Research Statement

Pei Wu

November 23, 2020

I have broad research interests in theoretical computer science. I am particularly passionate about computational complexity theory for its combination of mathematical depth, extensive and surprising connections to other disciplines, and broad relevance to real-world computing. In my doctoral work, I have focused on query complexity, communication complexity, and analytic measures of complexity. My Ph.D. thesis solves several decades-old problems. In this research statement, I will discuss my contributions to the following questions.

(i) What is the largest possible gap between quantum and randomized query complexity? This 18-year-old problem is broadly recognized as being central to understanding the phenomenon of quantum speedups.

(ii) What is the maximum *threshold degree* of constant-depth circuits? This 50-year-old problem has applications to several areas of theoretical computer science, including communication complexity and learning complexity.

(iii) The study of *interactive coding* started 30 years ago and has since blossomed into a fascinating area of computer science. What is the maximum noise rate that can be tolerated in interactive communication, in the general model of arbitrary substitutions, deletions, and insertions?

In the concluding section of this document, I will describe my vision for future work.

1 Background

Communication complexity. The classical model of two-party communication features two geographically separated parties, Alice and Bob. Alice and Bob have private inputs x and y, respectively, and they need to communicate back and forth to compute a given function $f(x, y)$. This model can be viewed as a powerful generalization of classical information theory, in the sense that information theory studies one-way transmission of information as opposed to interactive communication. Analogous to Shannon's noiseless coding theorem and capacity theorem, the natural questions here are: what is the minimum communication cost for Alice and Bob to compute f, and how does one handle noise if it is present?

Communication complexity theory is of great intrinsic importance because communication is a key resource in computing. Moreover, communication complexity is a powerful tool in studying various other computational models because virtually every computational process involves information flow among two or more components. Indeed, there is a vast body of research applying communication complexity to study computational phenomena as diverse as circuits, streaming algorithms, and computational learning.

Query complexity. In the query model, the task is to evaluate a given function f on an unknown n-bit input x. To access the input, we query an index i of our choice and receive x_i. The goal is to minimize the worst-case number of queries by choosing the query indices strategically.

Even though query complexity is among the simplest computational models, it remains the focus of a large body of research. This is because the query model captures the hardness of many important problems. To illustrate, the vast majority of known quantum algorithms, including Grover's search algorithm and Shor's period finding algorithm, are captured by the query model. In addition, query complexity sheds light on more sophisticated models. For example, it is well known that the query model is closely related to Turing machines with oracles. As another example, there are a variety of *lifting theorems* that make it possible to instantly translate lower bounds for the query model to the vastly more powerful model of communication complexity. This lifting approach has recently enabled the resolution of several important open problems.

2 Quantum versus Classical Computing

Quantum query complexity has been studied extensively and can be justly considered to be among the biggest achievements of quantum computing to date. Of particular prominence in this line of research are results demonstrating the superiority of quantum algorithms over their classical counterparts. I am particularly interested in the bounded-error regime, where the query algorithm is allowed to err with a small constant probability. In groundbreaking work, Simon [15] exhibited a partial Boolean function whose bounded-error quantum query complexity is exponentially smaller than its randomized (i.e., classical) query complexity. This raises the question: what is the largest possible separation between quantum and randomized query complexity? This question was first explicitly stated in 2002 by Buhrman et al. [5], and has since been popularized by Aaronson and Ambainis [1].

We settled this 18-year-old problem completely in [12]. Specifically, we proved that for any constant k, there is a partial function f with quantum query complexity at most k and randomized query complexity $\tilde{\Omega}(n^{1-1/2k})$. This gives an $O(1)$ versus $\Omega(n^{1-\epsilon})$ separation for any $\epsilon > 0$, which is a polynomial improvement on the best previous separation of $O(1)$ versus $\Omega(n^{2/3-\epsilon})$ due to Tal [16]. Moreover, our separation is optimal due to Aaronson and Ambainis' result [1] that any k-query quantum algorithm can be simulated by $O(n^{1-1/2k})$ randomized classical queries, for an arbitrary constant k. By the well-known framework of "cheatsheets" due to Aaronson et al. [2], our result also implies a cubic separation between quantum and randomized query complexity for *total* functions. This separation is the largest known and has been conjectured to be tight by other researchers [3]. As a technical centerpiece of our work [12], we prove a tight bound on the ℓ_1 norm of any given level of the Fourier spectrum of decision trees. This bound on Fourier weight settles a conjecture of Tal [16] and is of substantial interest in its own right, considering the central role of the Fourier spectrum in many recent breakthroughs in the area [7, 8, 10].

Via query-to-communication lifting, our results imply analogous separations for quantum versus randomized *communication* complexity. In particular, our results imply an $O(\log n)$ versus $\Omega(n^{1-\epsilon})$ separation for the quantum versus randomized communication complexity of partial functions, for any $\epsilon > 0$. Our separation is essentially optimal and a polynomial improvement on previous work.

