Candidate Project Topics

In the following, [AMC] refers to lecture notes of Andrew M. Childs, available here, and the references therein. A *single numbered paragraph* should be enough scope for one project. As a general rule, more points will be given for depth than for breadth.

The references below are generally to arXiv versions of these papers. You can sometimes find videos of talks on these papers by Googling their titles: videos sometimes convey the key ideas more quickly. You may use the references below as guides to the topic but write about *other* works (not appearing below) on the topic if you find them more interesting or accessible.

More commentary on a topic does *not* mean I prefer that topic more. It is also entirely okay to pursue a topic *outside* this list; though, in that case, I encourage you to discuss the topic with me first (by email or during office hours). If you'd like more information about any topic from below, please let me know.

Quantum circuit synthesis

1. *Solovay-Kitaev theorem.* This theorem shows that arbitrary unitaries can be approximately synthesized using a sequence of elementary quantum gates chosen from any finite set satisfying mild conditions. For an accessible proof of this result, see [AMC, Section 2]. Solve Problem 1 here to understand why the approximation can also be found efficiently. Recent developments on this topic include [Bouland and Giurgica-Tiron, 21] and [Kuperberg, 23].

2. *Clifford + T synthesis.* In practice, unitaries are often synthesized using Clifford + T gates. See [AMC, Section 3].

Quantum algorithms

I chose the following topics for their potential for *super-quadratic* quantum speedups. There are significantly more quantum algorithms that yield sub-quadratic speedups. While algorithms of the latter type often involve many beautiful ideas and their theoretical speedup is more secure, they may be much further away from real-world applications (say, ten years or more, see [Babbush et al.]). We will also cover some of them in class. Therefore, I decided to omit them in the following.

1. *Quantum algorithms for algebraic problems.* Study one or two sections from [AMC, Chapter 2] that look interesting to you. That chapter overlaps with [Childs and van Dam, 08].

2. *Quantum algorithms for lattice problems.* New cryptographic standards for online security rest on the hardness of lattice problems – see NIST announcement from Aug. 24. Therefore, you will become the next Peter Shor if you find an efficient quantum algorithm for solving lattice problems. A known approach goes via the dihedral hidden subgroup problem [Regev, 03]. Notable recent works include [Liu, 23], [Eldar and Hallgren, 22] (this work has received significant pushback, see, e.g., [Cryptography StackExchange]), [Chen, Liu, and Zhandry, 21], [Cramer, Ducas, Peikert, and Regev, 16] (motivated by work of the British spy agency). A recent attempt to break lattice cryptography that failed: [Chen, 24], what went wrong?

3. *Improved quantum algorithm for factoring.* We will cover Shor's algorithm in class, which factors an n-digit number by using a quantum circuit involving $\sim n^2$ gates. [Regev, 23] found an improved algorithm that uses a quantum circuit involving only $\sim n^{1.5}$ gates. [Ragavan, Vaikuntanathan, 23] shows a further space saving.

4. *Exponential quantum speedups for graph problems.* [Childs, Cleve, Deotto, Farhi, and Gutmann, and Spielman, 02] shows that a quantum algorithm can find the "exit" in a maze-like graph much faster than any classical algorithm. More recently, [Childs, Coudron, and Gilani, 22] studies whether the algorithm can also output the path it took. [Li and Tong, 24] shows how a quantum algorithm can find a path between some vertices in some graphs fast. [Ben-David, Childs, Gilyén, Kretschmer, Podder, and Wang, 20] shows that the input data structure of the graph is crucial to the question of exponential quantum speedup.

5. *Quantum algorithms for ground states.* The ground state of a quantum system is its lowest energy state and can be used to understand key properties of the system. [Lin and Tong, 20] describes a near-optimal algorithm for preparing the ground state *given* an approximation to it (so-called guiding state). [Gharibian and Le Gall, 21] studies this problem from a computational complexity perspective. If you're not given a guiding state, then this problem is hard (QMA-hard) even for a quantum computer. But there are still things you can do, see, e.g., [Chen, Huang, Preskill, and Zhou, 23]. Is there a way to claim large quantum advantage without going via BQP-completeness? This is a tricky question since classical algorithms can be very good too, see, e.g., [Chan, 24] and [Lee et al., 22].

6. *Quantum algorithms for preparing Gibbs states.* A quantum system described by Hamiltonian rests in its ground state at temperature $T = 0$. For $T > 0$, the system rests in the so-called Gibbs state. Latest works include [Bakshi, Liu, Moitra, and Tang, 24] and [Rouzé, Stilck França, Alhambra, 24] (covered in Quanta article).

