Scott Aaronson

David J. Bruton Centennial Professor of Computer Science
Department of Computer Science
The University of Texas at Austin
Austin, TX USA
aaronson@cs.utexas.edu
www.scottaaronson.com

January 31, 2017

Education

- **Cornell University (Ithaca, NY), 1997-2000**
  B.Sc. in Computer Science with Honors (Minor in Mathematics).
- **University of California, Berkeley (Berkeley, CA), 2000-2004**
  PhD in Computer Science.
  Thesis: *Limits on Efficient Computation in the Physical World.*
  Adviser: Umesh Vazirani.

Postdoctoral Fellowships

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

Faculty Positions

- **Department of Electrical Engineering and Computer Science, MIT (Cambridge, MA), 2007-2016.** Began as Assistant Professor in Fall 2007; promoted to Associate Professor with Tenure in Spring 2013.
- **Department of Computer Science, University of Texas at Austin (Austin, TX), 2016-.** Began as Full Professor (David J. Bruton Centennial Chair) in Fall 2016.

Awards

- National Science Foundation Graduate Fellowship, UC Berkeley, 2001-2004.
- C. V. Ramamoorthy Distinguished Research Award for "Quantum Lower Bound for the Collision Problem," UC Berkeley, 2002.
- Ronald V. Book Best Student Paper Award of IEEE Conference on Computational Complexity for "Quantum Certificate Complexity," 2003.
- Ronald V. Book Best Student Paper Award of IEEE Conference on Computational Complexity for "Limitations of Quantum Advice and One-Way Communication," 2004.
- Danny Lewin Best Student Paper Award of ACM Symposium on Theory of Computing for "Lower Bounds for Local Search by Quantum Arguments," 2004.
- 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.
- NSF CAREER Award, 2009.
- Sloan Research Fellowship, 2009.
- TIBCO Career Development Chair, MIT, 2009.
- DARPA Young Faculty Award, 2009.
- Junior Bose Teaching Award, MIT, 2009.
- United States PECASE (Presidential Early Career Award for Scientists and Engineers), 2010.
- Best Paper Award of International Computer Science Symposium in Russia (CSR) for "The Equivalence of Sampling and Searching," 2011.
- Alan T. Waterman Award of the National Science Foundation, 2012–2016.
- It from Qubit: Simons Collaboration on Quantum Fields, Gravity, and Information, 2015–.
- Vannevar Bush Faculty Fellowship (previously National Security Science and Engineering Faculty Fellowship), US Department of Defense, 2016–.

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* A463(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 and A. Drucker. A full characterization of quantum advice, *SIAM Journal on Computing* 43(3):1131–1183, 2014. Conference version in *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, F. Le Gall, A. Russell, and S. Tani. The one-way communication complexity of group membership, *Chicago Journal of Theoretical Computer Science* Article 6, 2011.
- S. Aaronson and D. van Melkebeek. On circuit lower bounds from derandomization, *Theory of Computing* 7(1):177–184, 2011.
- S. Aaronson and A. Ambainis. The need for structure in quantum speedups, *Theory of Computing* 10:133–166, 2014. Conference version in *Proceedings of Innovations in Computer Science (ICS)*, pp. 338–352, 2011.
- S. Aaronson and A. Arkhipov. The computational complexity of linear optics, *Theory of Computing* 4:143-252, 2013. Conference version in *Proceedings of ACM STOC*, pp. 333–342, 2011.
- S. Aaronson. The equivalence of sampling and searching, *Theory of Computing Systems* 55(2):281–298, 2014. Conference version in *Proceedings of Computer Science in Russia (CSR)*, pp. 1–14, 2011.
- S. Aaronson and A. Drucker. Advice coins for classical and quantum computation, *Proceedings of ICALP*, pp. 61–72, 2011.
- S. Aaronson. A linear-optical proof that the permanent is #P-hard, *Proceedings of the Royal Society A*, 467:3393–3405, 2011.
- S. Aaronson. Impossibility of succinct quantum proofs for collision-freeness, *Quantum Information and Computation (QIC)* 12:21–28, 2012.
- S. Aaronson and P. Christiano. Quantum money from hidden subspaces, *Theory of Computing* 9(9):349-401, 2013. Conference version in *Proceedings of ACM STOC*, pp. 41–60, 2012.
- M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. Ralph, and A. G. White. Photonic boson sampling in a tunable circuit, *Science* 339(6121):794-798, February 2013.

