

# Scott Aaronson

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

June 15, 2011

## 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

- Best Paper Award of International Computer Science Symposium in Russia (CSR) for “The Equivalence of Sampling and Searching,” 2011.
- United States PECASE (Presidential Early Career Award for Scientists and Engineers), 2010.

- Junior Bose Teaching Award, MIT, 2009.
- DARPA Young Faculty Award, 2009.
- TIBCO Career Development Chair, MIT, 2009.
- Sloan Research Fellowship, 2009.
- NSF CAREER Award, 2009.
- 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.
- 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.
- 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.

## Research Papers

- 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.
- S. Aaronson. Quantum lower bound for the collision problem, *Proceedings of ACM STOC*, pp. 635–642, 2002. Extended version (joint with Y. Shi) appeared as “Quantum lower bounds for the collision and the element distinctness problems” 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. Quantum lower bound for recursive Fourier sampling, *Quantum Information and Computation (QIC)*, March 2003.
- S. Aaronson. Multilinear formulas and skepticism of quantum computing, *Proceedings of ACM STOC*, pp. 118–127, 2004.
- S. Aaronson. Is quantum mechanics an island in theoryspace?, *Proceedings of the Växjö Conference* (A. Khrennikov, ed.), 2004.
- S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits, *Physical Review A* 70:052328, 2004.

- S. Aaronson. Quantum computing, postselection, and probabilistic polynomial-time, *Proceedings of the Royal Society A*, 461(2063):3473–3482, 2005.
- S. Aaronson. Quantum computing and hidden variables, *Physical Review A* 71:032325, March 2005.
- S. Aaronson. The complexity of agreement, *Proceedings of ACM STOC*, pp. 634–643, 2005.
- 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.
- 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.
- S. Aaronson. Lower bounds for local search by quantum arguments, *SIAM Journal on Computing* 35(4):804–824, 2006. Conference version in *Proceedings of ACM STOC*, pp. 465–474, 2004.
- S. Aaronson. QMA/qpoly is contained in PSPACE/poly: de-Merlinizing quantum protocols, *Proceedings of IEEE Conference on Computational Complexity*, pp. 261–273, 2006.
- S. Aaronson. Oracles are subtle but not malicious, *Proceedings of IEEE Conference on Computational Complexity*, pp. 340–354, 2006.
- S. Aaronson. The learnability of quantum states, *Proceedings of the Royal Society A* 463(2088), 2007.
- S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice, *Theory of Computing* 3(7):129–157, 2007. Conference version in *Proceedings of IEEE Conference on Computational Complexity*, pp. 115–128, 2007.
- S. Aaronson. Quantum certificate complexity, *Journal of Computer and System Sciences* 74(3):313–322, 2008. Conference version in *Proceedings of IEEE Conference on Computational Complexity*, pp. 171–178, 2003.
- S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement, *Theory of Computing* 5(1):1–42, 2009. Conference version in *Proceedings of IEEE Conference on Computational Complexity*, pp. 223–236, 2008.
- N. Harrigan, T. Rudolph, and S. Aaronson. Representing probabilistic data via ontological models, submitted, 2009.
- S. Aaronson. On perfect completeness for QMA, *Quantum Information and Computation (QIC)* 9:81–89, 2009.
- S. Aaronson and J. Watrous. Closed timelike curves make classical and quantum computing equivalent, *Proceedings of the Royal Society A*, 465:631–647, 2009.
- S. Aaronson and A. Wigderson. Algebrization: A new barrier in complexity theory, *ACM Transactions on Computing Theory* (inaugural paper), 1(1):2, 2009. Conference version in *Proceedings of ACM STOC*, pp. 731–740, 2008.
- S. Aaronson. Quantum copy-protection and quantum money, *Proceedings of IEEE Conference on Computational Complexity*, pp. 229–242, 2009.