3 Sign-Representation of Boolean Functions

Representations of Boolean functions by real polynomials are of great importance in many different contexts, from communication complexity and quantum computing to machine learning theory. For

example, the notion of *approximate degree* has played an essential role in quantum query complexity for decades. *Threshold degree* has an even broader range of applications, including various models of computational learning. The notion of threshold degree originates in the pioneering work of Minsky and Papert [9] and is defined, for a Boolean function $f : \{0,1\}^n \to \{-1,1\}$, as the minimum degree of a real polynomial p that represents f in sign: $f(x) = \operatorname{sgn} p(x)$ for all x.

In particular, the threshold degree of polynomial-size constant-depth circuits (AC^0) has been the focus of 50 years of work. Together with my advisor, we were able to essentially settle this longstanding problem in [13]. More specifically, we proved that for any $\epsilon > 0$, there is an AC^0 circuit with threshold degree $\Omega(n^{1-\epsilon})$. This lower bound essentially matches the trivial upper bound of $O(n)$ and is a polynomial improvement on the best previous lower bound, $\Omega(\sqrt{n})$. In fact, we proved a much stronger result that applies not only to threshold degree but also to *sign-rank*—a vastly more general notion than threshold degree.

Our results have important applications in communication complexity and learning theory. In communication complexity, our results give the strongest known lower bounds for AC^0, showing the optimality of the trivial protocol where Alice sends her entire input to Bob. Our lower bound holds even if Alice and Bob only need to compute f with an arbitrary nonzero advantage over random guessing. In learning theory, our results rule out the possibility of the distribution-free PAC learning of AC^0 based on the powerful dimension complexity paradigm. This framework captures nearly all known algorithmic results for distribution-free PAC learning.

Our work has been invited to appear in the special issue of *SIAM Journal of Computing* for STOC 2019.

4 Interactive Coding

Noise is omnipresent in communication. In the classical setting of one-way communication, the study of information transmission under noise forms a large part of classical information theory. In pioneering work, Schulman [11] considered noise in the setting of interactive communication. This area of research, called interactive coding, is a fascinating and highly active discipline at the crossroads of information theory and communication complexity. More concretely, consider the following scenario. Alice and Bob would like to execute a communication protocol π defined for a noiseless environment. However, the communication channel is controlled by an adversary who can corrupt any fraction ρ of symbols transmitted through the channel. The question is, can Alice and Bob use some interactive analogue of error-correcting codes to ensure that they are both able to recover, from their noisy communication, the transcript that π would have produced without noise? A far-reaching generalization of this model, proposed by Braverman et al. [4], allows *arbitrary* corruptions: insertions, deletions, and substitutions. For any constant $\epsilon > 0$, the authors of [4] showed how to faithfully simulate any protocol in this generalized model with corruption rate up to $\frac{1}{18} - \epsilon$, using a constant-size alphabet and a constant-factor overhead in communication.

Braverman et al. posed the following natural and fundamental question: what is the maximum corruption rate that can be tolerated in this generalized model of substitutions, insertions, and deletions? We gave a complete answer to this question in [14]. We showed that for any $\epsilon > 0$, there is an interactive coding scheme that uses a constant-size alphabet and achieves noise tolerance $\frac{1}{4} - \epsilon$, at the expense of a constant-factor overhead in communication complexity compared to π. This rate is easily seen to be optimal, even in the presence of substitution errors alone.

5 Future Directions

Theoretical computer science is a young and exceptionally active discipline. I look forward to pursuing my current areas of expertise as well as branching out into new areas of theoretical computer science. In what follows, I mention several of my favorite problems that are closely related to my thesis research.

Polynomials for shallow circuits

Our aforementioned threshold degree result for AC^0 uses circuits whose depth is a large constant. If we turn to extremely shallow circuits, there are many unsettled problems. The only case we understand fully is the trivial case of depth-1 circuits, which are just the AND and OR functions. Analyzing the sign-representation and pointwise approximation of circuits of depth as small as 2 is already very challenging—and very rewarding from the standpoint of applications. For example, a major open problem is to determine the quantum query complexity of *triangle detection*. As a function, triangle detection is easily computable by a depth-2 circuit. Establishing a tight approximate degree lower bound is currently the most promising approach to this fundamental problem.

Quantum query/communication complexity

In the query complexity world, our understanding is now more or less complete: we know that the quantum and randomized query complexity can be arbitrarily separated for partial functions. For total functions, my Ph.D. thesis gives a cubic separation, whereas Aaronson et al. [3] prove that any separation is at most quartic. Closing the gap for total functions is the main unresolved question in this line of work. In the communication world, things are more open, especially for total functions. It is a major open problem to decide if quantum protocols can be super-polynomially more efficient than randomized protocols for total functions. There are several reasons why this problem is so challenging. First, the lifting technique does not apply since quantum and randomized query complexity are polynomially related. Moreover, many canonical lower bound techniques for randomized communication complexity (e.g., approximate rank and the discrepancy method) also lower bound quantum communication complexity.