7. *Quantum simulation algorithms.* These are algorithms that simulate the time evolution of quantum systems themselves. This was the original application envisaged for quantum computers by [Feynman, 82]. This video gets you up to speed about recent developments.

8. *Quantum algorithms for differential equations.* Quantum simulation algorithms evolve a quantum state following the Schrödinger equation $i\hbar \frac{d}{dt} |\psi\rangle = H |\psi\rangle$. Quantum algorithms can also be used to perform evolution under more general differential equations. Some notable recent works include [An, Liu, and Lin, 23], [Babbush, Berry, Kothari, Somma, and Wiebe, 23], [Liu et al., 20]. Also see [Linden, Montanaro, and Shao, 20] for commentary on the caveats of claiming large quantum speedup for some quantum algorithms for differential equations.

9. *Yamakawa-Zhandry problem.* [Yamakawa and Zhandry, 22] describes a new type of problem that admits a provable exponential quantum advantage in the query model. The problem was originally motivated as a "proof-of-quantumness" but has since been related to problems in optimization [Jordan et al., 24] and complexity theory [Jain, Li, Robere, and Xun, 24].

10. *Optimization via quantum dynamics.* Classical optimizers often face trouble when the optimization landscape has many local minima. Recent proposals for quantum optimizers seek to overcome this issue by using quantum effects such as quantum tunneling. See, e.g., [Liu, Su, and Li, 23], [Leng, Zheng, and Wu, 23] and [Leng, Hickman, Li, and Wu, 23]. Also see [Zhang and Li, 21] (not quantum) and [Zhang, Leng, and Li, 21] for escaping saddle points.

11. *Quantum neural networks, or variational quantum algorithms.* Despite early promise, there is growing pessimism surrounding quantum neural networks. See [Cerezo et al., 24] and [Anschuetz, 24] that summarize the current situation. Is there a way around the pessimism?

Limitations of quantum algorithms in the query model

1. *Total Boolean functions.* A total Boolean function is a function of the form $f\colon \{0,1\}^n \to \{0,1\}$. Using a beautiful pure math result [Huang, 19], [Aaronson, Ben-David, Kothari, Rao, and Tal, 20] showed $D(f) \leq O(Q(f)^4)$ for such f. This is tight by [Ambainis, Balodis, Belovs, Lee, Santha, and Smotrovs, 15]. Of course, the previous inequality implies $R(f) \leq O(Q(f)^4)$ but whether this is tight is an open problem – see Problem 4 of [Aaronson, 21].

2. *Aaronson-Ambainis conjecture.* Let $f\colon D \subseteq \{0,1\}^n \to \{0,1\}$. This conjecture says that DDTs can simulate quantum query algorithms on most inputs $x \in D$ unless D is much smaller than $\{0,1\}^n$. It can be interpreted as saying that "there can be quantum advantage only for very special problems". The conjecture can be reduced to a purely mathematical result about polynomials. See [Aaronson and Ambainis, 14]. Recent progress on this conjecture includes [Bansal, Sinha, and de Wolf, 22] and [Gutiérrez, 23].

3. *k-distinctness.* This problem asks whether a list contains k locations that contain the same symbol. It lies at the frontier of quantum lower-bound techniques [Bun, Kothari, and Thaler, 17]. You may also study the upper-bound side as part of the project, see, e.g., [Belovs, 12] and [Jeffery and Zur, 22].

4. *Recording queries method.* There are two prevailing methods for proving worst-case quantum query complexity lower bounds: the polynomial and adversary methods. (I plan to cover these in class.) More recently, [Zhandry, 18] introduced an elegant method called the recording queries method that works particularly well for proving average-case quantum query lower bounds, which is particularly relevant for cryptography. This method has been further developed by, e.g., [Majenz, Malavolta, and Walter, 24], [Beame, Kornerup, and Whitmeyer, 24], [Hamoudi and Magniez, 20].

Classical simulation of quantum circuits and dequantization of quantum algorithms

1. *Classical simulation of quantum circuits.* Special classes of quantum circuits can be simulated efficiently classically, e.g., those with Clifford and few T gates [Bravyi and Gosset, 16], matchgates [Jozsa and Miyake, 08], low entanglement [Jozsa and Linden, 02], low tree-width [Markov and Shi, 05], noisy and random [Aharonov, Gao, Landau, Liu, and Vazirani, 22], shallow [Bravyi, Gosset, and Liu, 23], [Coble, and Coudron, 20], [Bravyi, Gosset, Movassagh, 19], etc. Investigate a few of these. Can some of them be combined?