- S. Aaronson, A. Bouland, L. Chua, and G. Lowther. Psi-epistemic theories: The role of symmetry, *Physical Review A* 88:032111, 2013.
- S. Aaronson and T. Hance. Generalizing and derandomizing Gurvits's approximation algorithm for the permanent, *Quantum Information and Computation*, 14(7-8):541-559, 2014.
- A. Bouland and S. Aaronson. Generation of universal linear optics by any beam splitter, *Physical Review A* 89:062316, 2014.
- S. Aaronson, R. Impagliazzo, and D. Moshkovitz. AM with multiple Merlins, *Proceedings of IEEE Conference on Computational Complexity*, pp. 44–55, 2014.
- S. Aaronson, A. Ambainis, K. Balodis, and M. Bavarian. Weak parity, *Proceedings of ICALP,* pp. 26–38, 2014.
- S. Aaronson and A. Arkhipov. BosonSampling is far from uniform, *Quantum Information and Computation*, 14(15-16):1383–1423, 2014.
- J. Barry, D. Barry, and S. Aaronson. Quantum POMDPs, *Physical Review A* 90:032311, 2014.
- S. Aaronson and H. Nguyen. Near invariance of the hypercube, *Israel Journal of Mathematics* 212(1):385–417, 2016.
- S. Aaronson, S. Carroll, V. Mohan, L. Ouellette, and B. Werness. Quantifying the rise and fall of complexity in closed systems: the coffee automaton, under revision.
- S. Aaronson and A. Ambainis. Forrelation: A problem that optimally separates quantum from classical computing, *Proceedings of ACM STOC*, pp. 307–316, 2015.
- R. Gross and S. Aaronson. Bounding the seed length of Miller and Shi's unbounded randomness expansion protocol, arXiv:1410.8019.
- S. Aaronson, A. Bouland, J. Fitzsimons, and M. Lee. The space "just above" BQP, *Proceedings of ACM Conference on Innovations in Theoretical Computer Science (ITCS)*, pp. 271–280, 2016.
- S. Aaronson, D. Grier, and L. Schaefer. The classification of reversible bit operations, submitted, 2016.
- A. Nayebi, S. Aaronson, A. Belovs, and L. Trevisan. Quantum lower bound for inverting a permutation with advice, *Quantum Information & Computation* 15(11-12):901-913, 2015.
- Z. Liu, C. Perry, Y. Zhu, D. Koh, and S. Aaronson. Doubly infinite separation of quantum information and communication, *Phys. Rev. A* 93:012347, 2016.
- S. Aaronson and D. J. Brod. BosonSampling with lost photons, *Phys. Rev. A* 93:012335, 2016.
- S. Aaronson, S. Ben-David, and R. Kothari. Separations in query complexity using cheat sheets, *Proceedings of ACM STOC*, 2016.
- S. Aaronson, A. Ambainis, J. Iraids, M. Kokainis, and J. Smotrovs. Polynomials, quantum query complexity, and Grothendieck's inequality, *Proceedings of Conference on Computational Complexity*, 2016.

- S. Aaronson and S. Ben-David. Sculpting quantum speedups, *Proceedings of Conference on Computational Complexity*, 2016.
- A. Yedidia and S. Aaronson. A relatively small Turing machine whose behavior is independent of set theory, *Complex Systems* 25(4), 2016.
- E. Demaine, F. Ma, A. Schvartzman, E. Waingarten, and S. Aaronson. The fewest clues problem, *Proceedings of International Conference on Fun with Algorithms (FUN)*, 2016.
- N. Roquet, A. P. Soleimany, A. C. Ferris, S. Aaronson, and T. K. Lu. Synthetic recombinase-based state machines in living cells, *Science* 353(6297), 2016.
- S. Aaronson, M. Bavarian, and G. Gueltrini. Computability theory of closed timelike curves, submitted, 2017.
- S. Aaronson, A. Bouland, G. Kuperberg, and S. Mehraban. The computational complexity of ball permutations, submitted, 2017.
- S. Aaronson and L. Chen. Complexity-theoretic foundations of quantum supremacy experiments, submitted, 2017.

Books

- S. Aaronson. *Quantum Computing Since Democritus*, Cambridge University Press, 2013.

Expository Writing and Reviews

- S. Aaronson. Book review on *A New Kind of Science* by Stephen Wolfram, *Quantum Information and Computation (QIC)*, September 2002.
- 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.
- 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. Quantum computing promises new insights, not just supermachines, *The New York Times*, December 5, 2011.