- A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and P. Shor. Breaking and making quantum money: toward a new quantum cryptographic protocol, *Proceedings of Innovations in Computer Science (ICS)*, pp. 20–31, 2010.
- S. Aaronson, F. Le Gall, A. Russell, and S. Tani. The one-way communication complexity of group membership, submitted, 2010.
- S. Aaronson and A. Drucker. A full characterization of quantum advice, *Proceedings of ACM STOC*, pp. 131–140, 2010.
- S. Aaronson. BQP and the polynomial hierarchy, *Proceedings of ACM STOC*, pp. 141–150, 2010.
- S. Aaronson and D. van Melkebeek. A note on circuit lower bounds from derandomization, 2010.
- S. Aaronson and A. Ambainis. The need for structure in quantum speedups, *Proceedings of Innovations in Computer Science (ICS)*, pp. 338–352, 2011.
- S. Aaronson and A. Arkhipov. The computational complexity of linear optics, *Proceedings of ACM STOC*, 2011.
- S. Aaronson. The equivalence of sampling and searching, *Proceedings of Computer Science in Russia (CSR)*, pp. 1–14, 2011.
- S. Aaronson and A. Drucker. Advice coins for classical and quantum computation, to appear in *Proceedings of ICALP*, 2011.
- S. Aaronson. A linear-optical proof that the permanent is  $\#P$ -hard, to appear in *Proceedings of the Royal Society A*, 2011.
- S. Aaronson. A counterexample to the Generalized Linial-Nisan Conjecture, submitted, 2011.
- S. Aaronson. Impossibility of succinct quantum proofs for collision-freeness, submitted, 2011.
- S. Aaronson and E. Dechter. Pretty-good quantum state tomography, in preparation.
- S. Aaronson, D. Chen, and D. Gottesman. Learning and random generation of stabilizer states, in preparation.
- S. Aaronson and A. Drucker. Transfer principles between Boolean and arithmetic complexity, in preparation.
- S. Aaronson and P. Christiano. Quantum money based on conjugate measurements, in preparation.

## Books, Expository Writing, and Reviews

- S. Aaronson. Book review on *A New Kind of Science* by Stephen Wolfram, *Quantum Information and Computation (QIC)*, September 2002. [quant-ph/0206089](http://quant-ph/0206089).
- S. Aaronson. Is P versus NP formally independent?, Computational Complexity Column, *Bulletin of the EATCS* 81, October 2003.

- S. Aaronson. NP-complete problems and physical reality, *ACM SIGACT News Complexity Theory Column*, March 2005. ECCC TR05-026, quant-ph/0502072.
- S. Aaronson. Review of *The Access Principle* by John Willinsky, *ACM SIGACT News* 38(4):19–23, 2007.
- S. Aaronson. The limits of quantum computers, *Scientific American*, March 2008.
- S. Aaronson. Why quantum chemistry is hard, *Nature Physics News & Views*, 5(10):707-708, 2009.
- S. Aaronson. QIP=PSPACE breakthrough (technical perspective), *Communications of the ACM*, 53(12):101, 2010.
- S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and A. Lutomirski. Quantum money, to appear in *Communications of the ACM*.
- S. Aaronson. *Quantum Computing Since Democritus* (working title), to be published by Cambridge University Press.

## 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

- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2011.
- 6.845 Quantum Complexity Theory, MIT, Fall 2010.
- 6.045 Automata, Computability, and Complexity Theory (with Nancy Lynch), MIT, Spring 2010.
- 6.045 Automata, Computability, and Complexity Theory (with Nancy Lynch), MIT, Spring 2009.
- 6.896 Quantum Complexity Theory, MIT, Fall 2008.

- 6.080/6.089 Great Ideas in Theoretical Computer Science, MIT, Spring 2008.
- “Quantum Computing Since Democritus,” University of Waterloo, Fall 2006.
- “Physics, Philosophy, Pizza” (with Allison Coates), UC Berkeley, Spring 2002.

## MIT Service

- Theory of Computing Colloquium Organizer, 2008–2011.
- EECS Graduate Admissions Committee, 2007–2011.
- EECS Doctoral Dissertation Awards Committee, 2010.
- Undergraduate Advisor and Hall Sponsor, 2008–2010.
- Lecturer in Quantum Information Science Summer School, 2009 and 2010.

## Students

- **PhD:** Aleksandr Arkhipov (in progress), Andrew Drucker (in progress), Michael Forbes (in progress).
- **Undergraduate Research Opportunities Program (UROP):** Aleksandr Arkhipov, Asilata Bapat, Valery Brobbey, David Chen, Edwin Chen, Eyal Dechter, William Fefferman, Michael Forbes, Christopher Granade, Leonid Grinberg, Ye Wang, Louis Wasserman.

## Professional Service

- Timeline Coordinator for MIT150 Celebration, 2011.
- Conference committee (elected member), Conference on Computational Complexity (CCC), 2008–2011.
- Program committee, Innovations in Computer Science (ICS) 2011.
- Program committee, IEEE Conference on Foundations of Computer Science (FOCS) 2010.
- Program committee, Quantum Information Processing (QIP) 2009.
- 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](http://www.complexityzoo.com)), an online encyclopedia of over 460 complexity classes.