2. *Stabilizer rank.* Motivated by a particular simulation algorithm for Clifford + T circuits [Bravyi and Gosset, 16], significant research has been devoted to lower bounding the stabilizer rank of magic states. See blog post and [Bravyi, Browne, Calpin, Campbell, Gosset, and Howard, 18]. The latest result on this question is [Mehraban and Tahmasbi, 24].

3. *Dequantization of quantum algorithms.* Instead of trying to classically simulate a quantum algorithm gate by gate, we can simply try to obtain the same output as that algorithm. This is known as dequantization. There have been several notable dequantizations; perhaps the most notable is [Tang, 18]. (The author, Ewin Tang, wrote this paper when she was 18). That paper

led to many subsequent dequantizations of quantum machine learning (QML) algorithms relying on Quantum Random Access Memory (QRAM). How does all this square with the BQP-completeness of the proto-typical QML algorithm, the quantum linear systems (or HHL) algorithm of [Harrow, Hassidim, and Lloyd, 09]? You may instead study dequantization of non-QML algorithms, e.g., recently [Begušic, Gray, and Chan, 24] claims to dequantize a quantum algorithm for physics in [Kim et al., 23]. Many so-called "quantum supremacy" algorithms have also been dequantized.

Quantum cryptography

1. *Quantum money.* A physically unclonable form of money, which was the first application of quantum in cryptography. See video for an introduction. (I also plan to cover this later in class.) A key open problem is to construct a *publicly verifiable* form of quantum money, see, e.g., [Zhandry, 24], [Liu, Montgomery, and Zhandry, 22] and [Aaronson and Christiano, 12].

2. *Quantum randomness generation.* Classically, we only know how to generate pseudo-random bits. But quantumly, the CHSH game can be used to generate truly random bits. See popular article and [Miller and Shi, 15].

3. *Device-independent quantum key distribution (QKD).* We will discuss the BB84 QKD protocol in class, but what if you're paranoid and don't trust the devices you're using? [Jain, Miller, and Shi, 18] and [Vazirani and Vidick, 12] (in which the CHSH game again appears).

4. *Classical control of quantum devices.* As weak classical beings, how can we trust the output of a powerful quantum computer? Using cryptography! [Mahadev, 18]: associated Quanta article and overview. You could also focus on a weaker task known as "proof-of-quantumness" in which you just want to trust that the output was generated by something quantum. See, e.g., [Alnawakhtha, Mantri, Miller, and Wang, 24], [Kalai, Lombardi, Vaikuntanathan, Yang, 22], [Kahanamoku-Meyer et al., 21] – all involve the CHSH game.

5. *Certified deletion.* A way for a cloud computer to prove to you that it deleted your information. This is impossible classically as the cloud computer could copy your information and just delete the original. But quantumly, we have the no-cloning principle. See, e.g., work by Bartusek, [Broadbent and Islam, 20], [Miller and Fu, 17].

6. *Minimal assumptions in quantum cryptography.* The minimal assumption for cryptography in a classical world is one-way functions. It is currently unclear what the answer should be in the quantum world that we actually live in. See, e.g., Quanta article, [Brakerski, Canetti, and Qian, 22], [Kretschmer, 21], [Ji, Liu, and Song, 17]

Additional topics

I may add more to these. You may come back to the Overleaf file later to check.

1. MIP* = RE. This is a landmark result in quantum complexity theory by [Ji, Natarajan, Vidick, Wright, and Yuen, 22]. See blog posts 1, 2 (also 2.1 about preceding work [Natarajan and Wright, 19]), and 3. First, understand the meaning of the result. Then understand a high-level overview of the proof strategy. Then dig into the details of one of the key proof components – the first blog post has some pointers on what these are.

2. *Classical learning of quantum states.* Given copies of a quantum state, what's the most efficient way to learn some description of it? See survey by [Anshu and Arunachalam, 23]. Some open questions in that survey have since been resolved, see, e.g., [Bakshi, Liu, Moitra, and Tang, 23].

3. *Classical learning of quantum channels.* Like the previous topic but for quantum channels. Recent work includes, e.g., [Huang and Liu et al., 24] and [Haah, Kothari, O'Donnell, and Tang, 24].