Research Statement

Gregory Rosenthal

November 12, 2024

My research is in quantum complexity theory, especially the complexity of *transformations between quantum states*. These are operations that classical computers fundamentally cannot perform, since the input and/or output may be a superposition of many different bit-strings. In contrast, traditionally quantum complexity theorists have studied the resources required to compute Boolean functions (which are a special type of transformation between quantum states) on quantum computers, as compared with the resources required to do so on classical computers.

Some motivating examples are as follows. Feynman's [Fey82] original impetus for the idea of quantum computers was to simulate the Hamiltonian evolution of physical systems. The goal in Gibbs state preparation [Con+23] is to output the equilibrium state of such a system at a given temperature. Quantum input states may come directly from nature rather than from human-generated data, for example in quantum state tomography [BCG13] or when decoding Hawking radiation from black holes [HH13]. A recent line of work [Kre21; LMW24; BHHP24; MH24] (surveyed in *Quanta Magazine* [Bru24]) suggests that it may be possible to base cryptography on transformations between quantum states, without relying on traditional cryptographic assumptions about Boolean functions. Even when the end goal is to compute a Boolean function, commonly used subroutines of quantum algorithms include state transformations such as Linear Combinations of Unitaries (LCU) [BCK15; CW12] and quantum error-correction [LB13].

Traditionally quantum state transformations have been studied on an ad hoc basis; my PhD thesis [**Ros23**] and recent work of other authors [Aar16; BEMPQY23] were among the first to propose a unified complexity theory for these types of problems. Below I discuss several directions of my research within this theme. Citations to my own papers are in boldface font.

1 The unitary synthesis problem

Aaronson and Kuperberg [AK07] asked whether questions about the complexity of quantum state transformations reduce to (generally better understood) questions about the complexity of Boolean functions. More formally, does it hold that for all physically realizable transformations U between quantum states, there exists a Boolean function f such that the task of (approximately) implementing U efficiently reduces to that of computing f? This question was named the "unitary synthesis problem" by Aaronson [Aar16] and also has implications in quantum cryptography [LMW24].

I gave the best known (albeit still exponential-complexity) algorithm for the unitary synthesis problem, along with a matching lower bound on the complexity for a restricted class of algorithms that generalizes the approach underlying my above upper bound [**Ros21b**]. The only other known lower bound says that at least two sequential quantum queries to f are necessary, unless the input or output of f is exponentially long [LMW24]. Additionally, for problems with *classical* input and quantum output, I gave a computationally efficient algorithm using just one quantum query to a Boolean function [**Ros24**]; previous algorithms required either polynomially many queries [Aar16] or exponential circuit size to perform the non-query operations [INNRY22].

Open problems I'm also interested in variants of the unitary synthesis problem that might be easier to resolve. For example, one may ask whether a *specific* transformation U (such as those used by Aaronson [Aar16; Aar21] to motivate the unitary synthesis problem) efficiently reduces to some Boolean function. One result of this nature is due to Irani, Natarajan, Nirkhe, Rao, and Yuen [INNRY22], who gave an efficient construction of QMA witness states using one query to a PP oracle, and asked whether the PP oracle can be replaced with a QMA oracle.

2 Quantum circuit complexity

The field of circuit complexity seeks to prove lower bounds on the size of any Boolean circuit that computes a given function. This is notoriously difficult (indeed, it might prove $\mathsf{P} \neq \mathsf{NP}$) so researchers instead seek lower bounds in weaker circuit classes such as circuits with low depth (i.e. with few layers of gates). Low-depth circuits model fast parallel computation, and this is especially important when the computation is quantum because quantum states decohere over time.

Concretely, AC^0 is a low-depth Boolean circuit class and QAC^0 is its quantum analogue [GHMP02]. AC^0 circuits famously require exponential size to compute the parity function [Hås86], but it is not even obvious that *arbitrarily large* QAC^0 circuits can compute parity: the reason QAC^0 circuits cannot directly simulate AC^0 circuits is that Boolean circuits can copy the input bits and the outputs of gates for free whereas quantum circuits cannot. In fact, making copies of a bit is *equivalent* to computing parity up to a low-complexity QAC^0 reduction [GHMP02], which further motivates the question of whether parity is in QAC^0.

