2063):3473–3482, 2005. ECCC TR05-003, quant-ph/0412187.
- S. Aaronson. Quantum computing and hidden variables, *Physical Review A* 71:032325, March 2005. quant-ph/0408035 and quant-ph/0408119.

- S. Aaronson. The complexity of agreement, *Proceedings of ACM STOC*, pp. 634–643, 2005. ECCC TR04-061.
- S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits, *Physical Review A* 70:052328, 2004. quant-ph/0406196.
- S. Aaronson. Limitations of quantum advice and one-way communication, *Theory of Computing* 1:1–28, 2005. Conference version in *Proceedings of IEEE Conference on Computational Complexity*, pp. 320–332, 2004. quant-ph/0402095.
- S. Aaronson. Is quantum mechanics an island in theoryspace?, *Proceedings of the Växjö Conference* (A. Khrennikov, ed.), 2004. quant-ph/0401062.
- S. Aaronson. Multilinear formulas and skepticism of quantum computing, to appear in *SIAM Journal on Computing*. Earlier version in *Proceedings of ACM STOC*, pp. 118–127, 2004. quant-ph/0311039.
- S. Aaronson. Is P versus NP formally independent?, Computational Complexity Column, *Bulletin of the EATCS* 81, October 2003.
- S. Aaronson. Lower bounds for local search by quantum arguments, *Proceedings of ACM STOC*, pp. 465–474, 2004. ECCC TR03-057, quant-ph/0307149.
- S. Aaronson and A. Ambainis. Quantum search of spatial regions, *Theory of Computing* 1:47–79, 2005. Conference version in *Proceedings of IEEE FOCS*, pp. 200–209, 2003. quant-ph/0303041.
- S. Aaronson. Quantum certificate complexity, *Proceedings of IEEE Conference on Computational Complexity*, pp. 171–178, 2003. quant-ph/0210020.
- S. Aaronson. Quantum lower bound for recursive Fourier sampling, *Quantum Information and Computation (QIC)*, March 2003. quant-ph/0209060.
- S. Aaronson. Book review on *A New Kind of Science* by Stephen Wolfram, *Quantum Information and Computation (QIC)*, September 2002. quant-ph/0206089.
- S. Aaronson. Quantum lower bound for the collision problem, *Proceedings of ACM STOC*, pp. 635–642, 2002. quant-ph/0111102. Extended version (joint with Y. Shi) in *Journal of the ACM*, 51(4):595–605, 2004.
- S. Aaronson. Algorithms for Boolean function query properties, *SIAM Journal on Computing* 32(5):1140–1157, 2003.
- S. Aaronson. Optimal demand-oriented topology for hypertext systems, *Proceedings of ACM SIGIR Conference on Research and Development in Information Retrieval*, pp. 168–177, 1997.

Research Positions

- Perimeter Institute for Theoretical Physics, Waterloo, Canada, Summer 2003 and Summer 2004.
- Hebrew University Computer Science Department, Jerusalem, Israel, Spring 2003.

- Centrum voor Wiskunde en Informatica (CWI), Quantum Computing and Advanced Systems Research Group, Amsterdam, Netherlands, Summer 2002.
- Caltech Institute for Quantum Information, Pasadena, CA, Summer 2001.
- Cornell RoboCup Robotic Soccer Team, Artificial Intelligence Group, Ithaca, NY, 1998–2000.
- Bell Labs Computing Sciences Research Center, Murray Hill, NJ, Summer 2000.
- Bell Labs Optical Physics Research Department, Murray Hill, NJ, Summer 1999.
- Bell Labs Networked Computing Research Department, Murray Hill, NJ, Summer 1998.
- Bell Labs Database Systems Research Department, Murray Hill, NJ, Summer 1997.

Teaching

- 6.080/6.089 "Great Ideas in Theoretical Computer Science," MIT, Spring 2007.
- "Quantum Computing Since Democritus," University of Waterloo, Fall 2006. Designed and taught. See www.scottaaronson.com/democritus.
- "Physics, Philosophy, Pizza," UC Berkeley, Spring 2002. Designed and co-taught (with Allison Coates).

Professional Service

- Program committee, IEEE Conference on Foundations of Computer Science (FOCS) 2008.
- Program committee, Quantum Information Processing (QIP) 2007.
- Program committee, Asian Conference on Quantum Information Science (AQIS) 2007.
- Program committee, ACM Symposium on Theory of Computing (STOC) 2006.
- Program committee, IEEE Conference on Computational Complexity (CCC) 2005.
- Creator of the Complexity Zoo (www.complexityzoo.com), an online encyclopedia of over 460 complexity classes.
- Maintainer of a weblog (www.scottaaronson.com/blog) that is widely read in the theoretical computer science community.