- S. Aaronson, E. Farhi, D. Gosset, A. Hassidim, J. Kelner, and A. Lutomirski. Quantum money, *Communications of the ACM* 55(8):84–92, August 2012.
- S. Aaronson. Why philosophers should care about computational complexity, in *Computability: Gödel, Turing, Church, and Beyond*, edited by B. J. Copeland, C. Posy, and O. Shagrir, MIT Press, 2013.
- S. Aaronson. The ghost in the quantum Turing machine, in *The Once and Future Turing*, edited by S. Barry Cooper and Andrew Hodges, Cambridge University Press, 2016.
- S. Aaronson. Read the fine print, *Nature Physics* 11:291–293, 2015.
- S. Aaronson. The complexity of quantum states and transformations: from quantum money to black holes, Barbados Lecture Notes, 2016.
- S. Aaronson. $\mathsf{P} \stackrel{?}{=} \mathsf{NP}$, in *Open Problems in Mathematics*, edited by John Nash and Michail Rassias, Springer, 2016.

Teaching

- "Physics, Philosophy, Pizza" (with Allison Coates), UC Berkeley, Spring 2002.
- "Quantum Computing Since Democritus," University of Waterloo, Fall 2006.
- 6.080/6.089 Great Ideas in Theoretical Computer Science, MIT, Spring 2008.
- 6.896 Quantum Complexity Theory, MIT, Fall 2008.
- 6.045 Automata, Computability, and Complexity Theory (with Nancy Lynch), MIT, Spring 2009.
- 6.045 Automata, Computability, and Complexity Theory (with Nancy Lynch), MIT, Spring 2010.
- 6.845 Quantum Complexity Theory, MIT, Fall 2010.
- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2011.
- 6.893 Philosophy and Theoretical Computer Science, MIT, Fall 2011.
- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2012.
- 6.845 Quantum Complexity Theory, MIT, Fall 2012.
- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2013.
- 6.845 Quantum Complexity Theory, MIT, Fall 2014.
- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2015.
- 6.S899 Seminar on Computation and Physics, MIT, Fall 2015.
- 6.045 Automata, Computability, and Complexity Theory, MIT, Spring 2016.
- CS395T Quantum and Classical Complexity Theory, UT Austin, Fall 2016.
- CS378 Introduction to Quantum Information Science, UT Austin, Spring 2017.

Students and Postdocs

- **PhD students:** Andrew Drucker (2008–2012; now an Assistant Professor at University of Chicago), Michael Forbes (2009–2014; now an Assistant Professor at the University of Illinois, Urbana-Champaign), Aleksandr Arkhipov (2010–), Adam Bouland (2011–), Luke Schaeffer (2013–), Daniel Grier (2013–), Saeed Mehraban (2014–).
- **Postdoctoral fellows:** Thomas Vidick (2011–2013; now an Assistant Professor at Caltech), Alexander Belov (2014; now a researcher at the University of Latvia), Thomas Wong (2016–, to become an Assistant Professor at Creighton University), Zak Webb (2016–), Supartha Podder (2016–).
- **Postdoctoral fellows jointly supervised with quantum information group:** Avinatan Hassidim (2008–2010), Xiaodi Wu (2013–), Lior Eldar (2014–), Robin Kothari (2014–).

Professional Service

- Creator of the Complexity Zoo (www.complexityzoo.com), an online encyclopedia of over 500 complexity classes.
- Program committee, IEEE Conference on Computational Complexity (CCC) 2005.
- Program committee, ACM Symposium on Theory of Computing (STOC) 2006.
- Program committee, Asian Conference on Quantum Information Science (AQIS) 2007.
- Program committee, Quantum Information Processing (QIP) 2007.
- Program committee, IEEE Conference on Foundations of Computer Science (FOCS) 2008.
- Conference committee (elected member), Conference on Computational Complexity (CCC), 2008–2011.
- Program committee, Quantum Information Processing (QIP) 2009.
- Program committee, IEEE Conference on Foundations of Computer Science (FOCS) 2010.
- Program committee, Innovations in Computer Science (ICS) 2011.
- Program committee, IEEE Conference on Foundations of Computer Science (FOCS) 2014.
- Program committee, Quantum Information Processing (QIP) 2016.
- Program committee, Innovations in Theoretical Computer Science (ITCS) 2017.