I proved the only known upper bound for this question, specifically that exponentially large QAC^0 circuits can (approximately) compute parity. Additionally I proved that this upper bound is optimal for a certain subclass of QAC^0 that generalizes the circuit from my upper bound, and that QAC^0 circuits require at least linear size and depth at least 3 to approximate parity [**Ros21a**]. The relation to the theme of this document is that the above proofs all go through an equivalence between parity and the task of constructing a certain quantum state that I introduced. My results complement a line of previous and subsequent work on QAC^0 lower bounds for parity [GHMP02; FFGHZ06; Ber11; PFGT20; NPVY24], culminating in a slightly superlinear size lower bound [ADOY24].

Shannon [Sha49] and Lupanov [Lup58] proved that most functions from n bits to 1 bit require Boolean circuit size roughly $2^n/n$, which motivates the search for explicit functions with this property. I [**Ros21b; Ros23; Ros24**] and others (see e.g. refs. [Kni95; NC10; STYYZ23; CDSSBZ22; ZLY22; GDASC23; YZ23; GKW24]) proved quantum analogues of this result, for different circuit models and complexity measures and types (classical or quantum) of the input and output.

Open problems I'd be happy to prove new QAC^0 lower bounds for *any* task. I'm also interested in low-depth quantum circuit classes beyond QAC^0. For example, QAC^0 circuits with parity gates can compute majority [HŠ05; TT16] and vice versa [GM24], but can they simulate the rest of QNC^1 (or at least NC^1)? Does QNC^1 equal $\mathsf{BQP/poly}$? On the easier side—potentially suited to an undergraduate—there are still some open problems regarding quantum Shannon–Lupanov bounds.

3 Interactive state synthesis

The complexity class IP (for "interactive proof") is the multi-round analogue of NP, capturing languages which can be verified by a multi-round exchange of messages between a randomized polynomial-time verifier and an unbounded-complexity prover. The famous $\mathsf{IP} = \mathsf{PSPACE}$ theorem [LFKN92; Sha92] implies that interactive proofs are quite powerful, since PSPACE is widely believed to include problems outside of P and even outside of NP. An analogous statement $\mathsf{QIP} = \mathsf{PSPACE}$ [JJUW11] holds when the verifier is quantum, even with just three messages [Wat03].

Henry Yuen and I proposed a model of quantum interactive proofs where the goal is to *produce a quantum state* rather than compute a Boolean function. Here the verifier accepts or rejects, and when accepting also outputs a quantum state; if the prover is honest then the verifier should accept, and regardless of whether the prover is honest the output state conditioned on accepting should be (approximately) correct. We proved that $\mathsf{statePSPACE} \subseteq \mathsf{stateQIP}$, where these classes are defined analogously to PSPACE and QIP respectively [**RY22**], and later I showed that six messages suffice for this [**Ros24**]. Other authors proved the converse inclusion $\mathsf{stateQIP} \subseteq \mathsf{statePSPACE}$ [MY23], gave a zero-knowledge version of our protocol (with cryptographic applications) [BKS23; CMS23], and studied the analogous class $\mathsf{stateQMA}$ with just one message [DGLM23].

Open problems The above results concern computational problems with *classical* input and quantum output; can we generalize them to problems with *quantum* input? Henry Yuen and I [**RY22**] and others [BEMPQY23] have already made some preliminary steps in this direction. Also, the error in the above protocols is polynomially small; can it be made exponentially small?

4 Quantum channel testing

How many queries to a quantum state transformation $\mathcal{M}$ (called a *channel*) are necessary to test whether it is equal to or far from some known channel $\mathcal{N}$? For example, due to the unreliability of near-term quantum hardware, one may fear that a physical device designed to implement $\mathcal{N}$ actually implements a completely different channel $\mathcal{M}$. Previous work [FFGO23] studied this question with respect to a *worst-case* distance between $\mathcal{M}$ and $\mathcal{N}$ (formally, the diamond norm distance) defined by the maximum error over all possible input states. However, as I showed in joint work with Hugo Aaronson, Sathyawageeswar Subramanian, Animesh Datta, and Tom Gur, worst-case error is unnecessarily stringent for many applications and makes channel testing prohibitively difficult; therefore we introduced an *average-case* distance between channels, generalizing previously studied average-case distances between specific types of channels, and proved several results to begin the study of channel testing and learning in this average-distance [**RASDG24**].

Open problems Can we give a complete answer to the question posed at the beginning of the previous paragraph, as a function of $\mathcal{N}$? (Or at least, for some physically motivated channels $\mathcal{N}$ for which the works mentioned above didn't already answer this question?) Such "instance optimality" results are already known for the special case of quantum *state* testing with unentangled measurements [CLO22; CLHL22]. With entangled measurements, optimal bounds for quantum state testing are proved using Schur-Weyl duality [OW21], and I'm interested in generalizing this approach to channel testing. I'm also interested in proving *any* nontrivial bound on the quantum circuit complexity of the measurement associated with Schur-Weyl duality, with the hope of making the associated state testing algorithms more physically realistic. Finally, does an analogue of the quantum fault-tolerance theorem hold for this average-case distance between channels (instead of diamond norm distance)?