Two-party communication complexity

Analogous to the structural complexity theory of Turing machines, two-party communication has its own complexity classes: P, BPP, NP, PH. A large number of questions regarding relationships among these complexity classes remain open. For example, in the Turing machine world, we know that BPP lies within the second level of PH and is conjectured to equal P. In the communication world, BPP is also contained in the second level of PH, but the conjecture is that $\text{BPP} \not\subseteq \text{P}^{\text{NP}}$. Recently, Chattopadhyay et al. showed that $\text{BPP} \not\subseteq \text{P}^{\text{GT}}$ [6], where GT is the greater-than function. An ambitious open problem is to prove that $\text{BPP} \not\subseteq \text{P}^{\text{NP}}$, which would give a highly accurate placement of BPP in the polynomial hierarchy. Looking out further, if we consider higher levels of the polynomial hierarchy, we reach the frontier of research in communication complexity. A central and notoriously hard problem in communication complexity is to exhibit functions that are not contained in PH. Currently, it remains open even to prove explicit lower bounds against AM, a subclass of PH.

References

[1] Scott Aaronson and Andris Ambainis. Forrelation: A problem that optimally separates quantum from classical computing. *SIAM J. Comput.*, 47(3):982–1038, 2018.

[2] Scott Aaronson, Shalev Ben-David, and Robin Kothari. Separations in query complexity using cheat sheets. In *Proceedings of the Forty-Eighth Annual ACM Symposium on Theory of Computing* (STOC), pages 863–876, 2016.

[3] Scott Aaronson, Shalev Ben-David, Robin Kothari, and Avishay Tal. Quantum implications of Huang's sensitivity theorem. Available at `https://arxiv.org/abs/2004.13231`, 2020.

[4] Mark Braverman, Ran Gelles, Jieming Mao, and Rafail Ostrovsky. Coding for interactive communication correcting insertions and deletions. *IEEE Trans. Information Theory*, 63(10):6256–6270, 2017.

[5] Harry Buhrman, Lance Fortnow, Ilan Newman, and Hein Röhrig. Quantum property testing. *SIAM J. Comput.*, 37(5):1387–1400, 2008.

[6] Arkadev Chattopadhyay, Shachar Lovett, and Marc Vinyals. Equality alone does not simulate randomness. In *Proceedings of the Thirty-Fourth Annual IEEE Conference on Computational Complexity* (CCC), volume 137 of *LIPIcs*, pages 14:1–14:11, 2019.

[7] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, and Shachar Lovett. Pseudorandom generators from polarizing random walks. In *Proceedings of the Thirty-Third Annual IEEE Conference on Computational Complexity* (CCC), volume 102, pages 1:1–1:21, 2018.

[8] Eshan Chattopadhyay, Pooya Hatami, Omer Reingold, and Avishay Tal. Improved pseudorandomness for unordered branching programs through local monotonicity. In *Proceedings of the Fiftieth Annual ACM Symposium on Theory of Computing* (STOC), pages 363–375, 2018.

[9] Marvin L. Minsky and Seymour A. Papert. *Perceptrons: An Introduction to Computational Geometry*. MIT Press, Cambridge, Mass., 1969.

[10] Ran Raz and Avishay Tal. Oracle separation of BQP and PH. In *Proceedings of the Fifty-First Annual ACM Symposium on Theory of Computing* (STOC), pages 13–23, 2019.

[11] Leonard J. Schulman. Coding for interactive communication. *IEEE Trans. Information Theory*, 42(6):1745–1756, 1996.

[12] Alexander A. Sherstov, Andrey A. Storozhenko, and Pei Wu. An optimal separation of randomized and quantum query complexity, 2020. Available at `https://arxiv.org/abs/2008.10223`. Submitted to STOC 2021.

[13] Alexander A. Sherstov and Pei Wu. Near-optimal lower bounds on the threshold degree and sign-rank of AC^0. In *Proceedings of the Fifty-First Annual ACM Symposium on Theory of Computing* (STOC), pages 401–412, 2019.

[14] Alexander A. Sherstov and Pei Wu. Optimal interactive coding for insertions, deletions, and substitutions. *IEEE Trans. Inf. Theory*, 65(10):5971–6000, 2019. Preliminary version in *Proceedings of the Fifty-Eighth Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2017.

[15] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.

[16] Avishay Tal. Towards optimal separations between quantum and randomized query complexities. In *Proceedings of the Sixty-First Annual IEEE Symposium on Foundations of Computer Science* (FOCS), 2020.