References

[Aar16] Scott Aaronson. "The complexity of quantum states and transformations: from quantum money to black holes". 2016. arXiv: 1607.05256.

[Aar21] Scott Aaronson. "Open problems related to quantum query complexity". In: *ACM Transactions on Quantum Computing* 2.4 (2021), pp. 1–9. URL: https://www.scottaaronson.com/papers/open.pdf.

[ADOY24] Anurag Anshu, Yangjing Dong, Fengning Ou, and Penghui Yao. "On the Computational Power of QAC0 with Barely Superlinear Ancillae". In: (2024). arXiv: 2410.06499.

[AK07] Scott Aaronson and Greg Kuperberg. "Quantum versus classical proofs and advice". In: *Theory Comput.* 3.7 (2007), pp. 129–157. DOI: 10.4086/toc.2007.v003a007. arXiv: quant-ph/0604056.

[BCG13] Konrad Banaszek, Marcus Cramer, and David Gross. "Focus on quantum tomography". In: *New Journal of Physics* 15.12 (2013), p. 125020. DOI: 10.1088/1367-2630/15/12/125020.

[BCK15] Dominic W. Berry, Andrew M. Childs, and Robin Kothari. "Hamiltonian simulation with nearly optimal dependence on all parameters". In: *FOCS*. 2015, pp. 792–809. DOI: 10.1109/FOCS.2015.54. arXiv: 1501.01715.

[BEMPQY23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. "Unitary Complexity and the Uhlmann Transformation Problem". In: (2023). arXiv: 2306.13073.

[Ber11] Debajyoti Bera. "A lower bound method for quantum circuits". In: *Inform. Process. Lett.* 111.15 (2011), pp. 723–726. DOI: 10.1016/j.ipl.2011.05.002.

[BHHP24] John Bostanci, Jonas Haferkamp, Dominik Hangleiter, and Alexander Poremba. "Efficient Quantum Pseudorandomness from Hamiltonian Phase States". In: (2024). arXiv: 2410.08073.

[BKS23] James Bartusek, Dakshita Khurana, and Akshayaram Srinivasan. "Secure Computation with Shared EPR Pairs (Or: How to Teleport in Zero-Knowledge)". In: (2023). arXiv: 2304.10480.

[Bru24] Ben Brubaker. *Cryptographers Discover a New Foundation for Quantum Secrecy*. Quanta Magazine. June 3, 2024. URL: https://www.quantamagazine.org/cryptographers-discover-a-new-foundation-for-quantum-secrecy-20240603/.

[CDSSBZ22] B David Clader, Alexander M Dalzell, Nikitas Stamatopoulos, Grant Salton, Mario Berta, and William J Zeng. "Quantum resources required to block-encode a matrix of classical data". In: *IEEE Transactions on Quantum Engineering* 3 (2022), pp. 1–23. arXiv: 2206.03505.

[CLHL22] Sitan Chen, Jerry Li, Brice Huang, and Allen Liu. "Tight Bounds for Quantum State Certification with Incoherent Measurements". In: *FOCS*. IEEE, 2022, pp. 1205–1213. DOI: 10.1109/FOCS54457.2022.00118. arXiv: 2204.07155.

[CLO22] Sitan Chen, Jerry Li, and Ryan O'Donnell. "Toward Instance-Optimal State Certification With Incoherent Measurements". In: *COLT*. Vol. 178. Proceedings of Machine Learning Research. PMLR, 2022, pp. 2541–2596. DOI: 10.48550/arXiv.2102.13098. URL: https://proceedings.mlr.press/v178/chen22b.html.

[CMS23] Léo Colisson, Garazi Muguruza, and Florian Speelman. "Oblivious Transfer from Zero-Knowledge Proofs, or How to Achieve Round-Optimal Quantum Oblivious Transfer and Zero-Knowledge Proofs on Quantum States". In: (2023). arXiv: 2303.01476.

[Con+23] Mirko Consiglio, Jacopo Settino, Andrea Giordano, Carlo Mastroianni, Francesco Plastina, Salvatore Lorenzo, Sabrina Maniscalco, John Goold, and Tony JG Apollaro. "Variational gibbs state preparation on NISQ devices". In: (2023). arXiv: 2303.11276.

[CW12] Andrew M. Childs and Nathan Wiebe. "Hamiltonian simulation using linear combinations of unitary operations". In: *Quantum Inf. Comput.* 12.11-12 (2012), pp. 901–924. DOI: 10.5555/2481569.2481570. arXiv: 1202.5822.

[DGLM23] Hugo Delavenne, François Le Gall, Yupan Liu, and Masayuki Miyamoto. "Quantum Merlin-Arthur proof systems for synthesizing quantum states". In: (2023). arXiv: 2303.01877.

[Fey82] Richard P. Feynman. "Simulating physics with computers". In: vol. 21. 6-7. Physics of computation, Part II (Dedham, Mass., 1981). 1982, pp. 467–488. DOI: 10.1007/BF02650179. URL: https://doi.org/10.1007/BF02650179.

[FFGHZ06] Maosen Fang, Stephen Fenner, Frederic Green, Steven Homer, and Yong Zhang. "Quantum lower bounds for fanout". In: *Quantum Inf. Comput.* 6.1 (2006), pp. 46–57. arXiv: quant-ph/0312208.

[FFGO23] Omar Fawzi, Nicolas Flammarion, Aurélien Garivier, and Aadil Oufkir. "Quantum Channel Certification with Incoherent Measurements". In: *Conference on Learning Theory (COLT)*. Vol. 195. Proceedings of Machine Learning Research. PMLR, 2023, pp. 1822–1884. DOI: 10.48550/arXiv.2303.01188. URL: https://proceedings.mlr.press/v195/fawzi23a.html.

[GDASC23] Kaiwen Gui, Alexander M Dalzell, Alessandro Achille, Martin Suchara, and Frederic T Chong. "Spacetime-Efficient Low-Depth Quantum State Preparation with Applications". In: (2023). arXiv: 2303.02131.

[GHMP02] Frederic Green, Steven Homer, Cristopher Moore, and Christopher Pollett. "Counting, fanout, and the complexity of quantum ACC". In: *Quantum Inf. Comput.* 2.1 (2002), pp. 35–65. arXiv: quant-ph/0106017.

[GKW24] David Gosset, Robin Kothari, and Kewen Wu. "Quantum State Preparation with Optimal T-Count". In: (2024). arXiv: 2411.04790.

[GM24] Daniel Grier and Jackson Morris. "Quantum Threshold is Powerful". In: (2024). arXiv: 2411.04953.

[Hås86] Johan Håstad. "Almost optimal lower bounds for small depth circuits". In: *STOC*. 1986, pp. 6–20. DOI: 10.1145/12130.12132.

[HH13] Daniel Harlow and Patrick Hayden. "Quantum computation vs. firewalls". In: *J. High Energy Phys.* 6 (2013), 085, front matter+55. DOI: 10.1007/JHEP06(2013)085. URL: https://doi.org/10.1007/JHEP06(2013)085.

[HŠ05] Peter Høyer and Robert Špalek. "Quantum fan-out is powerful". In: *Theory Comput.* 1.5 (2005), pp. 81–103. DOI: 10.4086/toc.2005.v001a005.

[INNRY22] Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. "Quantum search-to-decision reductions and the state synthesis problem". In: *CCC*. Vol. 234. 2022, 5:1–5:19. DOI: 10.4230/lipics.ccc.2022.5. arXiv: 2111.02999.

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. "QIP = PSPACE". In: *J. ACM* 58.6 (2011), pp. 1–27. DOI: 10.1145/2049697.2049704. arXiv: 0907.4737.

[Kni95] Emanuel Knill. "Approximation by quantum circuits". In: (1995). arXiv: quant-ph/9508006.

[Kre21] William Kretschmer. "Quantum pseudorandomness and classical complexity". In: (2021). arXiv: 2103.09320.

[LB13] Daniel A. Lidar and Todd A. Brun. *Quantum Error Correction*. Cambridge University Press, 2013. URL: www.cambridge.org/9780521897877.

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. "Algebraic methods for interactive proof systems". In: *J. ACM* 39.4 (1992), pp. 859–868. DOI: 10.1145/146585.146605.

[LMW24] Alex Lombardi, Fermi Ma, and John Wright. "A one-query lower bound for unitary synthesis and breaking quantum cryptography". In: *STOC*. 2024, pp. 979–990. arXiv: 2310.08870.

[Lup58] Oleg Lupanov. "On a method of circuit synthesis". In: *Izvestia VUZ* 1 (1958), pp. 120–140. DOI: 10.2307/2271493.

[MH24] Fermi Ma and Hsin-Yuan Huang. "How to Construct Random Unitaries". In: (2024). arXiv: 2410.10116.

[MY23] Tony Metger and Henry Yuen. "stateQIP= statePSPACE". 2023. arXiv: 2301.07730.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667.

[NPVY24] Shivam Nadimpalli, Natalie Parham, Francisca Vasconcelos, and Henry Yuen. "On the Pauli Spectrum of QAC0". In: *STOC*. 2024, pp. 1498–1506. arXiv: 2311.09631.

[OW21] Ryan O'Donnell and John Wright. "Learning and testing quantum states via probabilistic combinatorics and representation theory". In: *Current Developments in Mathematics* 2021.1 (2021), pp. 43–94. DOI: 10.4310/CDM.2021.v2021.n1.a2. URL: https://www.cs.cmu.edu/~odonnell/papers/learning-quantum-states.pdf.

[PFGT20] Daniel Padé, Stephen Fenner, Daniel Grier, and Thomas Thierauf. "Depth-2 QAC circuits cannot simulate quantum parity". 2020. arXiv: 2005.12169 [quant-ph].

[RASDG24] Gregory Rosenthal, Hugo Aaronson, Sathyawageeswar Subramanian, Animesh Datta, and Tom Gur. "Quantum Channel Testing in Average-Case Distance". 2024. arXiv: 2409.12566.

[Ros21a] Gregory Rosenthal. "Bounds on the QAC^0 Complexity of Approximating Parity". In: *ITCS*. Vol. 185. 2021, 32:1–32:20. DOI: 10.4230/LIPIcs.ITCS.2021.32. arXiv: 2008.07470.

[Ros21b] Gregory Rosenthal. "Query and Depth Upper Bounds for Quantum Unitaries via Grover Search". 2021. arXiv: 2111.07992.

[Ros23] Gregory Rosenthal. "Quantum state and unitary complexity". PhD thesis. University of Toronto, 2023. URL: https://www.cs.toronto.edu/~rosenthal/thesis.pdf.

[Ros24] Gregory Rosenthal. "Efficient Quantum State Synthesis with One Query". In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. 2024, pp. 2508–2534. DOI: 10.1137/1.9781611977912. arXiv: 2306.01723.

[RY22] Gregory Rosenthal and Henry Yuen. "Interactive Proofs for Synthesizing Quantum States and Unitaries". In: *ITCS*. Vol. 215. 2022, 112:1–112:4. DOI: 10.4230/LIPIcs.ITCS.2022.112. arXiv: 2108.07192.

[Sha49] Claude Shannon. "The synthesis of two-terminal switching circuits". In: *Bell System Tech. J.* 28 (1949), pp. 59–98. DOI: 10.1002/j.1538-7305.1949.tb03624.x.

[Sha92] Adi Shamir. "$\mathsf{IP} = \mathsf{PSPACE}$". In: *J. ACM* 39.4 (1992), pp. 869–877. DOI: 10.1145/146585.146609.

[STYYZ23] Xiaoming Sun, Guojing Tian, Shuai Yang, Pei Yuan, and Shengyu Zhang. "Asymptotically optimal circuit depth for quantum state preparation and general unitary synthesis". In: *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* (2023). DOI: 10.1109/TCAD.2023.3244885. arXiv: 2108.06150.

[TT16] Yasuhiro Takahashi and Seiichiro Tani. "Collapse of the hierarchy of constant-depth exact quantum circuits". In: *Comput. Complexity* 25.4 (2016), pp. 849–881. DOI: 10.1007/s00037-016-0140-0. arXiv: 1112.6063.

[Wat03] John Watrous. "PSPACE has constant-round quantum interactive proof systems". In: *Theoret. Comput. Sci.* 292.3 (2003), pp. 575–588. DOI: 10.1016/S0304-3975(01)00375-9.

[YZ23] Pei Yuan and Shengyu Zhang. "Optimal (controlled) quantum state preparation and improved unitary synthesis by quantum circuits with any number of ancillary qubits". In: *Quantum* 7 (2023), p. 956. DOI: 10.22331/q-2023-03-20-956. arXiv: 2202.11302.

[ZLY22] Xiao-Ming Zhang, Tongyang Li, and Xiao Yuan. "Quantum state preparation with optimal circuit depth: Implementations and applications". In: *Physical Review Letters* 129.23 (2022), p. 230504. DOI: 10.1103/PhysRevLett.129.230504. arXiv: 2201.11495.